cybereason | netskope

SOLUTION BRIEF

NETSKOPE AND CYBEREASON

The increasing use of cloud services and the ability to access them from any device makes both the cloud and the endpoint critical points of control. By providing a comprehensive view of threats across the cloud and endpoints, Netskope and Cybereason help organizations prevent, detect and respond more quickly and effectively to even the most complex of threats.

QUICK GLANCE

- Comprehensive and synchronized view of threats across cloud and endpoints
- Shared threat intelligence between cloud and endpoint
- Custom detections and automated remediation at the endpoint
- Adaptive access control based on endpoint security posture

Cybereason and Netskope Overview

The increasing use of cloud services coupled with the ability to access these cloud services from anywhere and from any device has dissolved the traditional enterprise perimeter. Today, the focus is moving to cloud services and endpoints as the enterprise's most critical control points. The Cybereason Cyber Defense Platform combines the industry's top-rated detection and response (EDR and XDR), multi-layered next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a Malop (malicious operation). Netskope provides comprehensive visibility and control of cloud services, including advanced, multi-layered threat protection. The result: defenders can end cyber attacks from endpoints to everywhere.

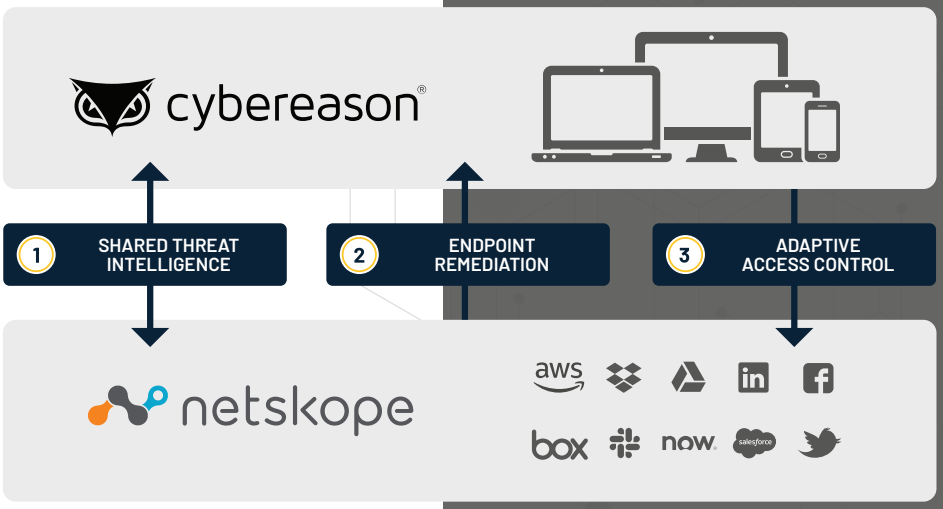
Together, Cybereason and Netskope deliver a comprehensive view of threats across the cloud and endpoints and work together to respond more quickly and effectively to today's threats. By sharing threat intelligence between Netskope and Cybereason, emerging threats can be quickly identified and neutralized across the organization. As new threats are discovered in the cloud, Netskope can coordinate with the Cybereason Defense Platform to rapidly remediate at the endpoint. Finally, Netskope is able to classify devices accessing cloud services and limit access to trusted devices secured by Cybereason.

Key Use Cases

Threat Intelligence Shared Between Cloud and Endpoint

Shared threat intelligence helps organizations get more value from their cloud and endpoint security investments. Netskope and Cybereason are able to exchange threat intelligence such as malicious file hashes between the cloud and the endpoint. This allows Netskope to more efficiently identify and protect against emerging, high-risk threats originally detected on endpoints by Cybereason. In a similar manner, Netskope can enrich Cybereason with the latest threat intelligence based on newly discovered threats in the cloud and web.

Closed-Loop Remediation Between Cloud and Endpoint



Netskope is able to detect and remediate threats such as malware both detected on or en route to cloud services. To close the loop for newly discovered cloud threats, Netskope integrates with Cybereason to drive remediation across an organization's endpoints as well. When new malware is discovered in the cloud, Netskope is able to pass the malicious file hash to the Cybereason Cyber Defense Platform for remediation. Based on the file hash, the Cybereason Cyber Defense Platform provides multiple remediation options to respond quickly and effectively to new threats, including alerting on affected endpoints, banning the malicious file from running on endpoints, and isolating affected endpoints from the rest of the network. Similarly, joint customers can configure Netskope Threat Prevention to leverage the hashes provided by Cybereason to remove, hold for inspection, or alert on matching malicious files.

Adaptive Access Control Based on Endpoint Security Posture

A key benefit of cloud services is the ability to access them from anywhere and from any device. However, unfettered access to cloud services can be a vector for malware to enter an organization. To address this, Netskope provides device classification capabilities that enable the identification of processes running on devices accessing cloud services. Netskope is able to identify Cybereason processes running on Windows or macOS, Linux, iOS & Android devices and apply adaptive access control policies based on device characteristics. For example, Netskope can allow uploads to cloud services from trusted devices secured by Cybereason.investigations as easy as possible. In fact, Vectra Cognito has been shown to reduce time spent on threat investigations by up to 90%. Incident responders can then trigger appropriate actions based on the type of threat, risk level, and certainty.

Integration with Cybereason further allows for built-in endpoint prevention, detection and remediation across the broadest range of endpoints, from mobile to fixed and virtual endpoints running Windows, MacOS, Linux, iOS & Android devices. Security staff can kill processes, quarantine files, prevent file execution, or isolate machines to effectively stop cyberattacks and prevent lateral movement across the enterprise.

ABOUT NETSKOPE

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.

ABOUT CYBEREASON

Cybereason is the champion for today's cyber defenders providing future-ready attack protection that unifies security from the endpoint, to the enterprise, to everywhere the battle moves. The Cybereason Defense Platform combines the industry's top-rated detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a Malop (malicious operation). The result: defenders can end cyber attacks from endpoints to everywhere. Cybereason is a privately held, international company headquartered in Boston with customers in more than 30 countries.

Learn more:
https://www.cybereason.com/