Akamai

7 Critical Questions to Build Ransomware Resilience in Financial Services

Introduction

Ransomware has become one of the most formidable cybersecurity threats facing financial institutions today. Once viewed as a minor nuisance, ransomware has rapidly evolved into a powerful weapon used by cybercriminals to exploit sensitive financial data, disrupt operations, and demand exorbitant ransoms. In the past year alone, more than 4,000 new victims of ransomware have been recorded — and financial institutions, given their vast repositories of high-value data, remain at the top of attackers' target lists. To safeguard against this ever-present threat, institutions must adopt a proactive and comprehensive defense that goes beyond traditional perimeter security.

Akamai for financial services

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 in which to do business.

Our clients include:

All top **20** brokerages

17 of the top **20** banks

7 of the top **10** fintech companies

7 critical questions

This ebook explores seven critical questions that financial institutions should consider to combat ransomware, mitigate its devastating effects, and secure their operations.

01. Do you have visibility? It's your first line of defense.

02. Ransomware is evolving — Are you?

03. 2024 saw more than 4,000 new victims — Can you stay protected?

04. Are you prepared to stop ransomware from spreading?

05. APIs are a prime target attackers — Can you secure yours?

06. Do you have rapid response capabilities for maximum containment?

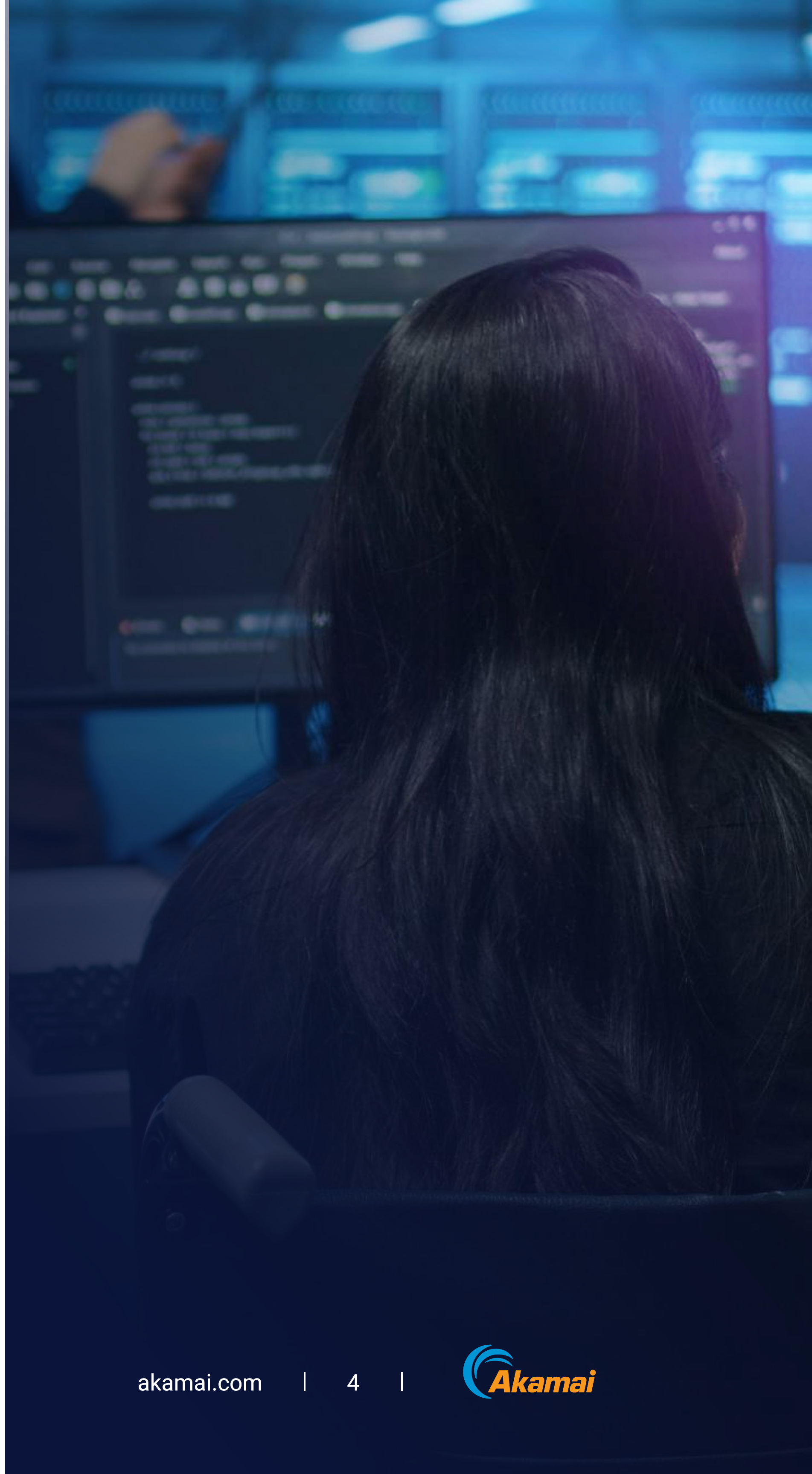
07. Do you know you can boost your ROI by avoiding costly attacks?

