SOLUTION BRIEF

Swimlane and Netskope

Together, we provide actionable intelligence for your cloud activities

WHY WE WORK TOGETHER

When integrated with Swimlane, Netskope provides visibility into and actionable intelligence on cloud activities. Enterprises receive event data that is often immediately actionable, enabling customers to make contextually-based decisions. Security admins can understand user activity across multiple cloud-based applications, device-types, files shared, and determine if there is unauthorized access. A consolidated view of alerts with the most relevant security information allows for faster triage and incident response times.

CHALLENGE

As enterprise applications increasingly move to the cloud, security teams are faced with new, expanded security challenges. Alert fatigue among SOC analysts, and the burden of swivel chair analytics for security teams tasked with triaging thousands of alerts across disparate tools, hinders their ability to pinpoint which security incidents may cause the organization the most damage.

Netskope provides a risk assessment for each cloud application used to calculate an enterprise-ready score that is aggregated into their Cloud Confidence Index. This helps increase the accuracy of the Swimlane Security, Orchestration, Automation & Response (SOAR) platform by reducing false positives and ensuring threats are mitigated in real-time. Swimlane orchestrates retrieval of event and alert information that can identify suspicious users and automate the Incident Response workflow. Together, Netskope and Swimlane can significantly enhance incident response times and accuracy, ensuring that cyber-threats are mitigated before they impact your business.

SOLUTION AT A GLANCE

Ingests key alerts from Netskope

Keys Swimlane workflows with holistic cloud activities and context

Allows for automated enrichment of alerts

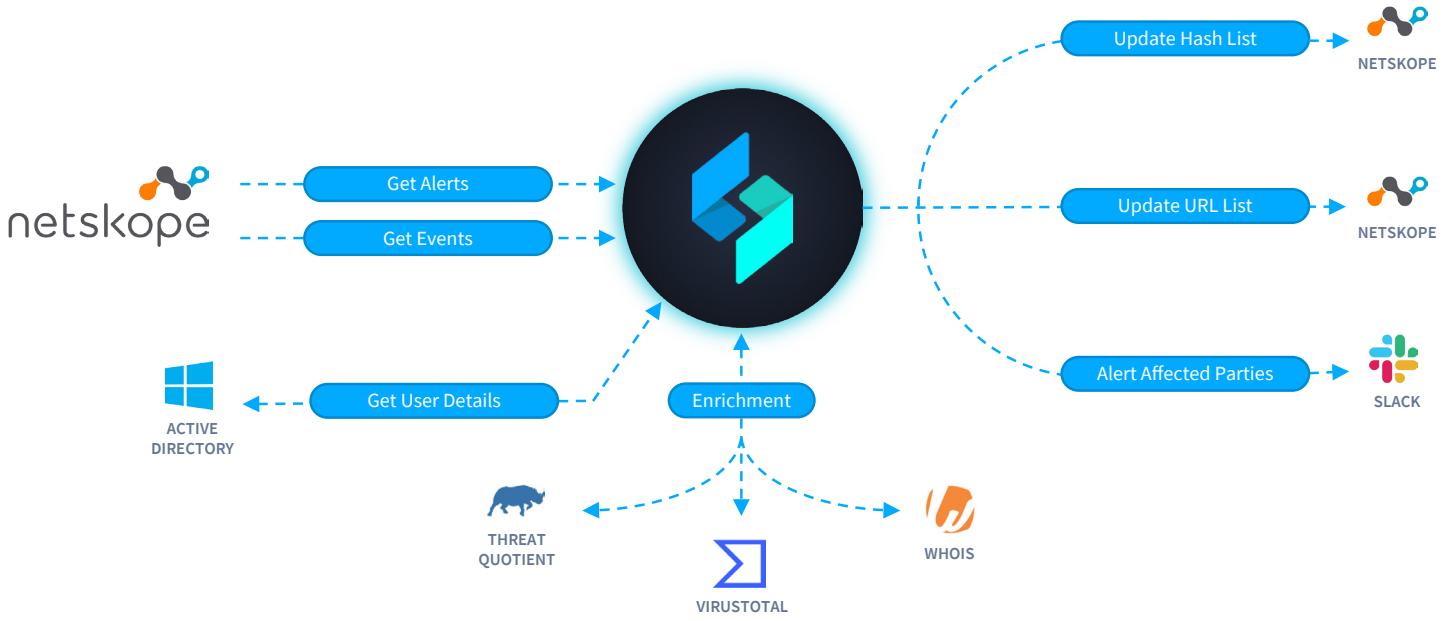
JOINT SOLUTION BENEFITS

- Speeds triage and incident response time to alerts
- Unifies view of product and alerts for easy management
- Automates workflows and incident response

SOLUTION OVERVIEW

The Swimlane Netskope API integration enables ingestion of Netskope alerts and around-the-clock automated queries for new alerts and events. Alerts can be enriched and/or integrated with other products connected to the Swimlane platform via pre-defined or custom automated workflows and applications. As an example of enrichment, Swimlane can reach out to your Active Directory for more information on the host or it could send alert details directly to your threat intelligence tools for additional analysis. Once the severity of the threat is determined, Swimlane can reach back out to Netskope to update the hash list, URL list, and/or to acknowledge the alerts have been investigated. Additionally, Swimlane can trigger real-time alerts to the teams responsible for additional triage. And Swimlane is flexible and powerful enough to automate even the most complex use cases with ease - which reduces alert fatigue and improves MTTR.

HOW IT WORKS



BETTER TOGETHER

About Netskope

Netskope is the leader in cloud security. We help the world's largest organizations take full advantage of the cloud and web without sacrificing security. The Netskope security cloud provides unrivaled visibility and real-time data and threat protection.

About Swimlane

Swimlane is at the forefront of the security orchestration, automation and response (SOAR) solution market and was founded to deliver scalable security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages.