ARMIS®

SOLUTION BRIEF

Detect and Protect Against Ransomware Attacks with Armis Centrix™

Proactively detect ransomware attacks and reduce operational disruption

Introduction

Ransomware attack prevalence and impact have been steadily on the rise over the past several years, with no sign of slowing down. Ransomware is a tried-and-tested method of threat actors that prevents organizations from accessing their computer files, systems, or networks and demands a ransom for their return. It accomplishes this by encrypting all of the files on networked computers and forcing businesses to pay a ransom for the decryption key.

The average ransom in 2024 was $2.73 million, which is an increase of nearly $1 million from the previous year. The economic impact of ransomware attacks is severe, but the operational downtime of almost a full month can have devastating effects on business continuity, production, safety, and reputational trust.

Adopting a proactive approach to attack surface management, intelligent prioritization and automation are key to preventing ransomware attacks before they happen, and containing any impact on your organization.

Key Challenges in Preventing Ransomware Attacks

- 12% of organizations still rely on End-of-Support (EoS) Operating Systems, which are particularly susceptible to attacks.
- Attack surface expansion from traditional technology to IoT, OT, cloud, and medical devices makes it difficult to manage risks across every asset.
- Ransomware attacks have doubled in frequency over the past two years alone, with financial services, medical/healthcare/pharmaceutical and government/public sector companies feeling the greatest impact.
- The median ransomware payment skyrocketed from 200k in 2023 to $1.5M in 2024.
- Increase in the combination of weaponized vulnerabilities being used by threat actors in a single attack, as reported by Armis Labs.
- The emergence of Ransomware-as-a-Service and AI tools manipulate information and execute attacks on a massive scale.

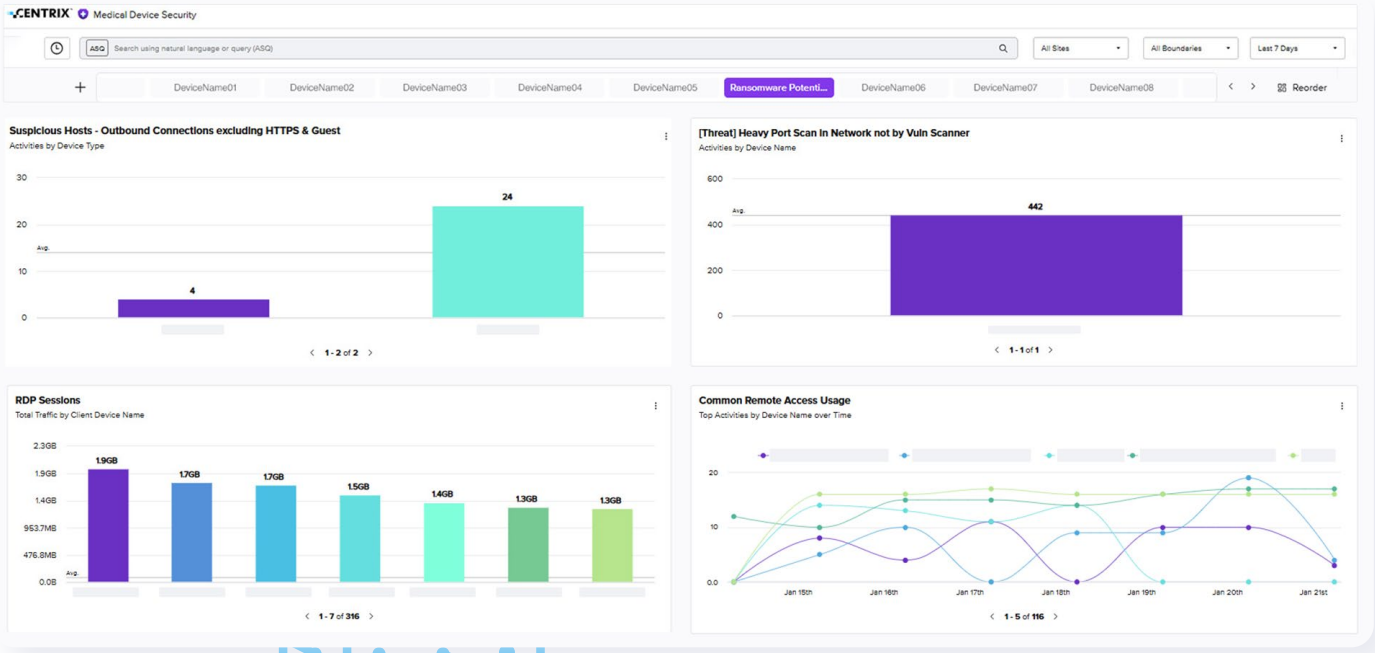
Proactively Protect Against Ransomware Attacks with Armis Centrix™

