CASE STUDY

Global Financial Services Organization Meets Its Goal of 100% Visibility as Part of Its Security Maturity Strategy

Multiple Armis integrations correlate device data to help surface and prioritize vulnerabilities

Industry

Financial services

IT environment

Over 5,000 employees worldwide and thousands of devices.

Introduction

This global financial services organization prides itself on striving for excellence in all areas—including cybersecurity. Armis was deployed as part of its security maturity initiative and provided the organization with 100% visibility to all assets.

Armis integrates with the extensive set of solutions in the organization’s security architecture amplified and correlated device data to help guide vulnerability management by identifying and prioritizing the most critical vulnerabilities to be remediated to reduce their attack surface.

Also, thanks to Armis, the security team was able to perform gap analysis to determine which devices lacked up-to-date and mission-critical security protections. By filling these gaps, the organization achieved a more robust risk profile and can confidently claim 100% coverage at audit time.

When it comes to securing its technology environment, this global financial services organization believes in being proactive and meticulous in its best practices. With over 5,000 employees across multiple locations worldwide, the technical estate is far-reaching, with thousands of devices in use.

The organization has a large arsenal of security tools— everything from vulnerability scanning to endpoint detection and response (EDR) to zero trust solutions. “We have nearly every tool in the world,” said the manager of security engineering. “But one thing was lacking: 100% visibility into all assets.”

He pointed out that the organization is on a security maturity mission, with the goal of being “the best in its sector.” He and his team conducted a self-audit and determined that one of the biggest gaps was visibility into the entire environment. He further went on to explain that it quickly became apparent that he and other teams lacked sufficient data on a significant portion of the organization’s assets in their configuration management database (CMDB).

Thousands of assets discovered during Armis PoV

The manager learned about Armis at a Black Hat Conference, where he was given a demo. He and his supervisor immediately agreed to a proof of value (PoV). As part of the PoV, he worked with his team to integrate close to 20 products in the existing technology stack to get a clearer picture of how Armis could help him and his team gain broader visibility by correlating relevant data from multiple sources. The rationale was to improve vulnerability management by gaining full visibility to all risks in the organization's environment and perform gap analysis for all security tools.

While the organization's CMBD team claimed that the organization had a little over 5,000 assets, Armis "uncovered about three to four times as many assets in just two weeks. Prior to that, the manager's supervisor spent many months manually building in-house tools that pulled application programming interfaces (APIs) from various tools into a database and correlated the data—everything that Armis could do in a matter of weeks.

"I can say, with complete confidence that Armis has given us a view of 100% of the assets in our environment," he said. "We're cross-referencing every tool, and that is getting us to the visibility we are after."

Integrations with security-related tools enhance and accelerate vulnerability management

After the Armis PoV, the manager showed the results to his supervisor, and it was "love at first sight." Armis revealed major gaps in the CMDB. The manager of security engineering and his team are using the gap analysis provided by Armis to determine which assets lack mission- critical security protections, such EDR.

Challenges

- Gaining visibility to all assets in the environment
- Extracting deeper insights on vulnerabilities
- Improving accuracy of the CMDB
- Maintaining compliance with industry and government regulations

At the top of the manager's to-do list is completing Armis integrations with the remaining software tools and services in the organization's extensive security architecture. These include directory services, virtual device management, advanced firewalls, vulnerability management, network mapping software, cloud computing platforms, identity and access management, and others. Through these integration efforts, the financial services organization will have a single dashboard that unifies data feeds and provides broader, more in-depth insights into assets that will help teams identify and remediate vulnerabilities.

The manager is currently working with Armis on three additional new integrations. This will not only help the financial service organization, it will also expand the Armis integration portfolio and help other Armis customers. "Armis is like an API database. If there's an API, Armis can scrape it and correlate the data," noted the manager of "security engineering. "I'm sure some good partnerships can come out of this."

Over the past several years, the financial services organization has been through a rapid growth phase, with nearly 20 mergers and acquisitions (M&As). For the technical teams, that means onboarding new network infrastructures, servers, and data centers. Armis plays a key role in streamlining those efforts and providing an accurate baseline of assets. "Without the visibility layer provided by Armis, things would fall through the cracks. Prior to Armis, we had to rely on tribal knowledge to know whether certain things existed or not," he remarked.

Armis fills in the gaps to reduce risk and maintain compliance

The financial services sector is one of the most heavily regulated industries in the U.S. Financial institutions are required to comply with an ever-expanding list of regulations, which include meeting stringent cybersecurity standards. Identifying and remediating vulnerabilities to prevent exploitation by attackers is a key focus at this organization and an integral part of its risk management effort.

Armis Results

- 100% visibility to all assets across the entire estate
- Integrations with cybersecurity related tools providing enriched device data
- A single, centralized dashboard for monitoring and compliance reporting
- Prioritization of vulnerabilities for faster remediation
- Less time spent on building home-grown API integration tools
- Simplified M&A integrations

As the manager observes, “There’s only so much vulnerability management tools can do, and they require a lot of ‘care and feeding.’ Armis provides risk-based assessments and gap analysis to ensure we have complete coverage. I like having the confidence to be able to say to an auditor that we have 100% coverage.”

He is currently in the process of creating key performance indicators (KPI) reports to measure security coverage. With its risk-based policy model, Armis can provide metrics for accurate assessment and continuous improvement.

“The risk-based approach to vulnerability is huge for us. It’s like finding the needles in the haystack first. If I went into “our current vulnerability manager, I would probably find over a million unpatched vulnerabilities. But in my mind, that’s not a real number,” explains the manager. “Armis can cut through the noise and pinpoint the most vulnerable assets, which may boil down to a few hundred based on Armis’s out-of-the-box criteria. It’s pretty nice to be able to sift through all that data within seconds.”

Next step: CMDB integration

One of the initiatives on the horizon is integrating Armis with the CMDB to enrich asset data. The project team, consisting of six engineers, have been working on manually integrating the asset warehouse with other tools for the past several months. Now, with Armis having done the heavy lifting by identifying thousands of previously unknown assets, their job will be made much easier.

“Our vulnerability management team is excited about being able to skip about a year’s worth of engineering work. Thanks to Armis, they can go from zero to 100 really quickly and be able to better identify the data gaps in our CMDB,” said the manager of security engineering.

Once the Armis integration with the CMDB is completed, the financial services will have a comprehensive single source of truth, which will help teams identify risks, prioritize vulnerabilities, and maintain compliance.

“I can say, with complete confidence that Armis has given us a view of 100% of the assets in our environment. We’re cross-referencing every tool, and that is getting us to the visibility we are after.”

Manager of Security Engineering
Financial

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
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial