Solution Brief

Securing Connected Care Innovation - The foundation for Zero Trust.

Modern care delivery is based upon the connection of a myriad of managed and unmanaged devices. Some are medical devices, such as MRI machines and infusion pumps, with obvious potential impact on patient treatment should they be disabled through a cyber attack, or misconfiguration. Some are less obvious but with at least equal the potential to impact care - elevator control systems, door badging systems, and vaccine storage thermostat controls. If these become unresponsive, they could quickly have a broad impact on a healthcare delivery organization's ability to move patients for surgery, securely access restricted areas of the hospital, or conduct routine vaccinations. Security teams struggle to understand where, what, and how vulnerable these devices are. The same Security teams also lack the ability to adequately and efficiently control and secure these devices.

Combining the Armis Asset Intelligence and Security Platform with Fortinet's Security Fabric creates a unified visibility, analysis, and enforcement ecosystem that delivers simpler, stronger, and more efficient security controls. **Armis and Fortinet offer a solution that lays the foundation for segmentation and Zero Trust.**

Key Capabilities

- Packet-level data ingestion at remote sites through FortiGate's API-enabled traffic collection functionality
- Integration with FortiGate's FortiManager platform to dynamically retrieve and update enforcement policies based on Armis' asset intelligence and threat detection
- Provide Armis' actionable device-, risk-, and threat-based information to FortiSIEM's unified analytics platform

Reduce Attack Surfaces with Armis + Fortinet

Armis and Fortinet provide unmatched asset visibility and security for the managed and unmanaged devices that are driving today's connected care innovation. Whether IoMT, IT, IoT, or OT, Armis utilizes existing management platforms and passive traffic monitoring to discover and identify every device in any environment—enterprise, medical, industrial, and more. Armis then analyzes device behavior and detects vulnerabilities to identify risks and threats.

Consolidating Armis asset intelligence platform's device visibility with Fortinet Security Fabric reduces your exposure to the risks of unmanaged and unknown devices and provides security teams with deeper device insights—all done without disrupting critical business and care delivery operations.

Discover Every Connected Device

Armis' integration with Fortinet's Fortigate appliances allows the collector to ingest network traffic for analysis and comparison to the Armis Collective Asset Intelligence Engine. Armis can leverage the existing Fortigate infrastructure to gather packet-level information about devices in remote locations, such as clinics and distributed hospitals, and is especially effective in environments with distributed internet connectivity and SD WAN.

Key Benefits

- Quickly discover managed and unmanaged devices across distributed care delivery and research environments
- Pro-actively and dynamically tighten security controls to meet compliance requirements based on Armis' asset intelligence, vulnerability, risk, and abnormal behavior detection
- Optimize FortiNet resources by focusing its security functionalities on critical or risky assets that impact patient care
- Detect and respond quickly to FDA recalls and common vulnerability and exposures (CVEs) with appropriate contextual information to focus IT and security teams on highest risk and exposure areas based on Armis' unique asset-based perspective

Armis utilizes FortiGate's API capabilities to regularly trigger the collection of packets on remote networks that will provide intelligence on connected devices and connections. This information is then retrieved into Armis' collectors for processing and is cross-correlated with other data sources as well as the Armis Collective Asset Intelligence Engine to provide contextual device intelligence. This enables Armis to differentiate risk on Windows devices being used for back office functionality vs those controlling medical devices.

Tighten Security Controls with Dynamic Policies

Armis also communicates with FortiManager's centralized manager to both receive policy information as well as modify policies in real time, based on configurable rules. As Armis discovers and identifies devices and their associated risks and behaviors in your environment, Armis can inform FortiManager to alter policies in response.

Source conditions can be dynamically added and changed in real time, allowing the administrator to automatically change traffic parameters. Use cases include applying additional logging or IDS and AV policies to high-risk devices, and even enforcing and blocking devices from accessing critical resources or the network altogether.

