Solution Brief

Drive your enterprise forward with Netskope One SD-WAN

Netskope One SD-WAN utilizes a single lightweight software platform and unified policy framework to provide secure, optimized access for remote users, branch offices, IoT devices, and multi-cloud environments. Rooted in zero trust principles, it employs context-aware policies to understand and manage users, devices, applications, and associated risks. This approach streamlines network operations, enhances intelligence, and strengthens security.

Quick Glance

- Granular policy controls with full visibility and contextual awareness about user, device, and application and associated risks
- Assured application experience over any transport—MPLS, internet, 4G/5G
- Unified policy and consistent experience at any location with cloud-native, four-tier management framework
- Zero-touch provisioning, proactive troubleshooting, anomalies detection with scalable, AI-driven operations
- Protect with single click to Netskope One SSE: cloud-delivered full-stack security built on zero trust principles
- Protect branches against modern threats with device intelligence integrated into the unified SASE gateway, enabling classification, context derivation, visibility, dynamic risk assessment, and adaptive access controls.

> "Endpoint SD-WAN helps us provide our customers with consistent visibility, security, and network optimization, anywhere their users and devices are."

Mike Hogenauer, Senior Director Network, at FIS Global

The Challenge

SD-WAN succeeded as a technology because users in branch offices needed to have much better support for routing their traffic and quality of service over a combination of low-cost internet links and MPLS. But the world kept expanding in ways that SD-WAN was not equipped to handle. Many IT architects are now struggling to manage each of the areas—exploding mobility, proliferation of apps and IoT devices, and multi-cloud networking—and must have wireless networking, edge computing, and cloud-delivered security. The current architecture results in an inability to apply uniform security or quality of experience (QoE) policy across all users, devices, sites, and clouds. These requirements stress traditional SD-WAN, and the products that have risen to help it, to the breaking point.

The Solution

Netskope One SD-WAN is a 100% SaaS-based, converged connectivity solution built on the Netskope One platform, unifying one software and one policy for diverse deployments. It delivers secure, optimized access for remote users, branch sites, and devices to applications and services across multi-cloud environments.

With simplified management and seamless integration between Netskope One SD-WAN and SSE, it provides a true single-vendor SASE solution. This enables organizations to bring remote users, devices, sites, and multi-cloud environments online in minutes, ensuring consistent network performance, security policies, and user experiences.

netskope

Secure SD-WAN

The evolving enterprise now needs zero trust-enabled, context-aware SD-WAN to provide fast, reliable, and secure access to any application and device at any location with full visibility and the right set of controls. This is possible using contextual policies that include understanding application, application risks, user, user risks, device, and device risks, all of which make network operations more intelligent and more secure.

Secure SD-WAN solution key highlights are:

- App and Network Traffic Prioritization: Fast, reliable connectivity with Context Aware Adaptive QoE that leverages Netskope Zero Trust Engine, which 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.

Bringing multi-tier, cloud-native management to any enterprise deployment, converging networking and security, to unify policy and deliver a consistent experience with context!

- Supports industry's highest number of applications 85K+ 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
- **Assured Application Experience:** Take advantage of context-aware adaptive QoE, dynamic path selection and sub-second failover (for two links), on-demand remediation (to mitigate packet loss even on a single unstable link) for all critical voice and video apps.
- **Integrated Security:** Protect your organization with one click to Netskope One SSE full-stack security services that are powered by the industry's highest-performing, lowest-latency NewEdge Network offering the highest global coverage.
- **Cloud On-Ramp:** Incorporates a distributed network of cloud delivered unified SASE gateways within the NewEdge network to provide high-performance datapath from any branch, data center, or remote user to any cloud, SaaS, or UCaaS application.
- **AI-driven Operations:** Autonomous monitoring to collect users' SLE data, detect anomalies, and predict SLA violations. Resolve policy violations with network-wide flow analytics.
- **Cloud-native Management:** Multi-tenant orchestrator brings all remote users, devices, sites, and multi-cloud environments online in minutes with zero-touch provisioning.

SD-WAN for Endpoint

Today's workforce expects zero-trust security and reliable connectivity, regardless of location. IT organizations, in turn, need simplicity and extended visibility to support remote users adequately. Despite its "software-defined" moniker, SD-WAN relies on specialized hardware at remote locations.

Leveraging the same technologies found in Netskope One SSE and Netskope One SD-WAN, Netskope One SD-WAN for Endpoint and unified SASE client deliver granular and dynamic network performance, visibility, and security capabilities. From a single unified platform, enterprise IT departments can now manage branch offices and individual remote users using a uniform zero trust and network performance policy across the entire corporate infrastructure.

