ARMIS®

SOLUTION BRIEF

Securing Financial Services with Armis Centrix™

Mitigate Systemic Risk and Improve Operational Resilience

Overview

Cybersecurity risks have become a critical concern for financial institutions, with increasing digital transformation and innovation expanding attack surfaces and exposures. Financial institutions, including banks, insurance, credit unions and investment firms, must balance technological innovation with resilient security measures and compliance with dynamic regulatory requirements to stay competitive.

Financial institutions are left struggling with a myriad of challenges, including incomplete asset inventories, siloed security operations with too much data and no unified view, manual prioritization of risk, and evolving regulatory requirements including PCI-DSS, the SEC's expanded disclosure requirements and those from the FDIC, NCUS, FFIEC, and NYDFS and DORA.

And, the stakes are high; cyber incidents can result in immense costs, averaging $5.9 million per data breach for the financial sector in 2023.

Armis Centrix™ delivers the comprehensive visibility, security, and cyber risk management capabilities financial institutions need to meet these challenges head-on and ensure integrity of financial data and records.

The Current Challenges in Financial Services Cybersecurity

1. Expanded Attack Surface and Increased Cyber Threats

ATMs, customer service kiosks, physical security devices, and other non-traditional hardware and software used for financial services can't always be seen or protected with traditional IT security tooling, leaving gaps in coverage and introducing cyber risk.

Innovations like AI-driven investment platforms, IoT-powered services, and increasingly digitized Building Management Systems (BMS) have revolutionized financial services—but have also created new vulnerabilities. Data from a recent survey shows that 74% of financial institutions experienced at least one ransomware attack in the past year, while 41% faced multiple breaches, according to the 2024 Armis Cyberwarfare Report.

74% of financial institutions experienced at least one ransomware attack in the past year, while 41% faced multiple breaches, according to the 2024 Armis Cyberwarfare Report.

2. Siloed Data and Manual Processes

The average financial institution uses 76 different cybersecurity systems, creating fragmented, duplicated, and often conflicting data. Without a consolidated solution, institutions rely on manual processes and spreadsheets for steps like asset enrichment and prioritization which can leave gaps in coverage. The end result is an increased exposure to threats.

76 different cybersecurity systems, creating fragmented, duplicated, and often conflicting data.

3. Regulatory Complexity

Keeping pace with constantly evolving regulations—such as DORA, PSD2, and the Sarbanes-Oxley Act—demands precision and agility. Financial institutions must maintain detailed, auditable records of cybersecurity efforts while aligning operations to stringent compliance frameworks. Additionally, there is greater scrutiny of security operations and processes to identify, address, and report on cyber risk as per regulation requirements.

4. Vulnerability Management

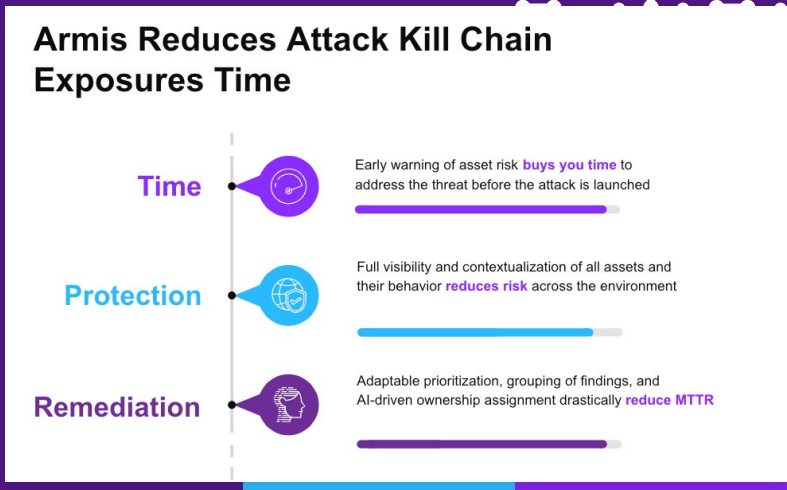
There were 3,348 cyber incidents in the financial industry in 2023, the highest number in ten years. Prioritizing and remediating vulnerabilities in a rapidly growing and complex attack surface requires comprehensive context and cross-functional collaboration. Yet most tools do not enable vulnerability management teams to identify the most critical and urgent risks and provide actionable guidance to remediation teams, leaving institutions overwhelmed and at risk.