Armis Centrix™, the cyber exposure management & security platform, allows you move the dial from reactive to proactive and leverage best-in-class cybersecurity to get ahead of ransomware attacks.

With Armis Centrix™, you can:

- **Understand Organizational Assets and Risks** in Real Time: Defending the unknown is impossible. Identify and prioritize critical assets, data, and systems within your organization. Understand the potential impact of security threats and the specific risks your environment faces.
- **Empower with Timely and Accurate Asset Intelligence:** AI-powered asset intelligence engines can monitor billions of assets worldwide to identify cyber risk patterns and behaviors and enrich existing assets.
- **Follow the Threat Actors with Early Warning Detection:** Employ indicators such as honeypots, intelligence, and research to predict potential threats and make real-time assessments. Stay informed of emerging threats and tactics employed by attackers, and address CVEs before globally accessible knowledge agencies and corporations publish them.

- **Detect Anomalous Behavior Early and Take Action:** Traffic anomaly detection, advanced network segmentation, and policy automation takes the guesswork out of ransomware detection and allows you to take action immediately at a threat's most granular level.

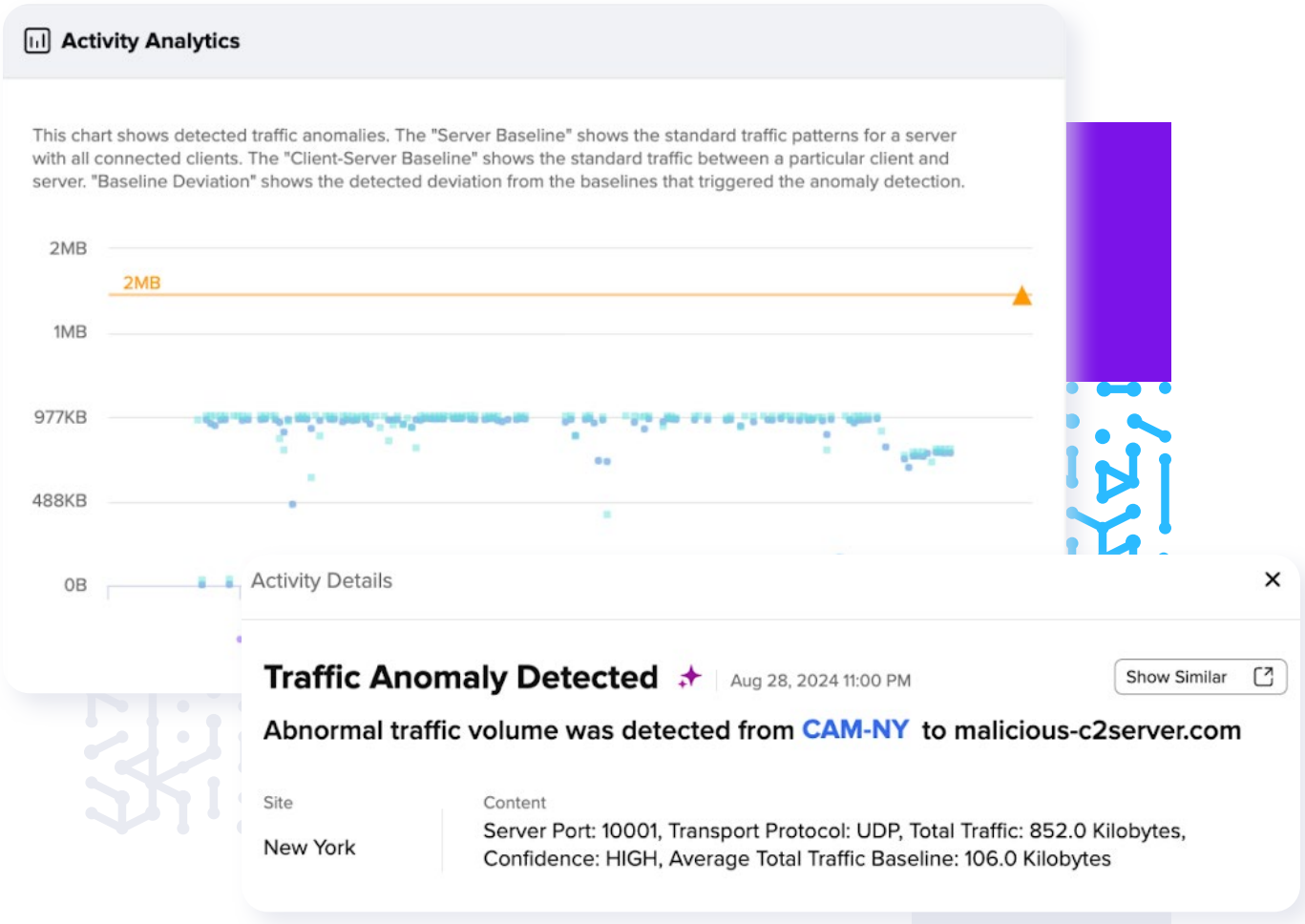


Here's How it Works

Anomaly Detection and Multi-Detection Engine

Modern cyberattacks are increasingly sophisticated and involve multiple stages. Imagine if you could detect malicious behaviors at their most subtle, granular level before they become a wide-scale attack. Armis Centrix™ provides a more accurate, intelligence-driven approach to aggregated anomaly detection, which ensures you are always one step ahead of potential threats.

Armis Centrix™ has a cloud-based threat detection engine that uses machine learning and artificial intelligence to detect when a device is operating outside its "known-good" baseline. Our multi-detection technology supports anomaly detection and policy-based detection for more comprehensive protection. Monitor any device's communication in your environment, and respond quickly and effectively to suspicious deviations.

