

EXHIBIT D – INFRINGEMENT CONTENTIONS OF U.S. PATENT NO. 12.126.695

Fortinet provides the disclosures below based on information reasonably available to it as of the date of these disclosures, before Fortinet has received any discovery or the Court has construed the asserted claims. Further, information about Netskope’s accused functionalities relevant to this asserted patent and its infringement contentions is not publicly available. Accordingly, Fortinet reserves the right to amend, modify, and/or supplement these disclosures to the full extent permitted under the Court’s rules as information becomes available, including in view of the Court’s findings on claim construction and/or positions taken by Netskope regarding infringement and/or invalidity.

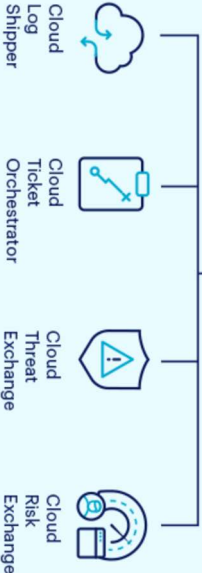
Fortinet contends that each limitation is met directly and/or indirectly, literally and/or under the doctrine of equivalents by the accused functionalities. For example, based on information available to date, the Accused ’695 Products include at least Netskope’s Cloud Exchange product and any Netskope products that incorporate or otherwise leverage the functionality provided by the same (*e.g.*, Netskope Secure Web Gateway (a.k.a., “SWG”, “Next Gen Secure Web Gateway,” “NG-SWG”, “Netskope for Web”) (collectively, “SWG”).

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. Information about Netskope’s accused functionalities, including information relevant to this asserted patent and Netskope’s infringement, is not publicly available. For example, functionality relevant to the asserted claims and Netscape’s infringement is present in Netskope software, firmware, source code, and/or configurations of the ’695 Accused Products. Accordingly, Fortinet specifically reserves the right to amend, modify, and/or supplement these contentions in response to Netskope (or third-parties where appropriate) producing, after Fortinet’s service of these contentions, additional documents, software, firmware, source code, and/or configuration files for or related to each of the Accused ’695 Products, as information becomes available including in view of the Court’s findings on claim constructions and/or positions taken by Netskope.

<u>U.S. Patent No. 12.126.695</u>	<u>Exemplary Evidence of Infringement</u>
1[pre]: A method of learning from other cloud deployments to combat security threats, the method comprising:	To the extent the preamble is found to be limiting, the Accused ’695 Products include a method of learning from other cloud deployments to combat security threats.
1[a]. identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning;	The Accused ’695 Products include identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning. For example, the Accused ’695 Products include Cloud Threat Exchange, which can be configured to share (<i>e.g.</i> , receive and/or provide) cloud threat intelligence (<i>e.g.</i> , IOCs and information related to the same) to/from different cloud vendors, including third party vendors operating additional cloud deployments (<i>e.g.</i> , cloud deployments separate from a Netskope customer’s cloud deployment).



Cloud Exchange



- Cloud Log Shipper
- Cloud Ticket Orchestrator
- Cloud Threat Exchange
- Cloud Risk Exchange

About Cloud Exchange

The Netskope Cloud Exchange (CE) platform and its four modules are provided at no charge to customers. One or more modules can be activated at a time. CE is deployed as a docker-based solution wherever Linux can be run and on systems that support docker. Customers can use their own resources to deploy and manage CE or they can have Netskope deploy and manage CE for them. The Netskope managed service offering for CE includes 99.9% availability and 24x7 support.

<https://www.netskope.com/products/cloud-exchange>
<https://docs.netskope.com/en/private-access-faqs/>

Netskope Unveils Cloud Threat Exchange, Enabling Peer-to-Peer Sharing of Threat Intelligence in the Cloud

A first of its kind, with Cloud Threat Exchange, technology vendors and customers can share cloud threat intelligence with each other to improve their overall threat prevention posture

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Cloud Threat Exchange features include: • Facilitates the exchange of threat indicators between vendors, including file hashes, malicious URLs, and DLP file signatures, thus providing customers with fast, up-to-date protection across their security investments. • Reduces time between new threat discovery and protection implementation, allowing organizations to keep up with the ever-evolving threat landscape. • Establishes full IOC exchange with leading security providers, including endpoint detection and response, threat intelligence, managed detection and response, email security, and ticket management systems. Other vendors are easily added by customers or partners building their own plug-ins. • Works with indicators delivered via STIX/TAXII standards enabling information sharing for real-time network defense. Netskope Unveils Cloud Threat Exchange, Enabling Peer-to-Peer Sharing of Threat Intelligence in the Cloud - Netskope “Netskope Threat Labs leverages anonymized usage data collected from the Netskope Security Cloud platform to gain visibility into cloud app usage on managed devices” Netskope Threat Labs: Combating Security Threats Netskope’s Cloud Exchange is a “cloud based solution” that includes the Netskope “security cloud” for any Netskope certified partner, vendor or customer using Cloud Exchange, which is a first cloud deployment as recited by this claim:

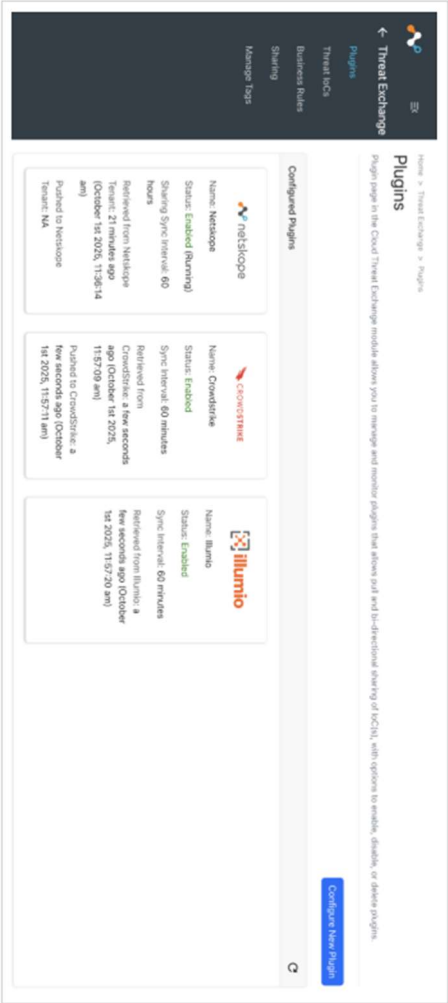
U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	SANTA CLARA, Calif., Sept. 3, 2020 /PRNewswire/ -- Netskope, the leading <u>security cloud</u>, today announced the <u>Cloud Threat Exchange</u>, one of the industry's first cloud-based solutions for the ingestion, curation, and real-time sharing of threat intelligence across enterprise security enforcement points. With this announcement, Netskope has made the Cloud Threat Exchange free and open to customers that wish to use the technology to collaborate on sharing indicators of compromise (IOCs). Any certified, partner, vendor, or customer may use Cloud Threat Exchange to automate the delivery and distribution of high-value, actionable threat intelligence, thus reducing the time to protection and eliminating gaps in coverage. Cloud Threat Exchange is supported by a wide range of members certified by Netskope, which include <u>VMware Carbon Black</u>, <u>CrowdStrike</u>, <u>Cyberason</u>, <u>Mimecast</u>, <u>SentinelOne</u>, and <u>ThreatQuotient</u>. Together, this ecosystem helps mutual customers maximize the benefit of their protections by leveraging threat intelligence across multiple enforcement points. <u>Netskope Unveils Cloud Threat Exchange, Enabling Peer-to-Peer Sharing of Threat Intelligence in the Cloud</u> Additionally, Cloud Exchange includes identifying “one or more additional cloud deployments to utilize for cross-customer learning.” For example, as discussed above, Cloud Threat Exchange “[f]acilitates the exchange of threat indicators between vendors. Additionally, Cloud Threat Exchange provides for the configuration of 3rd-party Threat Exchange plugins configures Cloud Exchange to “collect and share indicators [of compromise] related to file hashes of malicious software (malware) used in a Netskope DLP policy”

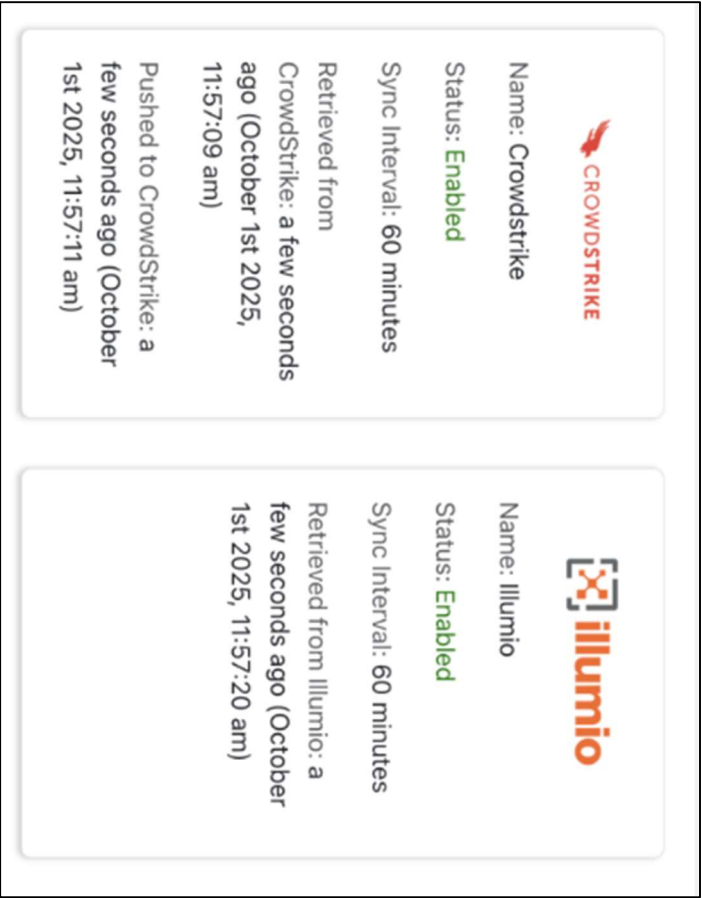
U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
	Configure 3rd-party Threat Exchange Plugins Only admins and write-access users can configure 3rd-party Threat Exchange plugins. Threat Exchange comes with a library of supported plugins. Plugins can be easily configured to collect and share indicators related to file hashes of malicious software (malware) used in a Netskope DLP policy by following the plugin guide. Refer to the Threat Exchange Custom Plugin Developers Guide to understand how to build and upload a custom plugin. You can also disable, enable, or delete existing plugin configurations. Threat Exchange can be configured with multiple plugins to the same system for different workflows from either the same Netskope tenant or multiple Netskope tenants. Threat Exchange ONLY pulls the following IoC's when they are available: 1. Malicious file file hashes in MD5 or SHA256 format. 2. URL: Depending on the nature of the plugin, these could be malicious URL, restricted URL, or allowed URL. The latter two would be for firewall, SWG, or CASB policy synchronization. Fetching malicious Hostnames, Domains and FQDNs are also supported. 3. IP addresses (CIDR): Depending on the nature of the plugin, these could be malicious IP (IPv4/IPv6), restricted IP, or allowed IP. The latter two would be for firewall, SWG, or CASB policy synchronization. https://docs.netskope.com/en/configure-3rd-party-threat-exchange-plugins

View Configured Threat Exchange Plugins

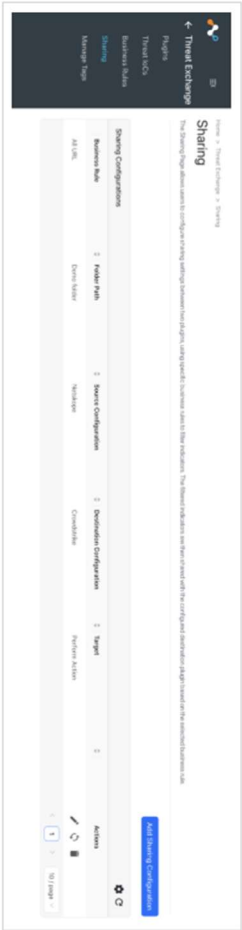
Write-access users can view the list of configured plugins and the status.

1. Go to **Threat Exchange** and click **Plugins**.
2. A list of configured plugins is displayed in the Configured Plugins section. Each plugin configuration is displayed as a card. There can be multiple plugin configurations for each vendor, each performing a task (sharing IoC, filtering, pulling IoC from Threat Exchange) a different way to the same or different vendor systems.



U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
	 The screenshot displays two configuration panels for threat exchange plugins in Netskope. The left panel is for CrowdStrike, showing it is enabled with a sync interval of 60 minutes and data retrieved from CrowdStrike a few seconds ago on October 1st, 2025, at 11:57:09 am. The right panel is for Illumio, also enabled with a 60-minute sync interval and data retrieved from Illumio a few seconds ago on the same date and time (11:57:20 am). https://docs.netkope.com/en/view-configured-threat-exchange-plugins Moreover, Netskope users identify the additional cloud deployment when they “map a threat exchange business rule to a target” cloud deployment (e.g., via plugins / connected vendor systems).

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Map a Threat Exchange Business Rule to a Target Write-access users can map a Threat Exchange business rule to a target. This section explains how to configure IOC sharing between the plugins (and therefore connected vendor systems). Make sure to identify the sharing requirements between systems in advance of configuration. The sharing filters (requires a business rule) allow for greater control over what data is shared with the plugin. 1. Go to Threat Exchange > Sharing. 2. Click Add Sharing Configuration.



- 2. Select a Source Configuration, Destination Configuration, and Business Rule.
- 3. Based on the selected Source Configuration, Destination Configuration list will be populated.
- 4. Based on the selection of Destination Configuration, a list of Target will be populated. Select a Target that you want to map to the selected Business Rule.
- 5. If the Target has some required parameters, user will need to add those.
- 6. Click **Save**.

Adding a new sharing configuration will share the existing IoCs (matching business rule) of the Source Configuration to the Destination Configuration.

The sharing configuration is unidirectional by default: data obtained from one plug-in is shared with another plugged-in system. To achieve bi-directional sharing, configure both directions of sharing separately.

<https://docs.netskope.com/en/map-a-threat-exchange-business-rule-to-a-target>

<u>U.S. Patent No. 12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	If you haven't already done so, create Threat Exchange sharing to use in your Netskope tenant. The Sharing configuration settings needed are: • Source configuration will be the plugin that provided the file hash. • Business rule will be the configured rule to be used to decide what data to share from the IoC database. • Destination configuration will be the plugin where the data is destined (different plugins have different abilities to ingest data from Threat Exchange). • Target dictates where the data will be stored in the destination system. In the Netskope tenant, the data is either pushed to a URL list or, in this workflow, a file hash list. • List Size specifies the maximum size of any file pushed by Threat Exchange. Netskope only supports a maximum file size of 8 MB to be sent via a single RESTful API (v1 only) or GUI upload workflows. • Default File Hash is no longer needed and can be ignored as of Cloud Exchange 3.1. https://docs.netskope.com/en/configure-threat-exchange-sharing-with-your-nskskope-tenant
1[b] receiving information describing a security threat to one or more of the additional cloud deployments;	The Accused '695 Products include receiving information describing a security threat to one or more of the additional cloud deployments. For example, Netskope's Cloud Threat Exchange allows Netskope (or its customers) to receive information for one cloud vendor that describes a security threat to one or more additional cloud vendors (e.g., "Peer-to-Peer Sharing of Threat Intelligence"), including, in one example, the URL and/or Hash (SHA256, MD5, etc.) for the security threat to one or more of the additional cloud deployments.

