netskope

White Paper

Achieving Zero Trust for Connected Devices

ZERO TRUST - A QUICK PRIMER

With organizations expanding out of network perimeters to cloud-based deployments, and users accessing corporate resources from any location and device, traditional security solutions are no longer sufficient for securing all the various sources of data. Traditional network security solutions, by design, grant unrestricted network access to every authenticated user, leading to the risk of sensitive data exposure through multiple cybersecurity threats and vulnerabilities, including credential misuse, configuration errors, malicious insiders, botnets, and malware.

The concept of zero trust proposes a granular, context-driven approach for securing users, data, and devices. The primary goal of a zero trust approach is to shift from a "trust, but verify" to a "verify, then trust" approach. By default, zero trust doesn't allow resources to place implicit trust in any entity that wants to connect to corporate networks, and access is granted in a least privileged manner only after evaluation of several contextual elements, including user identity, device identity, device security posture, geolocation, time of the day, sensitivity of the data being accessed, and others.

Core zero trust principles include:

- **Granting the right amount of privileges:** Allow access to a specific resource only for that specific interaction through assessment of user and device identity and security posture.
- **Maintaining an explicit trust model:** Every entity is untrusted and strong authentication must be established before allowing access to any resource.
- **Performing continuous assessment:** Continuously monitor for changes in context that require reassessment of trust. For example, re-authentication, step-up authentication, alteration of permissions, or increased/decreased access.

Achieving true zero trust requires transformation across networks, applications, data, users, and devices to reduce risk and increase business agility. In this paper we will focus on the essential requirements for enabling zero trust device security and how Netskope Device Intelligence, through its highly granular and context-rich device fingerprinting model, allows organizations to establish an effective zero trust approach for securing their networks against device-based threats.

Gartner, Inc. predicts that by 2026, **10%** of large enterprises will have a mature and measurable zero-trust program in place, up from less than **1%** today.

REALIZING ZERO TRUST FOR DEVICES

Securing devices with zero trust principles requires continuous evaluation of the device security posture and developing an appropriate level of confidence or trust for that specific interaction. Any changes to the device context should dynamically alter the trust levels and in turn re-evaluate the access granted to that device. Device monitoring and observation must involve device fingerprinting and risk profiling to get an accurate behavioral map, with access to other resources dependent on the outcome of this mapping and observations. Achieving this requires:

- **Granular device context:** Deep context about every device, resource, and user in and around the network
- **Micro-segmentation:** Ability to dynamically group devices into software defined perimeters based on the above context and geo location
- **Dynamic control:** Dynamically control the access these devices have to sensitive resources in the network, based on context and real time threat assessment
- **Security automation:** Automated alert handling and responses to security incidents

Need for granular device context

With the explosion of the volume and types of connected devices, gaining end-to-end visibility into all devices (i.e., device fingerprinting) has become of critical importance to ensure security, and enforce right access control across the network. Current device fingerprinting technologies boil down to type, category, OS, version, etc. which are woefully inadequate for correctly profiling the device behavior and setting adequate controls to protect the device and the infrastructure it operates in. To keep networks secure you need to have a deeper understanding of devices entering/exiting your network, their dynamic behavior, and the risk associated with them to take precise actions. This calls for developing rich and dynamic device context across multiple dimensions, combining them with machine learning algorithms to generate models and signatures for each device. This rich contextual device intelligence allows for granular visibility and control.

The critical role of micro-segmentation

Over the years companies have relied on traditional network segmentation tools, such as NAC, VLANs, authentication, and access control lists (ACL) for creating subnets within the networks. The coarse-grained segmentation offered by these tools based on static device information, such as IP Address, subnets, and ACLs, leads to flat trusted zones that fail to account for dynamic device behavior or risk posture, rendering them ineffective against rogue devices. For example, if the audio video conferencing devices are statically segmented into a specific subnet, it is easy to plug in a laptop in the same subnet and sniff and snoop on the SIP communications. It is also easy to make a mistake and connect a conferencing device into other subnets, thereby creating more exposure than necessary.

