Solution Brief

Netskope One Platform

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, Netskope One SSE, and the NewEdge network, Netskope One makes it easy for our customers to defend their businesses and protect their valuable data while delivering a phenomenal user experience.

Quick Glance

- Reduce costs and complexity by up to half by simplifying your IT security and networking—using one Zero Trust Engine, one client, one gateway, and one network.
- Mitigate security risks by decrypting and decoding cloud, SaaS, and web user activity with Netskope's patented AI innovations and the unmatched precision of the Zero Trust Engine.
- Accelerate the hybrid work model with the industry's fastest and most reliable network and security cloud infrastructure, including proactively managing (not just monitoring) the user-to-app experience, and everything in between.
- A converged SASE platform that brings together the functionality found in security service edge (SSE) and software-defined wide-area networking (SD-WAN) and enables organizations to easily implement an effective zero trust architecture.

"Leveraging a single vendor converged SASE platform to address security and networking use cases allows for a truly unified end-to-end strategy that results in reduced risk, greater agility, lower costs, and simplified operations while delivering a phenomenal end-user experience."

The Challenge

Legacy IT security and network architectures fail to overcome the disruption caused by hybrid work adoption, cloud applications, data ubiquity, and an ever-widening threat landscape—factors that lead to increased risk through disjointed policies, bypassing of security to maintain performance, and a poor user experience.

Network performance is critical to seamlessly delivering the right security controls. Outdated IT security architectures that route all traffic back to the data center security stack slow down performance. While siloed cloud security stacks provide an alternative, they often suffer from latency and service interruptions. In addition, disjointed security solutions result in an excess of redundant security policies, further degrading worker access and productivity.

A cloud-delivered SASE solution is the best choice to extend IT security and networking services beyond corporate boundaries—from the edge, to where users are located. But a fragmented SASE ecosystem composed of disparate, standalone IT security and networking services creates operational complexity for IT teams, saddling the enterprise with higher costs.

The Netskope One Platform

The Netskope One platform fulfills the promise of SASE by enabling the consolidation of tools and capabilities aligned with an enterprise's business needs, priorities, and operational timelines. This approach not only sidesteps the risk and costs associated with complete system overhauls or purchases of unnecessary products but also empowers IT teams with unprecedented visibility into SaaS, web, and private application traffic. It provides continuous adaptive controls, applying zero trust principles to thwart threats and regulate access to data.

The Power of One

The major components of the Netskope One platform include:

The Netskope Zero Trust Engine: Netskope's Zero Trust Engine lies at the heart of the platform, continuously gathering risk telemetry and generating extensive contextual awareness across all users, devices, applications, and data. Unlike other SSE offerings that bypass some types of traffic and services, the Zero Trust Engine decrypts and decodes traffic inline across web and SaaS applications, cloud services, and private applications for the broadest and deepest levels of visibility and protection.

The Netskope NewEdge Network: Netskope's one-of-a-kind network is purpose-built to deliver full compute SSE and SD-WAN. Featuring a global footprint of ultra-fast data centers in 75+ regions, and a local experience for every country, NewEdge is highly elastic, built for scale, and designed to provide cloud-delivered security and networking services directly to where the users and offices are without performance trade-offs.

The Netskope One Client: Netskope's endpoint agent unifies remote user access to web, cloud, and private apps, alongside data protection and voice and video optimization at the endpoint by converging SWG, CASB, ZTNA, FWaaS, DLP, and SD-WAN. Easy to use, lightweight, and deployed to perform at a high throughput, it delivers a single agent footprint for SASE and zero trust use cases, greatly simplifying desktop administration for a better user experience.

The Netskope One Gateway: The Netskope One Gateway, offers both hardware and virtual form factors and supports the widest range of deployment options, including cellular gateways, micro to large branch, data center and multi-cloud environments. Netskope One Gateway consolidates disjointed appliances into one unified SASE gateway. It offers multiple services like Routing, WiFi, SD-WAN, App FW, IPS, IoT Device Intelligence, DEM and Edge compute, along with a seamless on-ramp to Netskope One SSE.

