



Building a SASE-ready Architecture with Netskope Security Cloud and Your Existing Security Infrastructure

EXECUTIVE SUMMARY

The remote workforce has exploded globally with more employees working from home than ever before. On any given day, approximately 60% of workers are remote.¹ The overwhelming majority (89%) of enterprise users are in the cloud. More workloads are running in Infrastructure as a Service (IaaS) than in the enterprise data center and more applications are delivered via Software as a Service (SaaS) than from the enterprise infrastructure.

Embracing the cloud enhances workforce productivity, but brings numerous security challenges. Employees want to use their own devices to access a wide variety of both managed and unmanaged apps, increasing the opportunity for credential-based attacks. Attackers are moving to the cloud to blend in, increase success rates, and evade detections. Nearly half (44%) of threats are cloud-based, with the top techniques being phishing and malware delivery. Cloud services make it all too easy for employees to put sensitive information in the wrong place or share it with the wrong people. Not to be overlooked, malicious insiders or disgruntled employees are more likely to attempt exfiltration of company sensitive data when outside the office environment.

With the inversion of the traditional network, where users, data, and apps are now on the outside, traditional approaches to security fall short. At most enterprise organizations, the cyber security infrastructure grew organically, resulting in a potpourri of security tools rather than a cohesive security architecture. Legacy security solutions, typically located in the data center, are costly and complex, and can be bypassed by remote workers connecting directly to the internet. Remote access VPNs provide crude network-level access and cannot effectively provide access to specific applications hosted in public cloud environments.

A collaborative and coordinated approach is the key to stopping today's breaches. Moving forward, any enterprise using the cloud needs to quickly modernize and extend its security architecture. By seeking solutions with open architectures and partner ecosystems with ample third-party integrations, organizations can enhance their security tools and capabilities to better detect, investigate, and respond to security threats and data loss faster and more efficiently.

This white paper highlights how you can integrate the Netskope Security Cloud with your existing security tools to provide a safer, more scalable and less complex infrastructure that meets and exceeds security demands in a cloud-first world.



¹ Forbes: <https://www.forbes.com/sites/johnkoetsier/2020/03/20/58-of-american-knowledge-workers-are-now-working-remotely/#57a4f2f53303> (March 2020)

MAKE THE MOST OF YOUR SECURITY INVESTMENTS

The Netskope cloud-native security cloud platform enables seamless, third-party integrations with a robust ecosystem of alliance partners, allowing enterprises to make the most of existing security investments while protecting users across SaaS, IaaS, and web environments. Customers can integrate Netskope with endpoint detection and response (EDR), identity and access management/single sign-on (IAM/SSO), security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions within their environment to better tackle the most difficult security challenges. In addition, Netskope provides an open architecture that can help customers reduce the cost and complexity of MPLS connections, simplify branch and remote access to cloud resources, and increase scale to meet business challenges.

Endpoint Protection Solutions

The increasing use of cloud services, coupled with the ability to access them from any device, has dissolved the traditional enterprise perimeter. With the increase in remote workers comes an increase in the number of internet-connected endpoint devices, especially since workers are likely juggling multiple corporate and personal devices to do their jobs.

Remote workers aren't the only ones using cloud services. Cyber criminals are increasingly using cloud services as a reliable and scalable infrastructure for implementing a cyber-attack chain in the cloud. Consider phishing pages hosted in cloud storage services such as OneNote or Box, Command and Control (C2) networks using collaboration apps such as Slack or GitHub, or malware payloads hosted in AWS S3 buckets or Microsoft Azure.

With attacks increasingly being sourced in the cloud, organizations are viewing cloud services and endpoints as the most critical control points for security. Dual attack vectors of cloud and endpoint present unique challenges, particularly in the case of actively synchronized applications. Malware that starts on the endpoint syncs to the cloud, only to have active sync re-infect the remediated endpoint or spread laterally to other unprotected endpoints also accessing the cloud. Without a method of sharing threat intelligence information to break the synchronization that binds the cloud and the endpoint together in a live threat share, it becomes an endless cycle of transfer infection, remediate, transfer infection, repeat ad infinitum.

To enhance organizations' ability to protect endpoints based on cloud discoveries and vice versa, Netskope partners with endpoint protection (EPP) solution providers such as CrowdStrike and VMware Carbon Black. Netskope provides comprehensive visibility and control of cloud services, including advanced, multilayered threat protection. CrowdStrike's cloud-native Falcon Platform stops breaches by leveraging next-generation antivirus, endpoint detection and response, and threat intelligence.

The CrowdStrike Falcon Endpoint Protection Platform binds seamlessly with the Netskope cloud-native threat protection engine and shares detected Zero Day threats on the endpoint and other Indicators of Compromise (IOC) to bolster your ability to identify, prevent, and remove threats in the cloud. In the reverse direction, Netskope enriches CrowdStrike by sharing data on new threats discovered within cloud services and from websites visited by endpoints. Closing the loop, CrowdStrike can leverage this information to provide Netskope with details of endpoints which may already be compromised by the threat. Together, these CrowdStrike and Netskope enhanced capabilities provide joint customers with increased real-time, actionable threat forensics and enhanced malware protection on both endpoints and in the cloud.

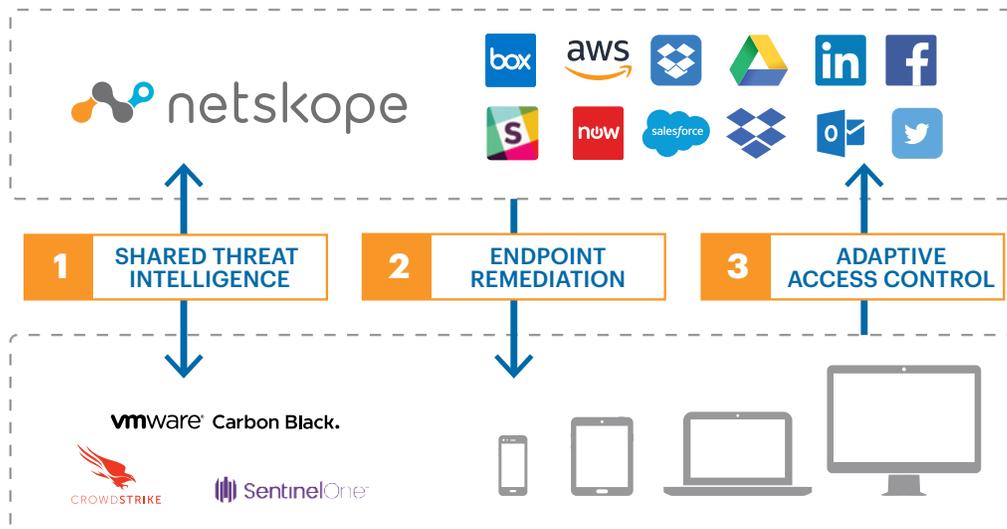


FIGURE 1: Netskope integration with EPP / EDR solutions

Single Sign On and Identity and Access Management

Adopting cloud services empowers people to get their jobs done more quickly and easily; however, it's hard to embrace the cloud without managing access and enforcing usage policies. IT struggles with cloud app "authentication sprawl," and with users accessing unmanaged cloud resources that are difficult to secure. User credentials are under constant attack from internal and external security threats. Users engage in highly sensitive transactions with enterprise resources from their corporate devices, but organizations lack control of users' personal, unmanaged devices. Enterprises need a solution centered on strong identity management that provides visibility into all user activity across multi-cloud environments and can automate policy enforcement for that activity without compromising the user experience.

Netskope integrates its cloud access security with identity management solutions, such as Okta, to give workforces flexibility while protecting enterprise apps and assets. The Netskope integration with Okta allows enterprises to discover and manage cloud services, govern cloud activities and access, and ensure consistent cloud security and compliance based on identity and context, regardless of device or location. At login, users authenticate once with Okta Single Sign On (SSO) and can immediately access all the enterprise cloud resources for which they're provisioned—but that's just the beginning.

Netskope uses the Okta identity to consistently enforce security policies for cloud access and usage beyond that which Okta has federated and authenticated. With the Netskope forward-proxy architecture, the Okta-provisioned identities are bound to each user's post-login activities, including web browsing and interactions with over 33,000 supported SaaS applications, whether approved or unapproved, on managed or unmanaged devices, regardless of location or network.

Beyond using Okta identity to federate access, Netskope uses it as a source of truth to automate and enforce strong access policies, including step-up authentication challenges for suspect behavior. Netskope continuously monitors user activities across the web and cloud services and integrates with third-party SIEM partners, such as Exabeam and Splunk, to correlate activity from on-premise security solutions.

When a legitimate user shows unusual behavior, such as excessive downloads that could indicate compromised credentials, privileged account abuse, or sensitive data loss, the questions that need to be answered are: Is the user who they say they are? Has a bad actor hijacked the credentials? Or is the device itself compromised? Netskope pauses the active session and triggers a call out to Okta to trigger multi-factor authentication and reauthenticate the user. Should the reauthentication fail, Netskope severs the active session in real-time.

