SOLUTION BRIEF

Armis asset vulnerability management.

Manage vulnerability mitigation efforts across the full asset attack surface with risk-based vulnerability management.

Modern organizations are overwhelmed by the sheer volume of vulnerable assets in their environment at any given moment. With the time it takes to exploit a new vulnerability dropping rapidly, and the 60-150 days it takes to patch vulnerabilities, combined with the number of connected devices growing exponentially, security and IT operations teams simply cannot address vulnerabilities as quickly as needed.

These issues, coupled with the need to ensure the availability and stability of business operations, make it necessary to prioritize mitigation efforts across all assets, according to their criticality to the business, and optimize the use of limited resources to minimize exposure.

Armis Asset Vulnerability Management (AVM) offers riskbased vulnerability management that enables security teams to quickly identify and remediate those vulnerabilities that are most likely to be exploited and negatively impact the business.

Full visibility into your asset attack surface

One of the most critical security issues today is the fact that IT and security teams don't know about all of their organization's digital infrastructure and assets, or whether they're vulnerable or not. With most vulnerability scanners missing 40% or more of the managed IT assets in an environment, and not scanning unmanaged assets like IOT devices, organizations are left to deal with an unknown attack surface. This leaves them exposed to a myriad of threats and risks.

Built on the asset discovery capabilities of Armis Asset Intelligence Platform, Armis AVM has a complete, unified view of every asset in your environment. This includes everything from your enterprise IT and network assets, to cloud and IoT devices like smart TVs, IoMT devices, OT devices like HMI panels, SCADA servers, and more.

Armis AVM provides information about vulnerabilities associated with each asset, no matter what the asset type is. If the organization is already using a vulnerability scanner for the IT environment, Armis can integrate with it to gather information for assets already scanned. For assets that are not covered by vulnerability scanners, Armis fills the gap by assessing devices against Armis's asset intelligence knowledge-base. This unique crowd-sourced knowledgebased tracks vulnerabilities for over 2 Billion assets around the world. It is continuously updated by Armis's research group with the latest information about vulnerabilities and exploits, ensuring you are always up-to-date.

Armis AVM also fills in gaps on scanner-identified assets, and provides important details for each asset about the asset owner, its location, and more. This ensures that you are fully aware of the organization's attack surface, and understand each device and asset that can expose the organization to risk.

"Armis helped increase vulnerability visibility to 95% and reduced manual operations immeasurably."

Large U.S. retailer with 2,000+ sites

“The single most important benefit of Armis is that it enables us to have a single source of truth. It consolidates our risks and vulnerabilities so that they are prioritized and actionable.”

CISO, Global Technology Company

Business critical risk-based prioritization

Prioritization of mitigation efforts by business criticality helps security and IT operations teams focus their efforts on the most pressing vulnerabilities that matter most. When your teams know exactly which critical assets are affected, by which vulnerabilities, they can act quickly and precisely to thwart the issues that pose the biggest threat to your business.

Armis continuously monitors and maps out the connections and communications between various assets and services in your environment. This allows Armis to understand the relationships and dependencies on assets in your environment. An asset with many connections and dependencies is more critical to your business, and therefore should be prioritized over a stand alone asset with no dependencies, even if the vulnerabilities of the stand-alone asset are more severe. (Note that the criticality of an asset can be set manually as well).

Armis AVM calculates a risk score for each asset based on its criticality to the business, the severity of its vulnerabilities, and the exploitability of these vulnerabilities. Unlike vulnerability management solutions that only consider the CVSS score (Common Vulnerability Scoring System), Armis also understands the business criticality of the asset allowing you to focus your efforts where they are needed most.

Key Benefits

- Get a complete, accurate view of assets and vulnerabilities in your inventory
- Prioritize remediation efforts based on business risk
- Reduce mean time to remediation
- Gain control over the full vulnerability management lifecycle
- Improve your overall risk posture

“Armis has been in our environment for about three years now, and we’ve developed some high-profile use cases, including the most important one— vulnerability management— which we found to be an extremely useful feature. Working in concert with our vulnerability management system, it has significantly shortened mean time to resolution (MTTR).”

Manufacturing company with multiple sites around the world.

Full vulnerability lifecycle management

Armis AVM offers full vulnerability lifecycle management features to continuously improve the security of your environment. Ongoing monitoring, dashboards, and reports help you track vulnerability mitigation efforts over time and demonstrate improvement in the organization's security posture.

Integration with security automation and orchestration solutions enables automated responses to detected vulnerabilities. The response can be as simple as opening a ticket in a ticketing system and alerting the responsible team, quarantining the vulnerable device until it is remediated and verified, or and even full automated remediation or patching of the vulnerable asset.

The Armis Difference

Meets Your Business Needs

Prioritize mitigation efforts based on the asset criticality and the severity of the vulnerabilities, to effectively reduce exposure to risk.

Comprehensive

Leverage a complete, unified inventory of every asset in the environment, including those that are outside your corporate network such as IIoT and IoMT devices, to ensure awareness across the full asset attack surface.

Quick time-to-value

Realize immediate value with a dashboard and customized reports that are specific to vulnerabilities and enable you to quickly and precisely mitigate the most important risks.

Accurate profiling

Eliminate false positives with added threat intelligence from more than 1 billion tracked assets.

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.

1.888.452.4011 | **armis.com**

20220425-1

ARMIS