Stay on Top of Medical Device Vulnerabilities with Complete IoMT and IoT Device Visibility and Vulnerability Assessment

Medical Devices Are Among the Most Vulnerable IoTs

While IoMTs enhance how healthcare delivery organizations (HDOs) provide patient service and care, they were not designed with security in mind. IoMTs have a longer functional life than their cyber life and often run outdated or even end-of-life operating systems, making them easy targets for threat actors. Security weaknesses, such as an unsupported operating system, make IoMTs particularly susceptible to attacks—our Unit 42 IoT Threat Report found that 41% of all cyberattacks exploit device vulnerabilities.

These are concerning statistics since unmanaged IoMT and IoT devices are connected to hospital net-

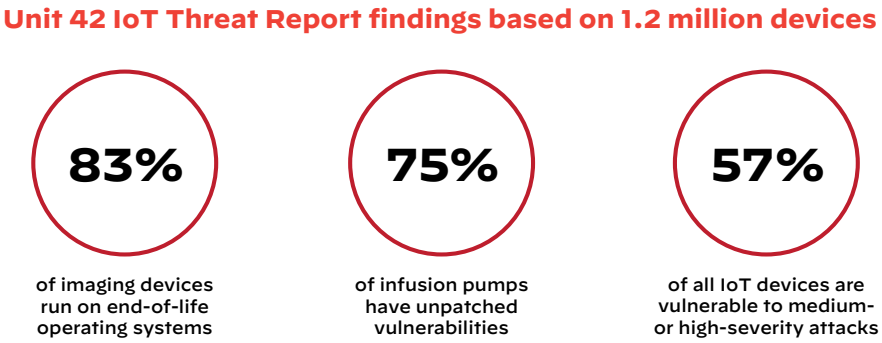

Figure 1: Device vulnerabilities in IoMTs

works with unrestricted access. An exploited vulnerability in IoMTs can compromise a patient's personal data and disrupt critical patient care.

Without IoMT Visibility, Vulnerability Management Is Incomplete

HDOs use Vulnerability Management (VM) solutions to stay on top of security weaknesses. These solutions help automate the process of identifying, assessing, prioritizing, and remediating vulnerabilities before they are maliciously exploited. VM tools initiate scans to identify security weaknesses in devices and generate scan reports which enable IT and security teams to evaluate the severity of the vulnerability and prioritize remediation actions.

However, IoMT device vulnerabilities aren't identified by VM solutions because:

- VMs only scan the "discoverable" (managed) devices for Common Vulnerabilities and Exposures (CVEs), leaving vulnerabilities in unknown IoMT and IoT devices undiscovered.
- An invasive or ill-timed IoMT vulnerability scan when the IoMTs are actively in use can disrupt patient care.
- Not all IoMTs can tolerate the same vulnerability scan templates and require scans to be adjusted based on the type and tolerance level of the device.

The exclusion of IoMT devices from the scope of VM solutions leaves a significant blind spot in an HDO's security risk posture analysis. Not only do unmanaged IoMT devices constitute a growing portion of all connected devices on hospital networks (currently estimated at 30%), but they are also the weakest link in the network's security with their inherent vulnerabilities and weak in-built security.

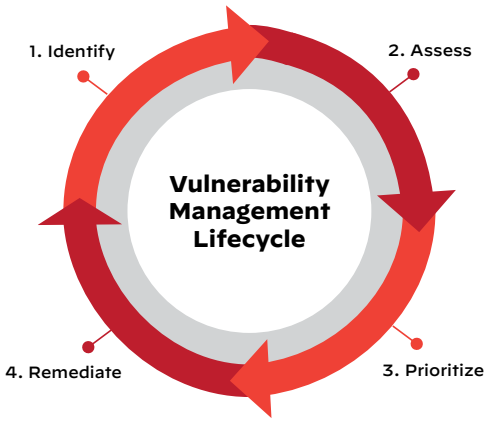

Figure 2: The Vulnerability Management process

Palo Alto Networks IoT Security Provides

Comprehensive IoMT Device Vulnerability Assessment

IoMT and IoT devices present a unique challenge to network security professionals because of their