01

Do you have visibility? It’s your first line of defense.

The cornerstone of any effective security strategy is visibility. Financial institutions manage highly complex, interconnected systems — and the more intricate these environments become, the easier it is for ransomware to hide and propagate. Visibility into the entire network — across applications, users, and data flows — is critical to detect suspicious activity before it becomes a full-blown ransomware attack. Unfortunately, many institutions suffer from siloed infrastructure and piecemeal tools, which can create blind spots in their security.

Akamai’s real-time visibility solutions give institutions a complete, integrated view of their infrastructure, which enables them to detect ransomware early and take swift action to isolate affected systems. This holistic approach to visibility ensures that nothing slips through the cracks, and security teams can respond to threats before they escalate.



02

Ransomware is evolving – Are you?

Ransomware has evolved significantly from its early days. Today's ransomware is more sophisticated, often combining encryption with data exfiltration, creating a dual extortion scenario in which attackers not only demand payment to unlock data but also threaten to release sensitive information publicly. The financial services sector, with its wealth of sensitive data such as banking credentials, personally identifiable information, and payment information, presents an attractive target for ransomware operators.

Additionally, ransomware attacks are now tailored, with attackers conducting reconnaissance to identify the most valuable assets, ensuring maximum disruption. As ransomware tactics evolve, so too must the defense strategies of financial institutions. A static defense is no longer enough — institutions need dynamic, adaptive solutions that can evolve in real time with the threat landscape. Has your institution evolved to meet this threat?

Financial services experienced a **64%** increase in ransomware attacks

Source: https://bankingjournal.aba.com/2024/08/ransomware-in-the-financial-sector

03

2024 saw more than 4,000 new victims — Can you stay protected?

The sheer scale of ransomware incidents continues to grow. In 2024 alone, more than 4,000 new victims were reported globally, a 77% year-over-year increase. Financial institutions are prime targets for these attacks because of the large volumes of valuable data they hold and the critical role they play in the global economy. A successful attack on a bank or investment firm can lead to significant financial losses, customer churn, reputational damage, and regulatory penalties.

The frequency and complexity of these attacks mean that financial institutions must always be on high alert. The growing number of incidents should serve as a wake-up call to ensure that financial institutions are continuously strengthening their security postures and adopting the latest tools to keep pace with these evolving threats. Are your defenses keeping up?

77%

year-over-year increase leading to significant financial losses, customer churn, reputational damage, and regulatory penalties

04

Are you prepared to stop ransomware from spreading?

