netskope

SOLUTION BRIEF

Netskope Security Service Edge (SSE)

Netskope Security Service Edge (SSE) is a data-centric, cloud-native, and fast security solution with adaptive access, advanced data and threat protection for users anywhere, on any device. Providing unrivaled visibility, real-time granular controls across an optimized global cloud infrastructure, Netskope enables security and networking teams to realize their digital transformation journey.

KEY USE CASES

- **Provide greatest visibility and context** for business and risk insights across web, apps, users, and data.
- **Secure web and cloud access** for IaaS, PaaS, SaaS, and enforce corporate policies, compliance regulations, and best practices.
- **Detect and mitigate threats** across web, SaaS applications, cloud services, and private applications.
- **Connect and secure remote workers** when accessing the web, cloud, and private applications.
- **Identify and protect sensitive information** across web, cloud, and private applications.

"SSE technologies allow organizations to support workers anywhere and anytime, using a cloud-centric approach for the enforcement of security policy."

https://www.gartner.com/smarterwithgartner/4-must-have-technologies-that-made-the-gartner-hype-cycle-for-cloud-security-2021
Contributor: Susan Moore

THE CHALLENGE

The inversion effect of cloud applications, users, and data outside of the corporate network, along with the new work-from-anywhere workforce, demands a new approach to IT security and network architecture.

Cloud application traffic has overtaken web traffic in the enterprise, creating blind spots and complexity with existing legacy security and network solutions that were designed for access to data centres through on-premises security stacks.

These challenges demand a new approach to cloud security that delivers the simplicity and agility for access, security, and performance that businesses need for their successful digital transformation journeys, while securing their critical data assets.

NETSKOPE SECURITY SERVICES EDGE

The Netskope Security Services Edge (SSE) solution is easy to use, and secures your transactions wherever your people and data go. Netskope reduces risk, accelerates performance, and provides visibility into any cloud, web, and private application activity. Be ready for anything on your SASE journey with the SSE that puts cloud and data security first.

NETSKOPE DELIVERS SIMPLICITY WITH POWERFUL INTEGRATED CAPABILITIES

At every license level and in every product configuration, Netskope's differentiated SSE offers customers deep visibility across ALL traffic, including web and SaaS applications, cloud services, and private applications. Our instance awareness and profiles for over 41,000 cloud applications provide granular control of activities that enable customers to secure their remote workforce and ensure successful cloud adoption. The Netskope SSE solution delivers these powerful access control, threat, and data protection capabilities in simple, straightforward packaging for customers to easily consume, and implement Netskope either in forward proxy or reverse proxy for web, private applications, and SaaS applications (both approved and unapproved), all managed through a single console

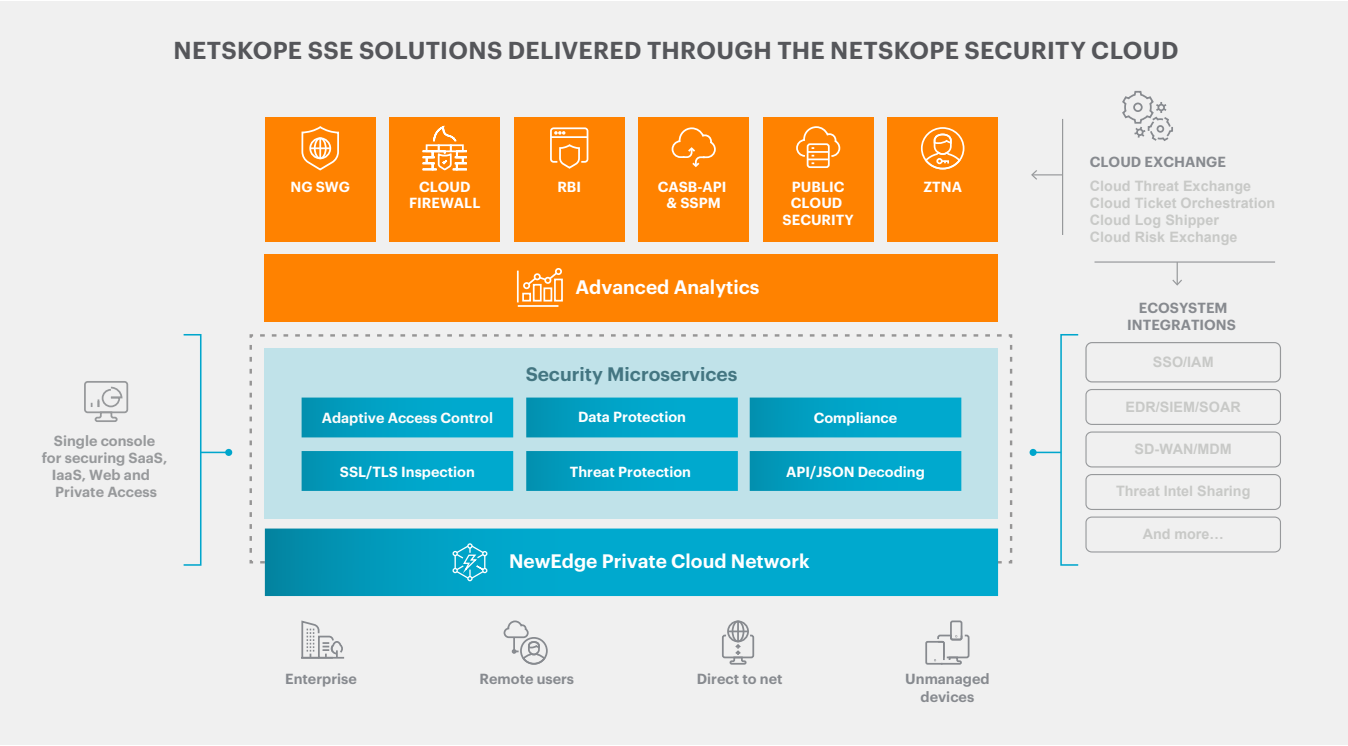
Netskope SSE delivers visibility into more than 41,000 cloud applications, with inline user coaching and controls for activities across these applications and their application instances.