Information about multiple failed re-authentications, policy violations, or anomalous behaviors can be used by integrated orchestration and governance systems like SailPoint or Splunk Phantom to place the user in a less-permissive group until IT Security teams can restore the user to a safer set of behaviors or a more appropriate set of policies. By going a step further and combining information about the status of the endpoint from CrowdStrike, security teams are better able to identify, isolate, and remediate anomalous behavior, be it identity, user, or device.

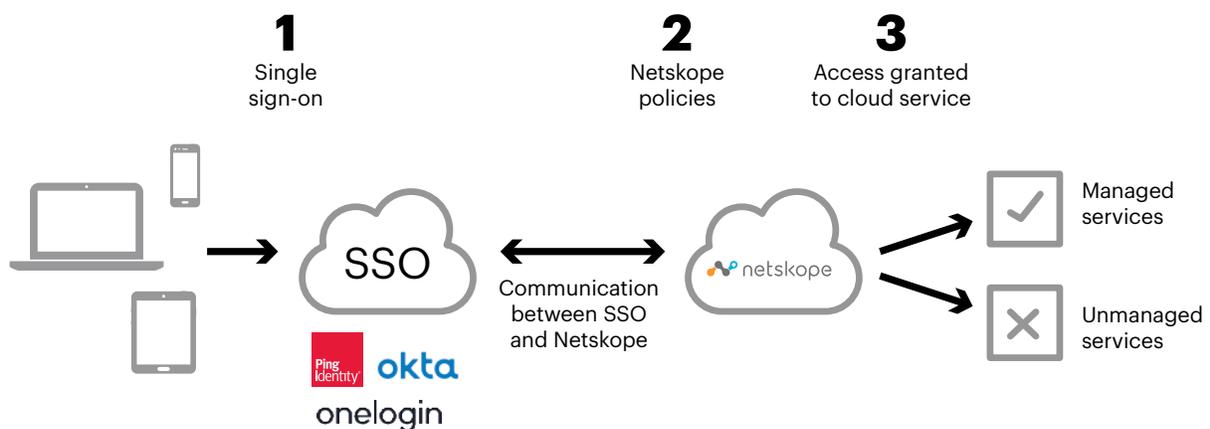


FIGURE 2: Netskope integration with IAM / SSO solutions

SIEM and SOAR for Event Management

Netskope partners with SIEMs, such as Exabeam or Splunk, to provide security teams with an integrated solution for cloud and web security and reporting, effectively making SIEMs cloud-aware and enabling enterprises to get more value from their SIEMs by discovering cloud usage and surfacing threats.

Netskope aggregates all SaaS, IaaS and web data, reducing the friction of pulling data from disparate sources and, through RESTful APIs, provides the data to Splunk for further analysis and follow-up. With the increasing volume and complexity of threats, however, security teams must capture and mine more and more mountains of data to avoid a breach. However, most SIEMs and threat detection tools that security teams use were not built with big data in mind, as they lack integrated machine learning algorithms. As the petabytes (PB) of data stored in SIEM data lakes continue to grow (and incur storage charges), security teams need to find a better way to process and correlate massive amounts of real-time and historical data, detect patterns that exist outside pre-defined rules, and reduce the number of false positives. What's needed is a way to streamline and accelerate the analysis process by surfacing relevant data in advance of funneling the data to the SIEM.

Netskope takes its integration with Splunk a step further by providing curated, high-value data points that are immediately useful for triggering SOAR workflows for automated, real-time response to the attack cycle. Netskope parses out the data and acts as an intermediary between Netskope and the receiving SIEM, enabling security teams to focus on the critical data elements that are most useful for understanding the attack and for triggering SOAR workflows. By implementing workflows in integrated SOAR solutions to surface Indicators of Compromise (IOCs) from the analysis back to Netskope for further action, orchestration tools automatically close the loop and enhance the Netskope threat prevention posture for each customer.

Netskope is expanding SOAR workflows to go beyond taking action at the beginning of an attack cycle to analyze data loss prevention (DLP) violations. By using a SOAR platform, such as Splunk Phantom, to correlate file drift activity across cloud, endpoint, and email vectors, Netskope delivers a single dashboard that presents a holistic view of DLP activity, empowering analysts to reverse engineer the attempt and answer such questions as: What ultimately failed? Was it the policy? Was it the user? Was it the device? Who else is touching the file? Where are the files ending up? How are they ending up there and who is moving them?

