Netskope One SASE

Data Sheet

Simplifying security and network transformation

The over reliance on legacy perimeter-based network security architectures to address digital transformation initiatives has resulted in heightened security concerns, poor user experience, and increase in overall costs and complexity of operations. Organizations need a solution that supports their digital transformation efforts without compromising between security, agility, simplification and user experience.

Why is Netskope the best choice?

Netskope One SASE combines Netskope's market-leading Intelligent SSE with its next-generation Borderless SD-WAN thereby converging networking and security services onto a unified platform to protect users, applications, and data everywhere with AI-powered zero trust security, while providing fast, reliable access and optimized connectivity to any application from any network location or device, including IoT– at scale.

Industry's First Converged SASE Offering

- Deliver a comprehensive, cloud-native SASE platform leveraging the power of one engine, one console, one network, one gateway and one client.
- Enhance visibility and control across web, SaaS, and private applications with Netskope's patented Zero Trust Engine, AI innovations, and New Edge network (the world's largest private SASE cloud).
- Deliver 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
- Provide secure, optimized connectivity for every remote user, device, site, and cloud with Borderless SD-WAN, along with a seamless on-ramp to Intelligent SSE, providing industry-best SLAs for latency, decryption, and in-depth security inspection.

Key Benefits and Capabilities

Full platform convergence

Reduce cost and complexity through a fully converged SASE solution with one Zero Trust Engine, one gateway, one network, one console, and the industry's first unified SASE client.

Ease of use

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

Enterprise-grade security

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

Context-driven Zero Trust Engine

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

SASE automation

Transform to SSE for any user, device, and location instead of hairpinning traffic to legacy security appliances unable to decode application and cloud services.

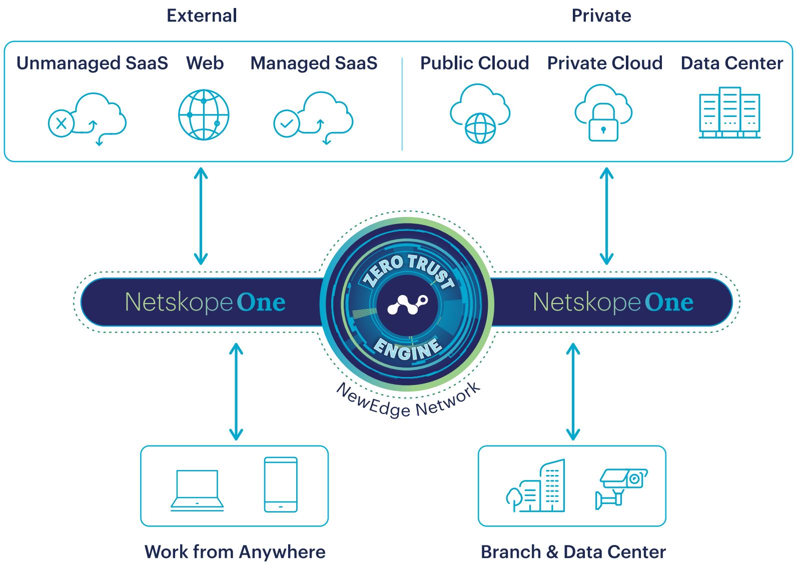
Global coverage

Unparalleled service coverage, performance and resilience with NewEdge, the industry's fastest and most reliable private security cloud infrastructure, with global PoP footprint across 70+ regions.

> "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

The Netskope Difference

Netskope One is a converged security and network as a service platform. Through its patented Zero Trust Engine, AI innovation, and the largest private security cloud we make it easy for our customers to defend their businesses and data while delivering a phenomenal end user experience and simplified operations. The platform delivers AI-powered data and threat protection that automatically adapts to the ever-growing data landscape, including the widespread adoption of generative AI and new AI-driven attacks.



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.
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 look-up 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 websites, 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.

