# 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 conjuncture with Netskope Device Intelligence and/or the Netskope One Client.

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 1[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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00002

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The Power of One**<br><br>The major components of the Netskope One platform include:<br><br>**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.<br><br>2025-03-Netskope-One-Platform-SB-719-5.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00003

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00004

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

# Netskope One Private Access

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.

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:

- 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
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00005

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 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; | 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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00006

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The Power of One**<br><br>The major components of the Netskope One platform include:<br><br>**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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00007

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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00008

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **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.<br>2025-03-Netskope-One-Platform-SB-719-5.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00009

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The Power of One**<br><br>The major components of the Netskope One platform include:<br><br>**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.<br><br>2025-03-Netskope-One-Platform-SB-719-5.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00010

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00011

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

# Netskope One Private Access

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.

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:

- 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
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00012

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 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; | 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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00013

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The Power of One**<br><br>The major components of the Netskope One platform include:<br><br>**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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00014

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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00015

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **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.<br>2025-03-Netskope-One-Platform-SB-719-5.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00016

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00017

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

# Netskope One Private Access

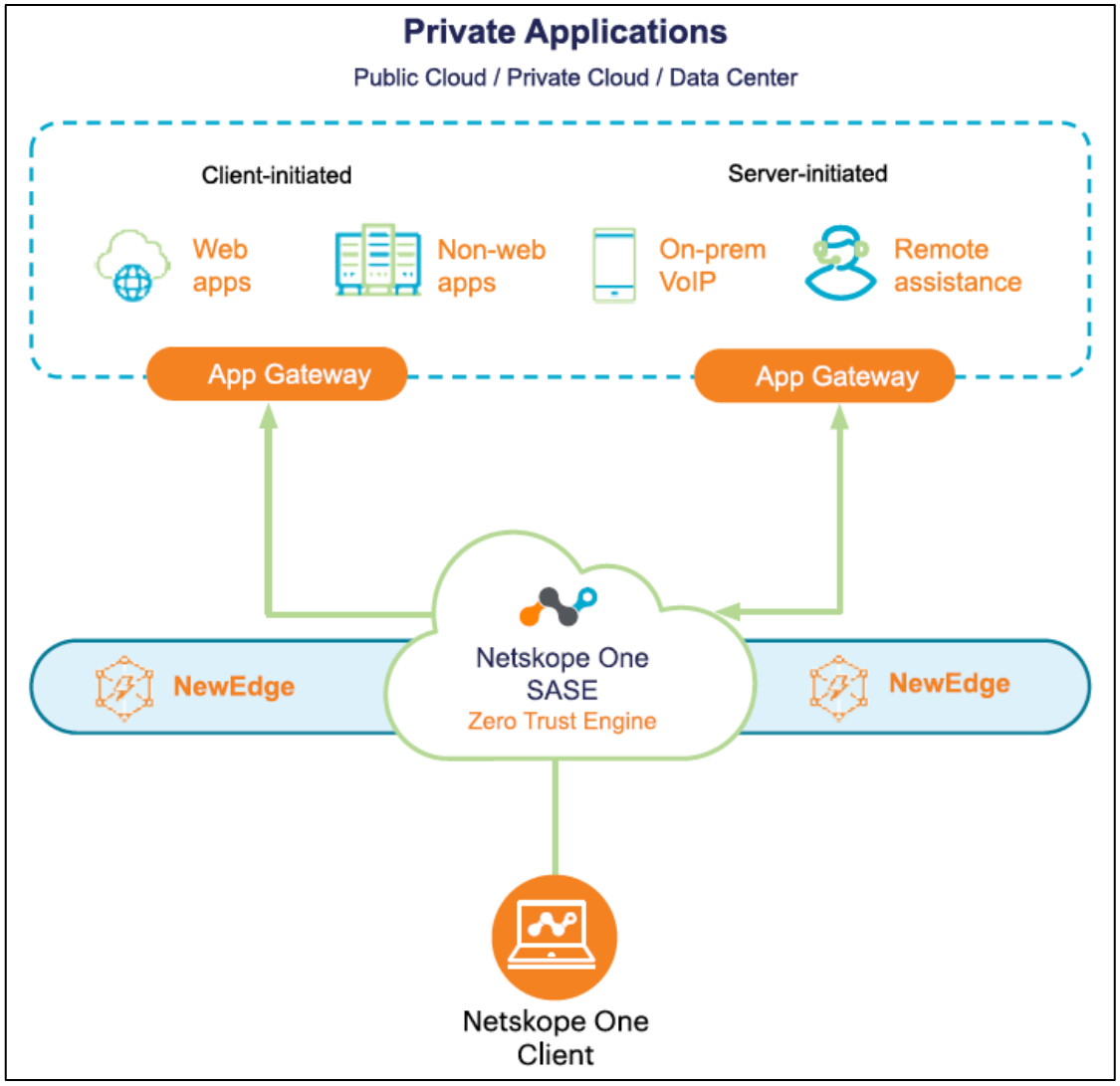
Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.

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:

- 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
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00018

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




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00019

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00020

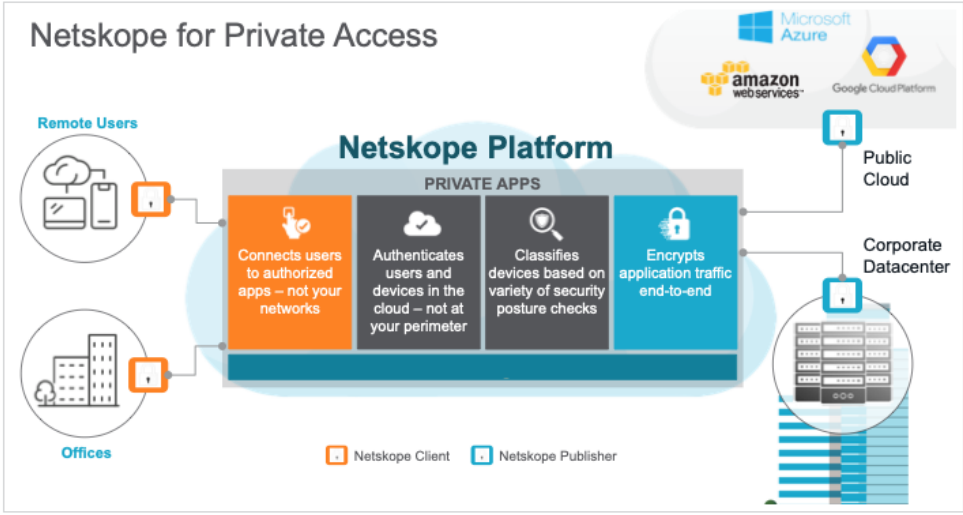
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|

### How It Works

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.

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.

NPA is illustrated in this diagram:




https://docs.netskope.com/en/netskope-private-access

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00021

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

### Connection

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.

### TLS

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.

### Inside Netskope POPs

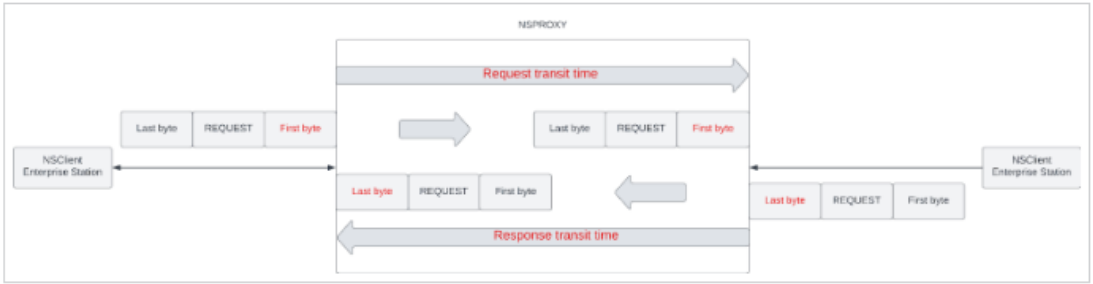
The following metric is processed at the NSProxy level.

## POP Transit Time

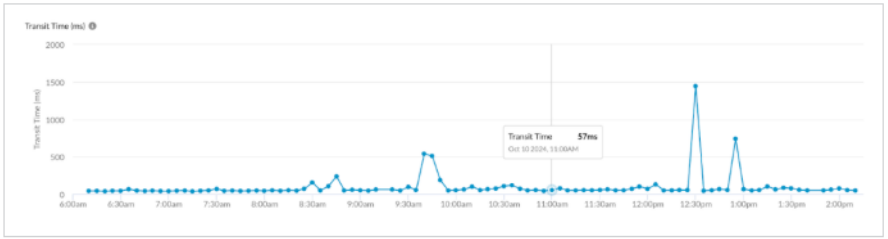
The POP Transit Time provides the total time spent within the NSProxy.

It is the addition of the "request transit time" and the "response transit time". These are defined as follows:

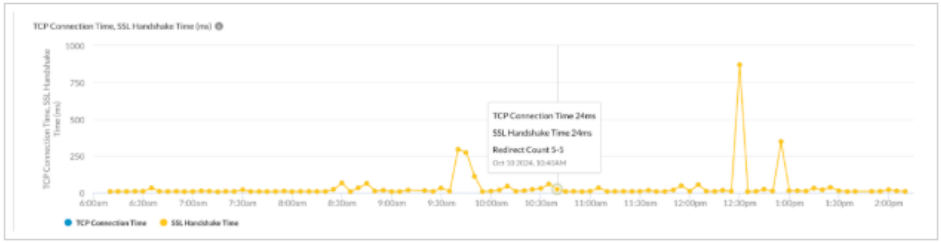
- Request transit time
  Time elapsed between the first byte of request reaching the NSProxy and this first byte of the request leaving the NSProxy
- Response transit time
  Time elapsed between the first byte of response reaching the NSProxy and this first byte of response leaving the NSProxy




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00022

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Netskope POPs to Applications**<br><br>The following metrics are processed at the NSProxy level.<br><br>**Connection**<br><br>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.<br><br>**Server**<br><br>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.<br><br>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.<br><br>https://docs.netskope.com/en/performance-metrics<br><br>**Transit Time**<br><br>  <br><br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00023

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **TCP Connection Time, SSL Handshake Time**<br>  <br>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.<br>https://docs.netskope.com/en/user-overview<br><br>The Netskope Private Access products, SWG 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00024

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Netskope Advances Netskope One Platform With AI-Driven Proactive DEM Solution, Key Security Innovations<br><br>***Network Visibility and Control, Advanced Evasive Threat Detection, Context-Aware Zero Trust Integrations Accelerate Cloud Networking and Security Operations***<br><br>**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.<br><br>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.<br><br>https://www.netskope.com/press-releases/netskope-advances-netskope-one-platform-with-ai-driven-proactive-dem-solution-key-security-innovations |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00025

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | <br>https://www.netskope.com/resources/data-sheets/netskope-newedge-data-sheet |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00026

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | <br>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.<br>. . . |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00027

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

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.

**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

# Inside the Netskope NewEdge Data Center Factory

Jul 13 2021 | 9 min. read

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00028

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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 *integrated racks* 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.<br>. . .<br>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<br>https://www.netskope.com/blog/inside-the-netskope-newedge-data-center-factory<br><br>Understanding Coverage Isn't Just About Counting Data Centers<br>Aug 04 2020 \| 6 min. read<br>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<br>https://www.netskope.com/blog/understanding-coverage-isnt-just-about-counting-data-centers<br><br>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 |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00029

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Netscope 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. |
| 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 unsecure network element on the remote network; | 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 unsecure network element on the remote network.<br><br>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.<br><br>**What is ZTNA?**<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00030

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

## 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

# Netskope One Private Access

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.

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00031

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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:<br><br>• 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<br><br>• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00032

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The Power of One**<br><br>The major components of the Netskope One platform include:<br><br>**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.<br><br>2025-03-Netskope-One-Platform-SB-719-5.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00033

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00034

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

# Netskope One Private Access

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.

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:

- 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
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00035

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 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; | 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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00036

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The Power of One**<br><br>The major components of the Netskope One platform include:<br><br>**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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00037

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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00038

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **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.<br>2025-03-Netskope-One-Platform-SB-719-5.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00039

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00040

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

# Netskope One Private Access

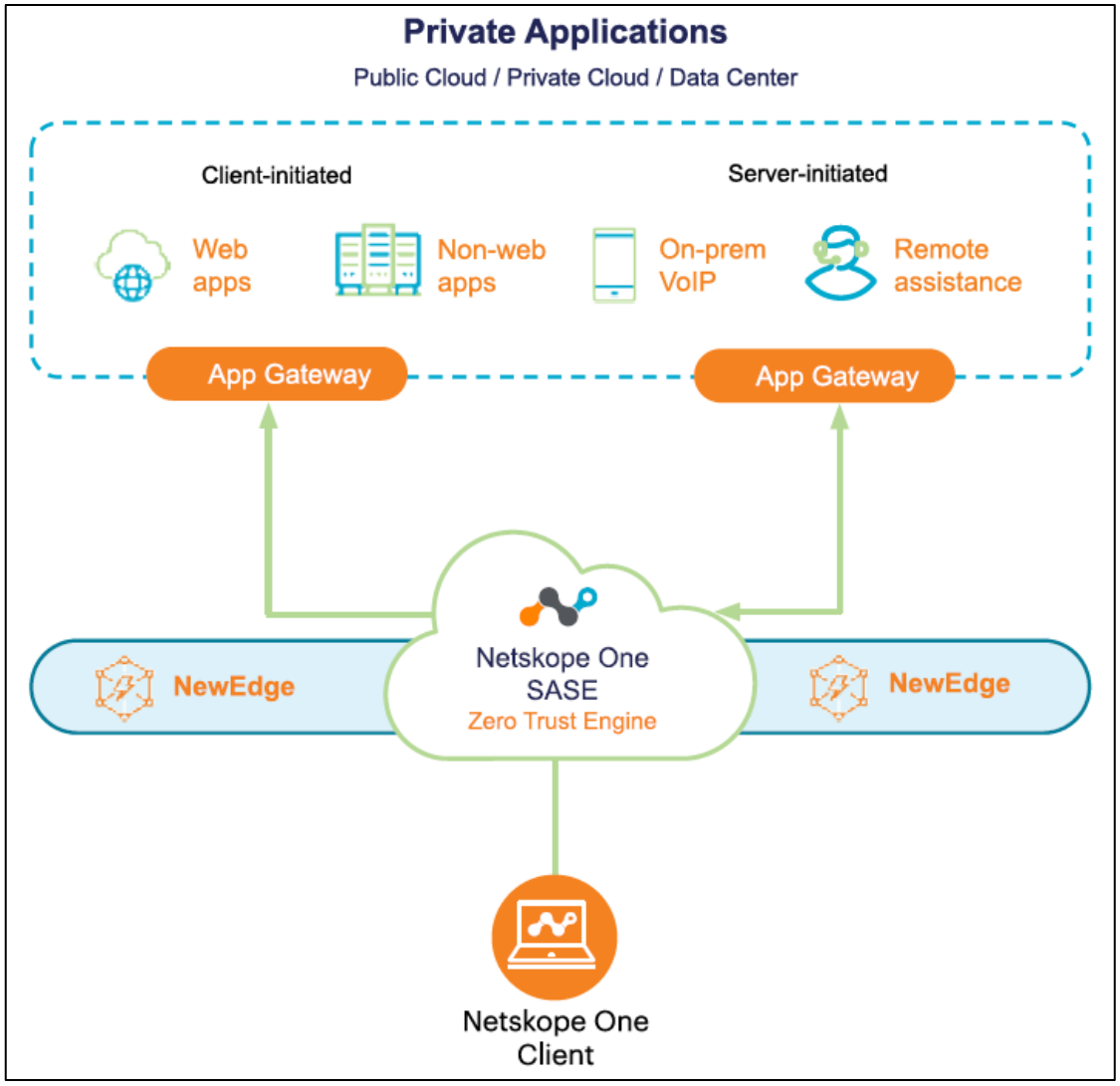
Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.

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:

- 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
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00041

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




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00042

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00043

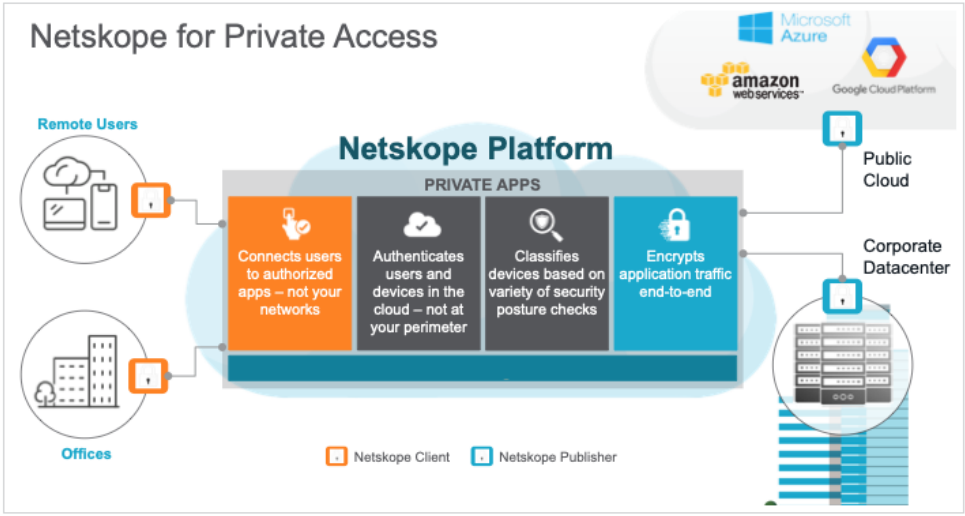
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|

### How It Works

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.

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.

NPA is illustrated in this diagram:




https://docs.netskope.com/en/netskope-private-access

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00044

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

### Connection

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.

### TLS

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.

### Inside Netskope POPs

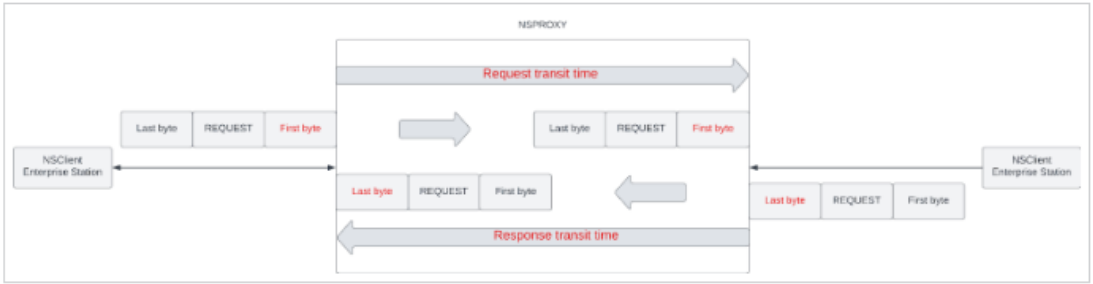
The following metric is processed at the NSProxy level.

## POP Transit Time

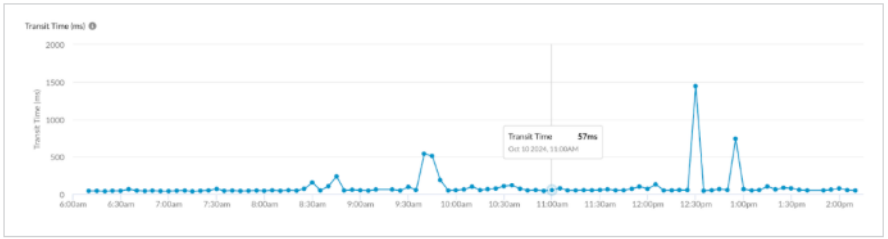
The POP Transit Time provides the total time spent within the NSProxy.

It is the addition of the "request transit time" and the "response transit time". These are defined as follows:

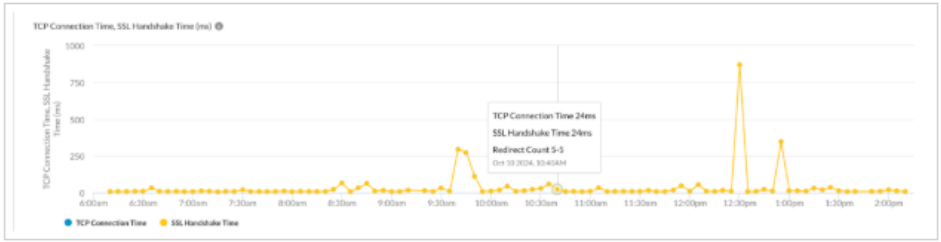
- Request transit time
  Time elapsed between the first byte of request reaching the NSProxy and this first byte of the request leaving the NSProxy
- Response transit time
  Time elapsed between the first byte of response reaching the NSProxy and this first byte of response leaving the NSProxy




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00045

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Netskope POPs to Applications**<br><br>The following metrics are processed at the NSProxy level.<br><br>**Connection**<br><br>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.<br><br>**Server**<br><br>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.<br><br>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.<br><br>https://docs.netskope.com/en/performance-metrics<br><br>**Transit Time**<br><br>  <br><br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00046

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **TCP Connection Time, SSL Handshake Time**<br>  <br>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.<br>https://docs.netskope.com/en/user-overview<br><br>The Netskope Private Access products, SWG 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00047

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Netskope Advances Netskope One Platform With AI-Driven Proactive DEM Solution, Key Security Innovations<br><br>***Network Visibility and Control, Advanced Evasive Threat Detection, Context-Aware Zero Trust Integrations Accelerate Cloud Networking and Security Operations***<br><br>**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.<br><br>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.<br><br>https://www.netskope.com/press-releases/netskope-advances-netskope-one-platform-with-ai-driven-proactive-dem-solution-key-security-innovations |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00048

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | <br>https://www.netskope.com/resources/data-sheets/netskope-newedge-data-sheet |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00049

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Netskope NewEdge**<br><br>**Cloud security without sacrificing performance**<br><br>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.<br><br>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.<br><br>. . . |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00050

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>**Future-proof, SASE-ready architecture**<br>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.<br><br>https://www.netskope.com/wp-content/uploads/2022/12/2023-04-NewEdge-DS-333-7-1.pdf<br><br>Inside the Netskope NewEdge Data Center Factory<br><br>Jul 13 2021 \| 9 min. read |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00051

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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 *integrated racks* 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.<br>. . .<br>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<br>https://www.netskope.com/blog/inside-the-netskope-newedge-data-center-factory<br><br>Understanding Coverage Isn't Just About Counting Data Centers<br>Aug 04 2020 \| 6 min. read<br>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<br>https://www.netskope.com/blog/understanding-coverage-isnt-just-about-counting-data-centers<br><br>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 |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00052

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Netscope 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. |
| 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 unsecure network element on the remote network; | 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 unsecure network element on the remote network.<br><br>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.<br><br> |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00053

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

## 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

# Netskope One Private Access

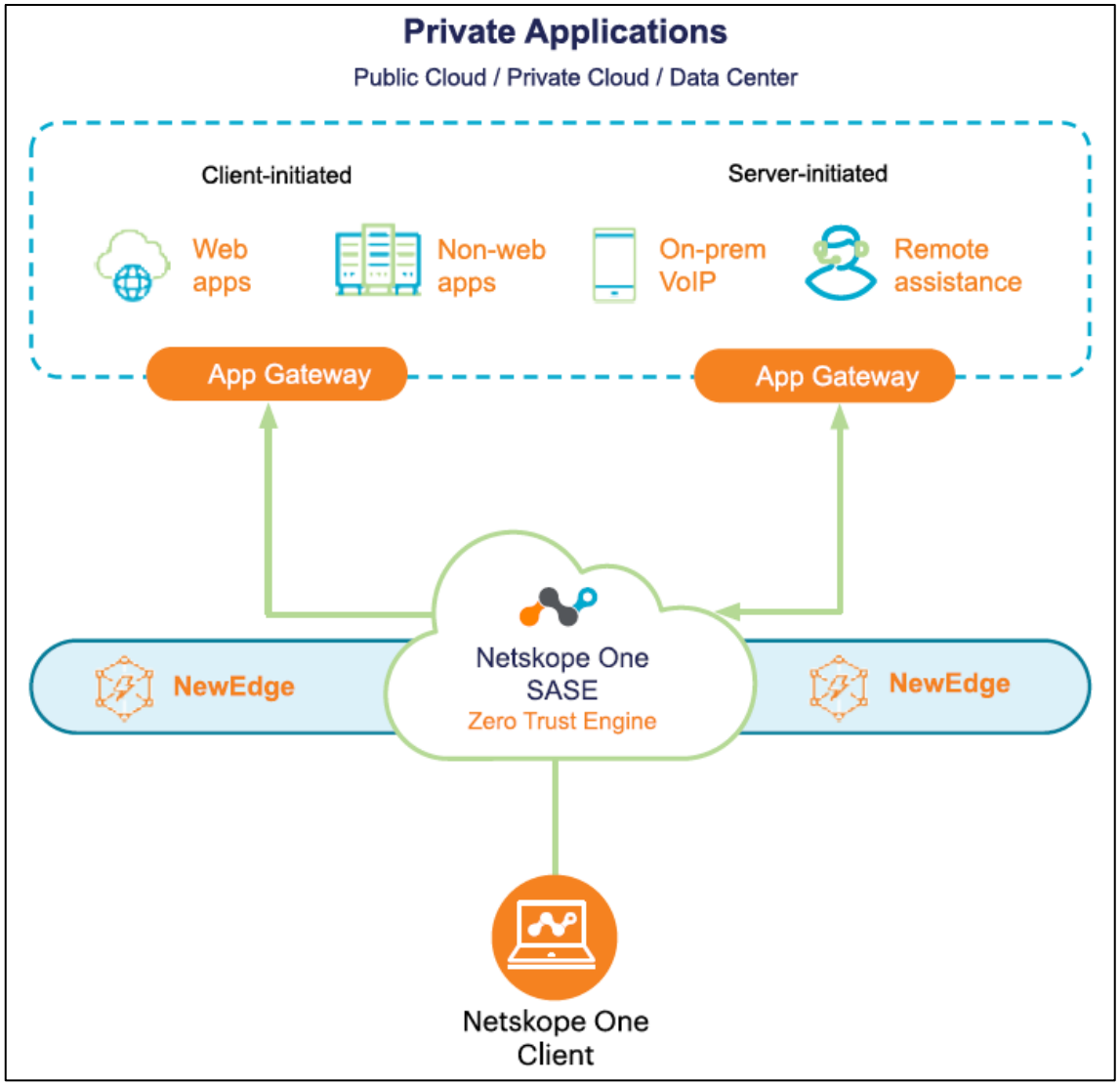
Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00054

