Solution Brief +

Netskope and Amazon Security Lake

Netskope Intelligent SSE integrates with Amazon Security Lake to enable faster and more comprehensive threat detection and response for organizations securing hybrid and multi-cloud environments. Customers can export logs, events, and alerts from Netskope to Amazon Security Lake to get a more holistic view of threats and vulnerabilities across both cloud and on-premises resources.

Quick Glance

- **Complete Visibility:** Organizations can easily export logs that Netskope collects to Amazon Security Lake to get a centralized view of threats and vulnerabilities across their environment.
- **Normalized Security Data:** All data is stored in the Open Cybersecurity Schema Framework (OCSF) standard for streamlined data management at scale.
- **Centralized Threat Analysis and Response:** Organizations can use their preferred tools to analyze security data and potential threats, and respond to alerts stored in a centralized security data lake.

> “Netskope Cloud Exchange provides powerful integration tools that automate sharing of threat information. CE allows us to distribute this information across our operations in near real-time which we can then consolidate into actionable alerts and notifications.”
>
> — Malhar Shah, CEO Crest Data Systems

The Challenge

Today’s organizations often have sensitive data and business-critical applications spread across public cloud, private cloud, SaaS, on-premises, and partner environments. To monitor and secure these dispersed resources, they typically collect and analyze logs, events, and alerts from security data sources.

Alarmingly, this security data is most often stored in multiple locations in incompatible data formats, leaving security practitioners with no centralized means of viewing and responding to threats and events. This results in “swivel chair” analysis which can quickly fatigue security teams, prevent correlation of related events, and allow serious problems and attacks to go unnoticed.

The Solution

Netskope’s Intelligent Security Service Edge (SSE) platform and Amazon Security Lake from Amazon Web Services (AWS) integrate to deliver a solution that collects, normalizes, and stores logs from all security data sources to a common location for detailed analysis and response. The solution helps organizations reduce overall risk and gain confidence that their data, hybrid workforce, and resources are safe from threats and attacks as they grow and embrace cloud transformation.

