SOLUTION BRIEF

Armis Centrix™ for VIPR Pro

Next-gen Approach to Close the Gap Between Finding and Fixing Risk

At a glance

Translates millions of alerts to thousands of grouped findings to drive risk reduction.

Contextualize findings and assets, automate prioritization, and collaborate with remediation teams.

Operationalize the remediation lifecycle, and maintain centralized visibility into risk posture.

The Current Model is Broken

Vulnerability management has long been a cornerstone of cybersecurity programs - but the current process is broken. Teams are spending more time and resources on triaging findings for more types of exposures from more security tools - but are having less effective impact on reducing risk. Meanwhile, vulnerability management has become more critical to identifying and fixing risk as part of a consolidated, proactive approach to attack surface management strategy.

Not built to handle and contextualize **huge volumes of alerts** - vulnerabilities, cloud, code, containers, and AppSec

Does not consider **security risk, asset profile, business impact and likelihood of exploit**

Does not bridge the gap between between teams identifying risk, and teams fixing risk

Because of inefficient processes and inconsistent risk prioritization, security teams struggle to scale **what** to fix, **who** should fix it, and **how** it should be fixed.

A New Approach is Needed

Operational efficiency and risk reduction

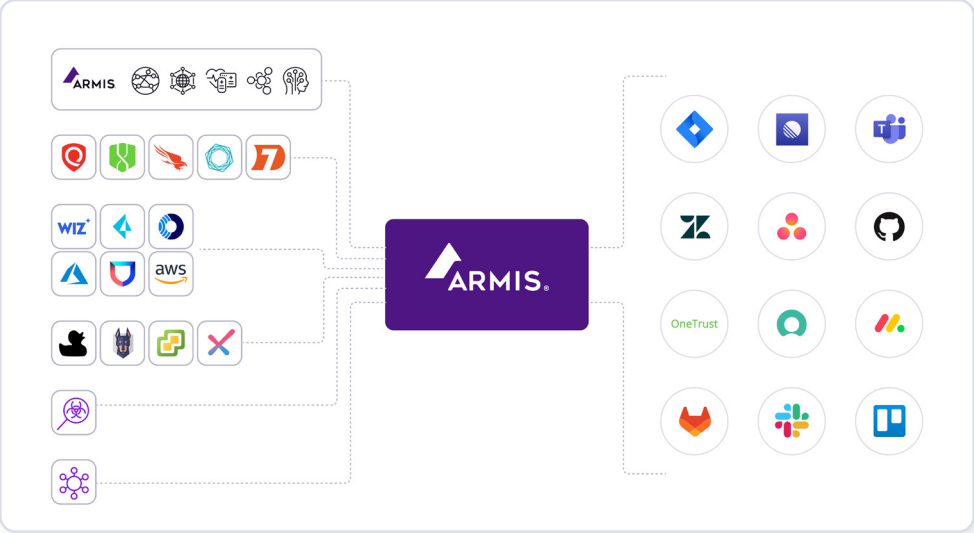
Alert fatigue, resource constraints, and competing priorities: how do you optimize the use of security resources and tool data to minimize the organization's exposure, and ensure the most urgent risks are addressed? The answer is risk prioritization and remediation, automating the process of identifying findings with the highest risk in your environment, and enabling the fix for remediation owners through actionable guidance using their day to day workflows.

Armis Centrix VIPR Pro – Prioritization and Remediation enables security teams to transform their vulnerability management programs to more efficiently and systematically reduce risk, for traditional vulnerabilities as well as asset, misconfigurations in code, cloud infrastructure and application exposures. VIPR Pro seamlessly ingests security tool findings, enriches prioritization based on asset profile and business risk weighting, then automates ownership assignment for remediation tasks, and the remediation lifecycle.

Armis takes a data-centric, AI-driven approach for adaptable prioritization to identify the most critical risks in the organization's environment and to their business, and facilitate an end to end remediation lifecycle. As an integral component of the Armis Centrix platform, VIPR Pro enables a consolidated, proactive approach to attack surface management.

Transforming Vulnerability Management

With Armis, security stakeholders can identify risks with greater fidelity, communicate priorities more effectively, automate accurate ownership assignment, and collaborate with IT, developers and operations stakeholders to efficiently manage the entire lifecycle of the risk resolution management process.



This approach extends across any security finding including infrastructure, code, cloud and application security tools, providing security teams with a consolidated view and clear understanding of how to prioritize and remediate along with how these activities impact overall risk posture that can impact the business.