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. 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 customers' internal remediation workflows.
App Discovery & Control	Discovery and instance detection for over 800 cloud services in any language. Granular activity visibility like viewing, uploading, downloading, sharing, editing, renaming, creating, deleting, etc. Add custom SaaS and IaaS services with the Universal Connector framework in order to get inline visibility like logins, uploads, downloads, posts, etc. and inline control benefits like 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 & 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.
Posture Management	Continuous posture management, which includes configuration monitoring, audit, adjusting security controls, and share settings, for over 30 cloud services. Compliance auditing of security posture is available for over 15 SaaS applications, 3 IaaS services, with more than 300 predefined configuration compliance policies that align to industry standards and 1000+ out-of-the-box configuration rules.
App Risk Assessment	Cloud Confidence Index (CCI) the industry's largest app trust database for SaaS apps, providing risk scoring for more than 80,000 apps. The risk scoring system assesses an app's enterprise readiness by evaluating dozens of attributes and then assigns an overall trust score to it. More than 100+ criteria are evaluated, including vulnerability and exploit assessment, recent breaches, compliance certifications, data protection features, privacy policies, access controls, audit readiness, etc. Customize CCI scoring by adjusting score weighting or adding custom attributes.
3rd party App Risk Assessment	Provide 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, permissions, etc.) as well as usage and activity.
Advanced Analytics	CASB-generated data (i.e. metadata, events, alerts, incidents, etc.) are available in Netskope Advanced Analytics for custom reporting and analysis.

PRIVATE APPLICATION SECURITY	
FEATURE	**CAPABILITY**
App Coverage	Support all ports and protocols for access to private apps. Unlike conventional ZTNA solutions that are limited to client-initiated apps, ZTNA Next supports connectivity to all types of apps: client-to-server (web apps, RDP/SSH/Telnet/VNC); server-to-client (Remote Assistance); and bi-directional (VoIP).
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. Steers agent-based traffic to the Netskope NewEdge network.
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.
Local Access	Provides a consistent access experience for seamless work, whether remote or on-premises at a branch or campus location. The ZTNA Next 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	Ensures reliable, optimized access to private apps - including critical voice and video - with integrated endpoint SD-WAN capabilities in the Netskope One Client. Provides app aware prioritization and on-demand remediation (for UDP traffic) to mitigate packet loss on a single or multiple unstable links such as WiFi & LTE tethering from the phone.The path selection and sub-second brownout & blackout protection are also available on unified SASE client. With a unified SASE client, users can utilize multiple links, enabling active/active or active/standby paths, with policies based on processes running on a laptop.
App 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 ZTNA Next deployment.
IoT/OT Security	Enables secure remote access to IoT devices and OT environments in branch or factory locations. Provides high-quality connectivity and microsegmentation for IoT/OT devices like ATMs, cameras, smart robots, and other IoT sensors. Reduces your attack surface and constraints lateral movement.
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.

FIREWALL AS A SERVICE	
FEATURE	**CAPABILITY**
Firewall Services	5-tuple based policies, user-based access control, FQDN/PQDN based access control, application identification and control on standard and non-standard ports, unified policies with web traffic, ability to export events, and Advanced Analytics integration.
DNS	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.
IDS/IPS	60,000+ IPS (snort) signatures that can be customized and curated per tenant, including allow lists per source IP, destination IP and domain. IPS signatures can be curated by CVE (mapped NIST NVD, MITRE databases, and the Microsoft Active Protection Program) and customized for specific actions.
Bandwidth Control	Enables effective use of customers' WAN link by rate limiting bandwidth-consuming applications and categories

PLATFORM SERVICE - DATA PROTECTION	
FEATURE	**CAPABILITY**
Integrated DLP	Single DLP solution for web in-line, SaaS at-rest and in-line (over 80,000+ 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	1,950+ 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-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 by training Netskope with customer-specific data.
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 & remediation workflow with Microsoft Purview, Digital Guardian Network DLP, Forcepoint, McAfee DLP Prevent, Symantec DLP, etc.
Encryption & Tagging Integration	Integration with Microsoft Information Protection, Fortra (Vera, Titus), Box Shield Classification Labels, Google Labels, etc.
DSPM Integration	Integration with third-party DSPM providers such as BigID, Eureka and Cyera in order to enforce real-time Zero Trust policies.

PLATFORM SERVICE - THREAT PROTECTION	
FEATURE	**CAPABILITY**
Standard Threat Protection	Antimalware, ML-based malicious PE file and phishing detection, sandboxing to corroborate all AV and ML detections, multiple threat intel feeds, Web IPS, and True File Types.
Advanced Threat Protection	De-obfuscation and recursive file unpacking for 350+ types, pre-execution and analysis for 3,500+ file format families with 3,000+ static binary threat indicators, cloud sandboxing for 30+ file types, machine learning deep analysis, patient zero protection and alerts, sandbox API, and retrohunt API.