Micro-segmentation, on the other hand, is a more granular dynamic method of creating secure or trusted zones of connected devices. Micro-segmentation utilizes zero trust principles to isolate devices from one another using deep contextual information and secure them individually. Micro-segmentation is implemented in the software, using a layer that is decoupled from the underlying network hardware and NAC tools. This makes the segmentation easier to deploy and manage, providing security beyond static rules and authentication mechanisms to limit the blast radius in case of a security event.

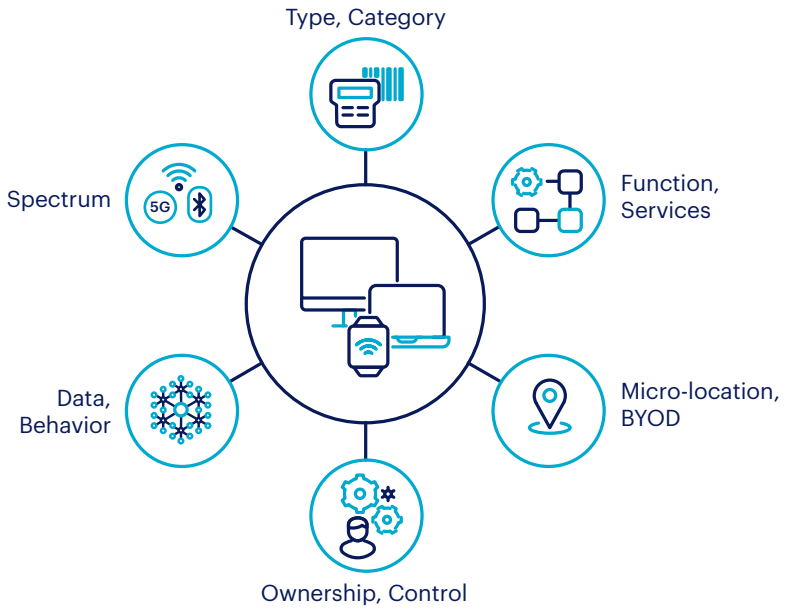
Employing AI/ML for intelligent, dynamic controls

Zero trust architecture should not be static, especially when the number of devices accessing the network is growing exponentially. A dynamic approach would entail a learning engine to classify devices and provide the right contextual information, and a policy engine to enforce nuanced security and access controls. The architecture should continuously monitor and adapt to the current state of the device, network, its threat exposure and should not be defined as a set of static rules.

HOW NETSKOPE DEVICE INTELLIGENCE ENABLES A ZERO TRUST ARCHITECTURE

Netskope Device Intelligence uncovers managed and unmanaged devices on the network spectrum and fingerprints those devices based on their unique characteristics across multiple dimensions. These dimensions include multiple layers; all the way from hardware, software, logical, functional and other operational characteristics. The device information is collected from multiple network interfaces, protocol information, traffic flow, and application heuristics. This is combined with organizational information from existing CMDB, tools like MDM, EDR, vulnerability assessment, firewall, times of operation and location amongst others to develop rich and dynamic device context. This context is then fed to machine learning algorithms to generate unique models and signatures for each device, which includes the following information, called HyperContext®:

- Association of all the physical interfaces of the device and the spectrum of operation of each interface
- Type, Category of the device and related information
- OS, patches, services, and applications running on the device
- Functionality or the "purpose in life" of the device
- Micro location of the device, its mobility patterns, and times of visibility
- Ownership information of the device and its control information
- Users on the device
- Behavior based analysis of all the data transmissions across all protocols and spectrums
- Risk and vulnerability information, other information collected by other tools used



Generating device TruID™

The device HyperContext information derived by Netskope Device Intelligence is used to generate a unique device identifier and authenticity rating called TruID which renders three types of device fingerprints: device identity fingerprint, device group fingerprint, and device operational fingerprint. These fingerprints accurately recognize the device, group devices of the same kind together, and establish the device's normal operation and function.