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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:<br><br>• 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<br><br>• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications |

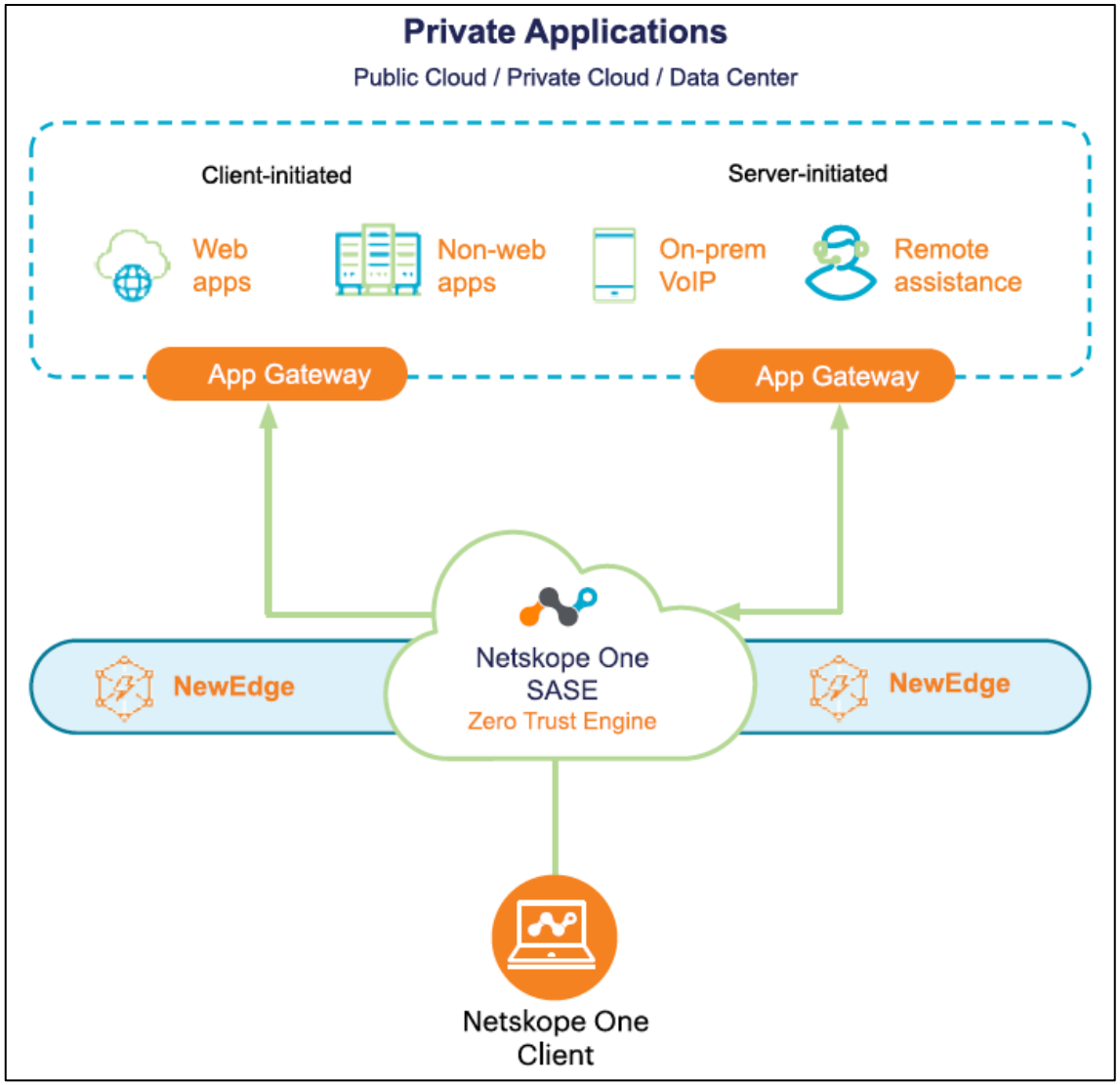
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00055

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




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00056

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




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00057

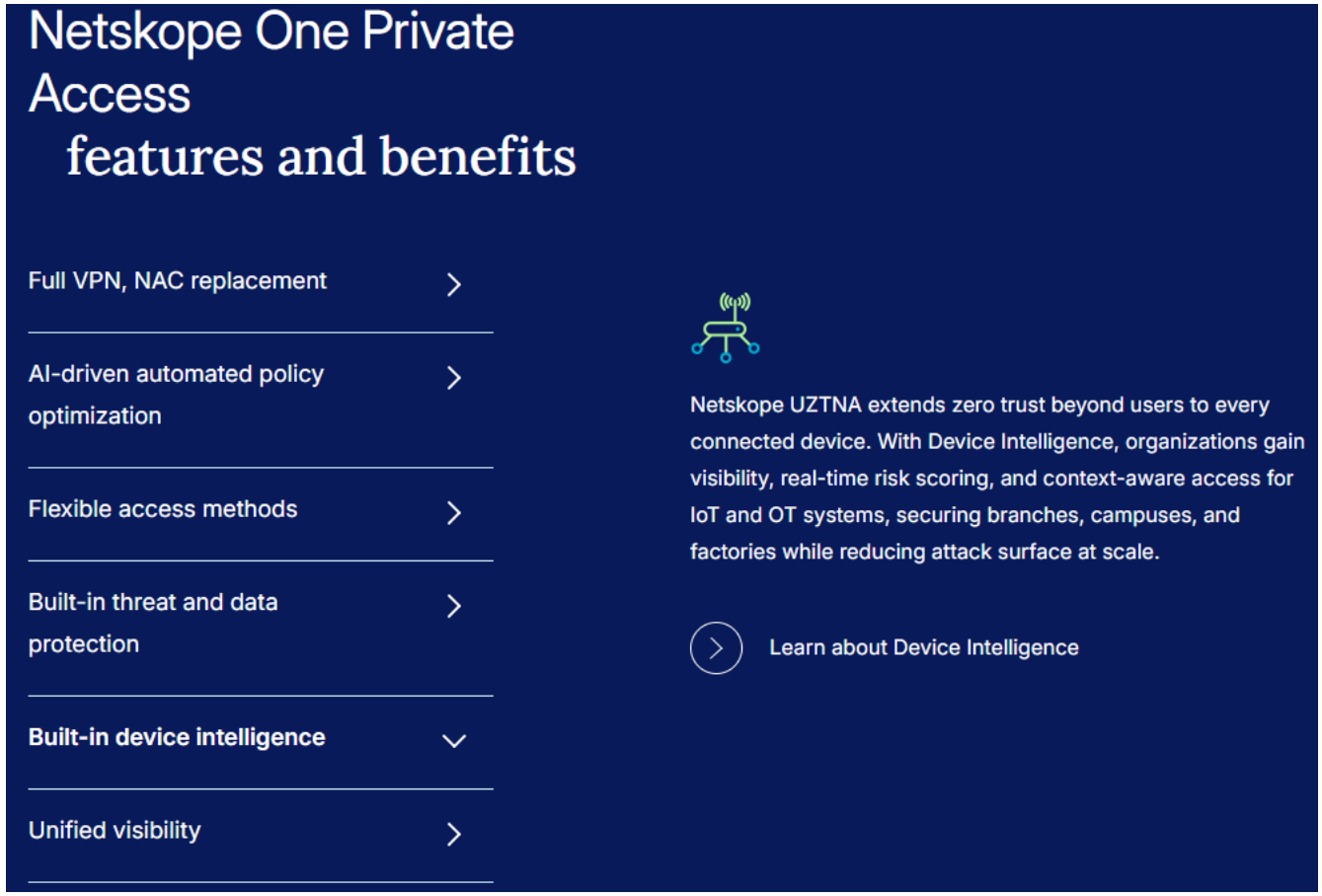
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00058

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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 (*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) to identify threats from unsecured network resources, or on a network with unsecured devices. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00059

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




https://www.netskope.com/products/private-access

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00060

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br><br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00061

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

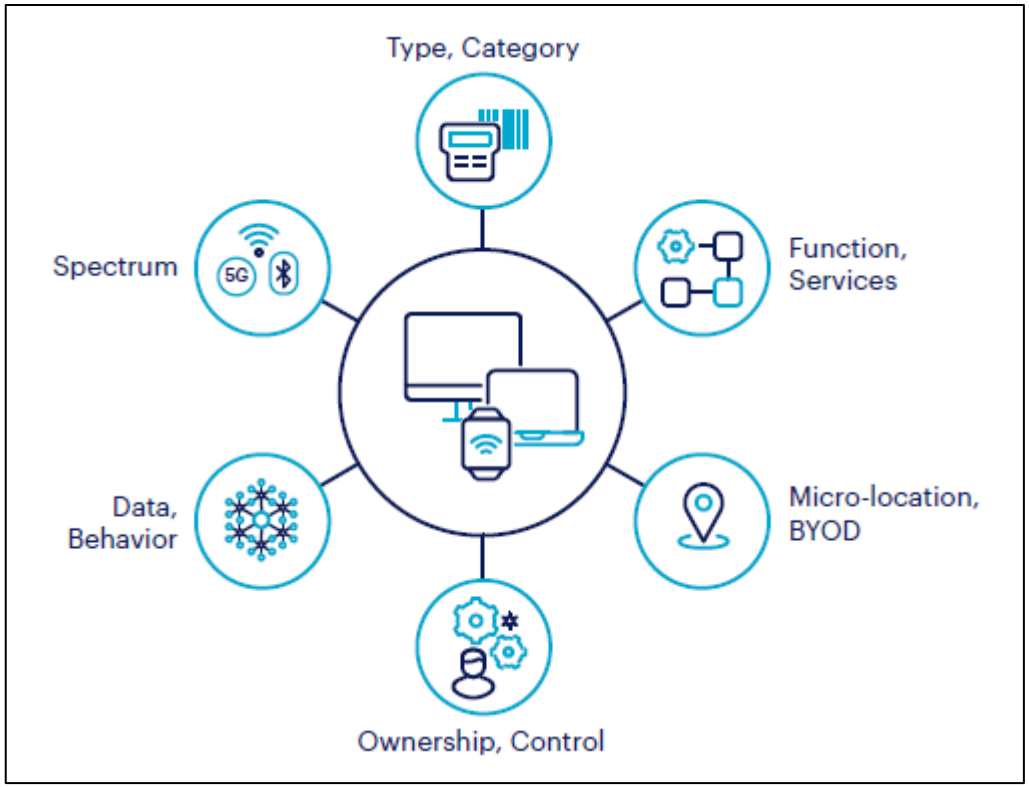
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00062

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00063

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE**<br><br>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®:<br>• Association of all the physical interfaces of the device and the spectrum of operation of each interface<br>• Type, Category of the device and related information<br>• OS, patches, services, and applications running on the device<br>• Functionality or the "purpose in life" of the device<br>• Micro location of the device, its mobility patterns, and times of visibility<br>• Ownership information of the device and its control information<br>• Users on the device<br>• Behavior based analysis of all the data transmissions across all protocols and spectrums<br>• Risk and vulnerability information, other information collected by other tools used |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00064

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00065

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

Home > Device Intelligence > Investigate Device Intelligence > Investigate Devices

## Investigate Devices

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.

> **Note**
>
> You can also sort the device summary in combination with the total of all devices, managed, unmanaged, new, automated, and user-controlled devices.

### Investigate Devices based on Spectrum

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.

https://docs.netskope.com/en/investigate-devices



Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00066

| 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.

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.

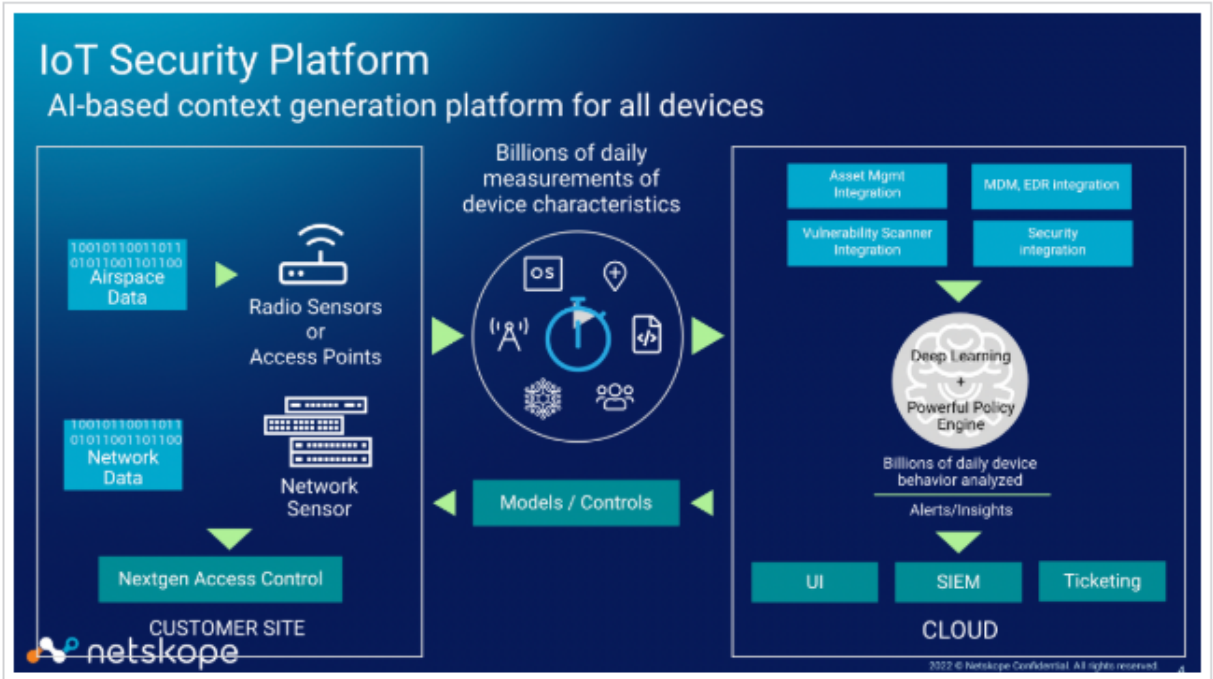
https://docs.netskope.com/en/investigate-risks

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00067

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00068

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00069

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

### Data Transfer

- 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.

### Data Analysis

- 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.

### Analytics and Protection

- 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.

https://docs.netskope.com/en/architecture-of-netskope-iot-security

The Accused '902 Products include each and every element of this limitation, either literally or under

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00070

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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. |
| 1[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 | 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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00071

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00072

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00073

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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.<br><br>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:<br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00074

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00075

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00076

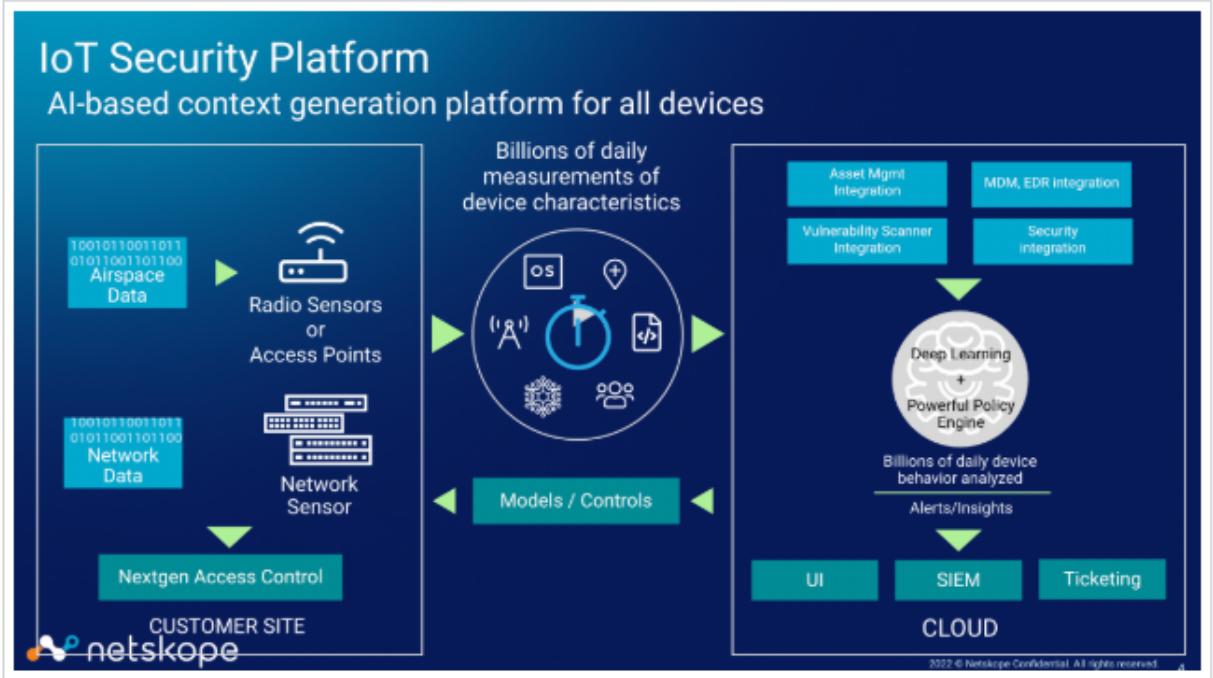
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Need for granular device context**<br>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to 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.<br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00077

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00078

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00079

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Analysis**<br>• On the cloud, various microservices analyze the metadata.<br>• 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.<br>**Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00080

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

Home > Device Intelligence > Protect Device Intelligence > Remediated Devices

## Remediated Devices

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.

You will see a list of devices that have triggered security policies. Each device entry includes the following information:

- **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 devi 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:
  - **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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00081

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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. |
| 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, | 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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00082

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00083

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00084

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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.<br><br>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:<br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00085

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00086

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00087

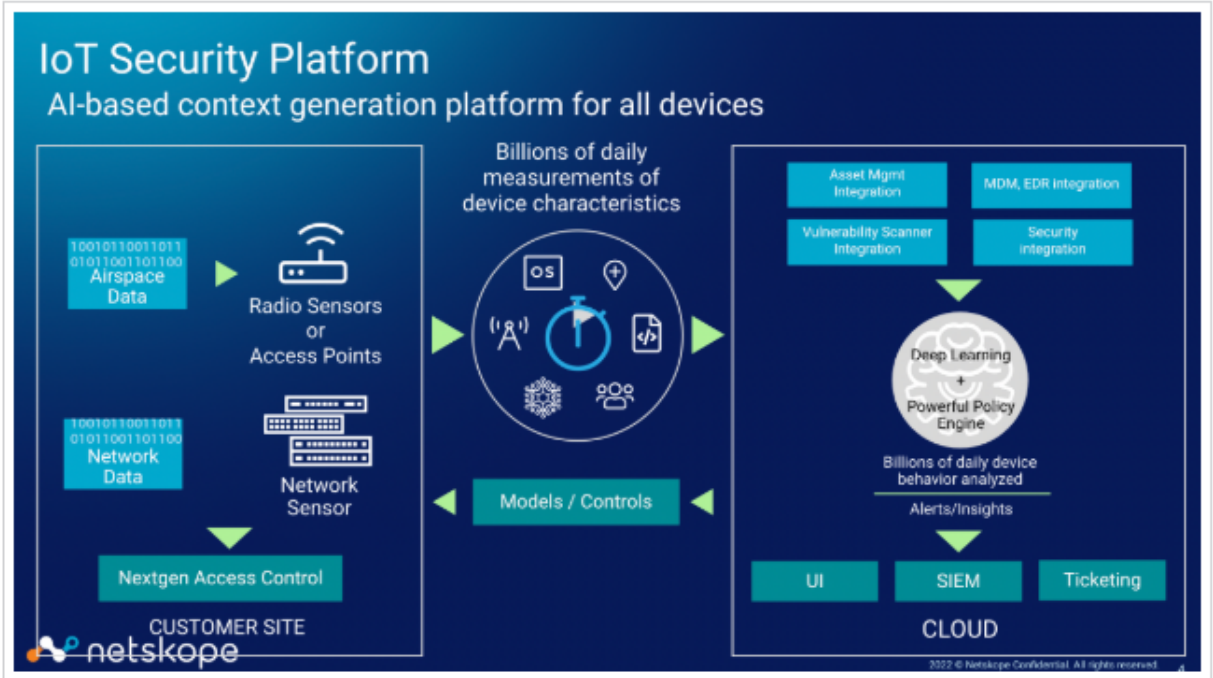
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Need for granular device context**<br>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to 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.<br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected- |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00088

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00089

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00090

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Analysis**<br>• On the cloud, various microservices analyze the metadata.<br>• 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.<br>**Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00091

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

Home > Device Intelligence > Protect Device Intelligence > Remediated Devices

## Remediated Devices

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.

You will see a list of devices that have triggered security policies. Each device entry includes the following information:

- **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 devi 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:
  - **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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00092

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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 requests 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. |
| 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. | 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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00093

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

# Netskope One Private Access

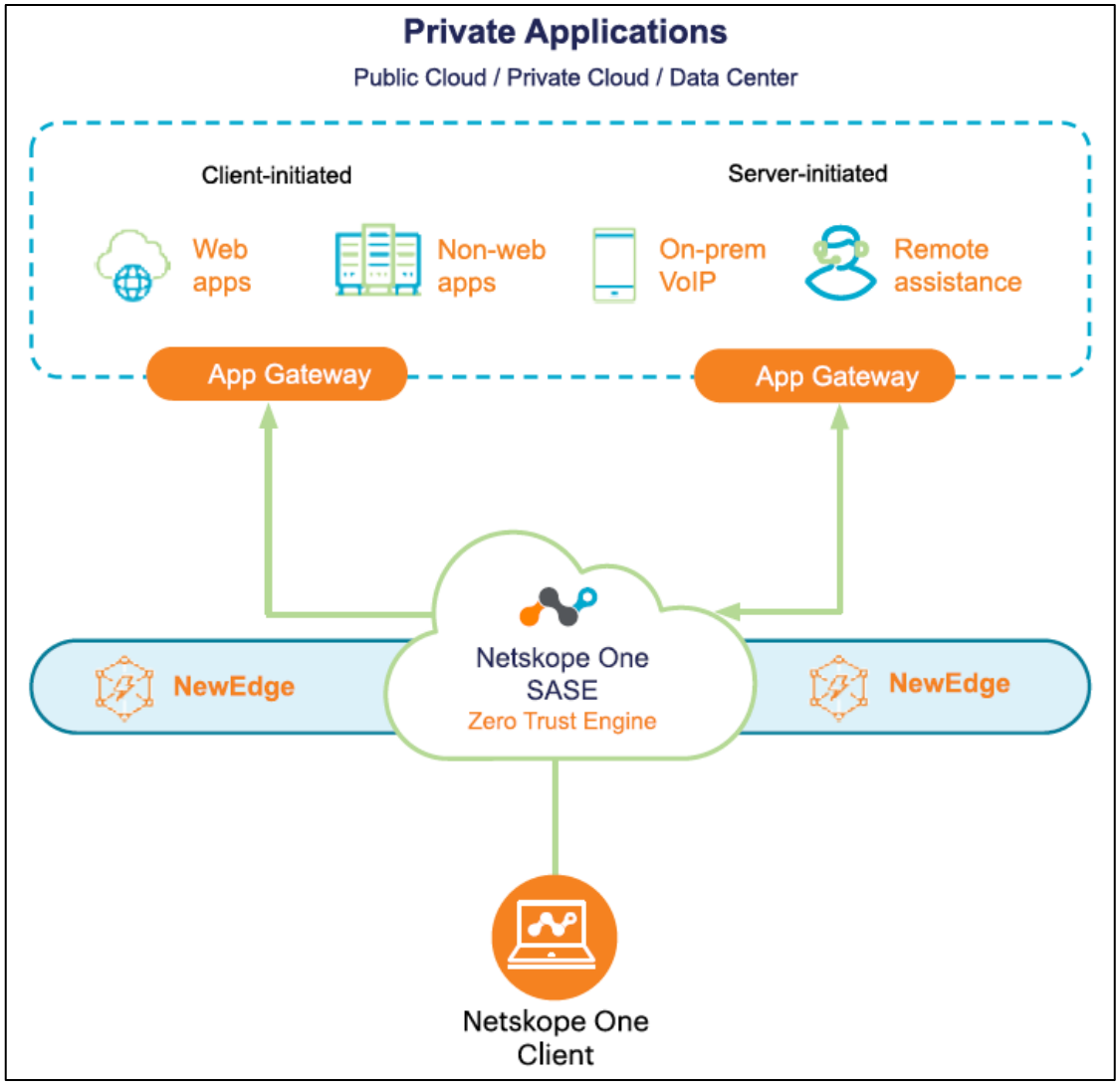
Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.

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:

- 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
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00094

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




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00095

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00096

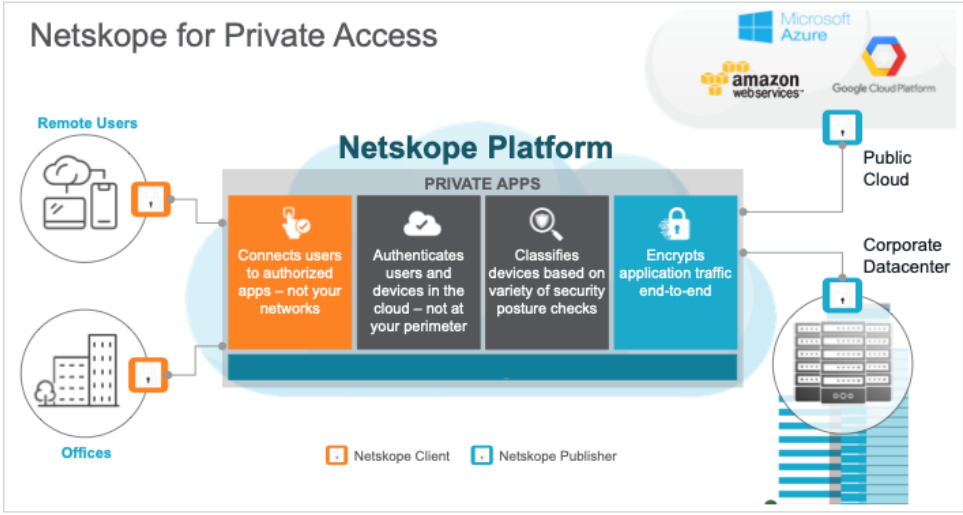
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|

### How It Works

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.