U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
	Configure 3rd-party Threat Exchange Plugins Only admins and write-access users can configure 3rd-party Threat Exchange plugins. Threat Exchange comes with a library of supported plugins. Plugins can be easily configured to collect and share indicators related to file hashes of malicious software (malware) used in a Netskope DLP policy by following the plugin guide. Refer to the Threat Exchange Custom Plugin Developers Guide to understand how to build and upload a custom plugin. You can also disable, enable, or delete existing plugin configurations. Threat Exchange can be configured with multiple plugins to the same system for different workflows from either the same Netskope tenant or multiple Netskope tenants. Threat Exchange ONLY pulls the following IoC's when they are available: 1. Malicious file file hashes in MD5 or SHA256 format. 2. URL: Depending on the nature of the plugin, these could be malicious URL, restricted URL, or allowed URL. The latter two would be for firewall, SWG, or CASB policy synchronization. Fetching malicious Hostnames, Domains and FQDNs are also supported. 3. IP addresses (CIDR): Depending on the nature of the plugin, these could be malicious IP (IPv4/IPv6), restricted IP, or allowed IP. The latter two would be for firewall, SWG, or CASB policy synchronization. https://docs.netskope.com/en/configure-3rd-party-threat-exchange-plugins

Exemplary Evidence of Infringement

Data Models

This section lists down the Data Models and their properties.

Indicator Type Model

- This class provides the Python data model for an IndicatorType object.
- This model has 3 fields: URL, SHA256, MD5 of type string.
- You will interact with the model in the pushmethod as you sending a list of Indicators to thirdparty.

Data Model Properties

Name	Type	Description
URL	string	It can be used for URLs
SHA256	string	It can be used for sha256 typ of file hashes
MD5	string	It can be used for md5 type of file hashes

<https://docs.netkope.com/en/threat-exchange-custom-plugin-developers-guide>

U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
	Cloud Threat Exchange Cloud Threat Exchange (CTE) is one of the most interesting and important modules. CTE allows customers to connect preventative tools such as EDR/EPP, email gateways, and threat intel platforms together to share IoC/IoA data. Integrations between these traditionally siloed protection tools strengthens a company's defense in depth and increases the ROI of all the tools within the environment. Netskope offers plugins for common prevention tools such as Proofpoint, Palo Alto Networks Panorama, Microsoft Defender, and STIX/TAXII. Cloud Risk Exchange The Cloud Risk Exchange (CRE) module is similar to CTE. However, instead of sharing threat data, CTE exchanges risk scores between platforms. CTE historically only shared user risk scores. Traditionally, security tools held their own risk engine—whether from a UEBA capability or based on another scoring algorithm. But users could never share this risk posture out to other tools. This all changed in early 2022, when applications gained the ability to exchange application risk scores within Cloud Exchange. By sharing risk scores, organizations can enable and adopt zero-trust principles across the customer ecosystem. Netskope offers plugins for common products that have risk engines such as CrowdStrike, Okta, and Google BeyondCorp. https://www.optiv.com/insights/discover/blog/integrate-all-things-netskope-cloud-exchange Netskope Unveils Cloud Threat Exchange, Enabling Peer-to-Peer Sharing of Threat Intelligence in the Cloud <i>A first of its kind, with Cloud Threat Exchange, technology vendors and customers can share cloud threat intelligence with each other to improve their overall threat prevention posture</i>

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Cloud Threat Exchange features include: • Facilitates the exchange of threat indicators between vendors, including file hashes, malicious URLs, and DLP file signatures, thus providing customers with fast, up-to-date protection across their security investments. • Reduces time between new threat discovery and protection implementation, allowing organizations to keep up with the ever-evolving threat landscape. • Establishes full IOC exchange with leading security providers, including endpoint detection and response, threat intelligence, managed detection and response, email security, and ticket management systems. Other vendors are easily added by customers or partners building their own plug-ins. • Works with indicators delivered via STIX/TAXII standards enabling information sharing for real-time network defense. Netskope Unveils Cloud Threat Exchange, Enabling Peer-to-Peer Sharing of Threat Intelligence in the Cloud - Netskope “Netskope Threat Labs leverages anonymized usage data collected from the Netskope Security Cloud platform to gain visibility into cloud app usage on managed devices.” Netskope Threat Labs: Combating Security Threats SANTA CLARA, Calif., Sept. 3, 2020 /PRNewswire/ -- Netskope, the leading security cloud, today announced the Cloud Threat Exchange, one of the industry's first cloud-based solutions for the ingestion, curation, and real-time sharing of threat intelligence across enterprise security enforcement points. With this announcement, Netskope has made the Cloud Threat Exchange free and open to customers that wish to use the technology to collaborate on sharing indicators of compromise (IOCs). Any certified, partner, vendor, or customer may use Cloud Threat Exchange to automate the delivery and distribution of high-value, actionable threat intelligence, thus reducing the time to protection and eliminating gaps in coverage. Cloud Threat Exchange is supported by a wide range of members certified by Netskope, which include VMware Carbon Black, CrowdStrike, Cyberason, Mimecast, SentinelOne, and ThreatQuotient. Together, this ecosystem helps mutual customers maximize the benefit of their protections by leveraging threat intelligence across multiple enforcement points. Netskope Unveils Cloud Threat Exchange, Enabling Peer-to-Peer Sharing of Threat Intelligence in the Cloud

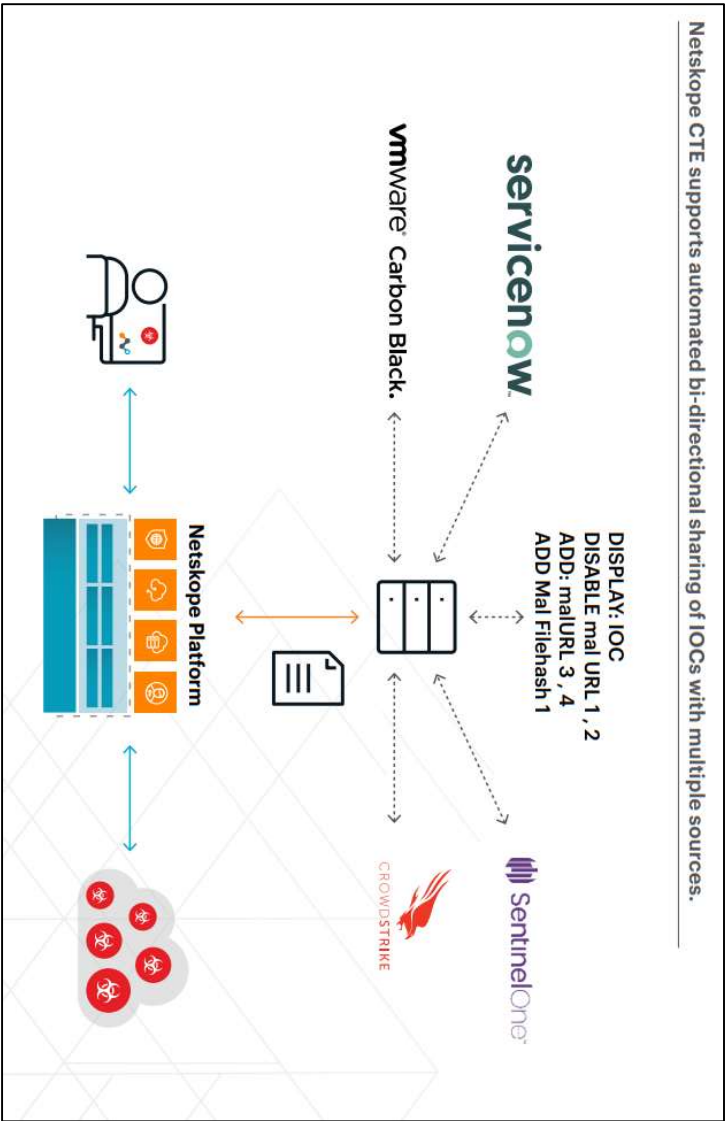
U.S. Patent No. <u>12,126,695</u>		Exemplary Evidence of Infringement
		• Share threat intelligence. Automate bidirectional IOC sharing between your defenses including Netskope, endpoints, email gateways, and SIEMs.
		https://www.netskope.com/wp-content/uploads/2021/11/2025-07-Netskope-Cloud-Exchange-SB-505-5.pdf
		• Exchange risk scores. Normalize multiple risk scores and invoke investigations for significant changes in user, device and application risk scoring.
		https://www.netskope.com/wp-content/uploads/2021/11/2025-07-Netskope-Cloud-Exchange-SB-505-5.pdf
		The Accused '695 Products include receiving information describing configuration settings used to combat the security threat.
I[c]: receiving information describing configuration settings used to combat the		For example, Netskope Cloud Exchange includes Netskope customers receiving “up-to-the-minute intelligence feeds that contain malicious URLs and file hashes” to integrate the same “into their security infrastructure products such as endpoints, firewalls, secure web-gateways, and cloud access

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
security threat; and	security brokers.” Netskope Cloud Threat Exchange - Netskope. Additionally, Netskope Cloud Exchange receives information regarding the Indicators of Compromise that are shared with a Netskope customer, including the reputation score of the indicator, a type associated with the indicator (e.g., whether the indicator is a “MD5” type, “SHA256” type, “URL” type, etc.) This information informs the Netskope customer’s “security cloud” on what security settings are changed as a result of the IoCs (e.g., what block and/or allow lists for hashes, URLs, etc. should be updated). This information determines how Netskope and/or Netskope customers utilize the IoCs that Cloud Exchange receives to combat the security threat associated with each IoC. Threat Exchange URL Handling Netskope Threat Exchange enables the sharing of IoC from 3rd-party platforms to and from Netskope (and each other). Though originally designed for managing attack indicators, it has evolved to support additional use cases including synchronizing and managing secure web gateway (SWG) to allow and block lists, populating SSL interception or bypass lists for CASB and SWG, and surfacing file hash information for Github repositories to prevent this data from being inappropriately shared using Netskope’s inline DLP functionality. Netskope will accept URLs, MD5 hashes, SHA256 hashes, IPv4 addresses, IPv6 addresses, hostnames, domains, and fully qualified domain names (FQDNs) to be used in the custom URL file for invocation as a destination match in a Netskope Real-time policy. The custom URL file must be used in policy, but that policy can result in any of the supported inline outcomes, including, but not limited to: block, alert, coach, justify, etc. https://docs.netskope.com/en/configure-threat-exchange-ioc-sharing

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	• Enable bi-directional threat intelligence sharing for Netskope solutions providing Advanced Threat Protection, including Next Generation Secure Web Gateway (NG SWG) • Selectively manage timely indicators of compromise (IOCs) throughout your security stack including malicious URLs and file hashes • Expands on pre-defined integrations for Netskope, Endpoint Security, Incident Response (IR), SIEMs, and other security solutions, plus define new custom integrations netskope-cloud-threat-exchange.pdf

<u>U.S. Patent No.</u> <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	HOW NETSKOPE CTE WORKS CTE is a light-weight collection of Docker applications that ingests, manages, and shares IOCs. Out of the box integrations include: CrowdStrike Falcon, VMware Carbon Black Cloud, SentinelOne, and ServiceNow. In addition, customers can add their own plug-ins to enable sharing between CTE and their own IT systems and/or scripts. Sharing threat intelligence is configurable between any two connected systems. For instance, a customer can facilitate sharing between different endpoint providers or even multiple Netskope cloud tenants. The CTE dashboard provides information on how frequently IOCs have been seen and from what systems, enabling customers to determine the scope of an attack surface. Customers can also configure when IOCs are timed-out due to staleness, plus choose which IOC sources to trust when they are provided with conflicting (e.g. 'safe' versus 'suspicious') information. As threat intelligence and IOCs are received via CTE, Netskope NG SWG customers can enforce real-time security enforcement, blocking user access to malicious sites or files that can endanger an organization's security posture.

Exemplary Evidence of Infringement



Trigger Workflows and Playbooks

Pervasive attacks and their IOCs can trigger IR workflows or orchestration playbooks to automate response steps making security analysts more efficient across multiple security tools.

[netskope-cloud-threat-exchange.pdf](#)

Data Model Properties			
Name	Type	Description ↑	
value	string	Indicator value. It can be MD5/SHA256 hash value in the case of Malware indicators, and domain-name/url in case of Malisite indicators.	
type	Enum (IndicatorType)	It can be IndicatorType.MD5 or IndicatorType.SHA256 in the case of Malware indicators. IndicatorType.URL in case of Malisite indicators.	
test	bool	Indicates whether it's a test indicator or not. Default – False	
reputation	int	Reputation score of indicator. Default – 5	
expiresAt	datetime.datetime	Time after which Indicator will be marked as inactive by Cloud Exchange.	

	firstSeen	datetime.datetime	datetime.datetime object indicating when the indicator was discovered for the first time. Default – Current System time when indicator object was created.
	lastSeen	datetime.datetime	datetime.datetime object indicating when the indicator was discovered for last time. Default – Current System time when indicator object was created.
	comments	string	Comment string which gives more information about the indicator.
	severity	Enum (SeverityType)	Severity of the indicator. Possible values are: SeverityType.LOW SeverityType.MEDIUM SeverityType.HIGH SeverityType.CRITICAL SeverityType.UNKNOWN
	https://docs.netskope.com/en/threat-exchange-custom-plugin-developers-guide		

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Netskope Cloud Threat Exchange (CTE) is a near real-time threat ingestion, curation, and sharing tool that enables Netskope customers and technology partners to bi-directionally exchange IOCs. Security teams can integrate up-to-the-minute intelligence feeds that contain malicious URLs and file hashes into their security infrastructure products such as endpoints, firewalls, secure web-gateways, and cloud access security brokers. For workflow and playbook automation, CTE can also integrate with IR, SIEM, SOAR, or custom API-based tools. Netskope Cloud Threat Exchange - Netskope Netskope Cloud Exchange is essentially a large API broker with four separate modules based on the type of data you want to share throughout your security stack. The Cloud Threat Exchange module allows us to share file hash and URL indicators between different tools through plugins. At the time, there was no plugin specifically for connecting to a Feedly stream, so we developed a custom CTE plugin that allows us to ingest IOCs found in our Feedly stream and automatically add them to objects serving as blocklists in our Netskope tenant. While an initial time investment was required to curate our Feedly stream and build the plugin, in the long run, this frees up time our analysts can use to be proactive in other areas, such as engaging in threat hunts.