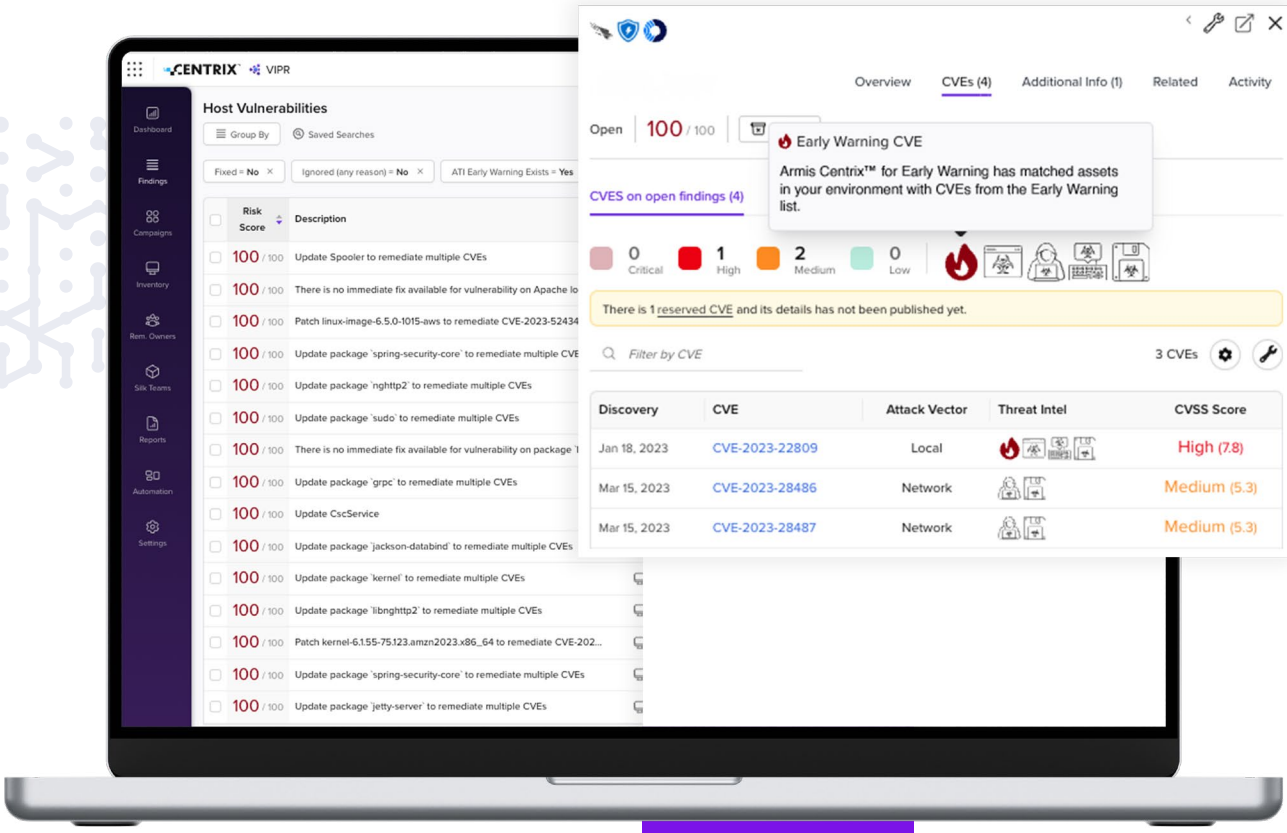


Early Warning Alerts

Armis Centrix™ leverages AI and machine learning that scours the dark web, to deliver an early warning system. These early indicators of potential attacks empower you with insights that let you take action before a vulnerability is announced, before an attack is launched, and before your organization is impacted.

Armis Centrix™ for Early Warning delivers real-time threat intelligence about tactics attackers use and their potential impact to protect against zero-day vulnerabilities and threats including ransomware. Prioritize mitigation based on the current threat landscape to remediate the biggest threats before attackers can leverage them, effectively moving the security posture from defense to offense.

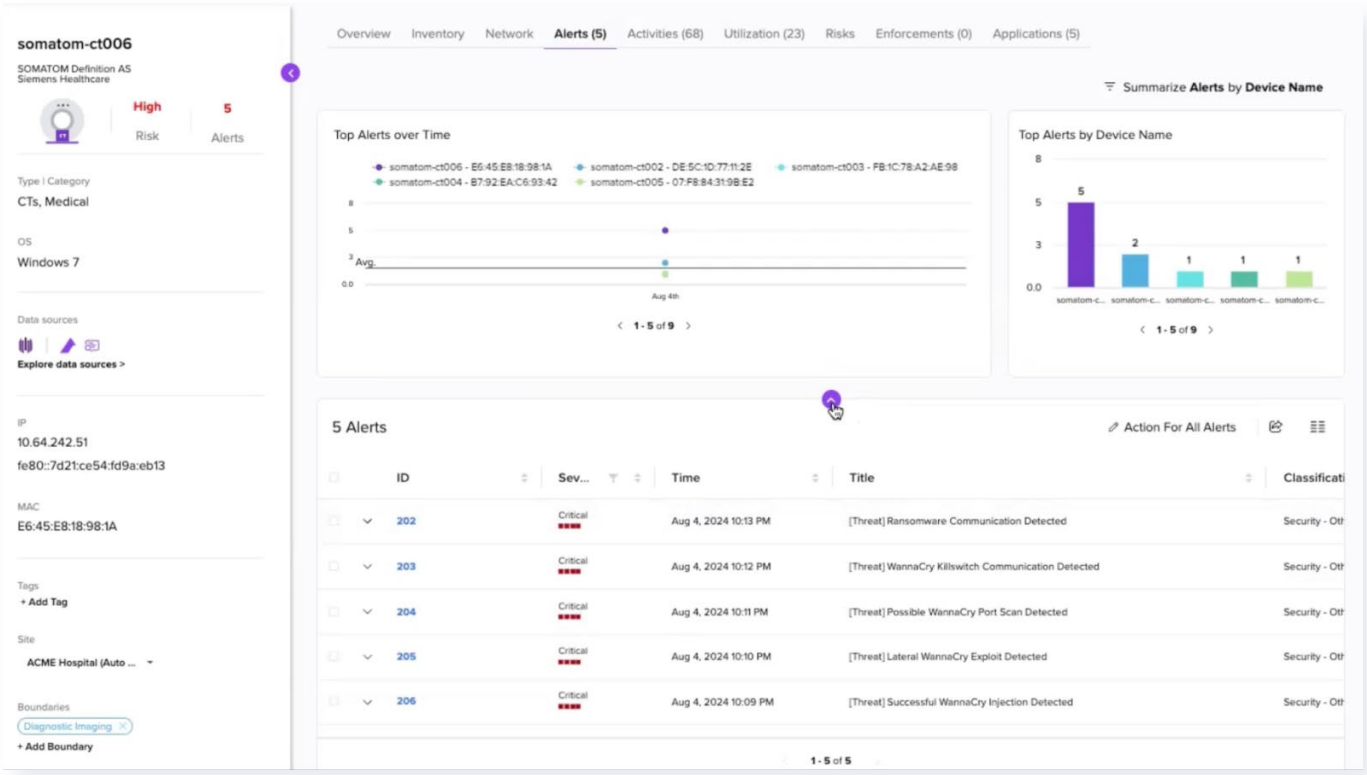
For the latest early warning insights from Armis Labs and information about emerging threats, visit https://www.armis.com/armis-labs/.



Ransomware Detection

Armis Centrix™ has advanced asset visibility and activity management that informs every step of ransomware detection and protection. Armis Centrix™ itemizes device activity including DNS queries, web surfing, and callouts to phishing or other suspicious domains, lateral movement and encryption. Immediately identify potential exploits and potential lateral movement and contain the threat. Simplify the view of which device is exploited and with what exploit. Armis Centrix™ sends automated alerts and can automatically create subtasks, execute playbooks and workflows.

Policy Enforcement can be set up per device type to ensure your business remains operational and services are not disrupted. Enforce actions, quarantine the device, remove network access, and take proactive measures against detected threats.

