CLOUDFLARE

Digital Heists:

The Evolution of Cyber Threats in Financial Services

Digital modernization brings new opportunities for financial services organizations to adopt game-changing technologies—and for attackers to exploit new vectors and vulnerabilities.

The adoption of regulations and industry mandates designed to ensure customers, data, and systems are protected only creates greater pressure to ensure that new technologies are secure, that attacks are prevented, and that regulatory compliance requirements are met.

Financial Services: Top target for cyberattacks

Lucrative Target
Valuable and sensitive data with potential for significant financial gain

Increased Attack Surface
Due to digital transformation and reliance on digital technologies and online banking

Security Gaps
Created by vulnerabilities in third-party vendors and expanding supply chain

22% Higher
The cost of a data breach in financial services vs. the global average[1]

51%
Of attacks against financial services organizations are by malicious actors[1]

20%
Of reported cyber incidents have affected the global financial sector[2]

Digital modernization can introduce new security vulnerabilities

Digital modernization efforts have created an expanded threat landscape—and potential entry points—for attackers to exploit critical systems and steal sensitive data.

Hybrid Cloud Adoption
Move infrastructure and apps to cloud to realize greater efficiency, scalability, and flexibility while meeting security and regulatory compliance mandates

APIs
Enhance financial services operations, facilitate the development of new products and services, and improve customer experiences

AI
Enable and transform how financial institutions deliver services, improve decision-making, and manage risk.

60%
Financial services organizations have >25% of their workloads residing in cloud[3]

90%+
Financial institutions using or planning to use APIs to generate additional revenue among existing customers[4]

80%
Financial institutions that consider AI relevant to their businesses[5]

Protecting against traditional and novel attacks

Financial services organizations are now challenged to protect against traditional and novel attack vectors—and that means managing, monitoring, and securing more access points, applications, and infrastructure than ever before.

Traditional Attack Vectors

DDoS attacks
Goal: Disrupt and halt operations

How: Overwhelm servers with fake connection requests, leading to disruptions and potential data breaches

49%
Quarter-on-quarter increase in DDoS attacks for Q3 2024, with banking and financial services bearing the brunt of cyber incidents[7]

Phishing
Goal: Steal personal and financial information by targeting financial services employees and customers

How: Using email, text messages, or phone calls to mimic trusted sources

8 out of 10
Organizations had at least one individual fall victim to a phishing attempt[8]

Ransomware attacks
Goal: Demand a ransom to restore access to, or return, files, systems, and networks

How: Systematically prevent access to files, systems, or networks, or exfiltrate files

+64%
Increase in ransomware attacks against financial services organizations in 2023[9]

Zero-day exploits
Goal: Gain unauthorized access to systems or steal sensitive information by exploiting unknown vulnerabilities

How: By targeting financial infrastructure, attackers identify a previously unknown vulnerability in software, firmware, or hardware

24%
Vulnerabilities exploited on or before the day their CVEs were publicly disclosed[10]

Insider threat
Goal: Steal information or degrade systems for financial, personal, or malicious purposes

How: Employees or partners with access to data or systems compromise security due to negligence or malicious intent

$4.99 million
Average cost of breaches initiated by malicious insiders[1]

Modern Attack Vectors

Cloud misconfigurations
Protecting against sensitive data exposure, ensuring API security, identifying misconfigurations and compliance with regulatory requirements are just a few of the areas to address when rehosting, refactoring, and/or replatforming applications.

80%
Security breaches caused by cloud misconfiguration-related issues[6]

Post-quantum computing
Protect data and systems from quantum computing attacks that can break widely used encryption algorithms and compromise data confidentiality, integrity, and authentication.

38%
TTPS traffic encrypted using post-quantum algorithms by March 2025[11]

AI
Stop AI-powered cyber threats and fraud:

- Attackers using ML to generate sophisticated phishing attacks, deepfake fraud and automated exploits
- Prevent cybercriminals, who target vulnerabilities in AI models or manipulate training data, leading to potentially severe consequences.
- Automate the detection of legitimate users and bad actors to prevent fraud and identity theft

93%
AI bots that are unverified and potentially malicious[5]

APIs
Secure open banking APIs to protect sensitive financial data and comply with regulations for evidence of customer consent.

60%
Internet traffic that is now API-based, with unsecured APIs a prime target for attackers[5]

Supply chain and 3rd party risk
Ensure cyber health of vendors in supply chain to optimize risk management and ensure overall security and compliance.

15%
Breaches that involve a third party[6]

Financial service organizations must protect against known and newly discovered or unknown threats that exploit vulnerabilities and stall digital modernization initiatives.

Discover how to secure against new threats to AI, APIs, and more.

Learn more

Sources:
1. IBM, Cost of a Data Breach Report 2024
2. International Monetary Fund, Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks, 2024
3. McKinsey & Company, The cyber clock is ticking: Defending emerging technologies in financial services, 2024
4. McKinsey & Company, From tech tool to business asset: How banks are using B2B APIs to fuel growth, 2021
5. Cloudflare, Cloudflare Signals Report 2025
6. Verizon, 2024 Data Breach Investigations Report
7. Cloudflare, DDoS threat report for 2024 Q4, 2024
8. CISA, Phishing Infographic
9. Norton, Ransomware statistics: Facts and trends for 2025
10. Infosecurity Magazine, 768 CVEs Exploited in the Wild in 2024
11. Cloud Security Alliance, Managing Cloud Misconfigurations Risks, 2023

© 2025 Cloudflare, Inc. All rights reserved.
CLOUDFLARE® and the Cloudflare logo are trademarks of Cloudflare. All other company and product names and logos may be trademarks of the respective companies with which they are associated.
1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

CLOUDFLARE

REV:BDES-7713.2025MAY28