netskope

White Paper

Securing Healthcare Organizations with Netskope IoT Security

Healthcare

NETSKOPE IOT SECURITY'S AGENTLESS NETWORK SEGMENTATION & ACCESS CONTROLS

The Internet of Medical Things (IoMT), consisting of interconnected medical devices and applications, has been a driving force in digitizing the healthcare industry. From patient monitoring and infusion pumps to early detection of illness through wearables, connected medical devices have come a long way in providing state-of-the-art patient care.

At the same time, the increased adoption of these devices in healthcare delivery organizations has expanded the cyber threat landscape and opened up multiple infiltration points for malicious actors to exploit. Ransomware attacks, in particular, have plagued the healthcare industry in recent times, derailing internal systems and critical infrastructure, putting both patient data and their lives at serious risk. According to the "State of Ransomware in Healthcare 2022" report, 66% of healthcare organizations surveyed were hit by ransomware in 2021 - almost double as compared to 2020.

With a majority of cyber-attacks being traced to device related vulnerabilities, adopting a comprehensive approach to mitigate device security risks, while tapping into the potential benefits of a connected ecosystem, should be one of the top cybersecurity priorities for the healthcare industry. More specifically, the focus needs to be on:

- Gaining end to end visibility into all the connected medical devices and unmanaged BYOD, along with deep actionable insights into their risk profiles
- Classifying internal, patient and guest devices for granular access control and policy enforcement at scale
- Identifying and isolating rogue devices to defend against cyber-attacks and botnet activity, that can get amplified by compromised devices

Defining best practices around the usage of IoT devices in healthcare and controlling their access to critical data and resources is the key to avoiding disasters in advance. Whether ransomware, DDoS, or even just misconfigured devices that saturate the network and bring it to a standstill, any incident can have profound consequences to both privacy and network availability.

KEY CYBERSECURITY CHALLENGES FROM IOT IN THE HEALTHCARE INDUSTRY

Increase in attack surface

Spurred by technological and connectivity advancements, such as 5G and Bluetooth, medical IoT device adoption is constantly on the rise. With each device acting as a potential attack vector, the explosion in the number, type and mix of smart devices in the healthcare sector has created a large attack surface to manage and control.

Medical device vulnerabilities

Vulnerabilities in connected medical devices, either due to lack of visibility, outdated software or the evolving threat landscape, coupled with the volume of sensitive PHI data they contain and exchange, has resulted in healthcare providers dealing with ransomware and DDOS threats on an ongoing basis. According to Cynerio's "The State of Healthcare IoT Device Security 2022" report, more than half of connected medical devices in hospitals contain critical vulnerabilities, creating significant data security and patient safety risks.

Sideways motion from smart devices

Medical 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) attacks, brute force attacks, phishing attacks, BlueBorne attacks, and can result in illegal access to internal resources through lateral movement.

The rise in BYOD

Hospitals are teeming with BYO devices, from wearables, smartphones and other gadgets carried by the doctors, patients and visitors. Most of these devices fall under the 'unmanaged' category, and can fly under the radar of the network and security operations teams, putting the hospital network at risk due to undetected vulnerabilities and unauthorized access from compromised devices.

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 medical IoT devices — 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 devices in the healthcare provider networks by floor or building, department, or group function to contain the attack surface.

NEED FOR CONTEXT-DRIVEN SECURITY FOR MEDICAL DEVICES

Medical institutes host multiple connected surgical and monitoring devices used for remote patient monitoring, heart rate monitoring, robotic surgery and radiotherapy, along with a wide set of managed IT equipment ranging from IP cameras, access points and audio-video conferencing systems, to unmanaged staff and patient devices, such as smartphones and wearables. Developing rich context around these devices has become of critical importance to ensure security and enforce the right network access controls. 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 hospital 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 healthcare 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