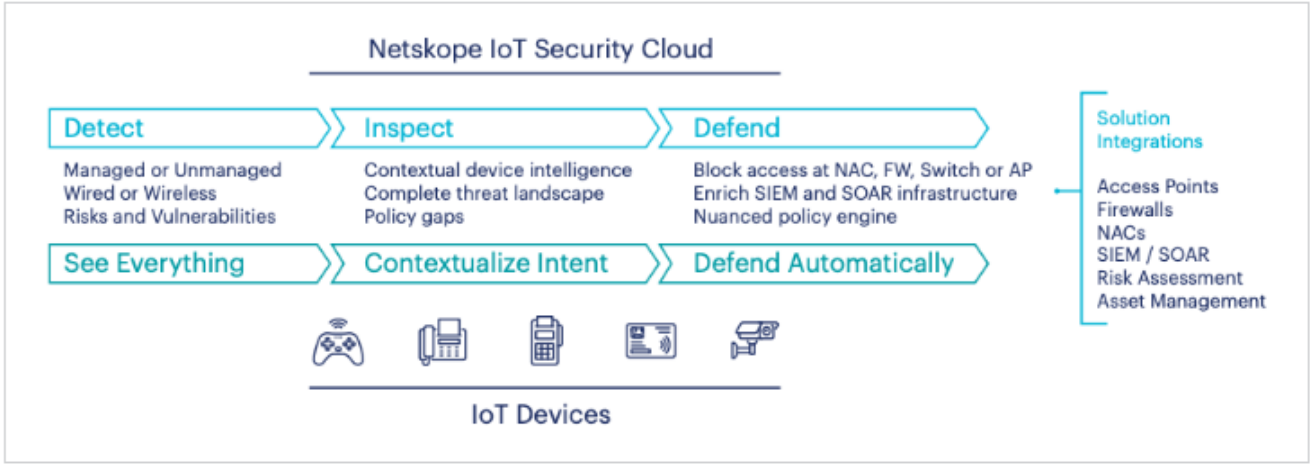
The Publisher, a lightweight connector deployed on-premises or in the cloud, establishes secure, encrypted communication between users and private applications without exposing applications to the internet. This architecture ensures that users gain access only to the specific applications they are authorized 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.

NPA is illustrated in this diagram:




https://docs.netskope.com/en/netskope-private-access

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00097

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



Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00098

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00099

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

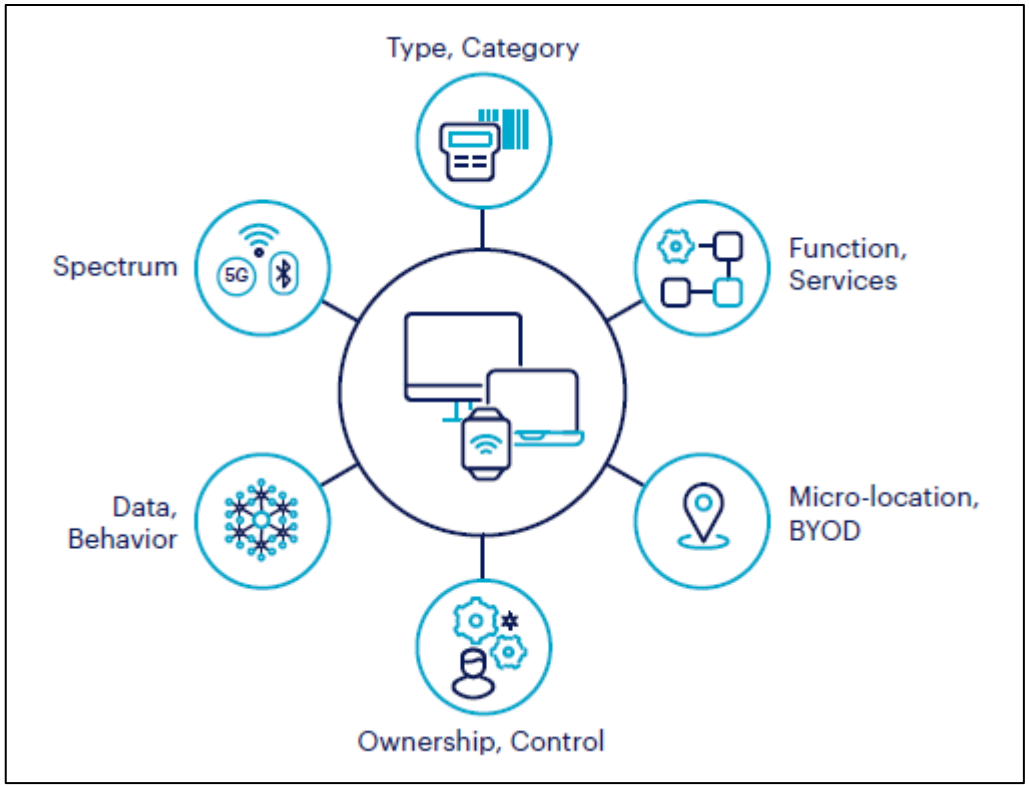
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00100

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE**<br><br>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®:<br><br>• Association of all the physical interfaces of the device and the spectrum of operation of each interface<br>• Type, Category of the device and related information<br>• OS, patches, services, and applications running on the device<br>• Functionality or the "purpose in life" of the device<br>• Micro location of the device, its mobility patterns, and times of visibility<br>• Ownership information of the device and its control information<br>• Users on the device<br>• Behavior based analysis of all the data transmissions across all protocols and spectrums<br>• Risk and vulnerability information, other information collected by other tools used |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00101

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The critical role of micro-segmentation**<br><br>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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00102

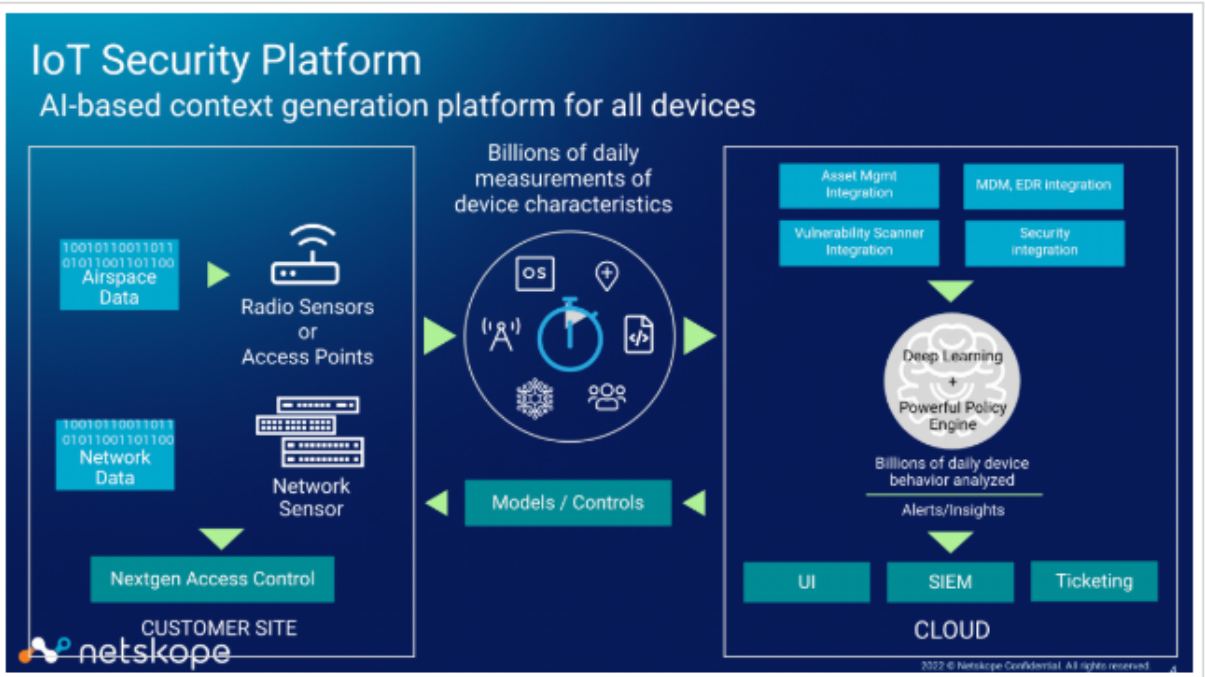
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00103

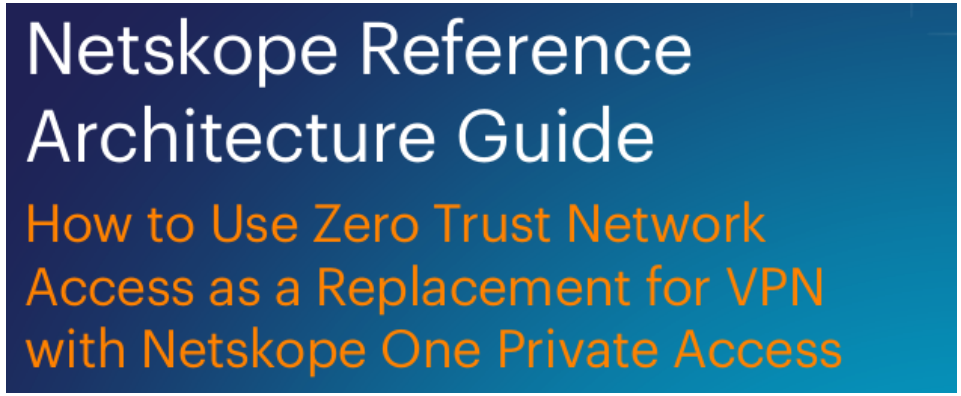
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|

## 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00104

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security<br>  |

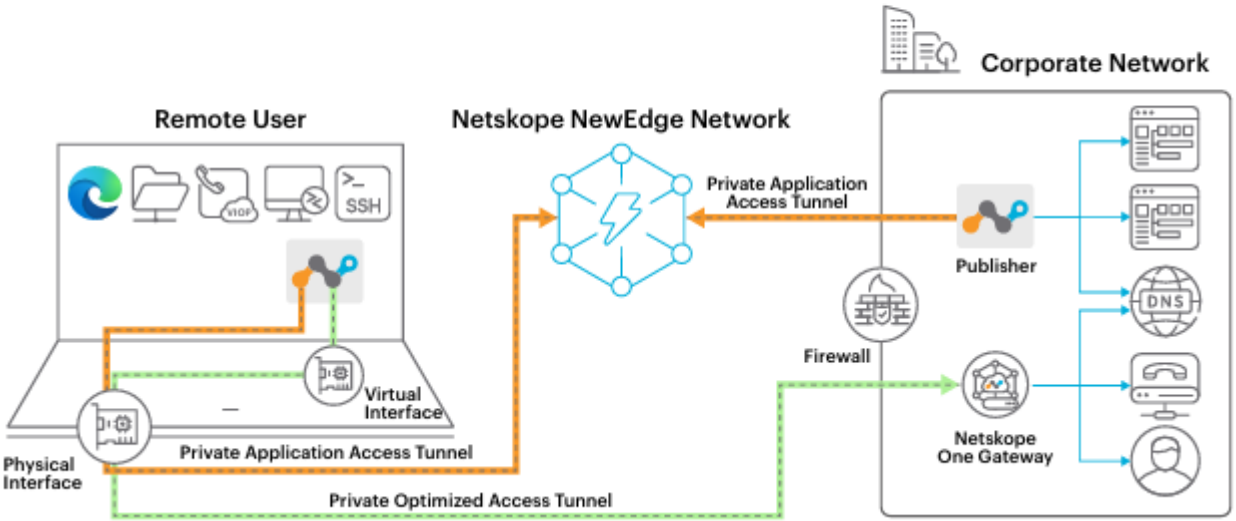
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00105

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Introducing Netskope One Private Access**<br><br>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.<br><br>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.<br><br>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. |

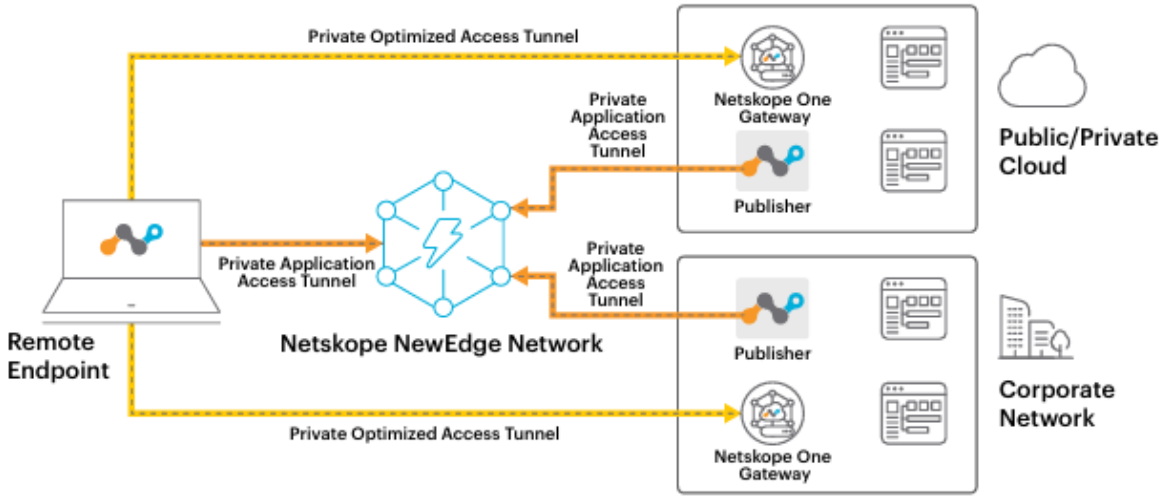
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00106

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Key Benefits**<br><br>**Enforces Zero Trust Principles**<br><br>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:<br><br>• Identity- and context-aware, least-privileged access to private applications hosted in public clouds or on-premises data centers.<br><br>• 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.<br><br>• 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.<br><br>• Reducing the opportunities for lateral movement of threats within the private networks and limiting the blast radius.<br><br>• Eliminating the dependence on public-facing VPNs or open inbound firewall ports for application access, securing networks from threats and DDoS attacks.<br><br>**Secures All Enterprise Applications**<br><br>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:<br><br>• 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.<br><br>• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all private applications. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00107

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Delivers a Phenomenal User Experience**<br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key benefits include:<br>• 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.<br>**Full Zero Trust Application Access: Netskope One Private Unified Access**<br>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.<br>  |

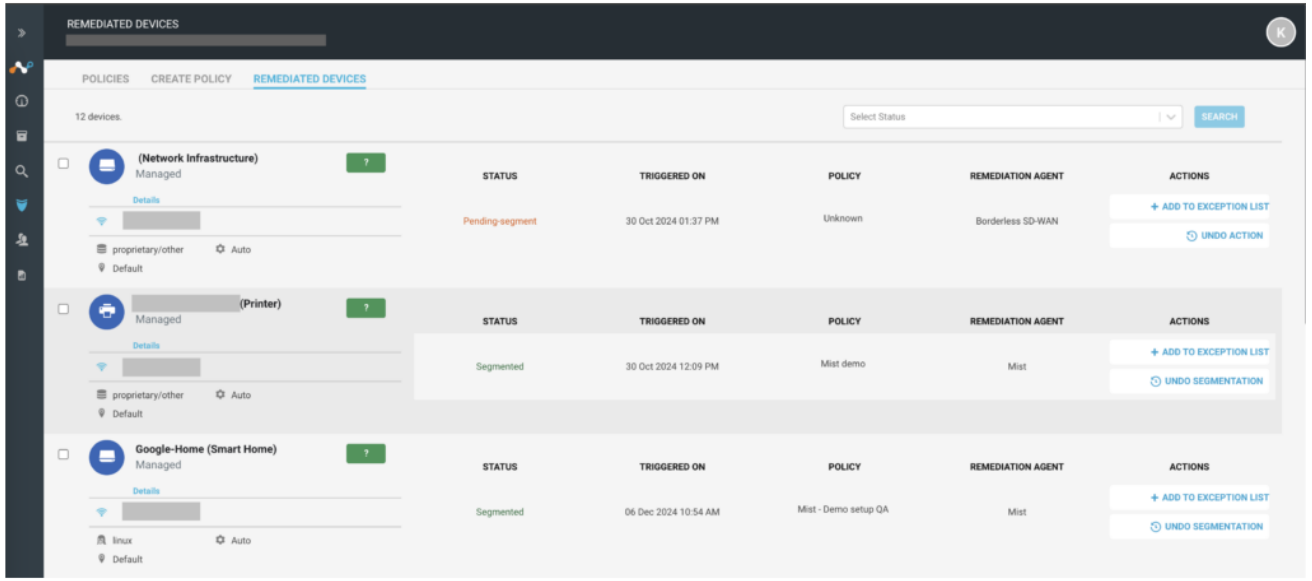
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00108

| 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.<br>  <br><br>2024-12-Reference-Architecture-Guide-for-ZTNA-Next-RA-709-3-1.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00109

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Remediated Devices**<br><br>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.<br><br>You will see a list of devices that have triggered security policies. Each device entry includes the following information:<br><br>• **Device Name:** The name or identifier of the device.<br>• **Device Type:** The type of device (e.g., computer, printer, IoT device).<br>• **Device Details:** By clicking on a **details** link, you will be navigated to a new page about the device details.<br>• **Status:** The current status of the remediation action (e.g., Pending Segment, Segmented).<br>• **Triggered On:** The date and time when the security policy was triggered.<br>• **Policy:** The name of the security policy that was triggered.<br>• **Remediation Agent:** The agent responsible for enforcing the remediation action.<br>• **Actions:** A set of actions that can be performed on the device, such as:<br>  • **Add to Exception List:** Excludes the device from future remediation actions.<br>  • **Undo Action:** Reverses the previous remediation action taken on the device.<br>  • **Undo Segmentation:** Reverses the previous segmentation action taken on the device. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00110

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://docs.netskope.com/en/remediated-devices<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00111

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 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. | In the Accused '902 Products, 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.<br><br>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).<br><br>**What is ZTNA?**<br><br>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. |

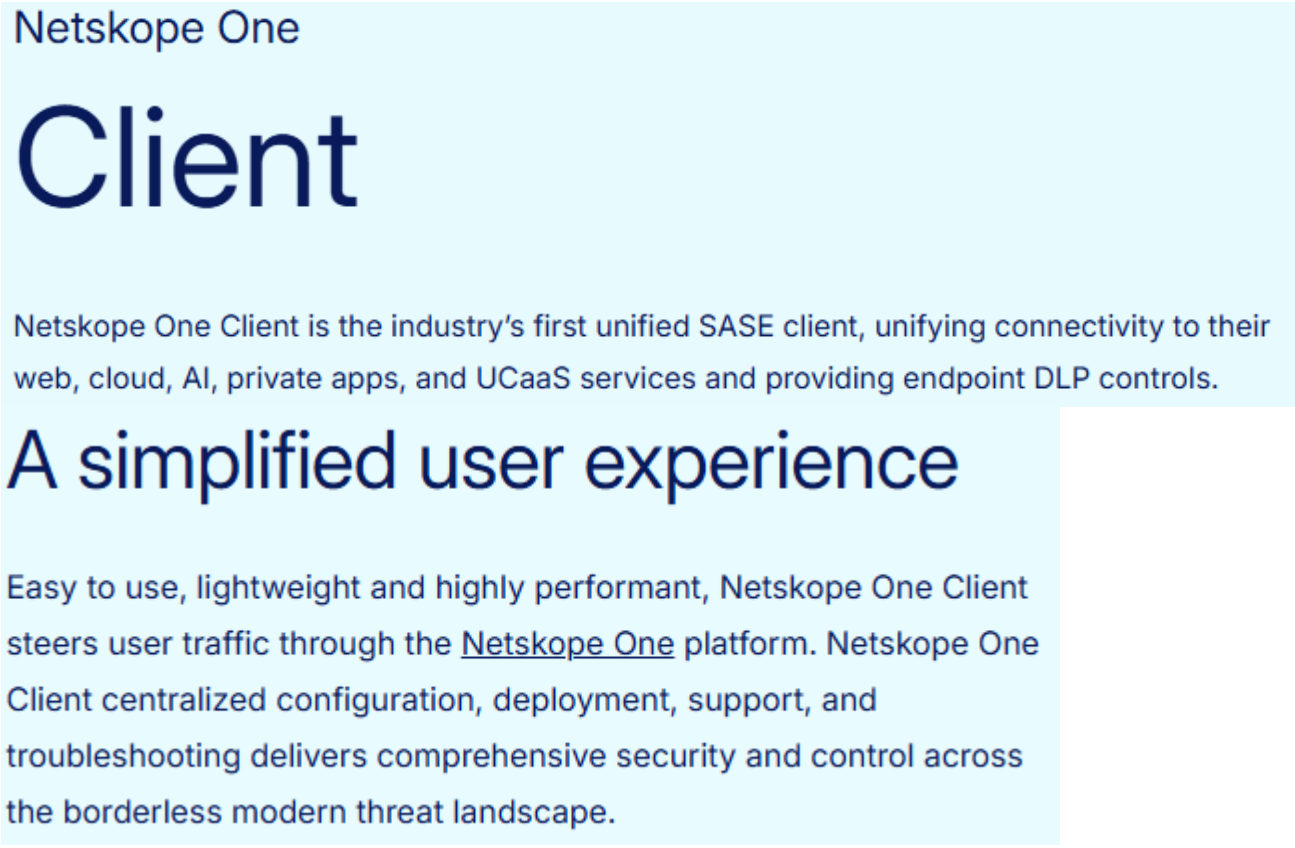
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00112

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Zero Trust Security Principles**<br>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.<br>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.<br>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.<br>https://www.netskope.com/security-defined/what-is-zero-trust-network-access |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00113

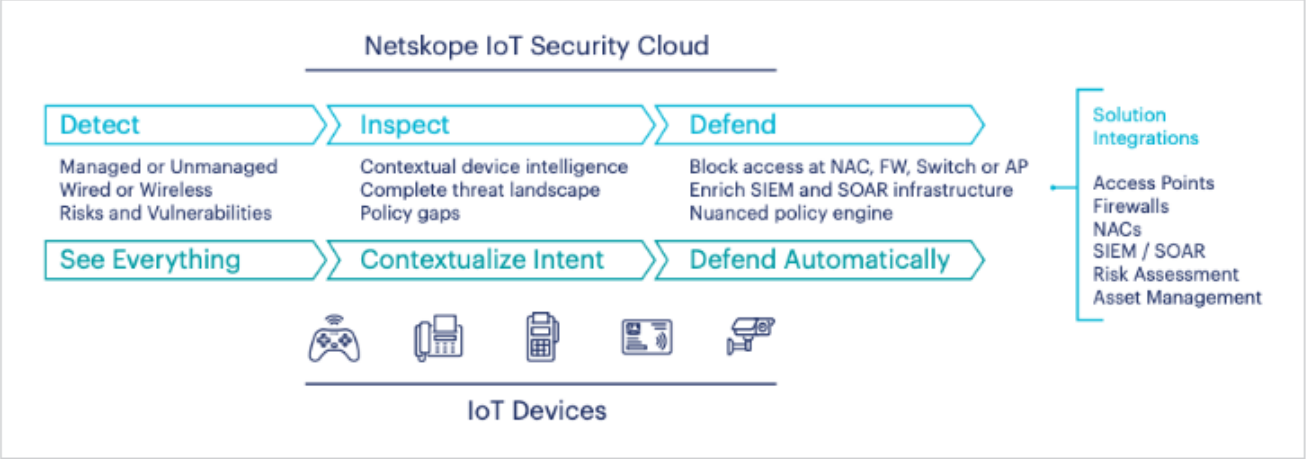
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00114

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://www.netskope.com/netskope-one/client |
| 3. The method of claim 1, wherein the unsecure network element is an Internet of Things (IoT) device. | The Accused '902 Products include wherein the unsecure network element is an Internet of Things (IoT) device.<br><br>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 |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00115

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




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00116

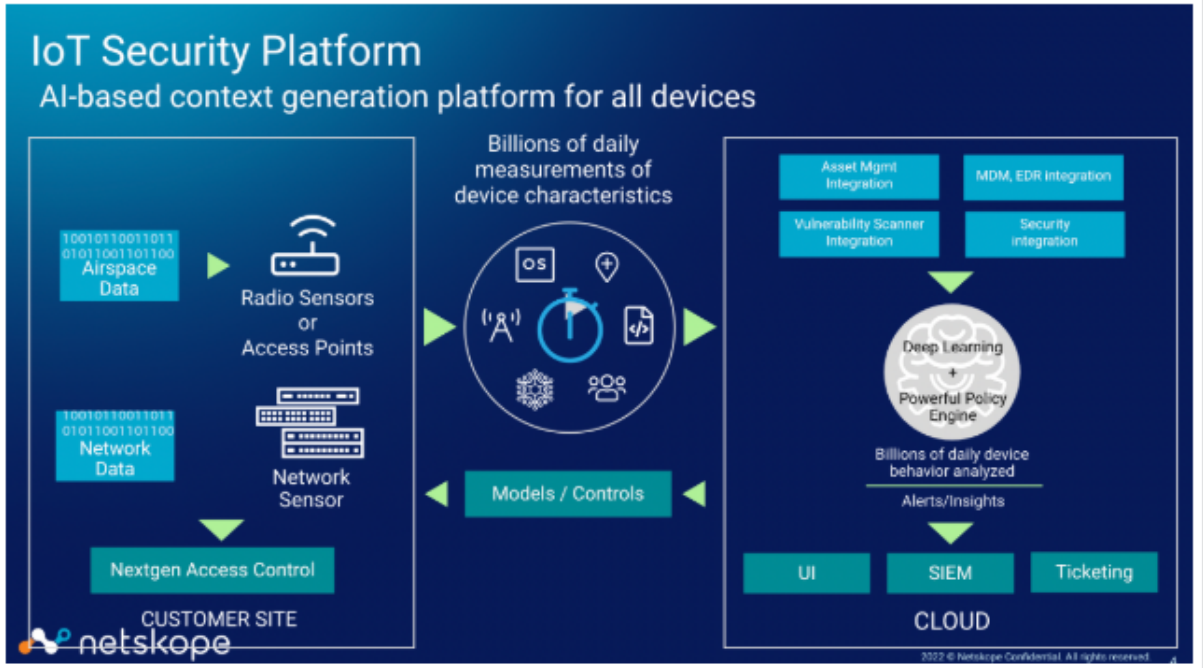
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00117

