Ivanti Neurons for Healthcare Cybersecurity Platform

Secure IoMT Devices. Faster.

Medical Device Safety Is Patient Safety

Patient care has seen incredible improvements thanks to the data, insight and timeliness provided by connected medical devices. However, as the footprint of these devices in hospitals expands, so do the number of threats, vulnerabilities, and attacker pathways towards them. The security of the devices connected to patients are now an essential part of their overall well-being, care, and health.

Ivanti enables hospitals and healthcare facilities to get unparalleled visibility into their IoMT, OT and connected medical devices, reduce their vulnerability and risk, and immediately respond to ransomware, breaches and other threats aimed at them. Don't just identify connected devices using asset management– secure them to ensure that they are an integral part of protecting patient safety, care, and data.

Healthcare IoMT Security by the Numbers
Do You Feel Confident in Your Hospital's Ability to Manage Connected Device Risk?

$9M

Average cost of a healthcare breach - highest of any industry

500%

healthcare ransomware increase since the pandemic's start

70%

of medical devices have critical vulnerabilities that would impact patient safety if exploited

The Benefits of the Ivanti Neurons for Healthcare Platform

- Go beyond inventory - Find and remediate the most critical healthcare IoMT risks in under 30 days
- Confidently micro- segment connected devices with no impact on patient outcomes or functionality
- Automated, actionable, and plain-English mitigation plans that prevent the widest variety of threats
- Extend your team with a Technical Account Manager to affordably accelerate IoMT risk reduction
- Identify and respond to ransomware and other attacks so they don't affect IoMT and medical devices
- Get the visibility to integrate IoMT, OT and connected medical devices within your IT security tools
- Ensure IoMT security alignment between BioMed, security, network, facilities, and executive teams
- Stay up to date with IoMT security compliance for HIPAA, NHS DSPT, and other international healthcare regulations
- Use device data to prioritize remediation based on potential critical risk to patients
- Healthcare is our only business – leverage our deep insight on medical device security and hospital best practices

Features

Ensure patient safety, data confidentiality and service continuity on IoMT devices

Network Segmentation Validation Engine for IoMT

Ivanti's medical-first network segmentation validation engine gives hospitals a virtual environment to test potential segmentation before execution, so that effective IoMT security can be confidently implemented and device lifecycles safely lengthened without disruptions or additional risk.

Extend Your IT Team with a Technical Account Manager

Pair Ivanti technology with an affordable, long-term Technical Account Manager (TAM). TAMs provide guidance and technical expertise to healthcare teams that might otherwise be understaffed or over stressed.

Attack Detection and Response for Healthcare IoMT

Ivanti's IoMT Attack Detection and Response module empowers hospitals to immediately identify and safely quarantine connected devices exhibiting malicious or suspicious activity. Ivanti IoMT forensics then allow for thorough remediation and rapid recovery measures to be carried out when the device is not in use.

Track and Analyze Organizational IoMT Risk Data in the Portal

The Ivanti portal provides comprehensive device and risk data in drill-down charts and dashboards, with step- by-step instructions on how to effectively remediate all vulnerabilities and attacks.

Updated Compliance with Global IoMT and Healthcare Security Standards

Built according to NIST Cybersecurity Framework standards, Ivanti provides continuous monitoring of current compliance with a variety of international norms such as HIPAA, alerts about anomalous activity and device risks, and generates full reporting for streamlining audits.

Align IT Security, Network, BioMed, facilities and Executive Teams around Healthcare IoMT Security

Dozens of implementations covering hundreds of thousands of devices at hospitals all around the world has allowed Ivanti to build an effective library of best practices to ensure alignment between the varied teams that need to make healthcare IoMT security effective.

Utilize Detailed Device Data to Optimize Resource Allocation

Ivanti collects comprehensive information about medical device usage to help biomedical engineers and hospital staff make informed decisions about new device purchases, carry out capacity planning and respond quickly to emergencies.

Vendor and Cloud Access Management

Gain visibility into who is connecting to your devices and why. Ensure that vendors and other external colleagues only connect to medical devices for necessary tasks, with full alerting and reporting available to corroborate security and compliance.

Assess, Score and Prioritize Device Risk Based on Potential Patient Impacts

The Ivant platform leverages machine learning to model the potential impact of dozens of device risk factors, generate mitigation outcomes that keep devices secure, and create a risk score that helps healthcare providers act quickly to remediate the most dangerous threats.

Integrate IoMT Visibility and Data into IT Security

Ivanti acts as the “brain” of your IoMT device infrastructure, collecting data on risks, vulnerabilities, and attacks. The platform then leverages integrations with firewalls, network access control (NAC), security information and event management (SIEM), and many other IT security technologies that act as the “muscle” to enforce the remediation policies that ivanti suggests for IoMT devices.

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 96 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

ivanti

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