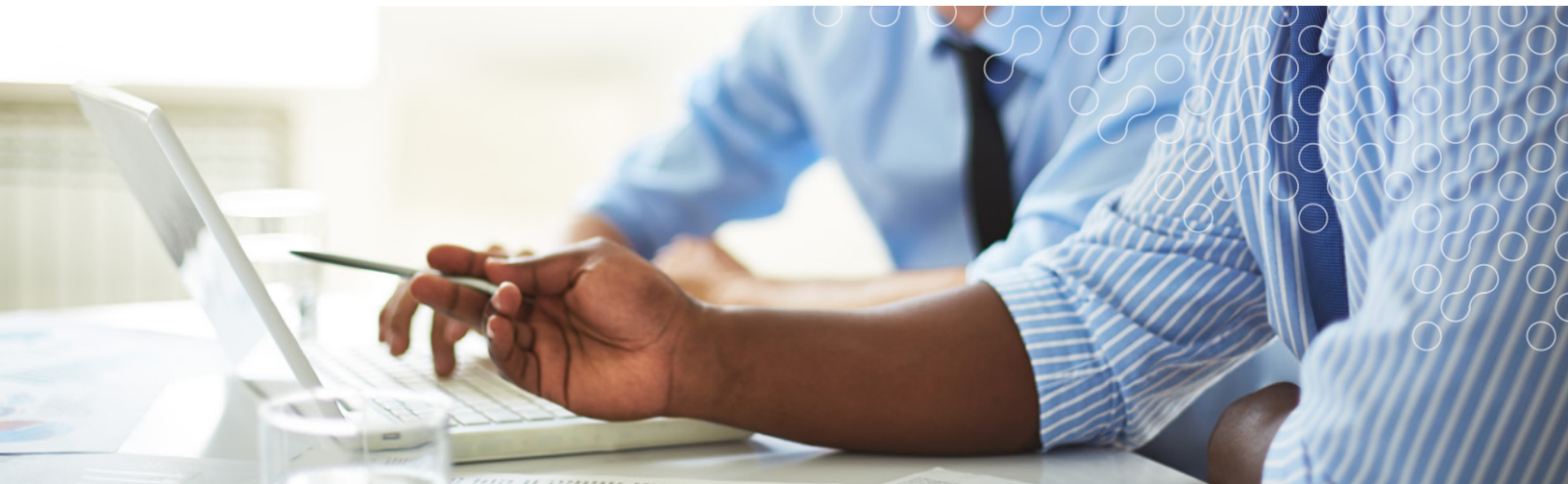# Netskope and Crowdstrike

The increasing use of cloud services and the ability to access them from any device makes cloud and endpoint critical points for security. Netskope and CrowdStrike together create a defense-in-breadth solution, extending advanced threat detection across endpoints, and into cloud applications. Automated exchange of threat information between Netskope and CrowdStrike reduces the time required for cloud threat detection, forensic analysis and prevention.
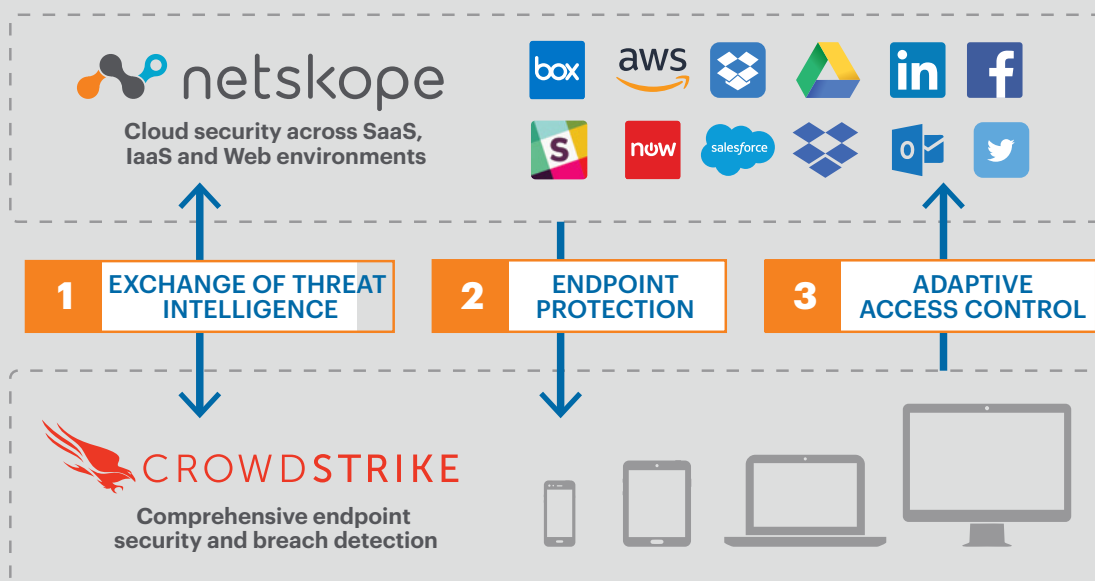
QUICK GLANCE