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

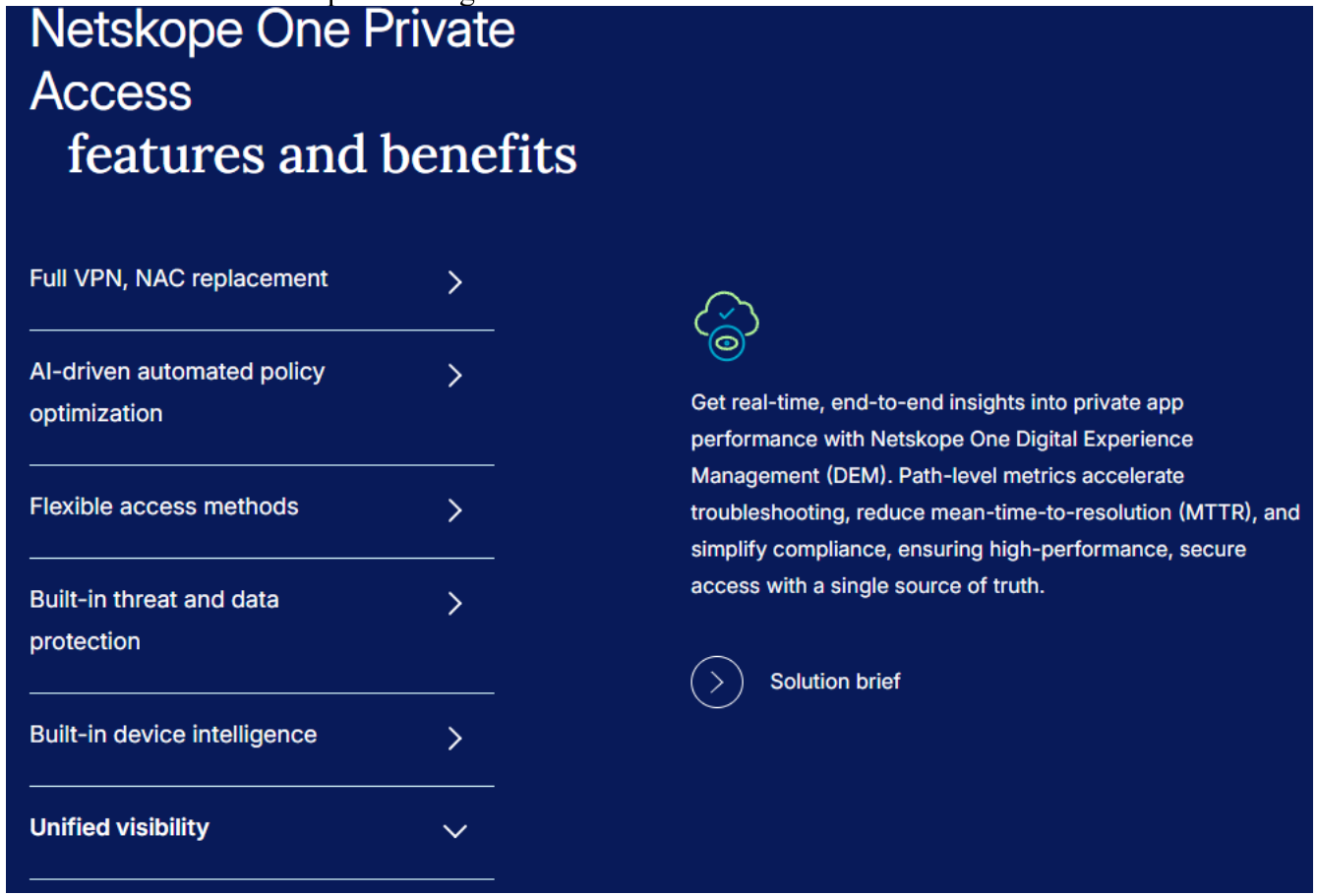
## Architecture of Device Intelligence

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.



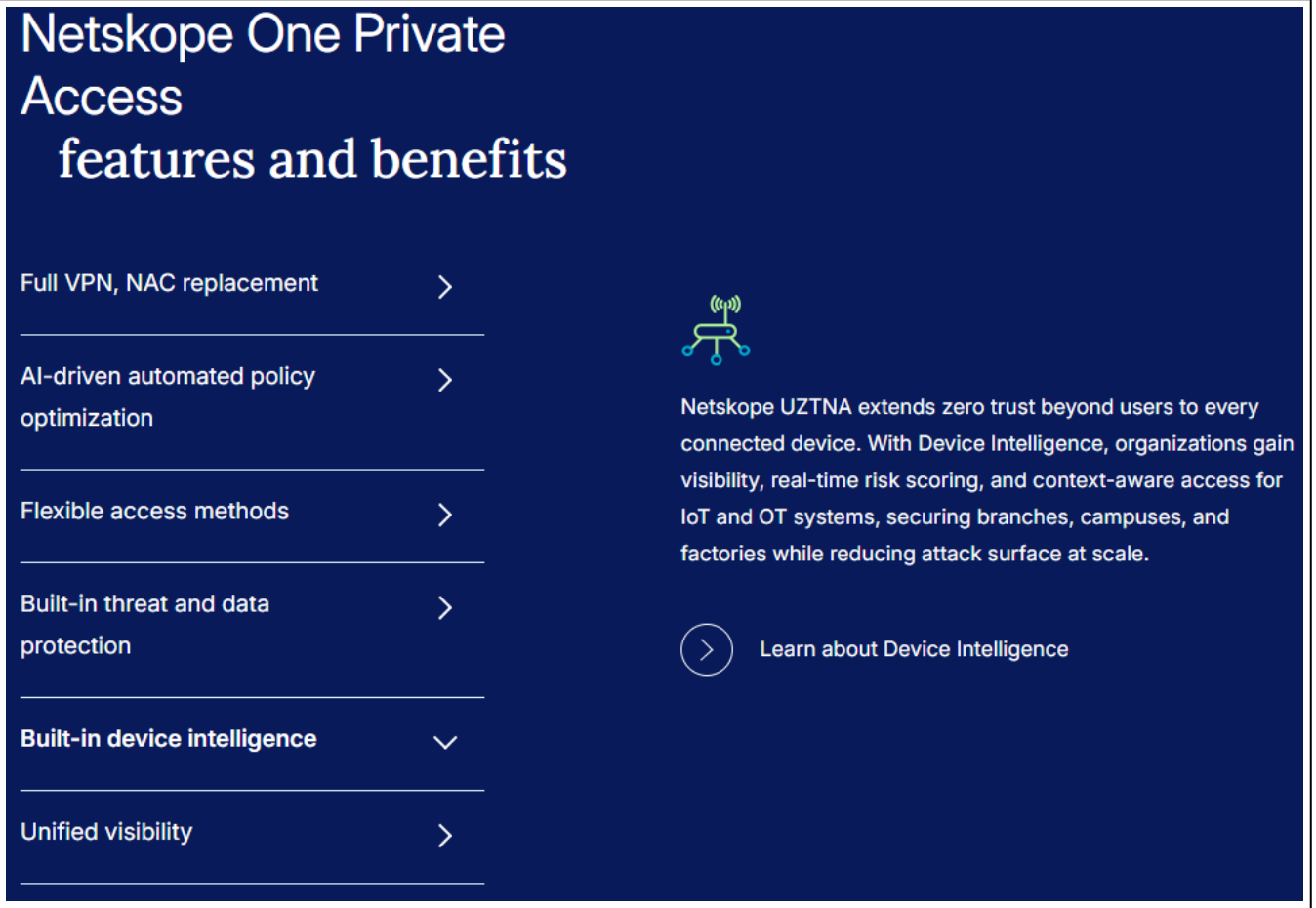

https://docs.netskope.com/en/architecture-of-netskope-iot-security

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00118

| 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. | The Accused '902 Products include wherein administration of the processing device and the known network is controlled by a common administration entity.<br><br>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.<br>  |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00119

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




https://www.netskope.com/products/private-access

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00120

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

# Netskope One Private Access

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.

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:

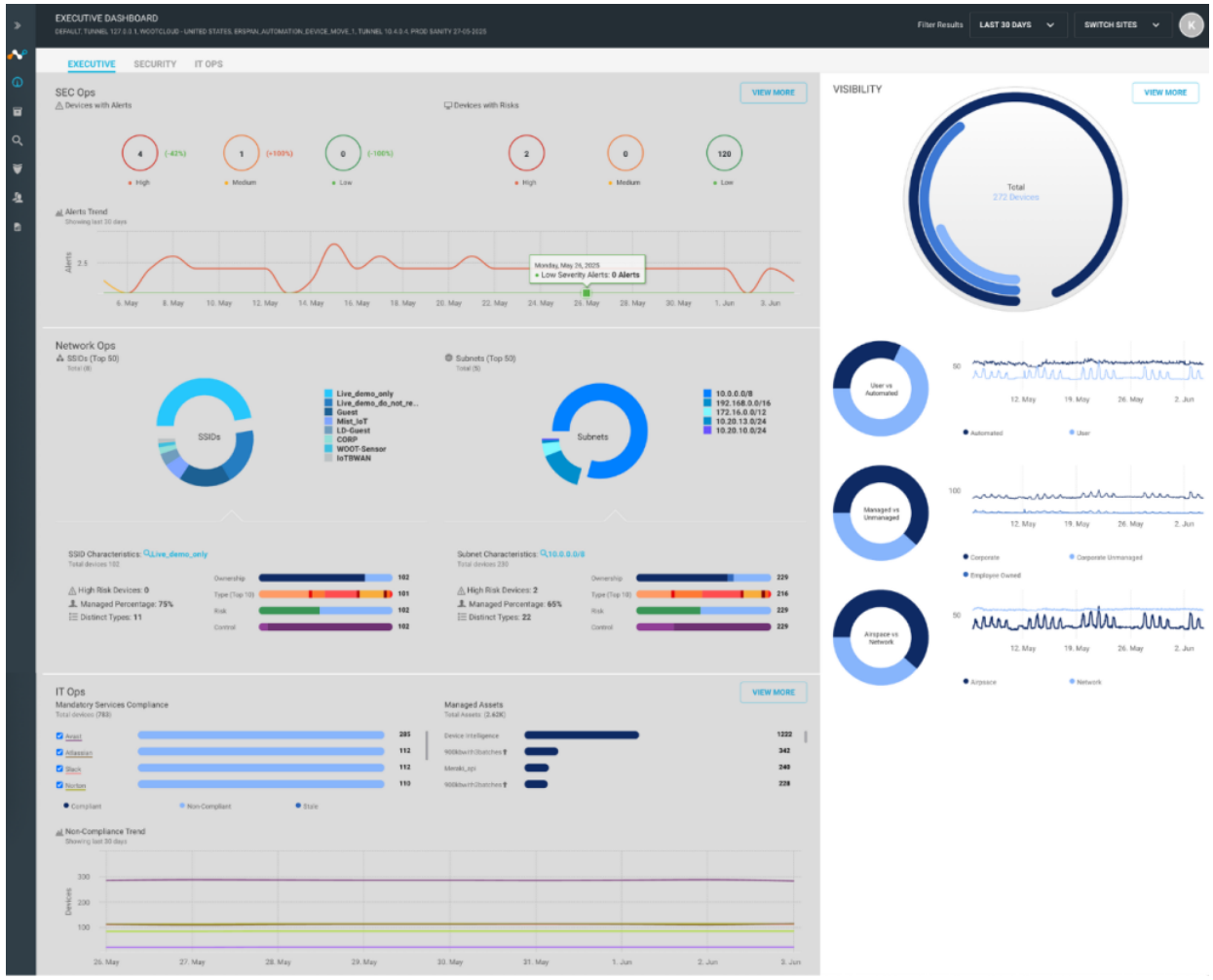
- Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00121

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Home > Device Intelligence > Executive Dashboard<br><br>**Executive Dashboard**<br><br>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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00122

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://docs.netskope.com/en/executive-dashboard-in-netskope-iot-security |
| 5. The method of claim 1, the method further comprising: | 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 |



Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00123

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 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. | network via another remote network.<br><br>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.<br><br>**What is ZTNA?**<br><br>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.<br><br>**Zero Trust Security Principles**<br><br>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.<br><br>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.<br><br>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.<br><br>https://www.netskope.com/security-defined/what-is-zero-trust-network-access |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00124

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00125

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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.<br><br>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:<br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br><br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00126

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00127

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00128

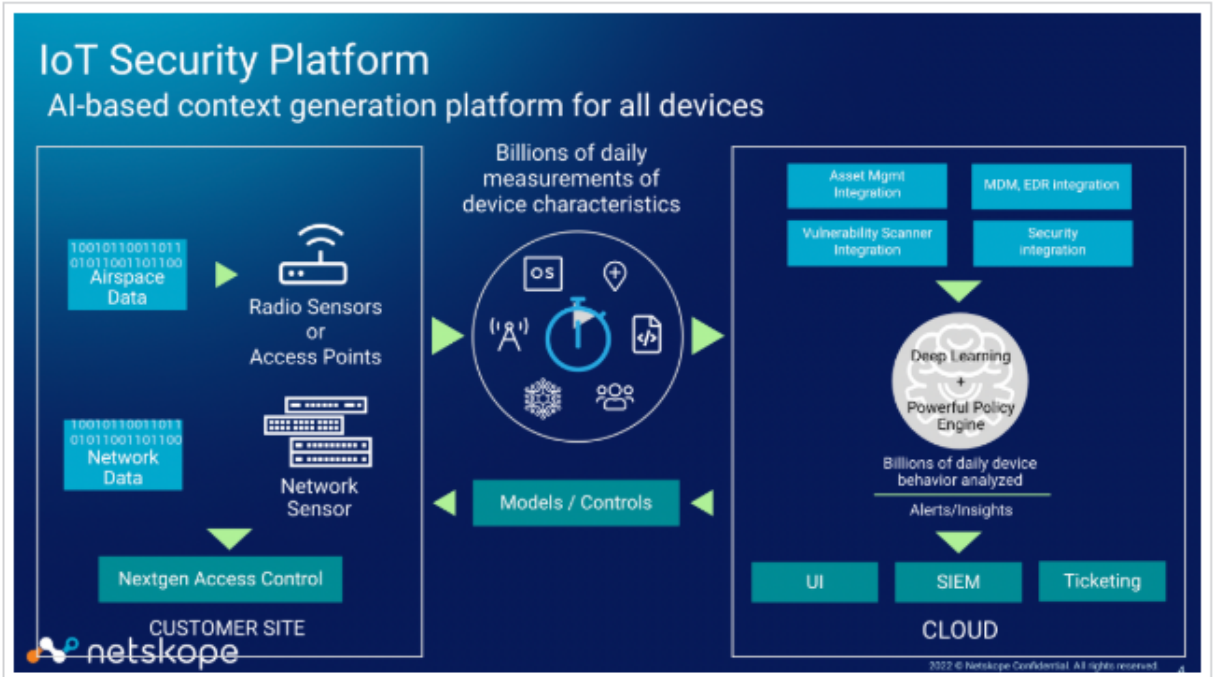
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Need for granular device context**<br>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to 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.<br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00129

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00130

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00131

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Analysis**<br>• On the cloud, various microservices analyze the metadata.<br>• 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.<br>**Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00132

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

Home > Device Intelligence > Protect Device Intelligence > Remediated Devices

## Remediated Devices

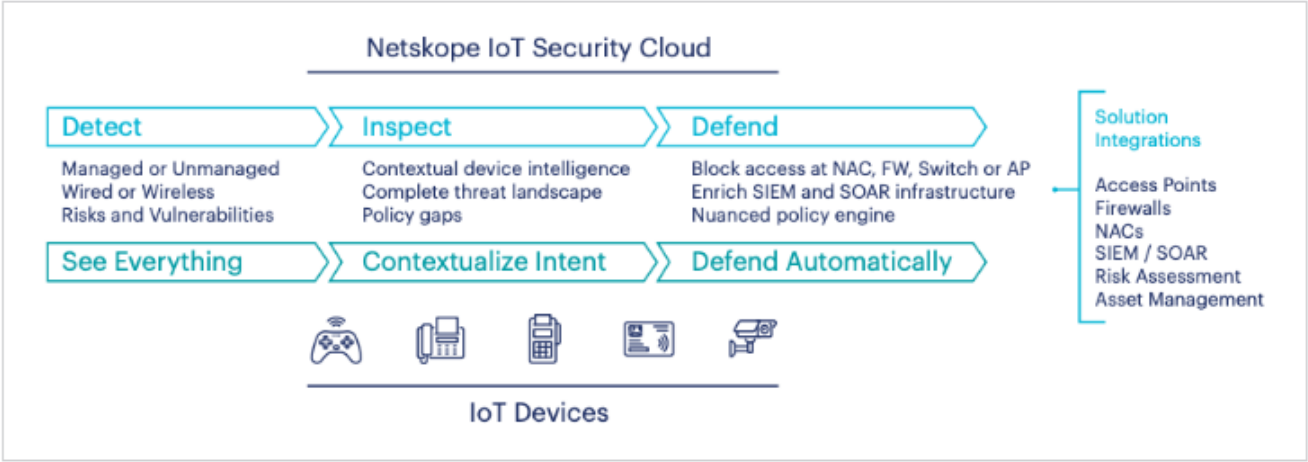
Navigate to **Policies** menu, in the **Remediated Devices** tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.

You will see a list of devices that have triggered security policies. Each device entry includes the following information:

- **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 devi 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:
  - **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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00133

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 6. The method of claim 1, 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. | 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.<br><br>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.<br><br>  |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00134

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br><br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00135

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

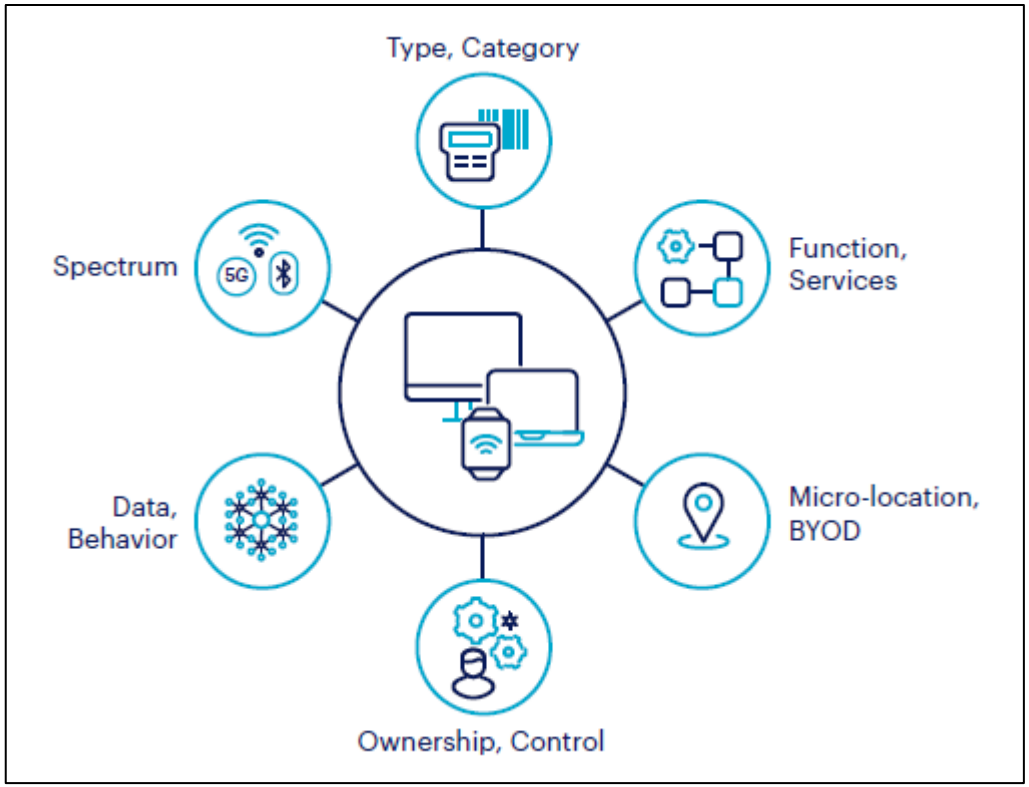
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00136

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE**<br><br>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®:<br>• Association of all the physical interfaces of the device and the spectrum of operation of each interface<br>• Type, Category of the device and related information<br>• OS, patches, services, and applications running on the device<br>• Functionality or the "purpose in life" of the device<br>• Micro location of the device, its mobility patterns, and times of visibility<br>• Ownership information of the device and its control information<br>• Users on the device<br>• Behavior based analysis of all the data transmissions across all protocols and spectrums<br>• Risk and vulnerability information, other information collected by other tools used |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00137

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The critical role of micro-segmentation**<br><br>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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00138

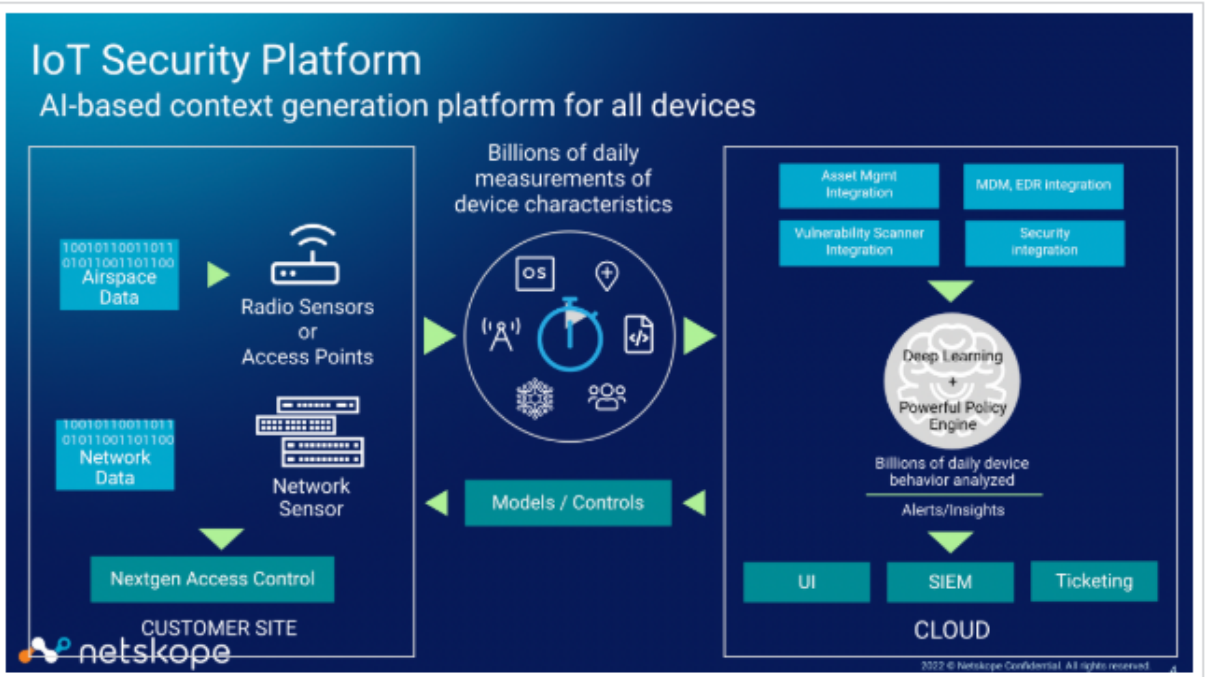
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00139

| 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.





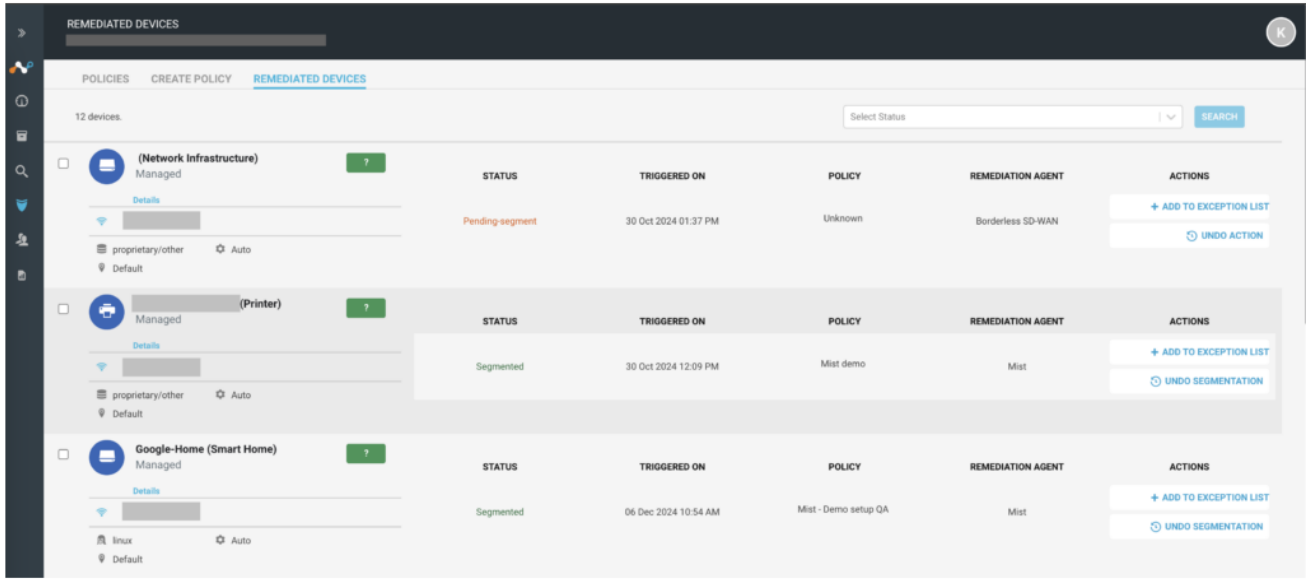

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00140

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

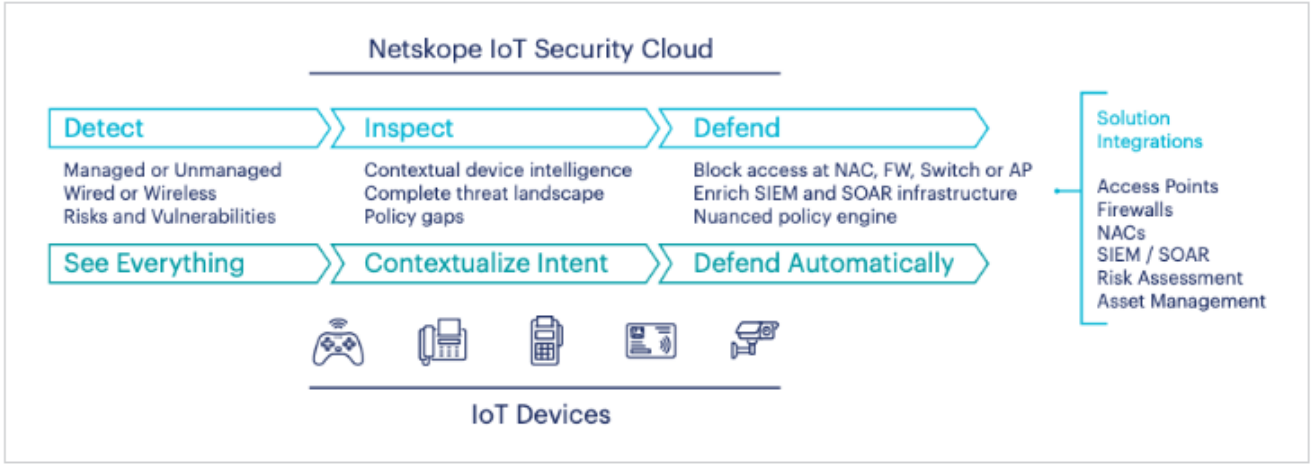
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00141

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Remediated Devices**<br><br>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.<br><br>You will see a list of devices that have triggered security policies. Each device entry includes the following information:<br><br>• **Device Name:** The name or identifier of the device.<br>• **Device Type:** The type of device (e.g., computer, printer, IoT device).<br>• **Device Details:** By clicking on a **details** link, you will be navigated to a new page about the device details.<br>• **Status:** The current status of the remediation action (e.g., Pending Segment, Segmented).<br>• **Triggered On:** The date and time when the security policy was triggered.<br>• **Policy:** The name of the security policy that was triggered.<br>• **Remediation Agent:** The agent responsible for enforcing the remediation action.<br>• **Actions:** A set of actions that can be performed on the device, such as:<br>  • **Add to Exception List:** Excludes the device from future remediation actions.<br>  • **Undo Action:** Reverses the previous remediation action taken on the device.<br>  • **Undo Segmentation:** Reverses the previous segmentation action taken on the device. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00142

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://docs.netskope.com/en/remediated-devices |
| 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. | 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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00143

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



Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00144

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00145

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

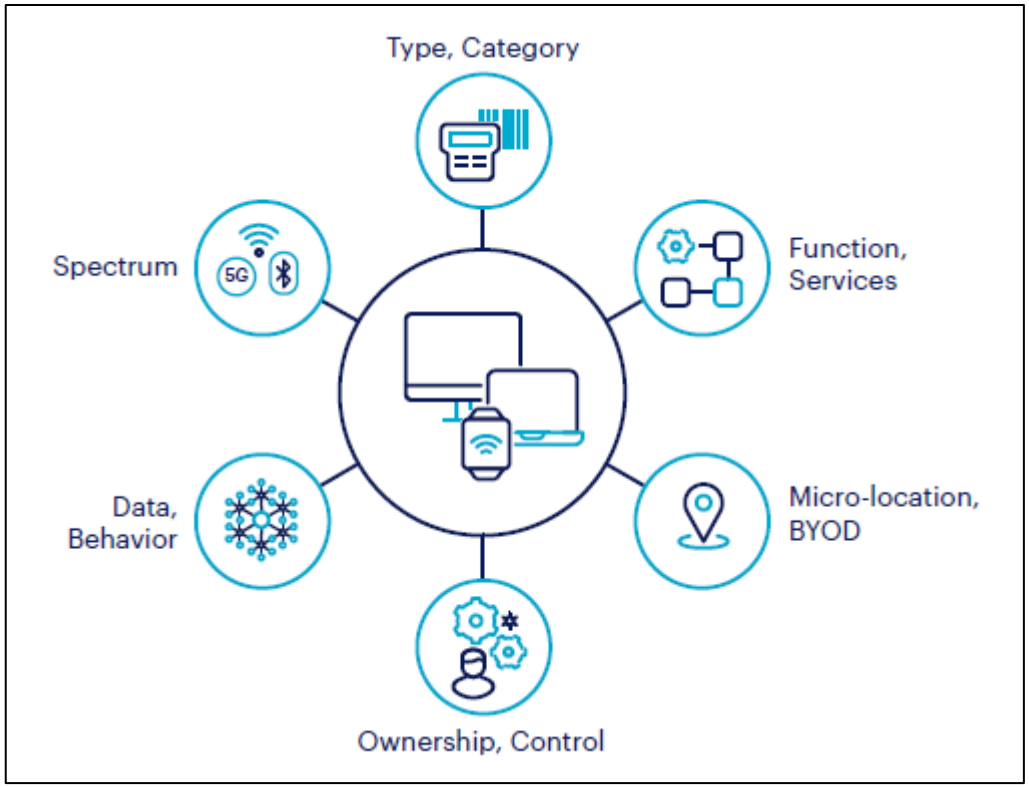
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00146

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE**<br><br>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®:<br>• Association of all the physical interfaces of the device and the spectrum of operation of each interface<br>• Type, Category of the device and related information<br>• OS, patches, services, and applications running on the device<br>• Functionality or the "purpose in life" of the device<br>• Micro location of the device, its mobility patterns, and times of visibility<br>• Ownership information of the device and its control information<br>• Users on the device<br>• Behavior based analysis of all the data transmissions across all protocols and spectrums<br>• Risk and vulnerability information, other information collected by other tools used |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00147

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The critical role of micro-segmentation**<br><br>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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00148

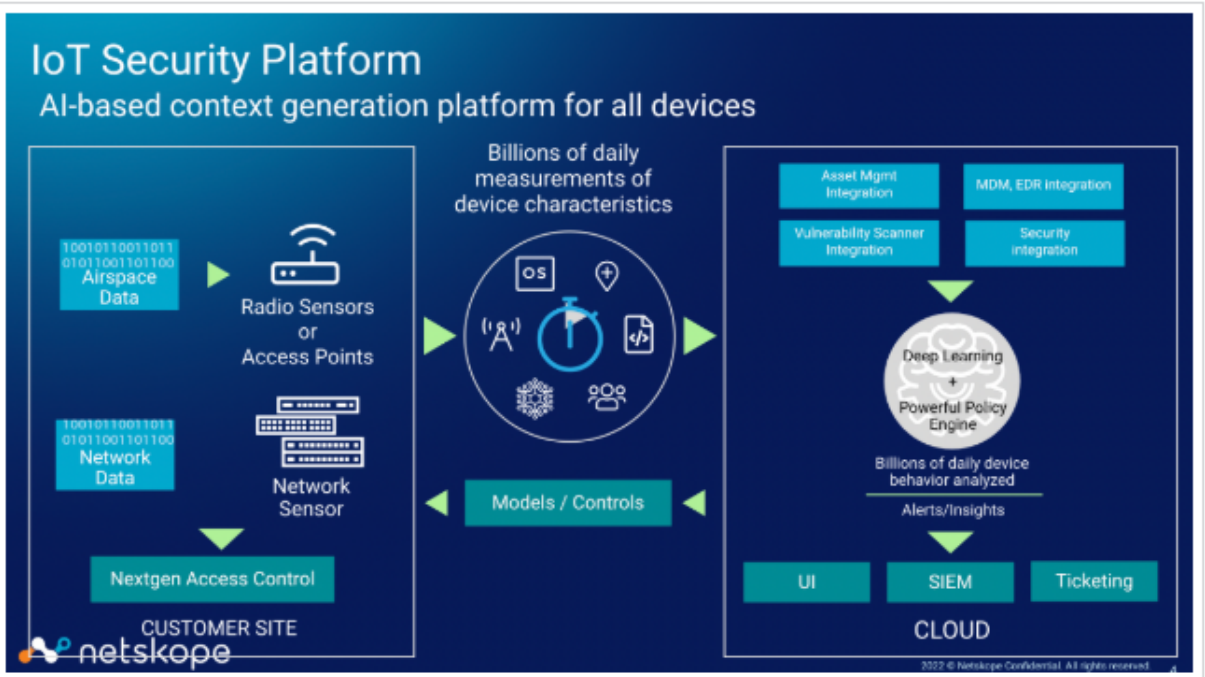
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00149

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00150

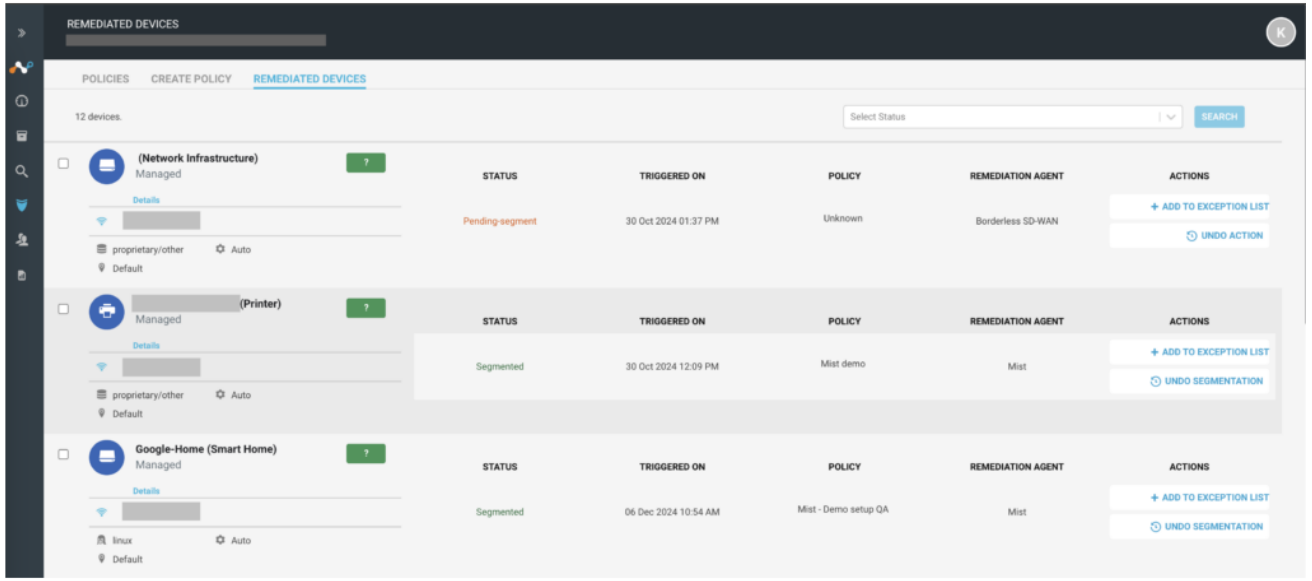
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Analytics and Protection**<br>• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00151

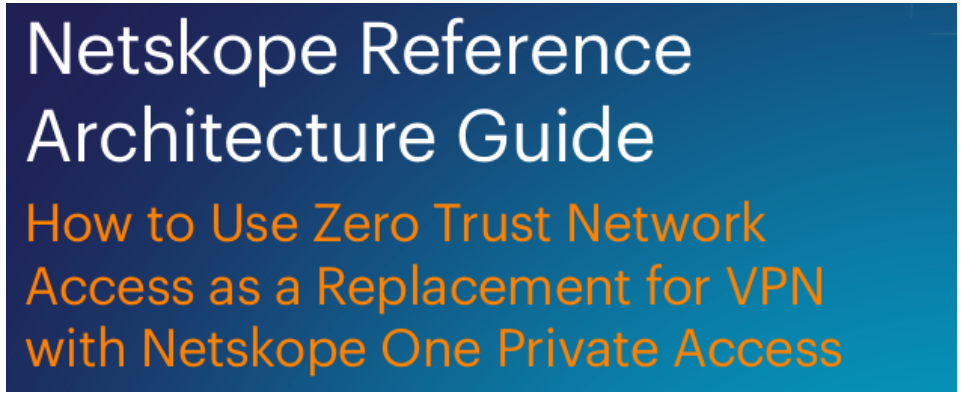
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Remediated Devices**<br><br>Navigate to **Policies** menu, in the **Remediated Devices** tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.<br><br>You will see a list of devices that have triggered security policies. Each device entry includes the following information:<br><br>• **Device Name:** The name or identifier of the device.<br>• **Device Type:** The type of device (e.g., computer, printer, IoT device).<br>• **Device Details:** By clicking on a **details** link, you will be navigated to a new page about the device details.<br>• **Status:** The current status of the remediation action (e.g., Pending Segment, Segmented).<br>• **Triggered On:** The date and time when the security policy was triggered.<br>• **Policy:** The name of the security policy that was triggered.<br>• **Remediation Agent:** The agent responsible for enforcing the remediation action.<br>• **Actions:** A set of actions that can be performed on the device, such as:<br>  • **Add to Exception List:** Excludes the device from future remediation actions.<br>  • **Undo Action:** Reverses the previous remediation action taken on the device.<br>  • **Undo Segmentation:** Reverses the previous segmentation action taken on the device. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00152

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




https://docs.netskope.com/en/remediated-devices



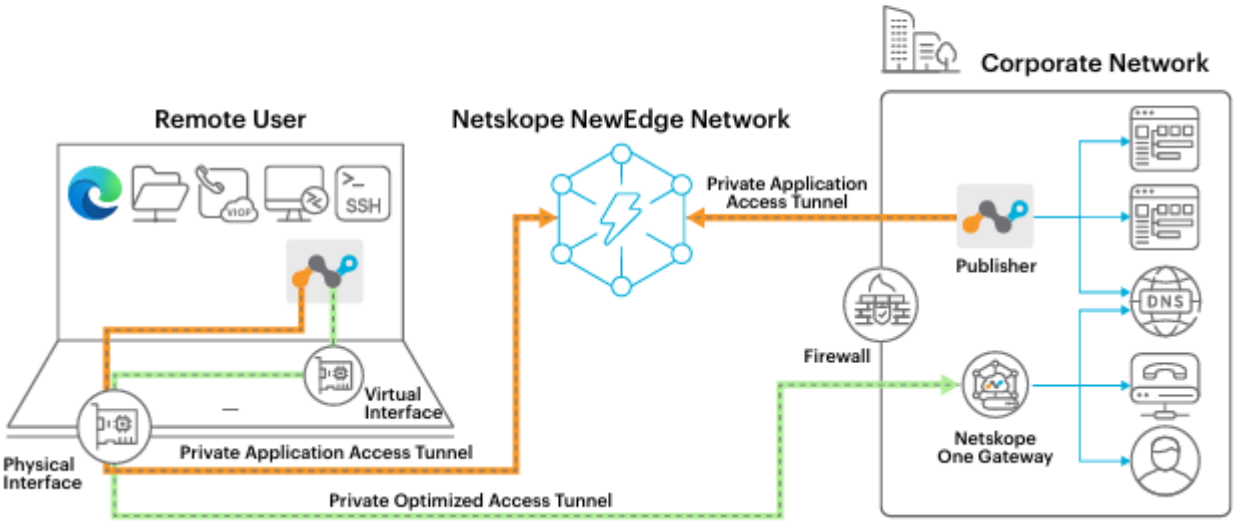

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00153

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Introducing Netskope One Private Access**<br><br>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.<br><br>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.<br><br>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. |

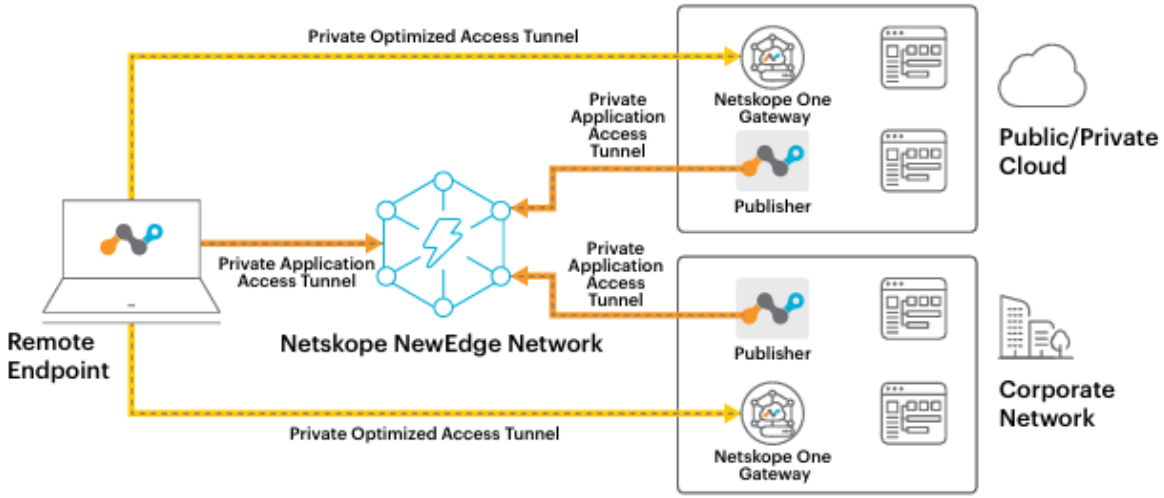
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00154

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Key Benefits**<br><br>**Enforces Zero Trust Principles**<br><br>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:<br><br>• Identity- and context-aware, least-privileged access to private applications hosted in public clouds or on-premises data centers.<br><br>• 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.<br><br>• 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.<br><br>• Reducing the opportunities for lateral movement of threats within the private networks and limiting the blast radius.<br><br>• Eliminating the dependence on public-facing VPNs or open inbound firewall ports for application access, securing networks from threats and DDoS attacks.<br><br>**Secures All Enterprise Applications**<br><br>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:<br><br>• 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.<br><br>• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all private applications. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00155

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Delivers a Phenomenal User Experience**<br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key benefits include:<br>• 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.<br>**Full Zero Trust Application Access: Netskope One Private Unified Access**<br>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.<br>  |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00156

| 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.<br>  <br><br>2024-12-Reference-Architecture-Guide-for-ZTNA-Next-RA-709-3-1.pdf<br><br>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 |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00157

| 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. |
| 8. The method of claim 1, the method further comprising:<br>using, by the processing device, a network connection between the processing device and the known network; and<br>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. | 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.<br><br>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.<br><br>**What is ZTNA?**<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00158

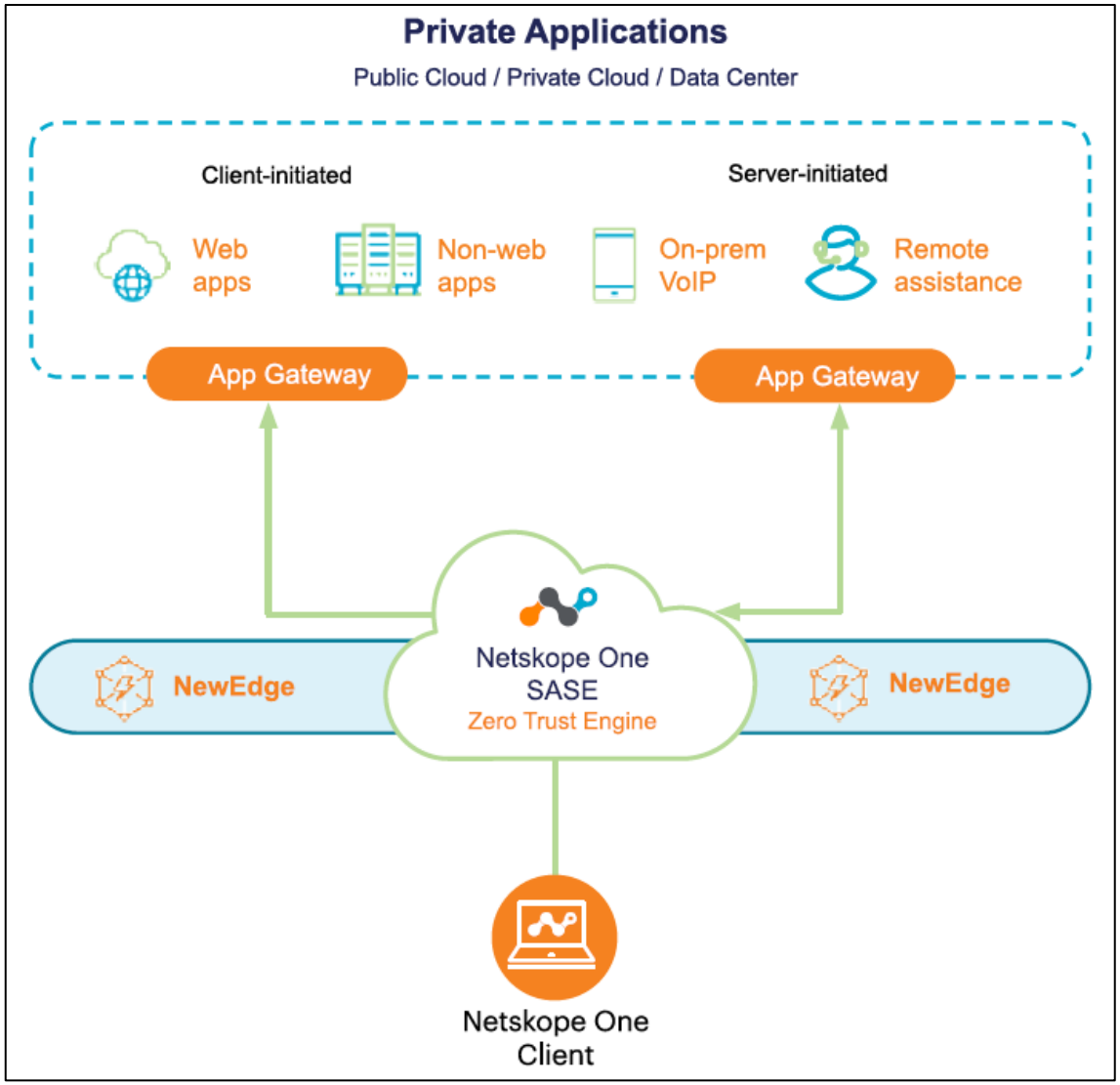
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Zero Trust Security Principles**<br>ZTNA creates a new security framework, based on the zero trust security model, for connecting users with enterprise resources. Private applications connect to the ZTNA broker via application 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.<br>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.<br>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.<br>https://www.netskope.com/security-defined/what-is-zero-trust-network-access<br>**Netskope One Private Access**<br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00159

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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:<br><br>• 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<br><br>• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00160

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




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00161

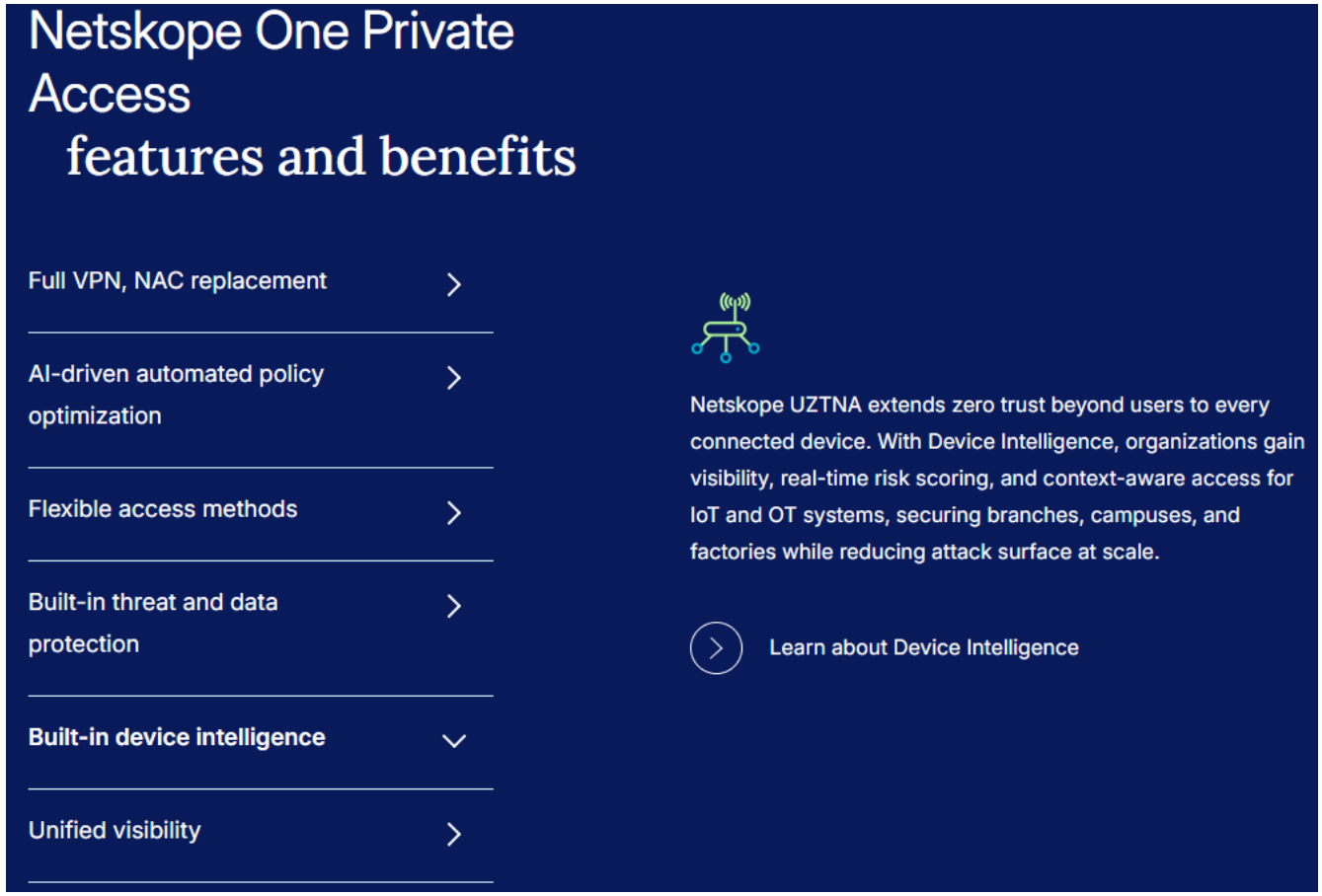
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00162

