Netskope One SASE

Data Sheet

Simplifying security, network and AI transformation

Legacy perimeter-based architectures were never built for today's AI, cloud, and hybrid work era, resulting in security gaps, poor user experience, uncontrolled AI adoption, and rising operational costs. Organizations need a converged platform that delivers security, agility, and simplicity without compromise

Why is Netskope the best choice?

Netskope One SASE converges market-leading SSE and next-generation SD-WAN onto a unified platform, protecting users, applications, data, and IoT with AI-powered zero trust security, securing cloud, AI, web, SaaS, private apps and on-premises environments, while delivering fast, reliable and optimized access from any location or device.

Industry's first converged SASE offering

- Comprehensive, cloud-native SASE platform, leveraging the power of one engine, one console, one network, one SASE gateway and one unified client.
- Enhanced visibility and control across web, SaaS, private applications, and the entire AI ecosystem—from shadow AI to agentic AI—with Netskope's patented Zero Trust Engine, AI innovations, and the NewEdge Network (the world's largest private SASE cloud).
- Phenomenal user experience with unparalleled service coverage, context-awareness, performance and resilience, along with full hop-by-hop visibility from the user to the application.
- Speed and resilience with one secure, optimized SD-WAN solution and a seamless on-ramp to Netskope One SSE services, providing industry-best SLAs for latency, decryption, and in-depth security inspection.

"Netskope is mature, and offers the full set of capabilities you would expect for a SASE solution at the enterprise level."

– Solution Architect and Security Lead, Diversified Financial Services Company

Key benefits and capabilities

Full platform convergence

Reduce cost and complexity through a fully converged SASE solution with one Zero Trust Engine, one SASE gateway, one SASE client, one network, one console, and a fully integrated AI security solution.

Ease of use

Streamlined management made possible by a unified platform and one console, offering an integrated view and control over networking and security functions. Fast, transparent, reliable user experience from the unified Netskope One client.

Enterprise-grade security

Extensive breadth of security services, encompassing SWG, CASB, ZTNA, firewall, and AI security supported by the most comprehensive data and advanced threat solution.

Context-driven zero trust

Unmatched risk context awareness across users, devices, applications and data, and policy enforcement with continuous adaptive trust.

SASE automation

Bring new sites, users, and cloud environments up in minutes with zero touch provisioning. Leverage AI-driven operations for network monitoring, anomaly detection, proactive troubleshooting and automatic rectification of any poor network conditions.

Global coverage

Unparalleled service coverage, performance and resilience with the industry's fastest and most reliable private security cloud infrastructure. A global footprint across 80+ regions also includes AI Fast Path to optimize connectivity to critical AI destinations.

Web security	
Feature	**Capability**
Authentication	Single sign-on (SSO) / multi-factor authentication (MFA) / identity and access management (IAM), SAML, AD, and LDAP across web, SaaS, and private applications.
User/admin authentication identity provider support	Netskope supports user authentication using turnkey integration by standardizing identity information exchange across different cloud applications. Netskope supports SCIM integration with Microsoft Entra ID (formerly Azure AD) and Okta, PingOne, OneLogin, Google Secure LDAP and other SAML 2.0 using REST API v2 token authentication. This setup facilitates seamless user management, automating identity synchronization and reducing manual tasks.
SSL/TLS inspection	Real-time end-to-end SSL/TLS decryption with native support for TLS 1.3 and support for customer signed CA certificates.
Web filtering	Granular policy enforcement across 130+ categories, including 14 security risk categories, languages for 190+ countries, custom categories, translation services, safe search, silent ad blocking, dynamic ratings for unrated web pages, site lookup tool, reclassification service, and traffic inspection by category.
Social media controls	Integrated SWG and CASB engine covers 290+ social media apps with control for 20+ activities.
Targeted or extended browser isolation	Remove the risk of active web-based threats and prevent data loss. Includes threat protection on file downloads and DLP on file uploads. Targeted RBI for risky website, or extended RBI for web categories and apps related to personal communications.
Transaction event streaming	Near real-time streaming of web proxy transaction events into SIEMs, data lakes, or cloud storage.
Bandwidth control	Ensure web bandwidth usage for business-critical applications is prioritized and bandwidth usage for non-work related traffic is limited.
SaaS security	
Feature	**Capability**
Real-time and API	Multimode provides comprehensive coverage of SaaS apps by combining the context harvesting and in-app remediation benefits of API with the real-time blocking, user coaching, and shadow IT/usage visibility benefits of inline security. Enrich real-time protection policies with API-harvested context for granular, surgical controls that lower alert fatigue and impact on end users.
Remediation	Robust set of remediation actions upon detecting risk. For example, block a risky action in real time, send an alert to a specific user, tag/label/delete/quarantine/legal hold/encrypt a file, change/restrict sharing and access to content, change content ownership, etc. Built-in integrations with industry-leading SIEMs, ticketing services, and other remediation/change management workflow services enable easy, seamless integration with your own internal remediation workflows.
App discovery and control	Discovery and instance detection for over 800 cloud services in any language. Granular activity visibility such as viewing, uploading, downloading, sharing, editing, renaming, creating, and deleting. Add custom SaaS and IaaS services with the Universal Connector Framework (UCF) in order to get inline visibility including logins, uploads, downloads, and posts, as well as inline control benefits such as user alerts (for user coaching), restricting access type (forward or reverse proxy, client or tunnel), triggering step-up authentication, device classification, alerting, and email notifications.
Data discovery and control	Discover and classify data with full SaaS repository and IaaS bucket retroscan, then apply remediation actions to take control of sensitive data. The content metadata as well as classification results are made available in an inventory dashboard for reporting and analysis.

