WHITE PAPER

Cybersecurity That Keeps Malaysia's Financial Services Industry Moving Forward

Malaysia's financial services industry (FSI) is rapidly evolving. The rise of online banking, mobile payments, and the growing influence of both traditional banks — such as Maybank and CIMB — and non-bank digital wallet providers — like Touch 'n Go, GrabPay, and ShopeePay — are reshaping how Malaysians interact with money. This digital momentum is creating great customer experiences around convenience and accessibility. However, it also expands the attack surface for cybercriminals, underscoring the need for robust cybersecurity measures across the entire digital payments ecosystem.

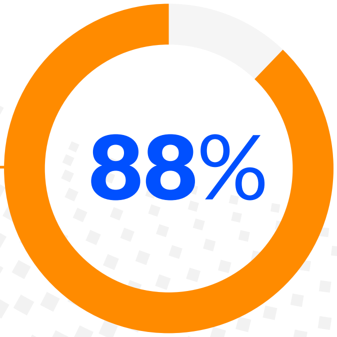
In 2024 alone, more than 4,000 cyber incidents were reported in Malaysia. Even more alarming, ransomware attacks spiked 78% in Q4 of that year. These trends reveal an urgent need for financial institutions to move away from reactive security practices and adopt more proactive, resilient defenses.

Akamai helps Malaysian financial institutions address these challenges head-on with solutions that deliver visibility, control, and resilience needed to ensure secure transformation. In this white paper, we'll explore how forward-looking defenses can support visibility while minimizing risk and complexity. You'll learn why:

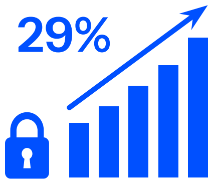
- **Digital transformation is accelerating.** Financial services innovators are driving rapid growth in digital services, but expanded attack surfaces are fueling rising fraud rates, especially in Q1 2025.
- **Cybersecurity risks are intensifying.** Last year, 88.7% of financial services companies experienced an attack on the APIs that handle their data, while Malaysia experienced a 29% increase in data breaches in Q1 2025 alone.
- **Proactive cybersecurity is becoming a competitive edge.** Addressing risks now prepares institutions for future challenges and builds the trust needed to lead in a digital-first market.

Akamai supports this shift by delivering the end-to-end awareness and cyber resiliency that's needed to secure digital experiences and reduce operational risk. By partnering with Akamai, financial institutions can take decisive steps to increase visibility, mitigate risk, and minimize complexity.

In 2024, **88.7%** of financial services companies experienced an attack on the APIs that handle their data.



Malaysia experienced a **29%** increase in data breaches in Q1 2025 alone.



Navigating a digital-first landscape: Challenges and opportunities

As Malaysia's financial services industry advances its digital transformation, the threat landscape is evolving just as rapidly. Financial institutions are under pressure to innovate, but doing so means confronting a growing list of cybersecurity risks.

Visibility and control create operational resilience. With better insight into how systems connect and communicate, financial institutions can detect threats earlier, contain incidents faster, and maintain service continuity.

Ransomware remains a critical threat. Modern attacks are more targeted and disruptive than ever, focusing on critical systems and operational downtime. A single successful campaign can result in significant financial loss, extended service outages, and reputational harm.

API sprawl is creating new attack surfaces. Most financial institutions now rely on tens of thousands of APIs — often between 15,000 and 25,000 per enterprise. Many of these APIs are poorly documented and/or misconfigured, leaving vulnerabilities that attackers can exploit to access data to accounts or critical financial data.

Hybrid IT environments add complexity. Securing a mix of technologies across different environments makes it difficult to maintain consistent controls and visibility. Most institutions today manage a combination of on-premises infrastructure, public and private cloud platforms, and Kubernetes or container-based services. Each environment introduces new risk factors and difficulty in deploying consistent security posture.

Third-party risk is expanding with fintech and cloud adoption. As banks integrate with more partners and platforms, the attack surface broadens. Without strong access controls and monitoring, data shared across systems becomes increasingly difficult to secure.

Posture management is an uphill battle. Due to factors like vulnerabilities, lack of visibility, and misconfiguration, not to mention operational challenges like compliance and budget restraints, posture management remains a challenge for many banks.