SOPHISTICATED CLOUD SECURITY

Netskope's sophisticated cloud security has the deepest visibility and granular context across apps, users, and data with Netskope patented CloudXD as the foundation for our SSE services. Upon this foundation are unique capabilities that create the structure and attributes that are key to effective SSE in action:

With rich context from CloudXD and trust scores for users and apps, Netskope SSE enforces the most adaptive, single pass policy controls across all cloud, web and private applications for stronger risk management with simplified operations.

- AI/ML-enabled web and cloud app categorization and private app discovery enable strong, granular policy enforcement.
- Cloud app instance awareness, Netskope patented TrueInstance, enables dynamic detection of app instances at scale and is critical for data protection and cloud enabled threat prevention.
- The API enrichment effect of app coverage across inline and API for the most visibility and control between personal and managed instances for any application or cloud service (i.e., support for 250+ services in AWS including by instance).
- ML-enabled trust scores for cloud applications, Netskope CCI - Cloud Confidence Index, and users, Netskope UCI - User Confidence Index capture anomalies and shifts that can trigger adaptive policy controls and automated workflows for investigations.



CONTINUOUS ADAPTIVE CONTROLS APPLY ZERO TRUST PRINCIPLES

Netskope Continuous Adaptive Controls apply Zero Trust to SASE, multi-cloud, and hybrid architectures to control access, threat protection, and data movement. Explicit, granular access controls across apps, app instances, and app activities reduce the attack surface against primary threat vectors such as risky cloud apps, cloud phishing, and data loss through personal or sanctioned instances of corporate applications, such as M365 or Google Workspace. With Cloud XD and the trust scores for apps and users, Netskope SSE solutions continuously enforce data movement policies, and threat prevention, with inline user coaching and step-up challenges for unintentional or unapproved access or data movement to or between applications.

Netskope has led the way to educate the market on the rise of cloud enabled threats and data theft through threat tactics exploiting personal instances of managed applications and public cloud environments. Netskope advanced threat protection is proven at preventing threats across web, SaaS, IaaS, and all ports/protocols, mitigating vulnerabilities with exploits, and minimizing blind spots for internal/insider user/entity behavior anomalies with real-time policy response options.

Netskope's rich cloud metadata from Cloud XD, and network and security events and alerts, for real-time views via pre-built customizable dashboards for any audience, from CxO, HR, BOD, to SecOps and IR teams, allow SecOps teams to work with data that they know best, without reliance on external tools, to get a deeper understanding and root cause analysis from any perspective – threats, users, data, traffic type (apps, web, custom apps and services, data). Netskope also provides high-performance log streaming services to SIEMs, data lakes, and cloud storage to enable SOC and MDR process workflows for incident response and investigations.

Inline user coaching effectively reduces the noise of inadvertent user activities, such as sharing a file to a personal app instance or uploading to the app instance for another business unit, which may include third-party users not authorized for the sensitive data placed in their app instance. Reducing the attack surface with granular controls and reducing the noise of user errors with inline coaching clears the field to apply advanced data loss protection to sensitive and business-critical data, a company's most important asset.

THE GOLD STANDARD FOR CLOUD DATA PROTECTION

Netskope is the gold standard for cloud data protection, as acknowledged by industry analysts and adoption in the market.