SaaS security - continued	
Feature	**Capability**
Posture management	Continuous posture management, including configuration monitoring, audit, asecurity control adjustment controls, and share settings for over 30 cloud services. Compliance auditing of security posture is available for over 15 SaaS applications and three IaaS services, with more than 300 predefined configuration compliance policies that align to industry standards and 1000+ out-of-the-box configuration rules.
Data lineage	Netskope One Data Lineage provides visibility with context, tracking a file's entire journey from origin to destination. By documenting every user modification, rename, and movement across SaaS, endpoints, and AI tools, it creates a definitive visual chain of custody. This visibility enables security teams to investigate insider risks in minutes and simplify compliance audits. It ensures sensitive IP remains protected and governed, regardless of how it transforms or where it travels.
Data security posture management (DSPM)	Netskope One DSPM leverages Netskope's robust DLP policies and automated AI-powered data classification (3K+ data identifiers, 30+ AI/ML models, 40+ regulatory and compliance templates) and ensures that you have full and continuous visibility to the structured and unstructured data your organization has at rest or in use across the authorized and unauthorized SaaS, PaaS, IaaS, and the on-premises locations your employees use. This visibility enables security teams to simplify data discovery and regulatory compliance.
App risk assessment	The Netskope Cloud Confidence Index™ (CCI) is the industry's largest app trust database, evaluating and risk-scoring cloud and SaaS applications based on objective criteria adapted from Cloud Security Alliance guidance. The risk scoring system assesses an app's enterprise readiness by evaluating dozens of attributes and then assigning an overall score. More than 100+ criteria are evaluated, including vulnerability and exploit assessment, recent breaches, compliance certifications, data protection features, privacy policies, access controls, and audit readiness. Customize CCI scoring by adjusting score weighting or adding custom attributes.
Total SaaS and AI app coverage	Netskope maintains the industry's most comprehensive SaaS and AI app inventory, covering a total of 632,688 SaaS apps and app activities, with risk scoring applied across the majority to enable precise, policy-driven access control. Total number of SaaS apps including app activities with risk score: 457,715 Total number of SaaS apps including app activities without risk score: 146,223 Total number of AI apps including app activities with risk score: 9,033 Total number of AI apps including app activities without risk score: 19,717
3rd party app risk assessment	Provides visibility for SaaS marketplace and custom 3rd party OAuth app (aka SaaS-to-SaaS or cloud-to-cloud apps) usage across the organization. Patent-pending risk assessment algorithm assigns a trust score based on static attributes (e.g. developer, OAuth scope or permissions) as well as usage and activity.
Advanced analytics	CASB-generated data (i.e. metadata, events, alerts, incidents) are available in Netskope One Advanced Analytics for custom reporting and analysis.
Dedicated egress IP addresses	Enhance SaaS security by only allowing access from unique, static dedicated egress IP addresses to your business-critical applications and cloud services.

