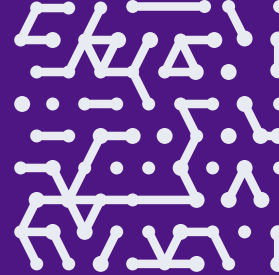


SOLUTION BRIEF

Armis Centrix™ for VIPR Pro – Prioritization and Remediation

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



At a glance

Go beyond vulnerabilities: obtain a unified and deduplicated view of all security findings.

Evaluate context, automate prioritization, and collaborate on fix remediation.

Incorporate and report progress on compliance and SLA metrics, across teams and tools.

The Current Model is Broken

The volume of accumulated security findings in the alert backlog is measured in the millions.(1) Faced with the adoption of new technologies straining their already overloaded processes, security teams have taken tactical approaches to dealing with a flood of security issue alerts, partial tool visibility into complex environments, and not enough information to prioritize and operationalize remediation for distributed operations teams.

Unfortunately, many organizations continue to put more money into revamped versions of stale technologies, or continue to leverage inadequate programs:



Security data often resides in a variety of disparate tools and locations, leading to duplicative or overlapping alerts.



Vulnerability management teams now have responsibility for a much broader range of security issues - not just host vulnerabilities, but also cloud, code and AppSec findings.



Attackers move fast using AI; many organizations move slowly using spreadsheets to mount a defense.

Because of ineffective processes and inconsistent risk prioritization, security teams can't achieve sustained clarity on **what** to fix, **who** should fix it, and **how** it should be fixed.

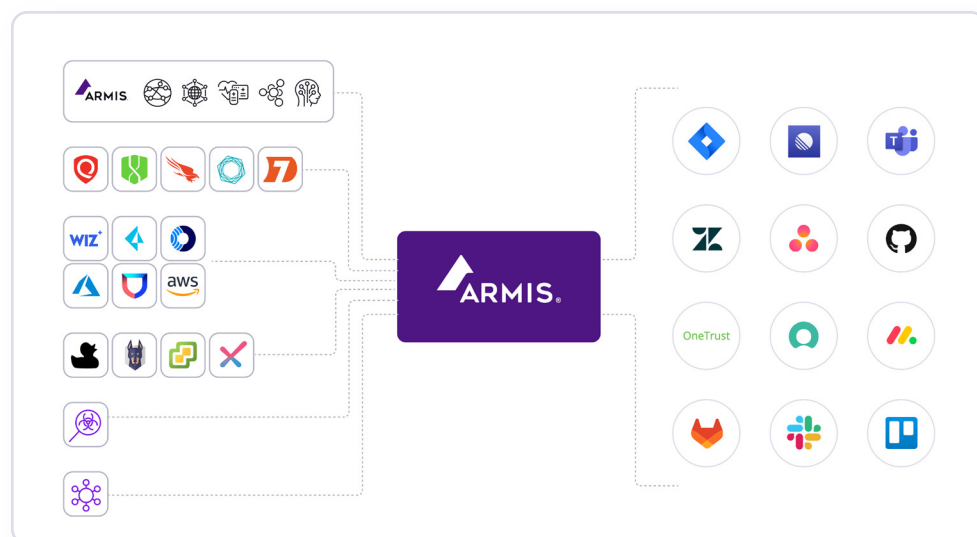
A New Approach is Needed

Alert fatigue, resource constraints, limited budgets, personnel shortages, and competing priorities: how do you optimize the use of resources while minimizing exposure to the business? The answer is risk prioritization and remediation, executed for the right findings, using effective workflows.

Armish has already been acclaimed by customers, partners, and analysts as it redefined vulnerability management by combining real-world threat intelligence and analytics applied to each individual business landscape. Our platform's comprehensive [Asset Intelligence Engine](#) adds risk scores, business criticality, and threat intelligence feeds to provide a single pane of glass for organizational assets, their vulnerabilities, and their business impact.

Armish Centrix™ for VIPR Pro – Prioritization and Remediation extends these capabilities and translates security findings into actionable operational remediation to revolutionize the risk resolution lifecycle.

