SOLUTION BRIEF

Armis Centrix™ for Vulnerability Prioritization and Remediation

Consolidate, Prioritize and Respond To The Vulnerabilities That Matter

The Current Model is Broken

The volume of accumulated vulnerabilities that organizations need to deal with is measured in the millions.[1] With every new asset deployed in support of growth, efficiency and innovation, the enterprise attack surface expands. According to the Cybersecurity and Infrastructure Security Agency (CISA), adversaries exploit vulnerabilities within just 15 days of their discovery, while it typically takes several months to patch them.

Unfortunately, many organizations continue to put more money into revamped versions of stale technologies, or continue to leverage inadequate scoring systems based on the characteristics of vulnerabilities rather than the risk to their business:

CVSS

(Common Vulnerability Scoring System) is a ranking system that marks the severity of known vulnerabilities using a score of 1-10. CVSS scoring however, does not take into account asset criticality in relation to the business context.

EPSS

(Exploit Prediction Scoring System) estimates the likelihood that a vulnerability will be exploited in the wild. While the intent behind this initiative is helpful, it still does not take into account specific conditions or compensating controls within an organization's network.

4 Days

IT security teams are spending an average of four days per week (or 16 days a month) manually prioritizing vulnerabilities.[2]

Our Solution at a Glance

- Obtain a consolidated real time view of all vulnerabilities
- Prioritize vulnerabilities that pose the greatest risk to your business
- Receive optional early warnings for targeted attacks - even before a CVE is published
- Gain full vulnerability lifecycle management through integration with your existing tools

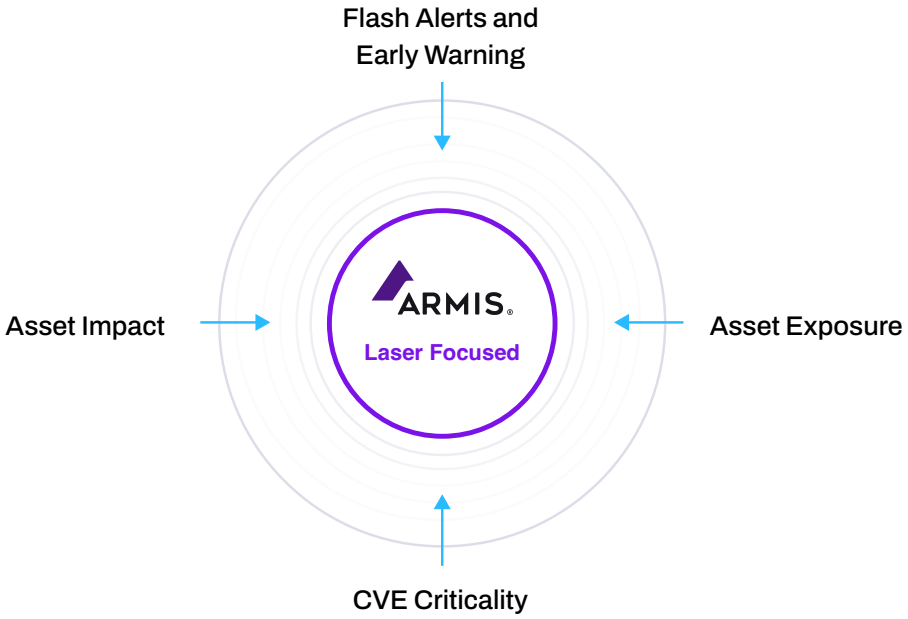
The result?

Hours wasted on addressing vulnerabilities that pose little or no risk to their business, while organizations still remain at risk.

A New Approach is Needed

Resource constraints, limited budgets, personnel shortages, and competing priorities: how do you optimize the use of limited resources and minimize exposure to the business? The answer is risk-based vulnerability prioritization, executed with surgical precision.

Armis Centrix™ for Vulnerability Prioritization and Remediation consolidates all vulnerabilities that are relevant to your business and enables security teams to quickly identify and remediate those vulnerabilities that are most likely to be exploited and negatively impact the business. Armis produces a laser focused list of vulnerabilities, based on the following key elements:



01 Asset Impact

What value does the asset have to the business?

02 Asset Exposure

Is the asset internet facing, exposed externally and/or internally?

03 CVE Criticality

Based on a multitude of facets including Armis Risk Factors, CISA KEV, CVSS, etc.

04 Early Warning

AI technology that leverages dark web, honeypots and human intelligence to stop targeted attacks before they impact you.

Armis Centrix™ for Vulnerability Prioritization and Remediation

Armis has been acclaimed by customers, partners, and analysts as it redefined vulnerability management by combining real-world threat intelligence and analytics with your own business landscape. By taking into account the actual risk to the business, we are able to deliver a manageable and prioritized list of vulnerabilities - and what to do about them.