PLATFORM SERVICE - USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)	
FEATURE	**CAPABILITY**
Standard UEBA	Sequential anomaly rules (9) to detect cloud app bulk uploads, downloads, deletes, plus 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	Machine learning (ML) based anomaly detection (62 models with 130+ 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 + risk import, and Cloud Risk Exchange for risk curation and remediation actions with technology partners.

IOT SECURITY	
FEATURE	**CAPABILITY**
Device discovery and classification	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.
Authentication	Support for 802.1x based authentication for the connected IT, IoT and OT devices.
Access control and micro segmentation	Automatic device grouping and micro segmentation based on dynamic device context and risk profile. The access control policies can be enforced from Netskope One Gateway or multiple third-party firewalls and network access controls.
IoT device protection	Integrated IDS/IPS capabilities identify device vulnerabilities and threats to dynamically update the device risk score and micro segment the devices, delivering zero trust security.

SD-WAN	
FEATURE	**CAPABILITY**
Form Factors	Client on laptop or servers / Physical Appliances / Virtual Appliances on hypervisor (ESXi, KVM, HyperV) / Cloud Image (AWS, GCP, Azure) / Container on Linux Single Tenant or Multi-Tenant unified SASE Gateway software (One Gateway), deployable in customer or SP/Partner data center.
Interfaces	Support 1Gbps, 2.5Gbps and 10 Gbps speed interfaces LAN interface: Fiber, Copper, WiFi 6 (switch or routed) WAN interface: Fiber, Copper, GPON, XDSL, Serial, Integrated Cellular and WiFi
Mobility (WiFi/Cellular)	WiFi (2.4GHz/5GHz, 802.11ax), WPA2-Enterprise, WPA2-Personal, 802.1X, WiFi as WAN, 4G, LTE, BLE 5.0, SIM management, advanced metering
Context-Aware	Leverages Netskope Zero Trust Engine that decodes thousands of apps and cloud services to understand content and context, including application and application risks, device and device risks, and user and user risks. Supports industry's highest number of applications 80K+ that are prioritized automatically with out of the box smart QoS defaults based on Netskope CCI (Cloud Confidence Index) scores, eliminating manual work and resulting efficient operations. Customized applications based on protocols/IP/Domain. Supported on Netskope One Client and One Gateway.
Application Assurance	Ensures best performance across any transport for demanding applications, leveraging network-condition-aware dynamic path selection measuring Packet Loss, Latency (One Way & Round trip), Jitter, MOS, Congestion, Server Response time and TCP transmits. Application Assurance includes sub-second (300ms) blackout/ brownout protection, packet stripping, link bonding for higher throughput and intent-driven remediation to protect concurrent degradation on all paths, e.g. Packet duplication, FEC and TCP optimization. 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.
AppQoE	Provide comprehensive 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 BW 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/web/SaaS including capabilities like inbound QoS.
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.
VPN Overlay	Supports diverse deployments including on-premise, and across public, private, hybrid clouds. Offers policy-based Auto VPN/Overlay topologies (full mesh, partial mesh, 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 & 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

SD-WAN - CONTINUED

FEATURE	CAPABILITY
Routing	Supports industry-standard protocols such as eBGP/iBGP, OSPF, static, route filtering, route redistribution, segmentation/VRF, VRRP, BFD for BGP, application-aware routing, NAT/Port Address Translation (PAT) and overlay NAT routing. Offers a 100% SaaS-based SDN controller with key distribution at cloud scale to expand your network on-demand & flexible topologies.
VLAN Tagging	Offers 802.1Q, native VLAN
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.
High Availability	High Availability (HA) for the Netskope unified SASE gateway, Netskope SASE Orchestrator, and Netskope SASE Controller through 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.
Multi-cloud	Turnkey automation (UI or Terraform) to deploy Netskope unified SASE Gateway Cloud Image in AWS, Azure and GCP and native integration with cloud infrastructure: - AWS Cloud WAN via either GRE or native "tunnel-less" design - MSFT Azure vWAN leveraging the vWAN BGP peering - GCP via GCP Cloud router with BGP peering Deployable in other cloud providers and carrier neutral locations that support ESXi, Hyper V, KVM e.g.: Alicloud, Oracle OCI, Equinix, Megaport, Rackspace, etc.
Cloud On-Ramp	Offers native cloud on-ramp via Netskope Borderless SD-WAN in NewEdge for all cloud and SaaS applications with end-to-end optimization. Traffic from Gateway/Client to NewEdge is symmetrically optimized with all of the SD-WAN benefits like active-active links, like TCP/UDP optimization and sub second black-out/brownout failover. Traffic from NewEdge to SaaS/Cloud SPs is asymmetrically optimized by NewEdge (3k+ network connections to 650 ASNs) measuring STM and RUM metrics and using BGP routing optimization to select the best peering network. Direct Connections/peering (cables, IX) from NewEdge to any cloud (e.g. Equinix, Megaport, Alicloud, Oracle OCI etc) offers customers high 100Gb ports. Steer traffic from users, devices, branches and data centers using the best path to any IaaS/SaaS for optimal application performance. Scale elastically to seamlessly interconnect VPCs and VNETs across any public and hybrid cloud.
Global WAN Backbone	Allow users/branches to access private applications located across continents leveraging Netskope's highly optimized global WAN backbone spanning all Netskope POPs worldwide. Support 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.
Edge Compute	One-click deployment of container services on Branch appliance from a catalog that includes Netskope services like IoT device intelligence and Proactive DEM, as well as partner containers such as Cisco Thousand Eyes, Microsoft Azure IoT Edge, and custom containers.
Zero Touch Provisioning	Email-based activation eliminating pre-stage, zero-touch activation, template with variables, enterprise-wide business intent-based policies, simple one-click RMA.

