Solution Brief

# Netskope SASE Gateway with Integrated Device Intelligence

Connected devices are rapidly proliferating with an estimated 55 billion internet-connected things by 2025.[1] Take control of the connected devices in your organization using an on-premises SASE Gateway enhanced with granular, context-aware Device Intelligence.

### Quick Glance

- Utilize AI/ML techniques to identify and profile network devices dynamically
- Prioritize application traffic for high-priority devices through device context-aware AppQoS
- Protect branch infrastructure from vulnerable devices with integrated security controls
- Automatically micro-segment devices based on device attributes, risk profile, and real-time behavior
- Delivers proactive support through zero trust secure access to remote devices inside the branch, including phones, ATMs, and servers

## The Challenge

The IoT revolution has brought about a proliferation of smart devices, from office cameras to factory sensors, demanding edge computing, low-latency, and high-bandwidth solutions at the branch level. However, managing and securing these IoT devices effectively are intertwined challenges and is a serious undertaking. Traditional SD-WAN solutions fall short in meeting the robust security requirements critical for modern branches. A staggering 97% of IT professionals fear the catastrophic consequences of a data breach caused by unsecured IoT devices. Furthermore, the remote management of IoT devices within the branch can be a formidable challenge, frequently leading to costly truck rolls.

As organizations embark upon their secure access service edge (SASE) journey, it is critical to gain deeper insights into devices and their risk profiles and behaviors in order to establish appropriate access controls and optimize access to critical resources.

## The Solution

Netskope Borderless SD-WAN seamlessly integrates Device Intelligence functionality with the SASE Gateway, enabling the automatic discovery and classification of both managed and unmanaged IP-connected devices within the branch network.

In contrast to conventional SD-WAN solutions that rely on static device parameters like IP and MAC addresses for policy enforcement, Borderless SD-WAN leverages context-aware intelligence to enforce access control policies. These policies are defined by granular and dynamic device attributes, including device type, real-time risk assessment, ownership, and control, among others.

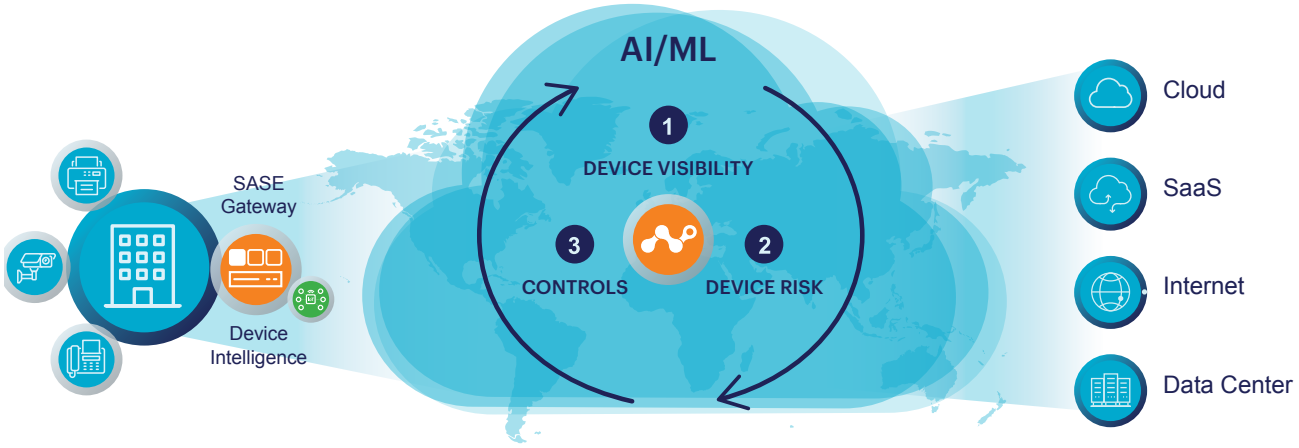


Figure 1: Device discovery and intelligence for context-aware policy

## Automated device discovery and classification

With the large number of IoT devices in use today, it becomes crucial for organizations to establish visibility into the connected devices, discover any shadow IoT device, and understand their operational purposes.

Netskope SASE Gateway uncovers managed and unmanaged devices within the branch network and shares the device telemetry with Device Intelligence for rich and dynamic device context. This is combined with machine learning algorithms to generate unique models and signatures for each device, which includes type, category, ownership, OS, functionality, location, risk, vulnerability information, and more.

The rich device context can be used for automated classification and device mapping, and establishes granular context-driven access control and policy enforcement. This is especially important when profiling IoT devices using deeper understanding of devices entering, exiting, or connected to a network. A corporate-owned security camera may have a different risk profile than a conferencing system or a wireless printer. Newly discovered devices can be automatically identified and grouped into the appropriate device category to granulary enforce its levels of service and access.

## Assured application experience for high-priority devices

In connected environments, such as industrial automation, real-time access to critical data and timely responses are essential for improving overall network performance and reliability. Unmanaged BYOD devices should not be allowed to seize up the network with unrestricted access, nor consume bandwidth needed by corporate devices that deliver business-critical functions.

Netskope SASE Gateway provides differentiated application experience for every connected device through device context-aware AppQoE policies, assuring optimal application performance for high-priority applications. The device context information is shared by Netskope Device Intelligence to the SD-WAN orchestrator, which leverages the information to assign priority to various device requests. For example, a QoS rule can be set up to prioritize the traffic from managed security cameras over any gaming traffic originating from any user's laptop.

## Blocking high-risk devices to prevent lateral movement

Traditional network security products use limited, static device attributes for enforcing firewall and access control policies. With users and devices dynamically connecting, and each device having a different risk profile, this leads to the growing number of entry vectors for malware and botnet attacks.

Netskope SASE Gateway manages device-initiated cybersecurity risks by monitoring branch networks, providing dynamic risk assessment on a device's posture, and by enforcing effective security policies based on integrated IPS capabilities. This allows organizations to implement risk-based security policies through the SASE Gateway based on the risk score computed for every connected device by Device Intelligence. For example, blocking high-risk devices from accessing critical applications and services, and preventing the spread of any potential malware from rogue devices.

## Zero trust security with micro-segmentation

Traditional segmentation tools, like NACs and VLANs, rely on coarse-grained segmentation methods that hinge on static device information (such as IP addresses, subnets, and ACLs). Their limitations become evident when faced with devices that can easily impersonate others. For example, a malicious actor could connect a laptop to the same subnet as a statically segmented audio-video conferencing device and eavesdrop on SIP communications.

Device Intelligence, on the other hand, provides robust device context, which the Netskope SASE Gateway leverages to identify breaches and automatically institute dynamic micro-segmentation for these devices based on detailed attributes. This precision enables the isolation and prevention of lateral movement of potential threats.

These advanced micro-segmentation capabilities empower organizations to segregate devices based on highly specific attributes. Security settings and access control policies can be fine-tuned by considering physical properties like device type, interface, and functionality, as well as logical properties such as ownership and control. Additionally, these settings can adapt based on dynamic threat and risk assessments, facilitating the implementation of a zero trust security model for all connected devices. Any device on the network segment that deviates from the established profile—particularly those with high risk scores—can be swiftly and automatically isolated and quarantined to thwart both vertical and horizontal threat propagation.

> Netskope SASE Gateway uses Device Intelligence for robust context to identify device-related risks and dynamically micro-segment vulnerable devices based on granular attributes, preventing lateral movement of potential threats

## Secure zero trust device access

Netskope Borderless SD-WAN delivers proactive (Day 2) support through zero trust secure access to remote devices inside the branch, including phones, ATMs, and servers via HTTP, RDP, SSH, and VNC, speeding up incident resolution. The importance of this capability becomes imminent when managing high-value assets remotely, e.g., upgrade or troubleshoot, normally the third-party support needs to go onsite, or remote desktop with the technician onsite, or open ports and VPN to the highly valuable asset machine, which is increasing operational cost and opens security vulnerability. With Netskope Borderless SD-WAN, the support team can remotely connect to the highly valuable asset machine from SASE Orchestrator and securely open the session with the device via the access method the machine supports.

| BENEFITS | DESCRIPTION |
|---|---|
| **Hardware consolidation** | Combining device discovery, data collection, and Borderless SD-WAN in a single appliance streamlines management and cuts costs. Hardware consolidation enables one-click Device Intelligence activation via the Borderless SD-WAN portal, enhancing simplicity. |
| **Agentless device discovery** | Obtain a full device inventory without agents, ensuring comprehensive asset management for unified control, security, and network scalability. |
| **Comprehensive visibility into granular device attributes** | Cloud-managed single-pane-of-glass at the Borderless SD-WAN portal offers a complete view of connected devices with attributes, telemetry data, including type, ownership, and risk scores. |
| **Optimized and secure connectivity** | Borderless SD-WAN ensures optimized, secure dynamic connectivity to critical applications from all network devices. |
| **AI/ML-driven device risk assessment** | Patented risk assessment and identification of known and unknown risks by correlating context, device activities, and known vulnerabilities. Unique device risk scores are generated for both managed and unmanaged devices based on their attributes and behavior. |
| **Automation and policy enforcement for large-scale networks** | Employs a powerful policy engine that automates and enforces policies across all devices participating in a large-scale deployment. |
| **Mitigate legal liabilities** | Micro-segmentation and integration with intrusion prevention system (IPS) helps in reducing the blast radius, ensuring data privacy and preventing unauthorized access to data from risky devices. |
| **Secure zero trust device access** | Delivers proactive (Day 2) support through zero trust secure access to remote devices inside the branch, including phones, ATMs, and servers via HTTP, RDP, SSH, and VNC, speeding up incident resolution. |