Private application security	
Feature	**Capability**
Private application coverage	Unlike conventional ZTNA solutions that are limited to endpoint-initiated apps, Netskope One Private Access supports connectivity to all enterprise applications.
Agent-based access	Easy to use, lightweight, and deployed to perform at a high throughput, the Netskope One Client unifies remote access to private apps, web, and cloud, alongside data protection and voice and video optimization at the endpoint. It efficiently steers agent-based traffic to the Netskope NewEdge Network for optimized security and performance.
Agentless access	Allows third parties and employees to connect to private apps from any unmanaged device using their web browser, without the need to install an agent. Supports web apps (HTTP/HTTPS), and non-web/ thick clients (RDP, SSH, Telnet, VNC). For added data protection, enable or disable DLP inspection for unmanaged devices.
Universal ZTNA/local broker	Provides a consistent access experience for seamless work, whether remote or on-premises, at a branch or campus location. The local broker delivers fast, direct access to private on-premises apps, eliminating unnecessary hairpinning of local user traffic to cloud-based PoPs for optimal performance.
Assured application experience	Delivers reliable, optimized access to private applications, including voice and video, directly from the Netskope One Client with the following capabilities: - App-aware prioritization: Classifies and prioritizes traffic by application to ensure consistent quality for latency-sensitive workloads. - On-demand remediation: Mitigates packet loss for UDP traffic across single or multiple unstable links (Wi-Fi, LTE, 5G tethering). - Path selection and brownout/blackout protection: Sub-second detection and failover to maintain session continuity across degraded or failed links. - Multi-link active/active and active/standby: Leverages multiple uplinks simultaneously with policy enforcement based on processes running on the endpoint.
Application discovery and management	Empowers administrators with visibility and insights into private app usage and traffic patterns. Combined with our API automation tools to programmatically manage discovery, infrastructure and policy objects, you can accelerate and scale your Netskpe One Private Access deployment.
IoT/OT security	Netskope One Device Intelligence integrated within the Netskope One Gateway enables secure IoT/OT environments in branch and factory locations through AI/ML-driven device discovery, classification, and risk assessment. Devices such as ATMs, cameras, smart robots, and industrial sensors are automatically identified, risk-scored, and segmented via SD-LAN policies—enforced locally on the Netskope One Gateway and SSE or through multi-vendor switches, APs and firewalls.
Adaptive access controls	Enforces identity- and context-aware access policies based on user identity, device identity, device posture, and app risk. Dramatically reduces the attack surface and constraints lateral movement.
Multiple IdP support	Seamless integration with identity providers such as Azure AD, Okta, and more, enabling authentication for third-party users and automated user provisioning and deprovisioning via SCIM for streamlined identity management.
Privileged access management controls	Netskope One SASE integrates the privileged access management controls within Netskope One Private Access, offering agentless access to web applications over RDP, SSH, VNC, HTTP, and HTTPS, along with a user portal for seamless access, user credential management and controls for inline data protection, security and session recording.

Firewall as a service	
Feature	**Capability**
Firewall services	FWaaS 5-tuple based policies, user-based access control, FQDN/PQDN based access control, application identification and control on standard and non-standard ports.
DNS security	DNS-based security, passive DNS inspection, identification and control of known and unknown DNS tunnels; support for DGA generated domains; support for newly registered domains; ability to control resource records; allow and block list; ability to sinkhole DNS connections further analysis; protect traffic going to private DNS servers (remote user protection); DNS resolver for DNS traffic steered to Netskope; ability to redirect DNS traffic to custom DNS servers; failover support to customer and Netskope resolvers in case primary DNS fails.
DNS-as-a-service	Netskope tracks and categorizes over 314 million domains globally. DNS security is a native platform component—no additional agents or secondary configurations are required. The Netskope DNS resolver runs over the NewEdge infrastructure across 120+ data centers, ensuring consistent protection at the edge without backhauling traffic. It is built on massively over-provisioned infrastructure to ensure resilience under extreme load and is capable of running any number of DNS queries
IDS/IPS support	IPS/IDS support with 136,000 signatures, bandwidth control for traffic, unified policies with web traffic, ability to export events, Netskope One Advanced Analytics integration.
SOCKS5 proxy	SOCKS5 proxy listener for all access methods (client, IPsec, GRE) supporting all TCP-based protocols including FTP, SFTP, FTPS, and Telnet. Handles TCP traffic on standard and non-standard ports, DNS resolution, and supports IP addresses and FQDNs. Inline policies for visibility and control including threat protection and data security, and no authentication required with usernames or passwords.
Platform service - data security	
Feature	**Capability**
Integrated DLP	Single DLP solution for web in-line, SaaS at-rest and in-line (93k+ apps and app instances), IaaS/PaaP at-rest and in-line, private apps, email in-motion and at-rest and on user endpoints. Common policy, reporting/analytics, logs, incident management and client management experience across all the supported channels, with DSPM capabilities to discover content across all channels with consistent remediation options.
Comprehensive DLP coverage	2,100+ different true content types (structured and unstructured content). 40+ compliance templates and customization with 3,000+ identifiers across 132 countries. Customization using keywords, regex, dictionaries. Exact match and fingerprinting for precise matches. OCR for automatic image coverage. ML-based detection for increased accuracy and reduced administrative overhead.
ML-based detection	26 out-of-the-box ML-based classifiers (e.g. source code, credit cards, resumes, patents, M&A docs, screenshots, passports, driver licenses, tax forms, medical) across both text and images. Customized ML classifiers available by providing customer-specific training data to Netskope, enabling detection of content types unique to the customer's environment.
Tokenization	Tokenization capabilities for formatted fields based on industry-standard methods. Tokenization of field data while preserving a configured number of leading or trailing characters/digits in plain text.
Encryption	File-level encryption for all file types using an AES-256 Galois Counter Mode (GCM) cipher. Choice of cloud-based KMS with a FIPS 140-2 Level 3 certified hardware security module (HSM) or the option to integrate with their existing KMS.
DLP integration	Seamless DLP policy integration and incident management and remediation workflow with vendors including Microsoft Purview, Digital Guardian Network DLP, Forcepoint, McAfee DLP Prevent and Symantec DLP.

Platform service - data security - continued	
Feature	**Capability**
Encryption and tagging integration	Integration with vendors including Microsoft Information Protection, Fortra (Vera, Titus), Box Shield Classification Labels, Google Labels.
DSPM integration	Netskope One includes DSPM capabilities natively as well as integrating with third-party DSPM providers such as BigID, Eureka and Cyera in order to enforce real-time zero trust policies.
DLP API	Netskope One DLP On Demand delivers unified data security by empowering developers to integrate data protection directly into custom applications and workloads via REST APIs. Deployable on-premises or in public clouds, it enables secure, local processing of structured and unstructured data while maximizing your existing DLP policy investments.
Platform service - threat protection	
Feature	**Capability**
Standard threat protection	Anti-malware, ML-based malicious PE file detection, phishing detection, and HTML smuggling, plus sandboxing to corroborate all AV and ML detections, multiple threat intel feeds, web IPS, and true file types.
Advanced threat protection	Multistage sandboxing with deobfuscation and recursive file unpacking for 350+ types, pre-execution and analysis for 3,500+ file format families with 3,000+ static binary threat indicators, machine learning for PE, Office, PDF malware, cloud sandboxing for 30+ file types, patient zero protection and alerts, sandbox API, retrohunt API, and inline malware retention. Plus add-on options for network threat hunting and deepscan on demand.
Cloud TAP	Enables traffic visibility and analysis with traffic packet captures (PCAPs) for compliance requirements, and exports traffic and session keys into third-party analysis solutions for traffic steered from endpoints and offices to the Netskope One platform.
Platform service - user and entity behavior analytics (UEBA)	
Feature	**Capability**
Standard UEBA	Sequential anomaly rules (9) to detect cloud app bulk uploads, downloads, deletes, proximity, failed logins, shared credentials, rare events, risky countries, and data exfiltration between company and personal instances. Instance awareness for apps in sequential anomaly rules.
Advanced UEBA	ML-based anomaly detection (65+ models with 180+ pre-built policies) for insider risk, compromised accounts, and data exfiltration. User Confidence Index (UCI) scoring and event correlation timelines with the ability to invoke policy actions based on score. REST API for UCI export, UCI reset + risk import, and Cloud Risk Exchange for risk curation and remediation actions with technology partners. Plus add-on C2 beacon detection using 16 ML models with the SOC detections pack.
Device security	
Feature	**Capability**
Device discovery and classification	Device security delivered through Netskope One Device Intelligence, integrated and run concurrently on the Netskope One SASE Gateway. Agentless discovery of IT, IoT and OT devices and rich context generation using AI/ML algorithms, enabling automated classification and deep insights into device activities and behavior.
Device risk assessment	AI/ML-driven device risk and threat assessment to detect anomalies, generate unique device risk scores, and identify known and unknown risks by correlating context, device activities, and known vulnerabilities.