With Armis you can manage the risk by prioritizing high-risk vulnerabilities, and quickly remediating those vulnerabilities to reduce your organization's risk. Our superior capabilities around consolidation, prioritization and remediation as well as completeness of the product sets us far above traditional vulnerability assessment and management tools. All of this, without disruption and working in conjunction with your existing tools and workflows.

See

- Consolidate vulnerabilities and security findings
- Fill in coverage gaps
- Enrich with context and recommendations

Protect

- Prioritize based on criticality to the business, severity of the vulnerability, exploitability
- Optional: receive early warnings for targeted threats, before they are ever launched

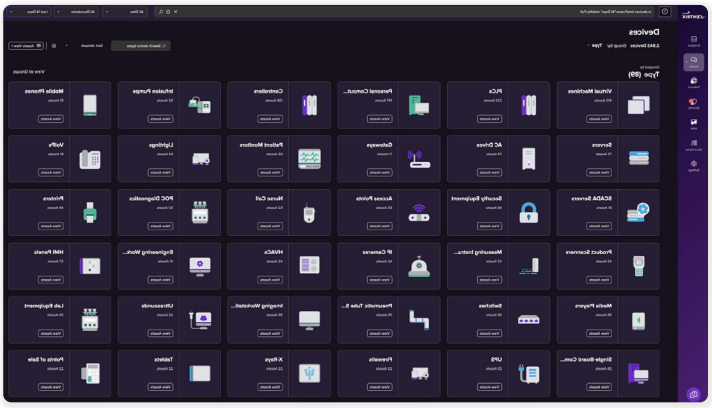
Manage

- Reduce risk through integrations with existing ticketing and enforcement tools
- Monitor progress through ongoing dashboards and reports

Consolidate Security Findings and Fill in Coverage Gaps

Unifying security findings from many different sources and feeds is a difficult and time consuming task. But with Armis, this is addressed and handled automatically for every asset in the environment.

Armis starts with a complete, unified view of every asset in your environment - physical and virtual - whether it is IT, Operational Technology (OT), Internet of Things (IoT) or medical (IoMT). For non-traditional assets, Armis leverages continuous traffic inspection and Smart Active Querying to extract details about all devices connected to the network.



Armis combines security findings from traditional scanners, endpoint detection and response (EDR) solutions and cloud vendors, with its native network traffic analysis and context from the Armis AI-driven Asset Intelligence Engine, which sees, secures, and manages billions of assets around the world in real time.

"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."

Chief Information Officer (CIO)
Global Technology Company

Enrich with Asset Context and Recommendations

Organizations already using a vulnerability scanner for the IT environment can integrate Armis with their existing scanner to gather further information and context about the CVEs.

For assets not covered by vulnerability scanners, Armis fills the gap by using agentless and non-intrusive techniques:

- Continuous monitoring of wired and wireless traffic to identify each device without disruption.
- Smart Active Queries to communicate proactively with devices in their native language in a safe manner.

Armis then assesses the results against the AI-driven Asset Intelligence Engine. This unique crowd-sourced knowledge base tracks profiles for billions of assets around the world. It is continuously updated with the latest information about vulnerabilities and exploits, ensuring you are always up to date. The end result is a single pane of glass for organizational assets, their vulnerabilities, and their business impact.

Armis AI-driven Asset Intelligence Engine

> Core to the Armis Centrix™ Platform is our Asset Intelligence Engine. It is a giant, crowd-sourced, cloud-based asset behavior knowledgebase—the largest in the world, tracking over four billion assets—and growing.

> Each profile includes unique device information such as how often each asset communicates with other devices, over what protocols, how much data is typically transmitted, whether the asset is usually stationary, what software runs on each asset, etc. And we record and keep a history on everything each asset does.

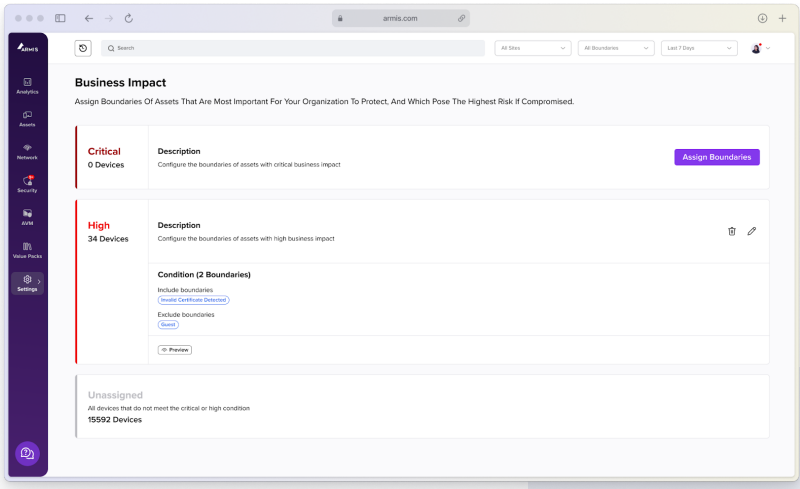
> These asset insights enable Armis to classify assets and detect threats with a high degree of accuracy. Armis compares real-time asset state and behavior to “known-good” baselines for similar assets we have seen in other environments. When an asset operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine an asset.