3,348 cyber incidents in the financial industry in 2023, the highest number in ten years.

The Armis Centrix™ Platform

Armis empowers financial institutions to take control of their complex infrastructure to see, protect and manage their assets and data in real-time. Armis Centrix™ is a seamless, frictionless, cloud-based platform that proactively identifies and mitigates all cyber asset risks, remediates vulnerabilities and security findings, blocks threats and protects your entire attack surface.

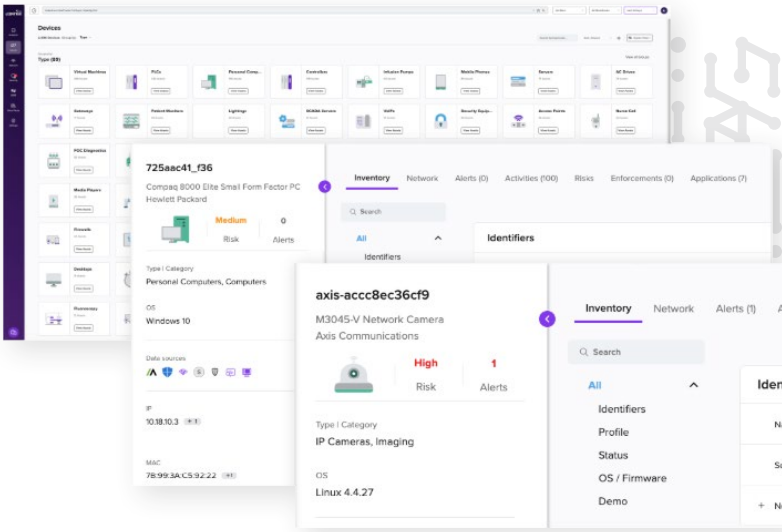
With Armis, financial institutions can detect and stop attacks, control the blast radius and ensure their most critical assets are protected.

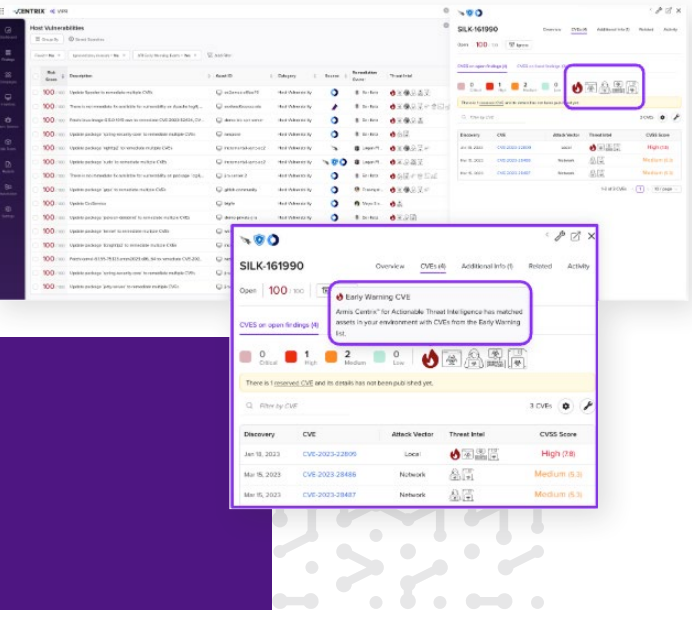


Complete, Real-Time Visibility

By providing complete asset visibility across all asset types, Armis Centrix™ gives financial services organizations complete control over their assets. It allows them to pull asset-related data from relevant IT and security tools to obtain rich, contextual intelligence about each asset in the inventory. The data is not only aggregated but also deduplicated and normalized. Armis Centrix™ then pushes this data to the CMDB to create an accurate and comprehensive view of all assets, complete with enriched contextual data.

