SOLUTION BRIEF

Armis and Google Cloud – IoT Security for Healthcare

An integrated IoT, IoMT, OT and IT device security and analysis solution

Connected devices are growing at an unprecedented rate within healthcare delivery organizations (HDOs). From MRI and CT scanners, to IoT surveillance systems and patient engagement platforms, the resulting attack surface is one that many HDOs don't have the tools or resources to manage. Many of these devices lack inherent security controls, can't easily receive software updates, and they can't be seen or managed by traditional security products. The result is repeated and sustained attacks often ending in headline grabbing breaches.

Protecting healthcare organizations with Armis

Armis provides HDOs with IoT and medical device (IoMT) visibility, contextual intelligence, vulnerability prioritization, real time threat analysis and risk assessment. It continuously collects and analyzes asset data through network activity monitoring and levereges hundreds of meaningful integrations with the existing IT and security tech stack.

Delivered as a SaaS-based service, Armis is quick to install and provide value. **The Armis Collective Asset Intelligence Engine** which monitors and analyzes the profiles of over 3 billion devices, enables it to quickly fingerprint unknown devices, enrich asset data and detect anomalies in configurations and behaviors. Integrations with CMMS/ CMDB, security, networking, and analytics platforms help provide organizations with a consistent and consolidated view of their device estate, pinpoint business critical devices that are vulnerable and at risk, and streamlines security automation and threat mitigation.

Key Benefits

- Armis is the only IoT security solution available from Google Marketplace.
- Unified Asset Intelligence puts IoT, IoMT, OT, and IT device identification and classification all in one place.
- Completely passive and agentless technology, won't impact your network or the availability of critical patient care devices.
- Dynamic vulnerability and risk analysis, including CVE, CVSS, FDA Recall, and manufacturer advisories, to help control and secure your attack surface.
- Continuous real-time threat detection and alerting that helps security teams quickly respond and mitigate threats.
- Frictionless Deployment and Integration that delivers immediate time-to-value.

Integration with Google Cloud services

Armis is available directly from the Google Marketplace enabling Google Cloud customers to quickly procure and deploy the Armis solution. Armis device, threat and utilization data can then be ingested by first party GCP tools such as Chronicle, Big Query and Looker for further analytics, visualization and machine learning to meet the specific reporting, forecasting or storage needs of any organization.

The Armis platform

Armis provides unified asset visibility and security in a single platform purpose-built for this new threat landscape of connected devices. The platform includes detailed device profiles and risk assessments helping resource strapped security, biomedical IT and OT teams to better understand and reduce your attack surface. The platform also improves threat detection and response by continuously analyzing the behavior of every device, dynamically updating risk scores in real-time, and triggering policy-based actions that can mitigate risks and attacks proactively.

Immediate time-to-value

Getting started with the Armis platform is fast and easy. Available from the Google Marketplace, it's agentless, completely passive, and requires no additional hardware. With just a few clicks, you can connect your existing IT/security tools with out-of-the box integrations to start seeing value immediately. You can also connect the platform to a virtual or physical SPAN/TAP to extract rich and contextual device details and behavioral analysis from network traffic metadata.

The extensive Armis Collective Asset Intelligence Engine eliminates the need for any learning period or baselining. It uses the collective intelligence of over two billion devices, their characteristics, vulnerabilities, and behaviors to identify and classify any device, evaluate risks, and stop threats accurately, quickly, and automatically.

Unified asset management

The Armis platform discovers and classifies every managed and unmanaged device in your environment including, but not limited to medical devices. It works with your existing IT/security tools and network infrastructure to identify every device, including off-network devices that use Wi-Fi, Bluetooth, and other IoT protocols. This comprehensive device inventory includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications, connections made over time, and individual risk assessment scores. As Armis collects information from across a wide number of industries, healthcare organizations will also be able to match other systems including operational technology (OT) and IT including critical building management systems and traditional endpoints. This enables a comprehensive view across all IoT, IoMT, OT and IT potential attack vectors.

Dynamic risk assessment

Each device profile in the Armis platform includes individual risk assessments based on factors like known hardware and software vulnerabilities, device and vendor reputation, and known attack vectors. The platform continuously compares the device profiles in your inventory with the known device characteristics and behavior patterns in the Armis Collective Asset Intelligence Engine. As new information is learned about devices from organizations around the globe, it updates device profiles and risk assessments in real-time, providing you with critical, actionable insights that help you better understand and proactively reduce your organization's attack surface.

Continuous threat detection and response

The Armis platform continuously analyzes device activity for abnormal behavior. Whether a device is misconfigured or is the target of an attack, the platform can alert your security team and trigger automated actions to help stop an attack. And, through integration with your network switches, wireless LAN controllers, and security enforcement points like firewalls and NAC, Armis can directly restrict access or quarantine suspicious or malicious devices. This automation provides peace of mind that an attack on any device—managed or unmanaged—can be stopped, even if your security team is busy with other priorities.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

1.888.452.4011 | **armis.com**

20220921-1

ARMIS