Netskope has pioneered modern data protection for multi-cloud and hybrid environments to be simple yet powerful. Unlike the rigid experience with legacy, appliance-based DLP, Netskope has innovated cloud data protection for SASE architectures with the scale, accuracy, and precision needed to deliver security with agility. Netskope uniquely applies AI/ML for scale, efficacy, and automation critical for app discovery, data detection, and classification for enterprises with business-critical data in the cloud.

Corporate traffic today has 20% images and image-borne text on average, further complicating data security. Netskope AI/ML-based image classification has deep learning models for content such as passports, government IDs, images of credit cards, and Social Security cards. Images are detected with higher accuracy and speed without extracting all text from images. Netskope also supports detection of screenshots, which has become highly relevant with remote workforces and is particularly important when screenshots are taken from employees that handle sensitive data. With this capability, security teams can detect screen captures from specific groups of employees, with fewer false positives on image matches, at scale. Netskope provides AI/ML-based classifiers for documents including source code, patents, contracts, resumes, and agreements.

BUSINESS PRODUCTIVITY, AGILITY WITH FAST USER AND DIGITAL EXPERIENCE

Netskope boosts business productivity and agility with the fastest user experience and optimized application performance with its NewEdge security private cloud. Leveraging extensive peering with web, cloud, and SaaS providers combined with fast, low-latency traffic on-ramps and more than 50 locations globally with compute for real-time, inline security traffic processing at the edge, closer to users, Netskope backs up its cloud security services with industry-leading Service Level Agreements (SLAs). By steering traffic to NewEdge using Netskope's flexible deployment options, including Netskope Client and integration with existing network investments such as SD-WAN, customers benefit from robust data-centric security without the performance trade-offs typical of legacy appliance-based approaches or competitive alternatives that rely on the unpredictable performance of the public cloud. Customers report that "enhancing user experience with NewEdge has been one of the most valuable parts of their Netskope experience," with customers typically seeing "applications perform 50% better" and in one instance a "6x improvement" for a customer's top SaaS application. Netskope also provides digital experience management to monitor, measure, and investigate performance of NewEdge and data center security services.

BENEFITS	DESCRIPTION
Cloud Native SSE solution	**Netskope SSE solution is integrated on a single platform and includes:** • Cloud-native **next-gen secure web gateway (NG SWG)**, multimode **cloud access security broker (CASB)**, and **zero trust network access (ZTNA).** • Additional converged capabilities include **data loss prevention (DLP), advanced threat protection (ATP), cloud firewall (CFW), remote browser isolation (RBI), user/entity behavior analytics (UEBA),** and **advanced analytics (NAA)**, all within a single-pass architecture, delivered from a single platform, managed by a single console, and driven by a single policy engine • Complete threat and data protection with sensitive data awareness and real-time enforcement and at-rest inspection, with the combination of inline traffic analysis and cloud API interaction • Resilience and availability with cloud-hyperscale designed, cloud-native infrastructure, NewEdge, with industry-leading uptime/availability and latency SLAs
Enable Future of Work	**The Future of Work requires direct access for all users and office locations:** **Work-from-anywhere model with:** • Direct access to cloud, web, and private applications • Open collaboration across apps and service • Increase productivity with fast, global user experience **Simplify and transform branch network and security:** • Reduce backhaul costs with direct access from branch locations • Apply consistent security controls in the cloud, regardless of location • Alternative traffic-steering approaches (e.g., SD-WAN at branch) for low-cost, in-region connectivity
Redefine Risk Management and Data Protection	**Modern risk management with advanced data protection and threat protection for all users and data:** **Advanced data protection includes:** • AI/ML-enabled detection for the most accurate and comprehensive coverage • Detection of sensitive data in newer risks like screenshot and image identification • Granular control of data movement, including between personal/corporate app instances • Posture management to ensure correct access and permissions, reduce threats from misconfiguration and configuration drift, and ensure compliance with regulations **Threat protection across SSE that will:** • Address web and cloud-delivered threats • Automate bidirectional IOC sharing for the latest threat intelligence • Unpack and deobfuscate for pre-execution analysis, sandbox files • Apply ML-based analysis including for malicious Office documents • Use remote browser isolation for risky websites • Determine behavior anomalies to assess risk and insider threats • Apply firewall controls across all egress ports and protocols for users and offices

BENEFITS	DESCRIPTION
Simplify Operations	**Simplify operations by consolidating and streamlining security to the cloud:** **IT consolidation to the cloud:** • Of key security services for web, cloud, and private apps to a cloud-native security platform • Reduces TCO (total cost of ownership) by eliminating appliances, multiple licenses for SW and support and via resource efficiencies associated with security services consolidated on a cloud platform • Enhances security effectiveness with single-pass inspection of cloud apps and web to stop threats and data loss **Enhance and simplify operations with:** • The single-pass policy approach of SSE for up to 10x policy simplification • Inline user coaching and policy refinement streamlines security operations • Dynamic visual analytics for real-time drill down investigation and analysis