ARMIS®

SOLUTION BRIEF

Solving Foundational Cybersecurity Challenges

Armis Centrix™ integrates with hundreds of existing IT and Security tools to aggregate, deduplicate and normalize data for every asset in your inventory.

The Problem

The average security organization has 76 security tools to manage – EDRs, vulnerability scanners, MDMs, CMDBs, cloud environments – so many tools they need to look at on a daily basis. These solutions are all managed separately, creating independent data points each of interest to the organization.

This siloed sea of data makes it difficult to answer simple questions like:

- How many Windows devices do I have?
- How many servers are missing a required endpoint security agent?
- How many legacy Operating Systems and applications do I have on my network?
- Am I going to pass my compliance audit?

Even though the answers to all the previous questions are there, you can't easily extract them. Even if you're able to manually run around from tool to tool and pull information out, many times you can't know how they coincide, let alone deal with cases where they conflict with one another. This is what we call the Security Mess.

How Armis Helps

Armis Centrix™ integrates with hundreds of existing IT and Security tools to aggregate, deduplicate and normalize data for every asset in your inventory. Through additional intelligence derived from its AI-driven Asset Intelligence Engine, Armis is also able to understand the context around every asset so IT and Security teams can make data driven decisions.

Foundational Use Cases

Full Asset Inventory and Enrich CMDB

IT & Security Hygiene and Gap Analysis

Risk Management

Internal and External Compliance Reporting

IT & Security Hygiene and Gap Analysis

Armis helps validate the implementation of existing security controls (EDR, vulnerability scanners, etc.) and identify gaps in deployment. It finds all assets that are not protected, and helps remediate the issue quickly. Follow the progress of this project live in Armis, and understand its subsequent influence on your security posture, without spending needless time on manual labor.

Risk Management

After identifying a device, Armis Centrix™ calculates a risk score based on multiple factors. Our Risk Factors provide a comprehensive assessment and prioritization approach, including precise remediation actions, streamlining the risk-mitigation process. By offering specific steps to address each risk, your security team take proactive steps to reduce your attack surface and help you comply with regulatory requirements.

Internal and External Compliance Reporting

Armis helps you adhere to your internal compliance requirements and prepare for external audits. Whether it's NIST, CIS Controls, GDPR, or other regulations, you can use Armis to ensure your security standards are met, avoid human errors in data collections, and pass your audits with flying colors.

Full Asset Inventory and Enrich CMDB

Many security teams rely on the CMDB for asset information. Armis ensures your CMDB is complete, accurate, and up-to-date, and includes all additional information you want to add to it.

Network Segmentation and Enforcement

Without proper segmentation, a single compromised device can be used to impact the overall network. Network segmentation helps prevent this by limiting the communication between devices and reducing the risk of east/west lateral movement across networks and devices. A visual matrix represents cross boundary communications, to assist with planning, enforcing and identifying gaps in existing segmentation projects.

Threats Detection and Response

Armis network detection and analysis capabilities provide security operations teams with full visibility to network-based threats in their environment. This allows teams to make informed, data-driven security response decisions based on data Armis collects from the network.

Summary

Armis Centrix™ offers a single-source-of-truth for all data sources and eliminates the need for manual cross-referencing, saving organizations valuable time and reducing the risk of errors. By leveraging contextual intelligence provided by our AI-driven Asset Intelligence Engine, organizations can prioritize remediation efforts based on risk and criticality. Lastly, by streamlining the process of identifying and managing all assets, Armis helps organizations maintain a strong security posture, reduce their attack surface, and protect their brand.

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