Gigamon® | ARMIS

Unmanaged and IoT Devices Are Vulnerable. Protect Them with Gigamon and Armis.

THE CHALLENGE

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 and are difficult to patch. 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.

THE SOLUTION

The Gigamon Visibility and Analytics Fabric™ and the Armis® Agentless Device Security Platform work together to reduce business risk and increase security by providing real-time and continuous protection for managed, unmanaged, and IoT devices.

JOINT SOLUTION BENEFITS

+ 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

Introduction

Armis is the leading agentless, enterprise-class device security platform designed to address the new threat landscape of unmanaged and IoT devices – from traditional devices like laptops and smartphones to new smart devices like TVs, webcams, printers, HVAC systems, industrial control systems and PLCs, medical devices, and more.

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

The Gigamon + Armis Joint Solution

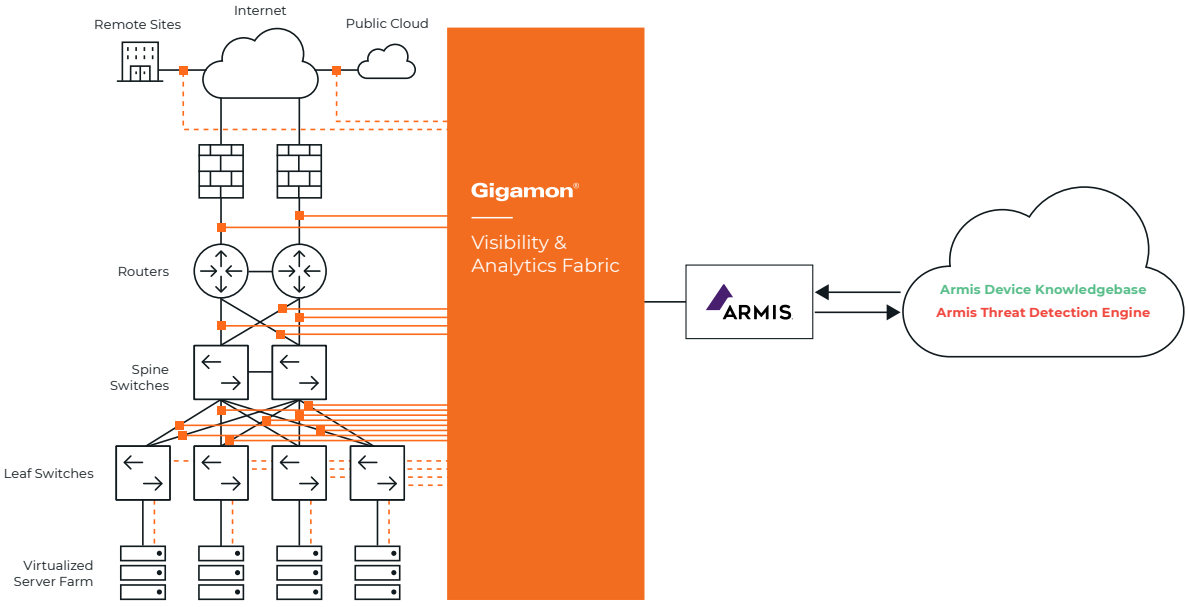
The Gigamon Visibility and Analytics Fabric provides full network traffic visibility and filters, deduplicates, decrypts and delivers relevant traffic to the Armis Agentless Security Device platform. This enables joint customers to develop use-cases that address issues including:

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 IoMT devices aren't going to be compromised by more vulnerable network devices?
+ Are there any IoMT devices in a guest 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?

A new forecast from IDC estimates that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data in 2025.

– IDC, WORLDWIDE GLOBAL DATASPHERE IOT DEVICE AND DATA FORECAST, 2019-2023

For more information on Gigamon and Armis, visit: www.gigamon.com and www.armis.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com