SOLUTION BRIEF

Armis Asset Management and Keysight Visibility Keeps Devices Safe

See, Protect, and Manage Every Asset Across Every Domain

KEYSIGHT

The Joint Solution

Securing today's digital business environments starts with an accurate, up-to-the-minute view of every managed and unmanaged device—whether they contain monitoring agents or not. The Armis Centrix™ Cyber Exposure Management Platform sees, protects, and manages billions of assets around the world in real time.

Combining Armis's asset management solutions with Keysight's network visibility creates a seamless, automated approach to securing every device across every domain – IT, cloud, operational technology (OT), industrial control systems (ICS), and the internets of things (IoT) and medical devices (IoMT).

- Sees, secures, protects and manages billions of assets around the world in real time
- Agentless discovery and analysis – no additional hardware required
- Up-to-the-minute asset inventory
- Analyzes behavior continuously to identify threats and vulnerabilities that lead to costly attacks
- Streamlines control of IoT and unmanaged devices

Armis and Keysight deliver a highly intelligent, automated, and agentless approach to achieving device visibility and security. The joint solution features agentless device discovery and analysis, scalable hybrid network visibility, and support for off-network devices communicating on wireless connections.

How it Works

Using device data provided by Keysight, the Armis platform discovers every managed, unmanaged, and IoT device on and off of your network, analyzes device behavior to identify risks or attacks, and protects your critical business information and systems. Armis is agentless and integrates easily with your existing security products. Armis uses device profiles and characteristics from the Armis Device Knowledgebase to identify each device, assess its risks, detect threats, and recommend remediation actions.

Integration with Keysight virtual SPAN/TAP makes getting Armis easy to deploy, so it can be up and running in minutes to hours. Not only does Armis integrate with your firewall or NAC, it also integrates with your security management systems like your SIEM, ticketing systems, and asset databases to allow these systems and incident responders to leverage the rich information Armis provides.

Armis Keeps Devices Safe and Inventories Up to Date

The Armis platform gathers data from your wired, wireless, and multi-cloud infrastructures. Armis uses device profiles and characteristics to identify each device, assess its risks, detect threats, and recommend remediation actions.

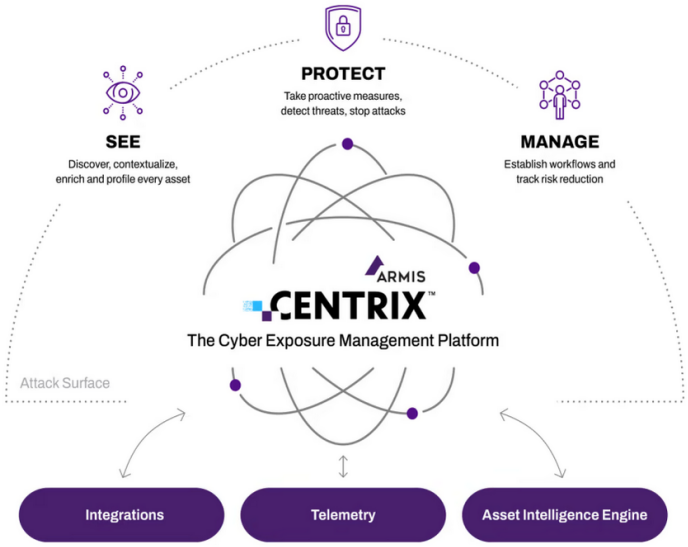

Figure 1. Agentless Visibility for Managed, Unmanaged, and IoT Devices

Together, Armis and Keysight extend visibility beyond laptops and smartphones to more specialized—and inherently vulnerable—devices like smart TVs, video cameras, HVAC systems, and equipment used in point of sale (POS), industrial, medical systems. Solution highlights include:

- Powered by the Armis AI-driven Asset Intelligence Engine
- Discovers every device in your physical and virtual environments in real time
- Seamlessly connects with existing data sources to protect assets from the ground to the cloud
- Automated behavior analysis and threat detection
- Streamlines management of devices and systems that aren't designed with security in mind (or haven't been hardened, patched, or updated)

Complete Hybrid Network Visibility Solution from Keysight

Keysight's visibility fabric provides the Armis platform with complete access to data via:

- Physical and virtual taps used to access data
- Vision network packet brokers (NPBs) that process and deliver the right data to the right security and monitoring tools
- Complete visibility coverage across public, private, and multi-cloud environments

Keysight NPBs uses passive network and virtual taps to collect data, conserving valuable switch mirror ports and ensuring packets never get missed. Vision packet brokers avoid overburdening monitoring solutions by load balancing traffic to optimize tool utilization and performance. Keysight NPBs also remove duplicate traffic and mask sensitive data to strengthen security and maintain compliance.