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Not all IoCs are created equal; the context around them is essential to analysts understanding the risk they pose to your organization. With our plugin, we made sure that we included Traffic Light Protocol, TTPs, and a link to the original article where the IoC was found. This affords us more granularity when writing our business rules and subsequent sharing configurations within Netskope Cloud Exchange while also providing analysts with additional information and resources to understand potential threats. Utilizing Feedly for Threat Intelligence to track vulnerabilities in an organization's tech stack also provides the benefit of uncovering research where vulnerabilities are chained together to cause compromise of greater severity than any one vulnerability. Getting insights on the latest methodologies of chaining these vulnerabilities allows security teams to fully gauge the risk of vulnerable assets. Leveraging Feedly and Netskope Cloud Threat Exchange to Accelerate Threat Intelligence Gathering, Analysis, and Sharing - Netskope

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Manage Threat Exchange Business Rules and IoC Sharing Write-access users can configure Business Rules and IoC sharing. This section describes how to configure the initial business rules used to identify IoCs to be shared, and the IoC sharing configured between plugins (and therefore connected vendor systems) based on the invoked business rules. The result is system-detected IoC sharing between two plugged-in solutions of all IoCs matching the business rule. • Configure Threat Exchange Business Rules • Map a Threat Exchange Business Rule to a Target • View Threat Exchange Business Rules • Configure Threat Exchange IoC Sharing • IoC Sharing Best Practices • List IoCs and Use Filter Options https://docs.netkope.com/en/manage-threat-exchange-business-rules-and-ioc-sharing

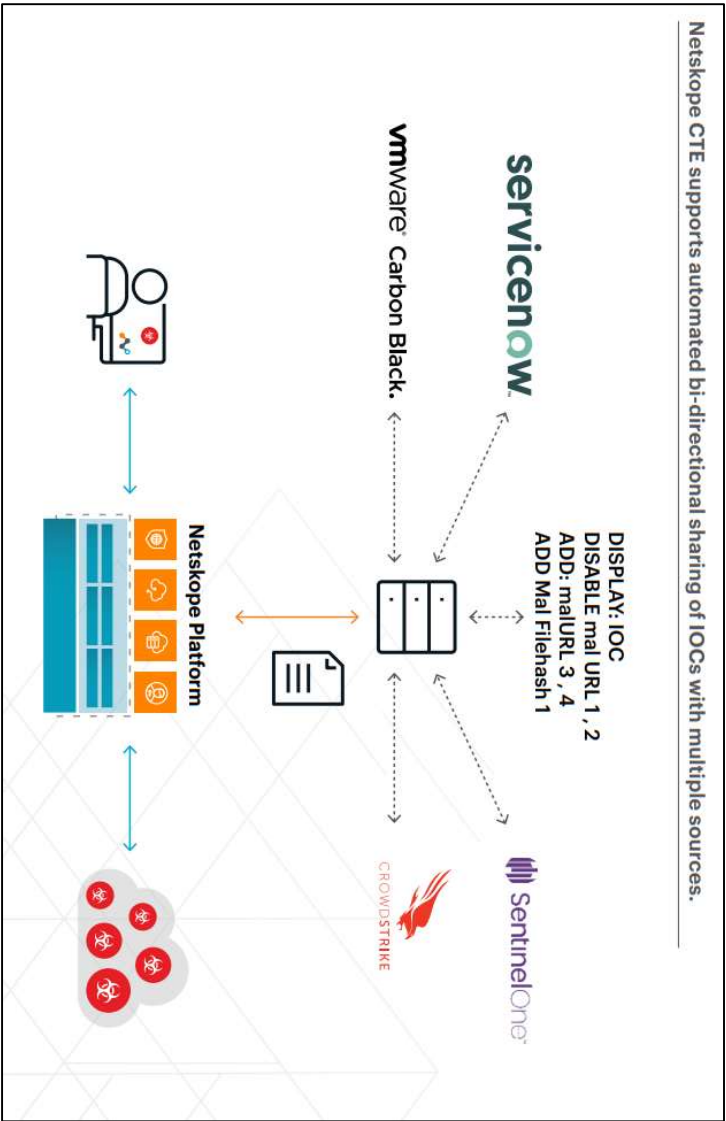
U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
	Threat Exchange URL Handling Netskope Threat Exchange enables the sharing of IoC from 3rd-party platforms to and from Netskope (and each other). Though originally designed for managing attack indicators, it has evolved to support additional use cases including synchronizing and managing secure web gateway (SWG) to allow and block lists, populating SSL interception or bypass lists for CASB and SWG, and surfacing file hash information for Github repositories to prevent this data from being inappropriately shared using Netskope's inline DLP functionality. Netskope will accept URLs, MD5 hashes, SHA256 hashes, IPv4 addresses, IPv6 addresses, hostnames, domains, and fully qualified domain names (FQDNs) to be used in the custom URL file for invocation as a destination match in a Netskope Real-time policy. The custom URL file must be used in policy, but that policy can result in any of the supported inline outcomes, including, but not limited to: block, alert, coach, justify, etc. To communicate with Netskope tenants, Threat Exchange uses the REST API V2 if it is enabled in the Netskope tenant and configured in Cloud Exchange, or REST API V1 if that is the only token either configured or available, as is the case for updating file hashes for use in threat prevention policies. https://docs.netskope.com/en/configure-threat-exchange-ioc-sharing

U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
1[d]: identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment.	The Accused '695 Products include identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment. For example, Netskope Cloud Exchange includes Netskope customers integrating the threat intelligence information received from other Netskope customers and/or cloud vendors. And Cloud Exchange “ingests, manages, and shares” information regarding the Indicators of Compromise that are received from third party cloud deployments, including information that identifies whether the IoC is a “malicious URL[,]” one or more “file hashes[,]” one or more “IPv4 addresses,” one or more “IPv6 addresses, hostnames, domains, [or] fully qualified domain names (FQDN)” for use in a Netskope policy. For example, that information is used by Netskope SWG to enforce the one or more Netskope Real-time policies. Accordingly, the one or more configurations to adopt can include one or more URLs, hash lists, IP addresses, or other information, to add to a block list and/or an allow list used by the customer’s Netskope SWG. Threat Exchange URL Handling Netskope Threat Exchange enables the sharing of IoC from 3rd-party platforms to and from Netskope (and each other). Though originally designed for managing attack indicators, it has evolved to support additional use cases including synchronizing and managing secure web gateway (SWG) to allow and block lists, populating SSL interception or bypass lists for CASB and SWG, and surfacing file hash information for Github repositories to prevent this data from being inappropriately shared using Netskope’s inline DLP functionality. Netskope will accept URLs, MD5 hashes, SHA256 hashes, IPv4 addresses, IPv6 addresses, hostnames, domains, and fully qualified domain names (FQDNs) to be used in the custom URL file for invocation as a destination match in a Netskope Real-time policy. The custom URL file must be used in policy, but that policy can result in any of the supported inline outcomes, including, but not limited to: block, alert, coach, justify, etc. To communicate with Netskope tenants, Threat Exchange uses the REST API V2 if it is enabled in the Netskope tenant and configured in Cloud Exchange, or REST API V1 if that is the only token either configured or available, as is the case for updating file hashes for use in threat prevention policies. https://docs.netskope.com/en/configure-threat-exchange-ioc-sharing

