SOLUTION BRIEF

Fortinet and Armis Healthcare Security Solution

Securing Connected Care Innovation

Executive Summary

Modern care delivery is based on the connection of a myriad 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 cyberattack, or misconfiguration. Some are less obvious but with at least equal the potential to impact care, such as 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 the Fortinet 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.

Joint Solution

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 the 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.

Solution Components

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.

Fortinet FortiGate Next-Generation Firewalls (NGFWs) provide industry-leading threat protection and decryption at scale with a custom ASIC architecture. They deliver secure networking with integrated features such as SD-WAN, switching and

Solution Components

- Fortinet FortiGate Next-Generation Firewall, FortiManager, and FortiSIEM
- Armis Collectors, Collective Asset Intelligence Engine, Threat Detection Engine

Solution Benefits

- Quickly discover managed and unmanaged devices across distributed care delivery and research environments
- Proactively 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

FORTINET FABRIC-READY

wireless, and 5G. Converge your security and networking point solutions into a simple-to-use, centralized management console powered by a single operating system, FortiOS, and simplify IT management.

Fortinet FortiManager delivers unified management for consistent security across complex hybrid environments, protecting against security threats. Key benefits include accelerated zero-touch provisioning with best-practice templates for deployment at the scale of SD-WAN and streamlined workflows within the Fortinet Security Fabric.

Fortinet FortiSIEM brings together visibility, correlation, automated response, and remediation in a single, scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and even prevent breaches.

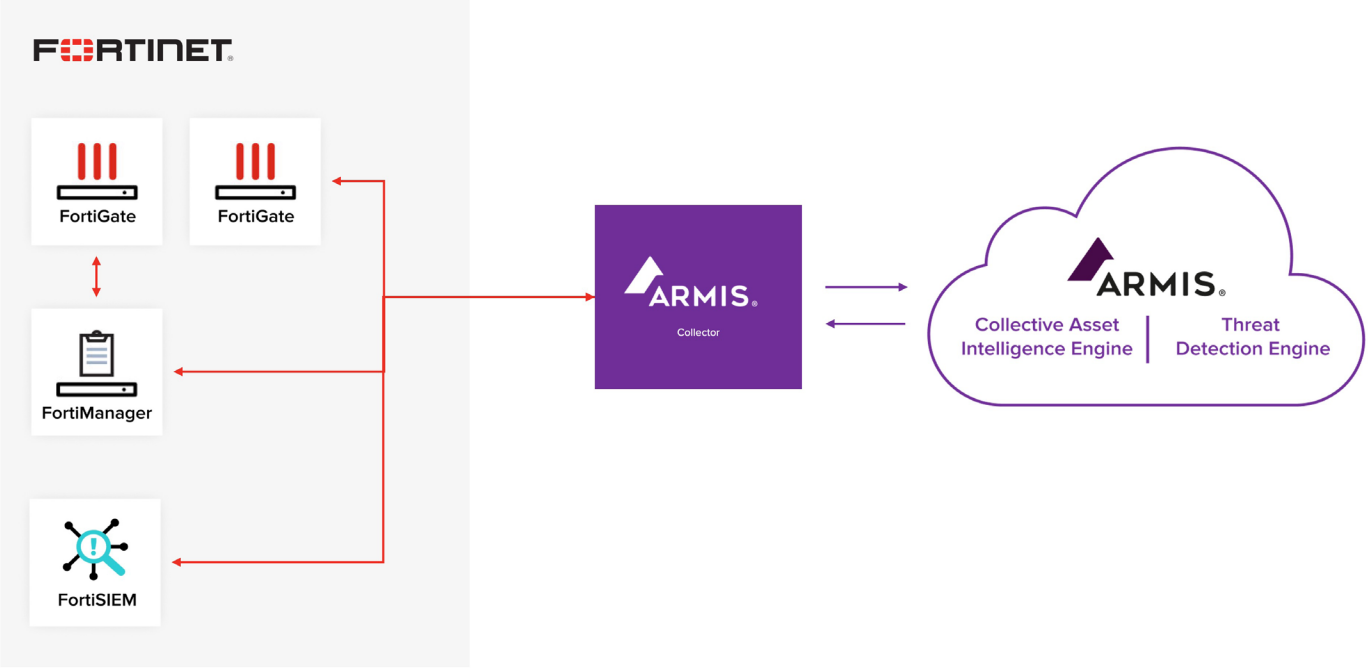

Figure 1: Fortinet and Armis integration architecture

Use Cases

Use Case #1: Discovering Every Connected Device

Armis's integration with Fortinet 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.

Armis utilizes the FortiGate 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's 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.

Use Case #2: Tighten Security Controls with Dynamic Policies

Armis also communicates with the centralized FortiManager to receive policy information and modify them 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.

Use Case #3: 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 (for example, CVEs and unsupported operating systems). 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 the FortiSIEM security information and event management system and provide contextual details to enhance its behavior analytics capabilities. Armis's visibility extends deep into all segments of the network, even where security devices or intrusion detection systems may not reach.

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.

September 13, 2023 5:13 PM

2344662-0-0-EN