In the financial services industry, achieving complete visibility is essential, and Armis' cloud, OT and IoT asset inventorying is at the forefront of this endeavor. The platform provides real-time insights into network assets with the option to deploy smart active querying to proactively quiz your network. This facilitates classifying devices and applications to differentiate authorized from unauthorized ones, across every type of device including IoT.





Business Critical Risk Prioritization and Remediation

Armis Centrix™ empowers financial institutions and banks to stop attacks before they happen. By combining early warnings of the vulnerabilities that matter with the context of all critical security findings and asset context, teams can focus resources on the highest-priority risks and reduce the exposure window for what may impact the business most.

This involves integrating vulnerability severity, asset profiling and contextualization, and early warning intelligence to automate prioritization of urgent risks to

the organization and operationalize the remediation lifecycle. Early warnings provide insights into the vulnerabilities that threat actors are exploiting in the wild or are about to weaponize, allowing financial institutions and banks to understand their impact and take preemptive action. The consolidated approach allows teams to understand which vulnerabilities truly matter, which assets in their environment are exposed, how critical those assets are within a business or compliance context, and who is responsible for remediation steps. Consolidating, de-duplicating, and contextualizing findings, along with asset profiles, attributes, and custom risk weightings, allows teams to prioritize based on the risks in their environment and what truly matters to their organization. With bidirectional integration to ticketing workflows and automated assignment of owners of remediation tasks, and centralized visibility across workflows, security teams can efficiently operationalize remediation and monitor progress to close the exposure window.

Address the Mounting Pressure of Financial Compliance Frameworks

Armis Centrix™ assists financial institutions and banks in navigating the complex landscape of regulatory compliance by providing comprehensive visibility, security and control over all connected assets, both IT, IoT and OT. The platform enables security teams to monitor and assess their asset inventories against regulatory standards in real-time, ensuring that all devices are accounted for and compliant with frameworks. By offering automated risk assessments and alerts, Armis helps financial institutions and banks quickly identify potential non-compliance issues and respond proactively, minimizing the risk of regulatory fines and penalties. Armis facilitates audit readiness by streamlining the documentation and reporting processes, allowing financial institutions and banks to efficiently demonstrate compliance to regulators. This integrated approach supports the maintenance of cybersecurity resilience while meeting stringent regulatory demands, ultimately helping financial institutions protect their reputation and consumer trust.

Bridge the IT/OT Gap

Using network segmentation visualizations to manage your IT/OT attack surface dramatically improves your cyber and operational resilience. With Armis Centrix™, you can display connections based on segments, asset types and defined boundaries.

As financial services companies continue to adopt cutting-edge technology to streamline operations, enhance customer experiences, and optimize resources, their reliance on smart building systems grows in parallel. Building Management Systems (BMS), often referred to as Building Automation Systems (BAS), have become vital components for managing HVAC systems, lighting, physical security, and other building functions. Whether connected assets are located onsite or in distributed locations, the Armis Centrix™ platform's holistic approach makes it easy to inventory and quickly understand all of them. Get visibility of financial services BMS assets, including thermostats, sensors, elevator controllers, and fire and safety systems. And keep a close eye on every other connected asset, including smart devices like TVs, IP cameras, and printers with comprehensive asset details.

Secure Innovation

Armis Centrix™ provides financial institutions with the tools necessary to secure their innovative infrastructures and maintain a competitive edge without compromising on security. By offering comprehensive visibility, security and control over all connected assets, Armis Centrix™ ensures that the most advanced OT systems are continuously monitored and safeguarded against potential vulnerabilities. Its proactive risk assessment capabilities and automated alerts enable banks to detect and mitigate risks in real-time, safeguarding the innovative environments they have worked hard to develop. With Armis Centrix™, financial institutions can confidently pursue their competitive strategies, knowing that their cutting-edge infrastructures are protected and compliant with the highest cybersecurity standards. This protection not only maintains operational integrity but also encourages other financial entities to follow suit in enhancing their workplace experiences, contributing to a safer, more innovative industry landscape.

Real Results for Financial Institutions

Financial institutions that partner with Armis consistently achieve better security outcomes, as demonstrated by this case study of a global financial services organization.