SD-WAN for Endpoint solution key highlights are:

- **AI-driven Operations:** Netskope One SD-WAN for Endpoint simplifies management with automated troubleshooting and insights into end-user experience with per-user AppX score, traffic flows, policy violations, and anomaly detection.
- **High-performance Connectivity for Critical Voice, Video, and Data Applications:** Netskope One SD-WAN for Endpoint offers fast and reliable connections with application-aware prioritization and automatically remediates poor performance on the last mile.

- **Optimized User Experience:** Netskope One SD-WAN for Endpoint eliminates single-tunnel shortcomings of existing remote access VPN by connecting with multiple public and private data centers simultaneously, enabling users to receive the most optimized experience with policy-based direct-to-app access.
- **360° Protection:** Netskope's unified SASE client smoothly delivers SD-WAN, SWG, CASB, ZTNA, DLP, FWaaS, and other security services.

Netskope SD-WAN for Endpoint leverages the industry's first software-based unified SASE client, converging SD-WAN and Security Service Edge (SSE) capabilities so organizations can easily reduce cost and complexity, and simplify operations. With Netskope One Private Access, it integrates Netskope One SD-WAN for Endpoint, with Netskope One Private Application Access, in the same unified SASE client, allowing organizatons to completely replace remote access VPNs while enhancing security and optimizing application access.

- **Unified Architecture and Consistent Context-aware Policy:** Netskope One SD-WAN extends context-aware zero trust policy, SD-WAN, and One SSE across the entire solution portfolio. The policy and user experience seamlessly follows the user, whether at branches or remote locations, ensuring both secure and optimized access to applications and multiple cloud services.
- **100% SaaS Controller:** Migrate away from traditional DIY SDN with a 100% SaaS SDN Controller for operational efficiency and SD-WAN scalability. Achieve resilience with control plane and data plane separation.

Micro Branch

The term "micro branch" refers to a small office, cafe, or retail store, which in today's remote work culture might be a location where a person is working. In these scenarios, there may only be a few users or devices; however, their needs for connectivity, quality of service, and security remain as crucial as they would be in a conventional branch office. They need a thin gateway that is cost-effective and offers quality connectivity and security.

Netskope One WAN supports the micro branch use case by providing lightweight software that resides on a compact unified gateway, or a hardware device located in a branch or a micro branch.
Micro Branch solution key highlights are:

- **Build a smart workspace:** with a lightweight All-in-One unified SASE gateway that converges security with SD-WAN, routing, Wireless, Wi-Fi, and edge compute.
- **Connectivity anywhere:** with integrated 4G/5G: Bring up any remote device/site in no time with integrated 4G/5G to overcome broadband long lead times.
- **On-demand services catalog:** Deploy out-of-the box container services on a unified gateway like Thousand Eyes and more from a services catalog or bring-your-own-container service.
- **Deployment flexibility:** Cloud-native, true multi-tier (4-tier) management platform for any type of deployment that delivers unified and consistent policies across distributed branches from a single console.

Deliver enterprise-grade SD-WAN, security, and more to enable secure, optimized access to all business resources.

Wireless WAN

To be able to work anywhere at any time in a many-to-many world, there is a need for more than what SD-WAN provides on the wireless front. What's required is fast and reliable connectivity in every location, whether it's in a perpetually mobile field vehicle or a stationary, enterprise access point on a wall that provides a strong signal from within IT closets. Traditional SD-WAN cannot do this. Netskope One SD-WAN can.

Netskope One Wireless WAN consolidates SD-WAN and Wireless Gateway into a single device and runs all applications on the existing broadband link, keeping the expensive wireless link as a backup. Netskope cellular gateway is PTCRB, AT&T, and Verizon certified, supports global carriers, and enables customers to bring their own cellular plans.
Wireless WAN solution key highlights are:

- **Designed to fit anywhere:** Cellular gateway, designed to optimize cellular signal strength, can be readily positioned in a window to provide cellular connectivity to any router downstream or Netskope unified SASE Gateway for primary or backup cellular support.
- **All-in-One-Converged:** Free yourself from the complexity of legacy networks with a single wireless gateway that converges cellular, SD-WAN, security, and edge compute.
- **Adaptive QoE to optimize cellular cost:** Industry's first adaptive QoE with circuit metering that dynamically adjusts application bandwidth to save cost on expensive cellular links.
- **Support life-cycle management of SIM:** Build and manage Wireless WAN (WWAN) without manual intervention.
- **Leverage zero-touch provisioning:** Bring your site on-line in minutes with automated SIM card activation and remote device management.
- **Meets regulatory compliance—Deploy with ease:** Netskope Cellular Gateways support high-gain directional external antennas built to scale. It is AT&T, Verizon, PTCR certified, C1D2, IP Rated—with thin wireless, ruggedized form factor suitable for IoT and other enterprise use cases that requires equipment to withstand harsh environments and to deal with natural disasters when the primary broadband connection fails.

Leverage an enterprise access point on a wall that provides a strong signal inside your IT closets.

