

Exhibit 10

EXHIBIT 10 – INFRINGEMENT CONTENTIONS OF U.S. PATENT NO. 11,916,902

Fortinet provides the disclosures below based on information reasonably available to it as of the date of these disclosures, before Fortinet has received discovery, and before the Court has construed the claims. Further, certain information about Netskope’s accused functionalities relevant to this asserted patent and Fortinet’s infringement contentions is not publicly available to the extent this functionality may be established solely or predominantly through analysis of software, firmware, source code, and/or configurations of the ’902 Accused Products that have not yet been disclosed. Accordingly, Fortinet specifically reserves the right to amend, modify, and/or supplement these contentions in response to Netskope (or third-parties where appropriate) producing non-public documents, software, firmware, source code, and/or configuration files for or related to each of the Accused ’902 Products, as information becomes available including in view of the Court’s findings on claim constructions and/or positions taken by Netskope.

Fortinet contends that each limitation is met directly and/or indirectly, literally and/or under the doctrine of equivalents by the accused functionalities, but reserves the right to supplement these infringement contentions and/or set forth additional infringement theories based on information received in discovery, in view of the Court’s findings on claim constructions, and/or positions taken by Netskope.

The Accused ’902 Products include at least Netskope’s Private Access products (a.k.a., “Zero Trust Network Access” and “ZTNA”) (collectively, “Private Access”) and/or Netskope Secure Web Gateway (a.k.a., “SWG”, “Next Gen Secure Web Gateway,” “NG-SWG”, “Netskope for Web”) (collectively, “SWG”), either or both of which may be hosted in a Netskope NewEdge Network and/or configured within the Netskope One Platform, and the associated features or functions (for example, NSProxy) of these product offerings, in conjunction with Netskope Device Intelligence and/or the Netskope One Client.

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
I[pre]. A method for reducing network threats, the method comprising:	To the extent the preamble is found to be limiting, the Accused ’902 Products perform a method for reducing network threats.

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 516 1057 1472"><p data-bbox="272 1058 321 1465">The Power of One</p><p data-bbox="358 716 451 1465">The major components of the Netskope One platform include:</p><p data-bbox="505 527 1045 1465">The Netskope Zero Trust Engine: Netskope's Zero Trust Engine lies at the heart of the platform, continuously gathering risk telemetry and generating extensive contextual awareness across all users, devices, applications, and data. Unlike other SSE offerings that bypass some types of traffic and services, the Zero Trust Engine decrypts and decodes traffic inline across web and SaaS applications, cloud services, and private applications for the broadest and deepest levels of visibility and protection.</p></div> <p data-bbox="1062 867 1094 1472">2025-03-Netskope-One-Platform-SB-719-5.pdf</p>

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement

What is ZTNA?

Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.

Zero Trust Security Principles

ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.

Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.

Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.

<https://www.netskope.com/security-defined/what-is-zero-trust-network-access>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="250 239 553 1478"> <h2 data-bbox="266 533 331 1478">Netskope One Private Access</h2> <p data-bbox="363 239 526 1478">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p> </div> <div data-bbox="553 611 1289 1478"> <p data-bbox="574 638 802 1451">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="867 638 1273 1451" style="list-style-type: none"> <li data-bbox="867 701 1094 1451">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="1127 638 1273 1451">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications </div> <div data-bbox="1289 212 1370 1478"> <p data-bbox="1289 212 1370 1478">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>1[a]. receiving, by a processing device, a request to access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;</p>	<p>The Accused '902 Products include receiving, by a processing device, a request to access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network.</p> <p>For example, a remote user device running the Netskope One Client (e.g., a known access device) receives a request to access one or more secure private network applications or resources in the Netskope NewEdge Network hosting Netskope Private Access, SWG, or related products, features or functions of the Netskope One Platform (a known private network that authorizes credentials associated with the known access device) associated with the private network. This known access device can be external to the private network—e.g., connected through a public network such as the internet—when the request to access is made to the processing device.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<div data-bbox="272 1020 326 1467"><h2>The Power of One</h2></div> <div data-bbox="367 646 467 1467"><p>The major components of the Netskope One platform include:</p></div> <div data-bbox="529 436 1118 1467"><p>The Netskope Zero Trust Engine: Netskope's Zero Trust Engine lies at the heart of the platform, continuously gathering risk telemetry and generating extensive contextual awareness across all users, devices, applications, and data. Unlike other SSE offerings that bypass some types of traffic and services, the Zero Trust Engine decrypts and decodes traffic inline across web and SaaS applications, cloud services, and private applications for the broadest and deepest levels of visibility and protection.</p></div>	

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="259 367 779 1470"><p>The Netskope NewEdge Network: Netskope's one-of-a-kind network is purpose-built to deliver full compute SSE and SD-WAN. Featuring a global footprint of ultra-fast data centers in 75+ regions, and a local experience for every country, NewEdge is highly elastic, built for scale, and designed to provide cloud-delivered security and networking services directly to where the users and offices are without performance trade-offs.</p></div> <div data-bbox="787 367 1372 1470"><p>The Netskope One Client: Netskope's endpoint agent unifies remote user access to web, cloud, and private apps, alongside data protection and voice and video optimization at the endpoint by converging SWG, CASB, ZTNA, FWaaS, DLP, and SD-WAN. Easy to use, lightweight, and deployed to perform at a high throughput, it delivers a single agent footprint for SASE and zero trust use cases, greatly simplifying desktop administration for a better user experience.</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 382 920 1474"><p>The Netskope One Gateway: The Netskope One Gateway, offers both hardware and virtual form factors and supports the widest range of deployment options, including cellular gateways, micro to large branch, data center and multi-cloud environments. Netskope One Gateway consolidates disjointed appliances into one unified SASE gateway. It offers multiple services like Routing, WiFi, SD-WAN, App FW, IPS, IoT Device Intelligence, DEM and Edge compute, along with a seamless on-ramp to Netskope One SSE.</p></div> <div data-bbox="920 865 959 1474">2025-03-Netskope-One-Platform-SB-719-5.pdf</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 516 1057 1472"><h3 data-bbox="272 1058 318 1461">The Power of One</h3><p data-bbox="358 716 448 1461">The major components of the Netskope One platform include:</p><p data-bbox="505 527 1049 1461">The Netskope Zero Trust Engine: Netskope's Zero Trust Engine lies at the heart of the platform, continuously gathering risk telemetry and generating extensive contextual awareness across all users, devices, applications, and data. Unlike other SSE offerings that bypass some types of traffic and services, the Zero Trust Engine decrypts and decodes traffic inline across web and SaaS applications, cloud services, and private applications for the broadest and deepest levels of visibility and protection.</p></div> <p data-bbox="1062 867 1092 1472">2025-03-Netskope-One-Platform-SB-719-5.pdf</p>

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement

What is ZTNA?

Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.

Zero Trust Security Principles

ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.

Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.

Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.

<https://www.netskope.com/security-defined/what-is-zero-trust-network-access>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 239 553 1472"> <h2 data-bbox="266 531 334 1472">Netskope One Private Access</h2> <p data-bbox="363 239 529 1472">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p> </div> <div data-bbox="553 611 1291 1472"> <p data-bbox="578 611 805 1446">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="870 642 1268 1446" style="list-style-type: none"> <li data-bbox="870 642 1097 1446">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="1135 642 1268 1446">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications </div> <div data-bbox="1295 210 1365 1472"> <p data-bbox="1295 210 1365 1472">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>1[a]. receiving, by a processing device, a request to access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;</p>	<p>The Accused '902 Products include receiving, by a processing device, a request to access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network.</p> <p>For example, a remote user device running the Netskope One Client (e.g., a known access device) receives a request to access one or more secure private network applications or resources in the Netskope NewEdge Network hosting Netskope Private Access, SWG, or related products, features or functions of the Netskope One Platform (a known private network that authorizes credentials associated with the known access device) associated with the private network. This known access device can be external to the private network—e.g., connected through a public network such as the internet—when the request to access is made to the processing device.</p>

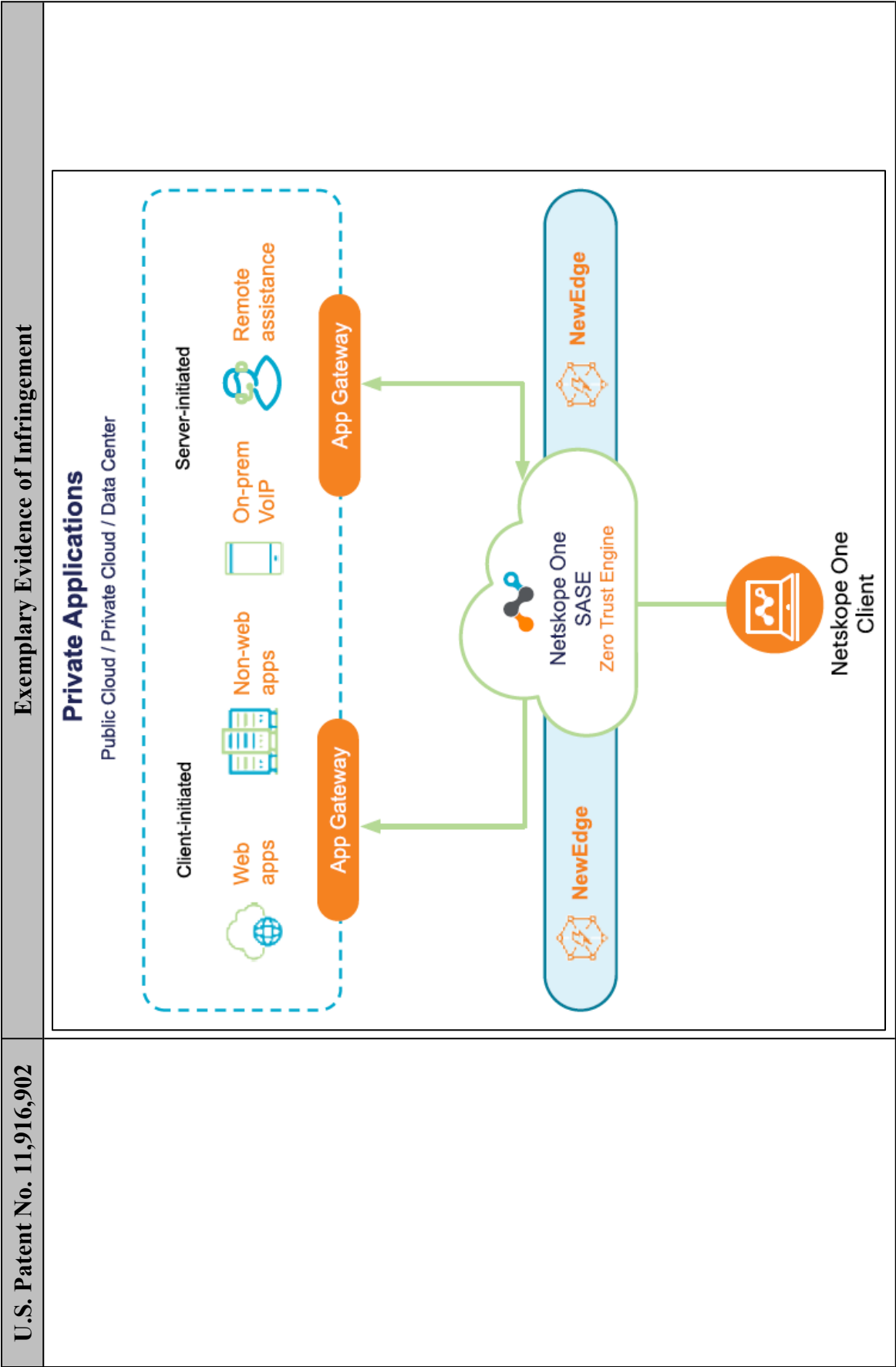
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<div data-bbox="272 1020 326 1467"><h2>The Power of One</h2></div> <div data-bbox="367 646 467 1467"><p>The major components of the Netskope One platform include:</p></div> <div data-bbox="529 436 1117 1467"><p>The Netskope Zero Trust Engine: Netskope's Zero Trust Engine lies at the heart of the platform, continuously gathering risk telemetry and generating extensive contextual awareness across all users, devices, applications, and data. Unlike other SSE offerings that bypass some types of traffic and services, the Zero Trust Engine decrypts and decodes traffic inline across web and SaaS applications, cloud services, and private applications for the broadest and deepest levels of visibility and protection.</p></div>	

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="259 367 779 1470"><p>The Netskope NewEdge Network: Netskope's one-of-a-kind network is purpose-built to deliver full compute SSE and SD-WAN. Featuring a global footprint of ultra-fast data centers in 75+ regions, and a local experience for every country, NewEdge is highly elastic, built for scale, and designed to provide cloud-delivered security and networking services directly to where the users and offices are without performance trade-offs.</p></div> <div data-bbox="787 367 1372 1470"><p>The Netskope One Client: Netskope's endpoint agent unifies remote user access to web, cloud, and private apps, alongside data protection and voice and video optimization at the endpoint by converging SWG, CASB, ZTNA, FWaaS, DLP, and SD-WAN. Easy to use, lightweight, and deployed to perform at a high throughput, it delivers a single agent footprint for SASE and zero trust use cases, greatly simplifying desktop administration for a better user experience.</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 382 920 1474"><p>The Netskope One Gateway: The Netskope One Gateway, offers both hardware and virtual form factors and supports the widest range of deployment options, including cellular gateways, micro to large branch, data center and multi-cloud environments. Netskope One Gateway consolidates disjointed appliances into one unified SASE gateway. It offers multiple services like Routing, WiFi, SD-WAN, App FW, IPS, IoT Device Intelligence, DEM and Edge compute, along with a seamless on-ramp to Netskope One SSE.</p></div> <div data-bbox="920 865 959 1474">2025-03-Netskope-One-Platform-SB-719-5.pdf</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="272 573 386 1463"> <h1>What is ZTNA?</h1> </div> <div data-bbox="483 191 824 1463"> <p>Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p> </div> <div data-bbox="849 972 885 1463"> <h2>Zero Trust Security Principles</h2> </div> <div data-bbox="906 191 1040 1463"> <p>ZTNA creates a new security framework, based on the <u>zero trust security model</u>, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p> </div> <div data-bbox="1073 191 1138 1463"> <p>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p> </div> <div data-bbox="1170 191 1268 1463"> <p>Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p> </div> <div data-bbox="1289 478 1321 1476"> <p>https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p> </div>

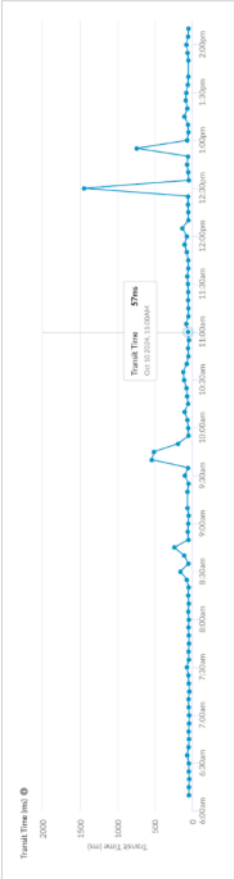
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<div data-bbox="251 197 565 1472"> <h2 data-bbox="266 499 337 1472">Netskope One Private Access</h2> <p data-bbox="370 197 542 1472">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p> </div> <div data-bbox="565 594 1317 1472"> <p data-bbox="589 594 821 1446">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="886 625 1292 1446" style="list-style-type: none"> <li data-bbox="886 695 1118 1446">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="1159 625 1292 1446">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications </div>	

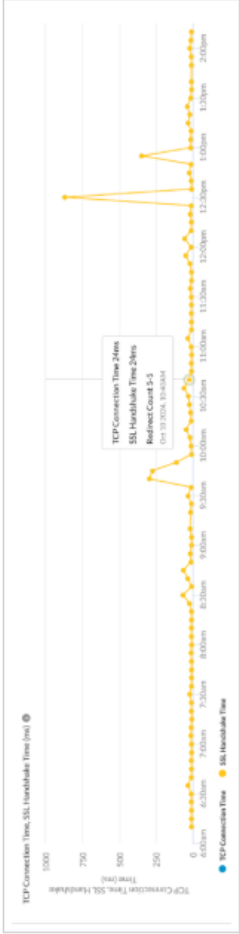


U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Seamless and optimized user experience</p> <p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul style="list-style-type: none">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="293 147 1198 1470"><p>How It Works</p><p>Netskope Private Application Access operates through the seamless integration of the Private Access Broker and the Publisher to enforce Zero Trust principles and provide secure access. The Private Access Broker functions as a cloud-native control plane that validates user identity, device posture, and access policies in real time before granting access to applications.</p><p>The Publisher, a lightweight connector deployed on-premises or in the cloud, establishes secure, encrypted communication between users and private applications without exposing applications to the internet. This architecture ensures that users gain access only to the specific applications they are authorized to use, with optimized routing and granular control, while eliminating the need for traditional VPNs. This combination provides a highly secure, scalable, and efficient access solution for endpoint-initiated workflows.</p><p>NPA is illustrated in this diagram:</p><p>The diagram, titled "Netskope for Private Access", illustrates the architecture of the Netskope Private Application Access solution. It shows "Remote Users" and "Offices" (represented by icons of a person with a laptop and a building) connecting to the "Netskope Platform". The platform is depicted as a central blue box containing four main functions: "Connects users to authorized apps – not your networks" (orange), "Authenticates users and devices in the cloud – not at your perimeter" (dark blue), "Classifies devices based on variety of security posture checks" (dark blue), and "Encrypts application traffic end-to-end" (light blue). To the right of the platform, a "Corporate Datacenter" is shown with server racks. Above the platform, "Public Cloud" services are listed, including Microsoft Azure, Amazon Web Services, and Google Cloud Platform. A legend at the bottom right identifies the "Netskope Client" (orange icon) and "Netskope Publisher" (blue icon).</p></div> <p>https://docs.netskope.com/en/netskope-private-access</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Connection</p> <p>The "Connection" time from the sites/users to Netskope POPs section corresponds to the time spent by the NSClient/Enterprise Station to establish a TCP connection with the NSProxy.</p> <p>TLS</p> <p>The "TLS" time from the sites/users to Netskope POPs section corresponds to the time spent by the NSClient/Enterprise Station to perform the TLS handshake process with the NSProxy.</p> <p>Inside Netskope POPs</p> <p>The following metric is processed at the NSProxy level.</p> <p>POP Transit Time</p> <p>The POP Transit Time provides the total time spent within the NSProxy.</p> <p>It is the addition of the "request transit time" and the "response transit time". These are defined as follows:</p> <ul style="list-style-type: none">• Request transit time Time elapsed between the first byte of request reaching the NSProxy and this first byte of the request leaving the NSProxy• Response transit time Time elapsed between the first byte of response reaching the NSProxy and this first byte of response leaving the NSProxy  <p>The diagram illustrates the POP Transit Time components. It shows the flow of data between the NSClient Enterprise Station and the NSProxy. The Request transit time is the time elapsed between the first byte of request reaching the NSProxy and this first byte of the request leaving the NSProxy. The Response transit time is the time elapsed between the first byte of response reaching the NSProxy and this first byte of response leaving the NSProxy.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Netskope POPs to Applications</p> <p>The following metrics are processed at the NSProxy level.</p> <p>Connection</p> <p>The "Connection" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to establish a TCP connection with the targeted server.</p>
	<p>Server</p> <p>The "Server" time corresponds to the time between the first byte of NSProxy request to the targeted server and the first byte of response received by the NSProxy.</p> <p>This Server time is the main server performance indicator, as it mainly takes the server processing time into account. Note though that there is also one RTT (between the NSProxy and the server) included. So bad network conditions between the NSProxy and the server may also impact the Server time value.</p> <p>https://docs.netskope.com/en/performance-metrics</p>
	<p>Transit Time</p>  <p>The Transit Time corresponds to the total time spent within the Netskope infrastructure. It includes the time spent in the NSProxy to forward the request from the NSClient to the application server, added to the time spent in the NSProxy to forward the response from the application server back to the NSClient.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="264 951 293 1465">TCP Connection Time, SSL Handshake Time</div> <div data-bbox="331 537 568 1465"><p>The graph displays three metrics over a period from 6:00am to 2:00pm. The Y-axis represents time in milliseconds (ms), ranging from 0 to 1000. The X-axis represents time in hours and minutes. The legend indicates: TCP Connection Time (blue line), SSL Handshake Time (yellow line), and Redirect Count (green line). The TCP Connection Time shows a sharp spike to approximately 1000ms at 12:30pm. The SSL Handshake Time remains relatively low, mostly below 250ms. The Redirect Count is mostly zero, with a small spike to 1 at 12:30pm.</p></div> <p data-bbox="617 147 792 1465">These metrics correspond to the time needed for the NSProxy to securely connect to the application server. This includes the TCP as well as SSL/TLS handshake processes. The Redirect count provides the number of redirections that have been observed during the select timeframe. The "Connection" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to establish a TCP connection with the targeted server. The "TLS" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to perform the TLS handshake process with the targeted server.</p> <p data-bbox="805 915 834 1476">https://docs.netskope.com/en/user-overview</p> <p data-bbox="876 147 982 1476">The Netskope Private Access products, SW/G and/or related products, features or functions of the Netskope One Platform are hosted in a Netskope NewEdge Network or a comparable network in data centers (such as in the cloud), and are accessible to users using the Netskope One Client.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div></div><div><h2>Netskope Advances Netskope One Platform With AI-Driven Proactive DEM Solution, Key Security Innovations</h2><p><i>Network Visibility and Control, Advanced Evasive Threat Detection, Context-Aware Zero Trust Integrations Accelerate Cloud Networking and Security Operations</i></p><p>SANTA CLARA, Calif. – September 10, 2024 – Netskope, a leader in Secure Access Service Edge (SASE), today announced several new innovations in the Netskope One platform, including expanded digital experience management (DEM) features and benefits. Combining key network and security capabilities, Netskope One continues to revolutionize the effectiveness of enterprise network infrastructure and operations (I&O) and security teams, enabling the entire organization to optimize the user experience while protecting critical data and reducing risk, cost, and complexity.</p><p>Coming on the heels of Netskope being recognized as a Leader in the 2024 Gartner Magic Quadrant™ for Single-Vendor SASE and as a Leader in the 2024 Gartner Magic Quadrant for Security Service Edge, the newly announced Netskope One platform advancements include the following.</p><p>https://www.netskope.com/press-releases/netkope-advances-netkope-one-platform-with-ai-driven-proactive-dem-solution-key-security-innovations</p></div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 367 878 1476"><h1 data-bbox="251 903 511 1476">Netskope NewEdge</h1><p data-bbox="673 399 868 1476">Netskope NewEdge is the world's largest, highest-performing security private cloud and powers the inline security services of the Netskope Security Cloud. NewEdge provides customers with unparalleled service coverage, performance and resilience. Today NewEdge is powered by data centers in 75+ regions with new data centers being added every month.</p></div> <div data-bbox="885 472 917 1476">https://www.netskope.com/resources/data-sheets/netkskope-newedge-data-sheet</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 388 878 1476"><h1 data-bbox="272 745 349 1459">Netskope NewEdge</h1><h2 data-bbox="553 394 602 1459">Cloud security without sacrificing performance</h2><p data-bbox="646 443 867 1459">As enterprises embrace digital transformation—with their applications and data quickly moving to the cloud and an increasingly remote workforce accessing from everywhere—selecting a cloud-native security platform that delivers real-time security without performance trade-offs is critical.</p></div> <div data-bbox="878 157 1224 1476"><p data-bbox="894 170 1214 1459">Netskope NewEdge is the world's largest, highest-performing security private cloud and powers the inline and API-driven security services of the Netskope Security Cloud. NewEdge provides customers with unparalleled service coverage, performance and resilience. Today NewEdge is powered by data centers in 70 regions with new data centers being added every month.</p><p data-bbox="1247 1430 1263 1459">...</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div>NewEdge deploys full compute at every service point for real-time, inline processing designed to scale to achieve more than two terabits per second at every data center—capable of serving hundreds of millions of users’ inline traffic—ensuring no performance trade-offs. Designed to provide a security service edge (SSE) and embracing a secure access service edge (SASE) architecture, this allows security to be deployed at the edge where and when it’s needed.</div> <div>Future-proof, SASE-ready architecture Powers Netskope SSE—including CFW, SWG, CASB, ZTNA and other services such as RBI, DLP, Threat Protection, CSPM/SSPM and more—without trade-offs even with all services enabled, plus full support for TLS 1.3 encryption, HTTP/2 and IPv6 clients. https://www.netskope.com/wp-content/uploads/2022/12/2023-04-NewEdge-DS-333-7-1.pdf</div> <div>Inside the Netskope NewEdge Data Center Factory</div> <div>Jul 13 2021 9 min. read</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>We've worked very hard to make our infrastructure single, unified, and 100% homogenous, so no single data center looks any different from any other. As part of moving to a lean, performance-focused footprint, we have implemented the concept of <i>integrated racks</i> into our data center factory approach. We build, pre-stage, configure, test, and ship a data center as a pre-built rack, with every rack constructed in exactly the same way. This approach ensures total consistency in every data center when it comes to what services are available and the related configuration of the surrounding infrastructure and underlying components.</p> <p>...</p> <p>Whether it's with our data center factory approach, in-the-weeds decisions about components that make up our integrated racks (e.g. bare metal servers, NVMe SSDs, or high-bandwidth network switches), data center site locations, peering or transit relationships, we take full responsibility for the customer experience and it's our job to architect around issues. It's important to https://www.netskope.com/blog/inside-the-netskope-newedge-data-center-factory</p> <h2>Understanding Coverage Isn't Just About Counting Data Centers</h2> <p>Aug 04 2020 6 min. read</p> <p>With the NewEdge network, we're not taking any shortcuts to deliver the security services of the Netskope Security Cloud Platform. We don't use vPoPs today and every data center offers full, local compute for real-time, in-line traffic processing. This allows us to inspect and enforce security policies without having to send the traffic halfway around the globe. All Netskope security services – including Next-Generation Secure Web Gateway (NG-SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and Zero Trust Network Access (ZTNA) – take advantage of this architectural approach. NewEdge is unique when compared to the approaches used by https://www.netskope.com/blog/understanding-coverage-isnt-just-about-counting-data-centers</p> <p>The Accused '902 Products include each and every element of this limitation, either literally or under the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that the Netskope Client remote device does not include a processing device that receives requests to access the</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Netskope NewEdge Network, the same function is achieved by the Netskope Private Access products, SWG, and/or related products (as referenced above) working in cooperation with the Netskope One Client distribute this functionality across devices to achieve the same result of receiving requests to access to one or more secure private network applications or resources in the Netskope NewEdge Network.</p>
<p>1[b]. scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an insecure network element on the remote network;</p>	<p>The Accused '902 Products include scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an insecure network element on the remote network.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Private Access products and Netskope One Platform act in a unified manner and scans the remote network identifying threats from unsecured network resources, or on a network with unsecured devices.</p> <div data-bbox="821 338 1333 1476"> <h2 data-bbox="837 680 938 1465">What is ZTNA?</h2> <p data-bbox="1024 359 1325 1465">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p> </div>

U.S. Patent No. 11,916,902	<div><div>Exemplary Evidence of Infringement</div><div><div><div><div><div><div>Zero Trust Security Principles</div><div>ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</div><div>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</div><div>Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</div><div>https://www.netskope.com/security-defined/what-is-zero-trust-network-access</div></div></div><div><div>Netskope One Private Access</div><div>Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</div></div></div></div></div></div>
----------------------------	---

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="280 604 516 1444">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="581 604 993 1444" style="list-style-type: none"><li data-bbox="581 604 816 1444">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure<li data-bbox="857 604 993 1444">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 516 1057 1472"><h3 data-bbox="272 1058 318 1465">The Power of One</h3><p data-bbox="358 716 448 1465">The major components of the Netskope One platform include:</p><p data-bbox="505 527 1049 1465">The Netskope Zero Trust Engine: Netskope's Zero Trust Engine lies at the heart of the platform, continuously gathering risk telemetry and generating extensive contextual awareness across all users, devices, applications, and data. Unlike other SSE offerings that bypass some types of traffic and services, the Zero Trust Engine decrypts and decodes traffic inline across web and SaaS applications, cloud services, and private applications for the broadest and deepest levels of visibility and protection.</p></div> <p data-bbox="1062 867 1094 1472">2025-03-Netskope-One-Platform-SB-719-5.pdf</p>

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement

What is ZTNA?

Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.

Zero Trust Security Principles

ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.

Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.

Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.

<https://www.netskope.com/security-defined/what-is-zero-trust-network-access>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 237 553 1472"> <h2 data-bbox="266 531 334 1472">Netskope One Private Access</h2> <p data-bbox="363 249 529 1472">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p> </div> <div data-bbox="553 611 1289 1472"> <p data-bbox="578 630 802 1449">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="870 638 1263 1449" style="list-style-type: none"> <li data-bbox="870 709 1094 1449">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="1133 638 1263 1449">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications </div> <div data-bbox="1295 210 1364 1472"> <p data-bbox="1295 210 1364 1472">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>1[a]. receiving, by a processing device, a request to access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;</p>	<p>The Accused '902 Products include receiving, by a processing device, a request to access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network.</p> <p>For example, a remote user device running the Netskope One Client (e.g., a known access device) receives a request to access one or more secure private network applications or resources in the Netskope NewEdge Network hosting Netskope Private Access, SWG, or related products, features or functions of the Netskope One Platform (a known private network that authorizes credentials associated with the known access device) associated with the private network. This known access device can be external to the private network—e.g., connected through a public network such as the internet—when the request to access is made to the processing device.</p>

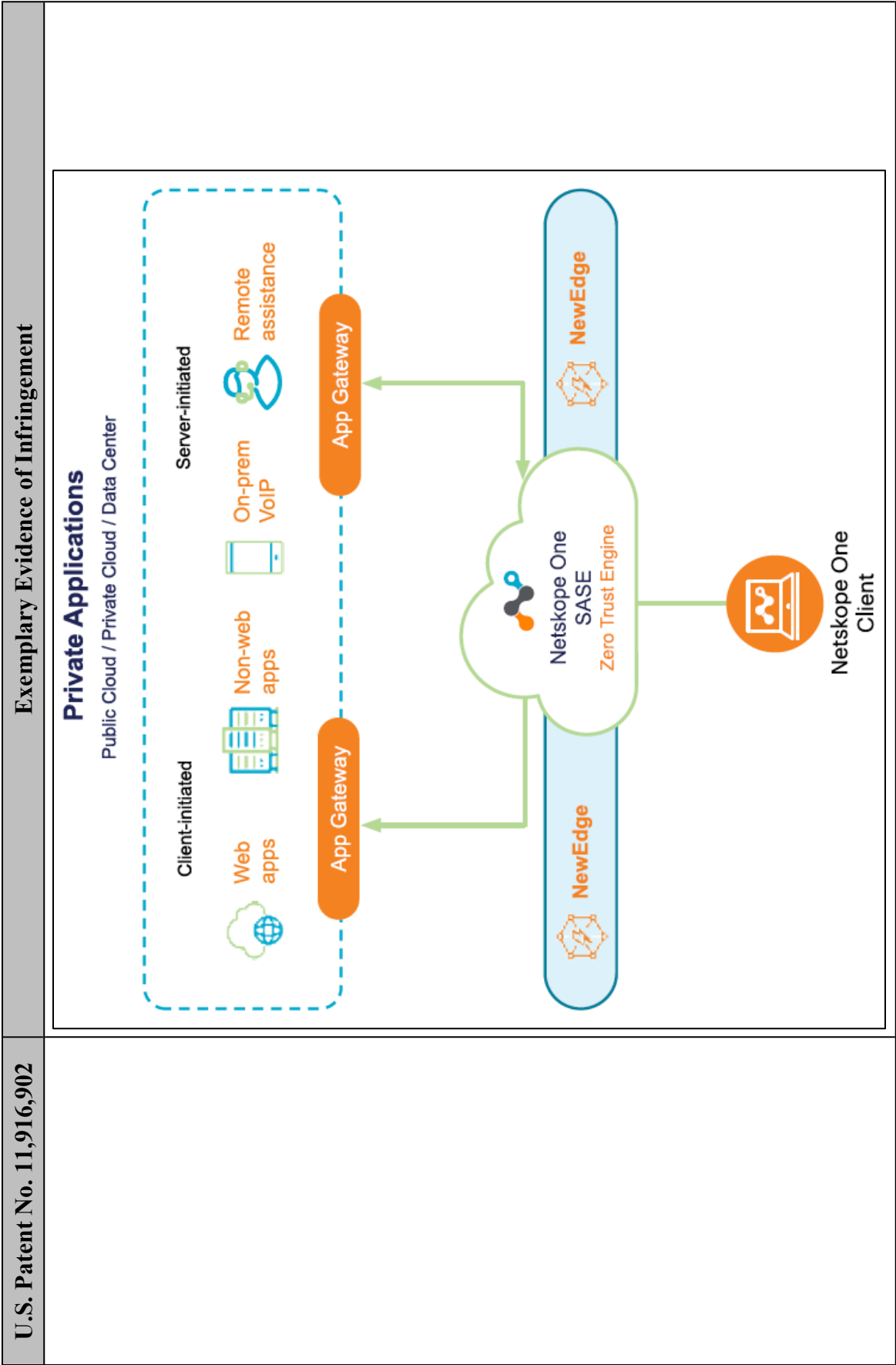
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<div data-bbox="272 1020 326 1467"><h2>The Power of One</h2></div> <div data-bbox="367 646 469 1467"><p>The major components of the Netskope One platform include:</p></div> <div data-bbox="527 436 1118 1467"><p>The Netskope Zero Trust Engine: Netskope's Zero Trust Engine lies at the heart of the platform, continuously gathering risk telemetry and generating extensive contextual awareness across all users, devices, applications, and data. Unlike other SSE offerings that bypass some types of traffic and services, the Zero Trust Engine decrypts and decodes traffic inline across web and SaaS applications, cloud services, and private applications for the broadest and deepest levels of visibility and protection.</p></div>	