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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 (*e.g.*, 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00163

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




https://www.netskope.com/products/private-access

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00164

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br><br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00165

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00166

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

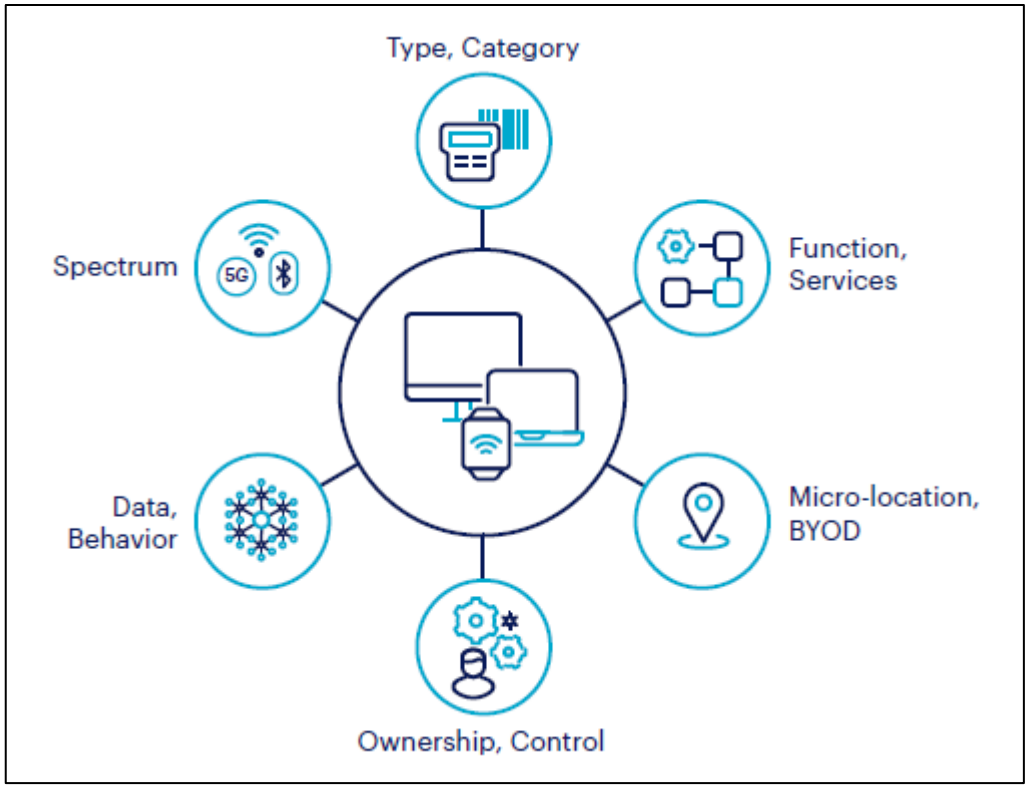
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00167

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE**<br><br>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®:<br>• Association of all the physical interfaces of the device and the spectrum of operation of each interface<br>• Type, Category of the device and related information<br>• OS, patches, services, and applications running on the device<br>• Functionality or the "purpose in life" of the device<br>• Micro location of the device, its mobility patterns, and times of visibility<br>• Ownership information of the device and its control information<br>• Users on the device<br>• Behavior based analysis of all the data transmissions across all protocols and spectrums<br>• Risk and vulnerability information, other information collected by other tools used |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00168

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The critical role of micro-segmentation**<br><br>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.<br><br>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.<br><br>**Employing AI/ML for intelligent, dynamic controls**<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00169

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00170

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

Home > Device Intelligence > Investigate Device Intelligence > Investigate Devices

## Investigate Devices

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.

> **Note**
>
> You can also sort the device summary in combination with the total of all devices, managed, unmanaged, new, automated, and user-controlled devices.

### Investigate Devices based on Spectrum

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.

https://docs.netskope.com/en/investigate-devices

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00171

| 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.

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.

https://docs.netskope.com/en/investigate-risks

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00172

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

Home > Device Intelligence > Protect Device Intelligence > Remediated Devices

## Remediated Devices

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.

You will see a list of devices that have triggered security policies. Each device entry includes the following information:

- **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 devi 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:
  - **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.

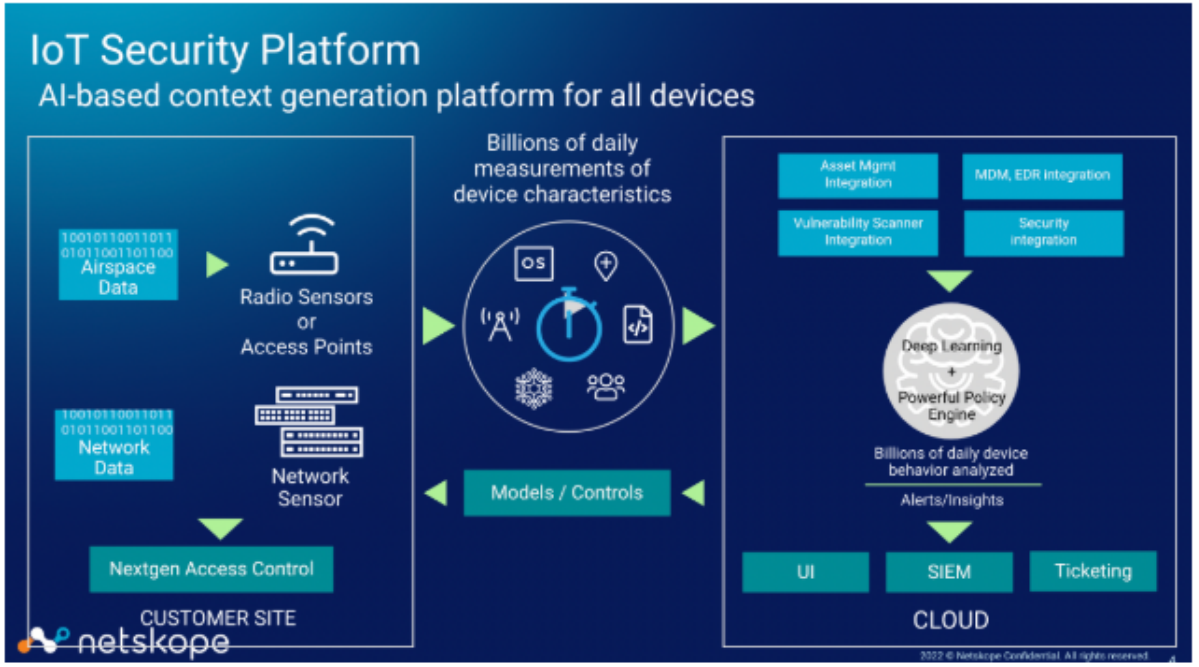
https://docs.netskope.com/en/remediated-devices

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00173

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00174

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00175

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Transfer**<br>• The network sensors do a deep inspection of the traffic, apply signatures and run algorithms to extract meta information.<br>• Network sensors send this meta information via encrypted channel to the cloud to analyze the traffic metadata and events in the environment.<br>**Data Analysis**<br>• On the cloud, various microservices analyze the metadata.<br>• 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.<br>**Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security<br>The Accused '902 Products include each and every element of this limitation, either literally or under |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00176

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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. |
| 11[pre]: A system comprising:<br>one or more processing resources;<br>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: | 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.<br><br>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). |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00177

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Netskope Advances Netskope One Platform With AI-Driven Proactive DEM Solution, Key Security Innovations<br><br>***Network Visibility and Control, Advanced Evasive Threat Detection, Context-Aware Zero Trust Integrations Accelerate Cloud Networking and Security Operations***<br><br>**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.<br><br>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.<br><br>https://www.netskope.com/press-releases/netskope-advances-netskope-one-platform-with-ai-driven-proactive-dem-solution-key-security-innovations |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00178

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | <br>https://www.netskope.com/resources/data-sheets/netskope-newedge-data-sheet |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00179

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | <br>**Cloud security without sacrificing performance**<br>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.<br>**Future-proof, SASE-ready architecture**<br>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.<br>https://www.netskope.com/wp-content/uploads/2022/12/2023-04-NewEdge-DS-333-7-1.pdf |
| 11[a]: receive a request to | The Accused '902 Products receive a request to access a known network from a known access device |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00180

| 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; | 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.<br><br>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). *See also* 1[a].<br><br>Netskope Advances Netskope One Platform With AI-Driven Proactive DEM Solution, Key Security Innovations<br><br>***Network Visibility and Control, Advanced Evasive Threat Detection, Context-Aware Zero Trust Integrations Accelerate Cloud Networking and Security Operations***<br><br>**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.<br><br>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.<br><br>https://www.netskope.com/press-releases/netskope-advances-netskope-one-platform-with-ai-driven-proactive-dem-solution-key-security-innovations |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00181

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | <br>https://www.netskope.com/resources/data-sheets/netskope-newedge-data-sheet |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00182

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | <br>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.<br>. . . |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00183

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>**Future-proof, SASE-ready architecture**<br>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.<br><br>https://www.netskope.com/wp-content/uploads/2022/12/2023-04-NewEdge-DS-333-7-1.pdf<br><br>Inside the Netskope NewEdge Data Center Factory<br><br>Jul 13 2021 \| 9 min. read |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00184

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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 *integrated racks* 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.<br>. . .<br>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<br>https://www.netskope.com/blog/inside-the-netskope-newedge-data-center-factory<br><br>Understanding Coverage Isn't Just About Counting Data Centers<br>Aug 04 2020 \| 6 min. read<br>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<br>https://www.netskope.com/blog/understanding-coverage-isnt-just-about-counting-data-centers |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00185

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00186

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

# Netskope One Private Access

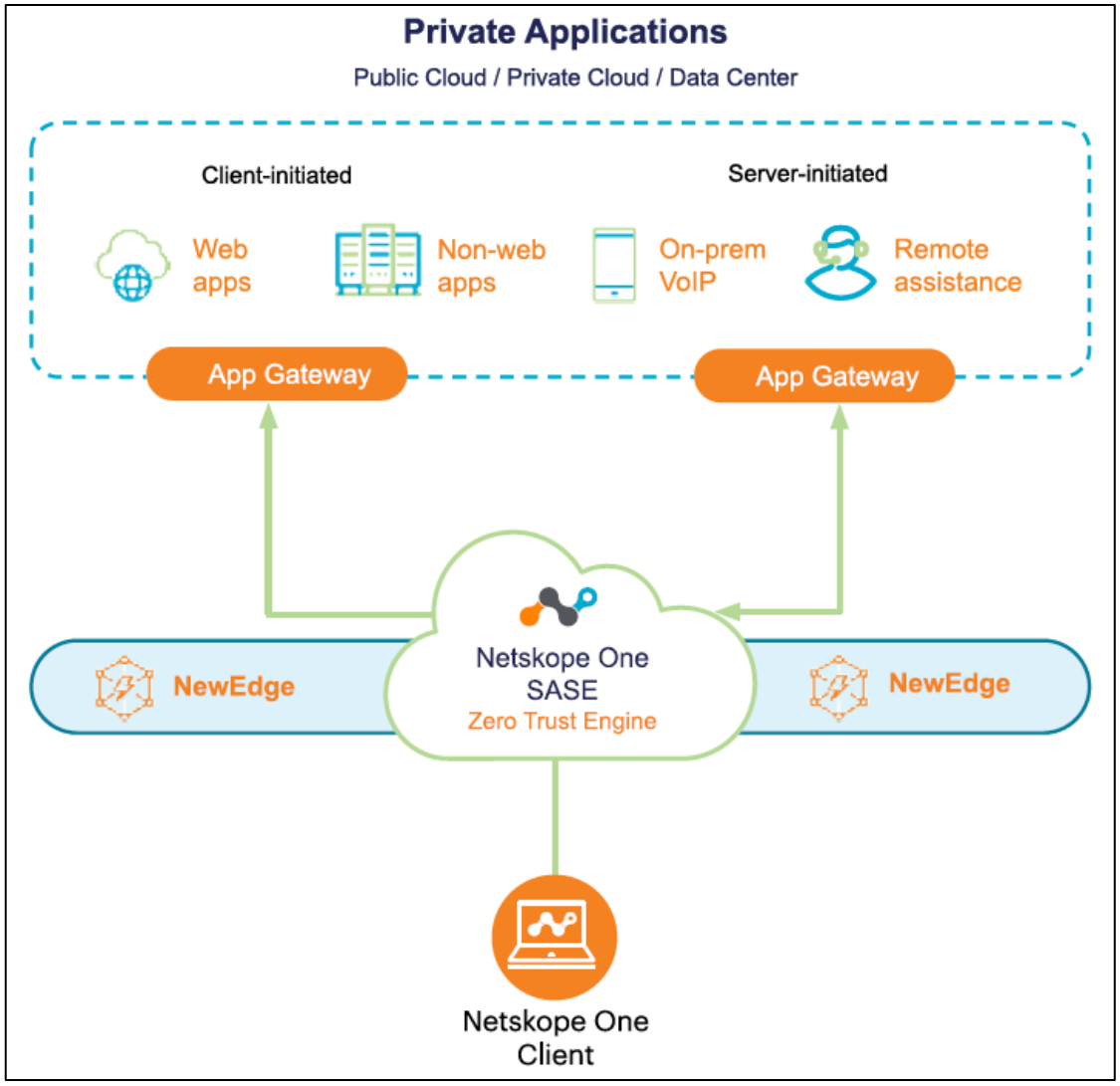
Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.

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:

- 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
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00187

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




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00188

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00189

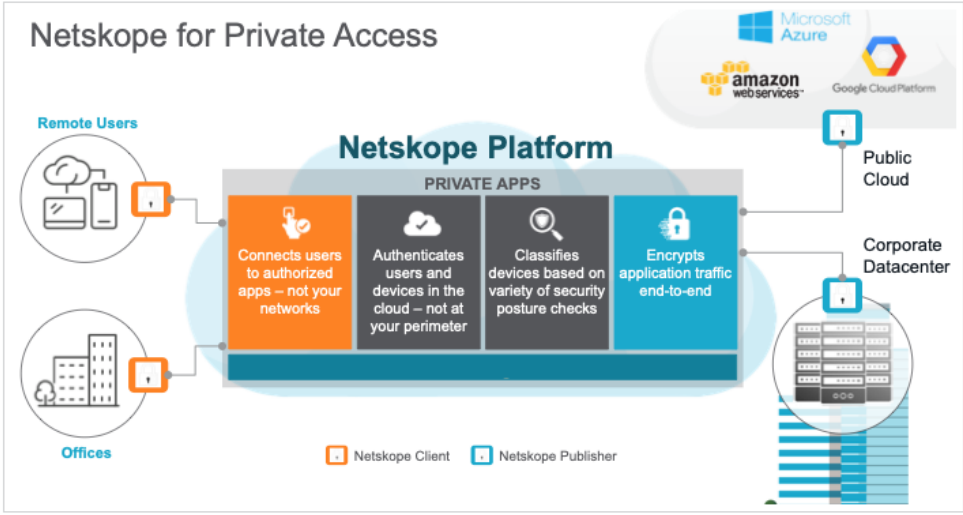
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|

## How It Works

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.

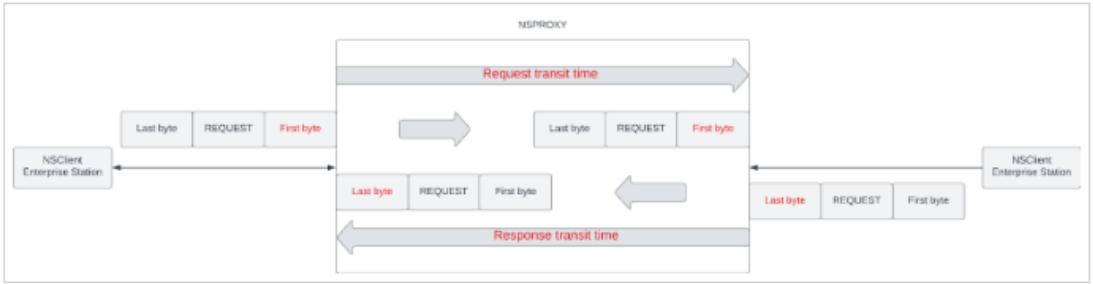
The Publisher, a lightweight connector deployed on-premises or in the cloud, establishes secure, encrypted communication between users and private applications without exposing applications to the internet. This architecture ensures that users gain access only to the specific applications they are authorized 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.

NPA is illustrated in this diagram:

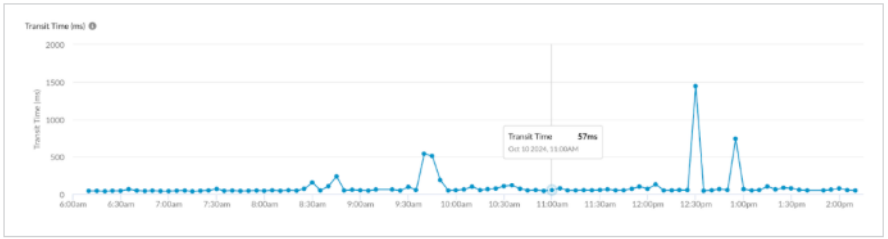



https://docs.netskope.com/en/netskope-private-access

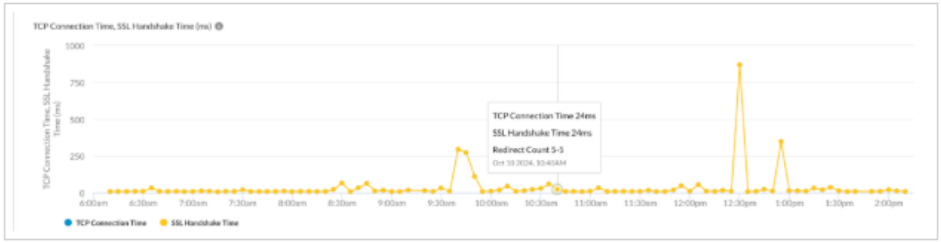
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00190

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Connection**<br>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.<br>**TLS**<br>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.<br>**Inside Netskope POPs**<br>The following metric is processed at the NSProxy level. |
| | **POP Transit Time**<br>The POP Transit Time provides the total time spent within the NSProxy.<br>It is the addition of the "request transit time" and the "response transit time". These are defined as follows:<br>• Request transit time<br>Time elapsed between the first byte of request reaching the NSProxy and this first byte of the request leaving the NSProxy<br>• Response transit time<br>Time elapsed between the first byte of response reaching the NSProxy and this first byte of response leaving the NSProxy<br>  |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00191

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Netskope POPs to Applications**<br><br>The following metrics are processed at the NSProxy level.<br><br>**Connection**<br><br>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.<br><br>**Server**<br><br>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.<br><br>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.<br><br>https://docs.netskope.com/en/performance-metrics<br><br>**Transit Time**<br><br>  <br><br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00192

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **TCP Connection Time, SSL Handshake Time**<br>  <br>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.<br>https://docs.netskope.com/en/user-overview |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00193

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The Power of One**<br><br>The major components of the Netskope One platform include:<br><br>**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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00194

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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00195

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **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.<br>2025-03-Netskope-One-Platform-SB-719-5.pdf |
| 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 unsecure network element on the remote network; | 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 unsecure network element on the remote network.<br><br>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. *See also* 1[b]. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00196

| 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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00197

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

# Netskope One Private Access

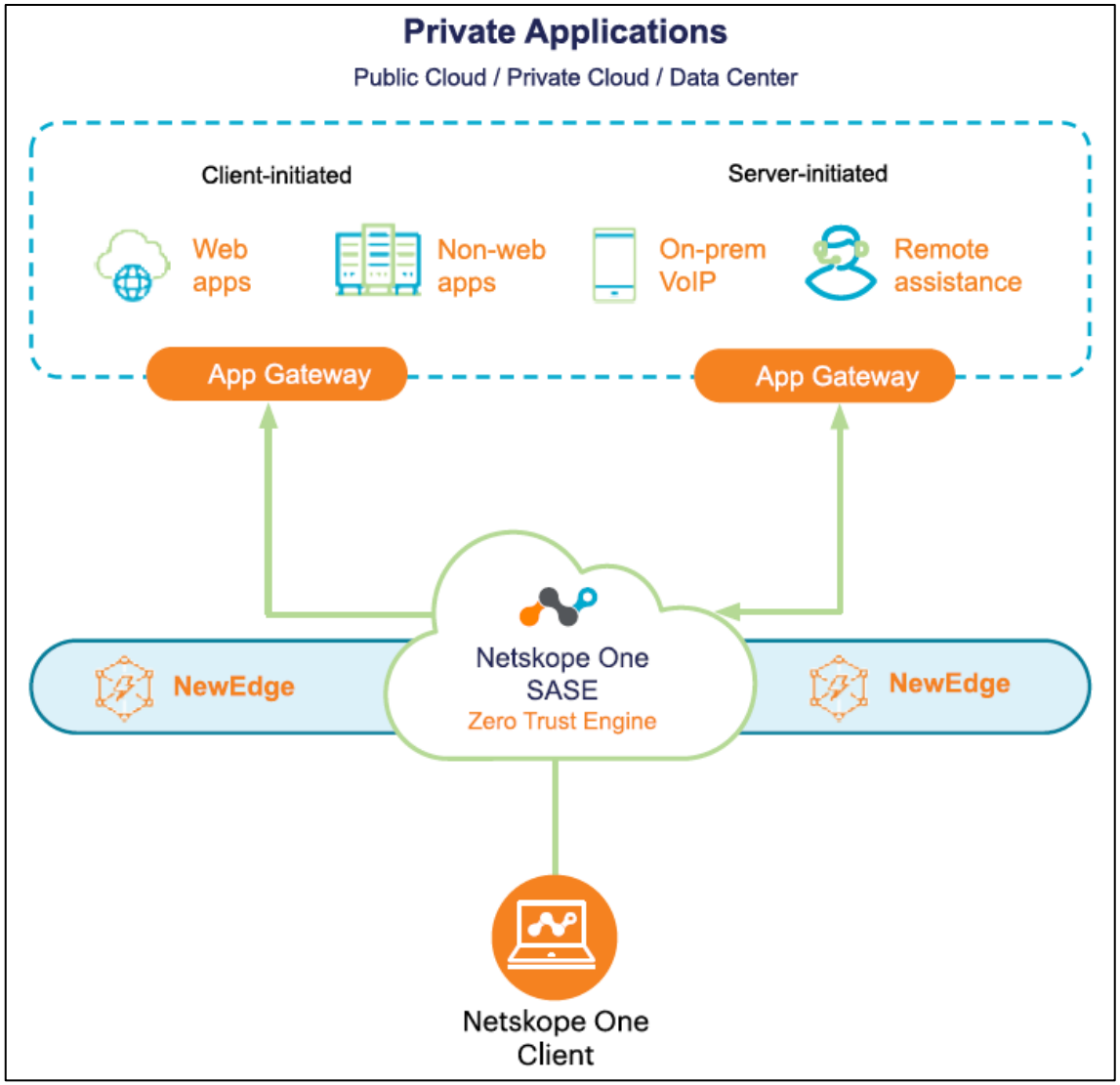
Netskope delivers the industry's first VPN replacement that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.