The Netskope One Orchestrator: A single point for policy management across all components of the Netskope One platform. The 100% cloud-based console unifies management of SSE & SD-WAN across branches, remote sites, multi-cloud and remote users, and provides a built-in SD-WAN controller that separates the control & data planes.

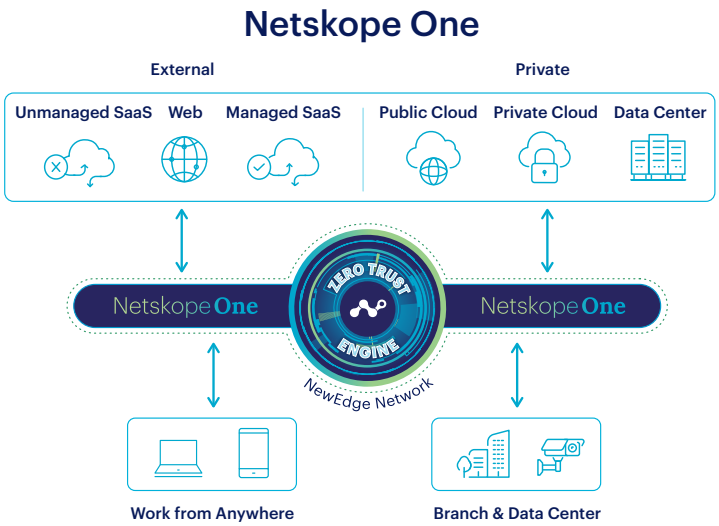
Risk Minimization with Context-Aware Continuous Adaptive Trust

Relying on typical castle and moat defenses, legacy network and security architectures implicitly trust authorized users to freely explore the corporate network and access data. The zero trust security model rejects this outdated approach, instead affirming that no user, device, or application should be trusted by default, unless verified. The Netskope Zero Trust Engine further advances this concept with continuous adaptive trust, using context to determine—in real time—the level of access that should be granted based on changing circumstances of the user, the app, the data, and many other factors.

The key to being able to do this is the Netskope Zero Trust Engine, which gathers real-time risk telemetry across all parts of the user's transaction and uses that context to enforce the most adaptive, single-pass policy controls across all cloud, web, and private applications—allowing IT admins to make real-time risk management decisions across all parts of every transaction.

This is a big difference for IT admins, who are used to the conventional, binary "allow or block" choices for access. Using a more sophisticated and nuanced execution of zero trust, IT admins minimize risks with actions that include allowing the traffic, blocking the transaction, coaching the user inline, prompting an authentication from the user, soliciting justification for any action, or isolating the access from other operations.

Continuous adaptive trust signifies a move away from the simplistic binary approach of "allow or deny" in policy controls, offering a more sophisticated and nuanced execution of zero trust.



Greater Business Agility with Lightning Speed and Dependable Resilience

Netskope One boosts business agility and productivity with the lightning-fast, single-pass inspection architecture of the Zero Trust Engine together with the dependable resilience and performance of the NewEdge network.

Netskope's single-pass architecture is designed to minimize end-to-end latency with average scan times of less than 15 milliseconds. This is accomplished by decrypting traffic only once instead of multiple times by each of the security services. The single-pass architecture also enables security events generated across Netskope One SSE offerings to be visible through a single console.

The NewEdge network has been designed to connect millions of users, offices, and locations to the full lineup of Netskope's SASE services from any location worldwide, with minimum latency. Customers enjoy full compute at every data center with traffic steered to NewEdge using flexible deployment options, including the Netskope One Client and Netskope One Gateway. Netskope One further layers on Netskope One Digital Experience Management (DEM) to monitor, measure, and investigate the user experience and performance from client to application, including hop-by-hop visibility and platform processing latency.