Device security - continued	
Feature	**Capability**
Diverse telemetry sources	Supports diverse telemetry sources: Netskope One Client, Netskope One Gateway, or 3rd party (AP, switches)
Authentication	Support for 802.1x based authentication for the connected IT, IoT and OT devices.
SD-LAN policies	Automatic device grouping, micro segmentation and access control based on dynamic device context and risk profile. SD-LAN policies seamlessly integrate with multi-vendor switches/APs, embedding intelligence and dynamically enforcing AI-powered micro-segmentation locally or/and via APIs.
IoT/IT/OT device protection	Integrated device intelligence leverages IDS/IPS capabilities to identify device vulnerabilities and threats, and dynamically update the device risk score and micro segment the devices, delivering contextual zero trust security.
Global cellular access	Global cellular access to 400+ networks, Netskope-managed 4G/5G SASE subscription (Zero Trust SASE SIM), advanced metering, and site-to-site communications, extending zero trust security and clientless remote troubleshooting to IoT/OT devices.
Partner ecosystem	Netskope's device intelligence partner ecosystem spans 20+ integrations, covering telemetry collection, security signal enrichment and enforcement, delivering comprehensive IoT/OT protection at scale. Telemetry collection integrations include Aruba switches, routers, and WLC; Cisco switches, routers, and WLC; Mist, and Meraki. Enforcement integrations include Palo Alto Networks and Juniper firewalls, as well as NACs such as Cisco ISE, Aruba ClearPass, and FortiNAC. Security and visibility enrichment integrations include CrowdStrike, Tanium, Qualys, Infoblox, Entra, ServiceNow, and more.
SD-WAN	
Feature	**Capability**
Form factors	Client can be installed on laptop, physical appliances, virtual appliances on hypervisor (ESXi, KVM, HyperV), cloud image (AWS, GCP, Azure, AliCloud, OCI, IBM, Tencent), VNF on white-box or within a container on Linux. Single tenant or multi-tenant unified SASE gateway software (Netskope One Gateway), with multiple deployment options including within a customer, SP or partner data center, or hosted by Netskope.
Interfaces	Support for 1Gbps, 2.5Gbps and 10Gbps speed interfaces. LAN interface (switch or routed): fiber, copper, PoE, BLE 5.0, WiFi 5, WiFi 6 WAN interface: fiber, copper, PoE, GPON, XDSL, serial, WiFi as WAN, integrated 4G/5G, eSIM with on-device LPA.

SD-WAN - continued	
Feature	**Capability**
Context awareness	Leverages Netskope Zero Trust Engine, decoding thousands of apps and cloud and AI services to understand content and context, including application and application risks, device and device risks, and user and user risks. Device context: Device intelligence supports AI/ML-based IoT device discovery, classification, risk assessment and security policy enforcement. Application context: Netskope secure SD-WAN recognizes 95,506 applications, automatically prioritizing traffic using smart QoS defaults based on Netskope CCI scores, eliminating manual configuration and delivering efficient, policy-driven operations. Custom applications can be defined by protocol, IP, or domain. User context: Netskope uses standard UEBA with customizable thresholds and anomaly policies, advanced UEBA with ML models for risk scoring focusing on insider threats and data exfiltration, and comprehensive scoring that factors in data/threat alerts, web filtering, and custom policy controls for a holistic risk view. Supported on the Netskope One Client, Netskope One Gateway and the muti-tenant Netskope One Cloud Gateway in NewEdge. Allows creation of granular zero trust policies based on device/application and user context.
Context-aware path selection	Path selection is both network aware and context aware to ensure best performance across any transport for demanding applications. Network-aware metrics for dynamic path selection include packet loss, latency (one way and round trip), jitter, MOS, congestion, server response time, TCP transmits and application perform from synthetic and RUM metrics. Context-awareness draws on the Netskope Zero Trust Engine capabilities for application and user risk assessment. Traffic steering can be further optimized based on controls such as applications, application categories, domains, address groups, priorities, 5 tuples, user-group, DSCP, metered/hot standby/active-active, policy based path steering. Clientless path selection via NewEdge Route Control which takes automated steps to regularly evaluate the best, optimized path from NewEdge to remote users.
Total SaaS & AI app coverage	Netskope maintains the industry's most comprehensive SaaS and AI app inventory, covering a total of 632,688 SaaS apps and app activities, with risk scoring applied across the majority to enable precise, policy-driven acces control. Total number of SaaS apps including app activities with risk score: 457,715 Total number of SaaS apps including app activities without risk score: 146,223 Total number of AI apps including app activities with risk score: 9,033 Total number of AI apps including app activities without risk score: 19,717
Context-aware application assurance	Context-aware application assurance supports sub-second (300ms) blackout/brownout protection, packet stripping, link bonding for higher throughput and context-aware remediation to protect concurrent degradation on all paths for high priority apps based on CCI score, e.g. packet duplication, adaptive FEC and TCP optimization.

