

Netskope One SASE Device Intelligence

Data Sheet



Netskope One SASE Device Intelligence enables Context Driven Security for Enterprise Branch IT, IoT and OT Devices

Protect all devices in your enterprise branch environments with device intelligence integrated into the unified SASE gateway, enabling classification, context derivation, and complete visibility for effective asset management. Dynamically assess risk, enforce controls, and orchestrate actions to defend against modern threats while ensuring compliance.

Why is Netskope the best choice?

The Netskope Device Intelligence solution utilizes HyperContext®, an agentless smart device security platform providing granular device context to discover managed and unmanaged devices on your corporate network. The solution further analyzes hundreds of parameters from the discovered devices and leverages the rich contextual intelligence for device classification, dynamic risk assessment, granular access control across LAN, WAN, in the Cloud and network segmentation, facilitating zero trust security for connected devices.

Unlocking the full power of AI/ML driven security

Device Intelligence is integrated within the Netskope unified SASE gateway as well as delivered from the Netskope SASE cloud.

- **Device classification and visibility:** Agentless device discovery with rich contextual intelligence, enabling automated classification and device mapping, and providing deep insights into device activities and behavior.
- **Cybersecurity asset management:** Granular search and reporting for the discovered assets, comprehensive cybersecurity asset management with built-in asset inventory engine, true-up asset inventory and asset management database through integration with ServiceNow CMDB, VA, MDM, EDR.
- **Device risk assessment:** Continuous device monitoring to detect anomalies, generate unique device risk scores and map alerts based on device classification and tags. Streamlined SOC automation and enriched alert handling with SIEM and SOAR integrations.
- **Access control and segmentation:** Dynamic device grouping and micro segmentation based on context and real-time device behavior for granular, precise access to sanctioned devices and orchestrating actions using existing network systems such as firewalls and network access controls.

Key Benefits and Capabilities

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

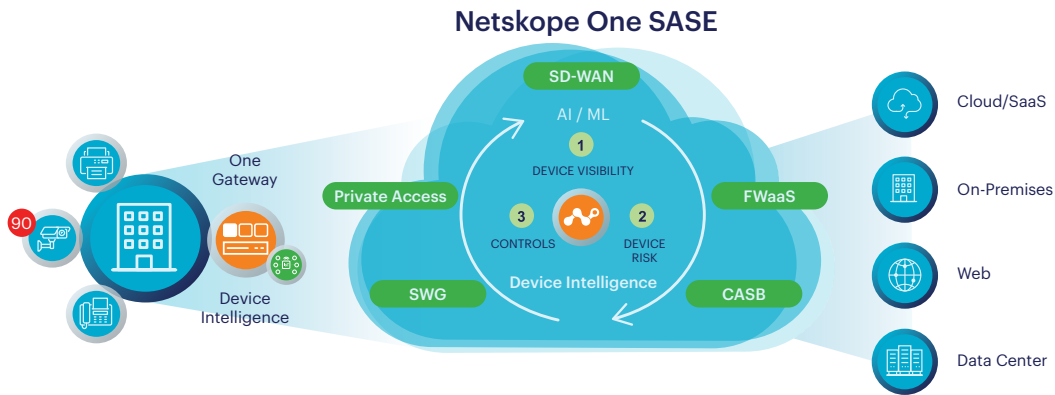
Dynamically groups devices within secure zones or micro segments to isolate risky devices and prevent lateral movement of threats (East-West) by integrating with Cisco Meraki, Juniper Mist, Aruba Clear pass, Cisco ISE, etc.

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.



In Action: A security camera, now assigned a risk score of 90 and deemed unsafe, is dynamically blocked by Netskope's Device Intelligence running on the unified SASE gateway after detecting communication with a command-and-control server.

The Netskope Difference

Netskope One SASE is a converged security and network as a service platform. Netskope One SASE is further enhanced by device intelligence, running as a service in the Netskope unified SASE gateway and across the Netskope SASE cloud, leveraging AI/ML to discover, classify, and create context. It augments this with third-party integrations to provide complete visibility and effective asset management for all IT, OT, and IoT devices. With continuous risk assessment and integration with anomaly detection tools, the solution incorporates LLM-assisted, context-enriched threat information, which can be used for precise access control based on real-time device behavior. These controls are enforced on the Netskope unified SASE gateway, SSE, and existing network infrastructure like firewalls and network access controls protecting your branch from all vulnerable IoT and IT devices.

YOUR NEEDS	THE NETSKOPE SOLUTION
Zero trust access	Netskope Device Intelligence extends zero trust to IT, IoT and OT environments through adaptive access controls, micro segmentation and continuous risk assessment of every authenticated device.
Operational compliance	Netskope Device Intelligence acts upon the rich device telemetry to identify and close security gaps, and meet the regulatory compliance needs.
Actionable alert intelligence	Netskope Device Intelligence responds to security incidents through integration with SIEM platforms. Alert handling is automated at scale through SOAR runbooks.
Bolster security and access management	Netskope Device Intelligence seamlessly integrates with network security systems, including firewalls, network access controls and access points for facilitating secure access to the devices.
Align with SASE vision	Netskope Device Intelligence aims to bring all the connected devices under the unified Secure Access Service Edge (SASE) framework called Netskope One SASE for complete visibility, flexible policy enforcement and incident management of distributed devices, from a centralized management platform.



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](https://www.netskope.com).