INDUSTRY SPOTLIGHT SERIES

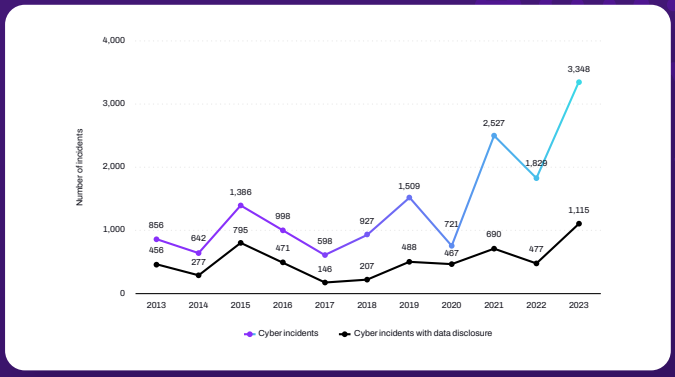
Financial Services

Top Trends

Attacks are on the rise. 74% of financial institutions experienced at least one ransomware attack in the past year, while 41% faced multiple breaches.

Competitive Innovation drives progressive change but also increases the attack surface.

Financial institutions are shifting their cybersecurity strategies from chasing compliance frameworks to proactively mitigating risk.



Number of cyber incidents in the financial industry worldwide (2013 to 2022) — **Statista**

Why is the Financial Services Industry Suffering?

Expanded Attack Surfaces and Cyber Threats

Innovations like AI investment platforms, digital banking, and increasingly digitized Building Management Systems (BMS) designed for an enhanced employee experience have revolutionized the financial sector—but have also created new vulnerabilities.

Siloed Data and Manual Processes

Without a centralized solution, institutions rely on spreadsheets and manual processes, which leave gaps in operational resilience and increase exposure to threats.

Regulatory Complexity

Keeping pace with constantly evolving regulations—such as PCI-DSS, the SEC's expanded disclosure requirements and those from the FDIC, NCUS, FFIEC, and NYDFS and DORA—demands precision and agility.

Vulnerability Management

Prioritizing and remediating vulnerabilities in a rapidly growing attack surface requires precise context and coordination. Yet most tools lack the capability to distinguish between critical and low-priority threats, leaving institutions overwhelmed and at risk.

Interested to learn how Armis delivers improved operational resilience while mitigating risk

for the financial services industry?

READ THE SOLUTION BRIEF

74%

of financial institutions experienced at least one ransomware attack in the past year.

76/systems

The average financial institution uses 76 different cybersecurity systems, creating fragmented, duplicated, and often conflicting data.

3,348

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

98%

98% of threat actor motives are for financial gains.

INDUSTRY SPOTLIGHT SERIES

Financial Services

Reports show attackers actively use known vulnerabilities that are several years old, often because organizations haven't properly patched or addressed them.

60% of compromises are from known vulnerabilities while the top 10 vulnerabilities in 2023 were discovered before 2020.

60% known vulnerabilities

Top 10 were discovered before 2020

Personas

CISO

Focuses on overseeing IT and cyber risks. The CISO prevents IT security breaches.

Challenges:

- Staying up-to-date with local and global security challenges, new technologies and compliance issues
- Delivering strategy and response reports to non-technical board and business leaders
- Liaise with Chief Compliance Officer to adhere to ever-growing list of compliance requirements

CTO/VP of IT

The CTO/VP of IT is responsible for overseeing the development and dissemination of technology for external customers, vendors, and other clients to help improve and increase business. They may also deal with internal IT operations if a company is small and doesn't have a chief information officer.

Challenges:

- Being the lead innovator and creative mind behind new technology solutions
- Listening to customers to deliver products that provide value

Risk Vulnerability Manager

The risk vulnerability manager manages the process of reducing vulnerabilities across the attack surface by prioritizing remediation based on the risks they pose to her organization.

Challenges:

- Prioritizing vulnerabilities based on risk
- Mitigate likelihood of a vulnerability being exploited

"Armis Centrix™ has been essential in providing a single source of truth for asset management and vulnerability detection. It has allowed us to automate processes and achieve operational resilience. Instead of working in silos and chasing compliance requirements, we now focus on mitigating risk with a holistic cybersecurity strategy. We've gained situational awareness, proactive vulnerability prioritization and remediation, and compliance reporting has become a seamless byproduct."

— **CISO, Financial Services Organization**