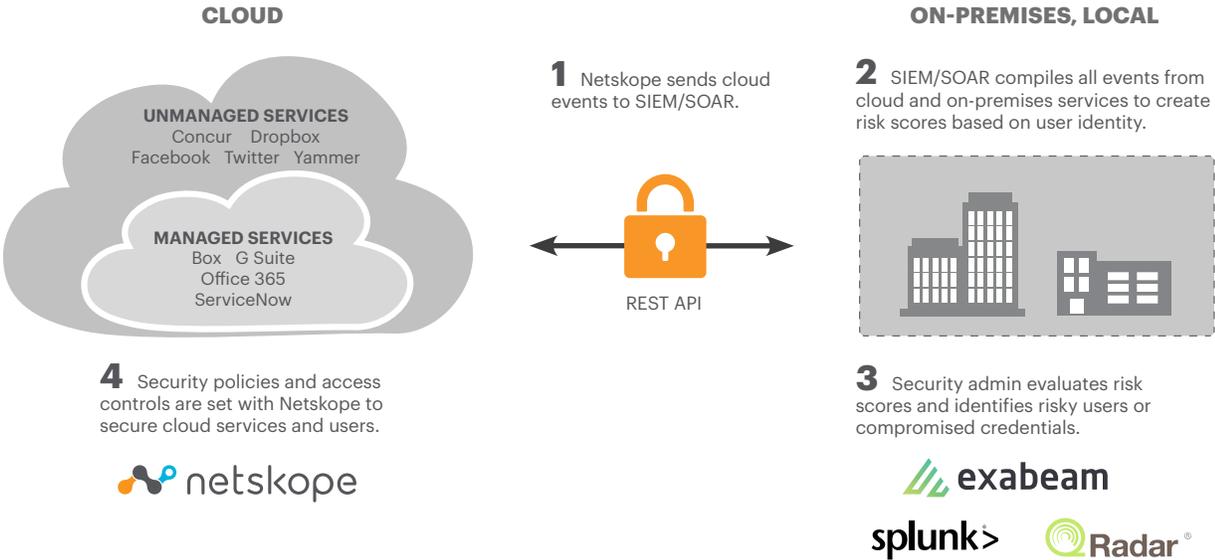


FIGURE 3: Netskope integration with SIEM / SOAR solutions

SD-WAN and Secure Access Service Edge (SASE)

It's worth noting that the traditional corporate network is vastly different from how it was five years ago. Employees are increasingly working from locations outside of the corporate network environment, bypassing perimeter-based security controls and leaving organizations vulnerable to data loss and threats. In addition, more corporate data is moving to the cloud and more data is flowing across multiple locations. Many companies already use, or are moving toward Software-Defined WAN (SD-WAN) or Network-as-a-Service (NaaS) models instead of traditional networks/MPLS (Multiprotocol Label Switching) for securely connecting an increasingly mobile workforce to their corporate applications.

Legacy approaches to security force a trade-off between performance, availability, and security, limiting the scope of what defenses can be provided, given the lack of an infrastructure that can deliver them fast, reliably, and at scale. Network gymnastics to route traffic to and from the enterprise data center make no sense when little of what a user needs remains in the data center. Neither does forcing branch-office traffic through the data center for inspection when users can directly access any cloud-based resource. These hairpinning methods only increase latency and the cost associated with dedicated MPLS circuits. The result is a growing need to reimagine network access and security to address the shortcomings that exist with legacy security and remote access tools.

Netskope provides a new approach that converges security defenses and networking services to deliver real-time security without the traditional security and performance trade-off. With Netskope NewEdge, a global, high-capacity, low-latency network infrastructure, remote workers and locations experience the full capabilities of the Netskope security cloud without compromise, resulting in a positive user experience from anywhere. NewEdge complements and enhances SD-WAN functionality with first-, middle-, and last mile access to help scale performance and delivery for remote office users.



Legacy approaches to security force a trade-off between performance, availability, and security, limiting the scope of what defenses can be provided

Lastly, this combination of software-delivered security and network services supports the emerging Secure Access Service Edge (SASE) architecture model, established by Gartner in mid 2019. SASE allows for a seamless integration of SD-WAN functionality in a cloud-based architecture where SD-WAN functionality is built natively alongside security services, which consolidates and simplifies the overall architecture. Converging security technologies such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) and Zero Trust Network Access (ZTNA) further strengthens and enhances this model whereby Security Operations teams have minimal policy enforcement points to manage and monitor across their cloud environments. The result is one common, scalable platform with unified policy controls and security capabilities to effectively protect users, data, and applications in any location.

THE NETSKOPE SECURITY CLOUD PLATFORM

The Netskope Platform was designed in the cloud, for the cloud, with high performance and scalable micro services on-demand.

