Armis Centrix™ for VIPR Pro – Prioritization and Remediation

State and Local Government

Reduce Risk with More Operational Efficiency

Security teams at state and local governments are squeezed: they contend with a growing volume of alerts from their vulnerability scanners, while being stretched to guide IT, application and infrastructure teams on how to manage and reduce the government's technology risk. Teams that are already resource constrained spend too much of their time chasing down individual vulnerabilities, rather improving risk posture.

Built for State and Local Governments

Alert fatigue, resource constraints, limited budgets, personnel shortages, and competing priorities: how do state and local governments optimize the use of resources while minimizing exposure to the business? The answer is exposure 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 state and local governments.

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.

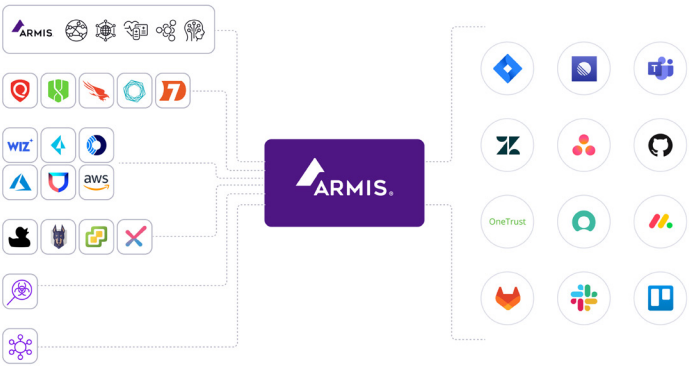
ARMIS

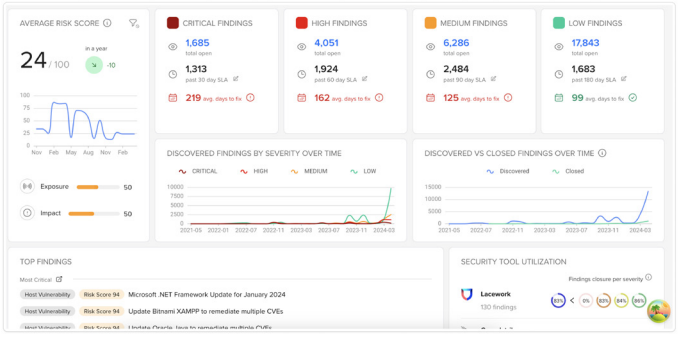
Key Differentiators that make Armis the go to approach:

- 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
- AI-driven automation for operational efficiency
- Whole-of-state approach

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





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

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