Ransomware's destructive power lies in its ability to move laterally across a network. Once ransomware gains a foothold, it seeks out other vulnerable systems, spreading like wildfire and causing widespread operational paralysis. Stopping lateral movement is one of the most effective ways to prevent ransomware from causing large-scale damage.

Software-based microsegmentation helps contain ransomware by ringfencing critical applications, databases, and systems, which limits the pathways ransomware can take. By segmenting the network into isolated zones, financial institutions can prevent ransomware from moving freely, ensuring that even if one part of the network is compromised, the rest remains protected. This containment strategy is crucial for reducing the impact of an attack and maintaining business continuity.

05

APIs are a prime target for attackers — Can you secure yours?

As financial institutions increasingly rely on APIs to deliver innovative services and connect with partners and customers, these interfaces have become a prime target for attackers. APIs serve as gateways to sensitive data and core financial systems, and poorly secured APIs can provide an entry point for ransomware and other cyberthreats. Attackers exploit vulnerabilities in APIs to steal data, launch attacks, or even introduce ransomware directly into the system.

Akamai's API security solutions provide financial institutions with comprehensive protection, monitoring API activity in real time to detect and prevent malicious activity. By securing APIs, institutions can ensure that their data flows remain protected and that ransomware operators are unable to exploit these valuable entry points.

06

Do you have rapid response capabilities for maximum containment?

When ransomware strikes, the speed of your response can mean the difference between a minor incident and a major disaster. The longer ransomware is allowed to move freely within your network, the more damage it can cause. Akamai's automated incident response tools are designed to act quickly to isolate infected systems and prevent the ransomware from spreading further. These tools provide real-time containment, ensuring that once an attack is detected, it can be swiftly neutralized.

With automated response protocols in place, financial institutions can minimize operational downtime, prevent data loss, and maintain customer trust. Rapid response capabilities not only reduce the damage caused by ransomware but also help institutions recover faster, ensuring that business operations can resume as quickly as possible.

07

Do you know you can boost your ROI by avoiding costly attacks?

Ransomware attacks are not only disruptive — they are expensive. The costs of paying the ransom, restoring operations, and recovering lost data can quickly spiral out of control, not to mention the potential regulatory penalties and reputational damage. For financial institutions, these costs can run into the millions.

By investing in Akamai's comprehensive security solutions, institutions can significantly reduce the risk of falling victim to a ransomware attack. Akamai's all-in-one platform provides everything from visibility and microsegmentation to API protection and incident response, offering a cost-effective solution that eliminates the need for multiple vendors and reduces the complexity of managing security. In addition to lowering the risk of costly attacks, Akamai's solutions deliver a strong return on investment (ROI) by reducing downtime, protecting critical assets, and ensuring compliance with regulatory requirements.

Akamai is the answer

As ransomware continues to evolve, financial institutions face growing challenges in defending their networks and protecting their sensitive data. The key to staying ahead of these threats is a proactive, multilayered defense strategy that includes real-time visibility, microsegmentation, API protection, and rapid response capabilities. Akamai's comprehensive security solutions provide financial institutions with the tools they need to safeguard their operations, meet regulatory obligations, and maintain customer trust. By taking a proactive approach and investing in cutting-edge defenses, financial institutions can protect themselves against the ever-evolving threat of ransomware and build resilience for the future.

Learn more about our solutions for financial services

Learn more

Akamai Security protects the applications that power industries like financial services, ensuring seamless interactions at every touchpoint without compromising performance or customer experience. By leveraging the scale and visibility of our global platform, we partner with financial institutions and other organizations to prevent, detect, and mitigate threats, so you can build trust with your customers, protect sensitive data, and confidently meet regulatory demands. Our solutions support your mission to innovate and deliver secure, reliable services in a rapidly evolving digital landscape. Learn more about Akamai's cloud computing, security, and content delivery solutions **akamai.com** and **akamai.com/blog**, or follow Akamai Technologies on **X**, formerly known as Twitter, and **LinkedIn**. Published 11/24.