netskope

White Paper

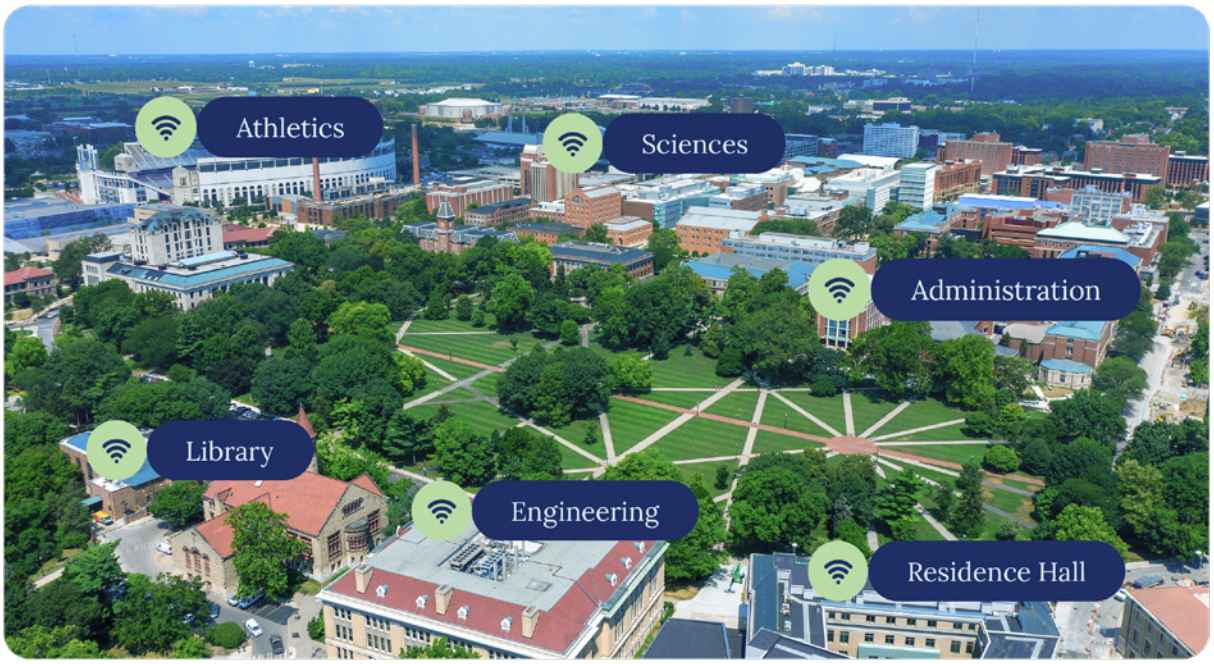
Netskope IoT Security for Higher Education

Education

NETSKOPE IOT SECURITY'S AGENTLESS NETWORK SEGMENTATION & ACCESS CONTROLS

Over the past few years, the Internet of Things (IoT) adoption has gone beyond an industry buzzword to a key business enabler, delivering significant value in the cloud and mobility era. According to IDC, by 2025, there will be 55.7 billion connected IoT devices (or "things"), generating almost 80B zettabytes (ZB) of data.

Higher education is predominant in the usage of IoT devices, utilizing them for infrastructure management and for improving the overall student and faculty experience within the premises. Collecting data from connected devices for personalized learning experiences, implementing energy-efficient utility systems, securing the campus networks through smart cameras—the benefits offered by IoT devices make them indispensable to educational institutes.



Potential high-level network segmentation zones

As Higher Ed starts tapping into the potential benefits of IoT, there is a need to focus on addressing security-related challenges, such as:

- Gaining visibility into every device entering and leaving the campus network
- Classifying the wide range of connected devices and grouping devices exhibiting similar behavior for policy enforcement and control at scale
- Identifying the device-level risks to defend against potential DDoS and botnet activity, which can get amplified by compromised devices
- Securing huge volumes of data generated by connected devices, especially highly confidential data such as student records, financials, and medical data

For multiple devices active within the campus networks, ranging from smartphones, smart watches, smart TVs, vending machines, gaming consoles, cameras, printers, and many more, defining best practices around the usage policy and access control can be key to avoiding disasters in advance. Whether ransomware, DDoS, or even just a misconfiguration from a device that saturates the network to a standstill, any incident can have profound consequences to both privacy and network availability.

