# Unlocking the Power of a Unified Partner Ecosystem

## Your One-Stop Directory for Zero Trust Security


netskope

# Unlocking the Power of a Unified Partner Ecosystem


## Table of Contents

# Executive Summary

## Introduction

As a security or network decision-maker, you know that the hybrid work environment has thrown traditional security and networking strategies out the window. So if you're navigating a security maze without a map—this guide is here to help!

**What you'll learn:**

- Understand the significant shifts taking place in the security and networking landscape
- Design a zero trust architecture that works for your organization
- Discover how to choose the right technology partners, and how to implement best-of-breed solutions that work together seamlessly

**Who should read this?**

Security and network decision-makers.

**Why read this ebook?**

To understand recent changes to the security and networking technology landscape, know how to assess your current security posture, and identify areas for improvement within your vendor roster.

**When to read these insights?**

At the start of a zero trust project or before starting a Security Service Edge (SSE) / Secure Access Service Edge (SASE) project and commencing an RFI. Whether you're just starting out with zero trust or looking to upgrade your existing solution, our guide is here to help.

# Designing a Zero Trust Strategy

A continuously adaptive zero trust architecture gathers together telemetry about users, applications, and data from multiple sources, and allows adaptive policies to make risk-based decisions in real time. That's why ecosystems and platform architectures are so important. Zero trust draws in disparate telemetry streams in order to continuously make complex trust decisions, including:

## User and identity management:

Idenity and Access Management (IAM), Role-based Access Controls (RBAC), and User and Entity Behavior Analytics (UEBA)

## Device management:

Device health checks and confidence ratings

## Application and workload management:

Secure Web Gateways (SWGs) and Security Service Edge (SSE) solutions with Cloud Access Security Broker (CASB) functionality

## Network security devices:

Next-generation firewalls (NGFWs), and SSE solutions with SWG, CASB, and Zero Trust Network Access (ZTNA) functionality


Zero trust is no longer an option; it's a necessity in today's genAI-driven world

# Where to Start—or Go Next—with Zero Trust

An effective zero trust security model delivers a seamless user experience, making security transparent and creating little to no friction across the company's workloads. An organization moving to a zero trust strategy should start by mapping out its business use cases and processes.

## Examples:

01 | Protecting cloud collaboration

02 | Unapproved data movement

03 | Secure access to internal apps

04 | Increasing visibility-value projects

Forrester Total Economic Impact (TEI) of Netskope SSE

## Navigating GenAI and Zero Trust

GenAI and zero trust are interconnected components of modern enterprise cybersecurity. To address the specific challenges posed by genAI, Netskope has developed a data protection strategy that incorporates granular context and instance awareness, advanced application access control, and advanced data protection measures comprised of several key solutions:

- **SASE + SSE integration**
- **Unified security management**
- **GenAI-powered CASB**
- **Advanced cloud data loss prevention (DLP)**
- **Continuous capture of genAI interactions:** Netskope has the ability to capture generative AI prompt and prompt responses.

# Designing a Zero Trust Partner Ecosystem with Netskope One

Netskope One is a cloud-native platform that offers converged security and networking services to enable your SASE and zero trust transformation. Through its patented Zero Trust Engine and NewEdge Network, Netskope One, makes it easy to protect valuable data while delivering a phenomenal user experience. The platform makes access decisions using adaptive controls based on rich context and user input, enhanced by more than 100 unique detailed activities for thousands of applications.

The Netskope One platform integrates with hundreds of partners and third-party solutions to provide a comprehensive security posture. Here are four key ways customers can benefit from these integrations:

- Consistent Threat Detection and Response
- Contextual Access Control
- Advanced Analytics and Visibility
- Automated Incident Response

As part of Netksope's SASE framework, our zero trust partner ecosystem enables enterprises to safely enable their hybrid workforce with a cloud-delivered, AI-powered data-centric approach.