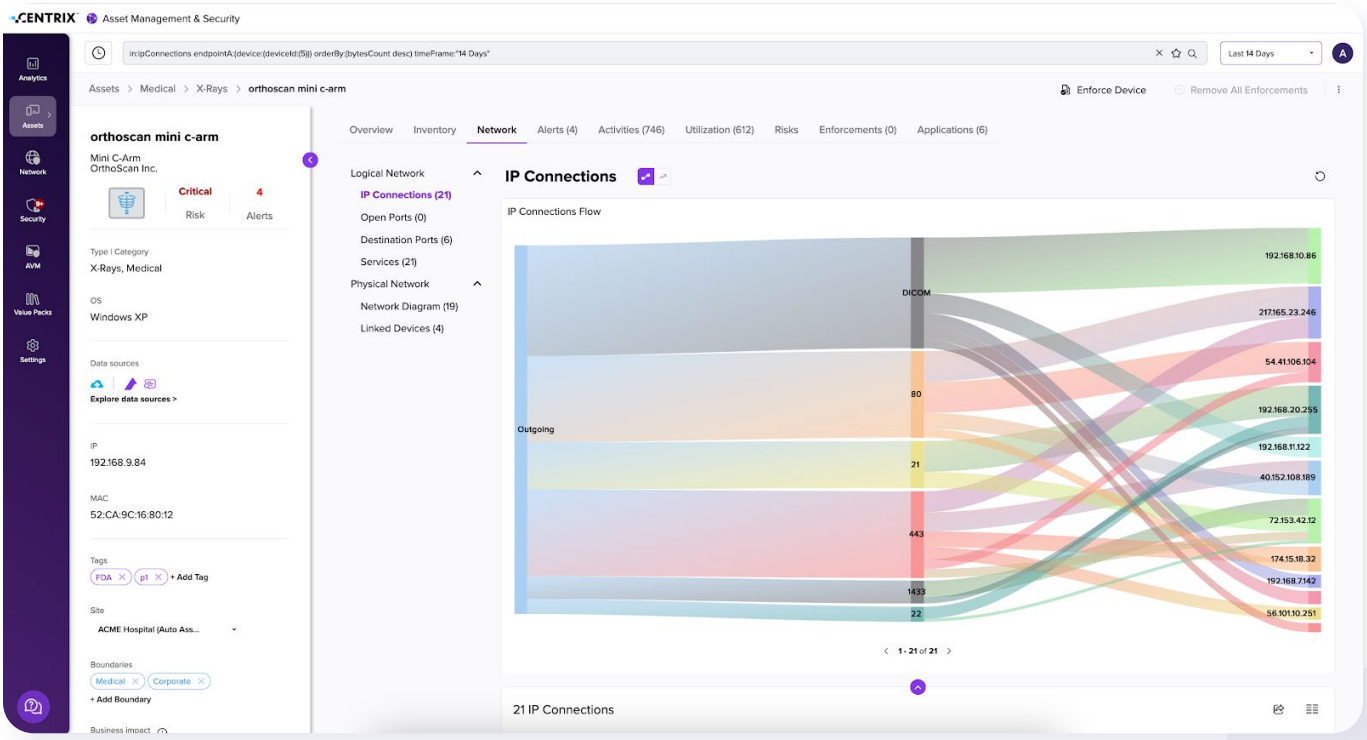


How Armis Can Help

Network Segmentation

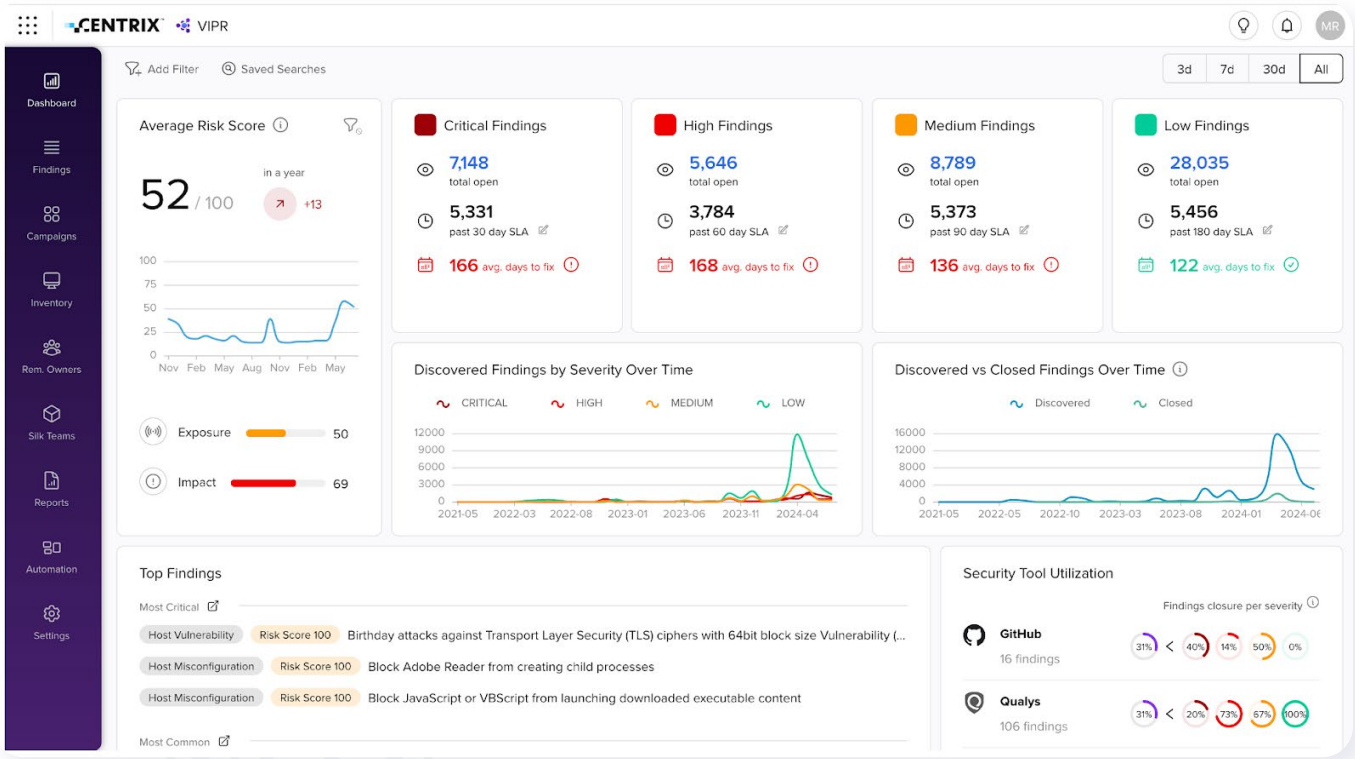
Without proper segmentation, a single compromised device can be used to impact the main network, resulting in outages or disrupted services. Network Segmentation helps prevent this by limiting the communication between devices and reducing the risk of east/west lateral movement across networks and device types. In turn, this helps prevent ransomware attacks, ensuring the security of every device, data, and other critical systems.

Armis Centrix™ simplifies the segmentation process and helps achieve attack surface reduction in a record time. Discover, inventory and accurately categorize every asset and continuously monitor for traffic insights. Armis supports both manual segmentation for single or small batches of devices and complete automation based on device properties like Type, Manufacturer, Model, and Risk for faster incident response.



Vulnerability Prioritization and Remediation

The true operational and business risk of any device or vulnerability requires the context of its individual technology environment. Armis Centrix™ for VIPR – Prioritization and Remediation enables security teams to transform their vulnerability management programs to more efficiently, systematically, and collaboratively remediate risks they prioritize. 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. Armis enables a consolidated, proactive approach to attack surface management to effectively action ransomware alerts once they are detected.



The Armis Difference

- **Comprehensive Protection of the Entire Attack Surface**
  Only Armis Centrix™ allows you to see, secure, and manage the risk of every device, whether IT, OT, IoT, or IoMT, covering every gap, threat, and vulnerability on one platform.

- **Risk Prioritization and Remediation**
  Only Armis prioritizes risks based on the organization's most critical assets, and when, where, and how it is used. Save hours of manual effort and quickly resolve the top-priority findings.

- **Best-in-Class Asset Intelligence**
  Only Armis has an AI-driven Asset Intelligence Engine an asset security data lake that understands "known good" behavior baselines for over 5 billion types of assets. Identify, classify, aggregate, and enrich assets with the context needed for effective prioritization.

- **Accurate Profiling and Threat Detection**
  Quickly discover, contextualize, enrich, and profile every asset using hundreds of pre-built integrations, network telemetry, and an AI-driven Asset Intelligence Engine. Early Warning data adds awareness of potential risks relevant to your industry.

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
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial