ARMIS®

SOLUTION BRIEF

ARMIS + GIGAMON

Unmanaged and IoT devices are vulnerable. Protect them with Gigamon and Armis.

Agent-based security approaches may be effective in protecting many of the assets on your network, but these approaches don't work for unmanaged, IoT, OT, and medical devices. These devices are inherently more vulnerable because they often lack robust security, they are difficult to patch, and they can't host security agents. As a result, they have become a favorite attack target for cybercriminals and pose a significant and growing security risk as these devices proliferate within the enterprise.

Armis® and Gigamon® work together to provide full visibility into all traffic across hybrid networks. With Gigamon, organizations gain pervasive hybrid cloud visibility, equipping the Armis platform with access to relevant traffic to assure stronger security, compliance, and business continuity.

The Armis & Gigamon Joint Solution

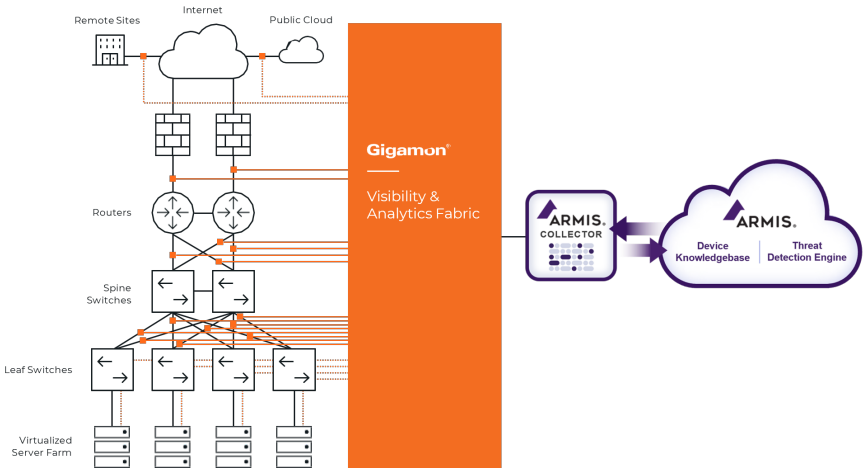
Armis provides unified asset visibility and security in a single platform purpose-built for this new threat landscape of connected devices. Our platform gives you the most comprehensive inventory of assets you've ever seen. It includes detailed device profiles and risk assessments so you can better understand and reduce your attack surface. It 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.

The Gigamon Visibility and Analytics Fabric™ provides full network traffic visibility and filters, deduplicates, decrypts, and delivers relevant traffic to the Armis platform. Gigamon provides full visibility into all the traffic on hybrid networks and provides the Armis platform with access to the relevant traffic to ensure stronger security, compliance, and business continuity.

JOINT SOLUTION BENEFITS

- Quick and easy deployment for Immediate time-to-value
- Gain visibility of unmanaged, IoT, OT, medical devices, and more
- Reduce business and compliance risk with continuous, real-time device vulnerability and behavioral risk assessments
- Align NetOps and SecOps teams using comprehensive device and network data
- Automatically detect and respond to suspicious or malicious device behavior

Together, this joint solution reduces business risk and increases security by providing real-time and continuous protection for managed, unmanaged, and IoT devices.



Immediate Time-to-Value

Getting started with the Armis platform is fast and easy. It's agentless, completely passive, and requires no additional hardware. With just a few clicks, you can connect your existing IT/security tools with our out-of-the-box integrations to start seeing value immediately. And when you connect with a Gigamon virtual TAP, the platform can extract rich and contextual device details and behavioral analysis from network traffic metadata for even greater visibility.

And only the extensive Armis Device Knowledgebase—the world's largest body of knowledge about devices and their behavior—eliminates the need for any learning period or baselining. It uses the collective intelligence of over one 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 any environment—enterprise, manufacturing, healthcare, retail, and more. 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. And whether you manage assets in the Armis console or integrate the platform's asset inventory with your existing IT asset management platform, the Armis platform enables having a single source for complete, comprehensive details about every device.

Joint Solution Use Cases

Asset inventory

- What devices are on my network, are they authorized and secure?
- How do I track and locate devices with unsupported operating systems or manufacturing/FDA recalls?

Compliance

- How do I ensure devices aren't going to be compromised by more vulnerable network devices?
- What devices are on the VLAN?

Device utilization

- What workload are my devices carrying and are they being fully or properly utilized?
- Analysis of utilization data for budgetary and planning purposes

Threat detection

- How do I find devices with vulnerabilities or that may have already been compromised?
- How do I identify devices exhibiting suspicious or malicious behaving?

Zero-trust micro-segmentation

- How do I proactively classify and securely segment devices on my network based on their roles or what they should be allowed to do?

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 Device Knowledgebase. As the Device Knowledgebase learns new information about devices, 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.

Meaningful Integrations

Inside the Armis console, you can choose from a curated selection of meaningful integrations that help get more value from your investments in existing IT and security tools. The Armis platform integrates quickly and easily with your security analytics and management products like SIEM, ticketing systems, asset databases, and more. These integrations enable your systems and incident responders with the rich, contextual information only the Armis platform can provide.

For more information, visit armis.com/gigamon.

The Armis Difference

Comprehensive
Discovers and classifies all devices in your environment, on or off your network.

Agentless
Nothing to install on devices, no configuration, no device disruption.

Passive
No impact on your organization's network. No device scanning.

Frictionless
Installs in minutes using the infrastructure you already have.

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.

armis.com
1.888.452.4011

20210917-1

ARMIS