



Cybersecurity Strategies for Financial Institutions

Cybersecurity threats are on the rise and evolving constantly. Financial institutions worry about data theft and exfiltration, phishing, ransomware, and damage to the brand/reputation. Many have significant budget constraints standing in the way of further investment in security. This report examines the ways financial institutions are protecting their assets in an ever-evolving cyberthreat landscape.



Today, the biggest brands in banking, capital markets, insurance, and fintech trust Akamai to transform the cloud from a chaotic place with unpredictable performance and hidden threats into a secure, reliable, and cost-effective environment to do business.

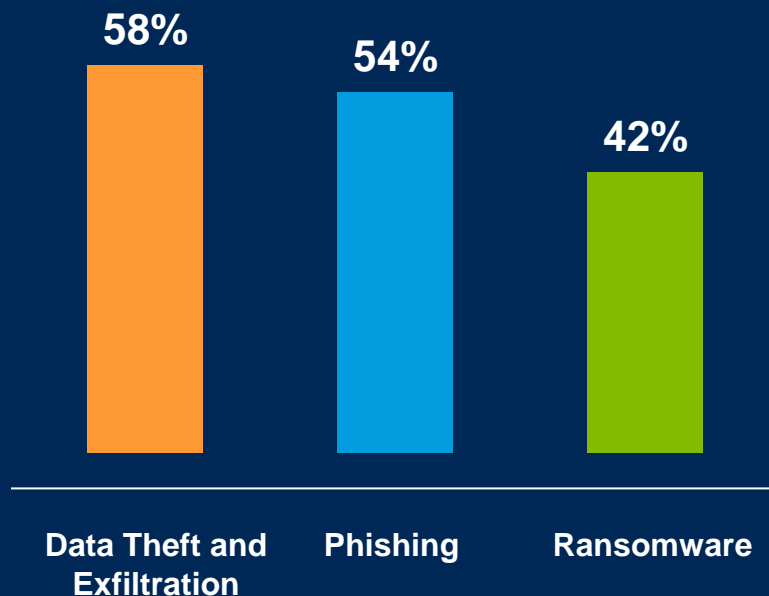
Data theft and exfiltration top security risk

Data theft in financial institutions extends beyond breaching security; it serves as a gateway to identity theft, financial fraud, and malicious activities, causing significant financial losses for both customers and institutions. Compliance concerns heighten with regulations like the Payment Card Industry Data Security Standard (PCI DSS), emphasizing the need to safeguard customer data. Intellectual property and trade secret theft directly jeopardize market standing, leading to severe penalties, fines, and reputational damage.

Recommendations:

- Conduct regular risk assessments
- Gain visibility to better understand anomalies, as well as good behaviors
- Stay informed about the evolving threat landscape through active membership in FS-ISAC

Which cyberthreat is a top concern for your business?



API vulnerability testing, adapting protections to evolving API attacks, and aligning security and development teams are key concerns.

1/3

of respondents are concerned with a lack of visibility into API attack activity

38%

say that monitoring, detecting, and mitigating API attacks would improve with improved investigation and threat hunting capabilities

42%

are concerned with their lack of continuous API discovery and inventory

What are your main concerns with monitoring, detecting, and mitigating API attacks?

Challenge:

APIs are fueling the rapid growth of market-changing initiatives in financial services, such as:

- Open banking
- Banking as a service (BaaS)
- Embedded finance
- Buy now, pay later (BNPL)

... but can expand the attack surface with:

- Shadow APIs
- Vulnerable APIs
- API abuse, where attackers use APIs in ways not intended by the organization that created them

Recommendations:

Extend your API security posture across the complete array of API threats, through these important strategies:

- Expand your thinking about API attacks
- Analyze significantly more data about APIs
- Harness APIs to spot abuse

Financial institutions need visibility so that developers, application owners, and security teams can identify and mitigate API security risks using security controls that are sophisticated enough to address this complex and fast-evolving threat landscape.



Financial services security leaders are concerned about the rise in DDoS attacks

80%

of respondents say operational disruption is a top concern

68%

of respondents cite brand/reputation damage as a top concern

3/4

of respondents say system downtime/inaccessible applications would pose the greatest challenge to recovery/remediation efforts

42%

fear that the DDoS attack could be masking an even more malicious attack

Challenge:

- DDoS attack volume is increasing.
- DDoS attacks can be large, distributed across the globe, and relatively easy to launch.
- DDoS often serves as a decoy, masking other more serious types of attacks, which makes them highly disruptive.



Recommendations:

DDoS preparedness must be based around an “always-on” mentality. Financial institutions should perform an evaluation of business-critical applications and their respective attack surfaces. They should also periodically reevaluate risk appetite and acceptance decisions, based on the evolving threatscape as well as market and regulatory changes. The evolution of DDoS means that financial institutions must update their risk profiles and mitigation measures accordingly.