The Netskope Security Cloud Platform includes the following solutions:

- CASB API-enabled protection for managed apps and cloud services (e.g. Office 365, Salesforce, Box, Dropbox), providing cloud policy controls with threat protection and DLP for data-at-rest.
- NG SWG with granular policy controls for protecting cloud services, applications, websites, and data for any user, location, or device. Decodes API / JSON-based communications, courtesy of the unique Cloud XD™ technology to better secure thousands of cloud applications, both managed and unmanaged. Includes inline defenses like advanced threat and data protection, SSL/TLS inspection, URL filtering, acceptable use, and more.
- Cloud security posture management (CSPM) providing continuous assessment of IaaS public cloud resources and configurations, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
- Zero Trust Network Access (ZTNA) providing secure, private access from users to specific apps, data resources, or cloud environments to replace legacy remote access VPN solutions.
- A single console and single architecture providing unified policy definition across SaaS, IaaS and web with cloud performance and scale, courtesy of the NewEdge global network infrastructure.

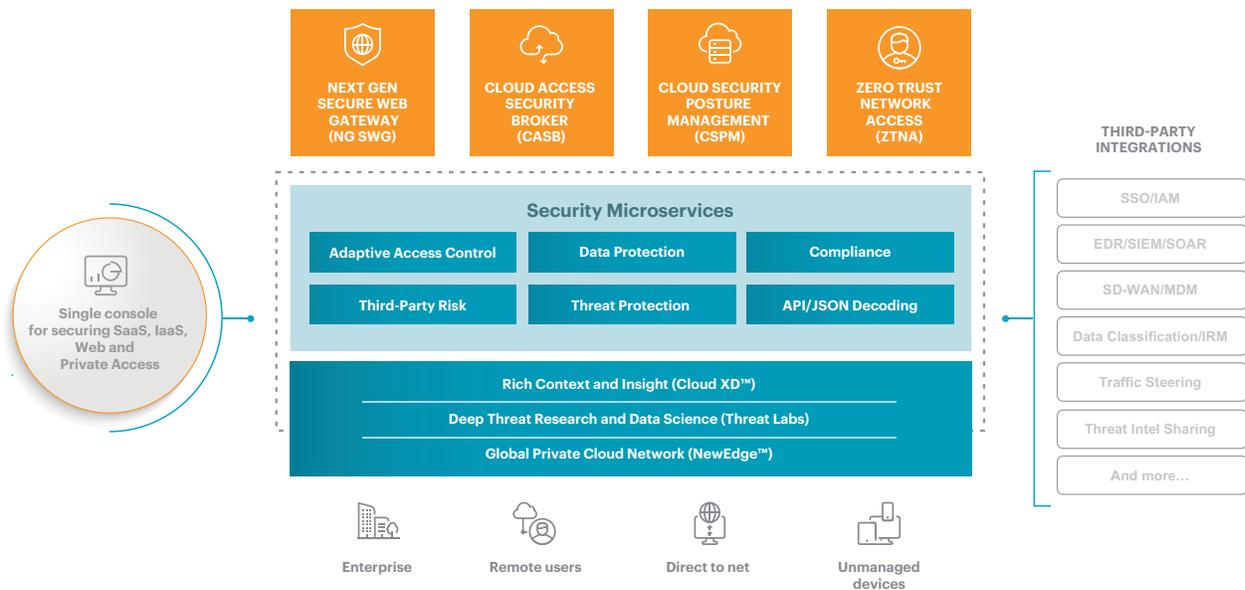


FIGURE 4: Netskope Security Cloud Platform

SUMMARY

The enterprise data center is no longer the foundation for all enterprise applications, data, users, and devices. Digital transformation, the adoption of SaaS, IaaS, and Edge computing platforms have turned the enterprise network inside out, inverting historical designs. Network and security architectures, designed for a waning era, are unable to effectively meet the dynamic secure-access needs of today's cloud-first business. It's increasingly clear that disparate point tools can no longer support enterprise security requirements. Security technology integration and architectural considerations are now equal to, or more important than, best-of-breed product functionality.

Netskope is partnering with the leading companies in cloud technology. From integrations with cloud storage services, to delivering cloud forensics to your SIEM, to providing closed-loop workflows with your identity management system, Netskope enhances your existing infrastructure to deliver the most comprehensive and efficient cloud security in the industry.

For more information

Contact your local Netskope channel partner or sales representative for more information on how Netskope can help you build a cloud-first security strategy that integrates with your existing tools.

Additionally, refer to the following webpages for more details:

Netskope Security Cloud Platform: <https://www.netskope.com/platform>

Netskope Technology Alliance Partners: <https://www.netskope.com/company/technology-partners>



The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.

To learn more visit, <https://www.netskope.com>.