- Automated forensic sharing between cloud and endpoint protection solutions
- Accelerated response in blocking malicious actors
- Comprehensive visibility and remediation of threats across cloud and endpoints
- Adaptive access policy for cloud based on endpoint security posture

NETSKOPE AND CROWDSTRIKE 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. Organizations are increasingly viewing cloud services and endpoints as the most critical control points. Netskope provides comprehensive visibility and control of cloud services, including advanced, multi-layered threat protection. CrowdStrike's cloud native Falcon Platform stops breaches by leveraging next-generation antivirus, endpoint detection and response, and threat intelligence.

Together, Netskope and CrowdStrike deliver a comprehensive view of threats across both cloud and endpoints and work together to respond more quickly and effectively to those threats. By sharing threat forensics Netskope and CrowdStrike can ensure newly discovered threats are quickly identified, endpoints protected, and the threat neutralized across the organization. Additionally, Netskope is able to identify those endpoint devices that are secured by CrowdStrike and granularly control the cloud access and activities of any endpoints where the CrowdStrike agent is not installed.

Netskope and Crowdstrike

netskope
Cloud security across SaaS, IaaS and Web environments

| **1** EXCHANGE OF THREAT INTELLIGENCE | **2** ENDPOINT PROTECTION | **3** ADAPTIVE ACCESS CONTROL |

CROWDSTRIKE
Comprehensive endpoint security and breach detection

KEY USE CASES

Threat forensics exchanged between cloud and endpoint

The CrowdStrike Falcon Endpoint Protection Platform binds seamlessly with Netskope's cloud-native threat protection engine and shares detected IOCs to bolster Netskope's already-robust malware detection. Together CrowdStrike and Netskope's enhanced capability provides joint customers with increased real-time, actionable threat forensics and enhanced malware protection on both endpoint and in the cloud. Netskope can enrich CrowdStrike by sharing data on new threats discovered within cloud services and from websites visited by endpoints. In return, CrowdStrike can leverage this information to provide Netskope with details of endpoints which may already be compromised by the threat.

Closed-loop remediation between cloud and endpoints

Netskope is able to detect and remediate threats, such as malware, being submitted or residing within cloud services. To close the loop for newly discovered cloud threats, Netskope integrates with CrowdStrike to drive discovery and prevention across an organization's endpoints. When new malware is discovered in the cloud, Netskope is able to pass the malicious file hash to CrowdStrike and based on this file hash CrowdStrike can alert on affected endpoints and/or prevent the malicious file from executing.

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 unsanctioned cloud services (Shadow IT) is often a vector for malware or more advanced threats 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 evaluate if the CrowdStrike agent processes are running on Windows and macOS endpoints and apply adaptive access control policies based on the result. For example, Netskope can allow uploads to cloud services only from endpoint devices that are secured by CrowdStrike.

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.