ivanti
Ivanti Neurons for Healthcare

AT&T Business

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 Neurons for Healthcare enables hospitals and healthcare facilities to get unparalleled visibility into their IoT, OT, and connected medical devices, reduce their vulnerability and risk, and respond to ransomware, breaches, and other threats aimed at them. Don't just identify connected devices using asset management – secure them as an integral part of protecting patient safety, care, and data.

Benefits

- **Go beyond inventory** – Find and remediate the most critical healthcare IoT risks in under 30 days
- **Automated, actionable,** and plain-English mitigation plans that prevent the widest variety of threats
- **Use device data** to prioritize remediation based on potential critical risk to patients
- **Identify and respond to ransomware** and other attacks so they don't affect IoT and medical devices
- **Get the visibility to integrate** IoT, OT, and connected medical devices within your IT security tools
- **Maintain IoT security alignment** between BioMed, security, network, facilities, and executive teams
- **Stay up to date with IoT security compliance** for HIPAA, NHS DSPT, and other international healthcare regulations

Features - Ensure patient safety, data confidentiality, and service continuity on IoT devices.

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

Attack detection and response for healthcare IoT - Ivanti's IoT Attack Detection and Response module empowers hospitals to immediately identify and safely quarantine connected devices exhibiting malicious or suspicious activity. Ivanti IoT 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 IoT risk data in the portal - The 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 IoT 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.

Vendor and Cloud access management - Gain visibility into who is connecting to your devices and why. Control how vendors and other external colleagues connect to medical devices for necessary tasks, with full alerting and reporting available to corroborate security and compliance.

Align IT security, network, BIOMed, facilities, and executive teams around healthcare IoT security - Dozens of implementations covering hundreds of thousands of devices at hospitals around the world allows Ivanti to build an effective library of best practices to maintain alignment between varied teams that need to make healthcare IoT security effective.

Assess, score, and prioritize device risk based on potential patient impacts - The Ivanti platform utilizes 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.

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.

Integrate IoT visibility and data into IT security - Ivanti acts as the "brain" of your IoT device infrastructure, collecting data on risks, vulnerabilities, and attacks. The platform integrates 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 IoT devices.

Why AT&T

AT&T's cybersecurity experts offer unique solutions to mitigate risk, secure the network and prevent costly hacks and breaches. We empower healthcare organizations to stay compliant and proactively manage every connection on their own terms with real-time IoT attack detection and response and rapid risk reduction tools, so that they can focus on healthcare's top priority: delivering quality patient care. Watch an on-demand demo presentation from AT&T partner Ivanti to learn more about how to secure healthcare IoT effectively against the rising tide of ransomware and breaches targeting hospitals.

For More Information, please visit www.ivanti.com/lp/esm/assets/s1/ivanti-neurons-for-healthcare.

ivanti

Ivanti Neurons for Healthcare

AT&T Business

Important information

General: Each Ivanti solution as described in this product brief (the "Solution") is available only to hospitals and health clinics that are eligible Business or government Customers with a qualified AT&T agreement ("Qualified Agreement") and a Foundation Account Number (FAN).
The Solution is subject to (a) the terms and conditions found https://www.ivanti.com/company/legal/eula (Additional Product Terms); (b) the Qualified Agreement; and (c) applicable Sales Information. Please see the service guides for additional information on service descriptions and pricing at http:// serviceguidenew.att.com. For government Customers, any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any material conflict between the Qualified Agreement and the Additional Product Terms.

A minimum of 25Solution subscriptions are required for an initial Ivanti Neurons for Healthcare purchase. The Solution's functionality is limited to certain operating systems. A list of supported operating systems can be obtained by contacting an AT&T Business Account Executive.. All amounts paid for the Solution are non-refundable. Billing begins as of Effective Date of applicable order.

The Solution administrative interface is accessed via a Web portal and requires a PC or laptop with internet connection. The Solution may be used as a tool to configure and customize certain settings and features and perform software updates only for compatible devices. Improper or incomplete configuration and/or downloads performed by Customer may result in service interruptions and/or device failures.

Customer must accept the Additional Product Terms as the party liable for each authorized user (End User) and agrees in such case that the End User will comply with the obligations under the Additional Product Terms, including but not limited to the limitations of use in certain countries. Customer is responsible for providing each End User of an enabled mobile device with a copy of the Additional Product Terms. With the use of the Solution by residents of and in countries other than the U.S., Customer agrees to comply with the additional terms and conditions of use located in the Country Specific Provisions portion of the Service Guides located at http:// serviceguidenew.att.com.

Data privacy: Customer Personal Data: Customer Personal Data may be transferred to or be accessible by (i) AT&T personnel around the world; (ii) third parties who act on behalf of AT&T or AT&T supplier's behalf as subcontractors; and (iii) third parties (such as courts, law enforcement, or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data and End User personal data accessible when Customer has the legal authority to do so and for which it has obtained any necessary consents from its end users and will camouflage or securely encrypt such data as needed in a manner compatible with the Solution. The term, Customer Personal Data, includes, without limitation, name, phone number, email address, location information, or any other information that identifies or could reasonably be used to identify or link to Customer or its end users. Customer is responsible for providing its end users with clear notice of AT&T and the Customer's collection and use of Customer Personal Data obtained via the Solution, including, without limitation, end user device location information, and for obtaining end user consent to that collection and use. Customer may satisfy its notification requirements as to AT&T by advising its end users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for end user review the Product Brief or other sales information that describes the Solution and to AT&T Privacy Policy at http://www.att.com/gen/privacy-policy?pid=2506. Customer is responsible for notifying end users that the Solution provides unified endpoint management (UEM) capabilities and allows Customer to have full visibility and control of end users' devices, as well as content on them.

Miscellaneous. Solution software warranty and liability rights are contained in the Additional Product Terms between Ivanti and Customer. As between AT&T and the Customer, the Solution is provided "AS IS" with all faults and without warranty of any kind. AT&T HAS NO DEFENSE, SETTLEMENT, INDEMNIFICATION, OR OTHER OBLIGATION OR LIABILITY ARISING FROM THE ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY BASED ON THE SOLUTION.

AT&T reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause AT&T reserves the right to conduct work at a remote location or use, in AT&T sole discretion, employees, Contractors, or suppliers located outside the United States to perform work in connection with or in support of the Solution. Exclusive Remedy: Customer's sole and exclusive remedy for any damages, losses, claims, costs, and expenses arising out of or relating to use of the Solution will be termination of service.