# The Netskope One Partner Ecosystem Directory

Welcome to our partner ecosystem directory of integrated technologies, designed to help you build a robust zero trust ecosystem with the Netskope One platform. With our extensive network of partners, you'll have access to best-of-breed solutions that seamlessly integrate with Netskope One, empowering you to create a more holistic security architecture that protects your organization. With this directory, you can design your own zero trust ecosystem that provides unparalleled visibility, control, and security for your users, applications, and data.

## Our partners, our approach, and business outcomes to each are laid out in the following sections:

# Cloud & Hyperscaler Platforms

Netskope provides consistent security across all public cloud deployments, including visibility into data risks and advanced threats.

## Amazon Web Services (AWS)

*Critical workload protection, flexible integration options*

The joint solution provides an understanding of your risk exposure, misconfigurations, and inventory assets, and can enforce compliance standards and protect against insider threats and malware.

*"With Netskope and AWS, we finally understand our cloud risks, fix mistakes, and stop threats like malware and insider attacks. It's a flexible solution that protects our most important cloud work."*

## Google Cloud Platform (GCP)

*Control over risky activities and sensitive data*

Netskope and Google security tools leverage Netskope findings for user and data behavior across public cloud and SaaS applications.

*"Netskope and Google Cloud give us strong control over risky activities and sensitive information. We can now use Netskope's findings about user and data behavior across all our cloud apps to make better security decisions."*

## Microsoft Azure

*Automatic data discovery, and classification, consistent real-time data protection, insider threat identification*

The solution ensures that consistent real-time data protection measures are in place to keep data within managed instances, enforce consistent policies across other cloud apps, oversee user behavior to identify insider threats, and counter attempts to exfiltrate data.

*"This partnership with Netskope and Microsoft Azure means our data is automatically found and classified, and protected in real-time. We can easily identify insider threats and prevent data from leaving our managed cloud instances."*

# Cloud Native Application Protection Platforms (CNAPP)

When integrated with Netskope One, CNAPP can provide valuable information to securely enable those systems and applications and block or change access in response to these insights.

## CrowdStrike

*Unified SOC data and workflows, accelerated threat investigation and remediation, enhanced zero trust controls*

The integration combines Netskope's Private Access with CrowdStrike's Cloud Workload Protection capabilities to provide a seamless solution for securing cloud environments, particularly by enabling workload quarantine.

> *"Netskope's integration with CrowdStrike brings our security data together, helping us investigate threats faster and block risky cloud workloads. It's a seamless way to secure our cloud setup."*

## Wiz

*Comprehensive cloud protection, enhanced security posture, streamlined cloud security operations*

The Netskope and Wiz solution provides visibility and control across Azure, GCP, and AWS resources, ensuring consistent security policies are enforced regardless of the cloud environment's complexity or scale. This collaboration enables organizations to leverage real-time insights from Wiz's comprehensive cloud security platform directly within Netskope.

> *"Thanks to Netskope and Wiz, we have clear visibility and control across all our cloud resources, no matter how complex. This partnership gives us real-time insights to keep our cloud security strong."*

# Email Security

Preventing email attacks like phishing and business email compromise ensures that organizations have a solid security posture to stop inbound threats and their propagation internally.

## Mimecast

*Advanced threat protection, efficient threat protection, omnichannel DLP across email, cloud, endpoint, and web*

Mimecast provides human risk management and advanced email security that complements Netskope and empowers mutual customers with enhanced protection, shared threat intelligence, and integrated workflows to optimize their security posture and operations, including an omnichannel DLP approach to detecting and protecting sensitive information across your cloud environment.

*"Mimecast and Netskope give us advanced threat protection for email, stopping attacks like phishing before they spread. Plus, we get a unified way to protect sensitive data across email, cloud, and web."*

## Microsoft

*Full life-cycle DLP protection, continuous zero trust management prevent misuse and data exfiltration*

Microsoft Purview provides a framework that enables labels and encryption throughout the life cycle of an email message or document. Netskope ensures that all Microsoft-labeled emails and documents are appropriately labeled and encrypted.