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:

- 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
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00198

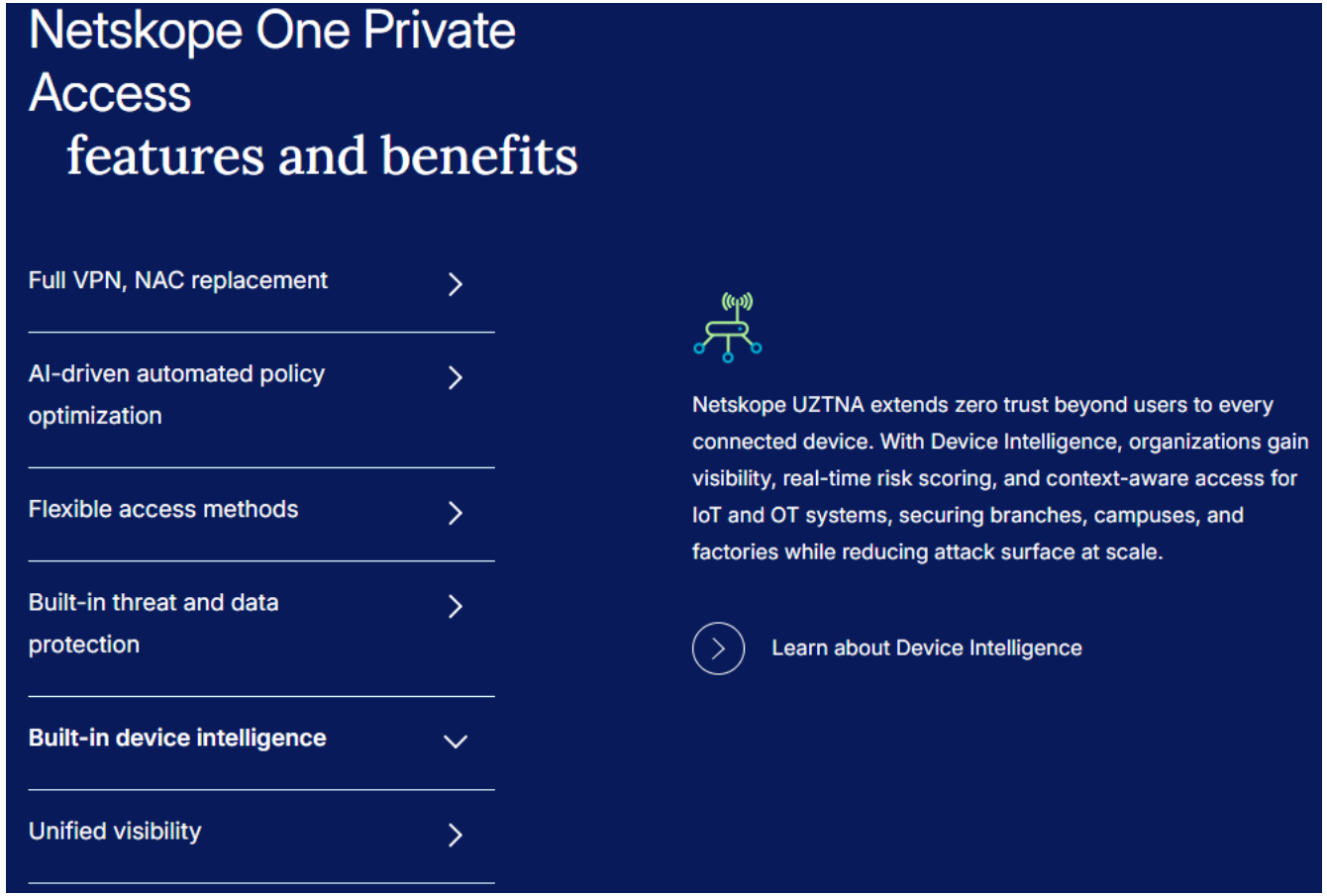
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00199

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00200

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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).<br>  <br>https://www.netskope.com/products/private-access |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00201

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br><br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00202

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

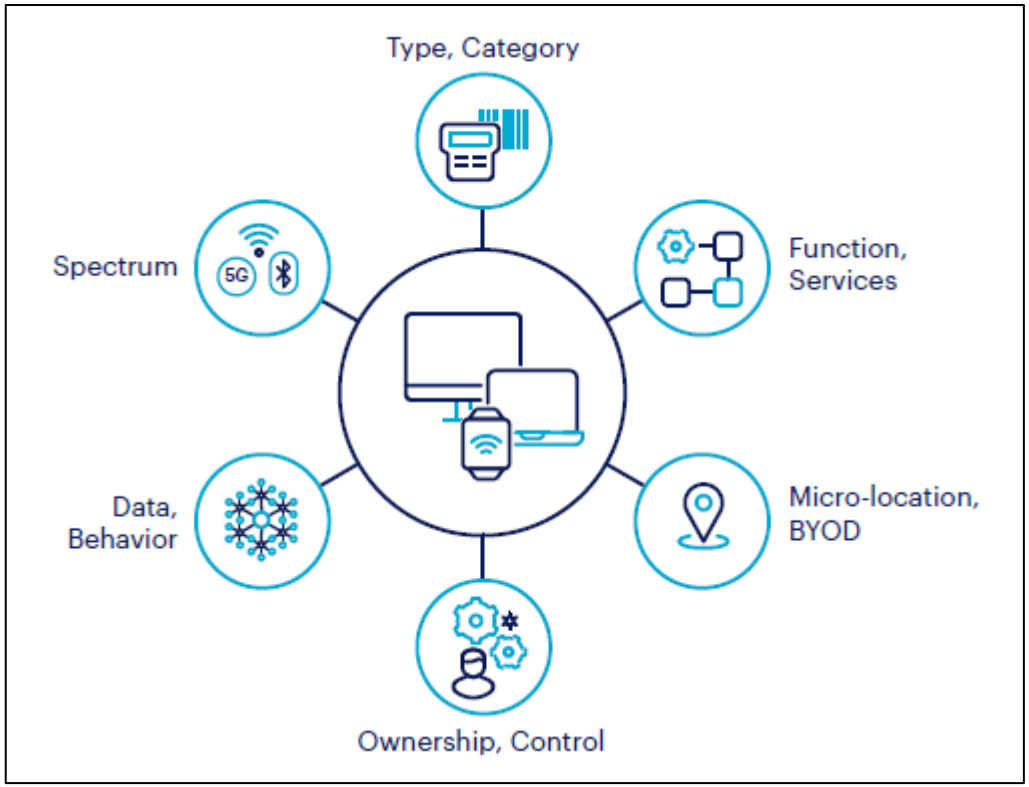
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00203

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00204

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE**<br><br>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®:<br>• Association of all the physical interfaces of the device and the spectrum of operation of each interface<br>• Type, Category of the device and related information<br>• OS, patches, services, and applications running on the device<br>• Functionality or the "purpose in life" of the device<br>• Micro location of the device, its mobility patterns, and times of visibility<br>• Ownership information of the device and its control information<br>• Users on the device<br>• Behavior based analysis of all the data transmissions across all protocols and spectrums<br>• Risk and vulnerability information, other information collected by other tools used |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00205

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00206

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

Home > Device Intelligence > Investigate Device Intelligence > Investigate Devices

## Investigate Devices

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.

> **Note**
>
> You can also sort the device summary in combination with the total of all devices, managed, unmanaged, new, automated, and user-controlled devices.

### Investigate Devices based on Spectrum

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.

https://docs.netskope.com/en/investigate-devices

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00207

| 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.

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.

https://docs.netskope.com/en/investigate-risks

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00208

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

Home > Device Intelligence > Protect Device Intelligence > Remediated Devices

## Remediated Devices

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.

You will see a list of devices that have triggered security policies. Each device entry includes the following information:

- **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 devi 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:
  - **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.

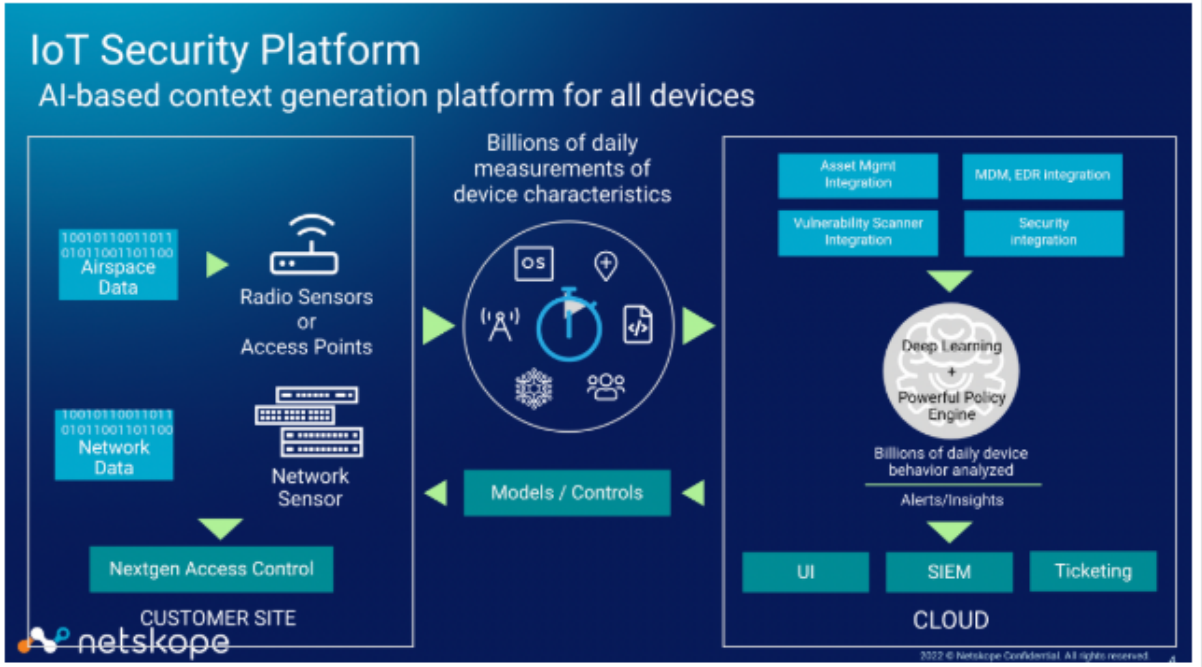
https://docs.netskope.com/en/remediated-devices

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00209

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00210

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00211

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Transfer**<br>• The network sensors do a deep inspection of the traffic, apply signatures and run algorithms to extract meta information.<br>• Network sensors send this meta information via encrypted channel to the cloud to analyze the traffic metadata and events in the environment.<br>**Data Analysis**<br>• On the cloud, various microservices analyze the metadata.<br>• 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.<br>**Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |
| 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 |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00212

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| identifying at least one unsecure network element on the remote network, deny access to the known network; and | element on the remote network, denying, by the processing device, access to the known network.<br><br>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 unsecure network elements. *See also* 1[c].<br><br>**What is ZTNA?**<br><br>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.<br><br>**Zero Trust Security Principles**<br><br>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.<br><br>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00213

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | https://www.netskope.com/security-defined/what-is-zero-trust-network-access<br><br>**Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB- |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00214

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 645-6.pdf<br><br>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.<br><br>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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br><br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00215

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00216

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00217

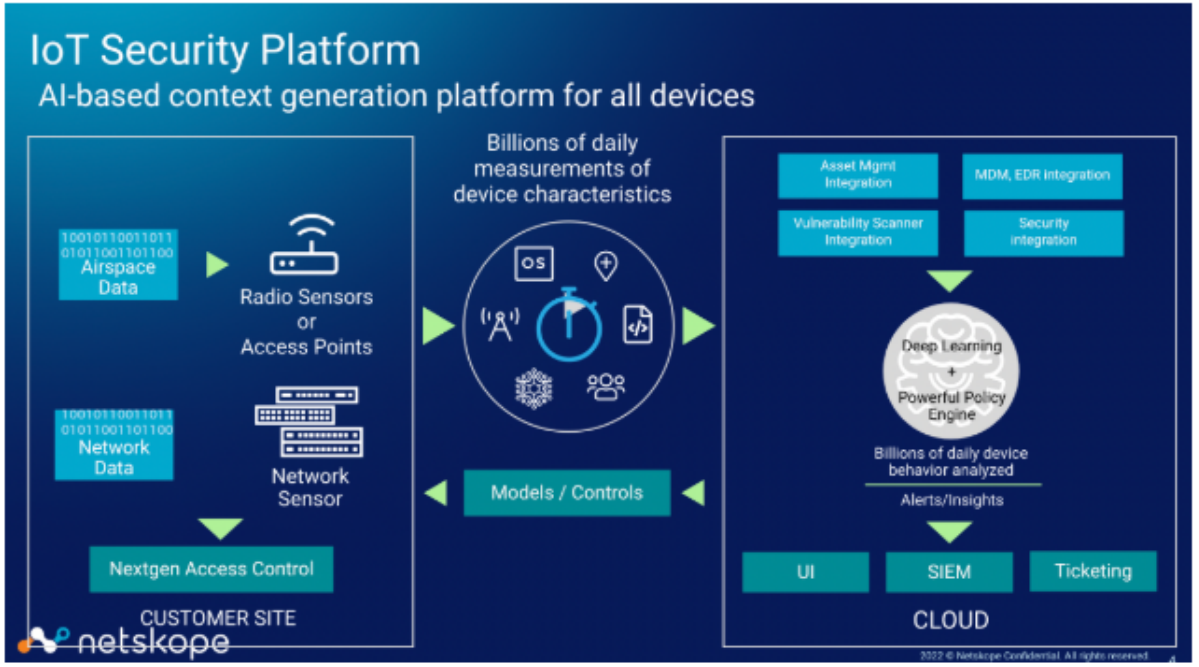
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Need for granular device context**<br>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to 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.<br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00218

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00219

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00220

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Analysis**<br>• On the cloud, various microservices analyze the metadata.<br>• 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.<br>**Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00221

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

Home > Device Intelligence > Protect Device Intelligence > Remediated Devices

## Remediated Devices

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.

You will see a list of devices that have triggered security policies. Each device entry includes the following information:

- **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 devi 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:
  - **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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00222

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 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. | 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.<br><br>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. *See also* 1[d].<br><br>**What is ZTNA?**<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00223

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Zero Trust Security Principles**<br>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.<br>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.<br>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.<br>https://www.netskope.com/security-defined/what-is-zero-trust-network-access |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00224

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00225

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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.<br><br>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:<br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br><br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00226

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00227

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00228

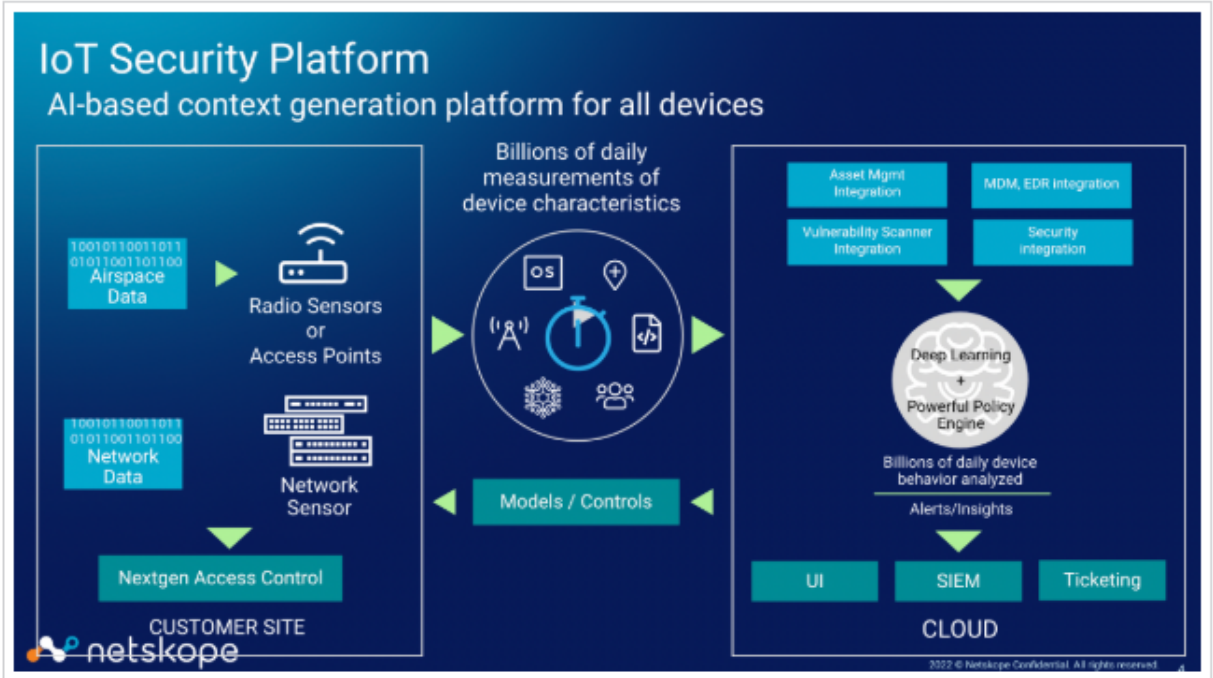
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Need for granular device context**<br>With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to 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.<br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected- |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00229

| 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.






Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00230

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00231

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Analysis**<br>• On the cloud, various microservices analyze the metadata.<br>• 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.<br>**Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00232

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

Home > Device Intelligence > Protect Device Intelligence > Remediated Devices

## Remediated Devices

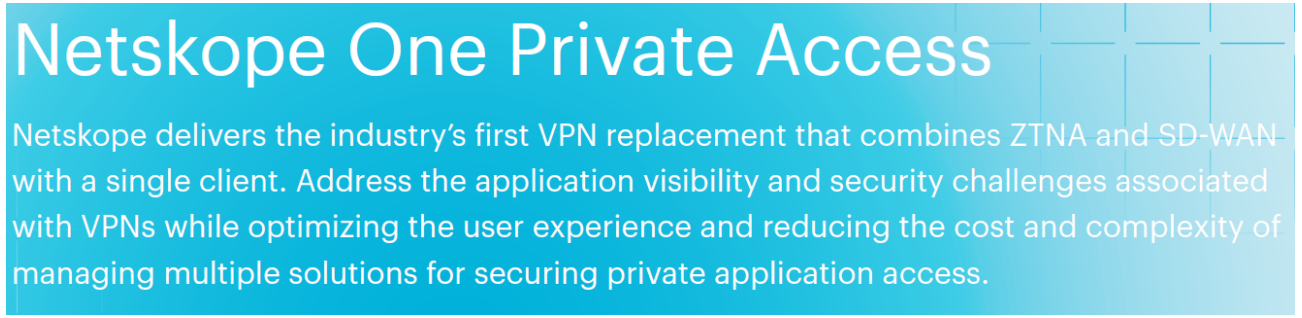
Navigate to **Policies** menu, in the **Remediated Devices** tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.

You will see a list of devices that have triggered security policies. Each device entry includes the following information:

- **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 devi 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:
  - **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

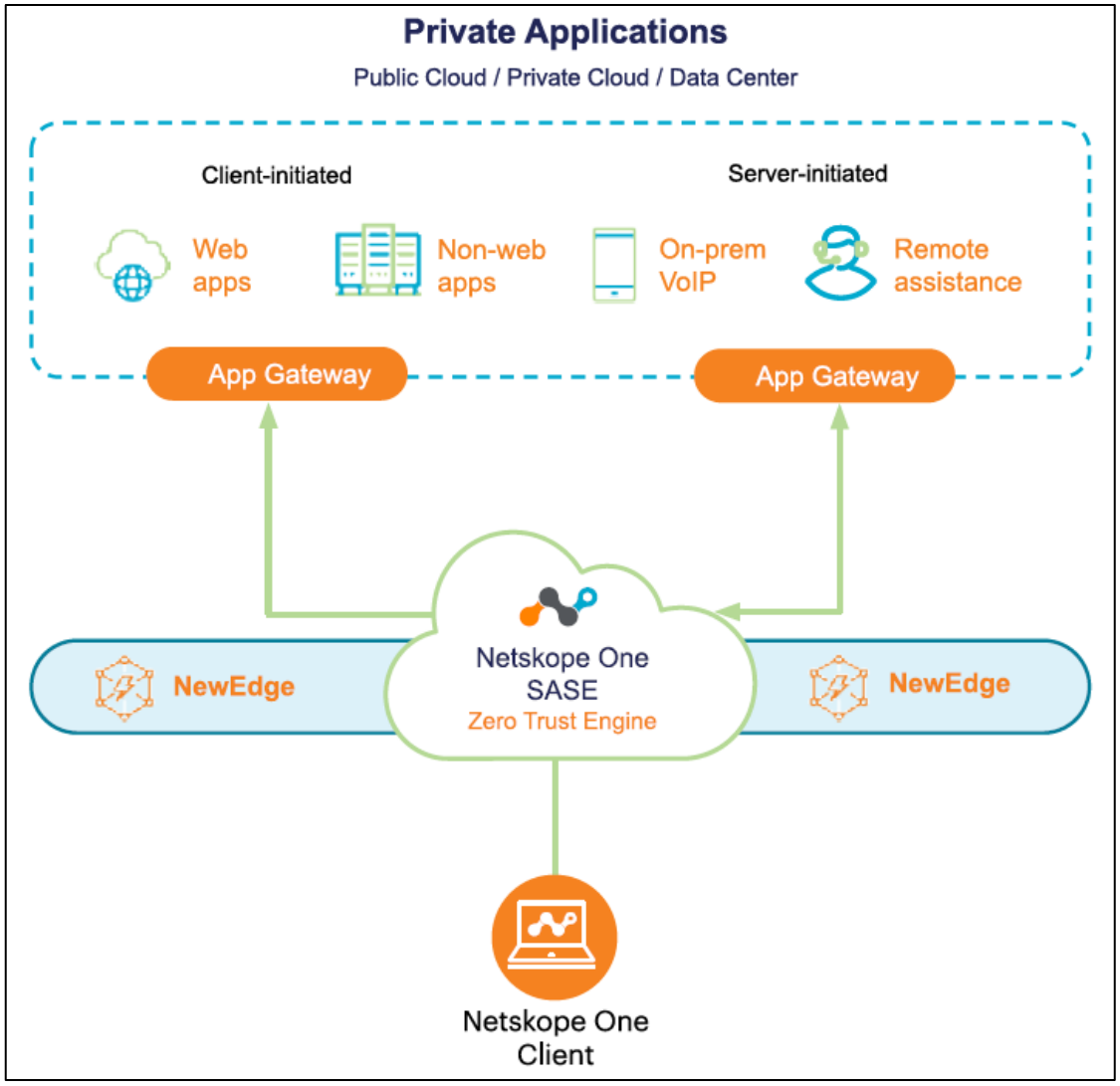
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00233

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 11[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. | 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.<br><br>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. *See also* 1[e].<br><br>  |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00234

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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:<br><br>• 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<br><br>• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00235

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



Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00236

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00237

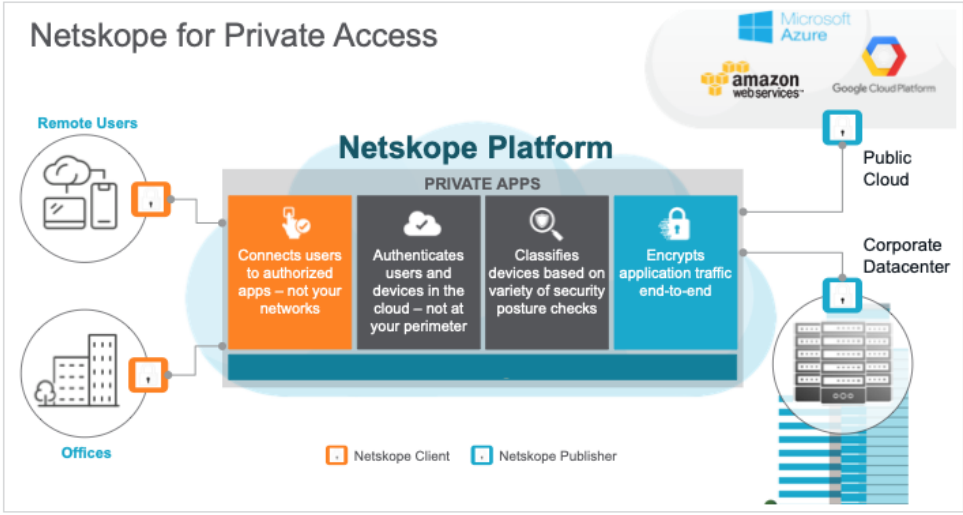
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|

### How It Works

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.

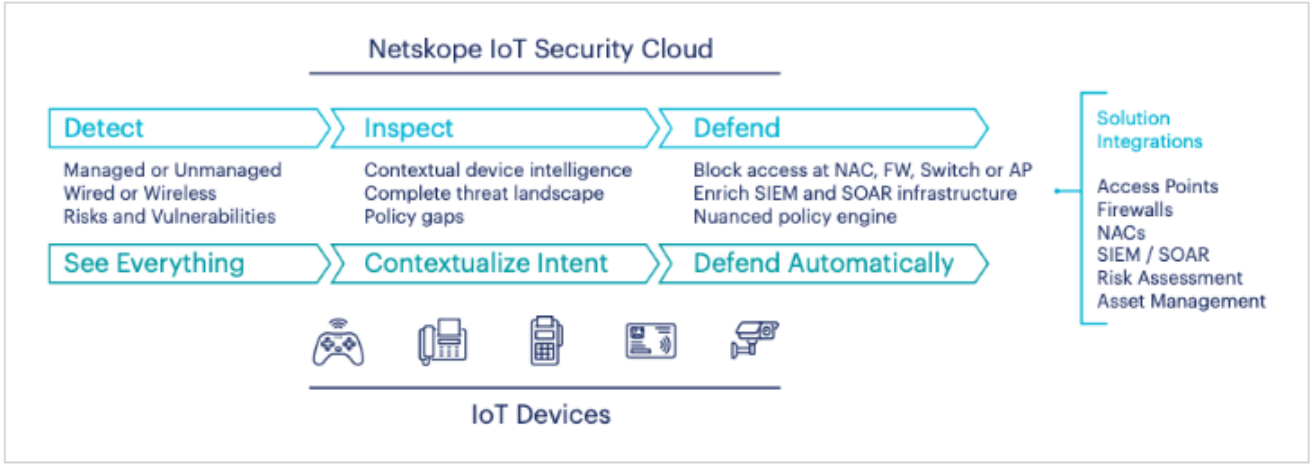
The Publisher, a lightweight connector deployed on-premises or in the cloud, establishes secure, encrypted communication between users and private applications without exposing applications to the internet. This architecture ensures that users gain access only to the specific applications they are authorized 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.

