Armis Centrix™ for VIPR Pro – Prioritization and Remediation

Financial Services

The Importance of Vulnerability Management in Financial Services

Financial services companies are under attack; with the New York Federal Reserve reporting that financial institutions experience cyber attacks 300 times more frequently than other industries. This heightened risk is due to the sensitive customer data and personal identification information that they handle and the lucrative nature of potential breaches. Complicating this challenge is that the entire financial industry is going through digital transformation. While innovations like AI-driven investment platforms and digital banking have brought benefits, they have also expanded the attack surface, creating more vulnerabilities for threat actors to exploit.

Given these challenges and risks, regulatory compliance requirements have mandated that vulnerability management be an essential component of cybersecurity strategies for financial institutions. By implementing robust vulnerability management programs, companies can proactively identify and address potential weaknesses before they're exploited, reducing the risk of data breaches, financial losses, reputational damage, and legal liabilities. This approach not only maintains regulatory compliance requirements but also protects the institution, maintaining customer trust in their ability to handle money and information securely.

Built for Financial Services

Complex infrastructures, stringent compliance requirements, alert fatigue, fragmented data sources and struggling to achieve risk-based prioritization: how does the financial services industry mitigate systemic risk while improving operational resilience? The answer is risk prioritization and remediation, executed for the right findings, using efficient, collaborative workflows.

Armis Centrix™ for VIPR Pro – Prioritization and Remediation unifies risk, prioritizes response, identifies the owner, and operationalizes the remediation lifecycle. Armis consolidates detection tool findings and deduplicates alerts, extending from vulnerability scanners, on-premise hosts and endpoints to code, cloud services and application security tools. 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 automated prioritization based on the most urgent risks, specific to the financial services market.

Critical Features:

Unify

Ingest data from existing sources, including Armis Centrix™, EDR, on premise, cloud services, code, and applications. Reduce the security findings volume with ML deduplication, and correlate all findings.

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.

Assign and Remediate

Leverage AI-driven predictive capabilities to determine who is most likely responsible for the asset and the remediation. Benefit from bidirectional integrations with existing workflows and enable self-service for risk resolution.

Monitor and Report

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

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

Visit **Armis.com** to find out more

ARMIS

Key Differentiators that make Armis the go to approach:

- ✓ Streamline risk assessment & remediation
- ✓ Adaptable prioritization for risk identification
- ✓ Integrated asset inventory and enrichment
- ✓ Predictive AI for remediation ownership
- ✓ Consolidated remediation activity monitoring
- ✓ Effective collaboration through bidirectional workflows integrations
- ✓ Centralized visibility into risk posture
- ✓ Robust security measures to meet regulatory compliance requirements
- ✓ Improve security posture across the entire infrastructure (from credit card holders and frequent ATM users to large organizations with enormous amounts of financial data stored on a bank's networks)
- ✓ Protection of sensitive data and assets
- ✓ Reduce cyber attack-related financial losses and reputational damage

Why more businesses are trusting Armis to drive measurable outcomes

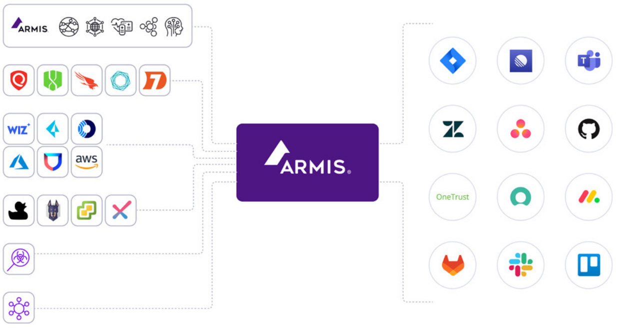
1 | 50-1 backlog reduction with alert consolidation and ML deduplication.

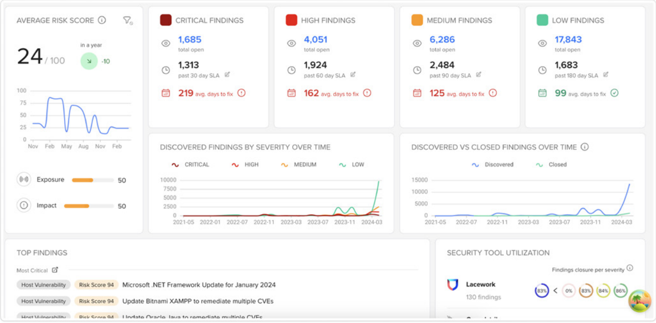
2 | 90% improved MTTR for prioritized findings

3 | 80% time savings by automating assessment

4 | 90% Remediation task efficiency improvement through ownership assignment and ticket automation

5 | 7x increase the number of closed findings on an annualized basis




AVERAGE RISK SCORE

24 / 100

in a year -10

Exposure 50

Impact 50

CRITICAL FINDINGS

1,685 total open

1,313 past 30 day SLA

219 avg. days to fix

HIGH FINDINGS

4,051 total open

1,924 past 60 day SLA

162 avg. days to fix

MEDIUM FINDINGS

6,286 total open

2,484 past 90 day SLA

125 avg. days to fix

LOW FINDINGS

17,843 total open

1,683 past 180 day SLA

99 avg. days to fix

DISCOVERED FINDINGS BY SEVERITY OVER TIME

DISCOVERED VS CLOSED FINDINGS OVER TIME

TOP FINDINGS

Most Critical

Host Vulnerability | Risk Score 94 | Microsoft .NET Framework Update for January 2024

Host Vulnerability | Risk Score 94 | Update Bitnami XAMPP to remediate multiple CVEs

Host Vulnerability | Risk Score 94 | Update Oracle Java to remediate multiple CVEs

SECURITY TOOL UTILIZATION

Findings closure per severity

Lacework 130 findings 83% < 0% 83% 84% 86%

Security findings overview in the Armis Centrix™ for VIPR Pro – Prioritization and Remediation dashboard

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

Visit **Armis.com** to find out more