More Than Vulnerability Management



Armish consolidates detection tool findings and deduplicates alerts, extending from on-premise hosts and endpoints to code, cloud services and application security tools. Organizations using Armish Centrix™ gain additional visibility into their asset attack surface, including unconventional assets like medical devices, IoT and OT.

Our technology assigns context to findings, including threat intelligence, likelihood of exploit, and asset attributes like business impact and compliance policies. The result is an automatically prioritized list of findings.

To facilitate resolution tasks, Armish 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.

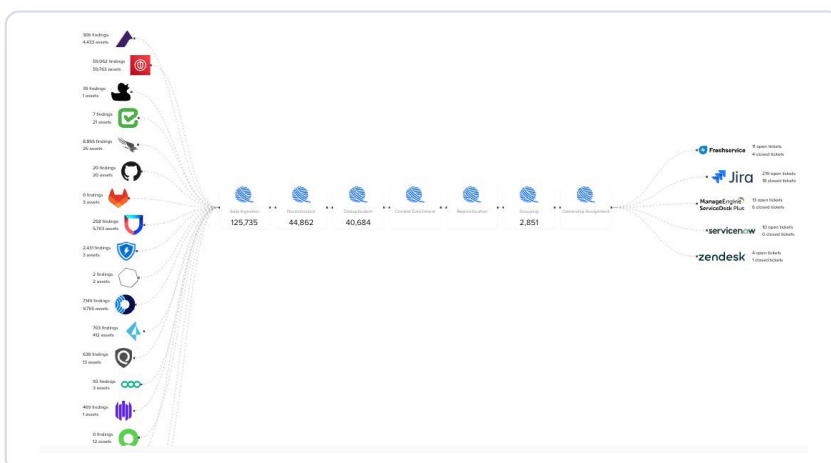
Advanced dashboards, reports and leaderboards help security leaders understand how teams and tools are performing, and measure the effectiveness of the remediation process for executive stakeholder reporting.



Unify

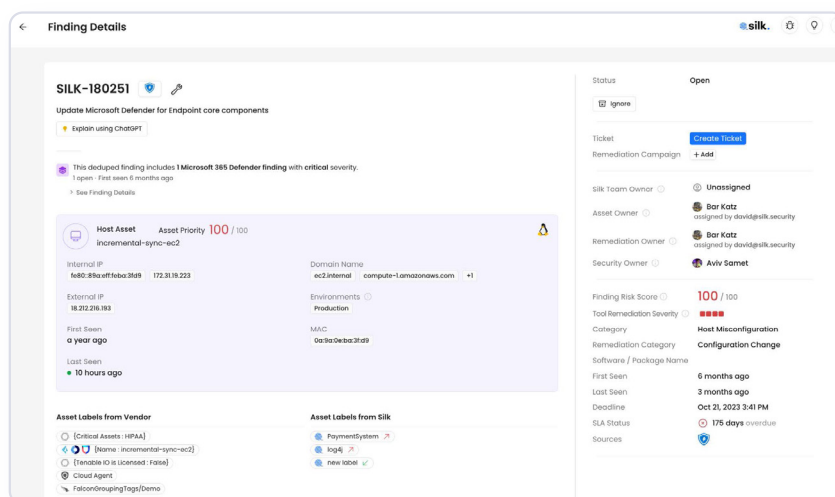
Ingest data from existing sources, including asset context, EDR, on premise, cloud services, code, and applications. Armis supports non-intrusive, read-only integrations to detection tools, vulnerability scanners, asset management tools, developer tools, developer security platforms and more.

Correlate all security findings and reduce the findings volume with ML deduplication.



Contextualize

Assign context to findings including threat intelligence, likelihood of exploit, and asset attributes like environmental information and business impact.



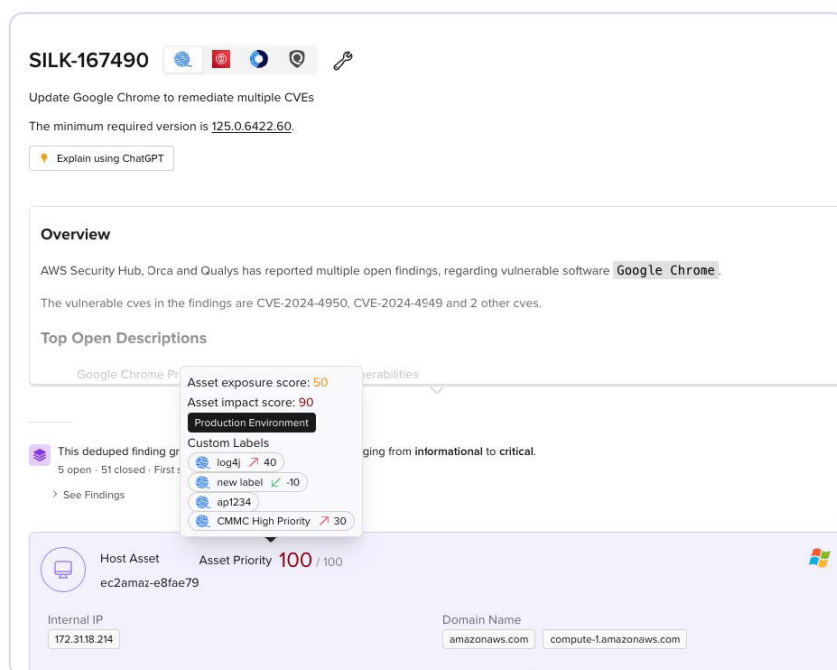


Prioritize

Automate prioritization based on business impact, adaptable risk severity and likelihood of the exploit.

Focus on high-impact fixes that will resolve the largest number of security issues. Pinpoint the earliest point in the code pipeline where a fix will resolve the largest number of related run-time and production findings.

Optional integration with [Armris Centrix™ for Actionable Threat Intelligence](#): AI technology and machine learning algorithms to stop attacks before they impact your organization.



SILK-167490 [Icons]

Update Google Chrome to remediate multiple CVEs

The minimum required version is [125.0.6422.60](#)

Explain using ChatGPT

Overview

AWS Security Hub, Orca and Qualys has reported multiple open findings, regarding vulnerable software **Google Chrome**.

The vulnerable cves in the findings are CVE-2024-4950, CVE-2024-4549 and 2 other cves.

Top Open Descriptions

Google Chrome Pr...

Asset exposure score: 50
Asset impact score: 90
Production Environment

Custom Labels

- log4j ↗ 40
- new label ✓ -10
- apt1234
- CMMC High Priority ↗ 30

This deduped finding gr...
5 open · 51 closed · First t...
> See Findings

giging from informational to critical.

Host Asset **Asset Priority 100 / 100**

ec2amaz-e8fae79

Internal IP: 172.31.18.214

Domain Name: amazonaws.com, compute-1.amazonaws.com

External IP: ...

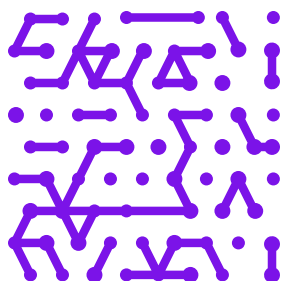
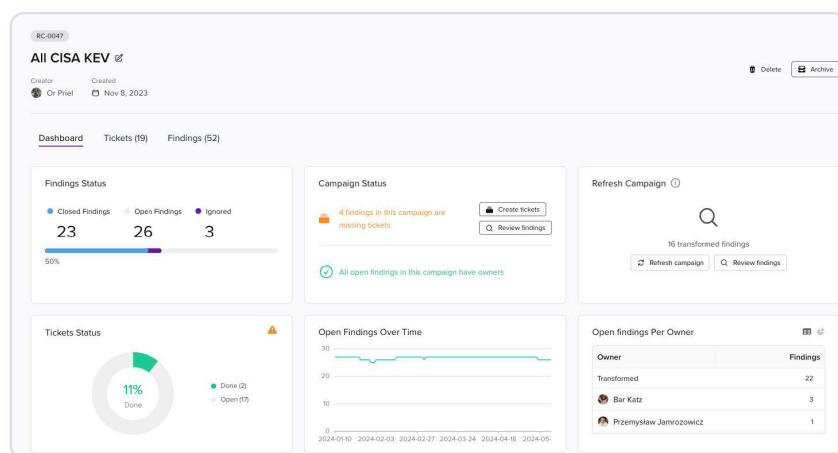


Assign and Remediate

Leverage AI-driven predictive capabilities to determine who is most likely responsible for the asset and the remediation. Assign ownership for prioritized fixes based on automated mapping, with ongoing AI-based refinement based on operations feedback.