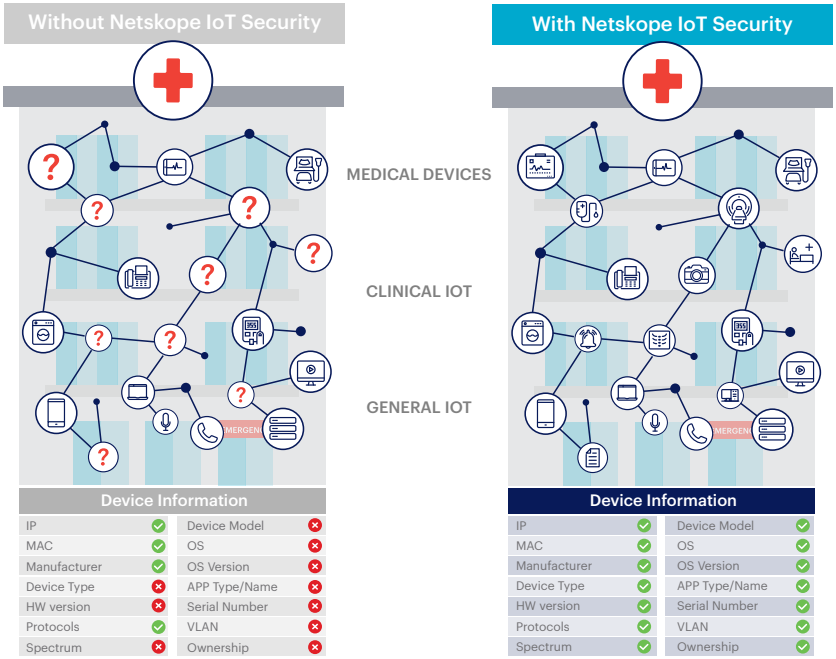
The deep device detection technology of Netskope IoT Security yields accurate device counts and renders a dashboard showing high-priority risk items requiring remediation. If a device has multiple network interfaces for sharing information, IoT Security correlates these multiple interfaces as belonging 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 Medical 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, 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 (personal fitness, personal medical use, e.g.) and zero in quickly on vulnerable devices constantly connected to your network — and prioritize mitigation and risk reduction appropriately.



Netskope IoT Security HyperContext®

Network Segmentation

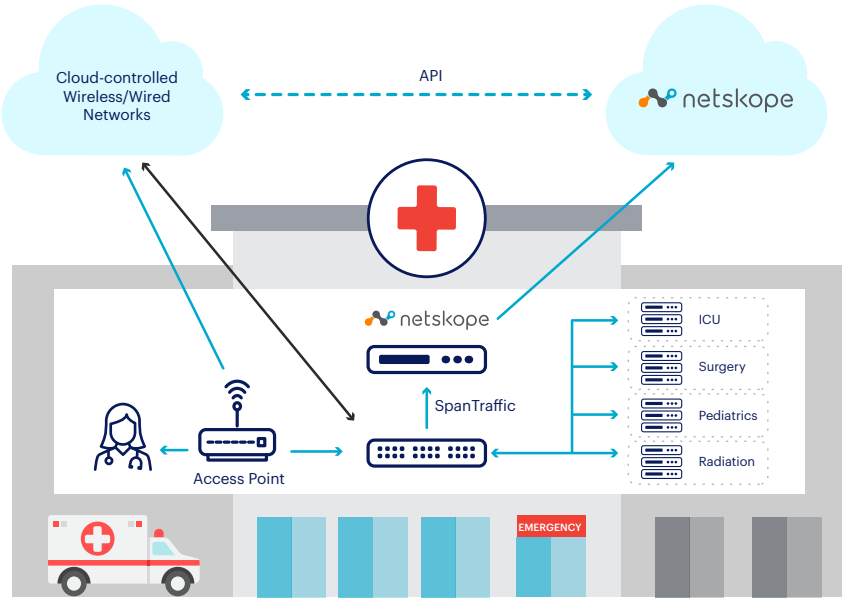
Netskope IoT Security's network segmentation is simpler to implement, more robust and scalable and closes a glaring gap found in traditional NAC solutions that fail to secure managed and unmanaged devices. The technology is based on the premise that each device has a completely different risk and threat assessment profile and hence needs different treatment for access control. For example, a monitoring system has a different risk profile than a wearable or a security camera.

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

PHYSICAL PROPERTIES	LOGICAL PROPERTIES	RISK CATEGORIES
Device Type	Ownership	Location
Interface	Controls	Time of Operation
Functionality	Department of Use	ICU, Surgery, 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 Network Segmentation

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 within the hospital network. 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 HEALTH DELIVERY ORGANIZATIONS

Protecting your patients: Netskope IoT Security can alert security managers, duty shift leaders, or others to current cyberattacks as well as any new compromised medical, clinical, and other smart device. This leads to a much faster incident response and allows for general staff awareness of potential dangers to their operations.

Protection against major ransomware attacks: Identify Conti, WannaCry and other types of system-stopping ransomware in real time. This reduces your potential downtime and risk to patients, not to mention the impact on the hospital's reputation.

Automated and dynamic device inventory: Most hospitals have never done a full IT survey of every hospital device, let alone specialized smart devices including medical equipment, as part of their network discovery. Netskope IoT Security automatically discovers every connected and non-connected device in your environment without requiring a physical search, and creates a comprehensive device database using its inbuilt cyber asset management capabilities.

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**.