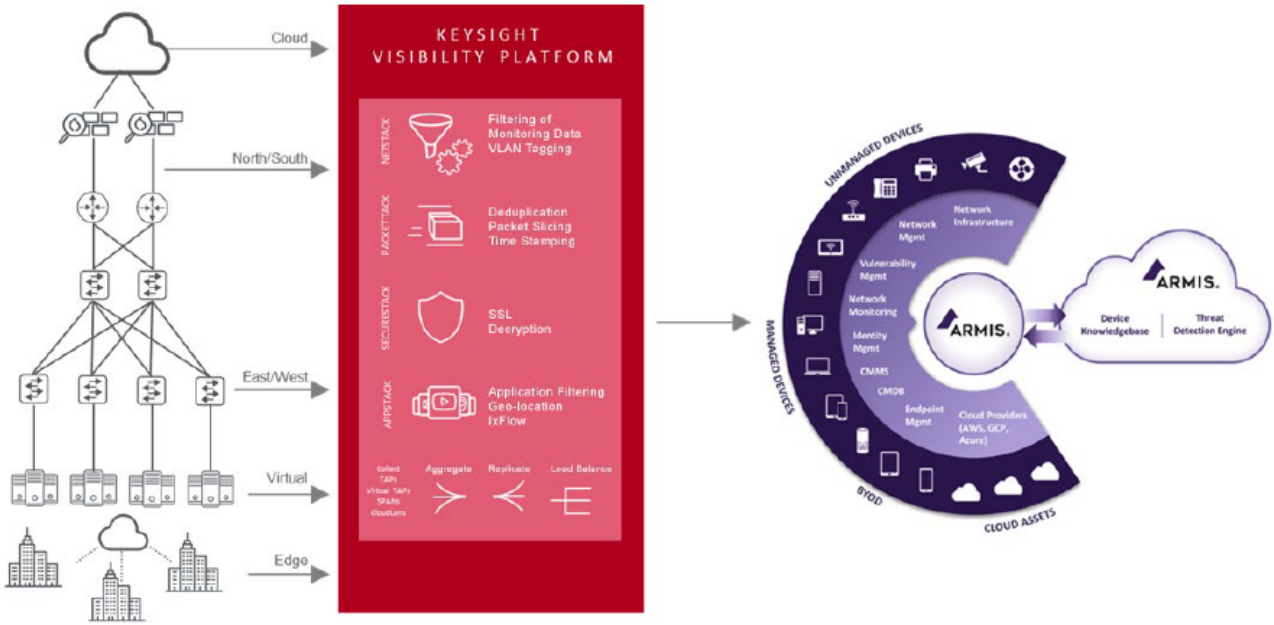

Figure 2. Agentless Visibility for Managed, Unmanaged and IoT Devices

Keysight's unique Network Packet Brokers load balance traffic to optimize utilization while ensuring Armis has access to reliable, ubiquitous data. Optionally, Vision NPBs can filter out duplicate traffic, mask sensitive data to support compliance, and easily share traffic with all security tools that need to see it. Whereas in the past a few switch mirror ports may have provided sufficient data access, using gateway points, monitoring is not predictable, static or robust enough to support today's security challenges.

Keysight's visibility solutions combining taps, Vision Network Packet Brokers, and CloudLens deliver a smarter, more reliable and cost-effective approach to delivering data from the network to each security and monitoring tool.

A perfect partnership

About Armis

Armis is the leading agentless, enterprise-class device security platform designed to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our real-time and continuous protection to see and control all managed, unmanaged, and IoT devices – _from traditional devices like laptops and smartphones to new smart devices like smart TVs, webcams, printers, HVAC systems, industrial control systems and PLCs, medical devices and more. 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.

Learn more at: www.armis.com

About Keysight Visibility

Connect and Secure the World with Dynamic Network Intelligence

The need for always-on networks is pervasive, and expectations are high when it comes to keeping them connected and secure. As technologies advance, edge computing, cloud environments, sophisticated security threats, increasing bandwidth requirements, and demanding compliance regulations make it challenging to extract actionable insight from your network.

Keysight can help. Customers rely on our solutions to deliver rich data about network traffic, applications, and users across any networking environment. This deep insight is what we call dynamic network intelligence. It helps you continuously innovate, meet aggressive service level agreements, and keep applications running smoothly and securely.

Learn more at: Network Visibility | Keysight