TruID works on zero trust principles and the assumption that all devices trying to gain access to the network are compromised and have their MAC addresses already spoofed. To authenticate such devices, TruID machine learning algorithms generate their own set of MAC addresses for every device presenting itself for credentialing and only provide access when there is a true match. This is a far superior measure and approach to establishing an effective zero trust security architecture because TruID:

- Automatically identifies all types of devices in the organization
- Instantly identifies anomalous behavior in the devices whose fingerprints have been collected
- Generates labels based on all the collected information, intermediate insights and final fingerprints and uses these labels in the micro-segmentation and policy layers
- Offers insights about the risks, threats associated and best practices

HyperContext® driven micro-segmentation

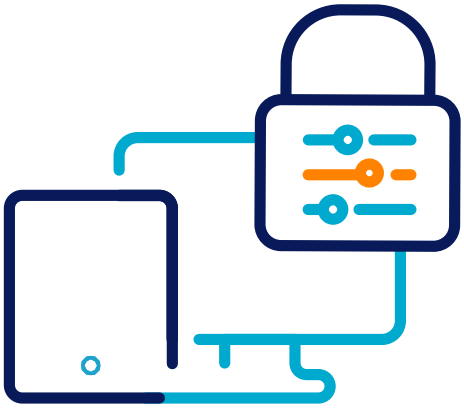
Netskope Device Intelligence drives advanced micro-segmentation capabilities with strong device context. As devices enter and leave a network, it's paramount to dynamically control the access for these devices and users to other resources in the network, based on context and real time threat assessment. Using Device Intelligence, network operations teams can tailor security settings and create access control policies that limit communication between devices based not just on authentication, traffic, and application information but by a combination of physical properties such as device type, interface, and functionality; logical properties such as ownership and control; by threat and risk assessment; and by dynamic properties such as location and time.

Irrespective of the authentication used, or the network segment that the device is connected to, device context allows granular access control based on many different device properties, aligned to zero trust principles.

Dynamic access control for smart devices on the move

Netskope Device Intelligence incorporates a dynamic, machine-learning driven approach that takes multiple device-level attributes into consideration, including security posture, context and real-time threat assessment, to offer next generation, software-defined access control. The benefits of this approach are many, including:

- Any device on the subnet that does not match the profile of others, for example a VoIP phone or an IP camera, can be isolated from other devices in that network segment.
- The system can monitor devices for their dynamically changing context, including as smart devices move across locations, and adapt to their current state, the network they are connected to, and their overall threat exposure to enforce policies based on real-time device behavior.



Automation for productivity and risk reduction

Through automated discovery of connected devices in the network and generating device context and fingerprints, Netskope Device Intelligence simplifies the process of security automation. The device-level intelligence can be fed to a sophisticated policy engine to automate device classification, asset management, dynamic risk assessment, segmentation, and access control. This ensures that the devices have the right configurations, meet the right compliance goals, are part of the right network subnets and have the right access they need. Anomalous devices not responding or repeatedly failing the automated policy controls are identified and alerts sent to the operations team, reducing workload, alert noise, and system stress.

Netskope Device Intelligence also integrates with leading SIEM and SOAR solutions for advanced threat detection and response. Advanced correlation capabilities that significantly reduce threat hunting time and allow security personnel to identify potential threats that may have been missed during manual inspection. The enriched SIEM alerts are ingested into SOAR playbooks for automating threat responses and improving the overall security hygiene of the connected devices.

CONCLUSION

The continued explosion of IoT devices and related cybersecurity risks demand a zero trust approach that tightens controls around connected devices to mitigate threats and prevent network breaches. Netskope Device Intelligence addresses the critical device discovery and governance challenges for managed and unmanaged devices, and utilizes zero trust principles for micro-segmentation and adaptive access control based on real-time device context.

By extending device context to Netskope's Secure Access Service Edge (SASE) platform, Netskope Device Intelligence aims to protect connected devices at scale and allow streamlined visibility, policy enforcement and incident management, from a converged, fully integrated platform.

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.