Prioritize Vulnerabilities

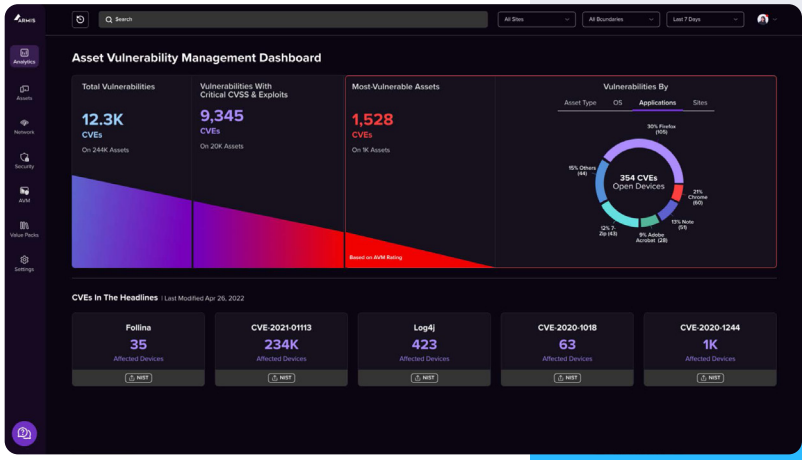
Prioritization of mitigation efforts by business criticality helps your security and IT/OT operations teams focus their efforts on the vulnerabilities that matter most. When your teams know exactly which critical assets are affected, by which vulnerabilities, they can act quickly and precisely to remediate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

Let's take an internet facing asset with many connections and dependencies that runs essential business operations or services.

This asset is more critical to your business and should be prioritized over a non-internet facing asset with no critical dependencies, even if the vulnerabilities are more severe.

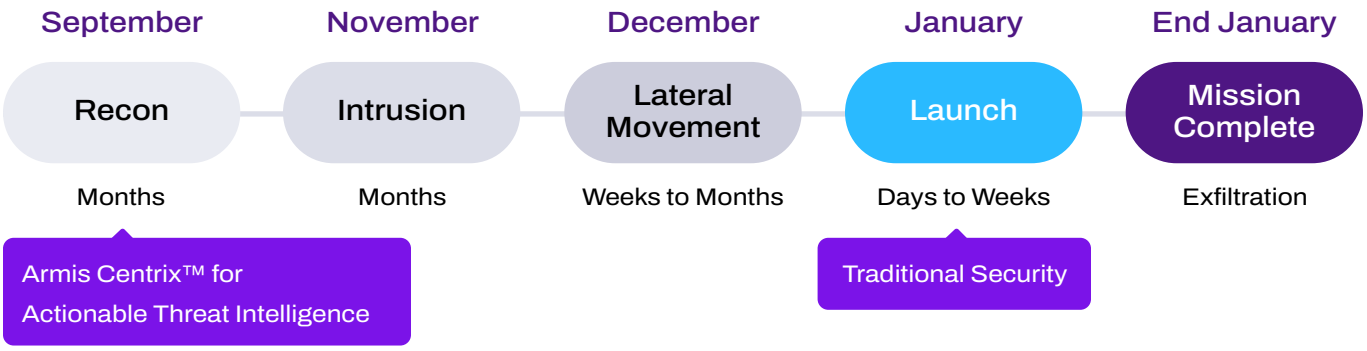


Armis calculates a risk score for each asset based on its criticality to the business, the severity of its vulnerabilities, and the exploitability of these vulnerabilities. Unlike raw scanner output data that only considers the CVSS score, Armis also takes into account the business criticality of the asset, its presence in CISA Known Exploited Vulnerabilities, ransomware association, etc. Our vulnerability intelligence allows you to focus your efforts where they are needed most.



Armis Centrix™ for Actionable Threat Intelligence

Armis Centrix™ for Actionable Threat Intelligence is an optional integration and introduces a paradigm shift. Whereas traditional security goes to work when an attack is launched, actionable threat intelligence enables organizations to find potential threats before they are ever launched and before their environment is ever impacted. In many cases, months earlier. In fact, Armis has hundreds of instances where customers were proactively alerted to a threat before a CVE was issued.



Armis Centrix™ for Actionable Threat Intelligence offers a revolutionary AI technology that leverages dark web, dynamic honeypots and human intelligence to stop attacks before they impact your organization.

Why do organizations choose to add Armis Centrix™ for Actionable Threat Intelligence?

- Protect against weaponized threats.
- Preempt threat actors and stop them before they impact your organization.
- Address the vulnerabilities that are actually being exploited by threat actors.
- Gain a head start before a CVE gets published.

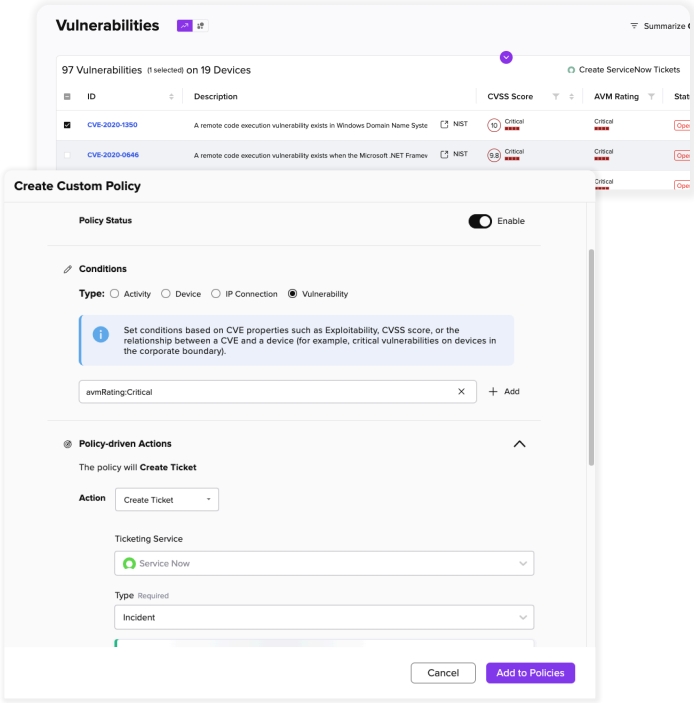
Remediate Vulnerabilities

Workflow integration with security and ticketing solutions like JIRA and ServiceNow help to reduce mean-time-to-resolution (MTTR) and manage the risk-reduction process. This includes the ability to:

- Manually or automatically create tickets
- Update existing tickets as new assets are discovered in your environment

Armis Centrix™ also connects to your existing security tools to set remediation and mitigation actions, including:

- Updating firewall rules
- Adding security tags
- Configuration changes
- Fully automated remediation and patching of the vulnerable asset



Jira servicenow

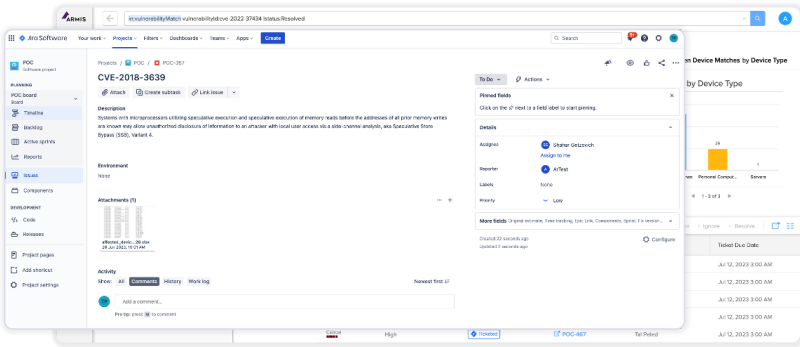
"Armis helped increase vulnerability visibility to 95% and reduced manual operations immeasurably."

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

Track Progress and Manage Process

Armis 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.



"Armis has been in our environment for over 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

With Armis Centrix™ for Vulnerability Prioritization and Remediation you get:

Efficiency

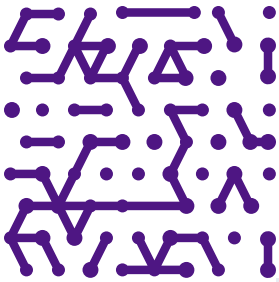
Dramatically improve efficiency by focussing on what matters most.

Accuracy

Leverage deep context based on billions of assets tracked worldwide.

Return On Investment

Stop wasting valuable time and money on vulnerabilities that post little or no risk to your business.



The Armis Difference

Understands Your Business and Threat Landscape

Prioritize mitigation efforts based on the asset criticality and the severity of the vulnerabilities, even before a CVE gets published.

Data Quality At Scale

The Armis AI-driven Asset Intelligence Engine tracks profiles for billions of assets around the world and is continuously updated with the latest information about vulnerabilities and exploits, ensuring you are always up to date.

Quick Time-to-value

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

End-to-end Platform

Armis is not a point solution. We connect to your existing workflows and security tools to deliver full vulnerability lifecycle management.

Sources

1. Ponemon Institute
2. IT Security Wire

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011