Netskope and Splunk

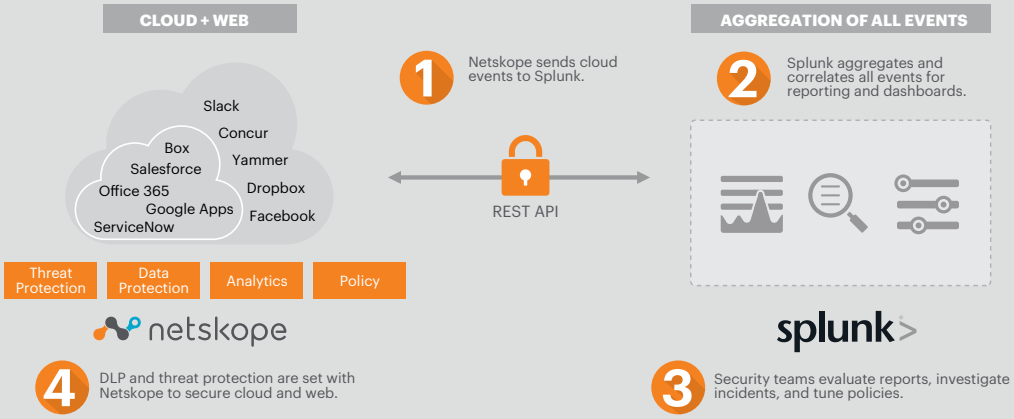
Netskope and Splunk offer a comprehensive security stack for granular visibility and control across organizations' cloud and web use. Gain rich reporting capabilities with data security, threat protection, and access controls across SaaS, IaaS, and web.

QUICK GLANCE

- Gain deep, 360-degree visibility into cloud and web use regardless of device, network, or location of user
- Create dynamic reports and dashboards with comprehensive information across SaaS, IaaS, and web use
- Protect against advanced threats with multi-layer threat detection and remediation

NETSKOPE AND SPLUNK OVERVIEW

Netskope and Splunk complement each other to provide security operations teams with an integrated solution for detailed cloud and web security and reporting. Netskope secures cloud and web use of users while funneling detailed, Common Information Model-compliant (CIM) events to Splunk for further analysis and follow-up. Netskope aggregates all cloud and web data, reducing the friction of pulling data from disparate sources. Splunk can then correlate with other relevant sources like EDR or IDS/IPS solutions, and more, to create a comprehensive view of an organization's security posture.



USE CASES

Visibility across cloud and web

Netskope provides rich information on all cloud and web use, including user, device, cloud service, cloud service activity, location, network, and more across all devices (managed or unmanaged), locations, and networks. Reduce administrative hassle from trying to obtain logs from separate cloud sources and configuring API access from each cloud service. Netskope provides real-time event information even from cloud services that do not have easily accessible APIs. Use the aggregated information to inform security policies across the organizational perimeter and user devices. Set controls in Netskope to restrict risky actions in cloud services or across integrated solutions like MDM or SSO providers to optimize security programs and processes.

Centralized SIEM reporting and forensics

Netskope provides rich, contextual information around all cloud and web use, with an event-by-event incident history of all relevant user activities, policy triggers, and actions taken to manage and remediate incident. Through Splunk, admins and analysts can easily create their own plug-ins and workflows to analyze Netskope data, write new dashboards with pre-built or custom correlation searches, and dive into events for forensic investigations. Run detailed reports for compliance and auditing purposes or general tracking and dashboarding.

Advanced threat protection and data security

Netskope funnels DLP and threat-related incidents to Splunk for further investigation and follow-up by analysts. With integration into Splunk's Adaptive Response framework, organizations can run ad-hoc commands from inside Splunk that leverage the correlated threat intelligence of the platform to populate URL blacklists and malicious file hashes into their Netskope tenant. This enables learnings from the entire customer ecosystem of connected products to be used inside the Netskope Security Cloud, just as those products are able to take advantage of the deep visibility into activities and data provided by Netskope.

About Splunk

Splunk Inc. turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to solve their toughest IT, Internet of Things and security challenges. Join millions of passionate users and discover your "aha" moment with Splunk today: http://www.splunk.com.

About Netskope

Netskope is the leader in cloud security. We help the 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.