SOLUTION BRIEF

Netskope for Microsoft Azure Sentinel

Netskope Cloud Security solutions work with Microsoft Azure Sentinel to deliver a comprehensive security stack for granular visibility and control across an organization's cloud and web use. Gain rich reporting capabilities with data security, threat protection, and access controls across web use, SaaS, IaaS, and Zero Trust network access.

KEY USE CASES

- **Gain deep, 360-degree visibility** into cloud and web use regardless of device, network,or location of the user.
- **Create dynamic reports and dashboards** with comprehensive information across web use, SaaS, IaaS, and Zero Trust network access.
- **Surface advanced threats and data exfiltration** attempts with an enterprise-grade inspection engine.

> "97% of the cloud apps in use in the enterprise are not managed by a centralized IT or security function."
>
> 2021 Netskope Cloud and Threat Report[1]

THE CHALLENGE

The usage of cloud apps in the enterprise continues to rise, with the average number in use increasing by 20% in 2020. Cloud activity now represents 53% of secure web gateway traffic. Part of this growth includes 47.5% of apps with a "Poor" Cloud Confidence Index™ rating, putting sensitive data at risk. The scale and complexity of this cloud app usage in the enterprise continues to grow with a mix of business-led and personal app instances (compared to known, IT-led and managed app instances), presenting a risk to enterprise data security. This means that organizations must protect against sensitive data leakage, cloud threats, and consequences associated with non-compliant behavior in managed cloud applications, such as Box, DropBox, and other cloud services.

NETSKOPE FOR AZURE SENTINEL

Netskope and Azure Sentinel complement each other to provide security operations teams with an integrated solution for detailed reporting for cloud and web security. Netskope secures cloud and web use of users while funneling detailed, Common Information Model-compliant events to Azure Sentinel for further analysis and follow-up. Netskope aggregates views in cloud and web activity, reducing the friction of pulling data from disparate sources. Azure Sentinel can then correlate with other relevant sources to create a comprehensive view of an organization's security posture.

[1] Research was performed on anonymized usage data collected by the Netskope Security Cloud platform for millions of users from January 1, 2020 through December 31, 2020 relating to a subset of Netskope customers with prior authorization.

CAPABILITIES

SURFACING SENSITIVE DATA EXFILTRATION ACROSS CLOUD AND WEB

Azure Sentinel monitors and collects data on infrastructure and applications that your team has chosen and deployed. Netskope provides unmatched, machine learning-enhanced 4-in-1 data loss prevention (DLP) for SaaS, IaaS, web, and email environments to surface exfiltration of sensitive data that extends to apps and locations that weren't sanctioned by the IT department. By combining protection for data-at-rest and data-in-motion with a unique understanding of the modern context of cloud and web access, Netskope accurately and effectively detects and protects sensitive content no matter where it resides.

Your administrators and analysts can use Netskope to gather rich information on all cloud and web use, across all devices (both managed and unmanaged). In addition, you'll be able to detect sensitive content across more than 1,500 file types, using 3,000+ data identifiers, metadata extraction, proximity analysis, fingerprinting, and exact match.

With the information surfaced by Netskope in Azure Sentinel, you'll have the complete context needed to create targeted DLP policies using context like user, group, device, service, and activity. And you'll get real-time event information even from cloud services – API not required. Use that aggregated information to inform security policies across the organizational perimeter and user devices. You can even set controls that restrict risky actions in cloud services or across integrated solutions like Intune MDM or Single-Sign-On providers.

83% of enterprise users with managed devices use personal app instances.

2021 Netskope Threat and Cloud Report

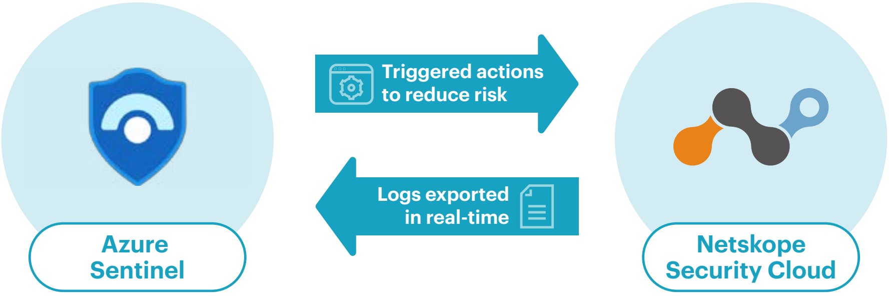
CENTRALIZED SIEM REPORTING AND FORENSICS

Azure Sentinel is the first cloud-native security information and event management (SIEM) platform from a major cloud provider, which helps ensure that storage or query limits won't prevent you from protecting your enterprise. Netskope adds 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 incidents. And it all happens within a single centralized administrative console.

97% of cloud apps used by employees each month are unknown to IT, adopted by business units and users

Through Azure Sentinel, administrators 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. You can create dynamic reports and dashboards with comprehensive information across web use, SaaS, IaaS, and Zero Trust network access. Netskope offers detailed forensic and audit trails to give security analysts a comprehensive view of each incident, including the specific policy violated, actions taken and a view of any sensitive data in complete context. This forensics view also includes a range of additional information including the user, device, location, app and app instance, and more, giving the analyst complete context to make a well-informed decision.

TECHNOLOGY INTEGRATIONS



Joint Solution Benefits

- **Send all logs generated by users to Azure Sentinel**
- **Correlate all logs in one place**
- **Helps address log storage requirements for compliance**

Azure Sentinel is a cloud-native security information and event manager platform. Netskope sends all logs generated by users to Azure Sentinel, correlates the logs in one place, and helps address log storage requirements for compliance.

ADVANCED THREAT PROTECTION AND DATA SECURITY

Netskope's Next Gen Secure Web Gateway is a cloud-based web and cloud traffic security solution that prevents malware, detects advanced threats, filters by category, protects data, and controls app use for any user, location, and device. It funnels DLP and threat-related incidents to Azure Sentinel for further investigation and follow-up by analysts. Through the Netskope integration with the security orchestration, automation, and response capabilities of Azure Sentinel, administrators can create commands that will work with Netskope to reduce the attack surface and enhance threat prevention. This enables learnings from the entire 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.

Customers also take advantage of Netskope's cloud-native Zero Trust Network Access solution that supersedes legacy VPNs and addresses the challenges of secure access to private applications in the public cloud and data centers. Surfacing the private applications that are being and the specific workers who are using them enables Azure Sentinel administrators to understand the scope and nature of data access and therefore data security.

61% of all threats are sourced from the cloud.

2021 Netskope Threat and Cloud Report

ABOUT AZURE SENTINEL

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Eliminate security infrastructure setup and maintenance, and elastically scale to meet your security needs.

ABOUT NETSKOPE

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing zero trust principles across data protection and threat prevention everywhere. Unlike others who force tradeoffs between security and networking, Netskope's global security private cloud provides full compute capabilities at the edge.

Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.