Do you have, or are you planning on implementing, a Zero Trust security strategy?

Respondents are at different stages in their journey toward Zero Trust.

24% have yet to develop a Zero Trust strategy.
The remainder are in various stages of progress.

only

20%

have successfully implemented and are maintaining a Zero Trust strategy

Challenge:

Lack of visibility into network traffic and digital assets can make the move to the cloud virtually impossible.

Providers of electronic funds transfer and payment systems demand strict separation of their services from the institution's general IT environment, reducing risk by limiting lateral movement.

Financial institutions need to demonstrate that they are taking effective measures to secure critical assets, mitigate fraud risk, and protect customer privacy.




Recommendations:

Zero Trust allows for protection of applications, threat detection, and prevention of lateral spread of attacks.

- Implement microsegmentation to limit the blast radius of potential attacks. M&A can introduce complexity during the integration or divestiture of entities.
- Enable secure Zero Trust Network Access (ZTNA) for enterprise resources while maintaining consistent and broad cybersecurity controls aligned to Zero Trust guiding principles.
- Gain visibility to understand where data resides, its criticality, how to protect it, and who and what should have access to it. This can support compliance with data sovereignty and privacy laws while enhancing overall data risk posture.
- Enforce least privilege and dynamic access control for identities, including employees, service accounts, customers, and third parties.

What organizational barriers stand in the way of further investment in security?

Budget constraints top the list of barriers.

A woman with long dark hair, wearing a white blazer, is looking down at her smartphone. She is in a dark, blue-lit office environment. In the background, there are blurred lights and a wall with a grid of small lights. The overall mood is professional and focused.

While nearly $\frac{1}{3}$ of respondents suggest that there are no major organizational barriers, 28% cite that staffing and lack of resources remain a hindrance to further security investment at their financial institution.

With unlimited resources, the majority say they would want continuous monitoring and threat hunting

- With continuous monitoring and threat hunting, financial institutions can proactively hunt for ongoing and emerging attacks, minimizing dwell time and reducing the time to mitigation.
- Monitor your environment for the existence of adversaries, saving you time, effort, and cost.
- Gain rapid response, giving you the confidence to focus on what matters most — your customers.
- By continually monitoring your environment for attacks, you get a baseline of your security configurations and can tailor hunting methods to your specific topology.



64%
want continuous
monitoring and
threat hunting

Challenge:

While technology is positively reshaping the financial transaction landscape for today's banking customers, it is simultaneously ushering in a new era of cyberthreats that directly challenge economic stability. Financial institutions remain prime targets for cybercriminals, as indicated by the [IBM Cost of a Data Breach Report 2023](#), which reported that finance firms suffer an average loss of approximately \$5.9 million per data breach — 28% higher than the global average.



Recommendations:

Mitigate the cost of failure through effective training and data governance. By implementing successful strategies in these areas, financial services institutions can safeguard both customers and employees from the escalating threat landscape, keeping them out of the headlines. In the current dynamic cybersecurity environment, protecting your financial institution and clients from hackers, bots, and fraud is crucial. Instead of grappling with each small battle, proactively invest in world-class protection for your clients. Additionally, empower clients and employees through training to recognize signs of suspicious behavior, enabling your entire organization to unite in defense against adversaries.

These insights come from the survey Cybersecurity Strategies for Financial Institutions, conducted by Gatepoint Research on behalf of Akamai, between September and November 2023.

Management levels represented are all senior decision-makers: 71% hold the title CXO or are VPs, 18% are directors, and 11% are senior or department managers.



More Resources

[The High Stakes of Innovation: Attack Trends in Financial Services](#)

The 2023 financial services State of the Internet (SOTI) report not only reaffirmed familiar threat trends seen throughout this year's security research but also provided some unique sector insights. The report is based on both the threat traffic we defend against and best practices we've learned from our customers.

[Adapting in Crisis: Tackling Cybersecurity Challenges in Financial Services](#)

Now more than ever, financial institutions need simple and creative solutions to reduce risks, meet compliance requirements, and safely embrace new technologies. Read this white paper to learn how financial institutions can achieve security while still moving at the speed their business demands.

[The Evolution of DDoS: Return of the Hacktivists](#)

This joint DDoS research report, written collaboratively with FS-ISAC and Akamai, provides insights on the hacktivist shift in motivations, targets, actors, and techniques — plus, how to stop them.



Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. Learn more about Akamai's solutions for financial institutions at akamai.com/finserv and akamai.com/blog, or follow Akamai Technologies on [X](#), formerly known as Twitter, and [LinkedIn](#). Published 12/23.