Integrate with existing workflows and tools. Manage a single, streamlined ticketing process for open findings with a common fix or associated with the same asset type using grouping, and track progress for grouped remediations.

Enable self-service for risk resolution: assign fix recommendations in teams workflow tools of choice and manage feedback and exception requests through bidirectional workflow integration.



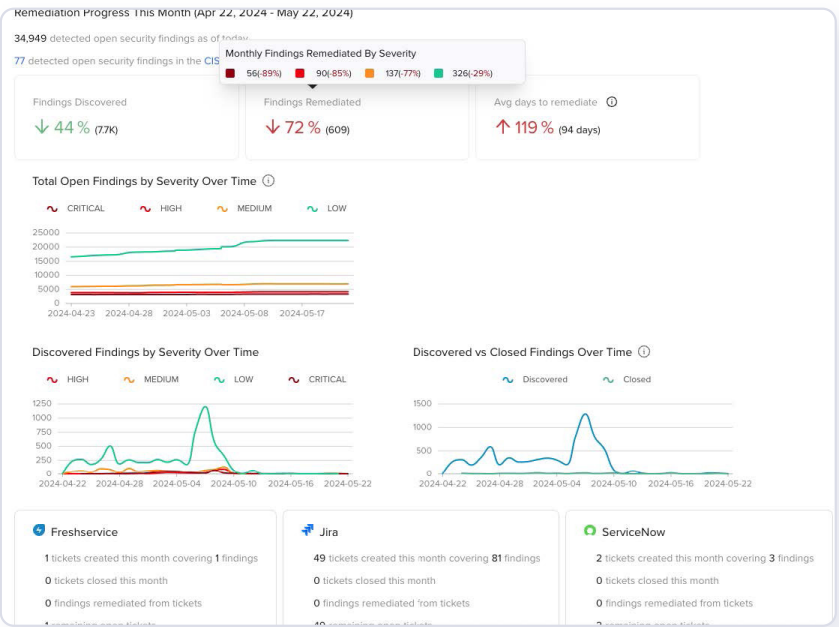


Monitor and Report

Track and demonstrate progress for both individuals tasks, as for overall risk trends in the organization.

Understand how your teams and the tools they are using are performing through a consolidated dashboard, and measure the effectiveness of the remediation process.

Maintain visibility into remediation progress and automate follow ups for exception requests.



With Armis Centrix™ for VIPR Pro – Prioritization and Remediation Pro you get:



Focus

Reduce Security Findings volume by 50-1 with ML deduplication.



Efficiency

Improve mean time to resolution (MTTR) by as much as 90%.



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 remediation based on actual business impact.

AI-driven Asset Intelligence Engine

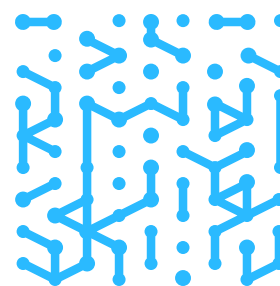
Being the industry's first, Armis monitors over 4 billion global assets. We define what's "normal" and instantly pinpoint anomalies. This vast data pool aids in enhancing data, and continually updating customers with fresh intelligence. Significantly, through integration with Armis Centrix™ we don't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

Broadest 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.

True 360-Degree Insight

While competitors stop at aggregating vulnerabilities, Armis delves deeper. Our product works both for teams focused on vulnerability management, cloud security, and application security, as well as across teams. We provide a centralized, customizable 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.





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

Website

Platform
Resources
Blog

Try Armis

Demo
Free Trial