*"Our team loves how Netskope works with Microsoft Purview to protect email and documents throughout their entire journey. It ensures all our labeled and encrypted data stays secure."*

# Endpoint Security (EPP) & Extended Detection and Response (XDR) Solutions

EPP and XDR vendors read Netskope telemetry and correlate information with their systems to create a higher fidelity understanding with deep contextual-based insights for detecting and analyzing malware and advanced persistent threats (APTs).

## CrowdStrike

*Reduced attack surface, effective incident investigations, device posture validation*

The CrowdStrike and Netskope integrations empower organizations to unify SSE with rich security telemetry and response capabilities from across the enterprise in the Falcon console for accelerated threat investigations.

> *"The integration of CrowdStrike and Netskope helps us reduce our attack surface and investigate incidents more effectively. It gives us a complete view of security across our entire organization."*

## SentinelOne

*Accelerated threat triage, device posture validation, reduced mean time to respond*

SentinelOne's XDR platform extracts alert logs from Netskope for automated correlation and to facilitate incident response inside their platform. They also extract Netskope User Confidence Index (UCI) scores for higher fidelity incident response triggers, and exchange IOCs of all types with Netskope.

> *"SentinelOne and Netskope together speed up our threat responses. We get automatic alerts and higher-quality triggers for incidents, helping us react much quicker."*

# Identity Providers (IDPs)

Netskope provides IDPs with the extended power of business-led apps, user-led apps, and websites, beyond federated applications, with the ability to quantify user risk and aggregate it for both systems to benefit from the other's unique view into risk.

## Okta

*Fine-grained access control, continuous real-time enforcement, visibility into federated identity behavior*

A common use case using Netskope and Okta is to extend your zero trust perimeter using Okta Network zones and the Netskope NewEdge Network. The Netskope One client checks the device compliance posture in real time, via Device Classification, to ensure that only compliant corporate-managed devices are allowed to connect to Okta. Netskope also exchanges risk scores with Okta.

> *"Netskope and Okta extend our zero trust security, giving us very precise control over who can access what. We can continuously enforce policies in real-time and see exactly what our federated identities are doing."*

## Microsoft

*Maximized value in existing investments*

Netskope is Microsoft's lead partner to integrate Netskope One SSE capabilities directly into Microsoft Entra. This enables a seamless end-user experience while simplifying SSE administration. Microsoft customers benefit from a native SSE experience utilizing their investment in Entra, while accessing Netskope's advanced SSE capabilities for all SaaS apps.

> *"Our Microsoft investment is maximized with Netskope. We get a seamless experience for our users while simplifying security administration, benefiting from advanced security features for all our apps."*

# Mobile Device Management (MDM)

The Netskope mobile client expands data security to mobile devices with various MDM solutions for seamless deployment on iOS and Android.

## CrowdStrike

*Seamless access experience through device posture validation*

The integration collects user IDs, scores, and host information from CrowdStrike and shares it with Netskope, providing a more comprehensive understanding of potential risks associated with users and devices.

> *"Integrating Netskope with CrowdStrike for MDM ensures only compliant devices can access our network. We get a comprehensive understanding of potential risks by sharing user and device information."*

## Infinipoint

*Comprehensive zero trust device access*

With InfiniPoint and Netskope, IT and security teams can verify device security posture, extend adaptive access, and enable auto-remediation as part of user authentication.

> *"Netskope and Infinipoint give us complete zero trust device access. Our IT and security teams can verify device security, extend access adaptively, and even auto-fix issues during user login."*

# Mobile Device Management (MDM)

The Netskope mobile client expands data security to mobile devices with various MDM solutions for seamless deployment on iOS and Android.

## Ivanti

*Comprehensive MDM protection for corporate data*

Using Ivanti MDM allows managed iOS and Android devices to connect to the Netskope One Platform using the per-app VPN mode.