SD-WAN - continued	
Feature	**Capability**
Context-aware app experience quality (AppQoE)	Provides comprehensive quality of experience (QoE) features including classification, low latency queuing, weighted fair queuing, remarking, shaping, scheduling, policing, inbound/outbound rate limiting and DSCP tagging. 4-level hierarchical QoS allowing customers to set bandwidth allocation, rate limit or prioritization per segment/traffic class/app. Smart defaults automatically categorize apps into 12 traffic classes using Netskope CCI. These traffic classes combine priority (high, normal, low) and service class (voice, video, transactional, bulk), creating a 4x3 matrix with 12 classes. Extends context-aware QoS benefits to traffic from branch or remote user to cloud/SaaS/AI including inbound QoS, with AI-aware prioritization of sanctioned enterprise AI using CCI and built-in instance awareness.
First packet detection and DNS caching	First-packet identification, achieved by learning prior flows via DNS caching and identifying SaaS providers' IP addresses (e.g., Zoom, Teams, RingCentral), enables granular and secure breakout of internet-bound traffic to the correct path based on application-driven business and security policies.
VLAN tagging	Offers 802.1Q, native VLAN.
High availability	High availability (HA) for the Netskope One Gateway, Netskope One Orchestrator, and the Netskope controller through virtual router redundancy protocol (VRRP), active-active WAN links, and active-active appliance HA without the need for a layer 2 switch on the WAN side. Multiple appliances can be deployed active-active to achieve full redundancy, unlimited tunnel or throughput.
VPN overlay	Supports diverse deployments, including on-premises, and across public, private, hybrid clouds. Offers policy-based auto VPN/overlay topologies (full mesh, partial mesh, hierarchical, tag-based dynamic site-to-site) as well as integration with 3rd party IPsec. Allows tag-based dynamic site-to-site functionality, enables on-demand topologies and zones enabling sites to communicate directly without relying on a central hub site. Tag-based dynamic site-to-site—combined with segment-aware topologies—addresses the most complex customer topologies needed to manage corporate traffic effectively. Netskope global WAN delivers high-performance SD-WAN optimization for SaaS/UCaaS applications and enables site-to-site (e.g. cross-continental connections via Netskope backbone.) Service providers hosted Netskope PoPs allow the extension of customer VPN overlays to SP infrastructure. Netskope Zero Trust SASE SIM supports the extension of zero trust security and site-to-site connectivity to IoT/OT.
Context-aware routing	Netskope's control plane is built on standards-based protocols for interop with existing infrastructure and further enriched with the Netskope Zero Trust Engine. This enables granular policies based on device, user and app trust. By sharing user/device context and risk info with the Netskope One Gateway, the Netskope Zero Trust Engine restricts access to apps, sites, and virtual routing and forwarding. Supports industry-standard protocols such as eBGP/iBGP, OSPF, static, route filtering, route redistribution, segmentation/VRF, VRRP, BFD for BGP, route automation, IP SLA for static route, policy based routing (PBR), application-aware routing, NAT/port address translation (PAT) and overlay NAT routing. Offers a 100% SaaS-based SDN controller (BGP reflector) with key distribution at cloud scale to expand your network on-demand and flexible topologies. NewEdge Route Control automatically evaluates the best path from NewEdge to the user or SaaS/AI app using 10M+ daily telemetry. This also enables a unique path selection mechanism towards the end user clients and mitigates ISP connectivity issues in real time, even those outside of Netskope's direct control such as backbone router failover.

SD-WAN - continued	
Feature	**Capability**
Segmentation	Employs VRF-based segmentation extending seamlessly across endpoints, branches, data centers, and clouds to share critical segmentation data network-wide. Offers segment-aware topologies, facilitating branch-to-branch connectivity with dynamic tunnels. Supports segment-aware AppQoE policies, prioritizing critical business applications over specific segments. Enables specific firewall rules per segment, providing granular control over network traffic. Additionally, allows for the automatic micro-segmentation of IoT devices based on dynamically updated risk scores. Supports VRF-based segmentation for site-to-site and NewEdge connections for cloud on-ramp. Netskope Zero Trust SASE SIM can be used to airgap/segment IoT/OT devices.
Multi-cloud	Netskope One SASE provides images to deploy virtual appliances in hypervisors (e.g. ESXi, KVM, & HyperV) and IaaS (eAWS/Azure/GCP/OCI/AliCloud/IBM/Tencent). Netskope SASE Gateway virtual image is available in AWS, Azure, and GCP marketplace. Deployment and activation can be fully automated via Netskope SASE Orchestrator or Terraform. Virtualized Netskope One Gateway also natively integrates with IaaS network infrastructure (i.e. AWS Cloud WAN via tunnel-less design, AWS TGW via Geneve protocol, Azure vWAN and GCP gWAN via BGP peering). Extensive peering exists between NewEdge and major NaaS (Equinix/Megaport/Console Connect). NewEdge Express Connect enables private peering with your own private network interconnect and permits up to 100G redundant ports.
Hosted cloud on-ramp service	Provides fast cloud on-ramps via Netskope One Cloud: cloud-delivered, multi-tenant unified SASE gateways in NewEdge. Traffic from Netskope One Gateway (at the branch), Netskope One Client (remote location) to NewEdge is symmetrically optimized with all of the SD-WAN benefits such as active-active links, TCP/UDP optimization and sub second black-out/brownout failover. Extends context-aware QoS benefits to traffic from branch or remote user to cloud/SaaS/AI including capabilities including inbound QoS. Traffic from NewEdge to SaaS/cloud SPs is asymmetrically optimized by NewEdge (4k+ network connections to 700 ASNs) measuring STM and RUM metrics and using BGP routing optimization to select the best peering network. Peering from NewEdge: Internet exchange (IX) peering, NaaS peering, and direct connections/NewEdge Express Connect exist from the Netskope NewEdge Network to all major CSPs, as well as optionally to customers. Optional customer peering allows you to connect directly to Netskope NewEdge using cross-connects, NaaS providers, metro ethernet, or via IXs and permits up to 100G redundant ports. Steers traffic from users, devices, branches and data centers using the best path to any IaaS/SaaS for optimal application performance. Scales elastically to seamlessly interconnect VPCs and VNETs across any public and hybrid cloud.
Global WAN backbone	Allows users/branches to access private applications located across continents leveraging Netskope's highly optimized global WAN backbone. Supports turnkey integration with IaaS networks, such as AWS Cloud WAN via a tunnel-less design, Azure vWAN, and GCP Cloud Router via BGP peering. This integration allows users and branches to seamlessly access applications spread across continents over the global WAN backbone built on top of the respective cloud providers.
Zero touch provisioning	Gateways allow zero touch provisioning. Netskope automatically adds sold appliances to customer inventory, which customers can associate with required policies. Once connected to the internet, the gateway will automatically activate, download a set of 3rd party and Netskope edge AI apps and relevant configurations. Based on the policy, it will build tunnels to NewEdge and customer data centers.
Network services	DNS, DHCP client, DHCP server, DHCP relay, PPPoE, Secure Shell (SSH), Secure Copy (SCP).
Location services	Geo-IP location
Port security	Supports Wi-Fi 802.1X with WPA2-Enterprise (EAP-MD5, EAP-TLS) and WPA2-Personal, 802.1X on both switched and route ports with Enterprise (EAP-MD5, EAP-TLS), MAC address-based access (local), MAC Address Bypass (MAB).

SD-WAN - continued	
Feature	**Capability**
Cloud security	One click to Netskope One SSE, leveraging the global coverage, extensive peering, and low-latency designs of the NewEdge infrastructure. 100% SaaS SDN controller with support for open-standard routing and cloud-scale key distribution.
On-premise security	Context-aware stateful firewall (L3/L4, L7, app/user/device context), IPS/IDS (60k+ signatures), URL filtering and one-click secure on-ramp to SSE. Policy controls include user groups, devices, applications, custom apps, ports/protocols, FQDNs and dynamic address groups.
VPN encryption	Supports AES 256/128, SHA1/SHA2, IKEv2 protocol, and public key authentication for overlay networks.
Edge AI services and inference	Edge AI Inference: AI/ML inference runs locally on the Netskope One Gateway, detecting and remediating threats at the edge without sending traffic to the cloud, reducing latency, increasing resilience, and accelerating threat detection and response. Edge AI Services: Full lifecycle management of Netskope, partner, and custom containerized applications on the gateway. Netskope apps include IPS/IDS, IoT/OT discovery and control, ZTNA publisher and broker, and DEM. Partner containers include Cisco Thousand Eyes, Microsoft Azure IoT Edge, and custom containers.
IPv6	5G carrier certified IPv6 over WAN. Advanced routing features such as BGP and OSPF are configurable via CLI, using FRR's native IPv6 support.
Client	
Feature	**Capability**
Supported OS	Windows OS, macOS, Android OS, iOS, Linux distributions (Ubuntu, Mint) and Chrome OS.
SD-WAN	Multiple interfaces (active/active, active/standby), sub-second brownout and blackout failover, context aware AppQoE/path selection/UDP optimization/adaptive FEC.
SSE	SWG, CASB, Private Access/ZTNA, FWaaS, DLP.
VPN	Supports all ports and protocols: - Client-to-server L7 (e.g., web apps) - Server-to-client L3 (e.g., remote assistance) - Bi-directional traffic (e.g., VoIP)
Clientless access protocols	HTTP/s, RDP, SSH, VPN and Telnet.
Enterprise Browser	
Feature	**Capability**
Managed chromium browser	Increase productivity and streamline secure access for employees and contractors on unmanaged devices to websites, company applications, collaboration, and resources while protecting data with unmatched security service edge (SSE) and browser data protection capabilities. Compatible with CASB Inline, SWG, and ZTNA.
Supported OS	Windows OS, macOS, iOS, iPadOS, Android, and Chromebook.

Management	
Feature	**Capability**
Unified management	Unified management, data lake and policy for all Netskope One SSE and SD-WAN services. empowering IT teams to unify network and security within one platform, eliminating the need for multiple products and policy inconsistencies. This ensures consistent and universal zero trust security and optimization across all branch offices, users, and cloud.
Simplified deployment and administration	Supports all aspects of networking and security policies (monitoring, configuration, troubleshooting, events and alerts) through an easy-to-use, unified management console, and the industry's first unified SASE client. This includes cloud delivered SD-WAN, SWG, CASB, ZTNA, FWaaS, IPS, IoT/OT device intelligence service and Netskope's best-in-class threat/data protection.
Unified dashboard for networking and security	Autonomous monitoring collects service-level experience data from users and branch offices to detect anomalies and forecast SLA violations. DEM provides per-hop connectivity monitoring from sites and end-user devices, with both overlay and underlay monitoring. Security dashboard provides insights into traffic inspected both on-prem and in the cloud.
Multi-tenancy and management plane flexibility	Multi-tiered, multi-tenancy support allows SPs and MSPs to create and manage their SASE tenants end to end. Management planes can be hosted by Netskope (standard), or deployed by an SP or customer within their own infrastructure. Management planes are available across 9+ countries (US, EU, UK, Australia, Saudi Arabia, Switzerland, Singapore, India, and Canada) enabling organizations to keep policy administration, metadata, and logs within a specific legal jurisdiction.
Extensible containerized gateway	Advanced capabilities include device intelligence for IoT/OT, AL/ML-based device discovery and protection, DEM for advanced WAN insights, publisher and broker for Universal ZTNA. Partner and custom apps can run on the fully containerized gateway.
Single sign on to advanced configuration	Advanced configurations including DLP, Advanced Analytics and RBI that are typically managed by separate teams are easily accessible through single sign on.
Authentication, authorization, and accounting (AAA)	Authentication with Google/Microsoft accounts, Enterprise SSO with Okta/AD/ADFS/Azure AD/LDAP/ Google Workspace/Ping/SAML/OpenId Connect, multi-tier RBAC architecture, RADIUS, auditing.
Troubleshooting	Bandwidth test, ping/trace route, packet capture and diagnosis, alerts, events, list active flows, console access to gateway from orchestrator portal.
Configuration and monitoring	REST API, GraphQL API, NetFlow, syslog, SNMP, per-flow visibility, per-path visibility, transactions, per-overlay path SLA metrics, application response time (ART) metrics, ML- based anomaly detection, device/user/application visibility, dashboard, PDF reports. Appliance can be configured via unified management and locally via CLI and local UI
AI services and advanced analytics	Netskope Private Access AIOps Agent delivers AI-powered configuration coaching, link recommendation, and troubleshooting, analyzing real user traffic to recommend fine-grained, least privilege access policies. AI-driven DLP incident categorization minimizes human review. MCP integration enables natural language queries. Netskope One Advanced Analytics provides comprehensive cloud risk posture visibility.
Edge AI services and inference	Edge AI Inference: AI/ML inference runs locally on the Netskope One Gateway, detecting and remediating threats at the edge without sending traffic to the cloud, reducing latency, increasing resilience, and accelerating threat detection and response. Edge AI Services: Full lifecycle management of Netskope, partner, and custom containerized applications on the gateway. Netskope apps include IPS/IDS, IoT/OT discovery and control, ZTNA publisher and broker, and DEM. Partner containers include Cisco Thousand Eyes, Microsoft Azure IoT Edge, and custom containers.

Netskope partner orchestrator	
Feature	**Capability**
Multi-tenancy	MSP/SP self-service portal for multi-customer tenant management and Salesforce integration.
Tenant creation	Production tenant creation in under 15 minutes across all NewEdge data centers, with base config via SASE lifecycle templates.
License management	License pool with real-time allocation and deallocation. Appliance inventory and license pool management.
Access management	Per-tenant admin and 3rd-party integrator access. Granular RBAC with infinite admin tiers across MSP/Partner/Customer.

04/26 DS-730-6