KEY CYBERSECURITY CHALLENGES FROM IOT ON CAMPUS

Increase in attack surface

Mobile devices on campus have exploded in recent years, with an average student bringing five to seven internet-connected devices to campus[1]. Most of these devices lack built-in security controls to secure the data transmissions. This makes them prime targets for cyberattacks, with about 60% of the education institutions globally suffering attacks in 2021 as against 44% in 2020, according to the "State of Ransomware in Education 2022" report.

Sideways motion from smart devices

IoT devices may likely be equipped with multiple interfaces for connectivity over Wi-Fi and RF spectrums like Bluetooth. These interfaces can be exploited by threat actors for launching denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attcks, brute force attacks, phishing attacks, BlueBorne attacks, and can result in illegal access to internal resources through lateral movement.

Student device vulnerabilities

From laptops and smartphones, to tablets and watches—devices are on campuses to stay. These mobile devices connect over multiple public and private networks, and continuously transmit data, often over unencrypted channels, making them a significant attack vector to infiltrate campus networks.

Patching and security updates

CCTV systems, smart routers, and others have all been used in highly publicized attacks over the last few years, and these are mandatory security systems for campus safety. However, many IT departments argue with physical security on who owns these devices, especially where patches and firmware updates are concerned.

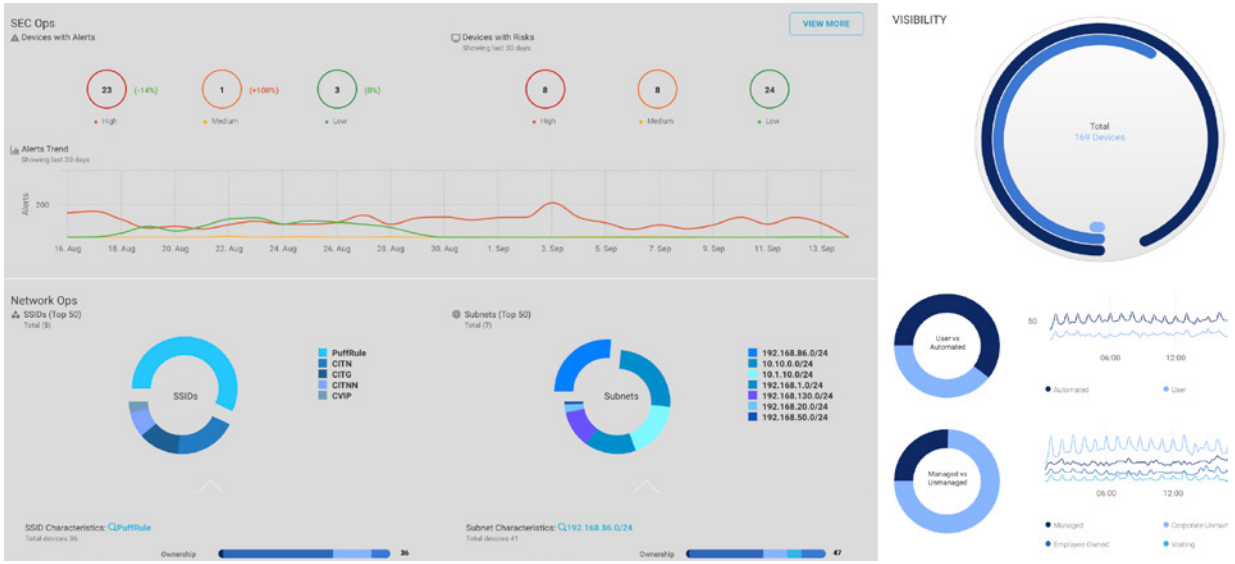
Netskope IoT Security is the single source of truth to provide deep visibility into all connected devices, assess their risk profiles, and control access.

The IoT Security platform conducts a site-wide survey of all smart devices used on campus—whether they are connected to a network or are operating in airspace, the system provides a prioritized list of risk exposure. With a highly nuanced policy engine, administrators can micro-segment their campus by floor or building, department, or group function to contain the attack surface.

[1] www.acuho-i.org/Portals/0/doc/res/resnet2019.pdf

NEED FOR CONTEXT-DRIVEN SECURITY FOR CAMPUS DEVICES

Educational institutes host a wide set of connected devices, ranging from IP cameras, access points, and video conferencing devices, to unmanaged student and faculty devices, such as smartphones and wearables. Developing rich context on these devices has become of critical importance to ensure security and enforce the right network access controls to the network. Current device fingerprinting technologies boil down to device type, category, OS, version, etc., which are woefully inadequate when it comes to making timely, informed security decisions. To keep networks secure, you need to have a deeper understanding of devices entering and exiting the campus networks, and map their dynamic behavior with associated risks to take necessary actions. This calls for developing rich and dynamic device context across multiple dimensions and combining them with machine-learning algorithms to generate models and signatures for each device, allowing granular visibility and control.



Netskope IoT Security Executive Dashboard

NETSKOPE IOT SECURITY CAPABILITIES

Device Detection By Scanning Multiple Spectra

Through a simple out-of-band connection to your network, the Netskope IoT Security platform profiles and classifies devices, users, connections, applications, and operating systems throughout the campus environment. Netskope IoT Security shows you all the devices and the connections that exist, including connections to unmanaged devices or rogue networks that your organization may otherwise not detect IoT Security scans multiple communication protocols like Wi-Fi, Bluetooth, and BLE, and looks for devices both on and off the network, including the RF spectra. If the device emits an RF frequency, IoT Security can see it, fingerprint it, and categorize the risk to the rest of the network along with providing recommended actions.

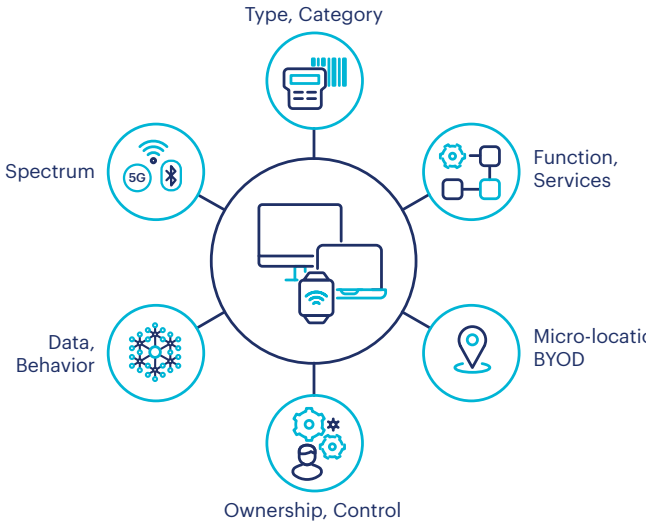
Accurate Smart Device Discovery

The deep device detection technology of Netskope IoT Security yields accurate device counts and renders a dashboard showing high-priority risk items requiring remediation. If a device has multiple network interfaces for sharing information, IoT Security correlates these multiple interfaces as belonging to a single entity, providing an accurate accounting of devices. The comprehensive device inventory that IoT Security generates includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications, classification, and connections made over time.

HyperContext® for Campus Devices

Netskope IoT Security profiles every detected device on hundreds of attributes to generate a granular device context database. These attributes include:

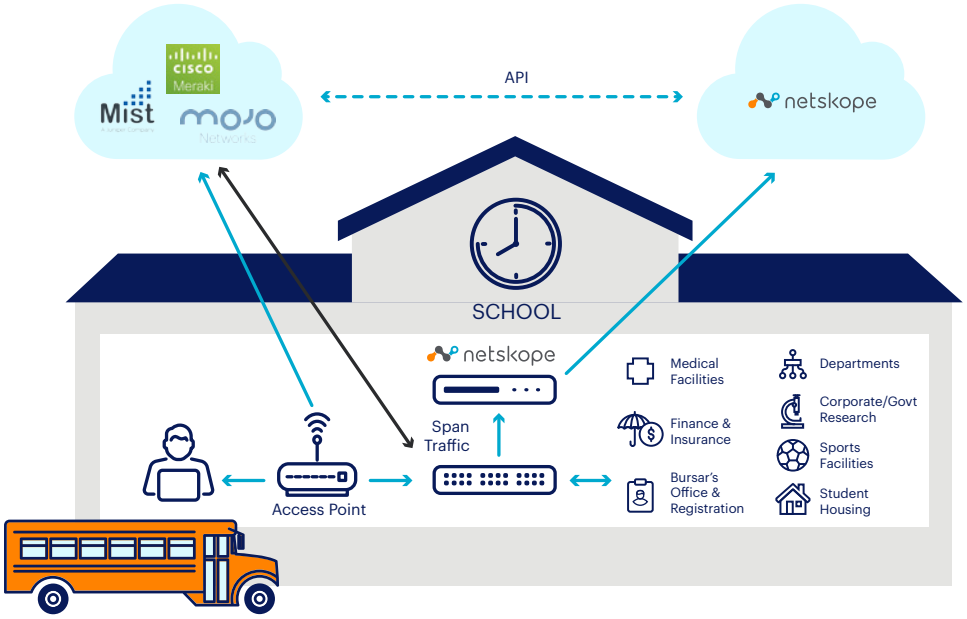
- Association of all the physical interfaces of the device and the spectrum of operation of each interface
- Type, category of the device, and related information
- OS, patches, services, and applications running on the device
- Functionality or the "purpose in life" of the device
- Micro-location of 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 and other information collected by other tools used