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Netskope Cloud Threat Exchange (CTE) is a near real-time threat ingestion, curation, and sharing tool that enables Netskope customers and technology partners to bi-directionally exchange IOCs. Security teams can integrate up-to-the-minute intelligence feeds that contain malicious URLs and file hashes into their security infrastructure products such as endpoints, firewalls, secure web-gateways, and cloud access security brokers. For workflow and playbook automation, CTE can also integrate with IR, SIEM, SOAR, or custom API-based tools. Netskope Cloud Threat Exchange - Netskope • Enable bi-directional threat intelligence sharing for Netskope solutions providing Advanced Threat Protection, including Next Generation Secure Web Gateway (NG SWG) • Selectively manage timely indicators of compromise (IOCs) throughout your security stack including malicious URLs and file hashes • Expands on pre-defined integrations for Netskope, Endpoint Security, Incident Response (IR), SIEMs, and other security solutions, plus define new custom integrations netskope-cloud-threat-exchange.pdf

U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
	HOW NETSKOPE CTE WORKS CTE is a light-weight collection of Docker applications that ingests, manages, and shares IOCs. Out of the box integrations include: CrowdStrike Falcon, VMware Carbon Black Cloud, SentinelOne, and ServiceNow. In addition, customers can add their own plug-ins to enable sharing between CTE and their own IT systems and/or scripts. Sharing threat intelligence is configurable between any two connected systems. For instance, a customer can facilitate sharing between different endpoint providers or even multiple Netskope cloud tenants. The CTE dashboard provides information on how frequently IOCs have been seen and from what systems, enabling customers to determine the scope of an attack surface. Customers can also configure when IOCs are timed-out due to staleness, plus choose which IOC sources to trust when they are provided with conflicting (e.g. ‘safe’ versus ‘suspicious’) information. As threat intelligence and IOCs are received via CTE, Netskope NG SWG customers can enforce real-time security enforcement, blocking user access to malicious sites or files that can endanger an organization’s security posture.

Exemplary Evidence of Infringement



Trigger Workflows and Playbooks

Pervasive attacks and their IOCs can trigger IR workflows or orchestration playbooks to automate response steps making security analysts more efficient across multiple security tools.

[netskope-cloud-threat-exchange.pdf](#)

Exemplary Evidence of Infringement

Netskope Cloud Exchange is essentially a large API broker with four separate modules based on the type of data you want to share throughout your security stack. The Cloud Threat Exchange module allows us to share file hash and URL indicators between different tools through plugins. At the time, there was no plugin specifically for connecting to a Feedly stream, so we developed a custom CTE plugin that allows us to ingest IoCs found in our Feedly stream and automatically add them to objects serving as blocklists in our Netskope tenant. While an initial time investment was required to curate our Feedly stream and build the plugin, in the long run, this frees up time our analysts can use to be proactive in other areas, such as engaging in threat hunts.

Not all IoCs are created equal; the context around them is essential to analysts understanding the risk they pose to your organization. With our plugin, we made sure that we included Traffic Light Protocol, TTPs, and a link to the original article where the IoC was found. This affords us more granularity when writing our business rules and subsequent sharing configurations within Netskope Cloud Exchange while also providing analysts with additional information and resources to understand potential threats.

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Utilizing Feedly for Threat Intelligence to track vulnerabilities in an organization's tech stack also provides the benefit of uncovering research where vulnerabilities are chained together to cause compromise of greater severity than any one vulnerability. Getting insights on the latest methodologies of chaining these vulnerabilities allows security teams to fully gauge the risk of vulnerable assets. Leveraging Feedly and Netskope Cloud Threat Exchange to Accelerate Threat Intelligence Gathering, Analysis, and Sharing - Netskope
2. The method of claim 1, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses.	The Accused '695 Products include information describing configuration settings that comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses. For example, the Netskope documentation below shows that Cloud Exchange includes "block lists," and "SSL interception ... lists" which can include "IPv4 addresses," and "IPv6 addresses."

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Threat Exchange URL Handling Netskope Threat Exchange enables the sharing of IoC from 3rd-party platforms to and from Netskope (and each other). Though originally designed for managing attack indicators, it has evolved to support additional use cases including synchronizing and managing secure web gateway (SWG) to allow and block lists, populating SSL interception or bypass lists for CASB and SWG, and surfacing file hash information for Github repositories to prevent this data from being inappropriately shared using Netskope's inline DLP functionality. Netskope will accept URLs, MD5 hashes, SHA256 hashes, IPv4 addresses, IPv6 addresses, hostnames, domains, and fully qualified domain names (FQDNs) to be used in the custom URL file for invocation as a destination match in a Netskope Real-time policy. The custom URL file must be used in policy, but that policy can result in any of the supported inline outcomes, including, but not limited to: block, alert, coach, justify, etc. To communicate with Netskope tenants, Threat Exchange uses the REST API V2 if it is enabled in the Netskope tenant and configured in Cloud Exchange, or REST API V1 if that is the only token either configured or available, as is the case for updating file hashes for use in threat prevention policies. https://docs.netskope.com/en/configure-threat-exchange-ioc-sharing
3. The method of claim 1, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist	The Accused '695 Products include configuration settings that comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more network domains. For example, the Netskope documentation below shows that Cloud Exchange includes “block lists,” and “SSL interception ... lists” which can include “domains, and fully qualified domain names (FQDNs).”

U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
one or more network domains.	Threat Exchange URL Handling Netskope Threat Exchange enables the sharing of IoC from 3rd-party platforms to and from Netskope (and each other). Though originally designed for managing attack indicators, it has evolved to support additional use cases including synchronizing and managing secure web gateway (SWG) to allow and block lists, populating SSL interception or bypass lists for CASB and SWG, and surfacing file hash information for Github repositories to prevent this data from being inappropriately shared using Netskope's inline DLP functionality. Netskope will accept URLs, MD5 hashes, SHA256 hashes, IPv4 addresses, IPv6 addresses, hostnames, domains, and fully qualified domain names (FQDNs) to be used in the custom URL file for invocation as a destination match in a Netskope Real-time policy. The custom URL file must be used in policy, but that policy can result in any of the supported inline outcomes, including, but not limited to: block, alert, coach, justify, etc. To communicate with Netskope tenants, Threat Exchange uses the REST API V2 if it is enabled in the Netskope tenant and configured in Cloud Exchange, or REST API V1 if that is the only token either configured or available, as is the case for updating file hashes for use in threat prevention policies. https://docs.netskope.com/en/configure-threat-exchange-ioc-sharing
5[pre]. The method of claim 1 further comprising:	The Accused '695 Products include the method of claim 1.
5[a] receiving information describing one or more actions associated with the additional cloud	The Accused '695 Products receive information describing one or more actions associated with the additional cloud deployments either literally or under the doctrine of equivalents. For example, Netskope's Cloud Threat Exchange allows Netskope (or its customers) to receive information for one cloud vendor that describes a

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
deployments; and	security threat to one or more additional cloud vendors (e.g., “Peer-to-Peer Sharing of Threat Intelligence”), including, in one example, the URL and/or Hash (SHA256, MD5, etc.) for the security threat to one or more of the additional cloud deployments. Threat Exchange URL Handling Netskope Threat Exchange enables the sharing of IoC from 3rd-party platforms to and from Netskope (and each other). Though originally designed for managing attack indicators, it has evolved to support additional use cases including synchronizing and managing secure web gateway (SWG) to allow and block lists, populating SSL interception or bypass lists for CASB and SWG, and surfacing file hash information for Github repositories to prevent this data from being inappropriately shared using Netskope’s inline DLP functionality. Netskope will accept URLs, MD5 hashes, SHA256 hashes, IPv4 addresses, IPv6 addresses, hostnames, domains, and fully qualified domain names (FQDNs) to be used in the custom URL file for invocation as a destination match in a Netskope Real-time policy. The custom URL file must be used in policy, but that policy can result in any of the supported inline outcomes, including, but not limited to: block, alert, coach, justify, etc. https://docs.netskope.com/en/configure-threat-exchange-ioc-sharing