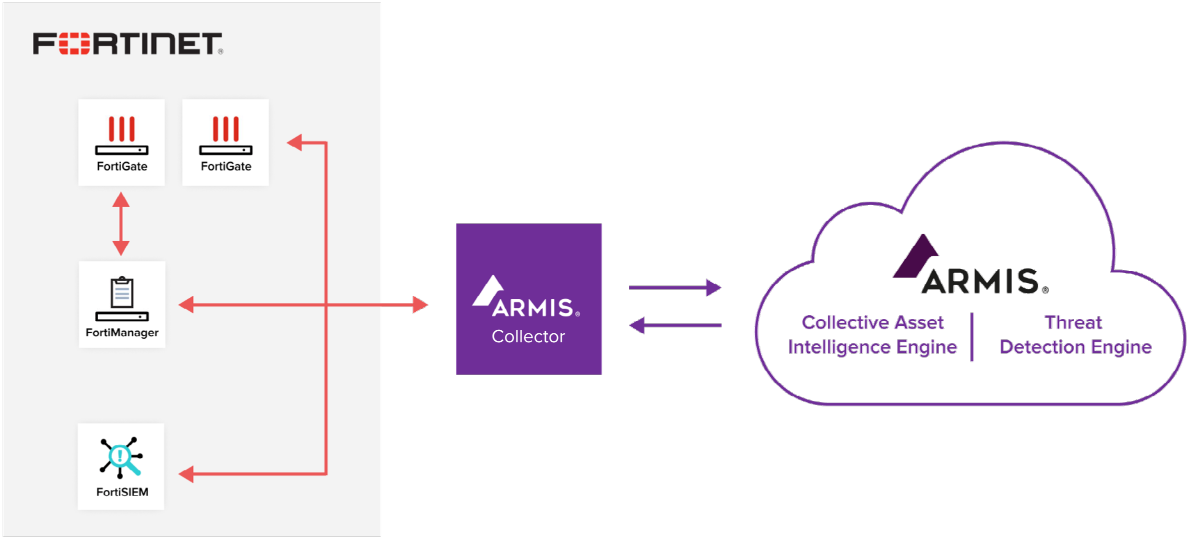
In addition, Armis provides visibility into traffic and protocol patterns in the context of device types. Administrators can utilize this knowledge to create more concise network policy rules and reduce the attack surface in critical networks, such as infusion pumps and other devices that cannot have security agents installed.

Detect and Respond Quickly to Threats and Vulnerabilities

Armis uses continuous device analysis to detect threats and vulnerabilities associated with managed, unmanaged and IoT, IoMT, IT and OT, devices (e.g., CVEs, unsupported operating systems, etc.). This analysis is based on information from the Armis Collective Asset Intelligence Engine which tracks more than 3 billion devices, and from threat intelligence feeds.

When Armis identifies a vulnerable or malicious device, it can automatically inform FortiSIEM's security information and event management system and provide contextual details to enhance its behavior analytics capabilities. Armis' visibility extends deep into all segments of the network, even where security devices or intrusion detection systems may not reach.

How it works



Integrations

Descriptions		Benefits
FortiGate	FortiGate Traffic Ingest	Identify devices and ingest traffic from remote locations without additional hardware, agents, or intrusive scanning
FortiManager	FortiManager Enforcement	Dynamically apply security controls on any device based on device type, vulnerabilities, risks, behaviors, and threats
FortiSIEM	FortiSIEM Event Feed	Provide automated, actionable information based on Armis' extensive behavioral database

The Armis Difference

Armis unites biomedical, security, and IT teams to deliver complete asset security:

Every Device - IoMT, IoT, OT AND IT

Medical devices are not the only attack surface that healthcare needs to protect. IoT such as security cameras, OT such as building management systems and IT are supporting networks where patients attach their own devices - we've even seen cars. Armis passively detects, identifies and assesses the risk of every device.

Knowledge

The Armis Collective Asset Intelligence Engine contains detailed accumulated anonymized knowledge of more than 3 billion devices from Armis customers. When Armis finds a device on your network, it can instantly compare configuration and traffic pattern information, removing a learning period and yielding fast time to value.

Industry Leader

Armis has been recognized as a leader in healthcare device security including the SPARK Matrix: Connected Medical Device Security, Q4 2022 report.

Armis is recognized as a top performer in the 2023 Best in KLAS awards for Healthcare IoT Security.

Agentless

Many IoT, IoMT and OT environments are unable to have agents installed, leaving them outside of the scope of traditional security tools. Armis utilizes passive monitoring. This enables detection of every device communicating on the network, removes the risk of crashing devices through active scanning and simplifies ongoing updating and maintenance.

About Armis

Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

1.888.452.4011 | armis.com

About Fortinet

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 615,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.