Ivanti Neurons for Healthcare:

Improve asset visibility and security risk mitigation for medical devices

Millions of healthcare IT and medical IoT devices are used to care for patients and streamline clinical workflows in healthcare organizations, but their inherent vulnerabilities to malware and cyber-attacks place hospitals and patients at risk. Connected medical devices represent a huge challenge for healthcare IT, biomedical and security organizations. They can't be disconnected because of their critical roles in patient care and IT network infrastructures, and standard IT solutions can't secure them. This leaves hospitals exposed and jeopardizes patient safety, data confidentiality, and service availability.

- **50%** of hospitals don't conform to NIST guidelines.
- **65%** of hospitals have low confidence in asset visibility.
- **40%** of all connected medical devices run an unsupported OS.
- **300%** rise in healthcare cyber-attacks since the beginning of 2020.

Ivanti Neurons for Healthcare improves asset visibility and security risk mitigation for medical devices. The solution discovers and intelligently profiles medical devices and Internet of Medical Things (IoMT), assessing security risks, reporting threats, and reconciling device information across multiple data sources. Know more about the various healthcare-specific devices across your facilities, including device classification and usage information, with the details to reduce security risk or to attend to anomalies. Collect and reconcile vendor data, creating a single source of truth for all your medical devices.

Identify medical devices, IoT, and OT systems

The challenge of connected medical devices is not well understood by IT, biomedical, and security teams at hospitals and healthcare organizations due to extremely limited visibility. It's critical to understand the complete environment. Active network scanning

can disrupt medical device operation, so you must use passive discovery. Traditional tools won't discover the vast majority of connected medical devices, or may indicate falsely that the device is a Windows workstation. Most connected medical devices do not advertise their information, and detecting them over the network requires careful analysis of traffic at the application layer. With Ivanti Neurons for Healthcare you can easily discover which IT and medical devices exist, classify them accurately, understand their clinical context, and identify their networking needs to understand how exposed they are to external and internal threats.

Assess and prioritize risk

Once you have a better understanding of your connected medical devices — and have built an inventory of the devices, their context and network behavior — you can use this inventory to assess the security risks affecting each device and their impact on the organization. With cross-organizational and device-level risk assessment, anomaly detection, real-time alerts and clinical insights, Ivanti Neurons for Healthcare prioritizes action plans based on risk impact and criticality. The advantage of a structured process for discovery and risk assessment is that you can rank devices according to the risks they represent.

Secure faster and cover all threat vectors

Ivanti Neurons for Healthcare identifies device vulnerabilities and network-related risks; assigns each device a risk index for patient safety, privacy, and service disruption; and provides recommendations for remediation. Your organization can define an acceptable level of risk, and the security team can focus on protecting devices with risk scores beyond the acceptable level and apply the appropriate security measures to devices with different risk scores. From vendor access to cloud access, forensics, and virtual segmentation, Ivanti Neurons for Healthcare automates risk reduction by offering the optimal remediation path. Starting from the most critical risks that have the highest impact on your organization, you can arrive at a quick and sustainable security posture.

Reduce risks, prevent threats, and improve compliance

Ivanti Neurons for Healthcare gives biomedical and clinical engineers the insights and solutions they need to take total control of their assets and sync with their IT Security counterparts with automated discovery, inventory, ePHI and location tracking, asset classification, utilization and device capacity dashboards, and risk assessments tailored to healthcare facilities' unique workflows and architectures. Healthcare organizations can leverage clinically contextualized, real-time insights to identify and manage security risks, optimize device performance, and achieve the quick and lasting wins needed to ensure patient safety and smooth operations.

Key capabilities

Automated discovery and asset management

Real-time medical device discovery finds, inventories, and classifies every device, tracks locations, and provides:

- Comprehensive data on device type, vendor, OS, department, serial number and more.
- Data on devices that receive and send ePHI, plus ongoing risk assessments, recall tracking and alerts.
- Seamless integration with Ivanti Asset Management and other third-party asset management solutions to manage medical assets efficiently and optimize their performance.

Resource planning and emergency preparedness

Operational insights and ongoing visibility into device utilization patterns help you make quick, informed decisions with:

- Drilldowns into usage, medical impact and criticality for individual devices and for device types by ward and site.
- Alerts on device capacity and real-time location (by ward, department, off-site locations).
- Insights on when devices can be scheduled for downtime and maintenance without disrupting clinical services.
- Troubleshooting to understand what went wrong and how to fix it.

ePHI tracking and device recall alerts

Continuous tracking of devices with ePHI and device recall alerts enables seamless alignment between biomedical and clinical engineering teams with their IT Security counterparts to:

- Pinpoint devices that might be vulnerable to cyberattacks.
- Immediately identify devices with compromised functionality or security and receive step-by-step mitigation plans.
- Ensure compliance with ePHI communications tracking and device-level security.

Procurement and lifecycle management

Access to digitized, searchable MDS2 library, plus in-house threat intelligence combined with the power of AI promotes cross-team alignment with IT Security and cost-savings on device procurement with:

- Easy access to MDS2 forms, including for devices not yet in your inventory to ensure devices adhere to organizational security policies pre-purchase.
- The ability to easily apply MDS2 data to device-level security policies to ensure necessary maintenance and support services and optimal (and prolonged) device functionality.
- Vulnerability identification that saves teams the time they'd take to communicate directly with device vendors.
- Real-time data extracted from external sources to ensure device functionality, security and compliance with information from the FDA, JCAHO and HIPAA.
- Device-performance benchmarking that enables teams to build patching and maintenance programs to ensure continued clinical workflow and medical services.

Vendor access management

Control over vendor and third-party access to devices on the hospital's IT networks ensures:

- Visibility into which vendors are connecting, when, and why.
- Vendors and other third parties only connect to devices for necessary maintenance and support services.
- Compliance with passive scanning of regulatory rules and real-time alerts on changes and violations.

Modular, role-based dashboards

Configurable and modular dashboards display varieties of data to give teams the perspective they need with the right information at the right time:

- Inventory and insights on device operations, vulnerabilities and recalls.
- Deep drilldowns into communications involving ePHI.
- Multi-site views for network hospitals.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

Copyright © 2021, Ivanti. All rights reserved. IVI-2500 04/21 MF/EG/DH

ivanti Neurons

ivanti.com/neurons
1 800 982 2130
sales@ivanti.com