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="259 367 779 1470"><p>The Netskope NewEdge Network: Netskope's one-of-a-kind network is purpose-built to deliver full compute SSE and SD-WAN. Featuring a global footprint of ultra-fast data centers in 75+ regions, and a local experience for every country, NewEdge is highly elastic, built for scale, and designed to provide cloud-delivered security and networking services directly to where the users and offices are without performance trade-offs.</p></div> <div data-bbox="787 367 1372 1470"><p>The Netskope One Client: Netskope's endpoint agent unifies remote user access to web, cloud, and private apps, alongside data protection and voice and video optimization at the endpoint by converging SWG, CASB, ZTNA, FWaaS, DLP, and SD-WAN. Easy to use, lightweight, and deployed to perform at a high throughput, it delivers a single agent footprint for SASE and zero trust use cases, greatly simplifying desktop administration for a better user experience.</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 382 920 1474"><p>The Netskope One Gateway: The Netskope One Gateway, offers both hardware and virtual form factors and supports the widest range of deployment options, including cellular gateways, micro to large branch, data center and multi-cloud environments. Netskope One Gateway consolidates disjointed appliances into one unified SASE gateway. It offers multiple services like Routing, WiFi, SD-WAN, App FW, IPS, IoT Device Intelligence, DEM and Edge compute, along with a seamless on-ramp to Netskope One SSE.</p></div> <div data-bbox="920 865 959 1474">2025-03-Netskope-One-Platform-SB-719-5.pdf</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="272 573 386 1463"> <h1>What is ZTNA?</h1> </div> <div data-bbox="483 191 824 1463"> <p>Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p> </div> <div data-bbox="849 972 885 1463"> <h2>Zero Trust Security Principles</h2> </div> <div data-bbox="906 191 1040 1463"> <p>ZTNA creates a new security framework, based on the <u>zero trust security model</u>, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p> </div> <div data-bbox="1073 191 1138 1463"> <p>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p> </div> <div data-bbox="1170 191 1268 1463"> <p>Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p> </div> <div data-bbox="1289 478 1321 1476"> <p>https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p> </div>

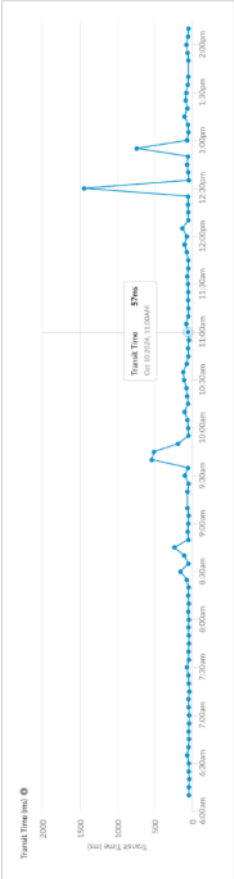
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 197 565 1472"> <h2 data-bbox="267 499 337 1472">Netskope One Private Access</h2> <p data-bbox="370 197 548 1472">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p> </div> <div data-bbox="570 594 1317 1472"> <p data-bbox="586 594 824 1444">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="889 625 1295 1444" style="list-style-type: none"> <li data-bbox="889 625 1117 1444">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="1166 625 1295 1444">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications </div>

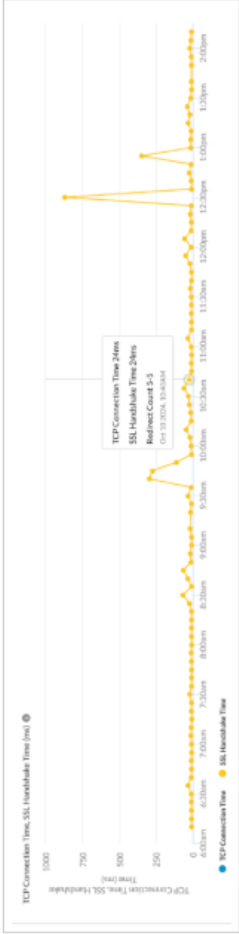


U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Seamless and optimized user experience</p> <p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul style="list-style-type: none">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

<p>U.S. Patent No. 11,916,902</p>	<p>Exemplary Evidence of Infringement</p>
	<p>How It Works</p> <p>Netskope Private Application Access operates through the seamless integration of the Private Access Broker and the Publisher to enforce Zero Trust principles and provide secure access. The Private Access Broker functions as a cloud-native control plane that validates user identity, device posture, and access policies in real time before granting access to applications.</p> <p>The Publisher, a lightweight connector deployed on-premises or in the cloud, establishes secure, encrypted communication between users and private applications without exposing applications to the internet. This architecture ensures that users gain access only to the specific applications they are authorized to use, with optimized routing and granular control, while eliminating the need for traditional VPNs. This combination provides a highly secure, scalable, and efficient access solution for endpoint-initiated workflows.</p> <p>NPA is illustrated in this diagram:</p>  <p>The diagram, titled "Netskope for Private Access", illustrates the architecture. On the left, "Remote Users" (represented by a smartphone icon) and "Offices" (represented by a building icon) are shown. Both connect to the "Netskope Platform" (labeled "PRIVATE APPS"). The platform is a central blue box containing four main functions: "Connects users to authorized apps – not your networks", "Authenticates users and devices in the cloud – not at your perimeter", "Classifies devices based on variety of security posture checks", and "Encrypts application traffic end-to-end". To the right of the platform, a "Public Cloud" section lists "Microsoft Azure", "amazon web services", and "Google Cloud Platform". Below this is a "Corporate Datacenter" represented by server racks. A legend at the bottom right identifies the "Netskope Client" (orange square icon) and "Netskope Publisher" (blue square icon).</p> <p>https://docs.netskope.com/en/netskope-private-access</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Connection</p> <p>The "Connection" time from the sites/users to Netskope POPs section corresponds to the time spent by the NSClient/Enterprise Station to establish a TCP connection with the NSProxy.</p> <p>TLS </p> <p>The "TLS" time from the sites/users to Netskope POPs section corresponds to the time spent by the NSClient/Enterprise Station to perform the TLS handshake process with the NSProxy.</p> <p>Inside Netskope POPs</p> <p>The following metric is processed at the NSProxy level.</p> <p>POP Transit Time</p> <p>The POP Transit Time provides the total time spent within the NSProxy.</p> <p>It is the addition of the "request transit time" and the "response transit time". These are defined as follows:</p> <ul style="list-style-type: none">• Request transit time Time elapsed between the first byte of request reaching the NSProxy and this first byte of the request leaving the NSProxy• Response transit time Time elapsed between the first byte of response reaching the NSProxy and this first byte of response leaving the NSProxy 

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Netskope POPs to Applications</p> <p>The following metrics are processed at the NSProxy level.</p> <p>Connection</p> <p>The "Connection" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to establish a TCP connection with the targeted server.</p>
	<p>Server</p> <p>The "Server" time corresponds to the time between the first byte of NSProxy request to the targeted server and the first byte of response received by the NSProxy.</p> <p>This Server time is the main server performance indicator, as it mainly takes the server processing time into account. Note though that there is also one RTT (between the NSProxy and the server) included. So bad network conditions between the NSProxy and the server may also impact the Server time value.</p> <p>https://docs.netskope.com/en/performance-metrics</p>
	<p>Transit Time</p>  <p>The Transit Time corresponds to the total time spent within the Netskope infrastructure. It includes the time spent in the NSProxy to forward the request from the NSClient to the application server, added to the time spent in the NSProxy to forward the response from the application server back to the NSClient.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="264 951 293 1465">TCP Connection Time, SSL Handshake Time</div> <div data-bbox="331 537 568 1465"><p>The graph displays three metrics over a period from 6:00am to 2:00pm. The Y-axis represents time in milliseconds (ms), ranging from 0 to 1000. The X-axis represents time in hours and minutes. The legend indicates: TCP Connection Time (blue line), SSL Handshake Time (yellow line), and Redirect Count (green line). The TCP Connection Time shows a sharp spike to approximately 1000ms at 12:30pm. The SSL Handshake Time remains relatively low, around 100ms. The Redirect Count shows a small peak around 12:30pm.</p></div> <p data-bbox="617 147 792 1465">These metrics correspond to the time needed for the NSProxy to securely connect to the application server. This includes the TCP as well as SSL/TLS handshake processes. The Redirect count provides the number of redirections that have been observed during the select timeframe. The "Connection" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to establish a TCP connection with the targeted server. The "TLS" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to perform the TLS handshake process with the targeted server.</p> <p data-bbox="805 915 834 1476">https://docs.netskope.com/en/user-overview</p> <p data-bbox="876 147 982 1476">The Netskope Private Access products, SW/G and/or related products, features or functions of the Netskope One Platform are hosted in a Netskope NewEdge Network or a comparable network in data centers (such as in the cloud), and are accessible to users using the Netskope One Client.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div></div><div><h2>Netskope Advances Netskope One Platform With AI-Driven Proactive DEM Solution, Key Security Innovations</h2><p><i>Network Visibility and Control, Advanced Evasive Threat Detection, Context-Aware Zero Trust Integrations Accelerate Cloud Networking and Security Operations</i></p><p>SANTA CLARA, Calif. – September 10, 2024 – Netskope, a leader in Secure Access Service Edge (SASE), today announced several new innovations in the Netskope One platform, including expanded digital experience management (DEM) features and benefits. Combining key network and security capabilities, Netskope One continues to revolutionize the effectiveness of enterprise network infrastructure and operations (I&O) and security teams, enabling the entire organization to optimize the user experience while protecting critical data and reducing risk, cost, and complexity.</p><p>Coming on the heels of Netskope being recognized as a Leader in the 2024 Gartner Magic Quadrant™ for Single-Vendor SASE and as a Leader in the 2024 Gartner Magic Quadrant for Security Service Edge, the newly announced Netskope One platform advancements include the following.</p><p>https://www.netskope.com/press-releases/netkope-advances-netkope-one-platform-with-ai-driven-proactive-dem-solution-key-security-innovations</p></div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 367 878 1476"><h1 data-bbox="261 905 511 1463">Netskope NewEdge</h1><p data-bbox="673 401 868 1467">Netskope NewEdge is the world's largest, highest-performing security private cloud and powers the inline security services of the Netskope Security Cloud. NewEdge provides customers with unparalleled service coverage, performance and resilience. Today NewEdge is powered by data centers in 75+ regions with new data centers being added every month.</p></div> <p data-bbox="883 470 915 1476">https://www.netskope.com/resources/data-sheets/netkskope-newedge-data-sheet</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 388 467 1476">  </div> <div data-bbox="467 388 878 1476"> <p>Cloud security without sacrificing performance</p> <p>As enterprises embrace digital transformation—with their applications and data quickly moving to the cloud and an increasingly remote workforce accessing from everywhere—selecting a cloud-native security platform that delivers real-time security without performance trade-offs is critical.</p> </div> <div data-bbox="878 147 1224 1476"> <p>Netskope NewEdge is the world's largest, highest-performing security private cloud and powers the inline and API-driven security services of the Netskope Security Cloud. NewEdge provides customers with unparalleled service coverage, performance and resilience. Today NewEdge is powered by data centers in 70 regions with new data centers being added every month.</p> <p>...</p> </div>

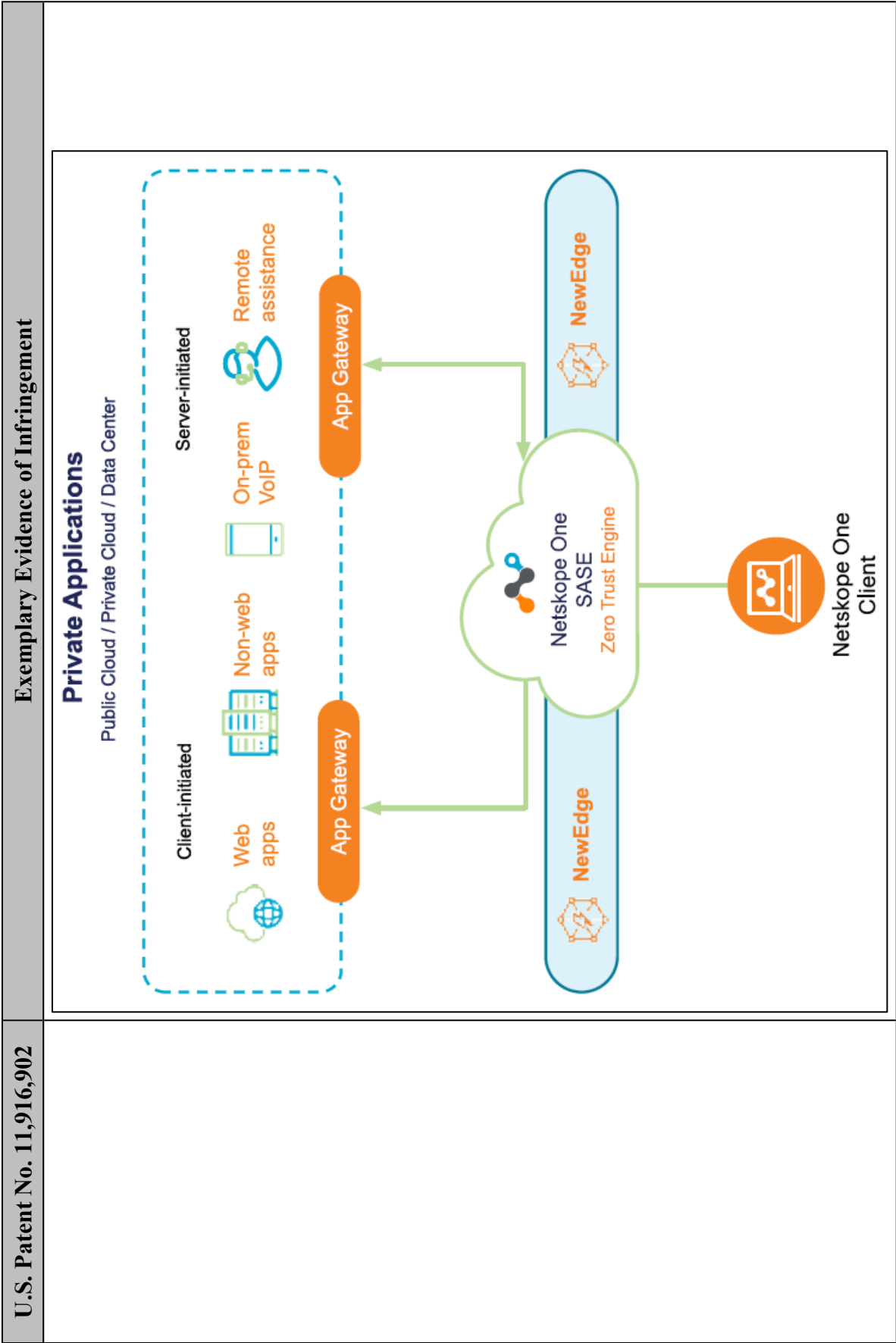
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div>NewEdge deploys full compute at every service point for real-time, inline processing designed to scale to achieve more than two terabits per second at every data center—capable of serving hundreds of millions of users’ inline traffic—ensuring no performance trade-offs. Designed to provide a security service edge (SSE) and embracing a secure access service edge (SASE) architecture, this allows security to be deployed at the edge where and when it’s needed.</div> <div>Future-proof, SASE-ready architecture Powers Netskope SSE—including CFW, SWG, CASB, ZTNA and other services such as RBI, DLP, Threat Protection, CSPM/SSPM and more—without trade-offs even with all services enabled, plus full support for TLS 1.3 encryption, HTTP/2 and IPv6 clients. https://www.netskope.com/wp-content/uploads/2022/12/2023-04-NewEdge-DS-333-7-1.pdf</div> <div>Inside the Netskope NewEdge Data Center Factory</div> <div>Jul 13 2021 9 min. read</div>

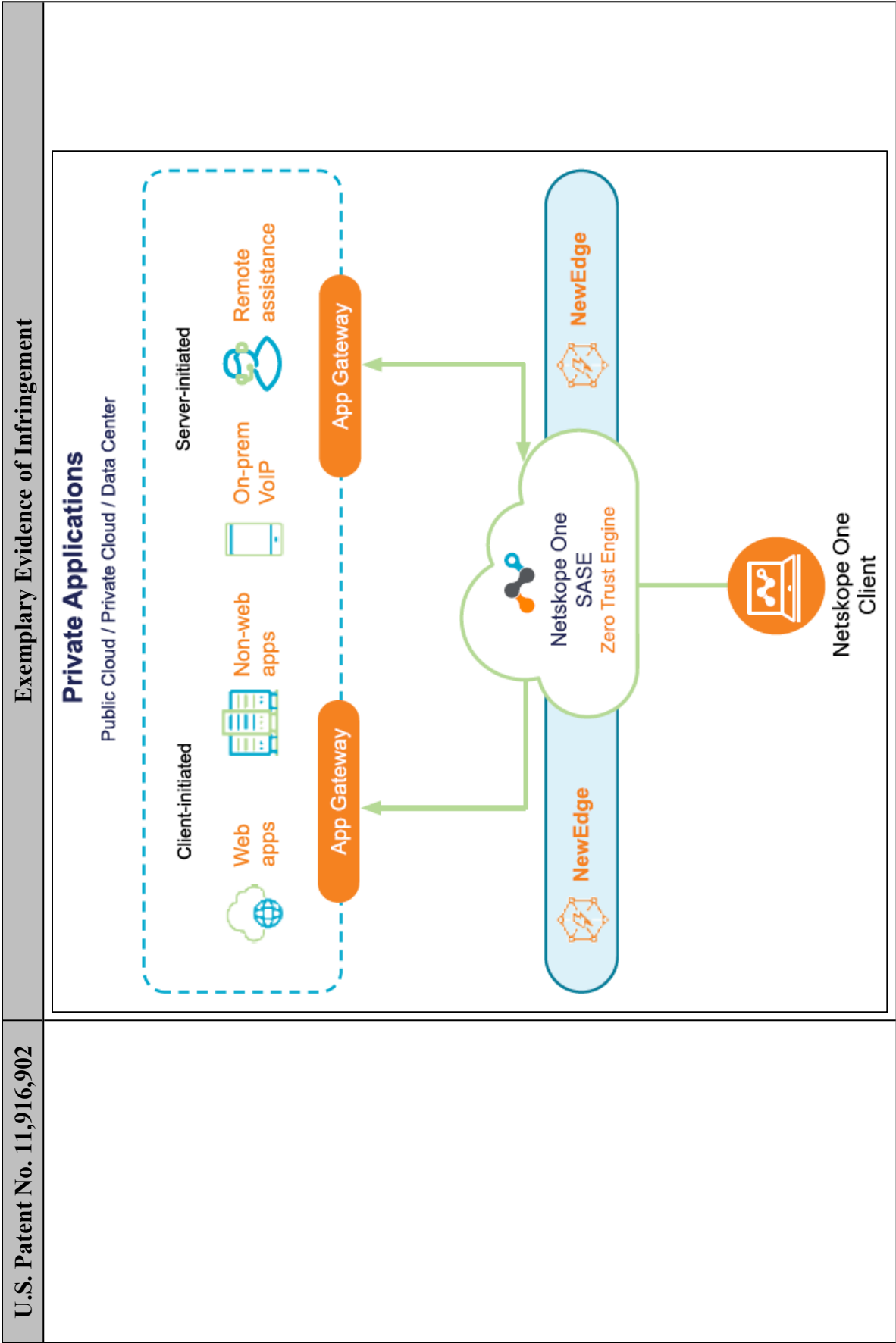
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>We've worked very hard to make our infrastructure single, unified, and 100% homogenous, so no single data center looks any different from any other. As part of moving to a lean, performance-focused footprint, we have implemented the concept of <i>integrated racks</i> into our data center factory approach. We build, pre-stage, configure, test, and ship a data center as a pre-built rack, with every rack constructed in exactly the same way. This approach ensures total consistency in every data center when it comes to what services are available and the related configuration of the surrounding infrastructure and underlying components.</p> <p>...</p> <p>Whether it's with our data center factory approach, in-the-weeds decisions about components that make up our integrated racks (e.g. bare metal servers, NVMe SSDs, or high-bandwidth network switches), data center site locations, peering or transit relationships, we take full responsibility for the customer experience and it's our job to architect around issues. It's important to https://www.netskope.com/blog/inside-the-netskope-newedge-data-center-factory</p> <h2>Understanding Coverage Isn't Just About Counting Data Centers</h2> <p>Aug 04 2020 6 min. read</p> <p>With the NewEdge network, we're not taking any shortcuts to deliver the security services of the Netskope Security Cloud Platform. We don't use vPoPs today and every data center offers full, local compute for real-time, in-line traffic processing. This allows us to inspect and enforce security policies without having to send the traffic halfway around the globe. All Netskope security services – including Next-Generation Secure Web Gateway (NG-SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and Zero Trust Network Access (ZTNA) – take advantage of this architectural approach. NewEdge is unique when compared to the approaches used by https://www.netskope.com/blog/understanding-coverage-isnt-just-about-counting-data-centers</p> <p>The Accused '902 Products include each and every element of this limitation, either literally or under the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that the Netskope Client remote device does not include a processing device that receives requests to access the</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Netskope NewEdge Network, the same function is achieved by the Netskope Private Access products, SWG, and/or related products (as referenced above) working in cooperation with the Netskope One Client distribute this functionality across devices to achieve the same result of receiving requests to access to one or more secure private network applications or resources in the Netskope NewEdge Network.</p>
<p>1[b]. scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an insecure network element on the remote network;</p>	<p>The Accused '902 Products include scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an insecure network element on the remote network.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Private Access products and Netskope One Platform act in a unified manner and scans the remote network identifying threats from unsecured network resources, or on a network with unsecured devices.</p> <div data-bbox="821 338 1346 1476"> <h2 data-bbox="841 680 938 1465">What is ZTNA?</h2> <p data-bbox="1024 359 1325 1465">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p> </div>

U.S. Patent No. 11,916,902	<div><div>Exemplary Evidence of Infringement</div><div><div><div>Zero Trust Security Principles</div><div><p>ZTNA creates a new security framework, based on the <u>zero trust security model</u>, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p><p>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p><p>Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p><p>https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p></div></div><div><div>Netskope One Private Access</div><div><p>Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p></div></div></div></div>
----------------------------	---

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="280 604 516 1446">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="581 604 995 1446" style="list-style-type: none"><li data-bbox="581 604 816 1446">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure<li data-bbox="857 604 995 1446">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications





U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Seamless and optimized user experience</p> <p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul style="list-style-type: none">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope’s Device Intelligence (formerly known as Netskope IoT Security) act in a unified manner and performs a deep context scan of every device and the collection and acquisition of data concerning all devices in, and “around,” the remote network (<i>e.g.</i>, assessing security of elements in the remote network to which the remote device running the Netskope Client is connected beyond merely the device seeking access) to identify threats from unsecured network resources, or on a network with unsecured devices.</p>

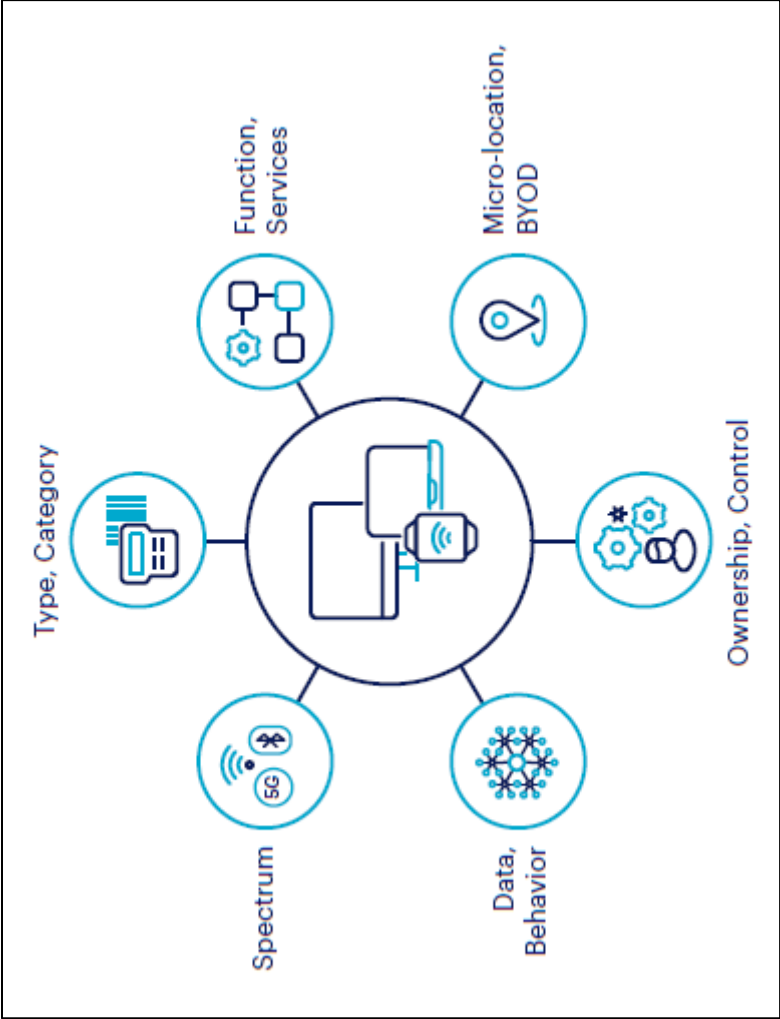
U.S. Patent No. 11,916,902	<div data-bbox="472 281 1125 598">Exemplary Evidence of Infringement</div> <div data-bbox="472 598 1125 1478"> <h1>Netskope One Private Access features and benefits</h1> <ul style="list-style-type: none"> Full VPN, NAC replacement > AI-driven automated policy optimization > Flexible access methods > Built-in threat and data protection > Built-in device intelligence v Unified visibility >  <p>Netskope UZTNA extends zero trust beyond users to every connected device. With Device Intelligence, organizations gain visibility, real-time risk scoring, and context-aware access for IoT and OT systems, securing branches, campuses, and factories while reducing attack surface at scale.</p> <p>> Learn about Device Intelligence</p> </div> <div data-bbox="472 1478 1125 1768"> https://www.netskope.com/products/private-access </div>
----------------------------	---

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="272 317 350 1444">Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul data-bbox="386 260 1036 1398" style="list-style-type: none"><li data-bbox="386 260 505 1398">• Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior.<li data-bbox="532 233 695 1398">• Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR.<li data-bbox="722 289 846 1398">• Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations.<li data-bbox="873 268 1036 1398">• Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p data-bbox="1089 722 1122 1476">https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 934 289 1465">REALIZING ZERO TRUST FOR DEVICES</p> <p data-bbox="354 176 578 1465">Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p> <ul data-bbox="605 197 906 1415" style="list-style-type: none"> <li data-bbox="605 197 667 1415">• Granular device context: Deep context about every device, resource, and user in and around the network <li data-bbox="695 197 756 1415">• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location <li data-bbox="784 197 846 1415">• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment <li data-bbox="873 197 906 1415">• Security automation: Automated alert handling and responses to security incidents

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 331 293 1472">HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE</p> <p data-bbox="354 149 699 1472">Netskope Device Intelligence uncovers managed and unmanaged devices on the network spectrum and fingerprints those devices based on their unique characteristics across multiple dimensions. These dimensions include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. The device information is collected from multiple network interfaces, protocol information, traffic flow, and application heuristics. This is combined with organizational information from existing CMDB, tools like MDM, EDR, vulnerability assessment, firewall, times of operation and location amongst others to develop rich and dynamic device context. This context is then fed to machine learning algorithms to generate unique models and signatures for each device, which includes the following information, called HyperContext®:</p> <ul data-bbox="727 149 1203 1472" style="list-style-type: none"> • Association of all the physical interfaces of the device and the spectrum of operation of each interface • Type, Category of the device and related information • OS, patches, services, and applications running on the device • Functionality or the “purpose in life” of the device • Micro location of the device, its mobility patterns, and times of visibility • Ownership information of the device and its control information • Users on the device • Behavior based analysis of all the data transmissions across all protocols and spectrums • Risk and vulnerability information, other information collected by other tools used

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 462 1031 1474"><p>The diagram illustrates various categories of IoT devices and their associated data. A central circle contains icons for a laptop, a smartphone, and a smartwatch. Six surrounding circles are connected to the center, each representing a category: 'Spectrum' (with 5G and Bluetooth icons), 'Data, Behavior' (with a network node icon), 'Ownership, Control' (with a gear and key icon), 'Micro-location, BYOD' (with a location pin icon), 'Function, Services' (with a gear and server icon), and 'Type, Category' (with a document and bar chart icon).</p></div> <p data-bbox="1036 300 1105 1474">https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Investigate Device Intelligence > Investigate Devices</div><div><div>Investigate Devices</div><div><div>Navigate to Investigate > Devices menu to see an entire dashboard stating the device summary in your environment based on different aspects like spectrum, type, ownership, etc.</div><div><div><div>Note</div><div>You can also sort the device summary in combination with the total of all devices, managed, unmanaged, new, automated, and user-controlled devices.</div></div></div><div><div>Investigate Devices based on Spectrum</div><div>Navigate to Investigate > Devices menu and select the Spectrum tab from the navigation bar to see the devices based on the network spectrum in the environment.</div><div><div><div>247 Total Devices</div><div>56 Managed Devices</div><div>191 Unmanaged Devices</div><div>52 New Devices</div><div>113 Automated Devices</div><div>127 User Devices</div></div><div><div>Spectrum</div><div>Types</div><div>Ownership</div><div>Control</div><div>Protocols</div><div>Internal Topology</div><div>External Topology</div></div><div><div>Device By Network Spectrum</div><div><div>1323</div><div>247</div><div>75</div><div>1</div></div><div><div>Spectrum</div><div>Network</div><div>WiFi</div><div>Bluetooth</div></div><div><div>20 dBm</div><div>0 dBm</div><div>10 dBm</div><div>20 dBm</div></div></div></div></div></div></div></div>

<https://docs.netkope.com/en/investigate-devices>

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement

Investigate Risks

Navigate to **Investigate > Risks** menu to see a list of devices with high, medium or low priority. The screen provides the event view and device view for the information representation. You can see the number of devices with risk at the top right chart.

Events view shows the information in device summary and event drill down table.

Computer

Managed

Network

Risk Score

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details

27

view

Details</

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 783 326 1423"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="365 289 651 1423"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="695 275 1357 1467"><p>The diagram illustrates the architecture of Device Intelligence, showing the flow of data and processing from a Customer Site to the Cloud.</p><p>Customer Site:</p><ul style="list-style-type: none">Airspace Data: Represented by a box with binary code (10010110011011, 01011001101100).Network Data: Represented by a box with binary code (10010110011011, 01011001101100).Radio Sensors or Access Points: Represented by a box with a signal icon.Network Sensor: Represented by a box with a server icon.Nextgen Access Control: A box containing the text "CUSTOMER SITE" and the "netskope" logo.<p>Processing and Analysis:</p><ul style="list-style-type: none">Billions of daily measurements of device characteristics: A central circular process involving "AI" and "ML" icons, with a "Deep Learning + Powerful Policy Engine" icon.Alerts/Insights: A box containing "Billions of daily device behavior analyzed".Models / Controls: A box that receives input from the "Alerts/Insights" and sends output to the "Cloud".<p>Cloud:</p><ul style="list-style-type: none">Asset Mgmt Integration: A box that receives input from the "Models / Controls" and sends output to the "Deep Learning + Powerful Policy Engine".Vulnerability Scanner Integration: A box that receives input from the "Models / Controls" and sends output to the "Deep Learning + Powerful Policy Engine".MDM, EDR Integration: A box that receives input from the "Deep Learning + Powerful Policy Engine" and sends output to the "Cloud".Security Integration: A box that receives input from the "Deep Learning + Powerful Policy Engine" and sends output to the "Cloud".UI: A box that receives input from the "Alerts/Insights" and sends output to the "Cloud".SIEM: A box that receives input from the "Alerts/Insights" and sends output to the "Cloud".Ticketing: A box that receives input from the "Alerts/Insights" and sends output to the "Cloud".<p>Footer: 2022 © Netskope Confidential. All rights reserved.</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="293 197 902 1474"><p data-bbox="326 1178 358 1436">Data Acquisition</p><ul data-bbox="399 247 870 1394" style="list-style-type: none"><li data-bbox="399 354 431 1394">• Customer environments have network sensors installed as physical or virtual appliances.<li data-bbox="448 247 570 1394">• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data.<li data-bbox="594 247 675 1394">• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<li data-bbox="691 247 773 1394">• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<li data-bbox="789 264 870 1394">• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 1220 321 1438"> <p>Data Transfer</p> </div> <div data-bbox="365 262 540 1396"> <ul style="list-style-type: none"> • The network sensors do a deep inspection of the traffic, apply signatures and run algorithms to extract meta information. • Network sensors send this meta information via encrypted channel to the cloud to analyze the traffic metadata and events in the environment. </div> <div data-bbox="581 1220 613 1438"> <p>Data Analysis</p> </div> <div data-bbox="657 233 878 1396"> <ul style="list-style-type: none"> • On the cloud, various microservices analyze the metadata. • The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools. </div> <div data-bbox="927 1094 959 1467"> <p>Analytics and Protection</p> </div> <div data-bbox="1003 203 1274 1438"> <ul style="list-style-type: none"> • Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies. • In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies. • Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. </div> <div data-bbox="1295 632 1328 1480"> <p>https://docs.netskope.com/en/architecture-of-netskope-iot-security</p> </div> <div data-bbox="1372 184 1404 1480"> <p>The Accused '902 Products include each and every element of this limitation, either literally or under</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that the Netskope Client remote device does not include a processing device that scans the remote network through which access to the known network is to be established, the same function is achieved by the Netskope Private Access products, SWG, and/or related products, features or functions of the Netskope One Platform working in cooperation with the Netskope One Client to distribute this functionality across devices to achieve the same result of scanning the remote network through which access to the Netskope NewEdge Network is to be established.</p>
<p>l[c]. based at least in part on identifying at least one unsecure network element on the remote network, denying, by the processing device, access to the known network; and</p>	<p>The Accused '902 Products include, based at least in part on identifying at least one unsecure network element on the remote network, denying, by the processing device, access to the known network.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Private Access products and/or related products, features or functions of the Netskope One Platform deny access to Netskope's NewEdge Network's private resources in association with identification of one or more unsecure network elements.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 371 753 1472"><h1 data-bbox="272 705 370 1465">What is ZTNA?</h1><p data-bbox="451 394 743 1465">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p></div> <div data-bbox="760 304 1154 1472"><h2 data-bbox="764 1024 797 1465">Zero Trust Security Principles</h2><p data-bbox="816 323 938 1465">ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p><p data-bbox="971 323 1024 1465">Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p><p data-bbox="1057 359 1143 1465">Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p><p data-bbox="1162 478 1195 1472">https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div>Seamless and optimized user experience<p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p><p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p><ul style="list-style-type: none">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity.<p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection (e.g., policy actions like blocking devices) in response to the information collected about devices in and around the network of the remote user's device for use in making access determinations for the device.</p> <div style="border: 1px solid black; padding: 10px;"> <p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-nskskope-iot-security</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="272 317 350 1444">Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul data-bbox="386 260 1036 1398" style="list-style-type: none"><li data-bbox="386 260 505 1398">• Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior.<li data-bbox="532 233 695 1398">• Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR.<li data-bbox="722 289 846 1398">• Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations.<li data-bbox="873 268 1036 1398">• Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p data-bbox="1089 722 1122 1476">https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 934 289 1465">REALIZING ZERO TRUST FOR DEVICES</p> <p data-bbox="354 176 578 1465">Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p> <ul data-bbox="605 197 906 1415" style="list-style-type: none"> <li data-bbox="605 197 667 1415">• Granular device context: Deep context about every device, resource, and user in and around the network <li data-bbox="695 197 756 1415">• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location <li data-bbox="784 197 846 1415">• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment <li data-bbox="873 197 906 1415">• Security automation: Automated alert handling and responses to security incidents

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="266 934 302 1463">Need for granular device context</p> <p data-bbox="326 787 1336 1463">With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to ensure security, and enforce right access control across the network. Current device fingerprinting technologies boil down to type, category, OS, version, etc. which are woefully inadequate for correctly profiling the device behavior and setting adequate controls to protect the device and the infrastructure it operates in. To keep networks secure you need to have a deeper understanding of devices entering/exiting your network, their dynamic behavior, and the risk associated with them to take precise actions. This calls for developing rich and dynamic device context across multiple dimensions, combining them with machine learning algorithms to generate models and signatures for each device. This rich contextual device intelligence allows for granular visibility and control.</p> <p data-bbox="1352 300 1419 1476">https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

<p>U.S. Patent No. 11,916,902</p>	<div data-bbox="203 562 235 1071"><p>Exemplary Evidence of Infringement</p></div> <div data-bbox="321 783 363 1425"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="401 287 685 1425"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="729 279 1386 1461"><p>The diagram illustrates the 'Architecture of Device Intelligence' for an IoT Security Platform. It is divided into three main sections: IoT Security Platform, AI-based context generation platform for all devices, and Cloud.</p><ul style="list-style-type: none">IoT Security Platform: This section shows data sources at the 'CUSTOMER SITE'. It includes 'Airspace Data' (represented by a binary string 10010110011011) and 'Network Data' (represented by a binary string 01011001101100). These data sources feed into 'Radio Sensors or Access Points' and a 'Network Sensor'. The output of these sensors is 'Nextgen Access Control'.AI-based context generation platform for all devices: This central section receives input from the IoT Security Platform. It features a circular diagram with icons for OS, AI, and a shield, labeled 'Billions of daily measurements of device characteristics'. This leads to 'Models / Controls'.Cloud: This section receives input from the AI-based platform. It includes a 'Deep Learning + Powerful Policy Engine' which processes 'Billions of daily device behavior analyzed' to produce 'Alerts/Insights'. These insights are then sent to a 'UI', 'SIEM', and 'Ticketing' system.<p>Additional components shown include 'Asset Mgmt Integration', 'Vulnerability Scanner Integration', 'MDM, EDR Integration', and 'Security integration'.</p><p><small>© 2024 Netskope Confidential. All rights reserved.</small></p></div>
-----------------------------------	---

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><p>Data Acquisition</p><ul style="list-style-type: none">• Customer environments have network sensors installed as physical or virtual appliances.• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data.• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 304 1024 1474"> <p>Data Analysis</p> <ul style="list-style-type: none"> • On the cloud, various microservices analyze the metadata. • The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools. <p>Analytics and Protection</p> <ul style="list-style-type: none"> • Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies. • In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies. • Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <p>https://docs.netkope.com/en/architecture-of-netkope-iot-security</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Protect Device Intelligence > Remediated Devices</div><h2>Remediated Devices</h2><p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p><p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p><ul style="list-style-type: none">• Device Name: The name or identifier of the device.• Device Type: The type of device (e.g., computer, printer, IoT device).• Device Details: By clicking on a details link, you will be navigated to a new page about the device details.• Status: The current status of the remediation action (e.g., Pending Segment, Segmented).• Triggered On: The date and time when the security policy was triggered.• Policy: The name of the security policy that was triggered.• Remediation Agent: The agent responsible for enforcing the remediation action.• Actions: A set of actions that can be performed on the device, such as:<ul style="list-style-type: none">• Add to Exception List: Excludes the device from future remediation actions.• Undo Action: Reverses the previous remediation action taken on the device.• Undo Segmentation: Reverses the previous segmentation action taken on the device.<p>https://docs.netskope.com/en/remediated-devices</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>The Accused '902 Products include each and every element of this limitation, either literally or under the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that the Netskope Client remote device does not include a processing device that denies access to the known network, the same function is achieved by the Netskope Private Access products, SWG, and/or related products (as referenced above) working in cooperation with the Netskope One Client to distribute this functionality across devices to achieve the same result of denying access to the Netskope NewEdge Network.</p>
<p>1[d]. based at least in part upon on failure to identify any unsecure network element on the remote network, requesting a grant of access from the known network to the processing device,</p>	<p>The Accused '902 Products include, based at least in part upon on failure to identify any unsecure network element on the remote network, requesting a grant of access from the known network to the processing device.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Private Access products and Netskope One Platform grant access to devices that are not found to be unauthorized or unsecured, or on a network with unsecured devices, to connect to the Netskope NewEdge Network.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 371 751 1472"><h1 data-bbox="267 703 370 1465">What is ZTNA?</h1><p data-bbox="451 394 743 1465">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p></div> <div data-bbox="760 304 1154 1472"><h2 data-bbox="764 1024 797 1465">Zero Trust Security Principles</h2><p data-bbox="816 321 938 1465">ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p><p data-bbox="971 321 1024 1465">Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p><p data-bbox="1057 359 1143 1465">Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p><p data-bbox="1162 478 1195 1472">https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p></div>

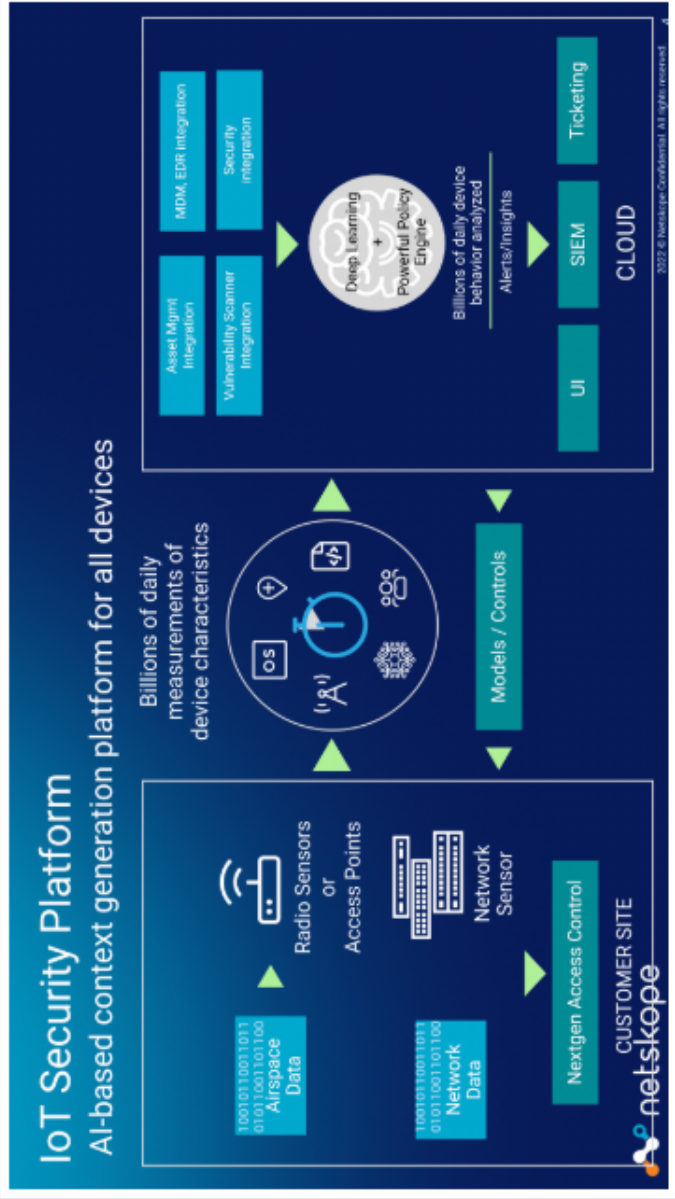
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div>Seamless and optimized user experience<p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p><p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p><ul style="list-style-type: none">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity.<p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection (e.g., policy actions like allowing, rather than blocking, devices) in response to the information collected about devices in and around the network of the remote user's device for use in making access determinations for the device.</p> <div data-bbox="475 195 1295 1476"> <p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-nsn-iot-security</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="272 321 349 1444">Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul data-bbox="386 233 1036 1402" style="list-style-type: none"><li data-bbox="386 233 505 1402">• Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior.<li data-bbox="532 233 695 1402">• Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR.<li data-bbox="722 233 846 1402">• Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations.<li data-bbox="873 233 1036 1402">• Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p data-bbox="1089 724 1122 1476">https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 1476 293 1908">REALIZING ZERO TRUST FOR DEVICES</p> <p data-bbox="354 1476 581 1908">Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p> <ul data-bbox="605 1476 914 1908" style="list-style-type: none"> <li data-bbox="605 1476 670 1908">• Granular device context: Deep context about every device, resource, and user in and around the network <li data-bbox="695 1476 760 1908">• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location <li data-bbox="784 1476 849 1908">• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment <li data-bbox="873 1476 914 1908">• Security automation: Automated alert handling and responses to security incidents

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Need for granular device context</p> <p>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to ensure security, and enforce right access control across the network. Current device fingerprinting technologies boil down to type, category, OS, version, etc. which are woefully inadequate for correctly profiling the device behavior and setting adequate controls to protect the device and the infrastructure it operates in. To keep networks secure you need to have a deeper understanding of devices entering/exiting your network, their dynamic behavior, and the risk associated with them to take precise actions. This calls for developing rich and dynamic device context across multiple dimensions, combining them with machine learning algorithms to generate models and signatures for each device. This rich contextual device intelligence allows for granular visibility and control.</p> <p>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<div><h3>Architecture of Device Intelligence</h3><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div><h3>IoT Security Platform</h3><p>AI-based context generation platform for all devices</p><p>The diagram illustrates the IoT Security Platform architecture, titled "IoT Security Platform AI-based context generation platform for all devices". It is divided into two main sections: "CUSTOMER SITE" and "CLOUD".</p><p>CUSTOMER SITE:</p><ul style="list-style-type: none">Airspace Data: Represented by a box with binary code (10010110011011, 01011001101100).Radio Sensors or Access Points: Represented by a box with a signal icon.Network Data: Represented by a box with binary code (10010110011011, 01011001101100).Nextgen Access Control: A box containing the "netskope" logo.<p>Central Processing:</p><ul style="list-style-type: none">Billions of daily measurements of device characteristics: A central circular hub containing icons for OS, AI, a shield, a document, and a group of people.Models / Controls: A box connected to the central hub.<p>CLOUD:</p><ul style="list-style-type: none">Integrations: Four boxes on the left: "Asset Mgmt Integration", "Vulnerability Scanner Integration", "MDM, EDR Integration", and "Security integration".Deep Learning + Powerful Policy Engine: A central circular hub in the cloud section.Alerts/Insights: A box connected to the central hub, with text below it: "Billions of daily device behavior analyzed".UI, SIEM, Ticketing: Three boxes on the right connected to the central hub.<p><small>© 2022 Netskope Confidential. All rights reserved.</small></p></div>	

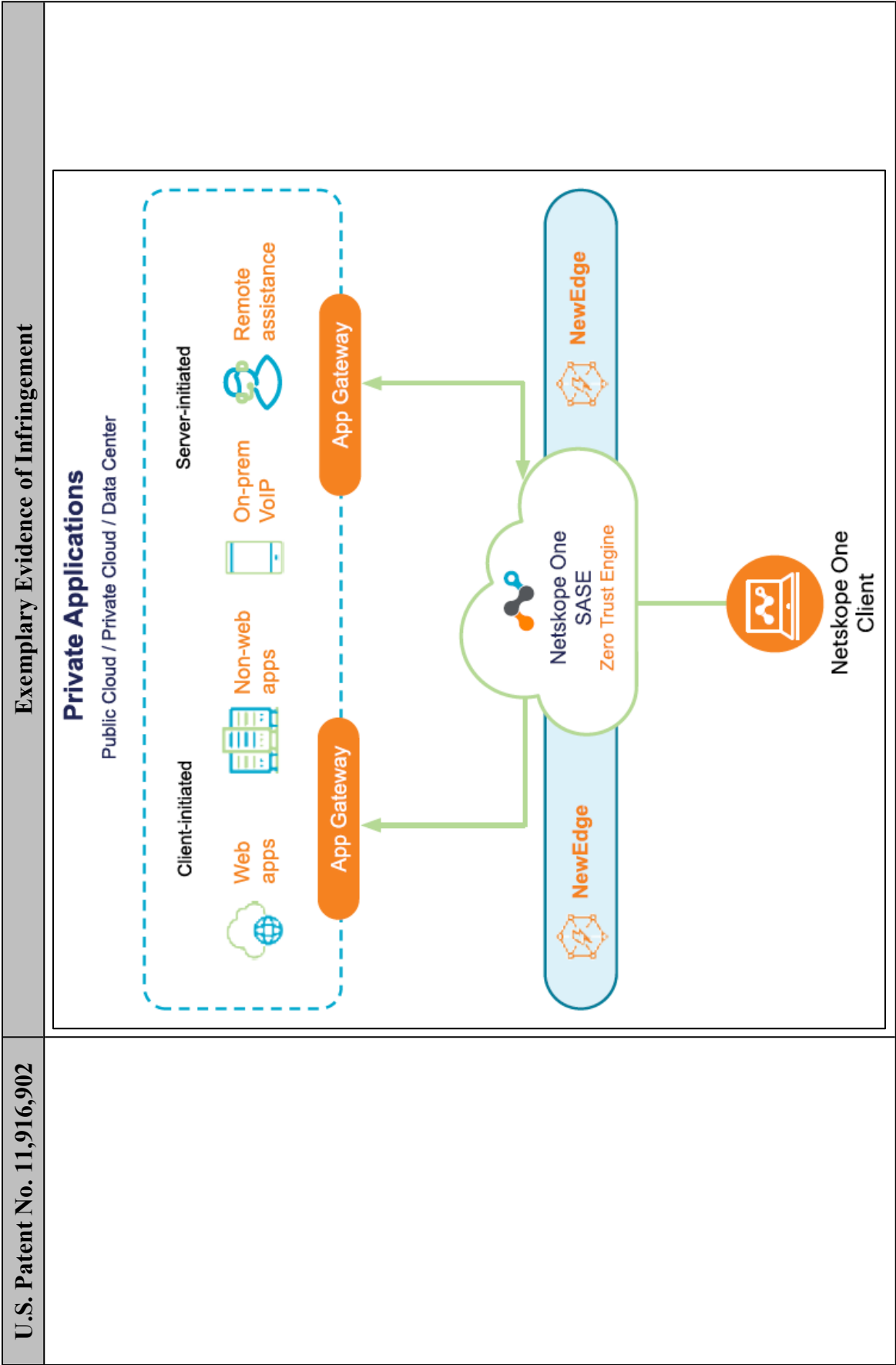
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="293 199 904 1476"><p data-bbox="326 1178 358 1436">Data Acquisition</p><ul data-bbox="399 247 870 1394" style="list-style-type: none"><li data-bbox="399 359 423 1394">• Customer environments have network sensors installed as physical or virtual appliances.<li data-bbox="451 258 570 1394">• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data.<li data-bbox="597 247 675 1394">• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<li data-bbox="703 254 776 1394">• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<li data-bbox="803 268 870 1394">• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 304 1024 1474"><p data-bbox="280 1249 313 1453">Data Analysis</p><ul data-bbox="345 346 553 1411" style="list-style-type: none"><li data-bbox="345 758 378 1411">• On the cloud, various microservices analyze the metadata.<li data-bbox="394 346 553 1411">• The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools.<p data-bbox="589 1094 621 1453">Analytics and Protection</p><ul data-bbox="654 331 998 1411" style="list-style-type: none"><li data-bbox="654 346 771 1411">• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies.<li data-bbox="787 388 865 1411">• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<li data-bbox="881 331 998 1411">• Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered.<p data-bbox="1031 632 1063 1474">https://docs.netskope.com/en/architecture-of-netskope-iot-security</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Protect Device Intelligence > Remediated Devices</div><h2>Remediated Devices</h2><p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p><p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p><ul style="list-style-type: none">• Device Name: The name or identifier of the device.• Device Type: The type of device (e.g., computer, printer, IoT device).• Device Details: By clicking on a details link, you will be navigated to a new page about the device details.• Status: The current status of the remediation action (e.g., Pending Segment, Segmented).• Triggered On: The date and time when the security policy was triggered.• Policy: The name of the security policy that was triggered.• Remediation Agent: The agent responsible for enforcing the remediation action.• Actions: A set of actions that can be performed on the device, such as:<ul style="list-style-type: none">• Add to Exception List: Excludes the device from future remediation actions.• Undo Action: Reverses the previous remediation action taken on the device.• Undo Segmentation: Reverses the previous segmentation action taken on the device.<p>https://docs.netskope.com/en/remediated-devices</p></div>

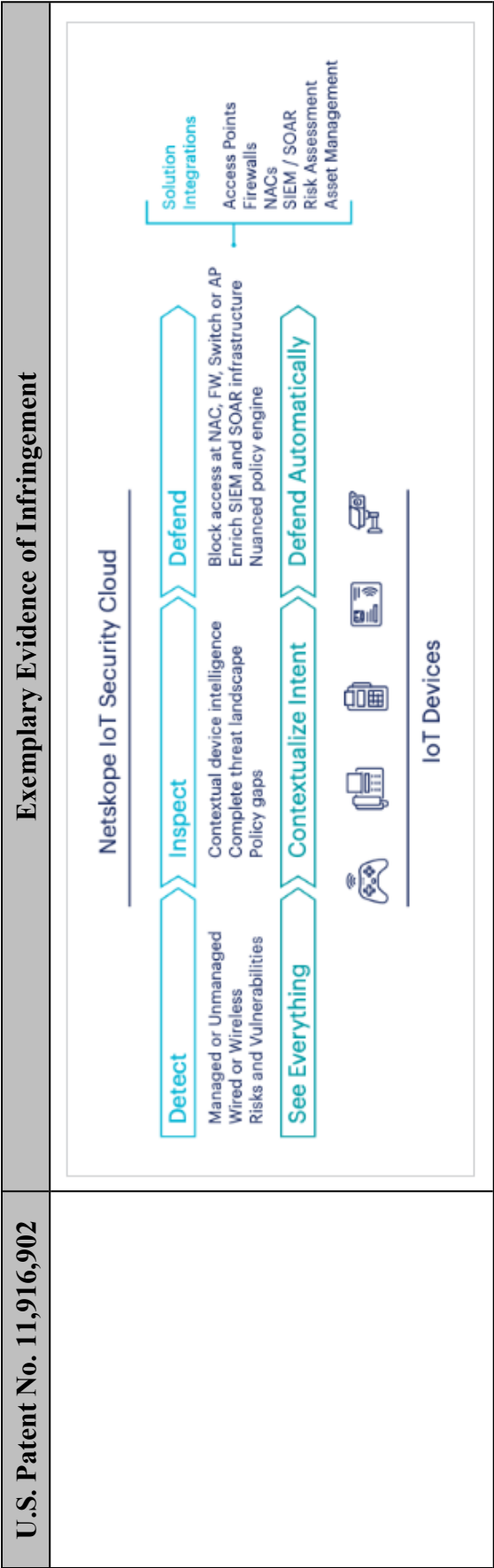
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>The Accused '902 Products include each and every element of this limitation, either literally or under the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that the Netskope Client remote device does not include a processing device that requested a grant of access from the known network of the processing device, the same function is achieved by the Netskope Private Access products, SWG, and/or related products (as referenced above) working in cooperation with the Netskope One Client to distribute this functionality across devices to achieve the same result of requesting a grant of access based in part upon on failure to identify any unsecure network element on the remote network.</p>
<p>1[e]. wherein mitigating a security issue of the unsecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.</p>	<p>The Accused '902 Products include wherein mitigating a security issue of the unsecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.</p> <p>For example, on information and belief, when a remote user seeks access to a private network employing Netskope One Private Access, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection of Internet of Things (IoT) devices in and around the network of the remote user's device for use in making access determinations for the device, and, based on these determinations, will mitigate identified security issues by initiating access to the private (known) network through private access tunnels specific to the device making the request in conjunction with one or more of micro-segmentation, isolation, and/or quarantining of devices in the known network.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 195 565 1476"> <h2 data-bbox="267 499 337 1470">Netskope One Private Access</h2> <p data-bbox="370 195 544 1476">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p> </div> <div data-bbox="565 594 1320 1476"> <p data-bbox="589 594 820 1449">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="885 625 1291 1449" style="list-style-type: none"> <li data-bbox="885 709 1117 1449">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="1161 625 1291 1449">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications </div>



U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Seamless and optimized user experience</p> <p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul style="list-style-type: none">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<div>How It Works</div> <p>Netskope Private Application Access operates through the seamless integration of the Private Access Broker and the Publisher to enforce Zero Trust principles and provide secure access. The Private Access Broker functions as a cloud-native control plane that validates user identity, device posture, and access policies in real time before granting access to applications.</p> <p>The Publisher, a lightweight connector deployed on-premises or in the cloud, establishes secure, encrypted communication between users and private applications without exposing applications to the internet. This architecture ensures that users gain access only to the specific applications they are authorized to use, with optimized routing and granular control, while eliminating the need for traditional VPNs. This combination provides a highly secure, scalable, and efficient access solution for endpoint-initiated workflows.</p> <p>NPA is illustrated in this diagram:</p> <div><p>The diagram, titled "Netskope for Private Access", illustrates the architecture of the Netskope Platform. On the left, "Remote Users" (represented by a smartphone icon) and "Offices" (represented by a building icon) are shown. Arrows indicate their connection to the "Netskope Platform". The platform is depicted as a central blue box containing four functional blocks: "Connects users to authorized apps – not your networks" (orange), "Authenticates users and devices in the cloud – not at your perimeter" (dark blue), "Classifies devices based on variety of security posture checks" (dark blue), and "Encrypts application traffic end-to-end" (light blue). To the right of the platform, a "Public Cloud" section shows logos for Microsoft Azure, Amazon Web Services, and Google Cloud Platform. Further right, a "Corporate Datacenter" is shown with server racks. A legend at the bottom right identifies the "Netskope Client" (orange icon) and "Netskope Publisher" (blue icon).</p></div> <p>https://docs.netskope.com/en/netskope-private-access</p>	

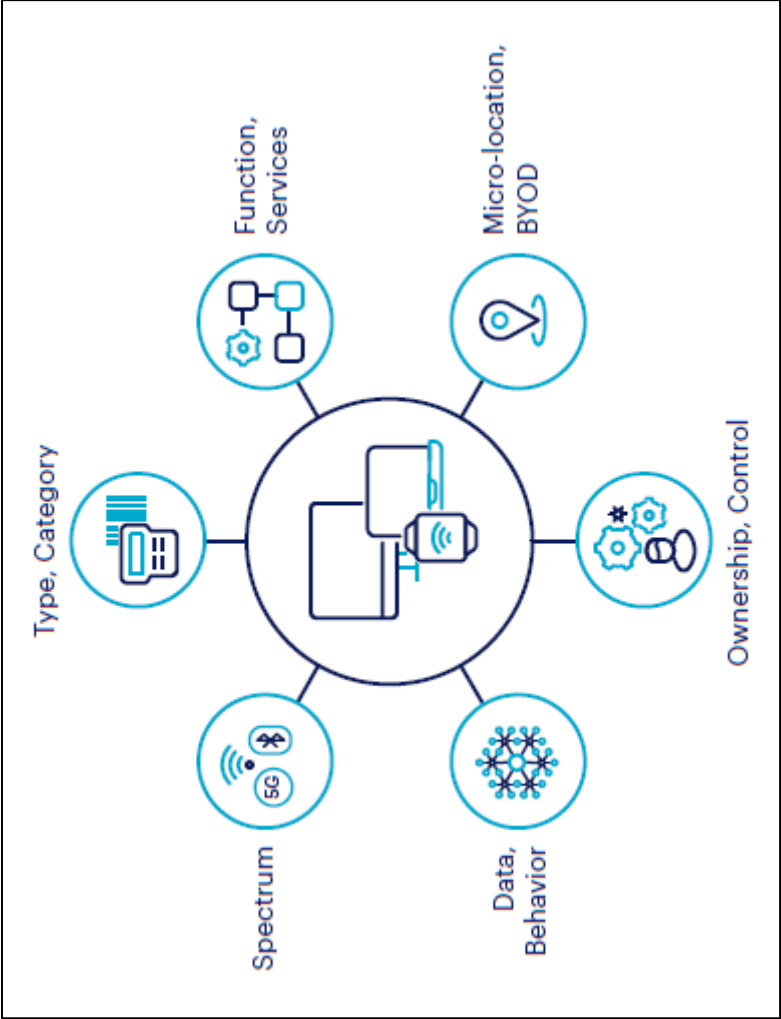


U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netkope.com/en/what-is-netkope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 940 289 1465">REALIZING ZERO TRUST FOR DEVICES</p> <p data-bbox="354 191 573 1465">Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p> <ul data-bbox="597 216 898 1417" style="list-style-type: none"> <li data-bbox="597 216 662 1417">• Granular device context: Deep context about every device, resource, and user in and around the network <li data-bbox="686 216 751 1417">• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location <li data-bbox="776 216 841 1417">• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment <li data-bbox="865 216 898 1417">• Security automation: Automated alert handling and responses to security incidents

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 422 289 1472">HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE</p> <p data-bbox="347 268 667 1472">Netskope Device Intelligence uncovers managed and unmanaged devices on the network spectrum and fingerprints those devices based on their unique characteristics across multiple dimensions. These dimensions include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. The device information is collected from multiple network interfaces, protocol information, traffic flow, and application heuristics. This is combined with organizational information from existing CMDB, tools like MDM, EDR, vulnerability assessment, firewall, times of operation and location amongst others to develop rich and dynamic device context. This context is then fed to machine learning algorithms to generate unique models and signatures for each device, which includes the following information, called HyperContext®:</p> <ul data-bbox="690 436 1122 1430" style="list-style-type: none">• Association of all the physical interfaces of the device and the spectrum of operation of each interface• Type, Category of the device and related information• OS, patches, services, and applications running on the device• Functionality or the "purpose in life" of the device• Micro location of the device, its mobility patterns, and times of visibility• Ownership information of the device and its control information• Users on the device• Behavior based analysis of all the data transmissions across all protocols and spectrums• Risk and vulnerability information, other information collected by other tools used

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>The critical role of micro-segmentation</p> <p>Over the years companies have relied on traditional network segmentation tools, such as NAC, VLANs, authentication, and access control lists (ACL) for creating subnets within the networks. The coarse-grained segmentation offered by these tools based on static device information, such as IP Address, subnets, and ACLs, leads to flat trusted zones that fail to account for dynamic device behavior or risk posture, rendering them ineffective against rogue devices. For example, if the audio video conferencing devices are statically segmented into a specific subnet, it is easy to plug in a laptop in the same subnet and sniff and snoop on the SIP communications. It is also easy to make a mistake and connect a conferencing device into other subnets, thereby creating more exposure than necessary.</p> <p>Micro-segmentation, on the other hand, is a more granular dynamic method of creating secure or trusted zones of connected devices. Micro-segmentation utilizes zero trust principles to isolate devices from one another using deep contextual information and secure them individually. Micro-segmentation is implemented in the software, using a layer that is decoupled from the underlying network hardware and NAC tools. This makes the segmentation easier to deploy and manage, providing security beyond static rules and authentication mechanisms to limit the blast radius in case of a security event.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 462 1032 1474"><p>The diagram shows a central circle containing icons of a laptop, a tablet, and a smartphone. Six lines radiate from this central circle to six surrounding circles, each with an icon and a label. Starting from the top and moving clockwise, the circles are: 1. 'Type, Category' with a bar chart icon; 2. 'Function, Services' with a gear and network icon; 3. 'Micro-location, BYOD' with a location pin icon; 4. 'Ownership, Control' with a gear and key icon; 5. 'Data, Behavior' with a network node icon; 6. 'Spectrum' with a 5G signal icon.</p></div> <p data-bbox="1036 300 1105 1474">https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

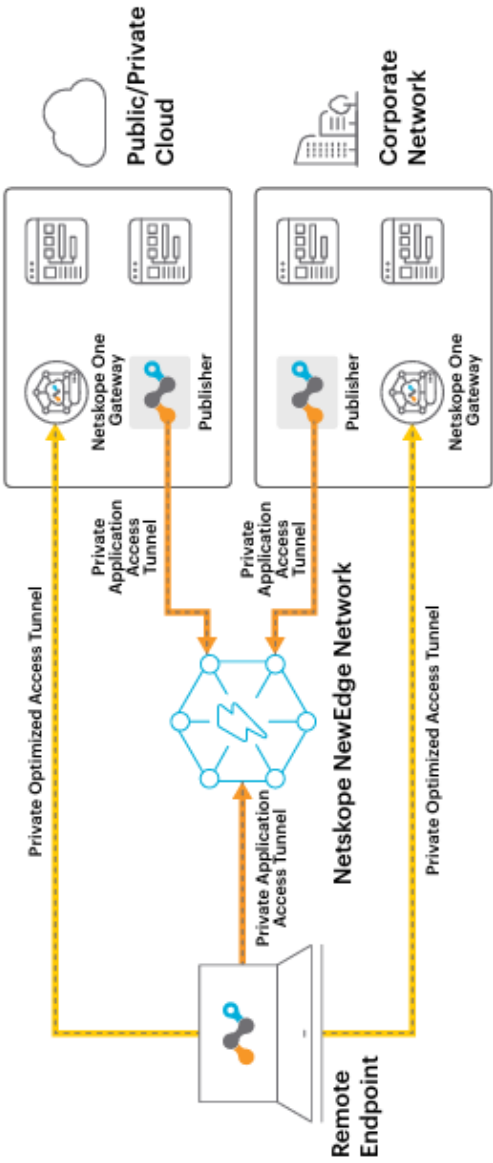
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="284 783 328 1425"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="365 287 651 1425"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="690 287 1352 1461"><p>The diagram illustrates the architecture of Device Intelligence, showing the flow of data and processing from a Customer Site to the Cloud.</p><p>Customer Site:</p><ul style="list-style-type: none">Airspace Data: Represented by a box with binary code (10010110011011, 01011001101100).Network Data: Represented by a box with binary code (10010110011011, 01011001101100).Radio Sensors or Access Points: Represented by a box with a signal icon.Network Sensor: Represented by a box with a server icon.Nextgen Access Control: A box containing the text "CUSTOMER SITE" and the "netskope" logo.<p>Processing and Analysis:</p><ul style="list-style-type: none">Billions of daily measurements of device characteristics: A central circular process involving "AI" and "ML" icons, with a "Deep Learning + Powerful Policy Engine" icon.Alerts/Insights: A box containing "Billions of daily device behavior analyzed" and "Alerts/Insights".Models / Controls: A box connected to the central processing stage.<p>Cloud Integration:</p><ul style="list-style-type: none">Asset Mgmt Integration: A box connected to the central processing stage.Vulnerability Scanner Integration: A box connected to the central processing stage.MDM, EDR Integration: A box connected to the central processing stage.Security Integration: A box connected to the central processing stage.UI: A box connected to the central processing stage.SIEM: A box connected to the central processing stage.Ticketing: A box connected to the central processing stage.CLOUD: The final destination for the data and insights.<p><small>© 2022 Netskope Confidential. All rights reserved.</small></p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p data-bbox="261 1056 297 1465">Analytics and Protection </p> <ul data-bbox="331 163 597 1430" style="list-style-type: none"><li data-bbox="331 163 402 1430">• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies.<li data-bbox="428 163 500 1430">• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<li data-bbox="526 163 597 1430">• Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <p data-bbox="613 632 646 1476">https://docs.netskope.com/en/architecture-of-netskope-iot-security</p> <div data-bbox="682 533 1070 1476"><p data-bbox="695 793 846 1459">Netskope Reference Architecture Guide</p><p data-bbox="878 646 1052 1459">How to Use Zero Trust Network Access as a Replacement for VPN with Netskope One Private Access</p></div>	

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="266 915 293 1467">Introducing Netskope One Private Access</p> <p data-bbox="318 268 492 1467">Delivered as a single solution, Netskope One Private Access integrates Zero Trust Network Access (ZTNA) and software-defined wide-area networking (SD-WAN) capabilities, enabling the complete retirement — not just partial replacement — of remote access VPNs for all relevant application access use cases, while enhancing security posture and boosting remote worker productivity with secure and seamless connectivity.</p> <p data-bbox="526 241 699 1467">The unified Netskope One Client sits in front of a converged architecture comprising Netskope One Private Application Access for access to client-initiated applications, and Netskope One Private Optimized Access to securely connect applications that require bi-directional, server-initiated traffic. The same Netskope One Client enables every other client inline Netskope service: NG-SWG, CASB Inline, FWaaS, DNS Security, Endpoint DLP.</p> <p data-bbox="734 241 914 1467">The solution utilizes zero trust principles to enhance overall security posture and reduce lateral threat movement, reduce deployment complexity, and optimize performance, and it enables ubiquitous access to corporate resources hosted anywhere through intelligent traffic steering. With Netskope One Private Access, organizations can avoid maintaining separate ZTNA and VPN clients, and instead provide consistent security for all applications with a unified client deployment.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>Key Benefits</p> <p>Enforces Zero Trust Principles</p> <p>Netskope One Private Access incorporates zero trust principles and proposes a shift from traditional network-centric access control to granular application-centric access control on a per-user or user group basis. The solution accelerates the time frame for decommissioning legacy applications and minimises associated security risks, including unauthorized lateral movement. Key benefits include:</p> <ul style="list-style-type: none"> • Identity- and context-aware, least-privileged access to private applications hosted in public clouds or on-premises data centers. • Device Classification options to assess the posture of the client before providing access to private applications hosted in public clouds or on-premises data centers. • Facilitating the connectivity through the ZTNA broker in Netskope One platform. The applications are hidden from discovery, and access is restricted only to authenticated and authorised users. • Reducing the opportunities for lateral movement of threats within the private networks and limiting the blast radius. • Eliminating the dependence on public-facing VPNs or open inbound firewall ports for application access, securing networks from threats and DDoS attacks. <p>Secures All Enterprise Applications</p> <p>Netskope One Private Access also supports server-to-client traffic connectivity, enabling access to both legacy and modern applications through a single client. Key benefits include:</p> <ul style="list-style-type: none"> • Eliminating the need to maintain two separate solutions — VPN and ZTNA — for accessing all private applications and achieving greater cost savings by reducing capital and operational expenditure. • Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all private applications. 	