All the collected data and insights are used to develop a unique device identifier and authenticity rating, called TruID™, which accurately recognizes the smart device or robot, groups devices of the same kind together, and establishes the device's normal operation and function. Once you know the TruID of each IoT device, you can create appropriate exclusions (e.g., personal fitness, personal medical use) and zero in quickly on vulnerable devices constantly connected to your network—and prioritize mitigation and risk reduction appropriately.

Network Segmentation

Netskope IoT Security's network segmentation is simpler to implement, more robust and scalable, and closes a glaring gap found in traditional NAC solutions that fail to secure managed and unmanaged devices. The technology is based on the premise that each device has a completely different risk and threat assessment profile and hence needs different treatment for access control. For example, smart vending machines tend to be managed separately from the smart locks and smart cameras, keeping your campus safe at night.



Netskope lets you continuously, dynamically, and automatically segment the network at the device level based on the needs and zones of your campus:

PHYSICAL PROPERTIES	LOGICAL PROPERTIES	RISK CATEGORIES
Device Type	Ownership	Location
Interface	Controls	Time of Operation
Functionality	Department of Use	Student/Faculty Data, etc.

By distilling it down to each device, your security teams can:

- Auto-enforce granular policies based on device context
- Enable more granular control of network systems
- Isolate devices in real time upon detection of security flaws

Dynamic Access Control for Smart Devices on the Move

Some smart devices are constantly on the move when needed in different departments, floors, or rooms. Netskope offers next-generation NAC-less, software-defined dynamic access control based on security posture, context, and real-time threat assessment. The benefits of this approach are many:

- Static rules based on L2-L3 based segmentation, access control lists (ACLs), and user authentications are inefficient for today's scenario, where the context of connecting devices should be an inherent element in the rules configuration. Instead, a dynamic and machine-learning driven approach is adopted, taking multiple device-level attributes into consideration.
- Any device on the subnet that does not match the profile of others, for example a vending machine or CCTV camera exhibiting anomalous behavior, can be quarantined from other devices in that network segment.
- Dynamic access control is critical for micro-locations within a specific location—as smart devices move between floors and rooms, the system continuously monitors devices for their location and adapts to their current state, the network they are connected to, and their overall threat exposure to enforce policies based on real-time device behavior.

OUR BUSINESS VALUE FOR EDUCATION

Automate device discovery: Netskope IoT Security discovers every connected device in your environment without requiring a physical search, and automatically classifies them based on user, protocols, type, function, ownership, etc.

Track smart device usage: With a dynamic and exhaustive inventory of all smart and other devices used in each floor and department, you can find lost equipment, drive utilization upwards by calculating peak usage in each department, and potentially reduce over-purchasing, thus freeing up resources that can be reused elsewhere.

Protect your infrastructure: Netskope IoT Security performs continuous device monitoring to detect unauthorized access, malicious behavior, and anomalous data transmission. The IoT security solution integrates with SIEM and SOAR platforms for providing unparalleled insights into possible network threats and automating alert handling at scale.

Bolster security and access management: The Netskope IoT solution seamlessly integrates with network security systems, including firewalls, network access controls, and access points for automating network segmentation and facilitating secure network access.

NETSKOPE'S PARTNER-FIRST APPROACH

Netskope partners with the world's leading consulting and service delivery partners to help organizations secure their digital transformation initiatives. With our combined strengths, we deliver customized, integrated, and fully managed solutions and services to help customers protect their users, their data, and their business. Learn more about our Service Delivery Partners and System Integrators.

Netskope also partners with the strongest companies in enterprise technology. From integrations with cloud storage services to delivering cloud forensics to your SIEM to closed-loop workflows with your identity management system, Netskope snaps into your infrastructure to deliver the most comprehensive and efficient security in the market. Learn more about our technology partners.

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope 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**.