Case Study Snapshot

This U.S.- headquartered organization faced serious challenges in managing a growing inventory of IT, cloud, and remote assets. With conflicting data from over a dozen sources, they struggled to achieve an accurate view of their environment. By implementing Armis Centrix™, the institution was able to:

- Achieve Comprehensive Visibility of all assets in real time.
- Consolidate and Reconcile Data across multiple systems into a centralized platform.
- Streamline Vulnerability Remediation, saving time and reducing exposure.
- Build a trusted, collaborative relationship with Armis, which worked closely to resolve challenges and implement improvements.

As the Director of Security Engineering exclaimed, “Armis has been critical in giving us a single source of truth for asset management and vulnerability detection.”

Real Results for Banks

Banks that partner with Armis see transformative improvements in security and operational efficiency, as shown in this case study of a leading international bank.

Case Study Snapshot

This investment bank, operating across multiple regions, faced challenges with fragmented asset management systems, increasing cyber threats, and the need for fast and accurate execution of orders to drive key business outcomes. By adopting Armis Centrix™, the bank was able to:

- Gain 360-Degree Visibility into IT, IoT, and OT assets across all branches and regions.
- Centralize Asset Management, integrating data from legacy systems into one unified platform.
- Ensure Fast and Accurate Execution of Orders by streamlining operations and reducing system vulnerabilities.
- Proactively Address Threats with automated risk prioritization and streamlined incident response.
- Improve Compliance Reporting by providing accurate, real-time audit data to regulators.

As the Chief Information Security Officer shared, “Armis has revolutionized how we manage and protect our assets, enabling us to stay ahead of constantly evolving threats and deliver seamless, secure services to our clients.”

Real Results for Insurance Companies

Insurance companies leveraging Armis experience enhanced security and operational control, as highlighted in this case study of a major global insurer.

Case Study Snapshot

This insurer, managing a vast network of remote offices, third-party vendors, and connected devices, faced challenges in securing their operations, meeting regulatory requirements, and ensuring adequate cyber insurance coverage. Partnering with Armis Centrix™ allowed them to:

- Identify and Mitigate Risks Across Distributed Assets, including IoT and third-party devices.
- Simplify Regulatory Compliance by providing clear, centralized visibility and audit-ready data.
- Enhance Cyber Insurance Readiness by delivering detailed insights into risk exposure and security posture.
- Reduce Downtime with proactive monitoring and faster incident response.
- Strengthen Vendor Security through enhanced visibility into third-party systems and integrations.

According to the Vice President of Technology, “Armis has been a game changer in helping us secure our operations, comply with regulations, and protect our customers' trust.”

Why Financial Institutions Choose Armis

1. **Enhanced ROI**
   Reduce MTTR by up to 90% and eliminate redundant manual labor.

2. **Cyber Resilience**
   Ensure complete asset discovery and secure all connected devices.

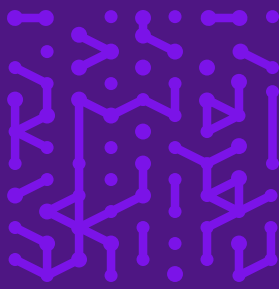
3. **Mitigate Risk**
   Integrate vulnerability severity, asset profiling and contextualization, and early warning intelligence to automate prioritization of urgent risks to the organization and operationalize the remediation lifecycle.

4. **Regulatory Assurance**
   Maintain compliance with evolving compliance standards and security frameworks with minimal overhead.

5. **Operational Efficiency**
   Automate routine tasks for quicker responses and resource optimization.

6. **Integration-First Approach**
   Built to integrate with your existing security stack, Armis Centrix™ enhances collaboration across departments and automates enforcement through trigger-based actions.

7. **Flexible and Non-Intrusive Deployment**
   Armis Centrix™ deploys without impacting system stability. Insights are available within minutes of deployment.



Secure Your Future with Armis Centrix™

With Armis Centrix™, financial institutions can tackle the most pressing cybersecurity challenges, from securing complex IT and OT environments to maintaining regulatory compliance and pushing forward innovation without risk.

Trusted by industry giants and supported by unmatched expertise, Armis stands ready to deliver the visibility and control financial institutions need to stay ahead of emerging threats.

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