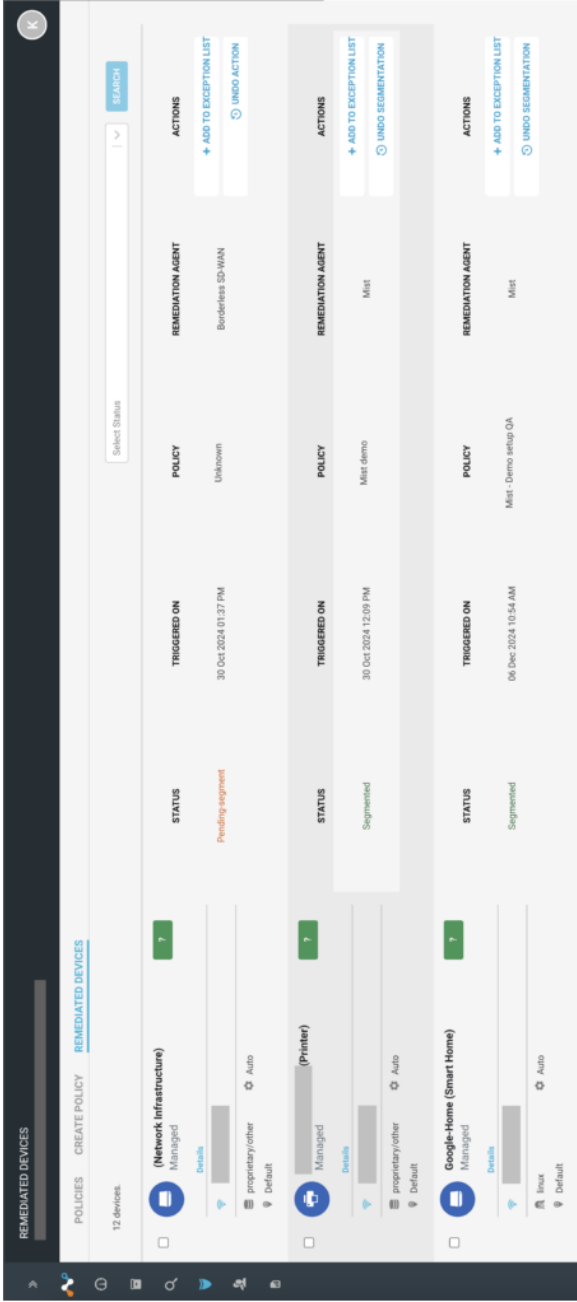
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="261 989 289 1461">Delivers a Phenomenal User Experience</div> <div data-bbox="313 226 378 1461"><p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key benefits include:</p><ul style="list-style-type: none">• Automatic traffic steering by the Netskope Client for connecting authorised users directly to specific resources regardless of where it is hosted. Strategically positioned Netskope NewEdge Network point of presence (PoP) helps achieve lowest possible latency and round-trip time for application access.</div> <div data-bbox="553 506 581 1461">Full Zero Trust Application Access: Netskope One Private Unified Access</div> <div data-bbox="605 241 703 1461"><p>Combining Private Application Access and Private Optimized Access capabilities on the same Endpoint, Netskope enables organisations to apply granular zero trust access to all Internal Applications, and support all use cases for a VPN replacement.</p></div> <div data-bbox="732 233 1243 1461"><p>The diagram illustrates the Netskope One Private Unified Access architecture. On the left, a 'Remote User' is shown with icons for a desktop, laptop, and mobile device. The user's traffic enters through a 'Physical Interface' and is routed to a 'Virtual Interface'. From the Virtual Interface, two paths are shown: 1) A 'Private Application Access Tunnel' (orange line) that connects to the 'Netskope NewEdge Network' (represented by a cloud with a lightning bolt). This network then connects to the 'Corporate Network' (represented by a server rack icon) via another 'Private Application Access Tunnel' (orange line). 2) A 'Private Optimized Access Tunnel' (green dashed line) that connects directly to a 'Firewall' in the Corporate Network. The Corporate Network contains various services including a 'Publisher', 'DNS', 'Mail', and a 'Netskope One Gateway'. The diagram shows how Netskope integrates with existing corporate infrastructure to provide secure, optimized access to private applications.</p></div>

<p>U.S. Patent No. 11,916,902</p>	<p style="text-align: center;">Exemplary Evidence of Infringement</p> <p>Netskope One Private Unified Access vastly improves the user experience by supporting multiple Private Application Access applications through a single connection to the NewEdge Network. Additionally, it supports multiple Private Data Centers or Private/Public Clouds. This enables customers to not only streamline access in private Data Centers or Private/Public Clouds. This enables customers to not only streamline access and improve performance for all types of private applications, but also ensure granular zero trust-based access.</p>  <p>The diagram illustrates the Netskope One Private Unified Access architecture. A Remote Endpoint (represented by a laptop icon) is connected to the Netskope NewEdge Network (represented by a central cloud icon with a lightning bolt). The NewEdge Network is connected to two Publisher environments. The Public/Private Cloud environment includes a Netskope One Gateway and a Publisher. The Corporate Network environment also includes a Netskope One Gateway and a Publisher. All connections between the Remote Endpoint, the NewEdge Network, and the Publishers are labeled as Private Application Access Tunnel or Private Optimized Access Tunnel.</p> <p>2024-12-Reference-Architecture-Guide-for-ZTNA-Next-RA-709-3-1.pdf</p>
--	--

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><h3>Remediated Devices</h3><p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p><p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p><ul style="list-style-type: none">• Device Name: The name or identifier of the device.• Device Type: The type of device (e.g., computer, printer, IoT device).• Device Details: By clicking on a details link, you will be navigated to a new page about the device details.• Status: The current status of the remediation action (e.g., Pending Segment, Segmented).• Triggered On: The date and time when the security policy was triggered.• Policy: The name of the security policy that was triggered.• Remediation Agent: The agent responsible for enforcing the remediation action.• Actions: A set of actions that can be performed on the device, such as:<ul style="list-style-type: none">• Add to Exception List: Excludes the device from future remediation actions.• Undo Action: Reverses the previous remediation action taken on the device.• Undo Segmentation: Reverses the previous segmentation action taken on the device.</div>

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement



<https://docs.netkope.com/en/remediated-devices>

The Accused '902 Products include each and every element of this limitation, either literally or under the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that tunneling, micro-segmentation, isolation, or quarantining is not a virtual private network or virtual private network application because it is a replacement thereof, the same function is achieved by the Netskope Private Access products, SWG, and/or related products (as referenced above) working in cooperation with the Netskope One Client to combine, unify, and/or distribute this functionality across devices to achieve the same result of mitigating the security issue of the unsecure network element by virtually providing secured network access.

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>2. The method of claim 1, wherein access by the processing device to the known network is granted upon a combination of the requesting a grant of access from the known network to the processing device and a correct authorization credential presented by the processing device to the known network.</p> <p>For example, the authorization further includes granting or denying access based on a correct authorization credential presented by the a remote user device having one or more processing devices executing the Netskope One Client (a known access device).</p>	<div data-bbox="548 373 1045 1474"><h1 data-bbox="565 709 662 1474">What is ZTNA?</h1><p data-bbox="743 394 1036 1474">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 304 651 1470"><p data-bbox="256 1018 297 1470">Zero Trust Security Principles</p><p data-bbox="313 304 438 1470">ZTNA creates a new security framework, based on the <u>zero trust security model</u>, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p><p data-bbox="464 304 524 1470">Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p><p data-bbox="550 304 643 1470">Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p></div> <p data-bbox="659 478 691 1470">https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div>Seamless and optimized user experience<p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p><p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p><ul style="list-style-type: none">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity.<p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="293 1178 337 1465">Netskope One</p> <h1 data-bbox="386 1121 500 1465">Client</h1> <p data-bbox="597 216 678 1465">Netskope One Client is the industry's first unified SASE client, unifying connectivity to their web, cloud, AI, private apps, and UCaaS services and providing endpoint DLP controls.</p> <h2 data-bbox="711 527 792 1465">A simplified user experience</h2> <p data-bbox="857 447 1117 1465">Easy to use, lightweight and highly performant, Netskope One Client steers user traffic through the <u>Netskope One</u> platform. Netskope One Client centralized configuration, deployment, support, and troubleshooting delivers comprehensive security and control across the borderless modern threat landscape.</p> <p data-bbox="1138 877 1166 1465">https://www.netskope.com/netkskope-one/client</p>
<p data-bbox="1224 1493 1365 1896">3. The method of claim 1, wherein the unsecure network element is an Internet of Things (IoT) device.</p>	<p data-bbox="1224 216 1289 1465">The Accused '902 Products include wherein the unsecure network element is an Internet of Things (IoT) device.</p> <p data-bbox="1338 180 1403 1465">For example, Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection of Internet of Things (IoT) devices in and around the network of the remote</p>

U.S. Patent No. 11,916,902	<div data-bbox="203 562 240 1071">Exemplary Evidence of Infringement</div> <div data-bbox="256 205 326 1478"> <p>user's device for use in making access determinations for the device and will correspondingly make access decisions responsive to identification on an unsecure IoT device.</p> </div> <div data-bbox="375 170 831 1470"> <p>The diagram illustrates the Netskope IoT Security Cloud architecture. It shows a flow from IoT Devices (represented by icons of a game controller, printer, server, and camera) through four sequential stages: Detect (Managed or Unmanaged, Wired or Wireless, Risks and Vulnerabilities), Inspect (Contextual device intelligence, Complete threat landscape, Policy gaps), Contextualize Intent (Block access at NAC, FW, Switch or AP; Enrich SIEM and SOAR infrastructure; Nuanced policy engine), and Defend (Defend Automatically). The final stage is Solution Integrations, which includes Access Points, Firewalls, NACs, SIEM / SOAR, Risk Assessment, and Asset Management.</p> </div>
----------------------------	--

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 783 326 1423"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="365 289 651 1423"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="695 275 1357 1461"><p>The diagram illustrates the 'IoT Security Platform' as an 'AI-based context generation platform for all devices'. It is divided into two main sections: 'CUSTOMER SITE' and 'CLOUD'. CUSTOMER SITE: Data flows from 'Radio Sensors or Access Points' and 'Network Sensor' to 'Nextgen Access Control'. This data is categorized as 'Airspace Data' (100100110011001100) and 'Network Data' (100100110011001100). Central Processing: Data is processed through 'Models / Controls' and 'Billions of daily measurements of device characteristics' (including OS, AI, and security icons). CLOUD: Data is processed by a 'Deep Learning Powerful Policy Engine' which integrates 'Asset Mgmt Integration', 'MDM, EDR Integration', 'Vulnerability Scanner Integration', and 'Security Integration'. This leads to 'Alerts/Insights' and 'Billions of daily device behavior analyzed'. The final output is sent to 'UI', 'SIEM', and 'Ticketing'.</p></div> <div data-bbox="1365 630 1398 1480"><p>https://docs.netskope.com/en/architecture-of-netskope-iot-security</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
4. The method of claim 1, wherein administration of the processing device and the known network is controlled by a common administration entity.	<p>The Accused '902 Products include wherein administration of the processing device and the known network is controlled by a common administration entity.</p> <p>For example, the Netskope Private Access products, SWG, and/or related products, features or functions of the Netskope One Platform, includes a single point to administer and control the Netskope One Platform and Netskope NewEdge Network.</p> <div><h2>Netskope One Private Access features and benefits</h2><div><div>Full VPN, NAC replacement ></div><div>AI-driven automated policy optimization ></div><div>Flexible access methods ></div><div>Built-in threat and data protection ></div><div>Built-in device intelligence ></div><div>Unified visibility ></div></div><div><div></div><div>Get real-time, end-to-end insights into private app performance with Netskope One Digital Experience Management (DEM). Path-level metrics accelerate troubleshooting, reduce mean-time-to-resolution (MTTR), and simplify compliance, ensuring high-performance, secure access with a single source of truth.</div><div><div>></div><div>Solution brief</div></div></div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><h2>Netskope One Private Access features and benefits</h2><div><div>Full VPN, NAC replacement ></div><div>AI-driven automated policy optimization ></div><div>Flexible access methods ></div><div>Built-in threat and data protection ></div><div>Built-in device intelligence <</div><div>Unified visibility ></div></div><div><p>Netskope UZTNA extends zero trust beyond users to every connected device. With Device Intelligence, organizations gain visibility, real-time risk scoring, and context-aware access for IoT and OT systems, securing branches, campuses, and factories while reducing attack surface at scale.</p><div>> Learn about Device Intelligence</div></div><p>https://www.netskope.com/products/private-access</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 197 565 1470"><h2 data-bbox="267 499 337 1470">Netskope One Private Access</h2><p data-bbox="370 197 544 1470">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p></div> <div data-bbox="565 594 1317 1470"><p data-bbox="589 594 820 1444">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p><ul data-bbox="885 625 1291 1444" style="list-style-type: none"><li data-bbox="885 625 1117 1444">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure<li data-bbox="1161 625 1291 1444">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications</div> <div data-bbox="1317 197 1393 1470"><p data-bbox="1317 197 1393 1470">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Executive Dashboard</div><div><h2>Executive Dashboard</h2><p>Device Intelligence offers a comprehensive suite of dashboards designed to monitor and enhance product health across various domains. The Executive Dashboard serves as the central hub, providing a high-level overview of key performance indicators (KPIs) from three specialized areas: Security, Network, and IT Operations. Each of these dashboards offers in-depth insights into their respective domains, enabling stakeholders to make informed, data-driven decisions.</p><p>In this article, we will delve into the functionalities and benefits of each dashboard, illustrating how they collectively contribute to a holistic understanding of your product's health.</p></div></div>

[illegible]

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>upon denying access to the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.</p>	<p>network via another remote network.</p> <p>For example, Netskope’s Private Access products and Netskope One Platform deny access to the Netskope NewEdge Network, and under information and belief the user is provided a message of this denial and requesting the user to connect via other means.</p> <div data-bbox="475 371 972 1476"> <h2 data-bbox="488 705 586 1465">What is ZTNA?</h2> <p data-bbox="667 392 959 1465">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it’s become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p> </div> <div data-bbox="972 304 1373 1476"> <h3 data-bbox="980 1024 1016 1465">Zero Trust Security Principles</h3> <p data-bbox="1032 321 1154 1465">ZTNA creates a new security framework, based on the <u>zero trust security model</u>, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user’s identity and security posture before connecting users to the authorized applications.</p> <p data-bbox="1183 321 1243 1465">Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p> <p data-bbox="1273 359 1362 1465">Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p> </div> <p data-bbox="1378 478 1411 1476">https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><p>Seamless and optimized user experience</p><p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p><p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p><ul style="list-style-type: none">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity.<p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>For example, Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection (e.g., policy actions like blocking devices) in response to the information collected about devices in and around the network of the remote user's device for use in making access determinations for the device, and under information and belief the user is provided a message of this denial and requesting the user to connect via other means.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-nsn-iot-security</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="272 317 350 1444">Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul data-bbox="386 239 1036 1398" style="list-style-type: none"><li data-bbox="386 239 505 1398">• Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior.<li data-bbox="532 239 695 1398">• Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR.<li data-bbox="722 239 846 1398">• Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations.<li data-bbox="873 239 1036 1398">• Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p data-bbox="1089 722 1122 1476">https://docs.netkope.com/en/what-is-netkope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 934 289 1465">REALIZING ZERO TRUST FOR DEVICES</p> <p data-bbox="354 176 578 1465">Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p> <ul data-bbox="605 197 906 1415" style="list-style-type: none"> <li data-bbox="605 197 667 1415">• Granular device context: Deep context about every device, resource, and user in and around the network <li data-bbox="695 197 756 1415">• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location <li data-bbox="784 197 846 1415">• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment <li data-bbox="873 197 906 1415">• Security automation: Automated alert handling and responses to security incidents

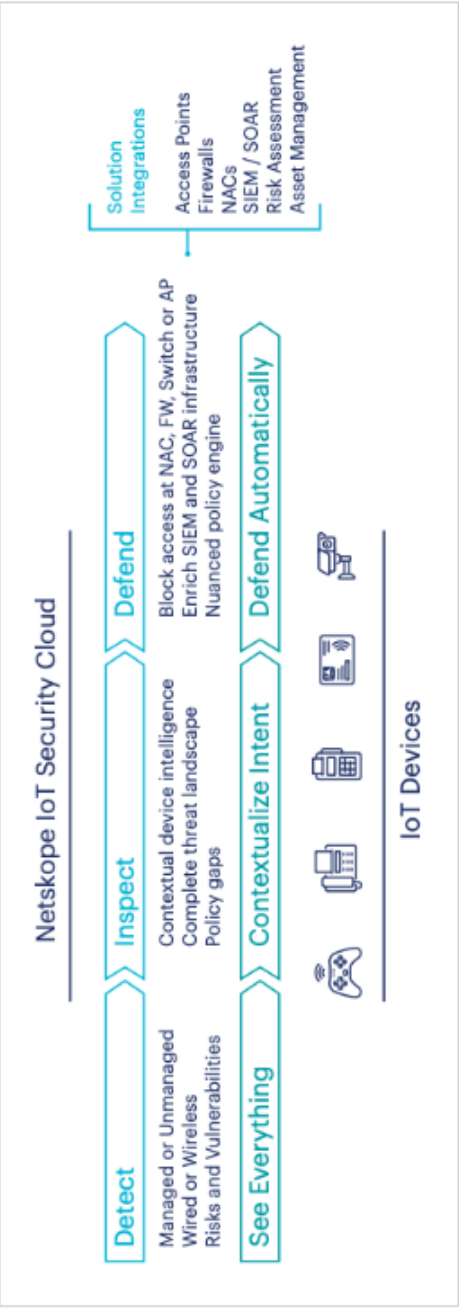
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Need for granular device context</p> <p>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to ensure security, and enforce right access control across the network. Current device fingerprinting technologies boil down to type, category, OS, version, etc. which are woefully inadequate for correctly profiling the device behavior and setting adequate controls to protect the device and the infrastructure it operates in. To keep networks secure you need to have a deeper understanding of devices entering/exiting your network, their dynamic behavior, and the risk associated with them to take precise actions. This calls for developing rich and dynamic device context across multiple dimensions, combining them with machine learning algorithms to generate models and signatures for each device. This rich contextual device intelligence allows for granular visibility and control.</p> <p>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

U.S. Patent No. 11,916,902	<div>Exemplary Evidence of Infringement</div> <div><div>Architecture of Device Intelligence</div><div><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div></div>	<div><div><div><div><div>IoT Security Platform</div><div>AI-based context generation platform for all devices</div></div><div><div><div><div><div>10010110011011 010110011001100</div><div>Airspace Data</div></div><div><div>Radio Sensors or Access Points</div><div><div>10010110011011 010110011001100</div><div>Network Data</div></div><div>Nextgen Access Control</div></div><div><div><div>Billions of daily measurements of device characteristics</div><div><div>OS AI Security</div></div><div>Models / Controls</div></div><div><div><div>Asset Mgmt Integration</div><div>Vulnerability Scanner Integration</div><div>MDM, EDR Integration</div><div>Security Integration</div></div><div><div>Deep Learning + Powerful Policy Engine</div><div>Billions of daily device behavior analyzed</div><div>Alerts/Insights</div></div><div><div>UI</div><div>SIEM</div><div>Ticketing</div></div><div>CLOUD</div></div></div></div><div><div><div><div>2017 © Netskope Confidential. All rights reserved.</div></div></div></div></div></div></div></div></div>
----------------------------	---	--

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="326 1178 358 1436">Data Acquisition</p> <ul data-bbox="396 247 870 1394" style="list-style-type: none"> <li data-bbox="396 354 428 1394">• Customer environments have network sensors installed as physical or virtual appliances. <li data-bbox="451 247 570 1394">• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data. <li data-bbox="592 247 672 1394">• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC. <li data-bbox="695 247 774 1394">• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices. <li data-bbox="797 264 870 1394">• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 306 1024 1472"><p data-bbox="280 1251 313 1451">Data Analysis</p><ul data-bbox="347 344 553 1409" style="list-style-type: none"><li data-bbox="347 758 380 1409">• On the cloud, various microservices analyze the metadata.<li data-bbox="399 344 553 1409">• The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools.<p data-bbox="591 1094 623 1451">Analytics and Protection</p><ul data-bbox="657 331 1000 1409" style="list-style-type: none"><li data-bbox="657 344 773 1409">• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies.<li data-bbox="792 386 865 1409">• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<li data-bbox="885 331 1000 1409">• Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered.<p data-bbox="1036 632 1068 1472">https://docs.netkope.com/en/architecture-of-netkope-iot-security</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 420 1344 1474"> <p>Home > Device Intelligence > Protect Device Intelligence > Remediated Devices</p> <h2>Remediated Devices</h2> <p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p> <p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p> <ul style="list-style-type: none"> • Device Name: The name or identifier of the device. • Device Type: The type of device (e.g., computer, printer, IoT device). • Device Details: By clicking on a details link, you will be navigated to a new page about the device details. • Status: The current status of the remediation action (e.g., Pending Segment, Segmented). • Triggered On: The date and time when the security policy was triggered. • Policy: The name of the security policy that was triggered. • Remediation Agent: The agent responsible for enforcing the remediation action. • Actions: A set of actions that can be performed on the device, such as: <ul style="list-style-type: none"> • Add to Exception List: Excludes the device from future remediation actions. • Undo Action: Reverses the previous remediation action taken on the device. • Undo Segmentation: Reverses the previous segmentation action taken on the device. <p>https://docs.netskope.com/en/remediated-devices</p> </div>

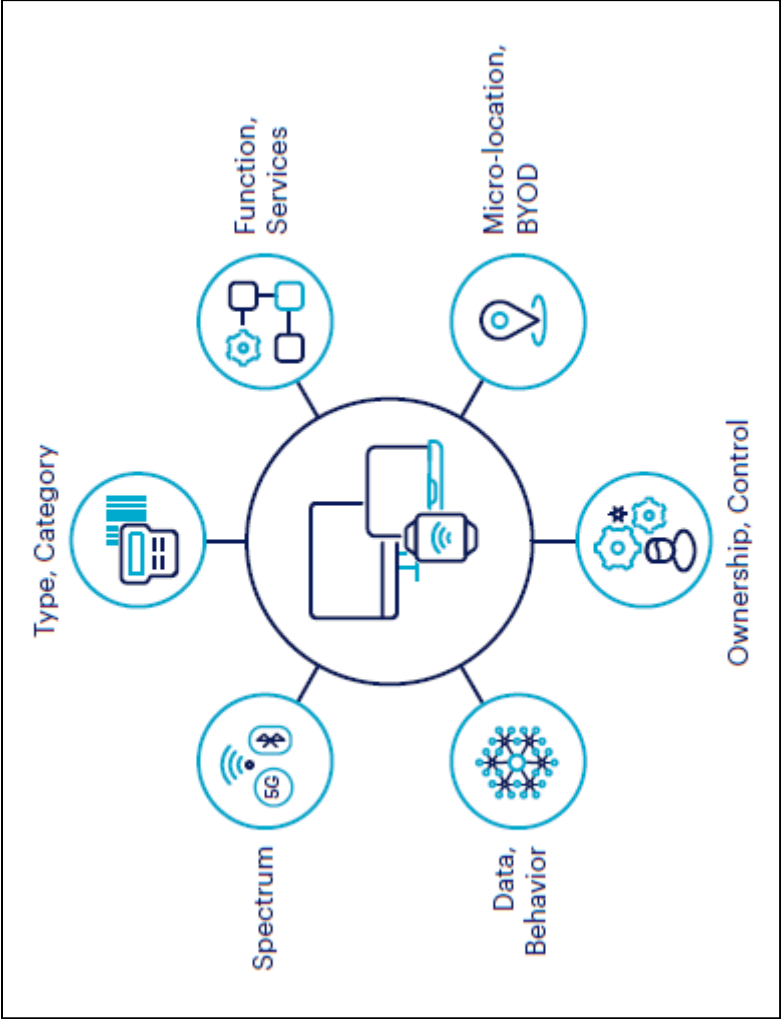
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>6. The method of claim 1, the method further comprising: mitigating a security issue of the insecure network element; and based at least in part upon the insecure network element, requesting a grant of access from the known network to the processing device.</p>	<p>The Accused '902 Products include mitigating a security issue of the insecure network element; and based at least in part upon mitigating the security issue of the insecure network element, requesting a grant of access from the known network to the processing device.</p> <p>For example, Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection of Internet of Things (IoT) devices in and around the network of the remote user's device for use in making access determinations for the device, and grant access to previously denied devices when security issues of the unsecured network element have been mitigated.</p>  <p>The diagram illustrates the Netskope IoT Security Cloud architecture. It shows a flow from IoT Devices (represented by icons of a game controller, a printer, a server, a smartphone, and a car) through three main stages: Detect, Inspect, and Defend. The Detect stage includes 'Managed or Unmanaged Wired or Wireless Risks and Vulnerabilities' and 'See Everything'. The Inspect stage includes 'Contextual device intelligence', 'Complete threat landscape', and 'Policy gaps', leading to 'Contextualize Intent'. The Defend stage includes 'Block access at NAC, FW, Switch or AP', 'Enrich SIEM and SOAR infrastructure', and 'Nuanced policy engine', leading to 'Defend Automatically'. Finally, the architecture connects to 'Solution Integrations' which include 'Access Points', 'Firewalls', 'NACs', 'SIEM / SOAR', 'Risk Assessment', and 'Asset Management'.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>REALIZING ZERO TRUST FOR DEVICES</div><div>Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</div><div><ul style="list-style-type: none">• Granular device context: Deep context about every device, resource, and user in and around the network• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment• Security automation: Automated alert handling and responses to security incidents</div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 327 293 1467">HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE</p> <p data-bbox="354 149 699 1467">Netskope Device Intelligence uncovers managed and unmanaged devices on the network spectrum and fingerprints those devices based on their unique characteristics across multiple dimensions. These dimensions include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. The device information is collected from multiple network interfaces, protocol information, traffic flow, and application heuristics. This is combined with organizational information from existing CMDB, tools like MDM, EDR, vulnerability assessment, firewall, times of operation and location amongst others to develop rich and dynamic device context. This context is then fed to machine learning algorithms to generate unique models and signatures for each device, which includes the following information, called HyperContext®:</p> <ul data-bbox="727 149 1203 1467" style="list-style-type: none"> • Association of all the physical interfaces of the device and the spectrum of operation of each interface • Type, Category of the device and related information • OS, patches, services, and applications running on the device • Functionality or the “purpose in life” of the device • Micro location of the device, its mobility patterns, and times of visibility • Ownership information of the device and its control information • Users on the device • Behavior based analysis of all the data transmissions across all protocols and spectrums • Risk and vulnerability information, other information collected by other tools used

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="272 919 305 1465">The critical role of micro-segmentation</p> <p data-bbox="326 176 630 1465">Over the years companies have relied on traditional network segmentation tools, such as NAC, VLANs, authentication, and access control lists (ACL) for creating subnets within the networks. The coarse-grained segmentation offered by these tools based on static device information, such as IP Address, subnets, and ACLs, leads to flat trusted zones that fail to account for dynamic device behavior or risk posture, rendering them ineffective against rogue devices. For example, if the audio video conferencing devices are statically segmented into a specific subnet, it is easy to plug in a laptop in the same subnet and sniff and snoop on the SIP communications. It is also easy to make a mistake and connect a conferencing device into other subnets, thereby creating more exposure than necessary.</p> <p data-bbox="667 159 889 1465">Micro-segmentation, on the other hand, is a more granular dynamic method of creating secure or trusted zones of connected devices. Micro-segmentation utilizes zero trust principles to isolate devices from one another using deep contextual information and secure them individually. Micro-segmentation is implemented in the software, using a layer that is decoupled from the underlying network hardware and NAC tools. This makes the segmentation easier to deploy and manage, providing security beyond static rules and authentication mechanisms to limit the blast radius in case of a security event.</p>

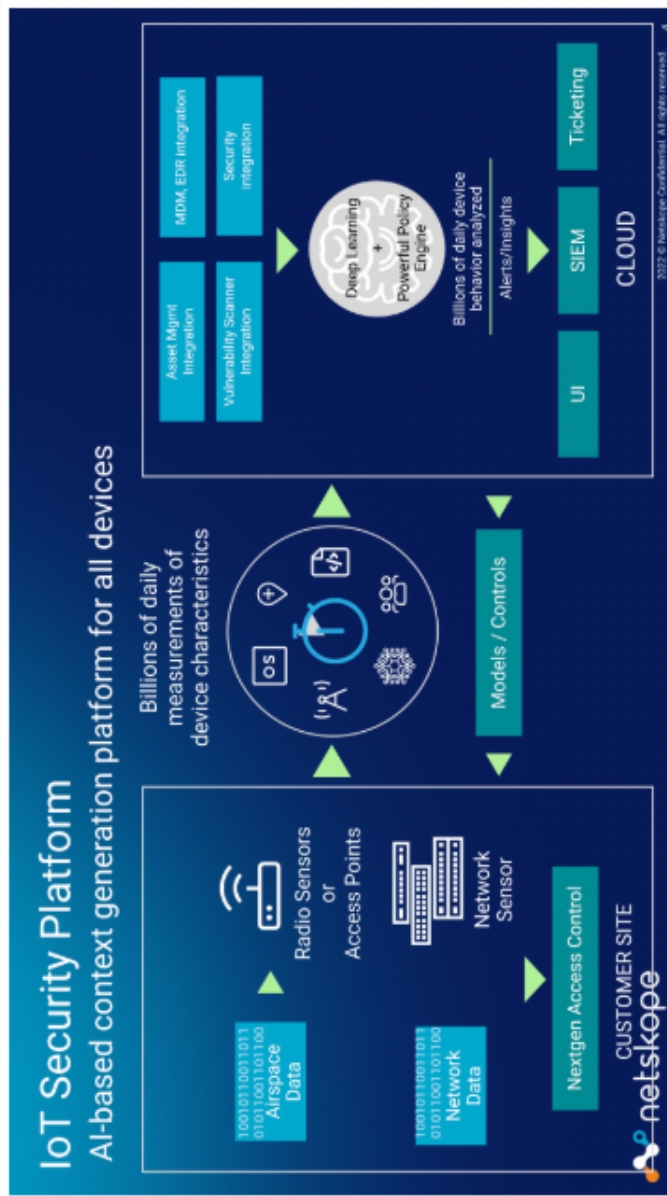
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 462 1032 1474"><p>The diagram illustrates a central device, represented by a laptop and a smartphone, connected to six categories of data or services. The categories are arranged in a circle around the central device, each with a corresponding icon in a blue circle. The categories are: Type, Category (top-left, icon of a document with a bar chart), Spectrum (top, icon of a radio tower and signal waves), Data, Behavior (top-right, icon of a network of nodes), Ownership, Control (bottom-right, icon of a person with a gear), Micro-location, BYOD (bottom, icon of a location pin), and Function, Services (bottom-left, icon of a gear and a document). The text 'Type, Category' is written vertically to the left of the top-left icon, 'Spectrum' is written vertically to the left of the top icon, 'Data, Behavior' is written vertically to the left of the top-right icon, 'Ownership, Control' is written vertically to the right of the bottom-right icon, 'Micro-location, BYOD' is written vertically to the right of the bottom icon, and 'Function, Services' is written vertically to the right of the bottom-left icon.</p></div> <p data-bbox="1036 300 1105 1474">https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement

Architecture of Device Intelligence

An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.

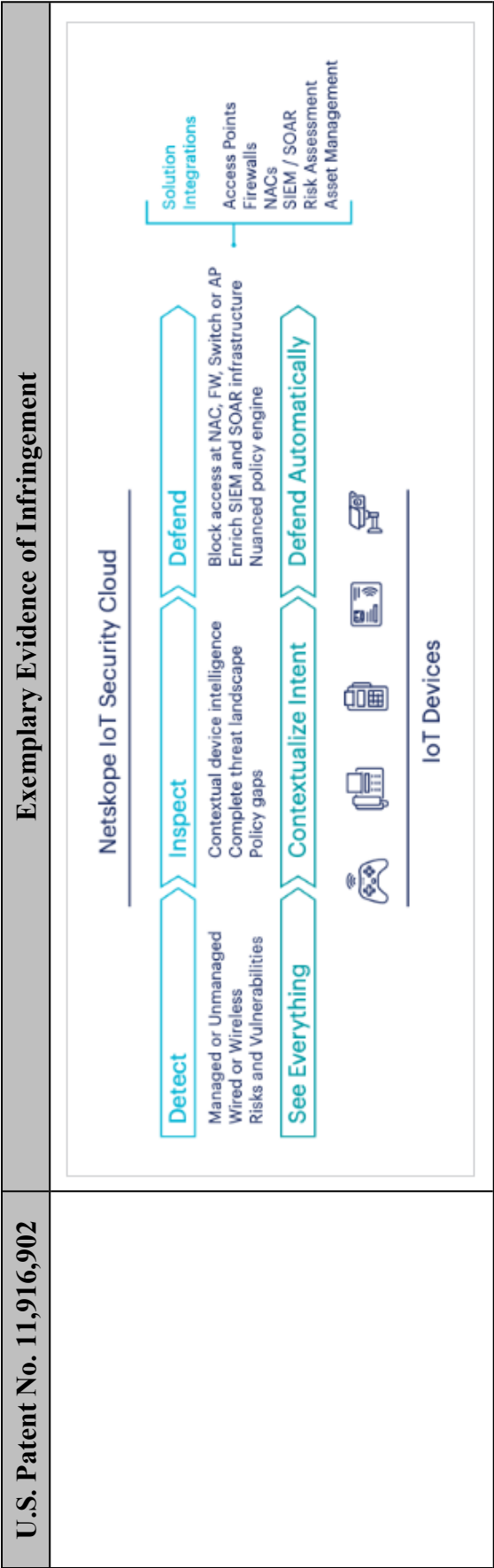


U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 846 297 1908">Analytics and Protection </p> <ul data-bbox="329 846 597 1908" style="list-style-type: none"> <li data-bbox="329 846 410 1908">• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies. <li data-bbox="427 846 508 1908">• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies. <li data-bbox="524 846 597 1908">• Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <p data-bbox="613 846 646 1908">https://docs.netskope.com/en/architecture-of-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="266 1094 305 1455">Remediated Devices</p> <p data-bbox="342 226 451 1455">Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p> <p data-bbox="483 226 509 1455">You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p> <ul data-bbox="542 310 1146 1419" style="list-style-type: none"> • Device Name: The name or identifier of the device. • Device Type: The type of device (e.g., computer, printer, IoT device). • Device Details: By clicking on a details link, you will be navigated to a new page about the device details. • Status: The current status of the remediation action (e.g., Pending Segment, Segmented). • Triggered On: The date and time when the security policy was triggered. • Policy: The name of the security policy that was triggered. • Remediation Agent: The agent responsible for enforcing the remediation action. • Actions: A set of actions that can be performed on the device, such as: <ul data-bbox="1003 436 1146 1356" style="list-style-type: none"> • Add to Exception List: Excludes the device from future remediation actions. • Undo Action: Reverses the previous remediation action taken on the device. • Undo Segmentation: Reverses the previous segmentation action taken on the device.

U.S. Patent No. 11,916,902	<div><div>REMEDIATED DEVICES</div><div><div>POLICIES</div><div>CREATE POLICY</div><div>REMEDIATED DEVICES</div></div><div>12 devices</div><div><div><div><div><div></div><div>(Network Infrastructure)</div><div>Managed</div></div><div>Details</div><div><div>proprietary:other</div><div>Auto</div><div>Default</div></div></div><div><div><div></div><div>(Printer)</div><div>Managed</div></div><div>Details</div><div><div>proprietary:other</div><div>Auto</div><div>Default</div></div></div><div><div><div></div><div>Google-Home (Smart Home)</div><div>Managed</div></div><div>Details</div><div><div>hour</div><div>Auto</div><div>Default</div></div></div></div><div><div><div>STATUS</div><div>Pending segment</div></div><div><div>TRIGGERED ON</div><div>30 Oct 2024 01:37 PM</div></div><div><div>POLICY</div><div>Unknown</div></div><div><div>REMEDIATION AGENT</div><div>Borderless SD-WAN</div></div><div><div>ACTIONS</div><div>+ ADD TO EXCEPTION LIST</div><div>UNDO ACTION</div></div></div><div><div><div>STATUS</div><div>Segmented</div></div><div><div>TRIGGERED ON</div><div>30 Oct 2024 12:09 PM</div></div><div><div>POLICY</div><div>Mini demo</div></div><div><div>REMEDIATION AGENT</div><div>Mini</div></div><div><div>ACTIONS</div><div>+ ADD TO EXCEPTION LIST</div><div>UNDO SEGMENTATION</div></div></div><div><div><div>STATUS</div><div>Segmented</div></div><div><div>TRIGGERED ON</div><div>06 Dec 2024 10:54 AM</div></div><div><div>POLICY</div><div>Mini - Demo setup QA</div></div><div><div>REMEDIATION AGENT</div><div>Mini</div></div><div><div>ACTIONS</div><div>+ ADD TO EXCEPTION LIST</div><div>UNDO SEGMENTATION</div></div></div></div></div> <div>https://docs.netkope.com/en/remediated-devices</div>	<p>7. The method of claim 6, wherein mitigating the security issue of the unsecure network element includes connecting, by the processing device, the processing device to another remote network.</p>
Exemplary Evidence of Infringement	<p>The Accused '902 Products include mitigating the security issue of the unsecure network element includes connecting, by the processing device, the processing device to another remote network.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection of Internet of Things (IoT) devices in and around the network of the remote user's device for use in making access determinations for the device, and mitigates security issues by segmenting or isolating/quarantining devices until addressed.</p>	

7. The method of claim 6, wherein mitigating the security issue of the unsecure network element includes connecting, by the processing device, the processing device to another remote network.

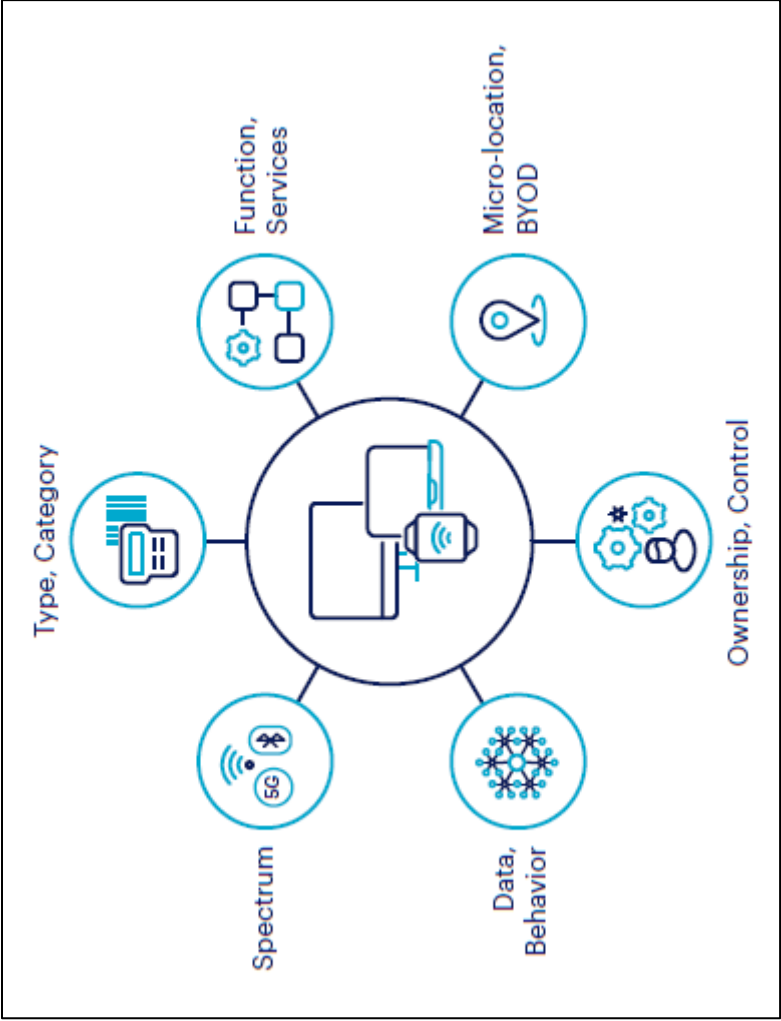


U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>REALIZING ZERO TRUST FOR DEVICES</div><div>Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</div><div><ul style="list-style-type: none">• Granular device context: Deep context about every device, resource, and user in and around the network• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment• Security automation: Automated alert handling and responses to security incidents</div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 331 293 1472">HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE</p> <p data-bbox="354 149 699 1472">Netskope Device Intelligence uncovers managed and unmanaged devices on the network spectrum and fingerprints those devices based on their unique characteristics across multiple dimensions. These dimensions include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. The device information is collected from multiple network interfaces, protocol information, traffic flow, and application heuristics. This is combined with organizational information from existing CMDB, tools like MDM, EDR, vulnerability assessment, firewall, times of operation and location amongst others to develop rich and dynamic device context. This context is then fed to machine learning algorithms to generate unique models and signatures for each device, which includes the following information, called HyperContext®:</p> <ul data-bbox="727 149 1203 1472" style="list-style-type: none"> • Association of all the physical interfaces of the device and the spectrum of operation of each interface • Type, Category of the device and related information • OS, patches, services, and applications running on the device • Functionality or the “purpose in life” of the device • Micro location of the device, its mobility patterns, and times of visibility • Ownership information of the device and its control information • Users on the device • Behavior based analysis of all the data transmissions across all protocols and spectrums • Risk and vulnerability information, other information collected by other tools used

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>The critical role of micro-segmentation</p> <p>Over the years companies have relied on traditional network segmentation tools, such as NAC, VLANs, authentication, and access control lists (ACL) for creating subnets within the networks. The coarse-grained segmentation offered by these tools based on static device information, such as IP Address, subnets, and ACLs, leads to flat trusted zones that fail to account for dynamic device behavior or risk posture, rendering them ineffective against rogue devices. For example, if the audio video conferencing devices are statically segmented into a specific subnet, it is easy to plug in a laptop in the same subnet and sniff and snoop on the SIP communications. It is also easy to make a mistake and connect a conferencing device into other subnets, thereby creating more exposure than necessary.</p> <p>Micro-segmentation, on the other hand, is a more granular dynamic method of creating secure or trusted zones of connected devices. Micro-segmentation utilizes zero trust principles to isolate devices from one another using deep contextual information and secure them individually. Micro-segmentation is implemented in the software, using a layer that is decoupled from the underlying network hardware and NAC tools. This makes the segmentation easier to deploy and manage, providing security beyond static rules and authentication mechanisms to limit the blast radius in case of a security event.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 462 1032 1476"><p>The diagram shows a central circle containing icons of a laptop, a smartphone, and a tablet. Six lines radiate from this central circle to six surrounding circles, each containing an icon and a label. The labels are: 'Spectrum' (with a radio tower icon), 'Data, Behavior' (with a network node icon), 'Ownership, Control' (with a gear and key icon), 'Micro-location, BYOD' (with a location pin icon), 'Function, Services' (with a gear and document icon), and 'Type, Category' (with a document icon). The labels 'Spectrum', 'Data, Behavior', and 'Ownership, Control' are positioned to the left of their respective circles, while 'Micro-location, BYOD', 'Function, Services', and 'Type, Category' are positioned to the right.</p></div> <p data-bbox="1036 300 1105 1476">https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

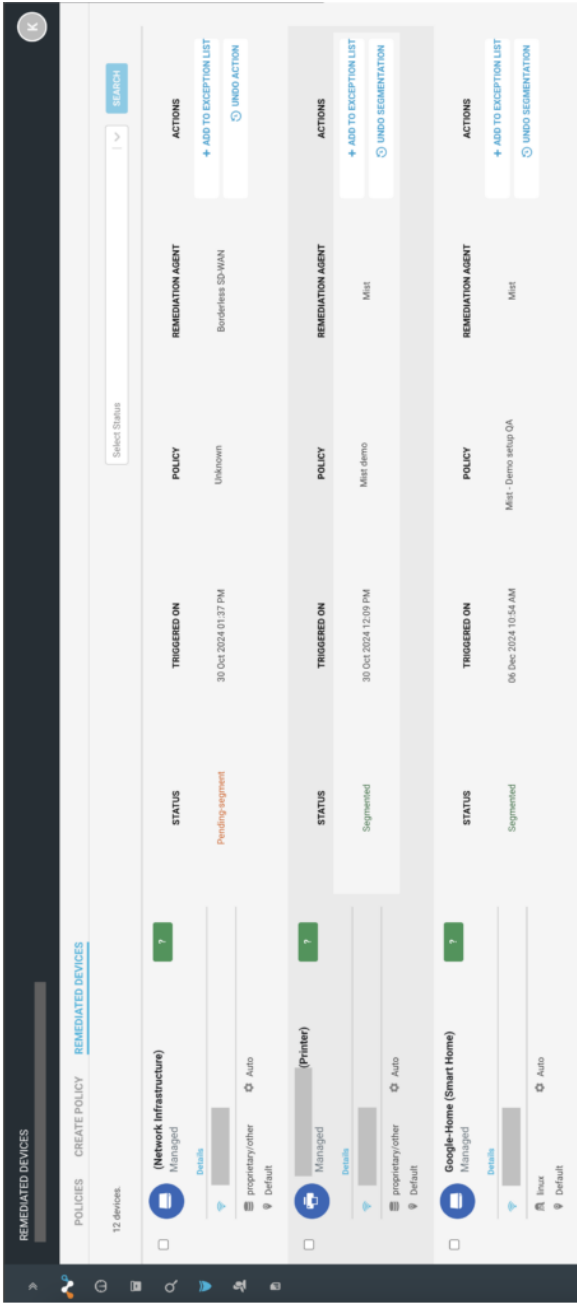
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="284 783 328 1425"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="365 285 651 1425"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="695 285 1349 1461"><p>The diagram illustrates the architecture of Device Intelligence, showing the flow of data and processing from a Customer Site to the Cloud.</p><p>Customer Site:</p><ul style="list-style-type: none">Airspace Data: Represented by a box with binary code (10010110011011, 01011001101100).Network Data: Represented by a box with binary code (10010110011011, 01011001101100).Radio Sensors or Access Points: Represented by a box with a signal icon.Network Sensor: Represented by a box with a server icon.Nextgen Access Control: A box containing the text "CUSTOMER SITE" and the "netskope" logo.<p>Processing and Analysis:</p><ul style="list-style-type: none">Billions of daily measurements of device characteristics: A central circular process involving "AI" and "ML" icons, with arrows indicating data flow from the Customer Site.Deep Learning + Powerful Policy Engine: A central circular process receiving input from the "Models / Controls" box and sending output to the "Alerts/Insights" box.Alerts/Insights: A box containing the text "Billions of daily device behavior analyzed".<p>Cloud Integration:</p><ul style="list-style-type: none">Asset Mgmt Integration: A box on the left.Vulnerability Scanner Integration: A box on the left.MDM, EDR Integration: A box on the right.Security Integration: A box on the right.Cloud: A box containing "UI", "SIEM", and "Ticketing".<p><small>© 2022 Netskope Confidential. All rights reserved.</small></p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 1056 297 1465">Analytics and Protection </p> <ul data-bbox="331 149 597 1430" style="list-style-type: none"><li data-bbox="331 149 407 1430">• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies.<li data-bbox="428 149 505 1430">• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<li data-bbox="526 149 597 1430">• Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <p data-bbox="613 632 646 1476">https://docs.netkope.com/en/architecture-of-netkope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="266 1094 305 1455">Remediated Devices</p> <p data-bbox="342 226 451 1455">Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p> <p data-bbox="483 226 511 1455">You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p> <ul data-bbox="540 310 1146 1419" style="list-style-type: none"> • Device Name: The name or identifier of the device. • Device Type: The type of device (e.g., computer, printer, IoT device). • Device Details: By clicking on a details link, you will be navigated to a new page about the device details. • Status: The current status of the remediation action (e.g., Pending Segment, Segmented). • Triggered On: The date and time when the security policy was triggered. • Policy: The name of the security policy that was triggered. • Remediation Agent: The agent responsible for enforcing the remediation action. • Actions: A set of actions that can be performed on the device, such as: <ul data-bbox="1003 436 1146 1356" style="list-style-type: none"> • Add to Exception List: Excludes the device from future remediation actions. • Undo Action: Reverses the previous remediation action taken on the device. • Undo Segmentation: Reverses the previous segmentation action taken on the device.

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement

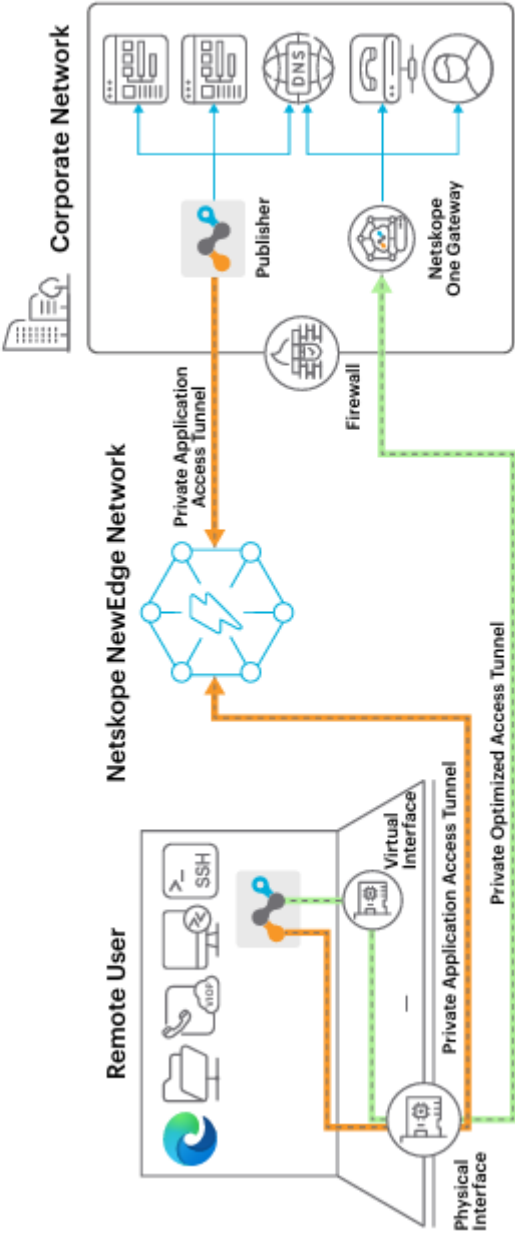


<https://docs.netkope.com/en/remediated-devices>



U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Introducing Netskope One Private Access</p> <p>Delivered as a single solution, Netskope One Private Access integrates Zero Trust Network Access (ZTNA) and software-defined wide-area networking (SD-WAN) capabilities, enabling the complete retirement — not just partial replacement — of remote access VPNs for all relevant application access use cases, while enhancing security posture and boosting remote worker productivity with secure and seamless connectivity.</p> <p>The unified Netskope One Client sits in front of a converged architecture comprising Netskope One Private Application Access for access to client-initiated applications, and Netskope One Private Optimized Access to securely connect applications that require bi-directional, server-initiated traffic. The same Netskope One Client enables every other client inline Netskope service: NG-SWG, CASB Inline, FWaaS, DNS Security, Endpoint DLP.</p> <p>The solution utilizes zero trust principles to enhance overall security posture and reduce lateral threat movement, reduce deployment complexity, and optimize performance, and it enables ubiquitous access to corporate resources hosted anywhere through intelligent traffic steering. With Netskope One Private Access, organizations can avoid maintaining separate ZTNA and VPN clients, and instead provide consistent security for all applications with a unified client deployment.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Key Benefits</p> <p>Enforces Zero Trust Principles</p> <p>Netskope One Private Access incorporates zero trust principles and proposes a shift from traditional network-centric access control to granular application-centric access control on a per-user or user group basis. The solution accelerates the time frame for decommissioning legacy applications and minimises associated security risks, including unauthorized lateral movement. Key benefits include:</p> <ul style="list-style-type: none"> • Identity- and context-aware, least-privileged access to private applications hosted in public clouds or on-premises data centers. • Device Classification options to assess the posture of the client before providing access to private applications hosted in public clouds or on-premises data centers. • Facilitating the connectivity through the ZTNA broker in Netskope One platform. The applications are hidden from discovery, and access is restricted only to authenticated and authorised users. • Reducing the opportunities for lateral movement of threats within the private networks and limiting the blast radius. • Eliminating the dependence on public-facing VPNs or open inbound firewall ports for application access, securing networks from threats and DDoS attacks. <p>Secures All Enterprise Applications</p> <p>Netskope One Private Access also supports server-to-client traffic connectivity, enabling access to both legacy and modern applications through a single client. Key benefits include:</p> <ul style="list-style-type: none"> • Eliminating the need to maintain two separate solutions — VPN and ZTNA — for accessing all private applications and achieving greater cost savings by reducing capital and operational expenditure. • Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all private applications.

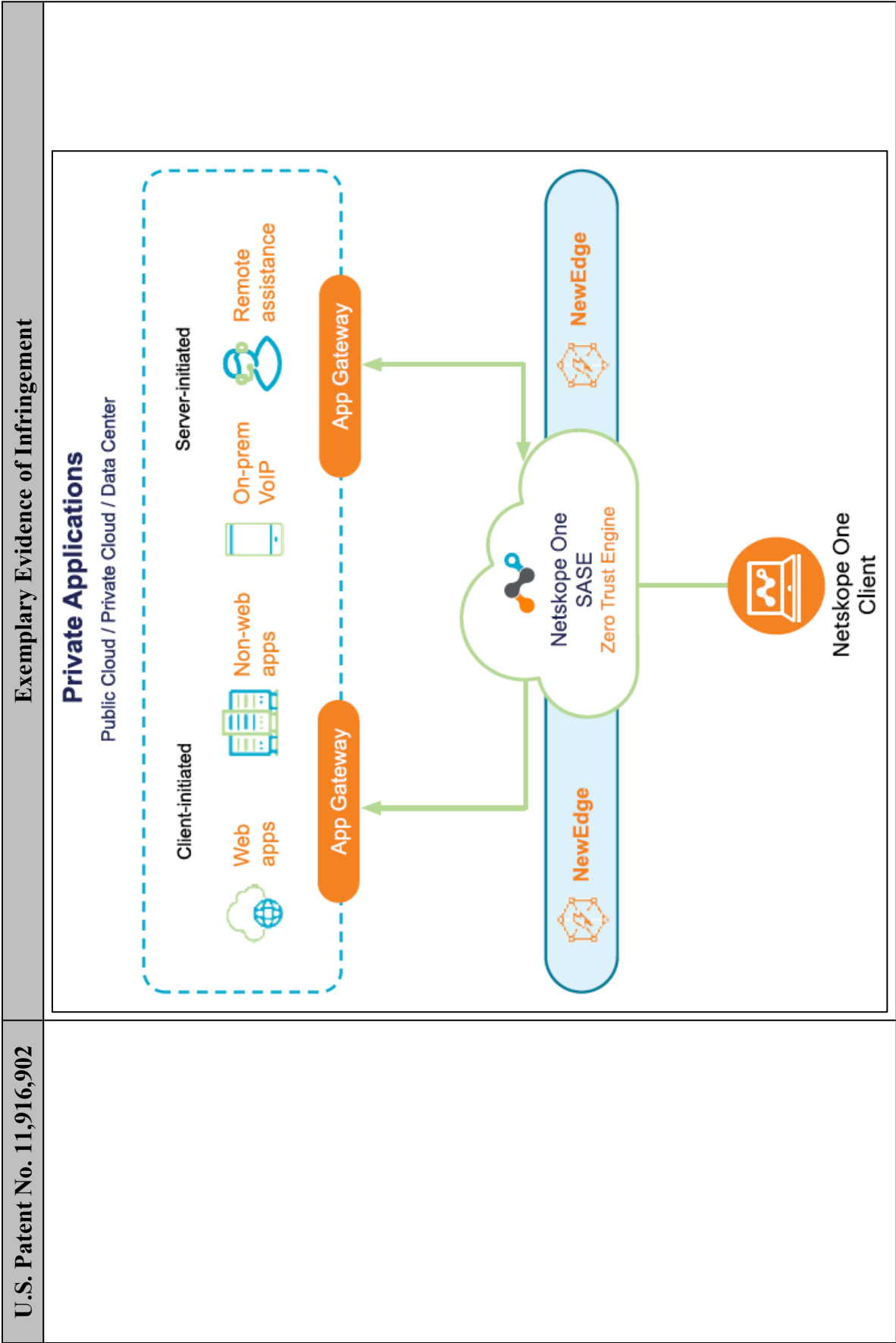
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="264 989 289 1461">Delivers a Phenomenal User Experience</p> <p data-bbox="313 226 378 1461">Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key benefits include:</p> <ul data-bbox="402 268 532 1413" style="list-style-type: none"> • Automatic traffic steering by the Netskope Client for connecting authorised users directly to specific resources regardless of where it is hosted. Strategically positioned Netskope NewEdge Network point of presence (PoP) helps achieve lowest possible latency and round-trip time for application access. <p data-bbox="557 506 581 1461">Full Zero Trust Application Access: Netskope One Private Unified Access</p> <p data-bbox="605 243 703 1461">Combining Private Application Access and Private Optimized Access capabilities on the same Endpoint, Netskope enables organisations to apply granular zero trust access to all Internal Applications, and support all use cases for a VPN replacement.</p> 

<p>U.S. Patent No. 11,916,902</p>	<div data-bbox="203 560 238 1071"> <p>Exemplary Evidence of Infringement</p> </div> <div data-bbox="261 262 464 1442"> <p>Netskope One Private Unified Access vastly improves the user experience by supporting multiple Private Application Access applications through a single connection to the NewEdge Network. Additionally, it supports multiple Private Data Centers or Private/Public Clouds. This enables customers to not only streamline access in private Data Centers or Private/Public Clouds. This enables customers to not only streamline access and improve performance for all types of private applications, but also ensure granular zero trust-based access.</p> </div> <div data-bbox="496 283 987 1442"> <p>The diagram illustrates the Netskope One Private Unified Access architecture. A Remote Endpoint (laptop icon) is connected to the Netskope NewEdge Network (a central cloud icon with a lightning bolt). The NewEdge Network is connected to two Publishers. The first Publisher is located in the Public/Private Cloud (cloud icon) and is connected to a Netskope One Gateway. The second Publisher is located in the Corporate Network (building icon) and is also connected to a Netskope One Gateway. The Publishers are connected to the NewEdge Network via Private Application Access Tunnels. The NewEdge Network is connected to the Publishers via Private Optimized Access Tunnels.</p> </div> <div data-bbox="1015 535 1050 1478"> <p>2024-12-Reference-Architecture-Guide-for-ZTNA-Next-RA-709-3-1-1.pdf</p> </div> <div data-bbox="1089 147 1414 1478"> <p>The Accused '902 Products include each and every element of this limitation, either literally or under the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that the Netskope Client remote device does not include a processing device that connects the processing device to another remote network, the same function is achieved by the Netskope Private Access products, SWG, and/or related products (as referenced above) working in cooperation with the</p> </div>
--	---

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	Netskope One Client to distribute this functionality across devices to achieve the same result of mitigating the security issue of the unsecure network element.
<p>8. The method of claim 1, the method further comprising: using, by the processing device, a network connection between the processing device and the known network; and while using the network connection between the processing device and the known network, scanning, by the processing device, the remote network through which access to the known network is established, wherein the scanning is configured to identify an unsecure network element on the remote network.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Private Access products and Netskope One Platform scan and process device's access to Netskope's NewEdge Network, identifying threats from unsecured network resources, or on a network with unsecured devices.</p> <div data-bbox="787 338 1297 1472"> <h2>What is ZTNA?</h2> <p>Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p> </div>	<p>The Accused '902 Products include using, by the processing device, a network connection between the processing device and the known network; and while using the network connection between the processing device and the known network, scanning, by the processing device, the remote network through which access to the known network is established, wherein the scanning is configured to identify an unsecure network element on the remote network.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Private Access products and Netskope One Platform scan and process device's access to Netskope's NewEdge Network, identifying threats from unsecured network resources, or on a network with unsecured devices.</p>

U.S. Patent No. 11,916,902	<div><div>Exemplary Evidence of Infringement</div><div><div><div><div><div><div>Zero Trust Security Principles</div><div><p>ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p><p>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p><p>Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p><p>https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p></div></div></div><div><div>Netskope One Private Access</div><div><p>Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p></div></div></div></div></div></div>
----------------------------	---

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="277 594 516 1446">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="581 594 995 1446" style="list-style-type: none"> <li data-bbox="581 594 816 1446">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="857 594 995 1446">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications



U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Seamless and optimized user experience</p> <p>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul style="list-style-type: none"> • Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access. • Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope’s Device Intelligence (formerly known as Netskope IoT Security) includes deep context of every device and the collection and acquisition of data concerning all devices in, and “around,” the remote network (<i>e.g.</i>, the remote network to which the remote device running the Netskope Client is connected) with this monitoring being performed continuously, including while a known access device is connected to the Netskope One Platform via the remote network.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<h1>Netskope One Private Access</h1> <h2>features and benefits</h2> <ul style="list-style-type: none"> Full VPN, NAC replacement > AI-driven automated policy optimization > Flexible access methods > Built-in threat and data protection > Built-in device intelligence v Unified visibility >  <p>Netskope UZTNA extends zero trust beyond users to every connected device. With Device Intelligence, organizations gain visibility, real-time risk scoring, and context-aware access for IoT and OT systems, securing branches, campuses, and factories while reducing attack surface at scale.</p> <p>> Learn about Device Intelligence</p>	<p>https://www.netskope.com/products/private-access</p>

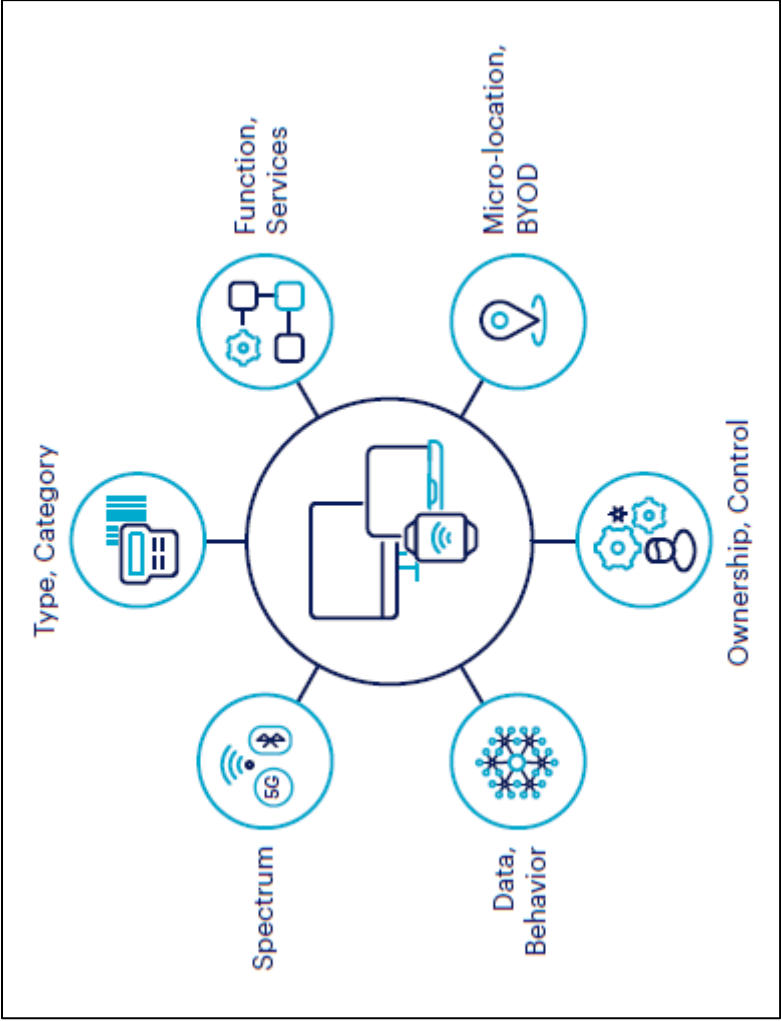
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul style="list-style-type: none"> • Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior. • Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR. • Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations. • Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p>https://docs.netkope.com/en/what-is-netkope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 936 289 1465">REALIZING ZERO TRUST FOR DEVICES</p> <p data-bbox="354 174 578 1465">Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p> <ul data-bbox="605 197 906 1415" style="list-style-type: none"> <li data-bbox="605 254 667 1415">• Granular device context: Deep context about every device, resource, and user in and around the network <li data-bbox="695 197 756 1415">• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location <li data-bbox="784 247 846 1415">• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment <li data-bbox="873 407 906 1415">• Security automation: Automated alert handling and responses to security incidents

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 327 293 1467">HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE</p> <p data-bbox="354 149 699 1467">Netskope Device Intelligence uncovers managed and unmanaged devices on the network spectrum and fingerprints those devices based on their unique characteristics across multiple dimensions. These dimensions include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. The device information is collected from multiple network interfaces, protocol information, traffic flow, and application heuristics. This is combined with organizational information from existing CMDB, tools like MDM, EDR, vulnerability assessment, firewall, times of operation and location amongst others to develop rich and dynamic device context. This context is then fed to machine learning algorithms to generate unique models and signatures for each device, which includes the following information, called HyperContext®:</p> <ul data-bbox="727 149 1203 1467" style="list-style-type: none"> • Association of all the physical interfaces of the device and the spectrum of operation of each interface • Type, Category of the device and related information • OS, patches, services, and applications running on the device • Functionality or the “purpose in life” of the device • Micro location of the device, its mobility patterns, and times of visibility • Ownership information of the device and its control information • Users on the device • Behavior based analysis of all the data transmissions across all protocols and spectrums • Risk and vulnerability information, other information collected by other tools used

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>The critical role of micro-segmentation</p> <p>Over the years companies have relied on traditional network segmentation tools, such as NAC, VLANs, authentication, and access control lists (ACL) for creating subnets within the networks. The coarse-grained segmentation offered by these tools based on static device information, such as IP Address, subnets, and ACLs, leads to flat trusted zones that fail to account for dynamic device behavior or risk posture, rendering them ineffective against rogue devices. For example, if the audio video conferencing devices are statically segmented into a specific subnet, it is easy to plug in a laptop in the same subnet and sniff and snoop on the SIP communications. It is also easy to make a mistake and connect a conferencing device into other subnets, thereby creating more exposure than necessary.</p> <p>Micro-segmentation, on the other hand, is a more granular dynamic method of creating secure or trusted zones of connected devices. Micro-segmentation utilizes zero trust principles to isolate devices from one another using deep contextual information and secure them individually. Micro-segmentation is implemented in the software, using a layer that is decoupled from the underlying network hardware and NAC tools. This makes the segmentation easier to deploy and manage, providing security beyond static rules and authentication mechanisms to limit the blast radius in case of a security event.</p> <p>Employing AI/ML for intelligent, dynamic controls</p> <p>Zero trust architecture should not be static, especially when the number of devices accessing the network is growing exponentially. A dynamic approach would entail a learning engine to classify devices and provide the right contextual information, and a policy engine to enforce nuanced security and access controls. The architecture should continuously monitor and adapt to the current state of the device, network, its threat exposure and should not be defined as a set of static rules.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 462 1032 1476"><p>The diagram shows a central circle containing icons of a laptop, a smartphone, and a tablet. Six lines radiate from this central circle to six surrounding circles, each containing an icon and a label. The labels are: 'Spectrum' (with a 5G and Bluetooth icon), 'Data, Behavior' (with a network node icon), 'Ownership, Control' (with a gear and key icon), 'Micro-location, BYOD' (with a location pin icon), 'Function, Services' (with a gear and document icon), and 'Type, Category' (with a server rack icon).</p></div> <p data-bbox="1036 300 1105 1476">https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Investigate Device Intelligence > Investigate Devices</div><div><div>Investigate Devices</div><div><div>Navigate to Investigate > Devices menu to see an entire dashboard stating the device summary in your environment based on different aspects like spectrum, type, ownership, etc.</div><div><div><div>Note</div><div>You can also sort the device summary in combination with the total of all devices, managed, unmanaged, new, automated, and user-controlled devices.</div></div></div><div><div>Investigate Devices based on Spectrum</div><div>Navigate to Investigate > Devices menu and select the Spectrum tab from the navigation bar to see the devices based on the network spectrum in the environment.</div><div><div><div>247 Total Devices</div><div>56 Managed Devices</div><div>191 Unmanaged Devices</div><div>52 New Devices</div><div>113 Automated Devices</div><div>127 User Devices</div></div><div><div>Spectrum</div><div>Types</div><div>Ownership</div><div>Control</div><div>Protocols</div><div>Internal Topology</div><div>External Topology</div></div><div><div>Device By Network Spectrum</div><div><div>133</div><div>247</div><div>79</div><div>46</div><div>35</div><div>28</div></div><div><div>Spectrum</div><div>active</div><div>idle</div><div>idle</div></div></div></div></div></div></div></div>

<https://docs.netkope.com/en/investigate-devices>

Events view shows the information in device summary and event drill down table.

1. You can see the host name, type, tags assigned and managed or unmanaged information.
2. Click on the *details* link to see the device summary.
3. You can see the risk score calculated by the Netskope proprietary risk engine, which categorizes packet alerts, device software vulnerabilities and device behavior anomalies into threat vectors.
4. It shows if the device is Wi-Fi, wired or undefined interface connected.
5. You can see the operating system and site assigned information. It shows if the device is user or automatically controlled.
6. Displays a list of risk factors with severity and number of occurrences. You can create policy by selecting one or multiple risk issues or modify the severity of the risks.

Netskope Ex. 1014
inet IPR2027-00011
Page 00172

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Protect Device Intelligence > Remediated Devices</div><h2>Remediated Devices</h2><p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p><p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p><ul style="list-style-type: none">• Device Name: The name or identifier of the device.• Device Type: The type of device (e.g., computer, printer, IoT device).• Device Details: By clicking on a details link, you will be navigated to a new page about the device details.• Status: The current status of the remediation action (e.g., Pending Segment, Segmented).• Triggered On: The date and time when the security policy was triggered.• Policy: The name of the security policy that was triggered.• Remediation Agent: The agent responsible for enforcing the remediation action.• Actions: A set of actions that can be performed on the device, such as:<ul style="list-style-type: none">• Add to Exception List: Excludes the device from future remediation actions.• Undo Action: Reverses the previous remediation action taken on the device.• Undo Segmentation: Reverses the previous segmentation action taken on the device.<p>https://docs.netskope.com/en/remediated-devices</p></div>

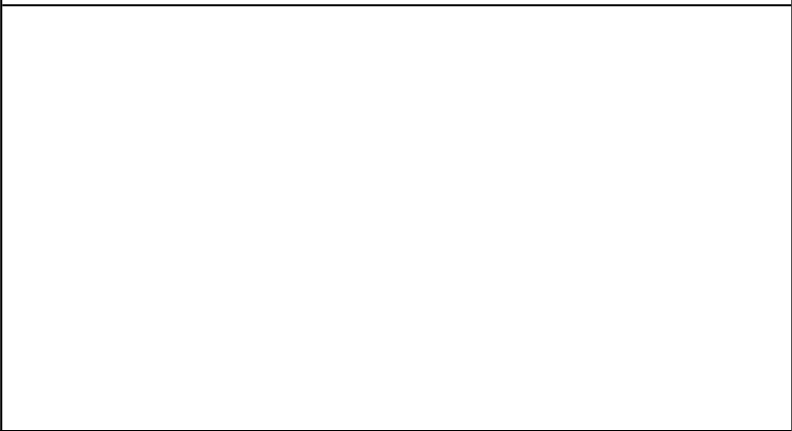
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 783 326 1425"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="365 285 651 1425"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="695 285 1357 1467"><p>The diagram illustrates the architecture of Device Intelligence, showing the flow of data and processing from a Customer Site to the Cloud.</p><p>Customer Site:</p><ul style="list-style-type: none">Radio Sensors or Access Points: Collect data from devices.Network Sensor: Collects network data.Nextgen Access Control: Manages access.Customer Site Data: Includes Airspace Data (10010310011011, 01011001101100) and Network Data (10010310011011, 01011001101100).<p>Processing:</p><ul style="list-style-type: none">Billions of daily measurements of device characteristics: Data is processed through a central hub.Deep Learning + Powerful Policy Engine: Analyzes the data to generate Alerts/Insights.<p>Cloud:</p><ul style="list-style-type: none">Asset Mgmt Integration: Manages device assets.Vulnerability Scanner Integration: Identifies security vulnerabilities.MDM, EDR Integration: Manages devices and monitors endpoint security.Security Integration: Integrates with other security systems.Alerts/Insights: Generated from the Deep Learning engine.UI, SIEM, Ticketing: Cloud-based interfaces for monitoring and management.<p>NetScope: CUSTOMER SITE</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="293 199 902 1476"><p data-bbox="326 1178 358 1436">Data Acquisition</p><ul data-bbox="399 247 870 1394" style="list-style-type: none"><li data-bbox="399 359 423 1394">• Customer environments have network sensors installed as physical or virtual appliances.<li data-bbox="451 258 570 1394">• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data.<li data-bbox="597 247 675 1394">• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<li data-bbox="703 258 776 1394">• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<li data-bbox="803 268 870 1394">• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 1220 321 1436">Data Transfer</div> <ul data-bbox="363 260 542 1394" style="list-style-type: none"> • The network sensors do a deep inspection of the traffic, apply signatures and run algorithms to extract meta information. • Network sensors send this meta information via encrypted channel to the cloud to analyze the traffic metadata and events in the environment. <div data-bbox="581 1220 613 1436">Data Analysis</div> <ul data-bbox="656 233 883 1394" style="list-style-type: none"> • On the cloud, various microservices analyze the metadata. • The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools. <div data-bbox="927 1089 959 1467">Analytics and Protection</div> <ul data-bbox="1002 201 1273 1436" style="list-style-type: none"> • Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies. • In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies. • Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <div data-bbox="1295 632 1328 1478"> https://docs.netskope.com/en/architecture-of-etskope-iot-security </div> <p data-bbox="1370 184 1403 1478">The Accused '902 Products include each and every element of this limitation, either literally or under</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that the Netskope Client remote device does not include a processing device that scans the remote network through which access to the known network is established, the same function is achieved by the Netskope Private Access products, SWG, and/or related products (as referenced above) working in cooperation with the Netskope One Client to distribute this functionality across devices to achieve the same result of scanning the remote network through which access to the Netskope Edge Network is established.</p>
<p>11[pre]: A system comprising: one or more processing resources; a non-transitory computer-readable medium coupled to the one or more processing resources, wherein the non-transitory computer-readable medium has stored thereon instructions that when executed by the one or more processing resources cause the one or more processing resources to:</p>	<p>To the extent the preamble is found to be limiting, the Accused '902 Products include a system comprising one or more processing resources and a non-transitory computer-readable medium coupled to the one or more processing resources, wherein the non-transitory computer-readable medium has stored thereon instructions that are executed by the one or more processing resources cause the one or more processing resources to.</p> <p>For example, the Netskope Private Access products, SWG, and/or Netskope One Platform has one or more processing resources with memory and instructions configured to authenticate access to a customer device that requests access to a private resource in the Netskope NewEdge network via a remote network (e.g., public network).</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div></div><div><h2>Netskope Advances Netskope One Platform With AI-Driven Proactive DEM Solution, Key Security Innovations</h2><p><i>Network Visibility and Control, Advanced Evasive Threat Detection, Context-Aware Zero Trust Integrations Accelerate Cloud Networking and Security Operations</i></p><p>SANTA CLARA, Calif. – September 10, 2024 – Netskope, a leader in Secure Access Service Edge (SASE), today announced several new innovations in the Netskope One platform, including expanded digital experience management (DEM) features and benefits. Combining key network and security capabilities, Netskope One continues to revolutionize the effectiveness of enterprise network infrastructure and operations (I&O) and security teams, enabling the entire organization to optimize the user experience while protecting critical data and reducing risk, cost, and complexity.</p><p>Coming on the heels of Netskope being recognized as a Leader in the 2024 Gartner Magic Quadrant™ for Single-Vendor SASE and as a Leader in the 2024 Gartner Magic Quadrant for Security Service Edge, the newly announced Netskope One platform advancements include the following.</p><p>https://www.netskope.com/press-releases/netkope-advances-netkope-one-platform-with-ai-driven-proactive-dem-solution-key-security-innovations</p></div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
 The image shows the Netskope NewEdge logo, which consists of the words "Netskope" and "NewEdge" in a white, sans-serif font on a dark blue background. Below the logo, there is a paragraph of white text on the same dark blue background. At the bottom of the image is a URL in white text.	<p>Netskope NewEdge is the world's largest, highest-performing security private cloud and powers the inline security services of the Netskope Security Cloud. NewEdge provides customers with unparalleled service coverage, performance and resilience. Today NewEdge is powered by data centers in 75+ regions with new data centers being added every month.</p> <p>https://www.netskope.com/resources/data-sheets/netkskope-newedge-data-sheet</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	 <p data-bbox="548 401 602 1465">Cloud security without sacrificing performance</p> <p data-bbox="639 449 867 1465">As enterprises embrace digital transformation—with their applications and data quickly moving to the cloud and an increasingly remote workforce accessing from everywhere—selecting a cloud-native security platform that delivers real-time security without performance trade-offs is critical.</p> <p data-bbox="894 726 938 1455">Future-proof, SASE-ready architecture</p> <p data-bbox="959 554 1273 1455">Powers Netskope SSE—including CFW, SWG, CASB, ZTNA and other services such as RBI, DLP, Threat Protection, CSPM/SSPM and more—without trade-offs even with all services enabled, plus full support for TLS 1.3 encryption, HTTP/2 and IPv6 clients.</p> <p data-bbox="1284 296 1321 1478">https://www.netskope.com/wp-content/uploads/2022/12/2023-04-NewEdge-DS-333-7-1.pdf</p>
11[a]: receive a request to	The Accused '902 Products receive a request to access a known network from a known access device

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;	<p>connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network.</p> <p>For example, the Netskope Private Access, SWG, and/or related products, features or functions (e.g. NSProxy) of the Netskope One Platform hosted in Netskope's NewEdge Network (a known private network that authorizes credentials associated with the known access device) receives requests from a known user's remote device (e.g., SD-WAN resource requests from the Netskope Client) to access one or more secure private network resources through a remote network such as a public network via the internet (a remote external network). <i>See also</i> 1[a].</p> <hr/>
	<h2>Netskope Advances Netskope One Platform With AI-Driven Proactive DEM Solution, Key Security Innovations</h2> <p>Network Visibility and Control, Advanced Evasive Threat Detection, Context-Aware Zero Trust Integrations Accelerate Cloud Networking and Security Operations</p> <p>SANTA CLARA, Calif. – September 10, 2024 – Netskope, a leader in Secure Access Service Edge (SASE), today announced several new innovations in the Netskope One platform, including expanded digital experience management (DEM) features and benefits. Combining key network and security capabilities, Netskope One continues to revolutionize the effectiveness of enterprise network infrastructure and operations (I&O) and security teams, enabling the entire organization to optimize the user experience while protecting critical data and reducing risk, cost, and complexity.</p> <p>Coming on the heels of Netskope being recognized as a Leader in the 2024 Gartner Magic Quadrant™ for Single-Vendor SASE and as a Leader in the 2024 Gartner Magic Quadrant for Security Service Edge, the newly announced Netskope One platform advancements include the following.</p> <p>https://www.netskope.com/press-releases/netkskope-advances-netkskope-one-platform-with-ai-driven-proactive-dem-solution-key-security-innovations</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	 <p>Netskope NewEdge is the world's largest, highest-performing security private cloud and powers the inline security services of the Netskope Security Cloud. NewEdge provides customers with unparalleled service coverage, performance and resilience. Today NewEdge is powered by data centers in 75+ regions with new data centers being added every month.</p> <p>https://www.netskope.com/resources/data-sheets/netkope-newedge-data-sheet</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 388 878 1474">  <h2 data-bbox="553 388 605 1474">Cloud security without sacrificing performance</h2> <p data-bbox="646 443 870 1474">As enterprises embrace digital transformation—with their applications and data quickly moving to the cloud and an increasingly remote workforce accessing from everywhere—selecting a cloud-native security platform that delivers real-time security without performance trade-offs is critical.</p> </div> <div data-bbox="878 157 1224 1474"> <p data-bbox="894 170 1219 1474">Netskope NewEdge is the world's largest, highest-performing security private cloud and powers the inline and API-driven security services of the Netskope Security Cloud. NewEdge provides customers with unparalleled service coverage, performance and resilience. Today NewEdge is powered by data centers in 70 regions with new data centers being added every month.</p> </div> <div data-bbox="1247 1430 1263 1474">...</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div>NewEdge deploys full compute at every service point for real-time, inline processing designed to scale to achieve more than two terabits per second at every data center—capable of serving hundreds of millions of users’ inline traffic—ensuring no performance trade-offs. Designed to provide a security service edge (SSE) and embracing a secure access service edge (SASE) architecture, this allows security to be deployed at the edge where and when it’s needed.</div> <div>Future-proof, SASE-ready architecture Powers Netskope SSE—including CFW, SWG, CASB, ZTNA and other services such as RBI, DLP, Threat Protection, CSPM/SSPM and more—without trade-offs even with all services enabled, plus full support for TLS 1.3 encryption, HTTP/2 and IPv6 clients. https://www.netskope.com/wp-content/uploads/2022/12/2023-04-NewEdge-DS-333-7-1.pdf</div> <div>Inside the Netskope NewEdge Data Center Factory</div> <div>Jul 13 2021 9 min. read</div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>We've worked very hard to make our infrastructure single, unified, and 100% homogenous, so no single data center looks any different from any other. As part of moving to a lean, performance-focused footprint, we have implemented the concept of <i>integrated racks</i> into our data center factory approach. We build, pre-stage, configure, test, and ship a data center as a pre-built rack, with every rack constructed in exactly the same way. This approach ensures total consistency in every data center when it comes to what services are available and the related configuration of the surrounding infrastructure and underlying components.</p> <p>...</p> <p>Whether it's with our data center factory approach, in-the-weeds decisions about components that make up our integrated racks (e.g. bare metal servers, NVMe SSDs, or high-bandwidth network switches), data center site locations, peering or transit relationships, we take full responsibility for the customer experience and it's our job to architect around issues. It's important to https://www.netskope.com/blog/inside-the-netskope-newedge-data-center-factory</p> <h2>Understanding Coverage Isn't Just About Counting Data Centers</h2> <p>Aug 04 2020 6 min. read</p> <p>With the NewEdge network, we're not taking any shortcuts to deliver the security services of the Netskope Security Cloud Platform. We don't use vPoPs today and every data center offers full, local compute for real-time, in-line traffic processing. This allows us to inspect and enforce security policies without having to send the traffic halfway around the globe. All Netskope security services – including Next-Generation Secure Web Gateway (NG-SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and Zero Trust Network Access (ZTNA) – take advantage of this architectural approach. NewEdge is unique when compared to the approaches used by https://www.netskope.com/blog/understanding-coverage-isnt-just-about-counting-data-centers</p>

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement

What is ZTNA?

Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.

Zero Trust Security Principles

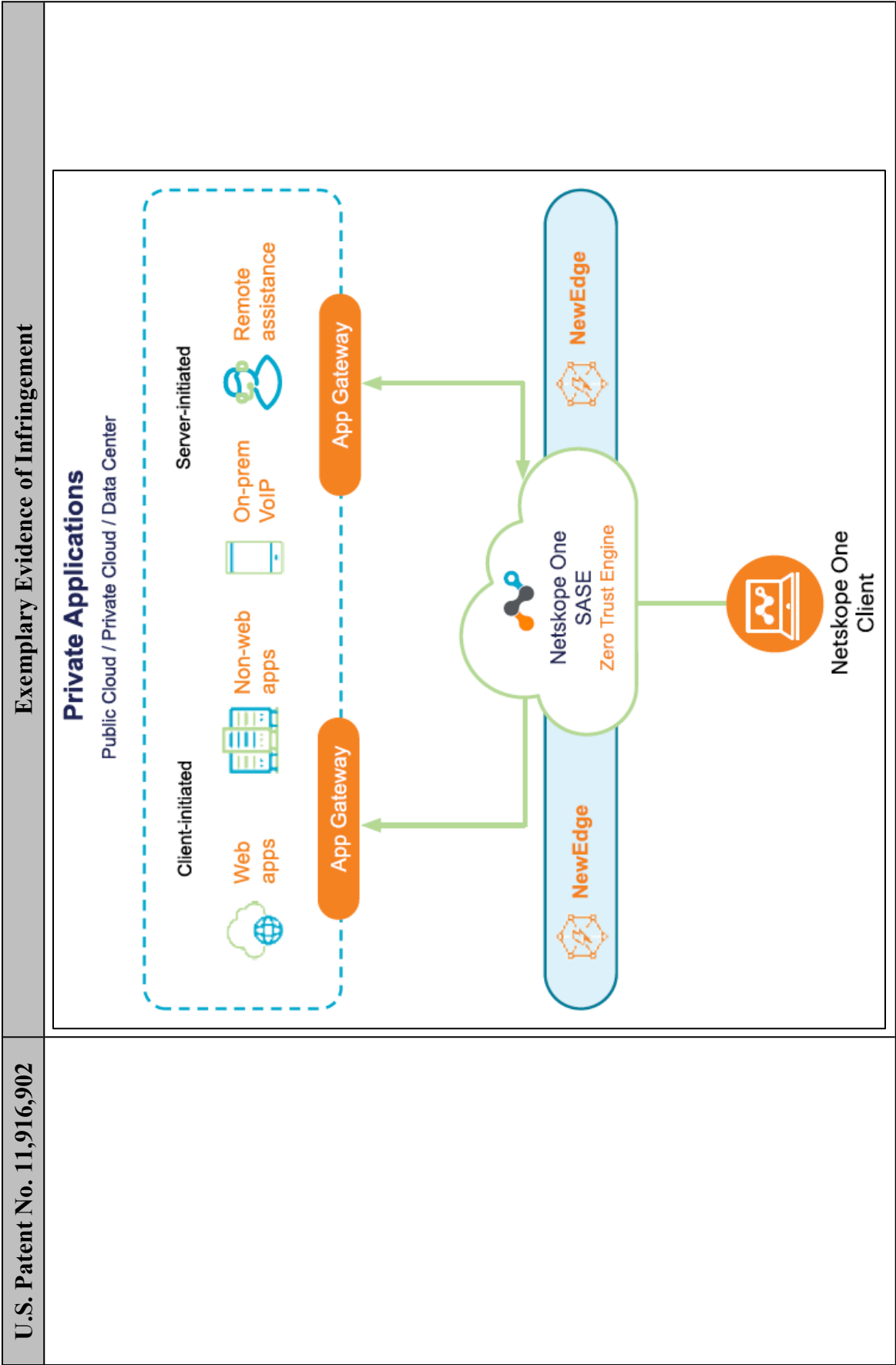
ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.

Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.

Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.

<https://www.netskope.com/security-defined/what-is-zero-trust-network-access>

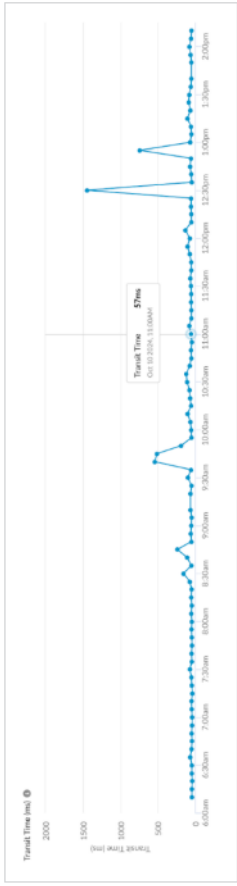
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 195 565 1476"> <h2 data-bbox="266 499 337 1476">Netskope One Private Access</h2> <p data-bbox="370 195 542 1476">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p> </div> <div data-bbox="565 594 1320 1476"> <p data-bbox="589 594 821 1449">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="886 625 1292 1449" style="list-style-type: none"> <li data-bbox="886 709 1118 1449">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="1159 625 1292 1449">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications </div>



U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="266 680 305 1463">Seamless and optimized user experience</p> <p data-bbox="336 680 505 1463">Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p data-bbox="570 680 691 1463">Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul data-bbox="756 680 1321 1463" style="list-style-type: none"> <li data-bbox="756 680 1065 1463">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access. <li data-bbox="1110 680 1321 1463">• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p data-bbox="1341 212 1406 1476">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

<p>U.S. Patent No. 11,916,902</p>	<p>Exemplary Evidence of Infringement</p>
	<p>How It Works</p> <p>Netskope Private Application Access operates through the seamless integration of the Private Access Broker and the Publisher to enforce Zero Trust principles and provide secure access. The Private Access Broker functions as a cloud-native control plane that validates user identity, device posture, and access policies in real time before granting access to applications.</p> <p>The Publisher, a lightweight connector deployed on-premises or in the cloud, establishes secure, encrypted communication between users and private applications without exposing applications to the internet. This architecture ensures that users gain access only to the specific applications they are authorized to use, with optimized routing and granular control, while eliminating the need for traditional VPNs. This combination provides a highly secure, scalable, and efficient access solution for endpoint-initiated workflows.</p> <p>NPA is illustrated in this diagram:</p>  <p>The diagram illustrates the Netskope for Private Access architecture. On the left, 'Remote Users' (represented by a person with a laptop) and 'Offices' (represented by a building) are shown. Both connect to the 'Netskope Platform'. The platform is divided into several functional blocks: 'Connects users to authorized apps – not your networks', 'Authenticates users and devices in the cloud – not at your perimeter', 'Classifies devices based on variety of security posture checks', 'Encrypts application traffic end-to-end', and 'Corporate Datacenter'. The platform also integrates with 'Public Cloud' services, specifically Microsoft Azure, Amazon Web Services, and Google Cloud Platform. A legend at the bottom right identifies the 'Netskope Client' (represented by a small orange square) and the 'Netskope Publisher' (represented by a small blue square).</p> <p>https://docs.netskope.com/en/netkskope-private-access</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Connection</p> <p>The "Connection" time from the sites/users to Netskope POPs section corresponds to the time spent by the NSClient/Enterprise Station to establish a TCP connection with the NSProxy.</p> <p>TLS</p> <p>The "TLS" time from the sites/users to Netskope POPs section corresponds to the time spent by the NSClient/Enterprise Station to perform the TLS handshake process with the NSProxy.</p> <p>Inside Netskope POPs</p> <p>The following metric is processed at the NSProxy level.</p> <p>POP Transit Time</p> <p>The POP Transit Time provides the total time spent within the NSProxy.</p> <p>It is the addition of the "request transit time" and the "response transit time". These are defined as follows:</p> <ul style="list-style-type: none"> • Request transit time Time elapsed between the first byte of request reaching the NSProxy and this first byte of the request leaving the NSProxy • Response transit time Time elapsed between the first byte of response reaching the NSProxy and this first byte of response leaving the NSProxy 

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="256 1087 289 1470">Netskope POPs to Applications</p> <p data-bbox="313 989 337 1470">The following metrics are processed at the NSProxy level.</p> <p data-bbox="362 1339 394 1470">Connection</p> <p data-bbox="418 159 475 1470">The "Connection" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to establish a TCP connection with the targeted server.</p> <p data-bbox="500 1392 532 1470">Server</p> <p data-bbox="557 184 605 1470">The "Server" time corresponds to the time between the first byte of NSProxy request to the targeted server and the first byte of response received by the NSProxy.</p> <p data-bbox="630 159 686 1470">This Server time is the main server performance indicator, as it mainly takes the server processing time into account. Note though that there is also one RTT (between the NSProxy and the server) included. So bad network conditions between the NSProxy and the server may also impact the Server time value.</p> <p data-bbox="703 831 735 1470">https://docs.netskope.com/en/performance-metrics</p> <p data-bbox="776 1339 808 1470">Transit Time</p> <div data-bbox="833 590 1068 1470">  </div> <p data-bbox="1109 159 1166 1470">The Transit Time corresponds to the total time spent within the Netskope infrastructure. It includes the time spent in the NSProxy to forward the request from the NSClient to the application server, added to the time spent in the NSProxy to forward the response from the application server back to the NSClient.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement																																																				
	<div><h3>TCP Connection Time, SSL Handshake Time</h3><p>The graph displays three metrics over time from 6:00am to 2:00pm. The Y-axis represents time in milliseconds (ms), ranging from 0 to 1000. The X-axis represents time in hours and minutes. The legend indicates: TCP Connection Time (blue line), SSL Handshake Time (yellow line), and Redirect Count (red line). The TCP Connection Time shows a sharp spike to approximately 1000ms at 12:30pm. The SSL Handshake Time remains relatively low, around 250ms. The Redirect Count is zero until 11:00am, then spikes to 5 at 11:30am and 12:00pm, and returns to zero at 12:30pm.</p><table><tr><th>Time</th><th>TCP Connection Time (ms)</th><th>SSL Handshake Time (ms)</th><th>Redirect Count</th></tr><tr><td>6:00am</td><td>~250</td><td>~250</td><td>0</td></tr><tr><td>7:00am</td><td>~250</td><td>~250</td><td>0</td></tr><tr><td>8:00am</td><td>~250</td><td>~250</td><td>0</td></tr><tr><td>9:00am</td><td>~250</td><td>~250</td><td>0</td></tr><tr><td>10:00am</td><td>~250</td><td>~250</td><td>0</td></tr><tr><td>11:00am</td><td>~250</td><td>~250</td><td>0</td></tr><tr><td>11:30am</td><td>~250</td><td>~250</td><td>5</td></tr><tr><td>12:00pm</td><td>~250</td><td>~250</td><td>5</td></tr><tr><td>12:30pm</td><td>~1000</td><td>~250</td><td>0</td></tr><tr><td>1:00pm</td><td>~250</td><td>~250</td><td>0</td></tr><tr><td>1:30pm</td><td>~250</td><td>~250</td><td>0</td></tr><tr><td>2:00pm</td><td>~250</td><td>~250</td><td>0</td></tr></table></div> <p>These metrics correspond to the time needed for the NSProxy to securely connect to the application server. This includes the TCP as well as SSL/TLS handshake processes. The Redirect count provides the number of redirections that have been observed during the select timeframe. The "Connection" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to establish a TCP connection with the targeted server. The "TLS" time from the Netskope POPs to Applications section corresponds to the time spent by the NSProxy to perform the TLS handshake process with the targeted server.</p> <p>https://docs.netskope.com/en/user-overview</p>	Time	TCP Connection Time (ms)	SSL Handshake Time (ms)	Redirect Count	6:00am	~250	~250	0	7:00am	~250	~250	0	8:00am	~250	~250	0	9:00am	~250	~250	0	10:00am	~250	~250	0	11:00am	~250	~250	0	11:30am	~250	~250	5	12:00pm	~250	~250	5	12:30pm	~1000	~250	0	1:00pm	~250	~250	0	1:30pm	~250	~250	0	2:00pm	~250	~250	0
Time	TCP Connection Time (ms)	SSL Handshake Time (ms)	Redirect Count																																																		
6:00am	~250	~250	0																																																		
7:00am	~250	~250	0																																																		
8:00am	~250	~250	0																																																		
9:00am	~250	~250	0																																																		
10:00am	~250	~250	0																																																		
11:00am	~250	~250	0																																																		
11:30am	~250	~250	5																																																		
12:00pm	~250	~250	5																																																		
12:30pm	~1000	~250	0																																																		
1:00pm	~250	~250	0																																																		
1:30pm	~250	~250	0																																																		
2:00pm	~250	~250	0																																																		

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><h3 data-bbox="272 1024 321 1465">The Power of One</h3><p data-bbox="365 646 467 1465">The major components of the Netskope One platform include:</p><p data-bbox="527 436 1117 1465">The Netskope Zero Trust Engine: Netskope's Zero Trust Engine lies at the heart of the platform, continuously gathering risk telemetry and generating extensive contextual awareness across all users, devices, applications, and data. Unlike other SSE offerings that bypass some types of traffic and services, the Zero Trust Engine decrypts and decodes traffic inline across web and SaaS applications, cloud services, and private applications for the broadest and deepest levels of visibility and protection.</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="259 367 779 1470"> <p>The Netskope NewEdge Network: Netskope's one-of-a-kind network is purpose-built to deliver full compute SSE and SD-WAN. Featuring a global footprint of ultra-fast data centers in 75+ regions, and a local experience for every country, NewEdge is highly elastic, built for scale, and designed to provide cloud-delivered security and networking services directly to where the users and offices are without performance trade-offs.</p> </div> <div data-bbox="787 367 1372 1470"> <p>The Netskope One Client: Netskope's endpoint agent unifies remote user access to web, cloud, and private apps, alongside data protection and voice and video optimization at the endpoint by converging SWG, CASB, ZTNA, FWaaS, DLP, and SD-WAN. Easy to use, lightweight, and deployed to perform at a high throughput, it delivers a single agent footprint for SASE and zero trust use cases, greatly simplifying desktop administration for a better user experience.</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="284 388 917 1459">The Netskope One Gateway: The Netskope One Gateway, offers both hardware and virtual form factors and supports the widest range of deployment options, including cellular gateways, micro to large branch, data center and multi-cloud environments. Netskope One Gateway consolidates disjointed appliances into one unified SASE gateway. It offers multiple services like Routing, WiFi, SD-WAN, App FW, IPS, IoT Device Intelligence, DEM and Edge compute, along with a seamless on-ramp to Netskope One SSE.</p> <p data-bbox="925 861 958 1470">2025-03-Netskope-One-Platform-SB-719-5.pdf</p>
<p data-bbox="1015 1480 1274 1900">11[b]: scan the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an insecure network element on the remote network;</p>	<p data-bbox="1015 147 1128 1480">The Accused '902 Products scan the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an insecure network element on the remote network.</p> <p data-bbox="1161 147 1307 1480">For example, Netskope's Private Access products and Netskope One Platform and/or Netskope One Client act in a unified manner and scan and process a device's access to private resources in the Netskope NewEdge Network, identifying threats from unsecured network resources on the remote network, or on a network with unsecured devices. <i>See also</i> 1[b].</p>

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement

What is ZTNA?

Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications--no matter where they are hosted.

Zero Trust Security Principles

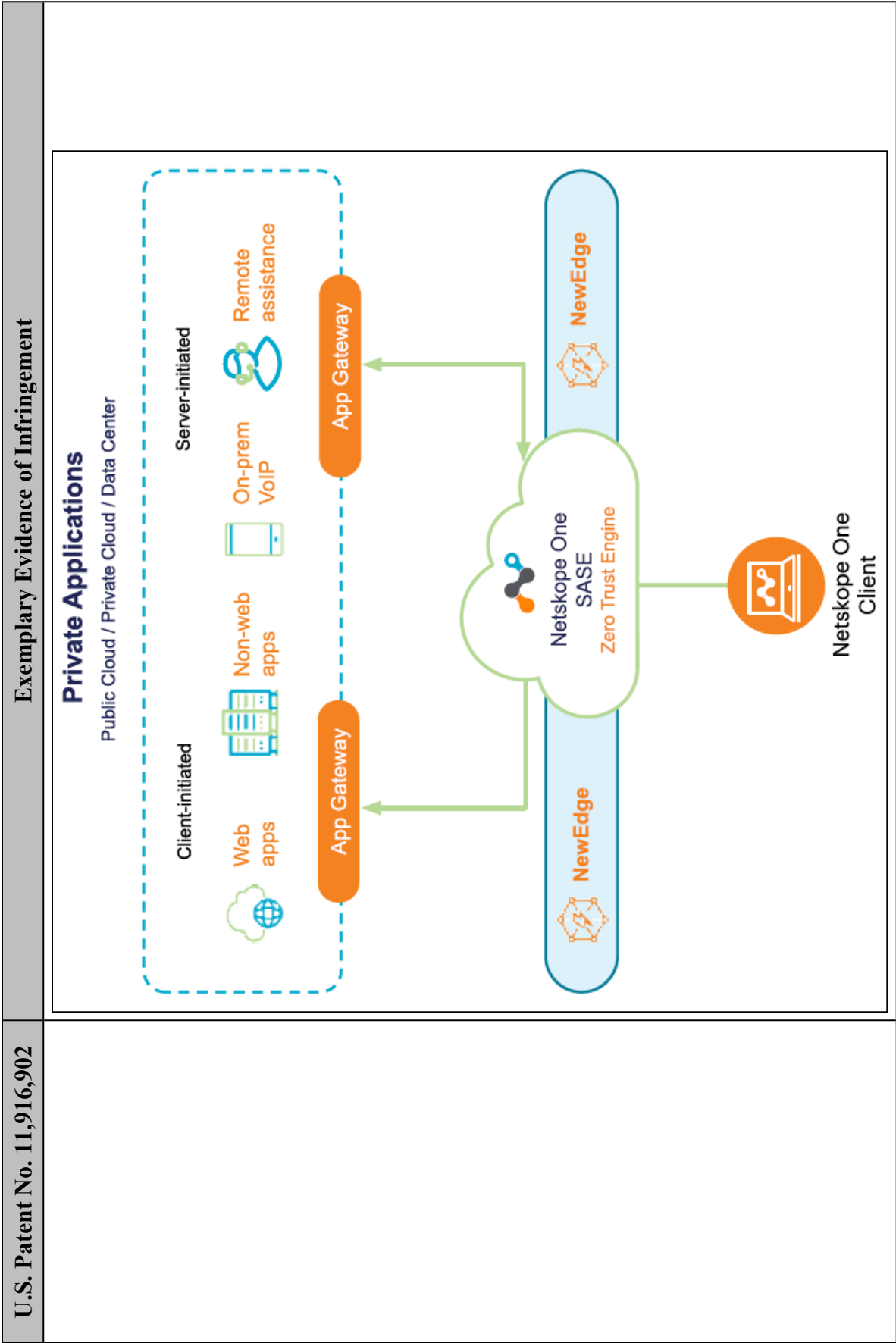
ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.

Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.

Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.