The Netskope One platform backs up its cloud security services with industry-leading service-level agreements (SLAs) to ensure customers benefit from robust data-centric security without the performance trade-offs typical of legacy appliance-based approaches or the unpredictable performance and added latency of either the public cloud or virtual points of presence (PoPs).

Advanced Data and Threat Detection Using AI/ML Innovations

The exponential rise of AI use by cyber criminals has caught most organizations' cyber defenses off guard. Therefore, a modern approach to data security and threat protection also uses AI and ML to overcome these emerging cybersecurity challenges. As a leader in the transformation of network, cloud, and data security, Netskope is committed to responsibly using AI/ML techniques to protect data and defend against threats.

Netskope has pioneered cloud data protection for SASE architectures to be simple yet powerful. Unlike legacy data security solutions that use a combination of regular expressions, keywords, and dictionaries to identify sensitive data, the Netskope One platform automatically applies over 3,000 advanced AI/ML-based data classifiers and 20 patented AI/ML detection techniques to perform high-fidelity detection and classification of sensitive data within business documents stored in the cloud. Additionally, Netskope's image detection AI/ML models use deep learning algorithms to detect and classify sensitive data embedded within image files and image-heavy documents.

In addition to this, Netskope's SkopeAI innovations—present in the platform since Netskope's founding—unleash the power of AI/ML to detect and protect new unstructured data with high reliability and speed by democratizing modern data and threat detection techniques to move at speeds the era of AI requires.

Key capabilities include:

- SkopeAI's user and entity behavior analytics (UEBA) uses over 50 trained models with 100+ detectors from inline and API inspection to discern normal behavior patterns from internal baselines versus those arising from malicious insiders and outside threat vectors.

Key capabilities continued...

- SkopeAI's threat protection prevents a wide range of evasive and never-seen-before threats, including AI-generated threats, multivarious attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content.
- SkopeAI showcases cutting-edge advancements in securing generative AI by safely enabling their use across the organization, offering the broadest classification and visibility of GenAI apps in use with ML-assisted discovery and risk categorization.
- SkopeAI also presents several enforcement options to stop the upload and posting of sensitive data to generative AI apps like ChatGPT and provides real-time coaching alerts to inform users of security policies in order to minimize repeated risky behavior.

BENEFITS	DESCRIPTION
Reduced security risks	Netskope customers report that they have reduced security risks by 14% for cost avoidance of a data breach using the Netskope One platform thanks to its ability to quickly target and control activities across cloud services and websites to protect sensitive data and stop threats.
Tighter overall security	In addition to risk reduction, security admins using Netskope One report numerous other benefits that tighten overall security, including the ability to instantly identify 1000s of shadow IT SaaS apps, manage endpoints regardless of location, significantly reduce the number of policies, and align policies at the level of the tenant.
Increased business agility	Customers using Netskope One have reported a 22% increase in employee productivity due to a remarkably better user experience, faster application performance, and increased overall satisfaction with IT.
Lower total cost of ownership	By eliminating ineffective legacy tools and using Netskope One, security admins have realized savings of 63.5% by reducing unpredictable CapEx expenditures and moving to a predictable OpEx model that supports operational cost efficiencies and simpler budget projections.
Reduced complexity	Security admins have recounted extraordinary ease in performing a continuous audit of their multi-cloud environment and automatically fixing security misconfigurations that inadvertently expose sensitive data.
Faster time to value	Customers stated Netskope One provides the right balance of protection and speed by shifting their mean time to security from months or years to days, for a much faster time to value toward secure digital transformation.
Accelerated network transformation	On the network side, Netskope One customers have reported significant acceleration in their network transformation because of being able to eliminate expenses related to legacy MPLS WANs and private connections to key SaaS or cloud providers, and by incorporating networking advancements like Netskope One SD-WAN.
Refocused FTEs	Netskope One customers report they are able to deploy more seats, with fewer people, and faster than they expected, allowing them to refocus their IT workforce on other strategic initiatives.