- **Single pane of glass management:** Effortlessly control the wireless gateway using the same intuitive centralized interface employed for other Netskope One SD-WAN solutions, delivering a unified management experience.

Multi-cloud Networking

Traditional SD-WAN also fails to properly handle multi-cloud networking and automated operations. Companies may access dozens of distinct clouds, each hosting different workloads. They are looking for a networking solution that provides secure connectivity to all these clouds while enabling policy-driven application-to-application communication. Some emerging vendors provide a cloud networking solution that supports visibility and control of intercloud connections through a set of policies and automated configuration of connections. These multi-cloud networking vendors solve an important problem: They enable companies to migrate their workloads to these clouds from a unified dashboard that provides the insights needed for effective orchestration.

Which is great—for as far as it goes.

But Netskope One SD-WAN goes further, providing integrated security and optimization for every user, device, site, and cloud. With Netskope One SD-WAN, customers get one-click access to Netskope One SSE, ensuring full-stack security to any cloud.

Imagine running thousands of servers across multiple clouds, where these servers need to fetch updates from the internet. Given the servers are exposed to cyber threats, Netskope One multi-cloud networking and Netskope One SSE convergence ensure that they are all fully protected with integrated services like SWG, CASB, ZTNA, FWaaS, and much more.

Multi-cloud Networking solution key highlights are:

- **Agility with cloud automation:** Automate cloud operations with a single console across your multi-cloud environment. Leverage cloud-native application networking constructs.
- **Consistent cloud traffic flows:** Deploy across any major cloud providers like AWS, Azure, and GCP and deliver policy-based, context-aware steering from user to the cloud and cloud to cloud.

- **ML-based analytics:** Proactively spot and isolate issues with autonomous enterprise-wide cloud AppX monitoring, detecting anomalies and predicting SLA violations.
- **Secure optimized multi-cloud networking:** Connect your clouds to intelligent SSE with a single click and protect it with the world's highest-performing, low-latency private security cloud called NewEdge.
- **Optimized cloud on-ramp:** Optimized access to and across clouds with full context-aware Quality of Experience.

Going beyond the branch and connecting applications across multiple clouds, by simplifying, accelerating, and protecting multi-cloud networking.

IoT Visibility and Control

Organizations are eager to harness the benefits of IoT, but many hesitate due to the risk these often-vulnerable devices pose to network integrity. A single compromised sensor or device can expose critical systems, disrupt operations, and impact business continuity.

Netskope One Device Intelligence, seamlessly integrated into the unified SASE Gateway, enables the secure adoption of IoT devices across any enterprise network. It leverages HyperContext®, an agentless smart device security platform, to provide deep visibility into managed and unmanaged devices. By analyzing hundreds of device parameters, it delivers rich contextual intelligence for device classification, dynamic risk scoring, granular access control, and real-time segmentation across LAN, WAN, cloud, and remote environments.

This AI/ML-powered intelligence dynamically informs SSE, SD-WAN, and SD-LAN policies to drive real-time security decisions. These controls are enforced through the Netskope unified SASE Gateway, SSE, and existing network infrastructure such as firewalls and network access controls—protecting your branches from threats posed by both IoT and traditional IT devices. For example, if a video camera with an initial risk score of 50 initiates abnormal SSH activity, its score escalates to 95—automatically triggering an SD-LAN policy to isolate the device across existing switches and access points.

IoT Visibility and Control key solution highlights are:

- **Device Discovery** Provides a complete picture of all devices connected to the network, along with their risk profiles by leveraging ML-powered insights for effectively tracking and controlling the devices, and complying with the stringent audit and compliance policies.
- **Unique device identity and grouping** Analyses hundreds of device parameters through traditional fingerprinting technology to generate unique device identifiers and authenticity ratings. Devices exhibiting similar characteristics can be grouped together for unified policy enforcement and establishing the group's normal function and behavior.
- **AI/ML driven risk assessment** Recognizes anomalous behavior at the device level and offers insights and analytics about device-level risks, threats, and best practices around mitigating threat profiles.
- **Reduced attack surface** Dynamically groups devices within secure zones or micro segments to isolate risky devices and prevent lateral movement of threats (East-West) by integrating with Cisco Meraki, Juniper Mist, Aruba Clear pass, Cisco ISE, etc.
- **Enriched device context** Ingest data from multiple security solutions deployed at the customer environment, including Tanium, Qualys, Infoblox, Microsoft Entra and ServiceNow, among other integrations, and implement highly precise and granular policy decisions.
- **Dynamic IDS alert tuning** Dynamic alert tuning ensures your team can prioritize real threats, streamlining workflows for more secure, responsive and effective network operations.

Secure your IoT landscape with real-time visibility, dynamic risk scoring, flexible access control, and intelligent micro-segmentation—powered by Netskope One Device Intelligence, seamlessly integrated into the unified SASE Gateway