> *"With Ivanti and Netskope, our managed iOS and Android devices can securely connect to the Netskope One Platform. It's a great way to ensure comprehensive mobile device protection for our company data."*

## Omnissa (VMware)

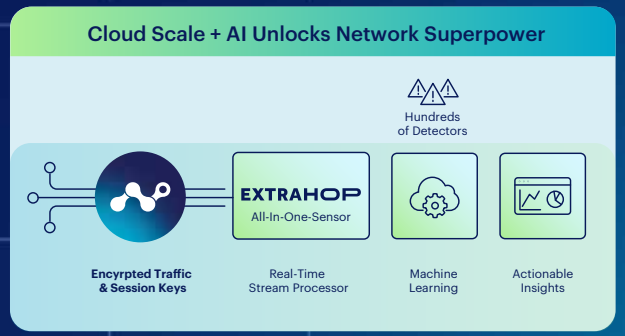
*Threat protection, device and cloud governance, SASE optimization*

Omnissa and Netskope enable organizations to comprehensively expand their kill chain view and response from endpoint to cloud. Omnissa can modify user access and application access based on Netskope alerts.

> *"Netskope and Omnissa provide comprehensive threat protection from endpoint to cloud. This partnership helps us expand our security view and quickly respond to threats by modifying user and application access."*

# Network Detection and Response (NDR)

Leverage your NDR solution with Netskope One for SSE traffic visibility, analysis, and forensics for evasive threats and anomalies.




## Extrahop

*Enhanced threat protection posture, expanded traffic and threat visibility, correlated IOCs across North/South and East/West activity*

ExtraHop RevealX with Netskope One Cloud TAP gives joint customers unprecedented visibility into their Netskope environments. This expanded visibility enables customers to detect advanced threats, monitor the performance of critical business services, and preserve forensic evidence for compliance purposes.

> *"ExtraHop and Netskope provide us with amazing visibility into our network traffic, allowing us to detect advanced threats and monitor critical services. We can also preserve forensic evidence easily."*

## Darktrace

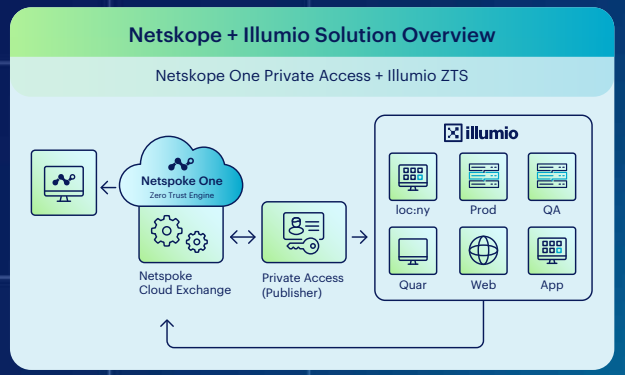
*Real-time threat detection, AI-powered autonomous response*

Together, the solution offers proactive cyber resilience by correlating threats across all digital environments, including SaaS, web, and private applications.

> *"Together, Netskope and Darktrace offer proactive cyber protection by connecting threats across all our digital environments, from web to private applications. This gives us real-time threat detection."*

# Microsegmentation Services

Microsegmentation defines every destination workload as a dedicated trust boundary. This means that only required traffic can move laterally between workloads, denying all other traffic by default.




## Illumio

*Visibility across hybrid environments, adaptive real-time enforcement, globally, dynamic zero trust policies*

When integrated with Netskope One, Illumio identifies a workload compromised by malware, re-labels it as quarantined, and notifies Netskope of this change. This allows Netskope to remove the quarantined workload from its remote access permissions. The benefits of this integration include real-time view(s) of user-to-application and application-to-application traffic to surface risk, risk-aware policies that protect end-users from quarantined workloads, and security policies that are automatically updated based on metadata from Illumio ZTS.

*"Netskope and Illumio help us identify compromised workloads, quarantine them, and instantly remove their remote access. This gives us real-time views of traffic and automatically updates our security policies."*

# Security Information and Event Management (SIEM)

The Netskope Zero Trust Engine is able to make a smart policy decision with information on users, instances, apps, data, etc. This information is captured in Netskope logs which can then be ingested/parsed to SIEMs for deeper insights into user activity to drive zero trust outcomes.


