Netskope Active Threat Protection™

At a glance:

- Netskope Active Threat Protection protects your organization with the most advanced cloud threat defense solution.
- Provides you with 360-degree cloud vantage point covering on-premises, remote, and mobile users.
- Automatically prioritizes threat protection and defends with remediation built for the cloud.
- Integrates with industry leaders for best-of-breed malware defense solution.

Overview

The cloud makes it extremely simple to be productive, collaborate and share data. While organizations and employees love using the cloud for these and its various other benefits, the underlying mechanism that cloud services put in place, especially to facilitate sync and sharing capabilities, can as easily be used as a propagation channel for malware. With these established channels, more than 900 cloud apps in the average enterprise, and one-third of business data now in the cloud, organizations are largely unprotected from cloud-based malware. Organizations need a solution that understands the complex threat landscape, can efficiently and accurately detect malware en-route to and from the cloud as well as resident in the cloud, and effectively remediate and protect against threats.

Introducing Netskope Active Threat Protection

From risky apps and users, to anomalous or non-compliant behavior, to compromised credentials and malware, threats come in various forms, each with its own severity and potential negative impact on an organization. In order to ensure protection against these threats, Netskope Active Threat Protection provides organizations with the most advanced defense against cloud threats across all these attack vectors. Unlike other vendors who only see 5 percent of cloud traffic because of their limited deployment options, Netskope is able to see all cloud app traffic and therefore has the most effective coverage.

How it works

Cloud threat protection begins when Netskope is first introduced in your organization using any one of its broad architectural deployment options. Netskope uncovers all cloud app usage, compiles a list of apps in use in your organization, and then uses advanced analytics to determine your riskiest users and their behavior. Along with determining risky users, Netskope Active Threat Protection also uncovers and surfaces information about whether any of your users have had their credentials compromised in a data breach or hack.

Additionally, the Netskope anomaly detection engine works behind the scenes using sophisticated machine-learning algorithms to continuously monitor user behavior. It then intelligently establishes a baseline and uses it to discover anomalous behavioral patterns, which could indicate risky activity. These risky behaviors could be failed logins, unnecessary sharing of credentials, users logging in from risky locations or unknown devices, data exfiltration activity such as downloading sensitive data from a sanctioned app and then uploading that same content to an unsanctioned app, and many more.

Next the platform proactively monitors and defends your organization against malware such as viruses, worms, Trojans, spyware and ransomware. The platform provides a rich set of malware detection capabilities including scanning for malicious IPs and URLs, static checks, static analysis, dynamic analysis such as sandboxing, and user entity behavioral analytics that automatically prioritize to ensure the most efficient and accurate threat detection capabilities. All of these elements come together to provide you with a comprehensive risk dashboard.

Remediation

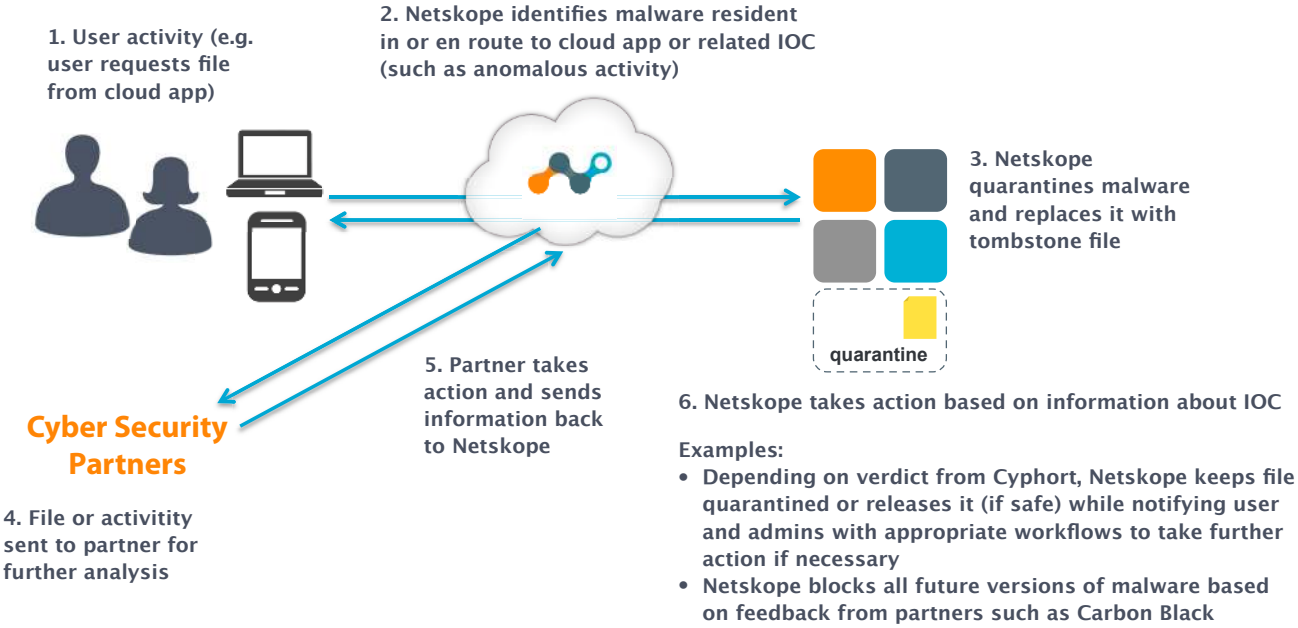
Once you've found the true representation of your organization's risk, you can easily use Netskope Active Threat Protection to progress from knowing into actively defending against these threats. Netskope Active Threat Protection provides you with workflows such as quarantine, which will automatically replace a file that has been determined to contain malware, with a tombstone file, and notify the user and admin that the file has been moved until further notice.

When the file is quarantined, it is zipped and placed in a password-protected archive that only you can access should you want to run additional forensics or attempt to clean. In the event that Netskope is not used to remediate malware, Netskope Active Threat Protection also provides you with an audit trail and context of users affected, as well as a visualization of the timeline of malware propagation.

Additionally, you can seamlessly integrate with your existing on-premises endpoint detection and response (EDR) or sandbox vendors to provide a more integrated experience that allows you to leverage any investments you've already made. You can also send automatic alerts to your security information and event management (SIEM) or security operations center (SOC) systems to take action on-premises.

This ability is brought about by the extensible Netskope threat intelligence platform that can seamlessly snap-in to your existing endpoint, network, and threat infrastructure using STIX/TAXII and OpenIOC standards to effectively establish a closed loop two-way communication channel between the cloud and your premises.

Figure 1. Third-party integrations



In order to provide the industry's best malware defense solution Netskope has integrated with industry leaders such as Cyphort and Carbon Black. These integrations allow organizations to include next-generation advanced persistent threat (APT) defense, and expansion of their kill chain view, to cloud apps and cloud-based malware. Netskope's 360-degree cloud vantage point allows the surgical view of content and activities en-route to and from sanctioned and unsanctioned cloud apps, as well as resident in those apps, for users and devices that are on-premises, remote or mobile. This includes unparalleled context such as the user, their device, their Active Directory group, the activity they're performing, the type of file they're dealing with, and very detailed information about the app.

On detecting content that is suspected of containing malware, Netskope Active Threat Protection can pass the suspected violation along with the rich contextual details to an on-premises next-generation APT defense solution, a dynamic threat protection solution to initiate sandboxing, or an end-point remediation solution. At the same time, Netskope provides you with an intuitive policy engine that allows you to define who should be notified of this event, such as the administrator and the user, as well as the action that should be taken. Based on figure 1 above, below are examples of actions that Netskope partners can take in step 5 with our information exchange.

- Cyphort identifies as malware and instructs enterprise network to break kill chain.
- Carbon Black takes action on the threat or anomaly such as network or file activity. If the malware has not yet reached the endpoint, it can watch for and block the malware. If the malware has reached the endpoint but not yet detonated, it can delete it. If the malware has reached the endpoint and has detonated, it can kill its processes and isolate the endpoint.

In the case of an endpoint solution, Netskope Active Threat Protection can alert the endpoint of the malware. If the malware has not yet reached the endpoint, the endpoint solution can anticipate it and block it before it executes. If it has already executed, the endpoint solution can kill the associated processes and isolate the end-point. In the case of next-generation APT or dynamic threat defense solutions, Netskope Active Threat Protection can route suspicious files to the on-premises solution and based on the result of the analysis and the policy configuration, quarantine and block future activity with those files.

Netskope Differentiators

Only Netskope provides you with:

ACTIVE THREAT PROTECTION – The industry's only machine learning-based anomaly detection solution that is multi-dimensional, adaptable, and provides prioritized analysis and remediation of threats.

ADVANCED, ENTERPRISE DLP – Efficient cloud DLP that leverages existing on-premises DLP solutions and dramatically reduces false positives.

GRANULAR POLICIES FOR ALL APPS – Granular visibility and governance of all cloud app usage, whether sanctioned or unsanctioned.

ARCHITECTED FOR ANY USE CASE – Largest variety of flexible deployment options to satisfy all current and future use cases and needs.

About Netskope

Netskope™, the leading cloud access security broker (CASB), helps enterprises find, understand and secure sanctioned and unsanctioned cloud apps. Through contextual awareness and a multi-mode architecture, Netskope sees the cloud differently. This results in the deepest visibility and control, the most advanced threat protection and data loss prevention and an unmatched breadth of security policies and workflows. The world's largest companies choose Netskope, the only CASB that ensures compliant use of cloud apps in real-time, whether accessed on the corporate network, remotely or from a mobile device. With Netskope, enterprises move fast, with confidence. To learn more, visit our website.