CASE STUDY

**INDUSTRY**
Healthcare

**ENVIRONMENT**
2000+ beds hospital serving more than 150 locations across the region with over 10,000 connected medical devices in operation

**KEY CHALLENGES**
- Identify connected medical devices by make, model, and version
- Continuous threat protection for networked medical devices
- Asset "source of truth" for biomedical CMMS
- Integration with existing ITSM workflow
- Compliance will not allow network tap b/c ePHI/HIPPA risk

**SOLUTION**
- Securolytics® IoT Security Appliance + Cloud
- Securolytics® Medical Device Catalog License

**RESULTS**
- Deployed without tapping core switches in less than 30 mins
- Profiled over **10,000+** medical IoT devices
- Gained visibility into **4,000+** at risk medical IoT devices
- Achieved integration with ServiceNow™ for support ticketing automation
- Streamlined IT and OT group with 1 "source of truth" IoT asset inventory
- Automated alerts for operators for incident detection

# One of the Nations Largest and Most Prestigious Medical Centers Trusts Securolytics® to Secure Connected Medical Devices and be "Source of Truth" for Automated IoT Asset Inventory

## Customer Profile

One of the nations largest and most prestigious medical centers that employs over 40,000+ people. Combining a population health perspective that focuses on the health needs of communities with nationally recognized clinical excellence, they deliver coordinated, compassionate, science-driven care where, when and how patients need it most using the latest medical IoT devices and connected technologies. The health system consists of many hospitals and extended care facilities that total 2,000+ beds, and state-of-the-art primary and specialty care provided through a network of more than 150 locations across the region which has over 100,000+ endpoints connected at any given time.

## Customer Challenge

The customer's existing firewall, IDS, and endpoint products only showed the number of active MAC and IP addresses in use. Their leading security vendors could not identify the type of medical devices connected to the network, evaluate the risk posed by each device, detect unusual or suspicious behavior exhibited by the devices or determine if and when an IoT device had become compromised. The customer compliance team also did not want a solution that used network tap/span ports to collect data to mitigate risk from exposing the organization to ePHI being sent to the cloud. A majority of their connected medical and infrastructure devices were unidentifiable and unmanageable.

The challenge the CISO posed to our team was:

**"How can I get immediate visibility today into my connected medical IoT devices on our network without having to collect network tap data that includes ePHI and sensitive data for the answer?"**

The devices also didn't support running agents or produce logs so they were hard to identify or monitor for security.

Manufacturers did not build-in security into the device itself.

The medical devices could not be configured and had commonly deployed default passwords that were easily available (even on the manufacturer's website). When manufacturers or their partners came in to assess the security of their devices such as IP cameras or surgical robots, the security team had no tool to validate their assessment.

They also lacked resources for methods of operation to research the device's behavior. The team also wanted to know what devices were sharing the network with the connected medical devices.

In their environment connected medical IoT was critical. Knowing exactly what IoT was on the network and where they were located on the network was important so they could be properly excluded from vulnerability scanning or NAC scans.

Their NAC vendor was identifying devices solely by MAC address lookup obtained from the NIC card. This would render inaccurate identification because many of the IoT manufacturers used 3rd party NIC cards in their devices.

They also exhibit risky behavior by default such as connecting to other devices and transmitting data, have hard-coded credentials that could not be changed, and automatically created insecure open ports services like TELNET and HTTP. Integrating with their ITSM ServiceNow™ was also a high-priority so they could operationalize the data and implement IoT incident detection into their workflow and alert the operator to dynamic threats.

## Why Securolytics®

The medical center security team was told directly by GE, Siemens, and Phillips that under no circumstance should they run a network access controller (NAC) scan or any vulnerability scanner against their connected medical devices as they were intrusive and could cause catastrophic consequences. The security team turned to Securolytics® and deployed in minutes without agents or network taps and did not collect any PHI, PCI, or sensitive data per the customers HIPPA compliance requirements. The implementation was a 100% automated post plug-in. Unlike NAC or vulnerability scans, Securolytics® runs non-intrusively using our unique PortSafe-Inspection™ Technology which is safe on sensitive medical IoT assets. The automated discovery of every device connected to the network that accurately identifies devices by make, model, and version that uses a proprietary method that does not solely rely on MAC address lookup and categorizes devices by type, including restricted devices, and identifies what network the device is on and all ports in use by each device. The continuous threat detection determined which devices could be hijacked or have vulnerabilities. When they connect to the network the software tracks at risk devices across networks from a central deployment and also optionally checks for default passwords, exploitable ports, ransomware and alerts when devices are on the network that come under CVE, ICS-CERT advisories. This automated, continuous, and device-specific security monitoring profiles each device's behavior and communications and compares it to the profile of the device's default behavior in the Securolytics® Device Library™. Results are operationalized by integrating with existing ITSM systems and generating alerts via SMS or e-mail.

## Customer Impact

Within 24 hours of passively plugging in the Securolytics® Appliance, the customer had a eye-opening experience when reviewing the results report. They were shown over 100,000+ devices connected to their network, which they were unaware of over 20% of the devices. They saw many connected medical devices on the wrong network segment and thousands of devices that were at risk. Many of the devices were subject to exploits and device takeover. Unmanageable devices accounted for 35% of total devices, but for 70% of at risk devices. All of this information was categorized and operationalized by integrating into ServiceNow™ and populating their support ticket with enough detailed information for the operator to troubleshoot and remediate the issue.

> "Within 24 hours of deployment, Securolytics® profiled hundreds of thousands of devices, immediately gave us at risk devices and actionable remediation steps. Our security team has peace of mind with continuous IoT device monitoring in place and incident detection alerting with ServiceNow™."

securolytics®