NPA is illustrated in this diagram:




https://docs.netskope.com/en/netskope-private-access

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00238

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



Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00239

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00240

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **REALIZING ZERO TRUST FOR DEVICES**<br><br>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:<br><br>• **Granular device context:** Deep context about every device, resource, and user in and around the network<br>• **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location<br>• **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment<br>• **Security automation:** Automated alert handling and responses to security incidents |

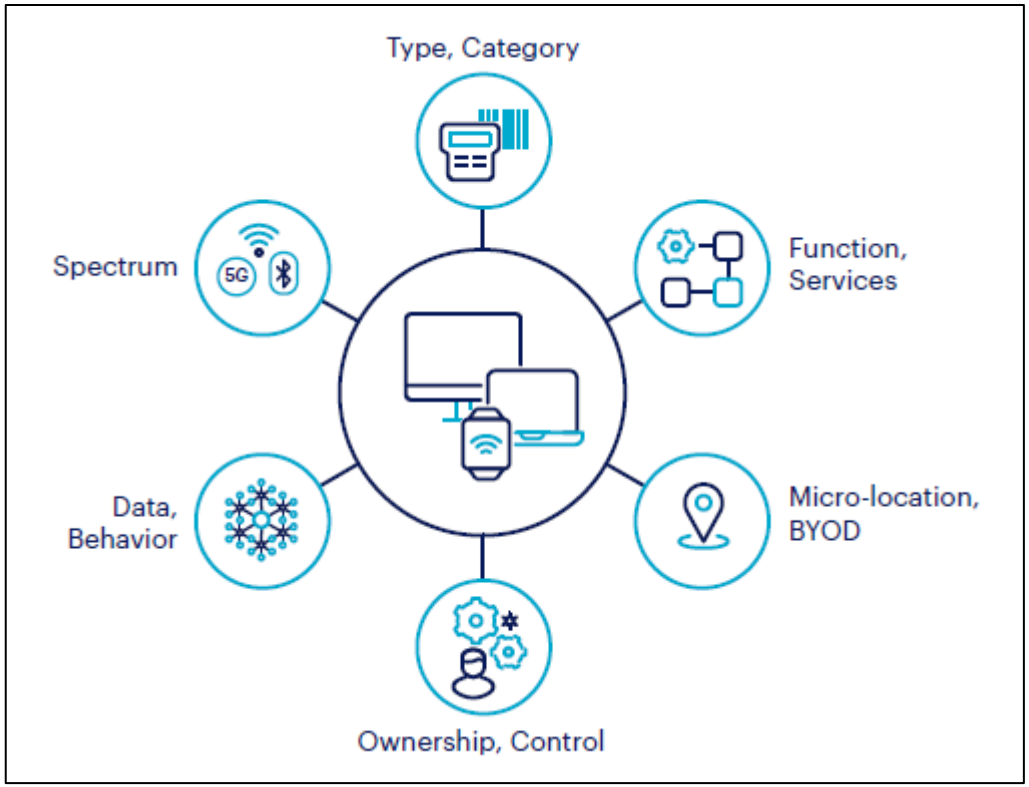
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00241

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE**<br><br>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®:<br><br>• Association of all the physical interfaces of the device and the spectrum of operation of each interface<br>• Type, Category of the device and related information<br>• OS, patches, services, and applications running on the device<br>• Functionality or the "purpose in life" of the device<br>• Micro location of the device, its mobility patterns, and times of visibility<br>• Ownership information of the device and its control information<br>• Users on the device<br>• Behavior based analysis of all the data transmissions across all protocols and spectrums<br>• Risk and vulnerability information, other information collected by other tools used |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00242

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **The critical role of micro-segmentation**<br><br>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.<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00243

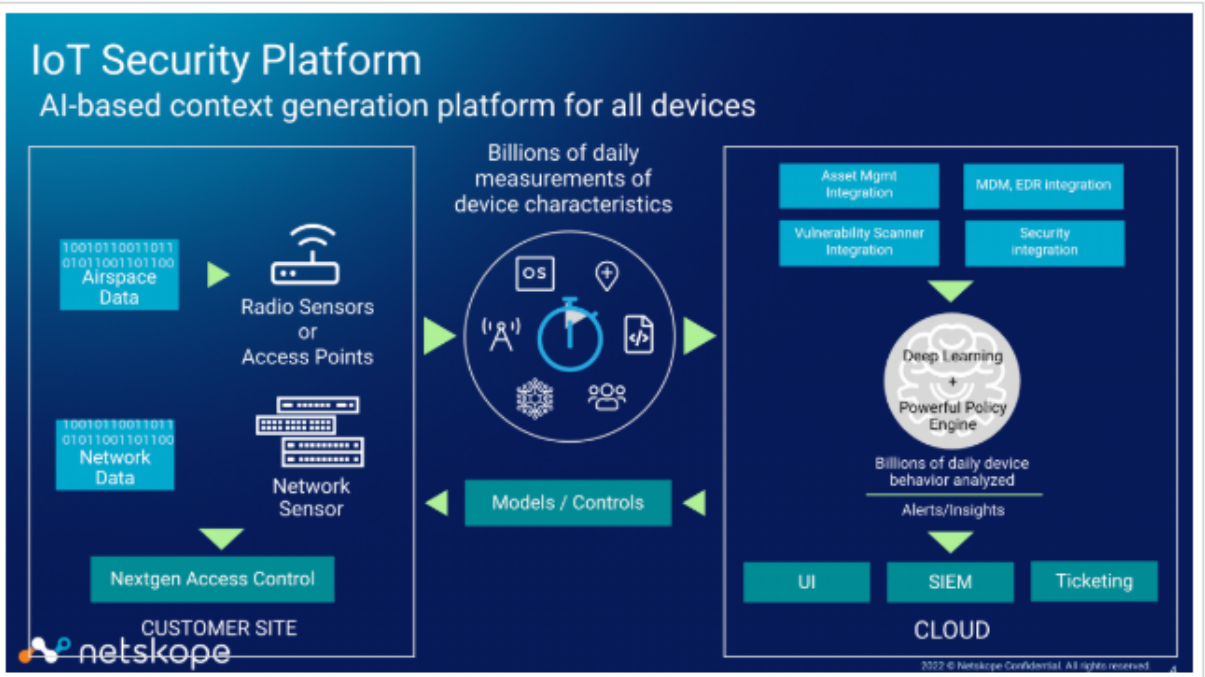
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| |  <br>https://www.netskope.com/wp-content/uploads/2023/06/achieving-zero-trust-for-connected-devices.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00244

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00245

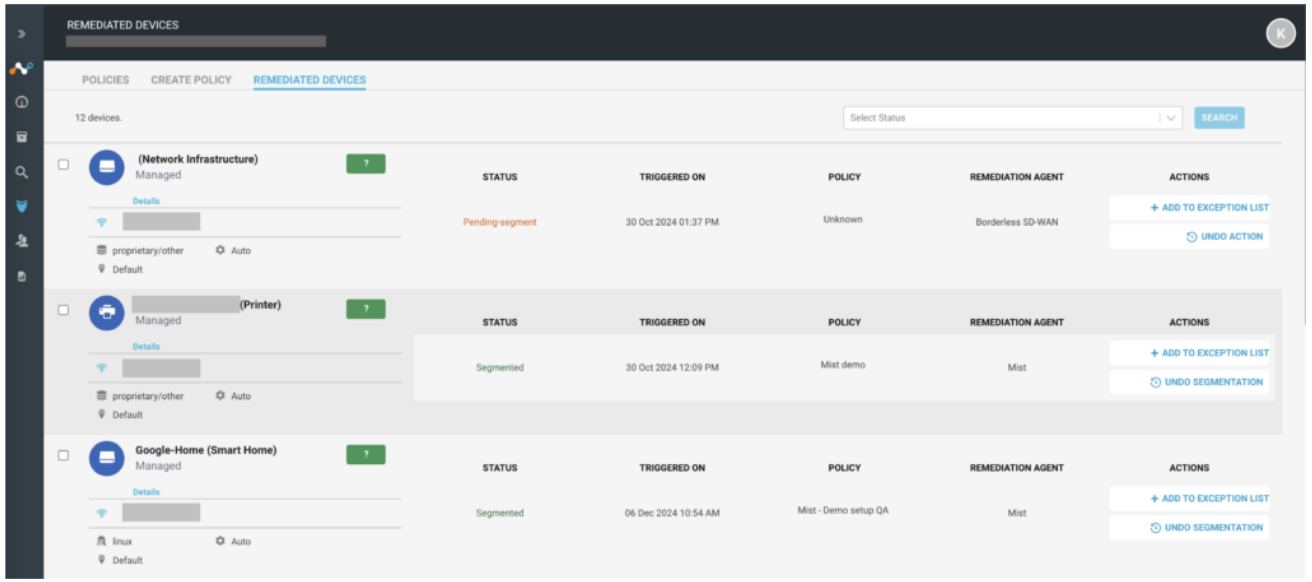
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Analytics and Protection**<br>• Device Intelligence sends the policy actions like blocking devices, assigning VLAN to devices, etc. to the network sensors. Network sensors, in turn, use on-premise NACs and firewalls to enforce policies.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00246

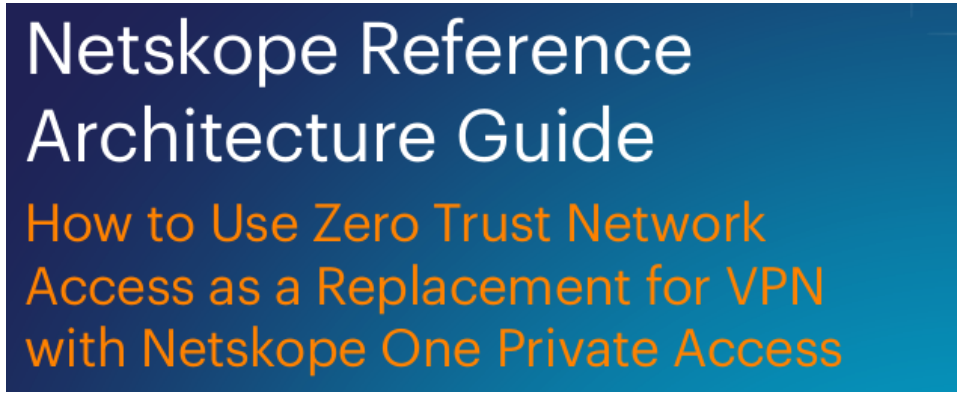
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Remediated Devices**<br><br>Navigate to **Policies** menu, in the **Remediated Devices** tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.<br><br>You will see a list of devices that have triggered security policies. Each device entry includes the following information:<br><br>• **Device Name:** The name or identifier of the device.<br>• **Device Type:** The type of device (e.g., computer, printer, IoT device).<br>• **Device Details:** By clicking on a **details** link, you will be navigated to a new page about the device details.<br>• **Status:** The current status of the remediation action (e.g., Pending Segment, Segmented).<br>• **Triggered On:** The date and time when the security policy was triggered.<br>• **Policy:** The name of the security policy that was triggered.<br>• **Remediation Agent:** The agent responsible for enforcing the remediation action.<br>• **Actions:** A set of actions that can be performed on the device, such as:<br>  • **Add to Exception List:** Excludes the device from future remediation actions.<br>  • **Undo Action:** Reverses the previous remediation action taken on the device.<br>  • **Undo Segmentation:** Reverses the previous segmentation action taken on the device. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00247

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




https://docs.netskope.com/en/remediated-devices



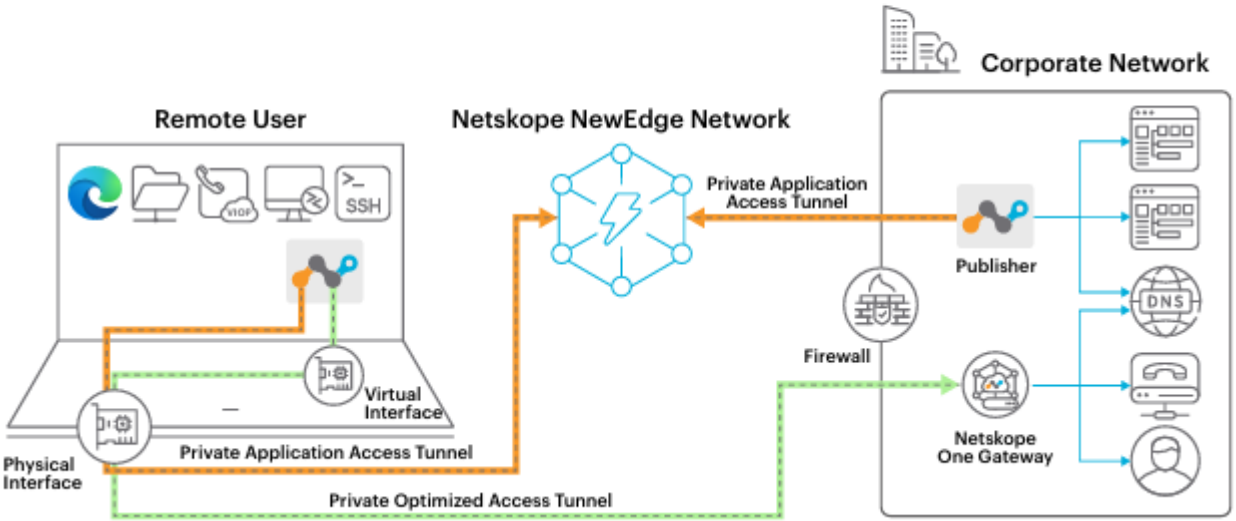

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00248

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Introducing Netskope One Private Access**<br><br>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.<br><br>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.<br><br>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. |

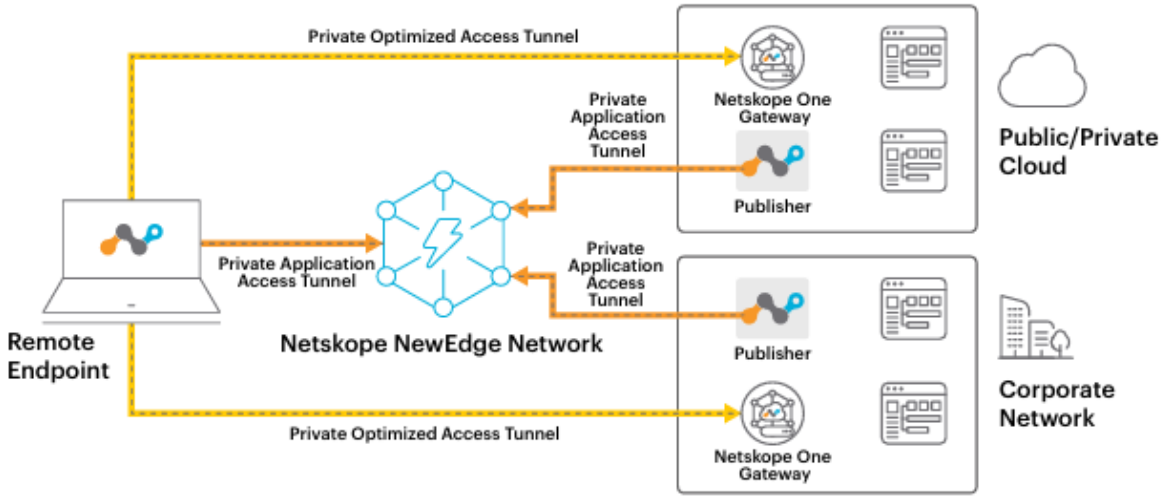
Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00249

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Key Benefits**<br><br>**Enforces Zero Trust Principles**<br><br>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:<br><br>• Identity- and context-aware, least-privileged access to private applications hosted in public clouds or on-premises data centers.<br><br>• 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.<br><br>• 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.<br><br>• Reducing the opportunities for lateral movement of threats within the private networks and limiting the blast radius.<br><br>• Eliminating the dependence on public-facing VPNs or open inbound firewall ports for application access, securing networks from threats and DDoS attacks.<br><br>**Secures All Enterprise Applications**<br><br>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:<br><br>• 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.<br><br>• Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all private applications. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00250

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Delivers a Phenomenal User Experience**<br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key benefits include:<br>• 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.<br>**Full Zero Trust Application Access: Netskope One Private Unified Access**<br>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.<br>  |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00251

| 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.<br>  <br><br>2024-12-Reference-Architecture-Guide-for-ZTNA-Next-RA-709-3-1.pdf<br><br>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 |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00252

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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. |
| 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. | 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.<br><br>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.<br><br>**What is ZTNA?**<br><br>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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00253

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Zero Trust Security Principles**<br>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.<br>Users everywhere, using any device, gain direct access to applications hosted anywhere, providing superior user experience with consistent policy controls.<br>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.<br>https://www.netskope.com/security-defined/what-is-zero-trust-network-access |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00254

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Seamless and optimized user experience**<br><br>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.<br><br>Netskope One Private Access provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:<br><br>• 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.<br><br>• 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.<br><br>https://www.netskope.com/wp-content/uploads/2023/04/2024-11-Netskope-one-private-access-SB-645-6.pdf |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00255

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Netskope One<br><br>Client<br><br>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.<br><br>A simplified user experience<br><br>Easy to use, lightweight and highly performant, Netskope One Client steers user traffic through the Netskope One platform. Netskope One Client centralized configuration, deployment, support, and troubleshooting delivers comprehensive security and control across the borderless modern threat landscape.<br><br>https://www.netskope.com/netskope-one/client |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00256

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br><br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00257

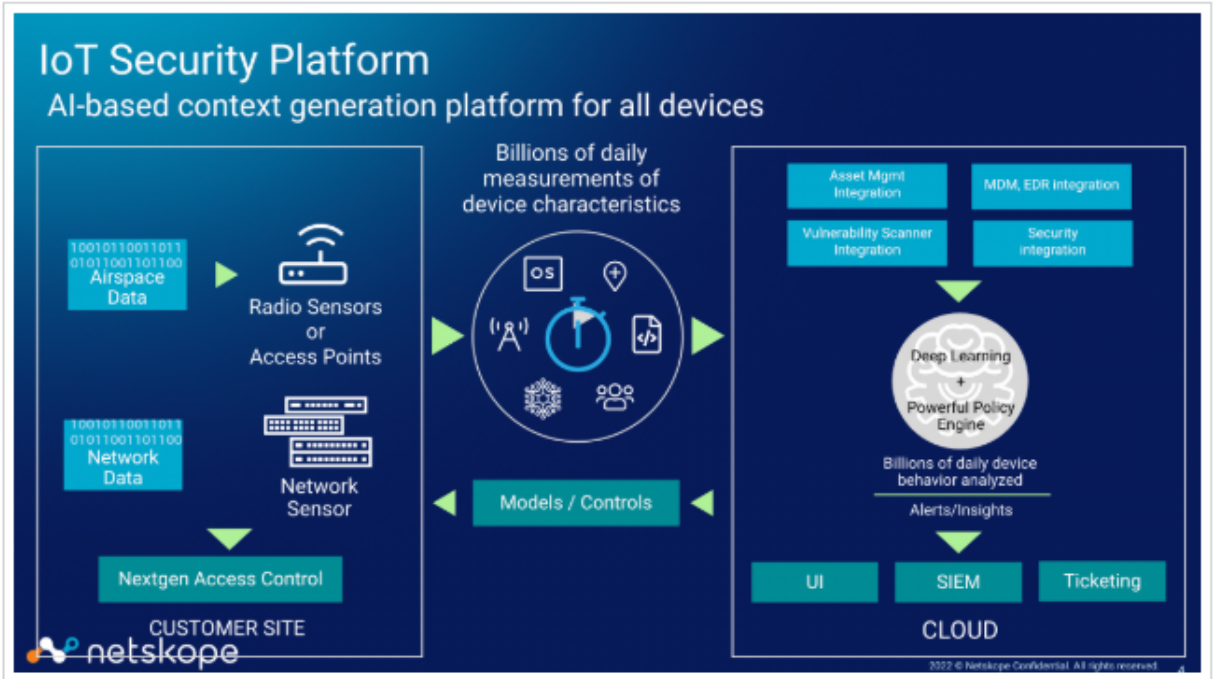
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence addresses the IoT device security gaps in the hybrid enterprise using artificial intelligence and machine learning:<br>• Device classification and visibility – Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior.<br>• 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.<br>• 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.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00258

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00259

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Acquisition**<br>• Customer environments have network sensors installed as physical or virtual appliances.<br>• 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.<br>• If available, network sensors query Wireless LAN Controller (WLC) networks to get information of all connected devices supported by WLC.<br>• If available, network sensors also query switching and routing networks in the environment to get information of all the connected wired devices.<br>• 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. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00260

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | **Data Analysis**<br>• On the cloud, various microservices analyze the metadata.<br>• 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.<br>**Analytics and Protection**<br>• 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.<br>• In the case of third party cloud based integrations like MIST and Meraki, the product uses the cloud access points to enforce the policies.<br>• 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.<br>https://docs.netskope.com/en/architecture-of-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00261

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

Home > Device Intelligence > Protect Device Intelligence > Remediated Devices

## Remediated Devices

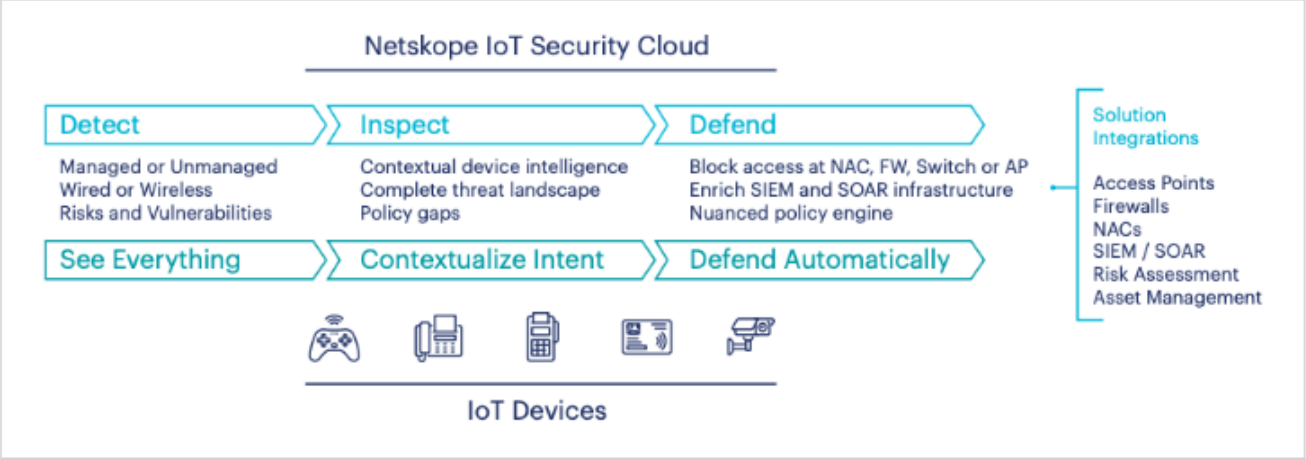
Navigate to **Policies** menu, in the **Remediated Devices** tab you can manage and control the remediation actions taken on devices that have triggered security policies. It provides a centralized view of devices that require attention and allows administrators to take appropriate actions to address security risks.

You will see a list of devices that have triggered security policies. Each device entry includes the following information:

- **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 devi 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:
  - **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

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00262

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 13. The system of claim 11, wherein the unsecure network element is an Internet of Things (IoT) device. | The Accused '902 Products include a system wherein the unsecure network element is an Internet of Things (IoT) device.<br><br>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.<br><br>  |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00263

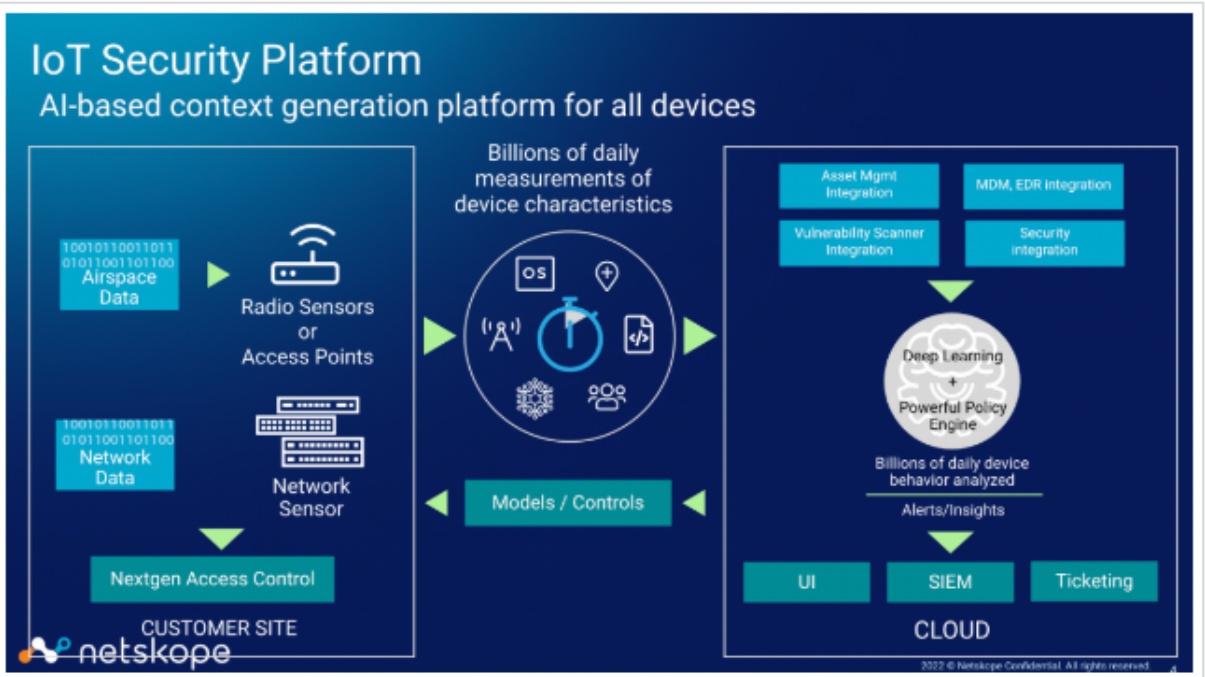
| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| | Device Intelligence extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The zero trust engine in the system network performs risk 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.<br><br>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:<br><br>• HyperContext – Deep context about every device, resource, and user in and around the network.<br>• Micro-Segmentation – Ability to dynamically micro segment devices based on the HyperContext and geolocation.<br>• Dynamic Control – User access control of devices and resources in the network based on context and real time threat assessment.<br>• 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.<br>https://docs.netskope.com/en/what-is-netskope-iot-security |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00264

| 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.




Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00265

| 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: | 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.<br><br>*See* 1[pre] and 1[a] incorporated here by reference. |
| 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; | 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.<br><br>*See* 1[a] incorporated here by reference. |
| 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 unsecure network | 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 unsecure network element on the remote network.<br><br>*See* 1[b] incorporated here by reference. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00266

| 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 unsecure network element on the remote network, denying access to the known network; and | The Accused '902 Products include based at least in part on identifying at least one unsecure network element on the remote network, denying access to the known network.<br><br>*See* 1[c] incorporated here by reference. |
| 14[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. | 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.<br><br>*See* 1[d] incorporated here by reference. |
| 14[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. | 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.<br><br>*See* 1[e] incorporated here by reference. |
| 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 | 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.<br><br>*See* claim 5 incorporated here by reference. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00267

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 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. | |
| 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. | 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.<br><br>*See* claim 6 incorporated here by reference. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00268

| U.S. Patent No. 11,916,902 | Exemplary Evidence of Infringement |
|---|---|
| 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. | 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.<br><br>*See* claim 8 incorporated here by reference. |

Netskope Ex. 1014
Netskope v. Fortinet IPR2027-00011
Page 00269