U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
	Configure 3rd-party Threat Exchange Plugins Only admins and write-access users can configure 3rd-party Threat Exchange plugins. Threat Exchange comes with a library of supported plugins. Plugins can be easily configured to collect and share indicators related to file hashes of malicious software (malware) used in a Netskope DLP policy by following the plugin guide. Refer to the Threat Exchange Custom Plugin Developers Guide to understand how to build and upload a custom plugin. You can also disable, enable, or delete existing plugin configurations. Threat Exchange can be configured with multiple plugins to the same system for different workflows from either the same Netskope tenant or multiple Netskope tenants. Threat Exchange ONLY pulls the following IoC's when they are available: 1. Malicious file file hashes in MD5 or SHA256 format. 2. URL: Depending on the nature of the plugin, these could be malicious URL, restricted URL, or allowed URL. The latter two would be for firewall, SWG, or CASB policy synchronization. Fetching malicious Hostnames, Domains and FQDNs are also supported. 3. IP addresses (CIDR): Depending on the nature of the plugin, these could be malicious IP (IPv4/IPv6), restricted IP, or allowed IP. The latter two would be for firewall, SWG, or CASB policy synchronization. https://docs.netskope.com/en/configure-3rd-party-threat-exchange-plugins

Data Models

This section lists down the Data Models and their properties.

Indicator Type Model

- This class provides the Python data model for an IndicatorType object.
- This model has 3 fields: URL, SHA256, MD5 of type string.
- You will interact with the model in the pushmethod as you sending a list of indicators to thirdparty.

Data Model Properties

Name	Type	Description
URL	string	It can be used for URLs
SHA256	string	It can be used for sha256 typ of file hashes
MD5	string	It can be used for md5 type of file hashes

<https://docs.netiskope.com/en/threat-exchange-custom-plugin-developers-guide>

U.S. Patent No. <u>12.126.695</u>	Exemplary Evidence of Infringement
	Cloud Threat Exchange Cloud Threat Exchange (CTE) is one of the most interesting and important modules. CTE allows customers to connect preventative tools such as EDR/EPP, email gateways, and threat intel platforms together to share IoC/IoA data. Integrations between these traditionally siloed protection tools strengthens a company's defense in depth and increases the ROI of all the tools within the environment. Netskope offers plugins for common prevention tools such as Proofpoint, Palo Alto Networks Panorama, Microsoft Defender, and STIX/TAXII. Cloud Risk Exchange The Cloud Risk Exchange (CRE) module is similar to CTE. However, instead of sharing threat data, CTE exchanges risk scores between platforms. CTE historically only shared user risk scores. Traditionally, security tools held their own risk engine—whether from a UEBA capability or based on another scoring algorithm. But users could never share this risk posture out to other tools. This all changed in early 2022, when applications gained the ability to exchange application risk scores within Cloud Exchange. By sharing risk scores, organizations can enable and adopt zero-trust principles across the customer ecosystem. Netskope offers plugins for common products that have risk engines such as CrowdStrike, Okta, and Google BeyondCorp. https://www.optiv.com/insights/discover/blog/integrate-all-things-netskope-cloud-exchange To the extent that claim 5[a] is not literally met by the Accused '695 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '695 Products are insubstantial and make no material difference. The Accused '695 Products performs substantially the same function in substantially the same way to obtain substantially the same result as claim 5[a]. For example, Netskope Cloud Exchange may receive information from third party cloud deployments that includes a URL and/or hash, or an IP address to be added to a blocklist. But receiving a URL and/or Hash to include in a blocklist is insubstantially different from information indicating the third party cloud deployment itself added the URL and/or Hash to its own blocklist, or an IP address, hostname, domain or FQDN will notify prospective users that have attempted to communicate with the third party cloud deployment, which would require performing substantially the same function of informing the cloud deployment of potential issues with third party cloud deployments, in substantially the same way by exchanging information that can be used to inform the cloud deployment's actions, to obtain substantially the same result of protecting the cloud deployment against potential threats. The Accused '695 Products receive information describing one or more actions associated with the additional cloud deployments.
5[b] wherein identifying the one or more configurations to adopt for the first cloud deployment is further based on the one or more actions.	For example, Netskope Cloud Exchange includes Netskope customers integrating the threat intelligence information received from other Netskope customers and/or cloud vendors. And Cloud Exchange "ingests, manages, and shares" information regarding the Indicators of Compromise that are received from third party cloud deployments, including information that identifies whether the IoC is a "malicious URL[,] " one or more "file hashes[,] " one or more "IPv4 addresses," one or more "IPv6 addresses, hostnames, domains, [or] fully qualified domain names (FQDN)" for use in a

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Netskope policy. For example, that information is used by Netskope SWG to enforce the one or more Netskope Real-time policies. Accordingly, the one or more configurations to adopt can include one or more URLs, hash lists, IP addresses, or other information, to add to a block list and/or an allow list used by the customer's Netskope SWG. Threat Exchange URL Handling Netskope Threat Exchange enables the sharing of IoC from 3rd-party platforms to and from Netskope (and each other). Though originally designed for managing attack indicators, it has evolved to support additional use cases including synchronizing and managing secure web gateway (SWG) to allow and block lists, populating SSL interception or bypass lists for CASB and SWG, and surfacing file hash information for Github repositories to prevent this data from being inappropriately shared using Netskope's inline DLP functionality. Netskope will accept URLs, MD5 hashes, SHA256 hashes, IPv4 addresses, IPv6 addresses, hostnames, domains, and fully qualified domain names (FQDNs) to be used in the custom URL file for invocation as a destination match in a Netskope Real-time policy. The custom URL file must be used in policy, but that policy can result in any of the supported inline outcomes, including, but not limited to: block, alert, coach, justify, etc. To communicate with Netskope tenants, Threat Exchange uses the REST API V2 if it is enabled in the Netskope tenant and configured in Cloud Exchange, or REST API V1 if that is the only token either configured or available, as is the case for updating file hashes for use in threat prevention policies. https://docs.netskope.com/en/configure-threat-exchange-ioc-sharing

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Netskope Cloud Threat Exchange (CTE) is a near real-time threat ingestion, curation, and sharing tool that enables Netskope customers and technology partners to bi-directionally exchange IOCs. Security teams can integrate up-to-the-minute intelligence feeds that contain malicious URLs and file hashes into their security infrastructure products such as endpoints, firewalls, secure web-gateways, and cloud access security brokers. For workflow and playbook automation, CTE can also integrate with IR, SIEM, SOAR, or custom API-based tools. Netskope Cloud Threat Exchange - Netskope • Enable bi-directional threat intelligence sharing for Netskope solutions providing Advanced Threat Protection, including Next Generation Secure Web Gateway (NG SWG) • Selectively manage timely indicators of compromise (IOCs) throughout your security stack including malicious URLs and file hashes • Expands on pre-defined integrations for Netskope, Endpoint Security, Incident Response (IR), SIEMs, and other security solutions, plus define new custom integrations netskope-cloud-threat-exchange.pdf

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
	Additionally, the Accused '695 Products include claim 5[a], either literally or under the doctrine of equivalents. To the extent that claim 5[a] is not literally met by the Accused '695 Products, it is satisfied under the doctrine of equivalents because any differences between the claimed invention and the Accused '695 Products are insubstantial and make no material difference. The Accused '695 Products performs substantially the same function in substantially the same way to obtain substantially the same result as claim 5[a]. For example, Netskope Cloud Exchange may receive information from third party cloud deployments that includes a URL and/or hash to be added to a blocklist. But receiving a URL and/or Hash to include in a blocklist is insubstantially different from information indicating the third party cloud deployment itself added the URL and/or Hash to its own blocklist, which would require performing substantially the same function in substantially the same way to obtain the same result.
8. The method of claim 1 further comprising receiving information describing one or more deployment processes associated with the additional cloud deployments.	The Accused '695 Products include the method of claim 1 further comprising receiving information describing one or more deployment processes associated with the additional cloud deployments. For example, the Accused '695 Products receive information (<i>e.g.</i>, via Cloud Exchange) that includes information regarding the deployment of Indicators of Compromise.