<https://www.netskope.com/security-defined/what-is-zero-trust-network-access>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="251 195 565 1476"> <h2 data-bbox="264 495 337 1470">Netskope One Private Access</h2> <p data-bbox="367 207 540 1470">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p> </div> <div data-bbox="565 575 1333 1476"> <p data-bbox="586 594 824 1446">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="889 606 1305 1446" style="list-style-type: none"> <li data-bbox="889 678 1127 1446">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="1167 606 1305 1446">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications </div>



U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="266 680 305 1465">Seamless and optimized user experience</p> <p data-bbox="337 680 505 1465">Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p data-bbox="570 680 695 1465">Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul data-bbox="760 659 1328 1465" style="list-style-type: none"> <li data-bbox="760 659 1068 1465">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access. <li data-bbox="1110 659 1328 1465">• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p data-bbox="1344 212 1409 1478">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

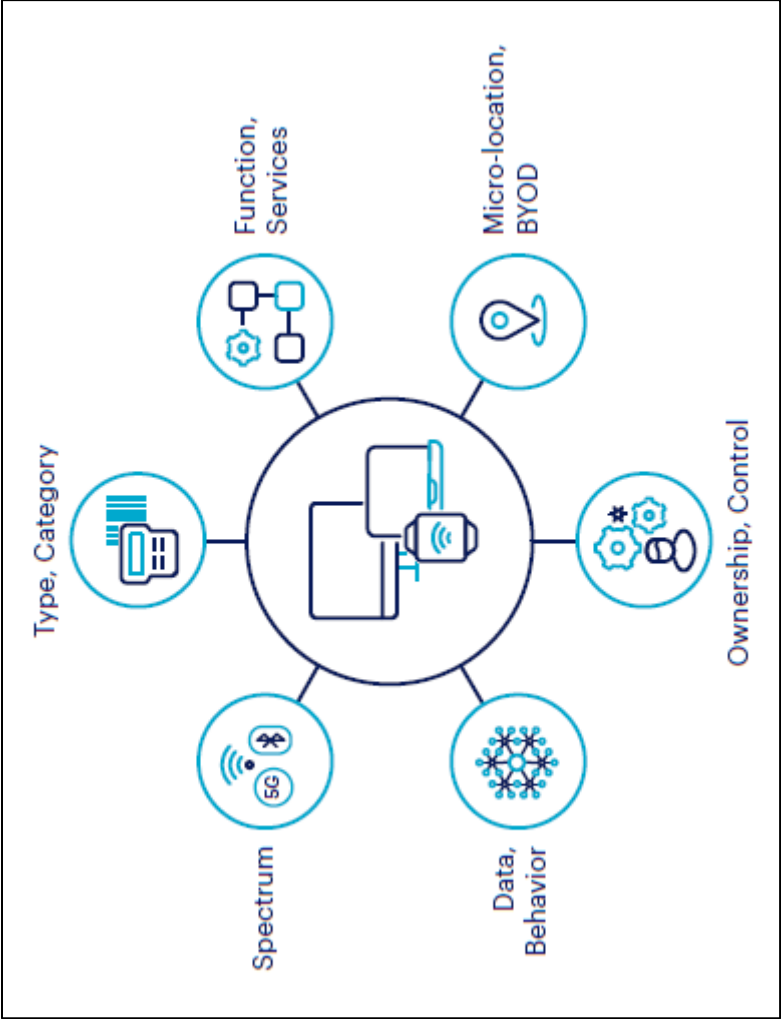
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>For example, Netskope’s Device Intelligence (formerly known as Netskope IoT Security) includes deep context of every device and the collection and acquisition of data concerning all devices in, and “around,” the remote network (e.g., assessing security of elements in the remote network to which the remote device running the Netskope Client is connected beyond merely the device seeking access).</p>  <p>The screenshot displays the Netskope One Private Access website. The header reads "Netskope One Private Access" followed by "features and benefits". A list of features is shown, each with a title, a description, and a right-pointing arrow: "Full VPN, NAC replacement", "AI-driven automated policy optimization", "Flexible access methods", "Built-in threat and data protection", "Built-in device intelligence", and "Unified visibility". To the right of the list is a green robot icon with signal waves. Below the list, a paragraph states: "Netskope UZTNA extends zero trust beyond users to every connected device. With Device Intelligence, organizations gain visibility, real-time risk scoring, and context-aware access for IoT and OT systems, securing branches, campuses, and factories while reducing attack surface at scale." At the bottom right is a circular button with a right arrow and the text "Learn about Device Intelligence". A URL is at the bottom: https://www.netskope.com/products/private-access</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul style="list-style-type: none"> • Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior. • Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR. • Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations. • Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 1478 917 1908"><div data-bbox="261 1478 310 1908">REALIZING ZERO TRUST FOR DEVICES</div><div data-bbox="354 1478 912 1908"><p>Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p><ul style="list-style-type: none">• Granular device context: Deep context about every device, resource, and user in and around the network• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment• Security automation: Automated alert handling and responses to security incidents</div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 327 293 1467">HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE</p> <p data-bbox="354 149 699 1467">Netskope Device Intelligence uncovers managed and unmanaged devices on the network spectrum and fingerprints those devices based on their unique characteristics across multiple dimensions. These dimensions include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. The device information is collected from multiple network interfaces, protocol information, traffic flow, and application heuristics. This is combined with organizational information from existing CMDB, tools like MDM, EDR, vulnerability assessment, firewall, times of operation and location amongst others to develop rich and dynamic device context. This context is then fed to machine learning algorithms to generate unique models and signatures for each device, which includes the following information, called HyperContext®:</p> <ul data-bbox="727 149 1203 1467" style="list-style-type: none"> • Association of all the physical interfaces of the device and the spectrum of operation of each interface • Type, Category of the device and related information • OS, patches, services, and applications running on the device • Functionality or the “purpose in life” of the device • Micro location of the device, its mobility patterns, and times of visibility • Ownership information of the device and its control information • Users on the device • Behavior based analysis of all the data transmissions across all protocols and spectrums • Risk and vulnerability information, other information collected by other tools used

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 462 1032 1474"><p>The diagram illustrates a central device, represented by a laptop and a smartphone, connected to six categories of data or services. The categories are arranged in a circle around the central device, each with a corresponding icon in a blue circle. The categories are: Type, Category (top-left, icon of a document with a bar chart), Spectrum (top, icon of a radio tower and signal waves), Data, Behavior (top-right, icon of a network of nodes), Ownership, Control (bottom-right, icon of a person with a gear), Micro-location, BYOD (bottom, icon of a location pin), and Function, Services (bottom-left, icon of a gear and a document). The text 'Type, Category' is written vertically to the left of the top-left icon, 'Spectrum' is written vertically to the left of the top icon, 'Data, Behavior' is written vertically to the left of the top-right icon, 'Ownership, Control' is written vertically to the right of the bottom-right icon, 'Micro-location, BYOD' is written vertically to the right of the bottom icon, and 'Function, Services' is written vertically to the right of the bottom-left icon.</p></div> <p data-bbox="1036 300 1105 1474">https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Investigate Device Intelligence > Investigate Devices</div><div><div>Investigate Devices</div><div><div>Navigate to Investigate > Devices menu to see an entire dashboard stating the device summary in your environment based on different aspects like spectrum, type, ownership, etc.</div><div><div><div>Note</div><div>You can also sort the device summary in combination with the total of all devices, managed, unmanaged, new, automated, and user-controlled devices.</div></div></div><div><div>Investigate Devices based on Spectrum</div><div>Navigate to Investigate > Devices menu and select the Spectrum tab from the navigation bar to see the devices based on the network spectrum in the environment.</div><div><div><div>247 Total Devices</div><div>56 Managed Devices</div><div>191 Unmanaged Devices</div><div>52 New Devices</div><div>113 Automated Devices</div><div>127 User Devices</div></div><div><div>Spectrum</div><div>Types</div><div>Ownership</div><div>Control</div><div>Protocols</div><div>Internal Topology</div><div>External Topology</div></div><div><div>Device By Network Spectrum</div><div><div>133</div><div>247</div><div>79</div><div>1</div></div><div><div>Spectrum</div><div>active</div><div>idle</div><div>idle</div></div></div></div></div></div></div></div>

<https://docs.netkope.com/en/investigate-devices>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Investigate Risks</div><div><p>Navigate to Investigate > Risks menu to see a list of devices with high, medium or low priority. The screen provides the event view and device view for the information representation. You can see the number of devices with risk at the top right chart.</p><p>Events view shows the information in device summary and event drill down table.</p></div><div></div><div><ol style="list-style-type: none">1. You can see the host name, type, tags assigned and managed or unmanaged information.2. Click on the <i>details</i> link to see the device summary.3. You can see the risk score calculated by the Netskope proprietary risk engine, which categorizes packet alerts, device software vulnerabilities and device behavior anomalies into threat vectors.4. It shows if the device is Wi-Fi, wired or undefined interface connected.5. You can see the operating system and site assigned information. It shows if the device is user or automatically controlled.6. Displays a list of risk factors with severity and number of occurrences. You can create policy by selecting one or multiple risk issues or modify the severity of the risks.<p>https://docs.netskope.com/en/investigate-risks</p></div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Protect Device Intelligence > Remediated Devices</div><h2>Remediated Devices</h2><p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p><p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p><ul style="list-style-type: none">• Device Name: The name or identifier of the device.• Device Type: The type of device (e.g., computer, printer, IoT device).• Device Details: By clicking on a details link, you will be navigated to a new page about the device details.• Status: The current status of the remediation action (e.g., Pending Segment, Segmented).• Triggered On: The date and time when the security policy was triggered.• Policy: The name of the security policy that was triggered.• Remediation Agent: The agent responsible for enforcing the remediation action.• Actions: A set of actions that can be performed on the device, such as:<ul style="list-style-type: none">• Add to Exception List: Excludes the device from future remediation actions.• Undo Action: Reverses the previous remediation action taken on the device.• Undo Segmentation: Reverses the previous segmentation action taken on the device.<p>https://docs.netskope.com/en/remediated-devices</p></div>

<p>U.S. Patent No. 11,916,902</p>	<div data-bbox="203 562 235 1066"> <p>Exemplary Evidence of Infringement</p> </div> <div data-bbox="284 783 326 1423"> <h3>Architecture of Device Intelligence</h3> </div> <div data-bbox="365 283 651 1423"> <p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p> </div> <div data-bbox="690 283 1356 1465"> <p>The diagram illustrates the IoT Security Platform architecture, an AI-based context generation platform for all devices. It is divided into three main sections: CUSTOMER SITE, Models / Controls, and CLOUD.</p> <ul style="list-style-type: none"> CUSTOMER SITE: This section includes 'Radio Sensors or Access Points' and 'Network Sensor'. It shows 'Airspace Data' (100100110011001100) and 'Network Data' (100100110011001100) being collected. A 'Nextgen Access Control' box is also present. Models / Controls: This central section receives data from the Customer Site and sends it to the Cloud. It features a circular diagram with icons for OS, AI, and a shield, labeled 'Billions of daily measurements of device characteristics'. CLOUD: This section contains a 'Deep Learning Powerful Policy Engine' which processes data from the Models / Controls. It also includes boxes for 'Asset Mgmt Integration', 'Vulnerability Scanner Integration', 'MDM, EDR Integration', and 'Security Integration'. The output is 'Alerts/Insights' which are then processed by 'SIEM' and 'Ticketing'. <p>The Netskope logo and 'CUSTOMER SITE' are visible at the bottom left of the diagram. A small copyright notice '© 2022 Netskope Confidential. All rights reserved.' is at the bottom right.</p> </div>
--	--

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="326 1178 358 1436">Data Acquisition</p> <ul data-bbox="396 247 870 1394" style="list-style-type: none"> <li data-bbox="396 354 428 1394">• Customer environments have network sensors installed as physical or virtual appliances. <li data-bbox="451 258 570 1394">• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data. <li data-bbox="592 247 672 1394">• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC. <li data-bbox="695 258 774 1394">• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices. <li data-bbox="797 268 870 1394">• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 1220 321 1436"> <p>Data Transfer</p> <ul style="list-style-type: none"> • The network sensors do a deep inspection of the traffic, apply signatures and run algorithms to extract meta information. • Network sensors send this meta information via encrypted channel to the cloud to analyze the traffic metadata and events in the environment. <p>Data Analysis</p> <ul style="list-style-type: none"> • On the cloud, various microservices analyze the metadata. • The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools. <p>Analytics and Protection</p> <ul style="list-style-type: none"> • Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies. • In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies. • Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <p>https://docs.netskope.com/en/architecture-of-netskope-iot-security</p> </div>
11[c]: based at least in part on	The Accused '902 Products include, based at least in part on identifying at least one unsecure network

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>identifying at least one insecure network element on the remote network, deny access to the known network; and</p>	<p>element on the remote network, denying, by the processing device, access to the known network.</p> <p>For example, Netskope's Private Access products and/or related products, features or functions of the Netskope One Platform deny access to private resources in the Netskope NewEdge Network, in association with identification of one or more insecure network elements. <i>See also</i> 1[c].</p> <div data-bbox="511 371 1008 1476"> <h2 data-bbox="527 703 625 1470">What is ZTNA?</h2> <p data-bbox="706 394 998 1470">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p> </div> <div data-bbox="1008 304 1421 1476"> <h3 data-bbox="1019 1024 1055 1470">Zero Trust Security Principles</h3> <p data-bbox="1071 321 1193 1470">ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p> <p data-bbox="1226 321 1282 1470">Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p> <p data-bbox="1315 359 1404 1470">Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="256 478 289 1476">https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p> <div data-bbox="329 682 1372 1476"> <p data-bbox="337 709 378 1465">Seamless and optimized user experience</p> <p data-bbox="402 716 573 1465">Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p data-bbox="630 716 751 1465">Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul data-bbox="816 695 1364 1465" style="list-style-type: none"> <li data-bbox="816 716 1117 1465">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access. <li data-bbox="1157 695 1364 1465">• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. </div> <p data-bbox="1377 212 1409 1476">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="256 1346 289 1478">645-6.pdf</p> <p data-bbox="331 149 472 1478">For example, Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection (e.g., policy actions like blocking devices) in response to the information collected about devices in and around the network of the remote user's device for use in making access determinations for the device.</p> <div data-bbox="513 195 1333 1478" style="border: 1px solid black; padding: 10px;"> <p data-bbox="532 226 748 1451">Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p data-bbox="784 226 906 1451">Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul data-bbox="943 226 1284 1409" style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. </div> <p data-bbox="1338 722 1370 1478">https://docs.netskope.com/en/what-is-nsn-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul style="list-style-type: none"> • Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior. • Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR. • Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations. • Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 936 289 1465">REALIZING ZERO TRUST FOR DEVICES</p> <p data-bbox="354 174 578 1465">Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p> <ul data-bbox="605 197 906 1415" style="list-style-type: none"> <li data-bbox="605 254 667 1415">• Granular device context: Deep context about every device, resource, and user in and around the network <li data-bbox="695 197 756 1415">• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location <li data-bbox="784 247 846 1415">• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment <li data-bbox="873 407 906 1415">• Security automation: Automated alert handling and responses to security incidents

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Need for granular device context</p> <p>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to ensure security, and enforce right access control across the network. Current device fingerprinting technologies boil down to type, category, OS, version, etc. which are woefully inadequate for correctly profiling the device behavior and setting adequate controls to protect the device and the infrastructure it operates in. To keep networks secure you need to have a deeper understanding of devices entering/exiting your network, their dynamic behavior, and the risk associated with them to take precise actions. This calls for developing rich and dynamic device context across multiple dimensions, combining them with machine learning algorithms to generate models and signatures for each device. This rich contextual device intelligence allows for granular visibility and control.</p> <p>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 783 326 1423"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="365 283 651 1423"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="695 283 1357 1465"><p>The diagram illustrates the IoT Security Platform architecture, an AI-based context generation platform for all devices. It is divided into three main sections: CUSTOMER SITE, Models / Controls, and CLOUD.</p><ul style="list-style-type: none">CUSTOMER SITE: This section includes 'Radio Sensors or Access Points' and a 'Network Sensor'. It shows 'Airspace Data' (100100110011001100) and 'Network Data' (100100110011001100) being collected. A 'Nextgen Access Control' box is also present.Models / Controls: This central section receives data from the Customer Site and sends instructions back. It features a circular diagram with icons for OS, AI, and a shield, labeled 'Billions of daily measurements of device characteristics'.CLOUD: This section contains a 'Deep Learning Powerful Policy Engine' which processes data from the Models / Controls. It also includes boxes for 'Asset Mgmt Integration', 'MDM, EDR Integration', 'Vulnerability Scanner Integration', and 'Security Integration'. The output is 'Alerts/Insights' which are sent back to the Models / Controls. A 'Ticketing' box is also shown.<p>The diagram is titled 'IoT Security Platform AI-based context generation platform for all devices' and includes a copyright notice: '© 2022 Netskope Confidential. All rights reserved.'</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="326 1178 358 1436">Data Acquisition</p> <ul data-bbox="396 247 870 1394" style="list-style-type: none"> <li data-bbox="396 359 428 1394">• Customer environments have network sensors installed as physical or virtual appliances. <li data-bbox="451 258 570 1394">• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data. <li data-bbox="592 247 672 1394">• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC. <li data-bbox="695 258 774 1394">• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices. <li data-bbox="797 268 870 1394">• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="280 1249 313 1451">Data Analysis</p> <ul data-bbox="349 346 553 1409" style="list-style-type: none"> • On the cloud, various microservices analyze the metadata. • The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools. <p data-bbox="589 1094 621 1451">Analytics and Protection</p> <ul data-bbox="657 331 998 1409" style="list-style-type: none"> • Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies. • In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies. • Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <p data-bbox="1034 632 1066 1478">https://docs.netskope.com/en/architecture-of-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 420 1344 1474"> <p>Home > Device Intelligence > Protect Device Intelligence > Remediated Devices</p> <h2>Remediated Devices</h2> <p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p> <p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p> <ul style="list-style-type: none"> • Device Name: The name or identifier of the device. • Device Type: The type of device (e.g., computer, printer, IoT device). • Device Details: By clicking on a details link, you will be navigated to a new page about the device details. • Status: The current status of the remediation action (e.g., Pending Segment, Segmented). • Triggered On: The date and time when the security policy was triggered. • Policy: The name of the security policy that was triggered. • Remediation Agent: The agent responsible for enforcing the remediation action. • Actions: A set of actions that can be performed on the device, such as: <ul style="list-style-type: none"> • Add to Exception List: Excludes the device from future remediation actions. • Undo Action: Reverses the previous remediation action taken on the device. • Undo Segmentation: Reverses the previous segmentation action taken on the device. <p>https://docs.netskope.com/en/remediated-devices</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>11[d]: based at least in part upon on failure to identify any unsecure network element on the remote network, request a grant of access from the known network to the processing device.</p>	<p>The Accused '902 Products include, based at least in part upon on failure to identify any unsecure network element on the remote network, requesting a grant of access from the known network to the processing device.</p> <p>For example, Netskope's Private Access products and/or related products, features or functions of the Netskope One Platform grant access to private resources in the Netskope NewEdge Network to devices that are not found to be unauthorized or in a network with an unsecured network element. <i>See also</i> 1[d].</p>
	<div data-bbox="586 373 1094 1415"> <h2 data-bbox="602 705 699 1465">What is ZTNA?</h2> <p data-bbox="781 394 1073 1465">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications--no matter where they are hosted.</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 304 652 1470"><p data-bbox="256 1018 297 1470">Zero Trust Security Principles</p><p data-bbox="313 321 438 1470">ZTNA creates a new security framework, based on the <u>zero trust security model</u>, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p><p data-bbox="467 321 524 1470">Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p><p data-bbox="553 359 643 1470">Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p><p data-bbox="659 478 691 1470">https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="264 709 305 1465">Seamless and optimized user experience</p> <p data-bbox="332 709 500 1465">Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p data-bbox="560 709 678 1465">Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul data-bbox="738 709 1295 1465" style="list-style-type: none"> <li data-bbox="738 709 1042 1465">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access. <li data-bbox="1079 709 1295 1465">• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p data-bbox="1307 210 1377 1476">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>For example, Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection (e.g., policy actions like allowing, rather than blocking, devices) in response to the information collected about devices in and around the network of the remote user's device for use in making access determinations for the device.</p> <div data-bbox="440 195 1256 1476"> <p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-nsn-iot-security</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul style="list-style-type: none"> • Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior. • Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR. • Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations. • Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p>https://docs.netkope.com/en/what-is-netkope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>REALIZING ZERO TRUST FOR DEVICES</div><div>Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</div><div><ul style="list-style-type: none">• Granular device context: Deep context about every device, resource, and user in and around the network• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment• Security automation: Automated alert handling and responses to security incidents</div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Need for granular device context</p> <p>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to ensure security, and enforce right access control across the network. Current device fingerprinting technologies boil down to type, category, OS, version, etc. which are woefully inadequate for correctly profiling the device behavior and setting adequate controls to protect the device and the infrastructure it operates in. To keep networks secure you need to have a deeper understanding of devices entering/exiting your network, their dynamic behavior, and the risk associated with them to take precise actions. This calls for developing rich and dynamic device context across multiple dimensions, combining them with machine learning algorithms to generate models and signatures for each device. This rich contextual device intelligence allows for granular visibility and control.</p> <p>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 783 326 1423"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="365 283 651 1423"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="695 283 1357 1465"><p>The diagram illustrates the architecture of Device Intelligence, showing the flow of data and processing from a Customer Site to the Cloud.</p><p>Customer Site:</p><ul style="list-style-type: none">Airspace Data: Represented by a box with binary code (10010110011011, 01011001101100).Network Data: Represented by a box with binary code (10010110011011, 01011001101100).Radio Sensors or Access Points: Represented by a box with a signal icon.Network Sensor: Represented by a box with a server icon.Nextgen Access Control: A box containing the text "CUSTOMER SITE" and the "netskope" logo.<p>Processing and Analysis:</p><ul style="list-style-type: none">Billions of daily measurements of device characteristics: A central circular process involving "AI" and "ML" (Machine Learning) icons, with a shield icon indicating security.Deep Learning + Powerful Policy Engine: A central circular process involving a brain icon and a gear icon.Alerts/Insights: A box containing the text "Billions of daily device behavior analyzed".<p>Cloud:</p><ul style="list-style-type: none">Asset Mgmt Integration: A box containing the text "MDM, EDR Integration".Vulnerability Scanner Integration: A box containing the text "Security integration".UI: A box containing the text "SIEM".Cloud: A box containing the text "Ticketing".<p><small>© 2022 Netskope Confidential. All rights reserved.</small></p></div>

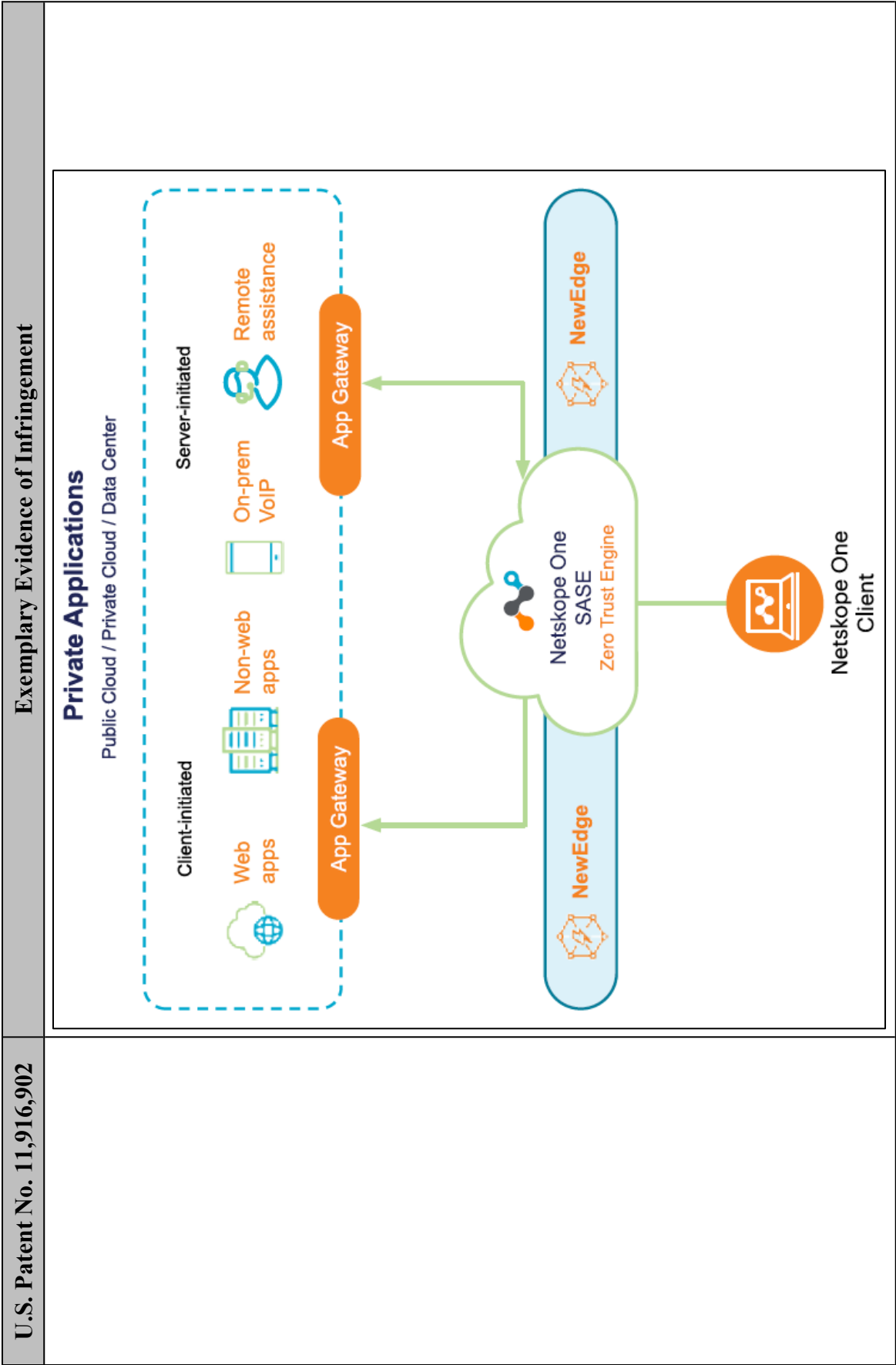
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="326 1178 358 1436">Data Acquisition</p> <ul data-bbox="399 247 870 1394" style="list-style-type: none"> <li data-bbox="399 359 423 1394">• Customer environments have network sensors installed as physical or virtual appliances. <li data-bbox="451 258 570 1394">• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data. <li data-bbox="597 247 672 1394">• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC. <li data-bbox="699 254 774 1394">• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices. <li data-bbox="802 268 870 1394">• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="280 1249 313 1451">Data Analysis</p> <ul data-bbox="345 344 553 1409" style="list-style-type: none"> • On the cloud, various microservices analyze the metadata. • The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools. <p data-bbox="589 1094 621 1451">Analytics and Protection</p> <ul data-bbox="654 331 998 1409" style="list-style-type: none"> • Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies. • In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies. • Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <p data-bbox="1031 632 1063 1478">https://docs.netkope.com/en/architecture-of-netkope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Protect Device Intelligence > Remediated Devices</div><h2>Remediated Devices</h2><p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p><p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p><ul style="list-style-type: none">• Device Name: The name or identifier of the device.• Device Type: The type of device (e.g., computer, printer, IoT device).• Device Details: By clicking on a details link, you will be navigated to a new page about the device details.• Status: The current status of the remediation action (e.g., Pending Segment, Segmented).• Triggered On: The date and time when the security policy was triggered.• Policy: The name of the security policy that was triggered.• Remediation Agent: The agent responsible for enforcing the remediation action.• Actions: A set of actions that can be performed on the device, such as:<ul style="list-style-type: none">• Add to Exception List: Excludes the device from future remediation actions.• Undo Action: Reverses the previous remediation action taken on the device.• Undo Segmentation: Reverses the previous segmentation action taken on the device.https://docs.netskope.com/en/remediated-devices</div>

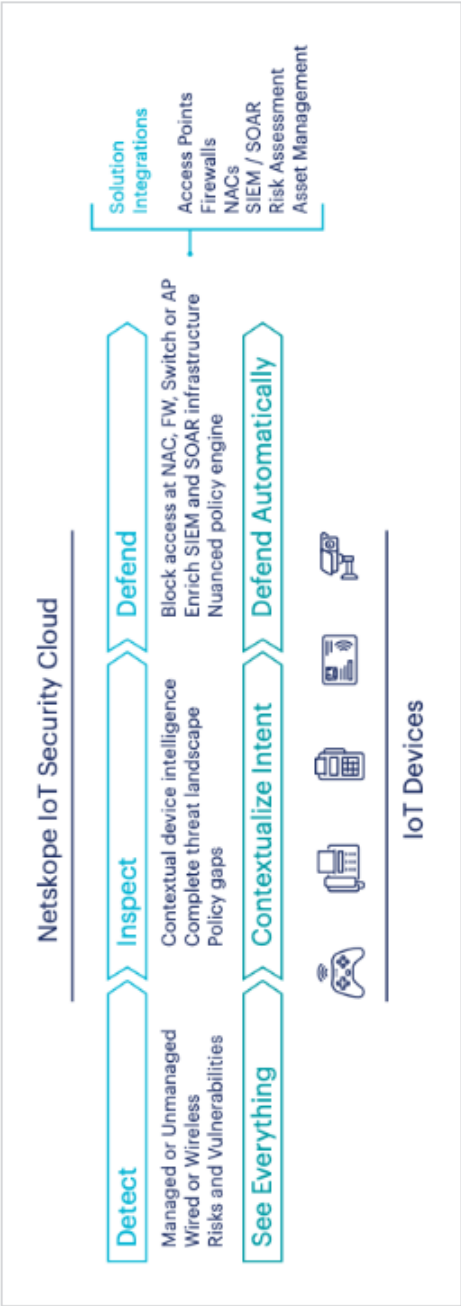
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>11[e]. wherein mitigating a security issue of the insecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection of Internet of Things (IoT) devices in and around the network of the remote user's device for use in making access determinations for the device, and mitigating a security issue by providing private access tunnels, micro-segmentation, isolation, and/or quarantining of devices. <i>See also</i> 1[e].</p>	<p>The Accused '902 Products include wherein mitigating a security issue of the insecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.</p> <p>For example, a remote user device having one or more processing devices executing the Netskope One Client (a known access device) together with Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection of Internet of Things (IoT) devices in and around the network of the remote user's device for use in making access determinations for the device, and mitigating a security issue by providing private access tunnels, micro-segmentation, isolation, and/or quarantining of devices. <i>See also</i> 1[e].</p> <div data-bbox="727 195 1049 1476"><h2 data-bbox="743 499 815 1476">Netskope One Private Access</h2><p data-bbox="846 195 1019 1476">Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="277 611 513 1446">Netskope One Private Access supports server-to-client or bidirectional connectivity with a single client capable of accepting inbound connections. This versatility enables secure access to both legacy and modern private applications. Key capabilities include:</p> <ul data-bbox="578 611 984 1446" style="list-style-type: none"> <li data-bbox="578 695 805 1446">• Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure <li data-bbox="854 611 984 1446">• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications



U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="266 680 305 1463">Seamless and optimized user experience</p> <p data-bbox="336 680 505 1463">Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p> <p data-bbox="570 680 691 1463">Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p> <ul data-bbox="756 667 1321 1463" style="list-style-type: none"> <li data-bbox="756 667 1065 1463">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access. <li data-bbox="1110 667 1321 1463">• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity. <p data-bbox="1341 210 1406 1476">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

<p>U.S. Patent No. 11,916,902</p>	<p>Exemplary Evidence of Infringement</p>
	<p>How It Works</p> <p>Netskope Private Application Access operates through the seamless integration of the Private Access Broker and the Publisher to enforce Zero Trust principles and provide secure access. The Private Access Broker functions as a cloud-native control plane that validates user identity, device posture, and access policies in real time before granting access to applications.</p> <p>The Publisher, a lightweight connector deployed on-premises or in the cloud, establishes secure, encrypted communication between users and private applications without exposing applications to the internet. This architecture ensures that users gain access only to the specific applications they are authorized to use, with optimized routing and granular control, while eliminating the need for traditional VPNs. This combination provides a highly secure, scalable, and efficient access solution for endpoint-initiated workflows.</p> <p>NPA is illustrated in this diagram:</p>  <p>The diagram illustrates the Netskope for Private Access architecture. On the left, 'Remote Users' (represented by a person with a laptop) and 'Offices' (represented by a building) are shown. They connect to the 'Netskope Platform'. The platform is divided into several functional blocks: 'Connects users to authorized apps – not your networks', 'Authenticates users and devices in the cloud – not at your perimeter', 'Classifies devices based on variety of security posture checks', 'Encrypts application traffic end-to-end', and 'Corporate Datacenter'. The platform also integrates with 'Public Cloud' services, specifically Microsoft Azure, Amazon Web Services, and Google Cloud Platform. A legend at the bottom right identifies the 'Netskope Client' (represented by a small orange square) and the 'Netskope Publisher' (represented by a small blue square).</p> <p>https://docs.netskope.com/en/netkskope-private-access</p>

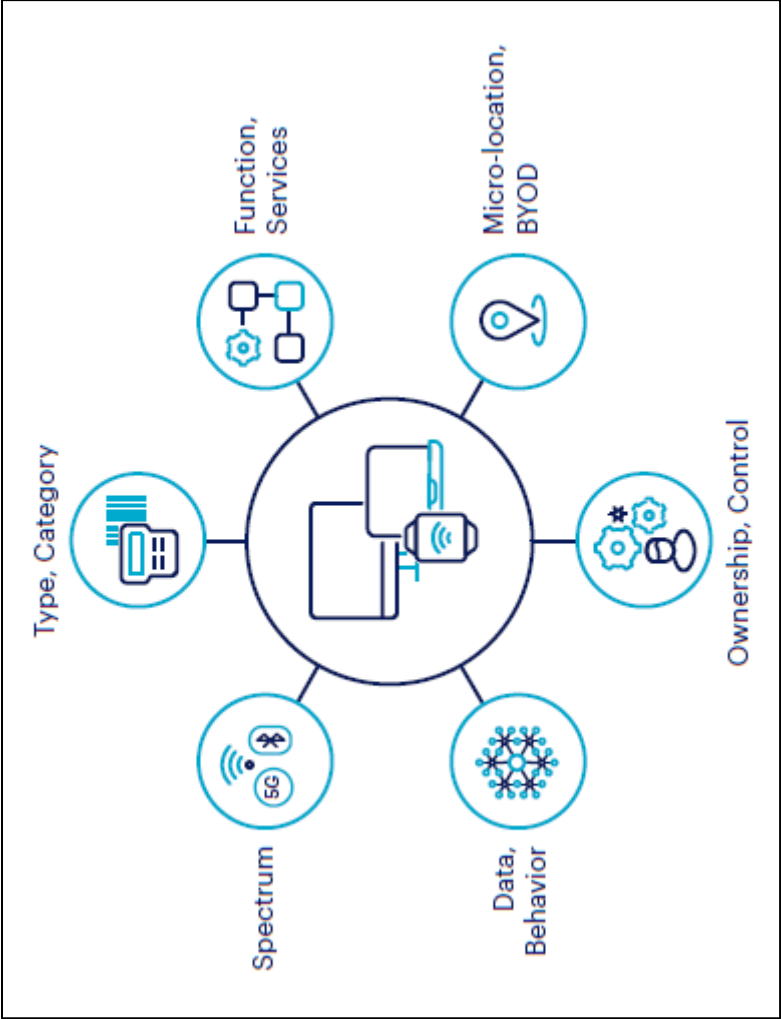
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	 <p>The diagram illustrates the Netskope IoT Security Cloud architecture. At the bottom, a horizontal line separates the 'IoT Devices' from the cloud components. Above this line, four icons represent different IoT devices: a game controller, a printer, a server rack, and a car. The main processing flow is shown as a series of four chevron-shaped boxes connected by arrows, moving from left to right. The first box is labeled 'Detect' and contains the text 'Managed or Unmanaged Wired or Wireless Risks and Vulnerabilities'. The second box is labeled 'Inspect' and contains 'Contextual device intelligence', 'Complete threat landscape', and 'Policy gaps'. The third box is labeled 'Contextualize Intent' and contains 'Block access at NAC, FW, Switch or AP', 'Enrich SIEM and SOAR infrastructure', and 'Nuanced policy engine'. The fourth box is labeled 'Defend Automatically'. To the right of the 'Defend Automatically' box, a vertical line separates it from a list of 'Solution Integrations'. These integrations include 'Access Points', 'Firewalls', 'NACs', 'SIEM / SOAR', 'Risk Assessment', and 'Asset Management'.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netkope.com/en/what-is-netkope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>REALIZING ZERO TRUST FOR DEVICES</div><div><p>Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:</p><ul style="list-style-type: none">• Granular device context: Deep context about every device, resource, and user in and around the network• Micro-segmentation: Ability to dynamically group devices into software defined perimeters based on the above context and geo location• Dynamic control: Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment• Security automation: Automated alert handling and responses to security incidents</div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 422 289 1472">HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE</p> <hr data-bbox="305 262 308 1472"/> <p data-bbox="347 262 662 1472">Netskope Device Intelligence uncovers managed and unmanaged devices on the network spectrum and fingerprints those devices based on their unique characteristics across multiple dimensions. These dimensions include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. The device information is collected from multiple network interfaces, protocol information, traffic flow, and application heuristics. This is combined with organizational information from existing CMDB, tools like MDM, EDR, vulnerability assessment, firewall, times of operation and location amongst others to develop rich and dynamic device context. This context is then fed to machine learning algorithms to generate unique models and signatures for each device, which includes the following information, called HyperContext®:</p> <ul data-bbox="690 438 1122 1425" style="list-style-type: none"> • Association of all the physical interfaces of the device and the spectrum of operation of each interface • Type, Category of the device and related information • OS, patches, services, and applications running on the device • Functionality or the "purpose in life" of the device • Micro location of the device, its mobility patterns, and times of visibility • Ownership information of the device and its control information • Users on the device • Behavior based analysis of all the data transmissions across all protocols and spectrums • Risk and vulnerability information, other information collected by other tools used

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="272 940 302 1465">The critical role of micro-segmentation</p> <p data-bbox="321 226 618 1465">Over the years companies have relied on traditional network segmentation tools, such as NAC, VLANs, authentication, and access control lists (ACL) for creating subnets within the networks. The coarse-grained segmentation offered by these tools based on static device information, such as IP Address, subnets, and ACLs, leads to flat trusted zones that fail to account for dynamic device behavior or risk posture, rendering them ineffective against rogue devices. For example, if the audio video conferencing devices are statically segmented into a specific subnet, it is easy to plug in a laptop in the same subnet and sniff and snoop on the SIP communications. It is also easy to make a mistake and connect a conferencing device into other subnets, thereby creating more exposure than necessary.</p> <p data-bbox="651 226 867 1465">Micro-segmentation, on the other hand, is a more granular dynamic method of creating secure or trusted zones of connected devices. Micro-segmentation utilizes zero trust principles to isolate devices from one another using deep contextual information and secure them individually. Micro-segmentation is implemented in the software, using a layer that is decoupled from the underlying network hardware and NAC tools. This makes the segmentation easier to deploy and manage, providing security beyond static rules and authentication mechanisms to limit the blast radius in case of a security event.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 462 1032 1474"><p>The diagram shows a central circle containing a laptop and a smartphone. Six smaller circles are connected to this central circle, each representing a different aspect of the device's operation or data collection:</p><ul style="list-style-type: none">Type, Category: Represented by a bar chart icon.Spectrum: Represented by a radio tower and signal waves icon.Function, Services: Represented by a gear and a network diagram icon.Micro-location, BYOD: Represented by a location pin icon.Ownership, Control: Represented by a gear and a key icon.Data, Behavior: Represented by a network diagram icon.</div> <p>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf</p>

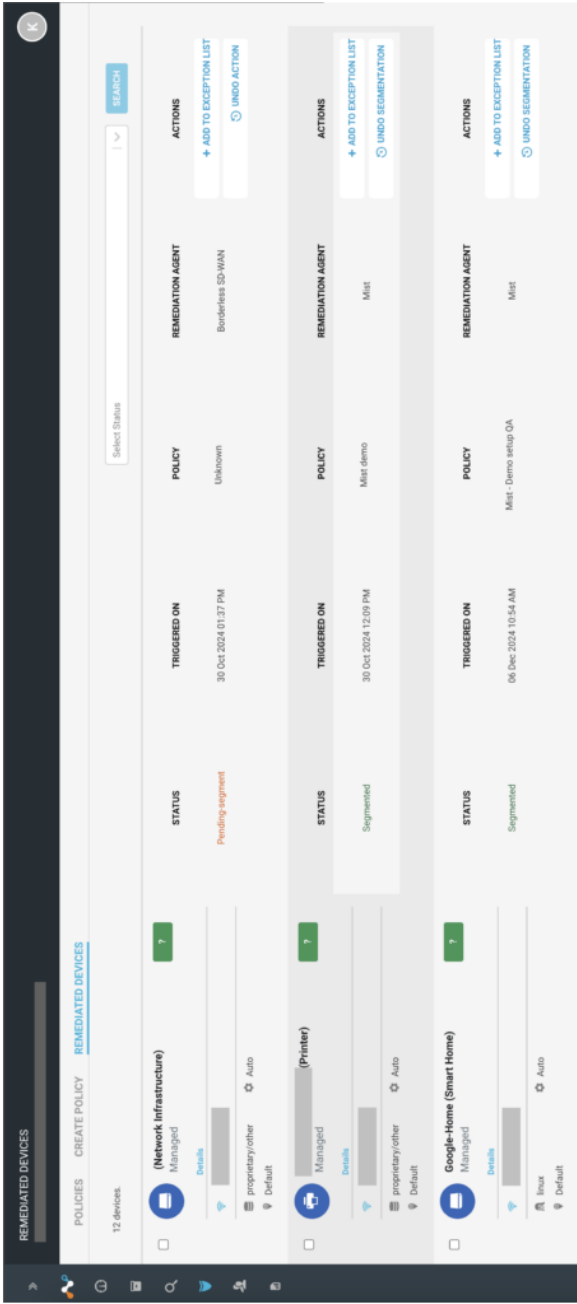
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 783 326 1423"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="365 289 651 1423"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="695 279 1352 1465"><p>The diagram illustrates the architecture of Device Intelligence, showing the flow of data and processing from a Customer Site to the Cloud.</p><p>Customer Site:</p><ul style="list-style-type: none">Airspace Data: Represented by a box with binary code (10010110011011, 01011001101100).Network Data: Represented by a box with binary code (10010110011011, 01011001101100).Radio Sensors or Access Points: Represented by a box with a signal icon.Network Sensor: Represented by a box with a server icon.Nextgen Access Control: A box at the bottom of the Customer Site section.netkope CUSTOMER SITE: The logo and name for the Customer Site.<p>Processing and Analysis:</p><ul style="list-style-type: none">Billions of daily measurements of device characteristics: A central circular area containing icons for OS, AI, and a shield, representing the core analysis engine.Deep Learning + Powerful Policy Engine: A circular area containing icons for a brain and a shield, representing the AI and policy processing engine.Alerts/Insights: A box below the central processing area.<p>Cloud:</p><ul style="list-style-type: none">Asset Mgmt Integration: A box on the left.Vulnerability Scanner Integration: A box on the left.MDM, EDR Integration: A box on the right.Security Integration: A box on the right.UI: A box on the left.SIEM: A box on the right.Ticketing: A box on the right.CLOUD: The overall environment.<p><small>© 2022 © Netskope Confidential. All rights reserved.</small></p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="261 1056 297 1465">Analytics and Protection </p> <ul data-bbox="331 149 597 1465" style="list-style-type: none"><li data-bbox="331 149 407 1465">• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies.<li data-bbox="428 149 505 1465">• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<li data-bbox="526 149 597 1465">• Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered. <p data-bbox="613 632 646 1476">https://docs.netskope.com/en/architecture-of-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="266 1094 305 1455">Remediated Devices</p> <p data-bbox="342 226 451 1455">Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p> <p data-bbox="483 226 511 1455">You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p> <ul data-bbox="540 310 1144 1419" style="list-style-type: none"> <li data-bbox="540 856 568 1419">• Device Name: The name or identifier of the device. <li data-bbox="597 688 625 1419">• Device Type: The type of device (e.g., computer, printer, IoT device). <li data-bbox="654 310 682 1419">• Device Details: By clicking on a details link, you will be navigated to a new page about the device details. <li data-bbox="711 468 738 1419">• Status: The current status of the remediation action (e.g., Pending Segment, Segmented). <li data-bbox="768 636 795 1419">• Triggered On: The date and time when the security policy was triggered. <li data-bbox="824 783 852 1419">• Policy: The name of the security policy that was triggered. <li data-bbox="881 552 909 1419">• Remediation Agent: The agent responsible for enforcing the remediation action. <li data-bbox="938 667 966 1419">• Actions: A set of actions that can be performed on the device, such as: <ul data-bbox="995 436 1144 1356" style="list-style-type: none"> <li data-bbox="995 531 1023 1356">• Add to Exception List: Excludes the device from future remediation actions. <li data-bbox="1052 531 1079 1356">• Undo Action: Reverses the previous remediation action taken on the device. <li data-bbox="1109 436 1136 1356">• Undo Segmentation: Reverses the previous segmentation action taken on the device.

U.S. Patent No. 11,916,902

Exemplary Evidence of Infringement



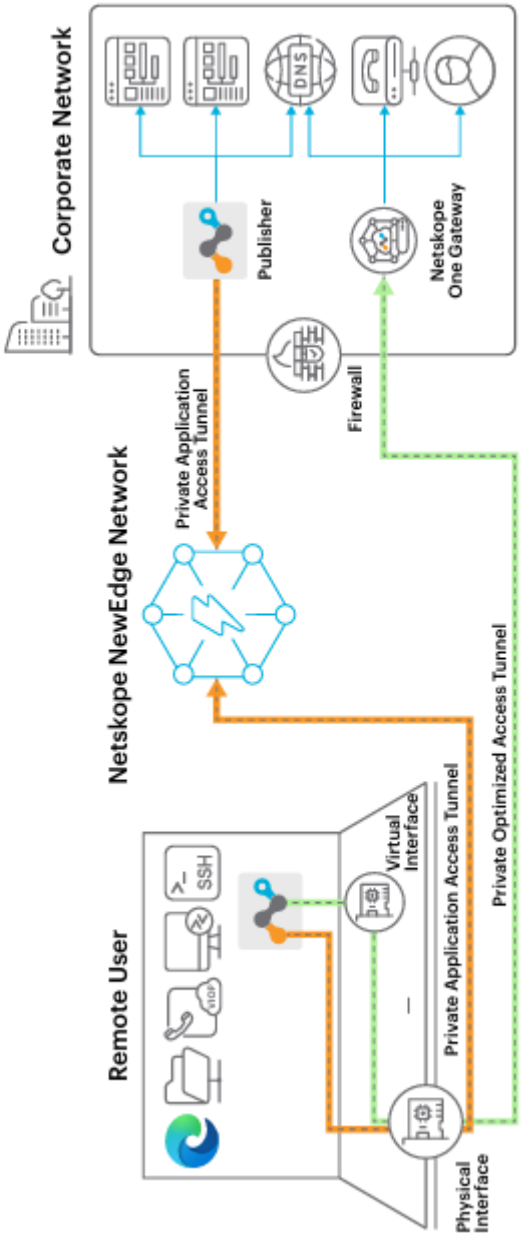
<https://docs.netkope.com/en/remediated-devices>

**Netskope Reference
Architecture Guide**

How to Use Zero Trust Network
Access as a Replacement for VPN
with Netskope One Private Access

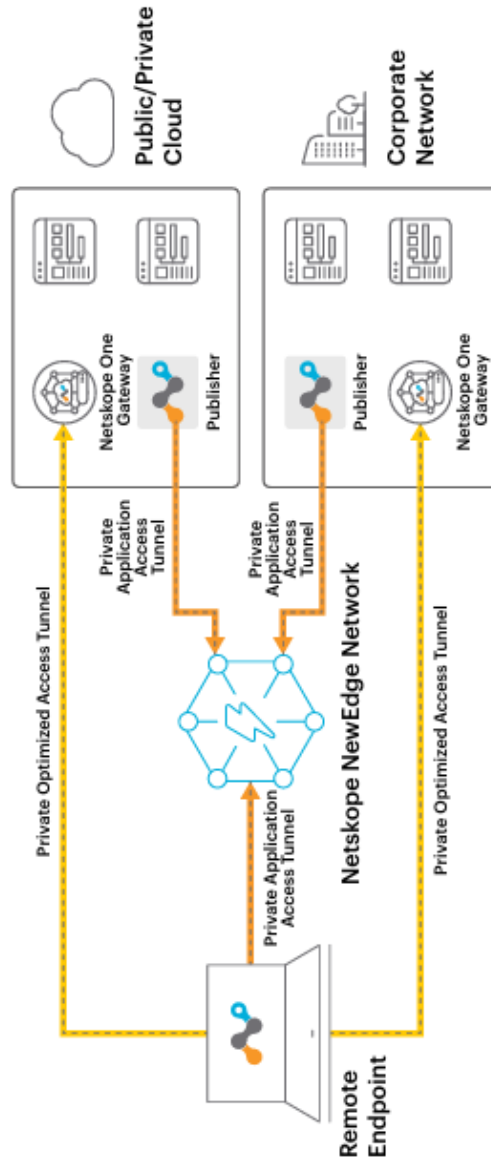
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Introducing Netskope One Private Access</p> <p>Delivered as a single solution, Netskope One Private Access integrates Zero Trust Network Access (ZTNA) and software-defined wide-area networking (SD-WAN) capabilities, enabling the complete retirement — not just partial replacement — of remote access VPNs for all relevant application access use cases, while enhancing security posture and boosting remote worker productivity with secure and seamless connectivity.</p> <p>The unified Netskope One Client sits in front of a converged architecture comprising Netskope One Private Application Access for access to client-initiated applications, and Netskope One Private Optimized Access to securely connect applications that require bi-directional, server-initiated traffic. The same Netskope One Client enables every other client inline Netskope service: NG-SWG, CASB Inline, FWaaS, DNS Security, Endpoint DLP.</p> <p>The solution utilizes zero trust principles to enhance overall security posture and reduce lateral threat movement, reduce deployment complexity, and optimize performance, and it enables ubiquitous access to corporate resources hosted anywhere through intelligent traffic steering. With Netskope One Private Access, organizations can avoid maintaining separate ZTNA and VPN clients, and instead provide consistent security for all applications with a unified client deployment.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Key Benefits</p> <p>Enforces Zero Trust Principles</p> <p>Netskope One Private Access incorporates zero trust principles and proposes a shift from traditional network-centric access control to granular application-centric access control on a per-user or user group basis. The solution accelerates the time frame for decommissioning legacy applications and minimises associated security risks, including unauthorized lateral movement. Key benefits include:</p> <ul style="list-style-type: none"> • Identity- and context-aware, least-privileged access to private applications hosted in public clouds or on-premises data centers. • Device Classification options to assess the posture of the client before providing access to private applications hosted in public clouds or on-premises data centers. • Facilitating the connectivity through the ZTNA broker in Netskope One platform. The applications are hidden from discovery, and access is restricted only to authenticated and authorised users. • Reducing the opportunities for lateral movement of threats within the private networks and limiting the blast radius. • Eliminating the dependence on public-facing VPNs or open inbound firewall ports for application access, securing networks from threats and DDoS attacks. <p>Secures All Enterprise Applications</p> <p>Netskope One Private Access also supports server-to-client traffic connectivity, enabling access to both legacy and modern applications through a single client. Key benefits include:</p> <ul style="list-style-type: none"> • Eliminating the need to maintain two separate solutions — VPN and ZTNA — for accessing all private applications and achieving greater cost savings by reducing capital and operational expenditure. • Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all private applications.

<p>U.S. Patent No. 11,916,902</p>	<p style="text-align: center;">Exemplary Evidence of Infringement</p> <p>Delivers a Phenomenal User Experience</p> <p>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key benefits include:</p> <ul style="list-style-type: none"> • Automatic traffic steering by the Netskope Client for connecting authorised users directly to specific resources regardless of where it is hosted. Strategically positioned Netskope NewEdge Network point of presence (PoP) helps achieve lowest possible latency and round-trip time for application access. <p>Full Zero Trust Application Access: Netskope One Private Unified Access</p> <p>Combining Private Application Access and Private Optimized Access capabilities on the same Endpoint, Netskope enables organisations to apply granular zero trust access to all Internal Applications, and support all use cases for a VPN replacement.</p> 
--	---

U.S. Patent No. 11,916,902**Exemplary Evidence of Infringement**

Netskope One Private Unified Access vastly improves the user experience by supporting multiple Private Application Access applications through a single connection to the NewEdge Network. Additionally, it supports multiple Private Optimized Access tunnels to multiple Netskope One Gateways, whether they're located in private Data Centers or Private/Public Clouds. This enables customers to not only streamline access and improve performance for all types of private applications, but also ensure granular zero trust-based access.



[2024-12-Reference-Architecture-Guide-for-ZTNA-Next-RA-709-3-1-1.pdf](#)

The Accused '902 Products include each and every element of this limitation, either literally or under the doctrine of equivalents. To the extent that this limitation is not literally met by the Accused '902 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '902 Products are insubstantial and make no material difference. The Accused '902 Products perform substantially the same function in substantially the same way to obtain substantially the same result as this limitation. For example, to the extent Netskope argues that micro-segmentation, isolation, or quarantining is not a virtual private network or virtual private network application, the same function is achieved by the Netskope Private Access products, SWG, and/or related products (as referenced above) working in cooperation with the Netskope One Client to

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>combine, unify, and/or distribute this functionality across devices to achieve the same result of mitigating the security issue of the unsecure network element by virtually providing secured network access.</p>
<p>12. The system of claim 11, wherein access to the known network is granted upon a combination of the requesting a grant of access from the known network to the processing device and a correct authorization credential presented by the processing device to the known network.</p>	<p>The Accused '902 Products include a system wherein access to the known network is granted upon a combination of the requesting a grant of access from the known network to the processing device and a correct authorization credential presented by the processing device to the known network.</p> <p>For example, Netskope's Private Access products and/or related products, features or functions of the Netskope One Platform grant or deny access to devices to connect to secure resources in the Netskope's NewEdge Network, including by the use of the Netskope One Client. This authorization further includes granting or denying access based on a correct authorization credentials presented.</p> <div data-bbox="748 371 1243 1476"> <h2 data-bbox="760 703 862 1465">What is ZTNA?</h2> <p data-bbox="943 392 1235 1465">Zero Trust Network Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA creates a new security and access framework for connecting users everywhere with enterprise resources. This security solution not only provides a modern security structure, but also enhances user experience with seamless connectivity to enterprise resources. With the rise of hybrid work and cloud adoption, it's become increasingly important to evolve access management to your key enterprise applications—no matter where they are hosted.</p> </div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 304 651 1470"><p data-bbox="256 1018 297 1470">Zero Trust Security Principles</p><p data-bbox="313 321 438 1470">ZTNA creates a new security framework, based on the <u>zero trust security model</u>, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application gateways. When a user connects, the cloud-based ZTNA broker verifies the user's identity and security posture before connecting users to the authorized applications.</p><p data-bbox="464 321 524 1470">Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.</p><p data-bbox="550 359 643 1470">Because ZTNA only grants application-specific access, not network access, it eliminates unauthorized lateral movement. With ZTNA, there is no inbound connectivity to the enterprise network and the resources remain hidden from discovery, reducing the digital attack surface.</p></div> <p data-bbox="659 478 691 1470">https://www.netskope.com/security-defined/what-is-zero-trust-network-access</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="261 682 1300 1472"><p data-bbox="261 709 305 1465">Seamless and optimized user experience</p><p data-bbox="331 716 496 1465">Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.</p><p data-bbox="558 716 678 1465">Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:</p><ul data-bbox="740 695 1292 1465" style="list-style-type: none"><li data-bbox="740 716 1040 1465">• Automatic traffic steering by Netskope One Client for connecting authorized users directly to specific resources regardless of where it is hosted. Powered by the Netskope NewEdge Network, the world's largest cloud security infrastructure, and advanced routing optimization, it optimizes performance across cloud and on-prem access.<li data-bbox="1081 695 1292 1465">• Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity.</div> <p data-bbox="1305 212 1373 1472">https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 191 1169 1480"><div data-bbox="289 191 695 1480"><h2 data-bbox="289 1178 342 1480">Netskope One Client</h2><p data-bbox="597 212 682 1480">Netskope One Client is the industry's first unified SASE client, unifying connectivity to their web, cloud, AI, private apps, and UCaaS services and providing endpoint DLP controls.</p></div><div data-bbox="695 426 1128 1480"><h2 data-bbox="711 527 792 1480">A simplified user experience</h2><p data-bbox="857 447 1117 1480">Easy to use, lightweight and highly performant, Netskope One Client steers user traffic through the <u>Netskope One</u> platform. Netskope One Client centralized configuration, deployment, support, and troubleshooting delivers comprehensive security and control across the borderless modern threat landscape.</p><p data-bbox="1133 877 1169 1480">https://www.netskope.com/netskope-one/client</p></div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netkope.com/en/what-is-netkope-iot-security</p>

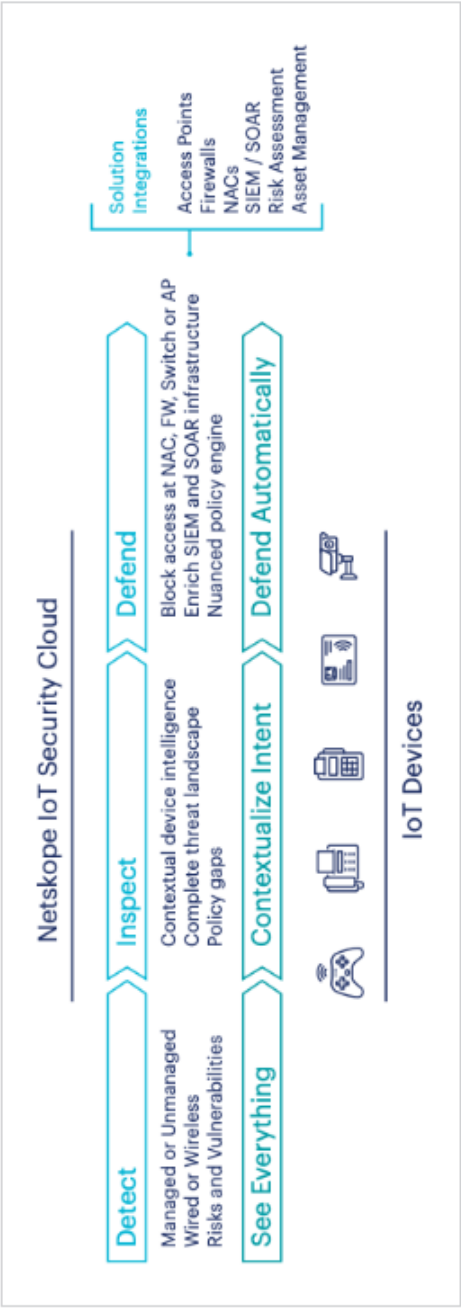
U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:</p> <ul style="list-style-type: none"> • Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior. • Cybersecurity asset management – Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR. • Device risk assessment – Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations. • Access control and segmentation – Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls. <p>https://docs.netkope.com/en/what-is-netkope-iot-security</p>

<p>U.S. Patent No. 11,916,902</p>	<div data-bbox="203 562 237 1066"> <p>Exemplary Evidence of Infringement</p> </div> <div data-bbox="285 783 326 1423"> <h3>Architecture of Device Intelligence</h3> </div> <div data-bbox="363 285 649 1423"> <p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p> </div> <div data-bbox="691 275 1357 1467"> <p>The diagram illustrates the IoT Security Platform architecture, which is an AI-based context generation platform for all devices. It is divided into two main sections: CUSTOMER SITE and CLOUD.</p> <p>CUSTOMER SITE:</p> <ul style="list-style-type: none"> Radio Sensors or Access Points: These collect data from devices. They are connected to the Nextgen Access Control module. Network Sensor: This module collects data from the network and sends it to the Nextgen Access Control module. Nextgen Access Control: This module processes the data and sends it to the Models / Controls module. Models / Controls: This module generates Billions of daily measurements of device characteristics, which are then sent to the Deep Learning + Powerful Policy Engine. <p>CLOUD:</p> <ul style="list-style-type: none"> Deep Learning + Powerful Policy Engine: This engine processes the data and generates Alerts/Insights. Alerts/Insights: These are sent to the UI, SIEM, and Ticketing modules. UI, SIEM, Ticketing: These modules provide a user interface, security information and event management, and ticketing services, respectively. <p>The diagram also shows the integration of various security services: Asset Mgmt Integration, Vulnerability Scanner Integration, MDM, EDR Integration, and Security Integration.</p> <p><small>© 2022 Netskope Confidential. All rights reserved.</small></p> </div>
--	--

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p data-bbox="326 1178 358 1436">Data Acquisition</p> <ul data-bbox="396 247 870 1394" style="list-style-type: none"> <li data-bbox="396 354 428 1394">• Customer environments have network sensors installed as physical or virtual appliances. <li data-bbox="451 247 570 1394">• These network sensors receive span traffic from core or distributed switches using Switched Port Analyzer port (SPAN), Test Access Point (TAP) or mirrored sensors and perform deep packet inspection on the traffic data. <li data-bbox="592 247 672 1394">• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC. <li data-bbox="695 247 774 1394">• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices. <li data-bbox="797 264 870 1394">• In the case of third party cloud managed access points like MIST and Meraki, the product directly retrieves device information using cloud integrations through API.

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="256 306 1024 1472"><p data-bbox="280 1251 313 1451">Data Analysis</p><ul data-bbox="345 344 553 1409" style="list-style-type: none"><li data-bbox="345 758 378 1409">• On the cloud, various microservices analyze the metadata.<li data-bbox="399 344 553 1409">• The deep learning and powerful policy engine defines the device properties, risk and threat assessment, and determines access restrictions. Device Intelligence sends this information to the customer through Security Information and Event Management (SIEM), user interface, and ticketing tools.<p data-bbox="589 1094 621 1451">Analytics and Protection</p><ul data-bbox="654 331 1000 1409" style="list-style-type: none"><li data-bbox="654 344 773 1409">• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies.<li data-bbox="794 390 867 1409">• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<li data-bbox="888 331 1000 1409">• Customers can create the policies in the UI. Device Intelligence dynamically applies policies on the devices and the metadata. When the policy conditions are met, the configured policy actions are triggered.<p data-bbox="1032 632 1065 1472">https://docs.netskope.com/en/architecture-of-netskope-iot-security</p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div><div>Home > Device Intelligence > Protect Device Intelligence > Remediated Devices</div><div><h2>Remediated Devices</h2><p>Navigate to Policies menu, in the Remediated Devices tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.</p><p>You will see a list of devices that have triggered security policies. Each device entry includes the following information:</p><ul style="list-style-type: none">• Device Name: The name or identifier of the device.• Device Type: The type of device (e.g., computer, printer, IoT device).• Device Details: By clicking on a details link, you will be navigated to a new page about the device details.• Status: The current status of the remediation action (e.g., Pending Segment, Segmented).• Triggered On: The date and time when the security policy was triggered.• Policy: The name of the security policy that was triggered.• Remediation Agent: The agent responsible for enforcing the remediation action.• Actions: A set of actions that can be performed on the device, such as:<ul style="list-style-type: none">• Add to Exception List: Excludes the device from future remediation actions.• Undo Action: Reverses the previous remediation action taken on the device.• Undo Segmentation: Reverses the previous segmentation action taken on the device.<p>https://docs.netskope.com/en/remediated-devices</p></div></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>13. The system of claim 11, wherein the insecure network element is an Internet of Things (IoT) device.</p>	<p>The Accused '902 Products include a system wherein the insecure network element is an Internet of Things (IoT) device.</p> <p>For example, Netskope's Device Intelligence (formerly known as Netskope IoT Security) implements Analytics and Protection of Internet of Things (IoT) devices in and around the network of the remote user's device for use in making access determinations for the device.</p>  <p>The diagram illustrates the Netskope IoT Security Cloud architecture. It shows a flow from IoT Devices (represented by icons of a game controller, a printer, a server, and a smartphone) through three main stages: Detect, Inspect, and Defend. The Detect stage includes 'Managed or Unmanaged Wired or Wireless Risks and Vulnerabilities' and 'See Everything'. The Inspect stage includes 'Contextual device intelligence', 'Complete threat landscape', and 'Policy gaps', leading to 'Contextualize Intent'. The Defend stage includes 'Block access at NAC, FW, Switch or AP', 'Enrich SIEM and SOAR infrastructure', and 'Nuanced policy engine', leading to 'Defend Automatically'. Finally, the architecture connects to 'Solution Integrations' which include 'Access Points', 'Firewalls', 'NACs', 'SIEM / SOAR', 'Risk Assessment', and 'Asset Management'.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<p>Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk analysis against a particular request or action. It creates a numeric assessment of the riskiness of allowing a particular request/action, which the policy engine uses to make an ultimate authorization decision.</p> <p>Zero trust in a smart device context means that each user, device, data flow, and location is monitored continuously and granted/revoked access to other resources on the network based on these observations. To do this effectively, the Device Intelligence solution studies:</p> <ul style="list-style-type: none"> • HyperContext – Deep context about every device, resource, and user in and around the network. • Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation. • Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment. • Automation – A policy engine driven by a combination of an understanding of the organization's requirements and automation to handle devices at the IoT scale. <p>https://docs.netskope.com/en/what-is-netskope-iot-security</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	<div data-bbox="289 783 326 1423"><h3>Architecture of Device Intelligence</h3></div> <div data-bbox="367 289 651 1423"><p>An organization has a number of devices connected to the network in the environment. It is important to classify and protect these devices for security reasons. Device Intelligence discovers all the managed and un-managed devices in the network and the product gives a deep visibility of the connected devices. The solution uses traffic characteristics to derive metadata information and sends the metadata to the cloud for analysis and check for any potential threats using AI and machine learning. Device Intelligence dynamically applies policies to protect the devices by assigning the devices to VLANs, quarantining the devices, reporting to the administrators, etc.</p></div> <div data-bbox="695 289 1349 1461"><p>The diagram illustrates the architecture of Device Intelligence, showing the flow of data and processing from a Customer Site to the Cloud.</p><p>Customer Site:</p><ul style="list-style-type: none">Airspace Data: Represented by a box with binary code (10010110011011, 01011001101100).Network Data: Represented by a box with binary code (10010110011011, 01011001101100).Radio Sensors or Access Points: Represented by a box with a signal icon.Network Sensor: Represented by a box with a server icon.Nextgen Access Control: A box containing the text "CUSTOMER SITE" and the "netskope" logo.<p>Processing and Analysis:</p><ul style="list-style-type: none">Billions of daily measurements of device characteristics: A central circular process involving "AI" and "ML" icons, with arrows indicating data flow from the Customer Site.Deep Learning + Powerful Policy Engine: A central circular process receiving input from the "Models / Controls" box and outputting to the "Alerts/Insights" box.Alerts/Insights: A box containing the text "Billions of daily device behavior analyzed".<p>Cloud:</p><ul style="list-style-type: none">Asset Mgmt Integration: A box with a gear icon.Vulnerability Scanner Integration: A box with a magnifying glass icon.MDM, EDR Integration: A box with a document icon.Security Integration: A box with a shield icon.UI: A box with a monitor icon.SIEM: A box with a document icon.Ticketing: A box with a ticket icon.<p>Cloud: A box containing the text "CLOUD" and the "netskope" logo.</p><p><small>© 2022 Netskope Confidential. All rights reserved.</small></p></div>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
	https://docs.netskope.com/en/architecture-of-netskope-iot-security
14. A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processing resources of a computer system, causes the one or more processing resources to perform a method comprising:	<p>The Accused '902 Products include a non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processing resources of a computer system, causes the one or more processing resources to perform a method.</p> <p><i>See</i> 1[pre] and 1[a] incorporated here by reference.</p>
14[a] receiving, by a processing device, a request to access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;	<p>The Accused '902 Products include receiving, by a processing device, a request to access a known network from a known access device connected through a remote network, wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network.</p> <p><i>See</i> 1[a] incorporated here by reference.</p>
14[b] scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an insecure network element on the remote network.	<p>The Accused '902 Products include scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an insecure network element on the remote network.</p> <p><i>See</i> 1[b] incorporated here by reference.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
element on the remote network;	
14[c] based at least in part on identifying at least one insecure network element on the remote network, denying access to the known network; and	<p>The Accused '902 Products include based at least in part on identifying at least one insecure network element on the remote network, denying access to the known network.</p> <p><i>See</i> 1[c] incorporated here by reference.</p>
14[d] based at least in part upon on failure to identify any insecure network element on the remote network, requesting a grant of access from the known network to the processing device.	<p>The Accused '902 Products include based at least in part upon on failure to identify any insecure network element on the remote network, requesting a grant of access from the known network to the processing device.</p> <p><i>See</i> 1[d] incorporated here by reference.</p>
14[e]. wherein mitigating a security issue of the insecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.	<p>The Accused '902 Products include wherein mitigating a security issue of the insecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.</p> <p><i>See</i> 1[e] incorporated here by reference.</p>
15. The non-transitory computer-readable storage medium embodying the set of instructions of claim 14, which when executed by one or more processing resources of the	<p>The Accused '902 Products include upon denying access to the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.</p> <p><i>See</i> claim 5 incorporated here by reference.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>computer system, causes the one or more processing resources to perform the method further comprising: upon denying access to the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.</p>	
<p>16. The non-transitory computer-readable storage medium embodying the set of instructions of claim 15, which when executed by one or more processing resources of the computer system, causes the one or more processing resources to perform the method further comprising: mitigating a security issue of the unsecure network element; and based at least in part upon mitigating the security issue of the unsecure network element, requesting a grant of access from the known network to the processing device.</p>	<p>The Accused '902 Products include mitigating a security issue of the unsecure network element; and based at least in part upon mitigating the security issue of the unsecure network element, requesting a grant of access from the known network to the processing device.</p> <p>See claim 6 incorporated here by reference.</p>

U.S. Patent No. 11,916,902	Exemplary Evidence of Infringement
<p>17. The non-transitory computer-readable storage medium embodying the set of instructions of claim 15, which when executed by one or more processing resources of the computer system, causes the one or more processing resources to perform the method further comprising: using a network connection between the processing device and the known network; and while using the network connection between the processing device and the known network, scanning the remote network through which access to the known network is established, wherein the scanning is configured to identify an unsecure network element on the remote network.</p>	<p>The Accused '902 Products include using a network connection between the processing device and the known network; and while using the network connection between the processing device and the known network, scanning the remote network through which access to the known network is established, wherein the scanning is configured to identify an unsecure network element on the remote network.</p> <p>See claim 8 incorporated here by reference.</p>