SD-WAN - CONTINUED

FEATURE	CAPABILITY
Network Services	DNS, DHCP client, DHCP server, DHCP relay, PPPoE, Secure Shell (SSH), Secure Copy (SCP), 802.1X
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)
Cloud Security	One-Click to Netskope Intelligent SSE, leverages 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	Supports Application/User-Identity aware stateful firewall, IPS/IDS (60k+ signatures), URL filtering, one-click secure on-ramp to SSE. Allows policy controls include matching criteria like user groups, devices, applications, custom apps, port/protocol, fully qualified domains. In addition, firewall supports dynamic address groups that can be leveraged by Netskope or ecosystem partners.
IoT/OT Security	On-appliance integrated IoT device intelligence and security with 802.1x authentication, AI/ML-powered device discovery, classification, and risk assessment, IPS/IDS security, and automated micro-segmentation.
VPN Encryption	Supports AES 256/128, SHA1/SHA2, IKEv2 protocol, public key authentication for overlay networks

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), AppQoE, Sub-second brownout and blackout failover, TCP/UDP optimization, FEC
SSE	SWG, CASB, ZTNA, FWaaS, DLP
Remote Access	Support all ports & protocols: - Client-to-server (e.g., web apps) - Server-to-client (e.g., remote assistance); - Bi-directional traffic (e.g., VoIP). - App QoE for all traffic
Clientless Access Protocols	HTTP/s, RDP, SSH, VPN and Telnet

MANAGEMENT	
FEATURE	CAPABILITY
Single, unified management	A single pane to manage data lake and policy for SD-WAN and SSE which empowers IT teams to unify SD-WAN and SSE management with one platform, eliminating the need for multiple products and policy inconsistencies. This ensures consistent universal zero trust security and optimization across all branch offices, users, and cloud
Simplified deployment and administration	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, Firewall, IPS, Netskope IoT/OT Device Intelligence service and Netskope's best-in-class threat/data protection
Unified dashboard for networking and security	Autonomous monitoring to collect service level experience data from users and branch offices to detect anomalies and forecast SLA violations. Allows IT teams to do enterprise-wide WAN predictive analytics to identify and resolve policy violations. Further, the security dashboard provides customers insights into traffic inspected by both on-premise & cloud security
Multitenancy	Four tiered multi-tenancy support (Netskope Operator, Master SP, MSP, Customer) allows SP and MSPs to create and manage their SASE tenants end to end
Extensible containerized gateway	Advanced capabilities like IoT Device Intelligence for IoT/OT AL/ML based device protection, P-DEM for advanced WAN insights, and Speedtest are integrated into the fully containerized gateway
Single sign on to advanced configuration	Advanced configurations like 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	Alerts, events, list active flows, console access to Gateway from Orchestrator portal
Configuration & 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
AI-driven Operations	Simplify operations with automated troubleshooting, proactive support, and insights into traffic flows and policies. Minimize time to resolution with autonomous monitoring to detect anomalies and predict Service Provider SLA violations

Interested in learning more? Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Thousands of customers trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.

©2024 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 04/24 DS-730-2