To facilitate resolution tasks, Armis generates predictive ownership rules through AI to assign fix responsibilities, and enables ongoing communication for distributed teams through bidirectional integration with their preferred workflow or ticketing system.

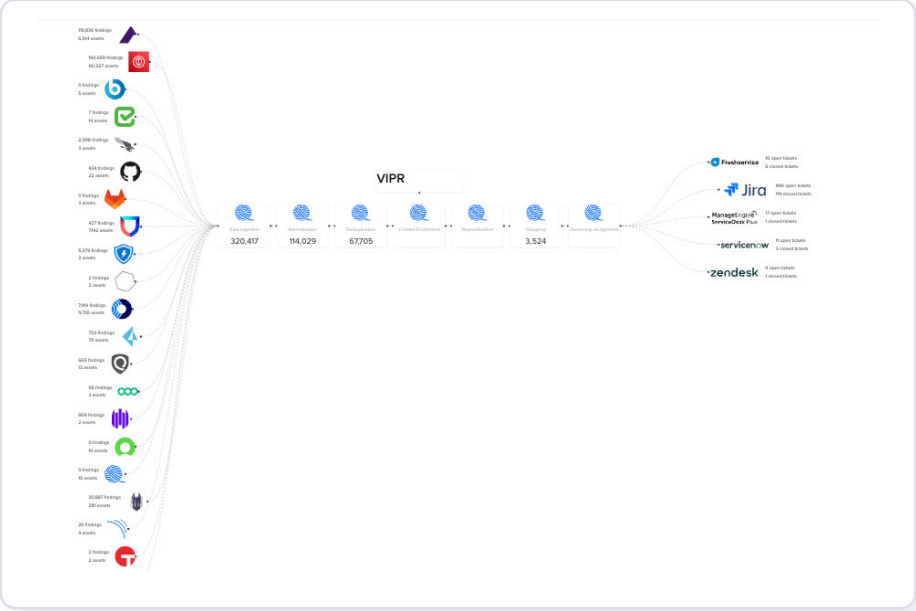
Security teams can centrally monitor both remediation task status and exceptions requests. With consolidated visibility across ticketing systems, security teams can easily track the remediation performance of teams or business units, and their relative risk posture status.

For reporting to security and executive stakeholders, Armis provides a comprehensive dashboard for trend tracking, along with widgets to provide another layer of detail, or customization for specific operational metrics and objectives.

Unify

Aggregate, normalize and de-duplicate data from security scanner and detection tools for endpoints, physical devices, cloud, code and applications.

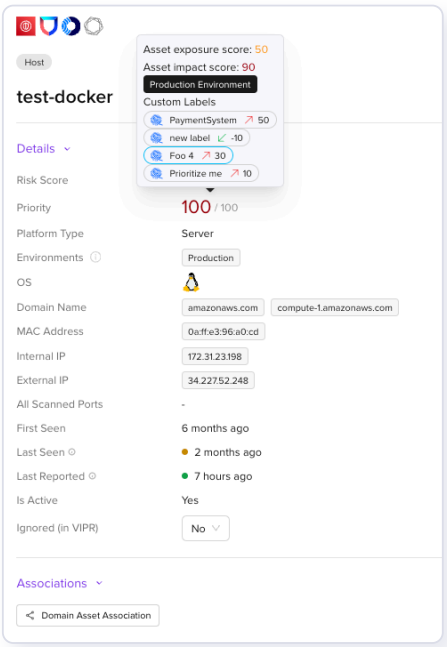
Ingest and inventory asset data from asset management, security tools, ITSMs and infrastructure - including Armis Centrix Asset Management and Security.



Contextualize

Assign context to findings for prioritization-asset profiles and attributes such environmental information and security risk weighting, threat intelligence, likelihood of exploit.

Understand how findings are related, group findings with a common fix and identify high-impact fixes for code and cloud.

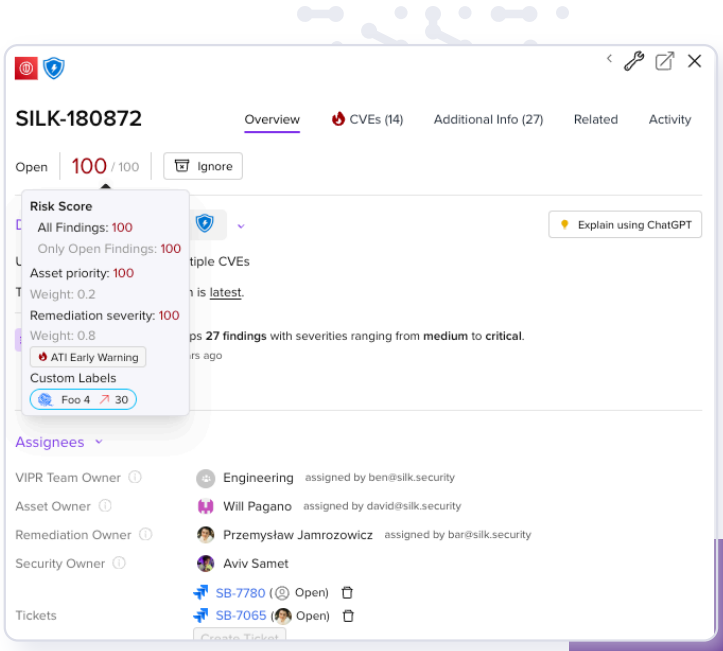


Prioritize

Automate prioritization based on adaptable risk assessment, likelihood of the exploit and active exploit activity. Integration with Armis Centrix AMS for asset profiles and enrichment.

Associate and propagate custom metadata with assets to reflect specific attributes, and apply risk weightings.

Optional integration with Armis Centrix™ for Early Warning: AI technology and machine learning algorithms to stop attacks before they impact your organization.

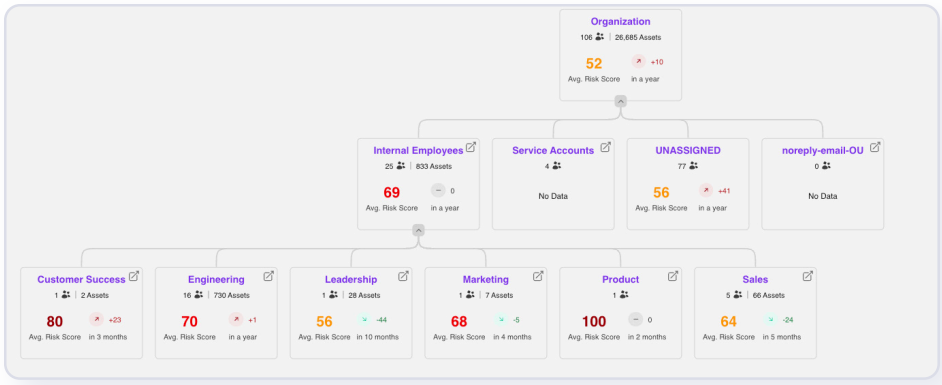


Assign and Remediate

Leverage AI-driven predictive capabilities to determine who is most likely responsible for the remediation task, and apply asset ownership rules.

Ongoing communication for distributed teams thr ough bidirectional integration with their preferred workflow or ticketing system.

Leverage bulk ticketing automation for grouped findings, and flexible remediation campaigns to logically group together and manage finding.

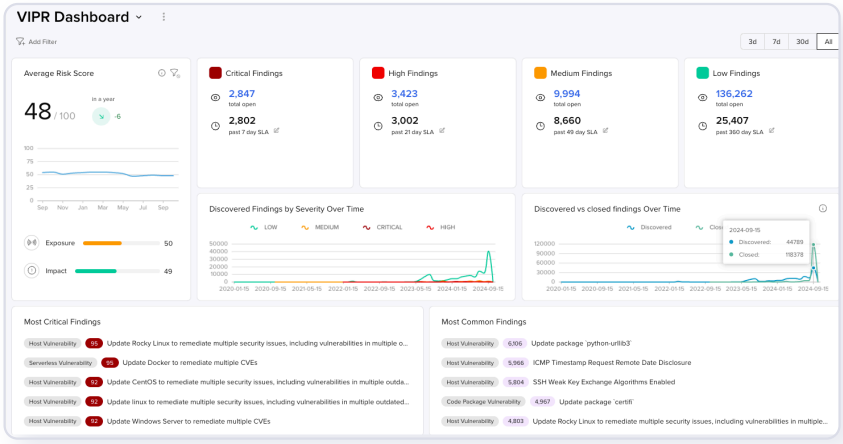


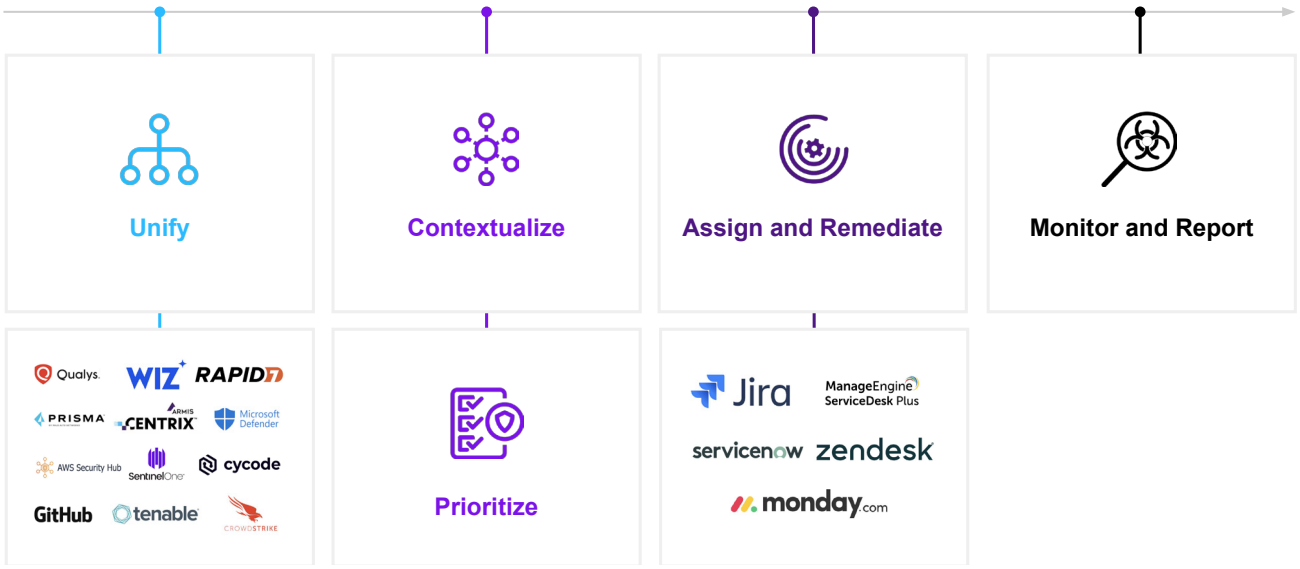
Monitor and Report

Centralized tracking and monitoring of remediation task status, by criticality, finding category and asset class.

Measure the effectiveness of the remediation process for executive stakeholder reporting.

Maintain consolidated visibility of exception requests and automate follow ups for accepted exceptions.





With Armis Centrix™ for VIPR Pro you get:

Clarity

Eliminate alert overload, and leverage adaptable prioritization for visibility across tools

Efficiency

Automate assessment, fix ownership assignment, and operationalize the remediation lifecycle.

Impactful Actions

Assign limited resources to the findings with the highest impact, and measurably reduce risk.

The Armis Difference

Remediation-Driven and Risk-Based Vulnerability Prioritization

We uniquely address the historical gap in cybersecurity between security findings and actionable remediation. Armis enables organizations to target and operationalize remediation based on contextualized risk.

Integrated asset & finding risk understanding

Armis enables security teams to prioritize and remediate risk across security domains, integrating asset intelligence, exploitability, and threat intelligence. Our product works both for teams focused on vulnerability management, cloud security, and application security, as well as across teams. We provide a centralized view of risk across teams, and visibility across infrastructure and run time environments to identify the fix with the most impact at the earliest point in the pipeline

Comprehensive Coverage

Armis provides the broadest coverage of detection tools, with new integrations added on an ongoing basis. Integrations are non-intrusive, taking an agentless approach based on security best practices.

Holistic Approach to Lifecycle Operationalization

Being the industry's first, Armis monitors over 4 billion global assets. We define what's "normal" and instantly pinpoint anomalies. This vast data pool aids in enhancing data, and continually updating customers with fresh intelligence. Significantly, through integration with Armis Centrix™ we don't leave any asset behind, identifying vulnerabilities and other risks even on unconventional assets like medical devices, IoT and OT.

With Armis, security stakeholders can identify risks with greater fidelity, communicate priorities more effectively, automate accurate ownership assignment, and collaborate with IT, developers and operations stakeholders to efficiently operationalize the entire lifecycle of the risk resolution management process.

ARMIS CENTRIX™

THE Cyber Exposure Management Platform

- Armis Centrix™ for Asset Management and Security
- Armis Centrix™ for OT/IoT Security
- Armis Centrix™ for Medical Device Security
- **Armis Centrix™ for Vulnerability Prioritization and Remediation**
- Armis Centrix™ for Early Warning

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. 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 stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Resources
Blog

Try Armis

Demo
Free Trial