## CrowdStrike

*Unified telemetry, faster time to remediate*

Netskope integrates with the CrowdStrike Falcon Next-Generation SIEM solution to share critical Netskope event logs and alerts for cloud security edge activity to improve visibility and unify telemetry from endpoints and additional domains.

*"Netskope and CrowdStrike's NG SIEM solution give us unified security data, helping us respond to threats much faster. We get better visibility and combine all our security information."*

## Microsoft

*Detailed reporting, aggregate visibility into cloud and web activity*

Netskope aggregates views in cloud and web activity, reducing the friction of pulling data from disparate sources. Azure Sentinel can then correlate to create a comprehensive view of an organization's security posture.

*"Netskope and Azure Sentinel give us a detailed and combined view of all our cloud and web activity, making it easier to understand our overall security."*

# Security Information and Event Management (SIEM)

The Netskope Zero Trust Engine is able to make a smart policy decision with information on users, instances, apps, data, etc. This information is captured in Netskope logs which can then be ingested/parsed to SIEMs for deeper insights into user activity to drive zero trust outcomes.


## Cribl

*Eliminate risky business, maximize investments*

Valuable Netskope telemetry can be shaped or routed using Cribl Stream for monitoring, dashboard, or storage locations with governance, speed, flexibility, and control.

> *"With Netskope and Cribl, we can easily manage and route our valuable security data to monitoring, dashboards, or storage. It gives us incredible flexibility and control, further enable our teams to send the right information to the right destination."*

## Splunk

*Single-pane-of-glass view, adaptive orchestration*

The Netskope App for Splunk enables admins to ingest, parse, normalize, and search on all Netskope data inside the Splunk platform.

> *"The Netskope App for Splunk allows us to bring all our Netskope data into Splunk, giving us a single view of our security information and making it easier to manage."*

# Workflow Automation

Programmatically open tickets on IT service management (ITSM) and collaboration systems from your Netskope One platform, streamlining how the tickets are created and effectively mapping them to workflows in those systems.

## ServiceNow

*Integrate and share telemetry, inspect data-at-rest, track usage and movement of sensitive data across platforms*

Netskope works with ServiceNow as an application and independent software vendor platform to inspect transactions, settings, and data stored within ServiceNow, and to integrate and share telemetry. The Netskope DLP integration supports the ingestion of DLP incidents created on the Netskope DLP deployment.

> *"Netskope works with ServiceNow to help us inspect transactions and data, and share important security information. This integration also supports pulling in our data loss prevention incidents into a single pane of glass."*

## Jira

*Automatic ticket creation streamlines incident response, automated workflows*

The Netskope plug-in for Jira extracts alerts generated by Netskope, and the fields in those alerts, in response to user and system behaviors/discoveries, and creates tickets and/or notifications in Jira to streamline incident response.

# Workflow Automation

Programmatically open tickets on IT service management (ITSM) and collaboration systems from your Netskope One platform, streamlining how the tickets are created and effectively mapping them to workflows in those systems.

## Ivanti

*Automated ticketing, streamlined workflow processes*

The integration allows customers to select critical alerts and map important fields into existing workflows, reducing the need to pivot between systems.

## Slack

*Granular access controls, policy-based DLP, automated workflows*

The integration offers surgical visibility into usage of Slack and its integrated ecosystem apps, granular access controls, DLP, and threat and malware protection.

## Microsoft

*Deep visibility and control of sensitive data, comprehensive risk dashboard*

Enforce policies on messages and files that may contain sensitive information or even take action to restrict files shared with Microsoft or third-party cloud storage apps.

Congrats, you have now mastered the basics of zero trust outcomes, and are also now equipped to implement a game-changing architecture that boosts user performance and happiness. And we've got just the thing to help you achieve this: Netskope One, our platform that's packed with all the tools you need to secure your organization. That is all possible with the Netskope One platform.

Interested in learning more?

Request a Demo


Visit the Netskope website to learn more about Netskope One.

# About Netskope

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.

Resources

- Technology Partners & Integrations
- Get Started with Netskope One
- Netskope Cloud Exchange
- Netskope AI Security Playbook

netskope