aws PARTNER Security Software Competency

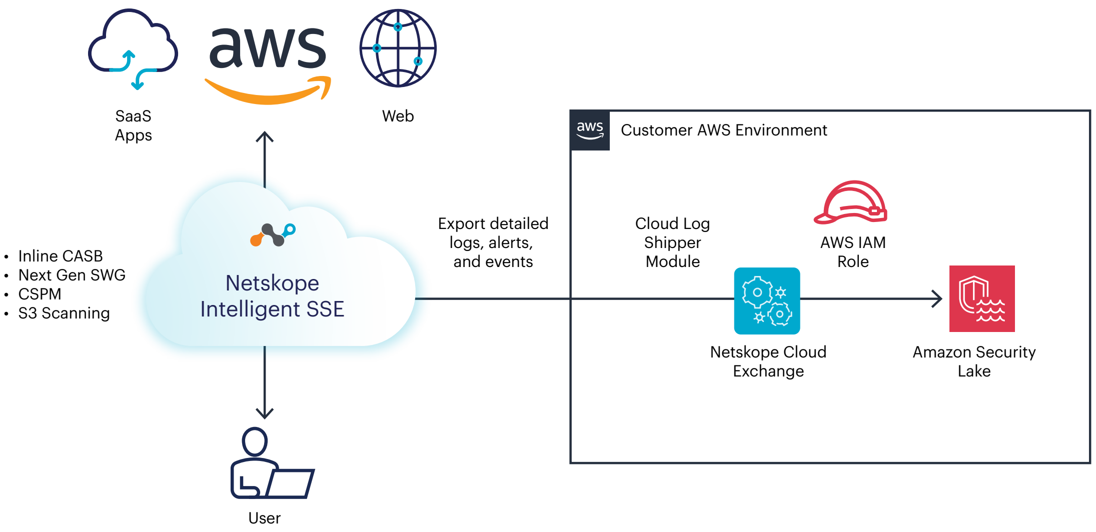

Figure 1: Netskope and Amazon Security Lake

How Netskope and Amazon Security Lake Work Together

Netskope Cloud Exchange plays a key role in the solution by enabling the exchange of information between Netskope Intelligent SSE and Amazon Security Lake. Cloud Exchange's Cloud Log Shipper (CLS) module regularly queries Intelligent SSE for detailed log and event information and then forwards it on to Amazon Security Lake. Security Lake stores logs and events from Netskope and other AWS services and sources in the Open Cybersecurity Schema Framework (OCSF), an open community schema.

Now security analysts can view and respond to normalized security findings from across their entire IT environment—public cloud, private cloud, SaaS, remote devices, on-premises, and partners—from a single centralized location. Organizations can use their preferred tools to analyze data stored in Security Lake while other AWS and third-party services can subscribe to the data that's stored in Security Lake for analysis and incident response.

About Key Solution Components

Amazon Security Lake

Amazon Security Lake is a service that automatically centralizes an organization's security data from across their AWS environments, leading SaaS providers, on-premises, and cloud sources into a purpose-built data lake. Security Lake allows customers to act on security data faster and simplify security data management across hybrid and multi-cloud environments.

Netskope Intelligent SSE

Netskope is a leader in Secure Access Service Edge (SASE), offering an Intelligent Security Service Edge (SSE) platform that provides comprehensive visibility and real-time data and threat protection for cloud services, applications, and data. Netskope Intelligent SSE is fast, easy to use, and secures transactions wherever people and data go. Intelligent SSE converges security capabilities including zero trust network access (ZTNA), next-gen secure web gateway (SWG), cloud access security broker (CASB), SaaS security posture management (SSPM), cloud security posture management (CSPM), data loss prevention (DLP), Threat Protection, firewall as a service (FWaaS), remote browser isolation (RBI), and more, into a single-pass cloud platform with one policy framework and a single console.

Netskope Cloud Exchange and Cloud Log Shipper

Netskope Cloud Exchange (CE) provides powerful integration capabilities that enable organizations to leverage new and existing investments across their security and IT stacks. CE consumes valuable Netskope telemetry, external threat intelligence, and risk scores, enabling improved policy implementation, automated service ticket creation, and log exportation from Netskope Intelligent SSE. The CE platform and its four modules; Cloud Log Shipper, Cloud Ticket Orchestrator, Cloud Threat Exchange, and Cloud Risk Exchange are provided to Netskope customers at no charge.

The Cloud Exchange Cloud Log Shipper (CLS) module enables organizations to export context-rich logs from Netskope Intelligent SSE into security information and event management (SIEM) tools and data lakes such as Amazon Security Lake. This additional context assists analysts and security operations centers (SOCs) in exposing and responding to threats from across their entire IT environment. CLS regularly and persistently executes polls against the Netskope Intelligent SSE to extract events, alerts, and web transaction logs.

> Netskope and Amazon Security Lake enable organizations to normalize, store, and analyze security data from across diverse environments at a centralized location.

BENEFIT	STANDARD
Complete visibility	Netskope and Amazon Security Lake enable organizations to easily collect security and activity logs into a centralized data lake to get a complete and centralized view of user interactions with data and resources in AWS, private cloud, SaaS, on-premises, and partner environments.
Normalized security data	All data is stored in the Open Cybersecurity Schema Framework (OCSF) standard for streamlined data management at scale.
Centralized threat analysis and response	Organizations can use their preferred tools to analyze security data, respond to alerts, and remediate threats stored in a centralized security data lake.
Simplified compliance monitoring and reporting	Centralized security data from across your entire AWS and IT environment makes it easier to monitor and report on compliance.
Analyze multiple years of security data	Centralize petabytes of data from cloud, on-premises, and custom sources in Amazon Security Lake for quick and detailed analysis.

aws **Available in AWS Marketplace**

netskope

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.