Data Model Properties			
Name	Type	Description ↑	
value	string	Indicator value. It can be MD5/SHA256 hash value in the case of Malware indicators, and domain-name/url in case of Malisite indicators.	
type	Enum (IndicatorType)	It can be IndicatorType.MD5 or IndicatorType.SHA256 in the case of Malware indicators. IndicatorType.URL in case of Malisite indicators.	
test	bool	Indicates whether it's a test indicator or not. Default – False	
reputation	int	Reputation score of indicator. Default – 5	
expiresAt	datetime.datetime	Time after which Indicator will be marked as inactive by Cloud Exchange.	

	firstSeen	datetime.datetime	datetime.datetime object indicating when the indicator was discovered for the first time. Default – Current System time when Indicator object was created.
	lastSeen	datetime.datetime	datetime.datetime object indicating when the indicator was discovered for last time. Default – Current System time when Indicator object was created.
	comments	string	Comment string which gives more information about the indicator.
	severity	Enum (SeverityType)	Severity of the indicator. Possible values are: SeverityType.LOW SeverityType.MEDIUM SeverityType.HIGH SeverityType.CRITICAL SeverityType.UNKNOWN

U.S. Patent No. <u>12,126,695</u>	Exemplary Evidence of Infringement
	Threat Exchange URL Handling Netskope Threat Exchange enables the sharing of IoC from 3rd-party platforms to and from Netskope (and each other). Though originally designed for managing attack indicators, it has evolved to support additional use cases including synchronizing and managing secure web gateway (SWG) to allow and block lists, populating SSL interception or bypass lists for CASB and SWG, and surfacing file hash information for Github repositories to prevent this data from being inappropriately shared using Netskope's inline DLP functionality. Netskope will accept URLs, MD5 hashes, SHA256 hashes, IPv4 addresses, IPv6 addresses, hostnames, domains, and fully qualified domain names (FQDNs) to be used in the custom URL file for invocation as a destination match in a Netskope Real-time policy. The custom URL file must be used in policy, but that policy can result in any of the supported inline outcomes, including, but not limited to: block, alert, coach, justify, etc. To communicate with Netskope tenants, Threat Exchange uses the REST API V2 if it is enabled in the Netskope tenant and configured in Cloud Exchange, or REST API V1 if that is the only token either configured or available, as is the case for updating file hashes for use in threat prevention policies. https://docs.netskope.com/en/configure-threat-exchange-ioc-sharing To the extent the Accused '695 Products do not practice claim 8 literally, it practices this claim under the doctrine of equivalents because any differences between the claimed invention and the Accused '695 Products are insubstantial and make no material difference. The Accused '695 Products performs substantially the same function in substantially the same way to obtain substantially the same result as claim 8. For example, Netskope Cloud Exchange may receive information from third party cloud deployments that can include include information concerning the name of the file associated with an identified threat, which is insubstantially different from information concerning the deployment processes employed in the cloud deployment as the file name (as incorporated in the "comment" field) can establish the component (e.g., program) within the cloud deployment associated with the identified threat.

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
9[pre]. A system for learning from other cloud deployments to combat security threats, the system comprising at least one processor and memory storing computer program instructions that, when executed, cause the system to carry out the steps of:	The Accused '695 Products include a system for learning from other cloud deployments to combat security threats, the system comprising at least one processor and memory storing computer program instructions.
9[a]. identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning;	The Accused '695 Products include identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning. <i>See, e.g., claim 1[a].</i>
9[b]. receiving information describing a security threat to one or more of the additional cloud deployments;	The Accused '695 Products include receiving information describing a security threat to one or more of the additional cloud deployments. <i>See, e.g., claim 1[b].</i>
9[c]. receiving information describing configuration settings used to combat the security threat; and	The Accused '695 Products include receiving information describing configuration settings used to combat the security threat. <i>See, e.g., claim 1[c].</i>
9[d]. identifying, based on the information describing	The Accused '695 Products include identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment.

<u>U.S. Patent No.</u> <u>12.126.695</u>		<u>Exemplary Evidence of Infringement</u>
configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment.		<i>See, e.g., claim 1[d].</i>
10. The system of claim 9, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses.	The Accused '695 Products include the system of claim 9, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses. <i>See, e.g., claim 2.</i>	
11. The system of claim 9, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more network domains.	The Accused '695 Products include the system of claim 9, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more network domains. <i>See, e.g., claim 3.</i>	
13[pre]. The system of claim 9, wherein the steps further comprise:	The Accused '695 Products include the system of claim 9.	
13[a]. receiving information describing	The Accused '695 Products include receiving information describing one or more actions associated with the additional cloud deployments.	

U.S. Patent No. <u>12,126,695</u>	<u>Exemplary Evidence of Infringement</u>
one or more actions associated with the additional cloud deployments; and	<i>See, e.g., claim 5[a].</i>
13[b]. wherein identifying the one or more configurations to adopt for the first cloud deployment is further based on the one or more actions.	The Accused '695 Products include wherein identifying the one or more configurations to adopt for the first cloud deployment is further based on the one or more actions. <i>See, e.g., claim 5[b].</i>
16. The system of claim 9 wherein the steps further comprise receiving information describing one or more deployment processes associated with the additional cloud deployments.	The Accused '695 Products include the system of claim 9 wherein the steps further comprise receiving information describing one or more deployment processes associated with the additional cloud deployments. <i>See, e.g., claim 8.</i>
17[pre]. A computer program product for learning from other cloud deployments to combat security threats, the computer program product disposed on a non-transitory computer readable medium, the computer program product including computer	The Accused '695 Products include a computer program product for learning from other cloud deployments to combat security threats, the computer program product disposed on a non-transitory computer readable medium, the computer program product including computer instructions.

U.S. Patent No. <u>12.126.695</u>		Exemplary Evidence of Infringement
program instructions that, when executed, carry out the steps of:		
17[a]. identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning;	The Accused '695 Products include identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning. <i>See, e.g.,</i> claim 1[a].	
17[b]. receiving information describing a security threat to one or more of the additional cloud deployments;	The Accused '695 Products include receiving information describing a security threat to one or more of the additional cloud deployments. <i>See, e.g.,</i> claim 1[b].	
17[c]. receiving information describing configuration settings used to combat the security threat; and	The Accused '695 Products include receiving information describing configuration settings used to combat the security threat. <i>See, e.g.,</i> claim 1[c].	
17[d]. identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment.	The Accused '695 Products include identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment. <i>See, e.g.,</i> claim 1[d].	
18. The computer program	The Accused '695 Products include the computer program product of claim 17, wherein the configuration settings comprise configuration settings	

<u>U.S. Patent No.</u> <u>12.126.695</u>		<u>Exemplary Evidence of Infringement</u>
product of claim 17, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses.		that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses. <i>See, e.g., claim 2.</i>
19. The computer program product of claim 17, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more network domains.		The Accused '695 Products include the computer program product of claim 17, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more network domains. <i>See, e.g., claim 3.</i>