Palo Alto Networks Announces Medical IoT Security to Protect Connected Devices Critical to Patient Care

December 5, 2022

SANTA CLARA, Calif., Dec. 5, 2022 /PRNewswire/ -- As healthcare providers use digital devices such as diagnostic and monitoring systems, ambulance equipment, and surgical robots to improve patient care, the security of those devices is as important as their primary function. Today, Palo Alto Networks (NASDAQ: PANW) announced Medical IoT Security — the most comprehensive Zero Trust security solution for medical devices — enabling healthcare organizations to deploy and manage new connected technologies quickly and securely. Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust by continuously verifying every user and device.

"The proliferation of connected medical devices in the healthcare industry brings a wealth of benefits, but these devices are often not well secured. For example, according to Unit 42, an alarming 75% of smart infusion pumps examined on the networks of hospitals and healthcare organizations had known security gaps," said Anand Oswal, senior vice president of products, network security at Palo Alto Networks. "This makes security devices an attractive target for cyberattackers, potentially exposing patient data and ultimately putting patients at risk."

While a Zero Trust approach is critical to help protect medical devices against today's innovative cyberthreats, it can be hard to implement in practice. Through automated device discovery, contextual segmentation, least privilege policy recommendations and one-click enforcement of policies, Palo Alto Networks Medical IoT Security delivers a Zero Trust approach in a seamless, simplified manner. Medical IoT Security also provides best-in-class threat protection through seamless integration with Palo Alto Networks cloud-delivered security services, such as Advanced Threat Prevention and Advanced URL Filtering.

The new Palo Alto Networks Medical IoT Security uses machine learning (ML) to enable healthcare organizations to:

- **Create device rules with automated security responses:** Easily create rules that monitor devices for behavioral anomalies and automatically trigger appropriate responses. For example, if a medical device that typically only sends small amounts of data unexpectedly begins to use a lot of bandwidth, the device can be cut off from the internet and security teams can be alerted.
- **Automate Zero Trust policy recommendations and enforcement:** Enforce recommended least-privileged access policies for medical devices with one click using Palo Alto Networks Next-Generation Firewalls or supported network enforcement technologies. This eliminates error-prone and time-consuming manual policy creation and scales easily across a set of devices with the same profile.
- **Understand device vulnerabilities and risk posture:** Access each medical device's Software Bill of Materials (SBOM) and map them to Common Vulnerability Exposures (CVEs). This mapping helps identify the software libraries used on medical devices and any associated vulnerabilities. Get immediate insights into the risk posture of each device, including end-of-life status, recall notification, default password alert and unauthorized external website communication.
- **Improve compliance:** Easily understand medical device vulnerabilities, patch status and security settings, and then get recommendations to bring devices into compliance with rules and guidelines, such as the Health Insurance Portability Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and similar laws and regulations.
- **Verify network segmentation:** Visualize the entire map of connected devices and ensure each device is placed in its designated network segment. Proper network segmentation can ensure a device only communicates with authorized systems.
- **Simplify operations:** Two distinct dashboards allow IT and biomedical engineering teams to each see the information critical to their roles. Integration with existing healthcare information management systems, like AIMS and Epic Systems, helps automate workflows.

Healthcare organizations are using Palo Alto Networks products to secure the devices that deliver cutting-edge care to millions of patients all over the world.

"Establishing and maintaining acute situational awareness of the Internet of Medical Things (IoMT) environment is paramount to establishing an effective enterprise cybersecurity program. The ability to accurately detect, identify and respond to cyber threats is critical to ensuring minimal operational impact to clinical operations during a cyber event," said Tony Lakin, CISO, Moffitt Cancer Center. "Palo Alto Networks IoT capability seamlessly integrates with our continuous monitoring processes and threat-hunting operations. The platform consistently provides my teams with actionable information to allow them to proactively manage the threat surface of our medical device portfolio."

"With thousands of devices to manage, healthcare environments are extremely complex and require intelligent security solutions capable of doing more. Palo Alto Networks understands this requirement and is leveraging machine learning (ML) for Medical IoT security. Adding intelligence will enable providers to improve operational efficiency, which will enhance patient and practitioner experience and alleviate the burden of an ongoing IT skills shortage," said Bob Laliberte, principal analyst, ESG.

"Healthcare providers continue to be high-value targets for attackers. This reality, combined with the diversity of medical IoT devices and their inherent vulnerabilities, points to a real need for device security that is purpose-built for healthcare use cases. The ability to defend against threats targeting critical care devices while maintaining operational availability and strengthening the alignment of device governance responsibilities between IT and Biomed engineering teams is quickly becoming a necessity for the protection of patient data and lives," said Ed Lee, research director, IoT and Intelligent Edge Security, IDC.

More Information

- Learn more about Medical IoT Security here.
- Read the Medical IoT Security announcement blog here.
- Register to attend the Palo Alto Networks Ignite Conference on December 12th - 15th, 2022, here.
- Follow Palo Alto Networks on Twitter, LinkedIn, Facebook and Instagram.

Availability

Medical IoT Security will be available in January 2023.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021), Comparably Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-announces-medical-iot-security-to-protect-connected-devices-critical-to-patient-care-301694295.html

SOURCE Palo Alto Networks, Inc.

jweinberg@paloaltonetworks.com