Table 1: How IoT Security Enhances Vulnerability Management	
Vulnerability Management without IoT Security	**Vulnerability Management with IoT Security**
• **Lack of visibility into unmanaged IoMTs**, leaving 30% of your network inaccessible to Vulnerability Management solutions	• Gain **visibility into all managed and unmanaged IoT** endpoints and ensure comprehensive coverage for vulnerability assessment
• **Incomplete assessment of risk exposure** due to lack of visibility and sufficient device context to identify all device vulnerabilities	• Get a **holistic IoMT and IoT device risk score**, including passively and actively discovered vulnerability data and other risk indicators
• **Patient care due to delayed remediation** since IoT devices remain undiscovered and are hard to patch	• Allow "unpatchable" IoMT devices to safely continue operating through **Zero Trust least-privileged access** (also known as virtual patching)
• **Failure to assess** device security and regulatory **compliance gaps** (e.g., HIPAA, The EU Cybersecurity Act, etc.) due to incomplete vulnerability reports	• **Narrow compliance gaps** by bringing unmanaged IoMT and IoT device visibility and vulnerability assessment into your vulnerability reporting

undiscoverability and undetected risk. So, the approach to identifying and assessing their vulnerabilities needs to go beyond simply associating known vulnerabilities to discoverable devices. This is where IoT Security's comprehensive vulnerability and device risk assessment helps.

IoT Security passively collects data on IoT and IoMT device vulnerability and risk context from multiple sources to generate a comprehensive device risk score:

Table 2: Device Risk Score		
Device Vulnerability Data	**+**	**Device Risk Context**
• CVEs • Weak or default passwords • Unsecure protocol usage • Incorrect device usage • End-of-life OS/Apps/Devices • Obsolete protocols • Misconfiguration of IoT devices • FDA recalls		• Third-party/Manufacturers logins attempts • Decommissioned medical devices connected to the network • Deviance from manufacturer specifications • Risk indicators captured in MDS2 documents • Devices storing or transmitting ePHI data • Access to malicious domains • Unusual software running • Security policy violations

Built-in Third-Party Integrations for IoMT Vulnerability Management

Palo Alto Networks IoT Security offers built-in integrations with leading Vulnerability Management solutions to provide a comprehensive IoMT device visibility and vulnerability assessment. IoT Security-powered Vulnerability Management provides:

- Deep IoT and IoMT device visibility and context through passively collected device data
- In addition to passive monitoring, the ability to initiate active scans of a selected device from the IoT Security portal to get a comprehensive view of vulnerabilities
- Ability to ingest vulnerability scan reports from the scanner and update the device risk score within the IoT Security dashboard

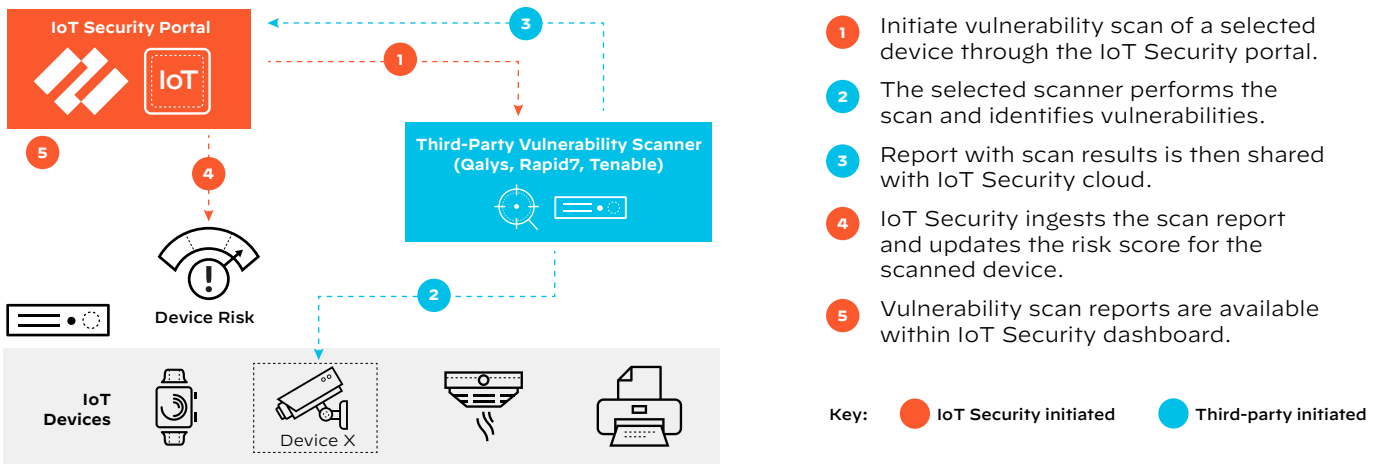

Figure 3: IoT Security—Vulnerability Management integration workflow

Refer to our datasheet on playbook-driven integrations for more on the built-in integrations we support.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com