Evolving threats complicate runtime protection. An evolving threat landscape makes runtime protection more of a challenge, as banks attempt to control malicious behaviors like abuse, API scraping, and credential stuffing.

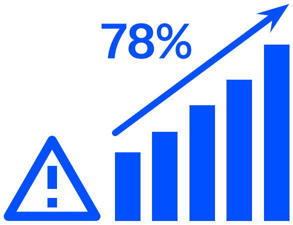
But these same forces that introduce risk also create opportunity.

A preemptive security posture enables secure digital growth. Institutions that invest in strong defenses can confidently scale mobile and online services, meeting customer expectations while maintaining control.

Trust becomes a differentiator. Consumers are more aware than ever of data security. Institutions that can demonstrate resilience and transparency will build stronger, more loyal customer relationships.

Security lays the foundation for secure innovation. When risks are managed up front, teams are free to pursue fintech partnerships and new digital offerings that drive growth without compromising protection or compliance.

Ransomware attacks spiked 78% in Q4 of 2024.



Akamai's solutions for security and resilience at scale

To meet the rising demands of cybersecurity in a hybrid, high-velocity environment, financial institutions need security solutions that are both powerful and practical. Currently trusted by the world's top 10 banking companies, Akamai's portfolio is built to help banks and financial services providers in Malaysia mitigate risk without slowing down innovation.

With capabilities designed for visibility, threat containment, and secure access, Akamai offers services to stop attacks earlier, and streamline operations across even the most complex infrastructure.

Akamai Guardicore Segmentation: Isolating threats before they spread

Akamai Guardicore Segmentation enables financial institutions to implement microsegmentation, providing fine-grained control over application-level traffic and blocking lateral movement inside the network. This helps isolate threats before they can compromise sensitive systems.

Key capabilities include:

- **Microsegmentation** that enforces granular visibility and control of access policies around critical assets like databases and payment systems
- **Ransomware containment** that uses global deny rules and application ringfencing to prevent malware from moving laterally
- **Hybrid environment visibility** that maps flows and provides rich context across on-premises, cloud, and Kubernetes platforms, reducing blind spots
- **Zero Trust enforcement** provides the industry standard that's powered by pre-built policy templates for fast, consistent deployment

A global financial services provider used Akamai Guardicore Segmentation to quickly contain a ransomware attack before it could spread from a compromised VDI environment to backup servers and production systems — protecting over 23,000 servers across hybrid infrastructure.

API security: Defending one of the fastest-growing attack surfaces

As mobile banking, fintech platforms, and customer-facing apps expand, APIs have become a primary vector for attacks. Akamai's API Security solution offers automated detection and protection to help institutions manage API risk at scale, from shadow endpoints to credential abuse.

Core capabilities include:

- **Automated API discovery** that identifies undocumented or rogue APIs to ensure full visibility
- **Posture management** that detects vulnerabilities like weak authentication and helps teams prioritize remediation
- **Runtime protection** that monitors and blocks malicious behaviors such as API scraping, credential stuffing, and abuse
- **Bot mitigation tools** that combine rate limiting and behavioral analysis to stop automated threats before they impact systems

Use case

A global payments provider used Akamai API Security to gain visibility into shadow APIs, which allowed them to move them behind security controls and secure millions of high-value financial transactions that the team had no visibility on. This improvement to risk posture was a big win for the security team.

Complementary solutions: Full-spectrum protection across layers

Akamai's platform offers a holistic defense framework that goes beyond segmentation and APIs, helping financial institutions prepare for volumetric attacks and application-layer threats.

- **DDoS protection** defends against 29.25% of Layer 3 and Layer 4 attacks affecting the financial services industry, ensuring service availability.
- **Web application and API protection (WAAP)** mitigates OWASP Top 10 threats, providing robust safeguards for front-end and back-end digital services.
- **AI-powered firewall (AI FW)** delivers intelligent threat detection and response, continuously learning from attack patterns to strengthen defenses over time.

Together, these solutions form a comprehensive cybersecurity stack designed to support the speed, scale, and trust expectations of Malaysia's digital financial services industry.

Future-ready infrastructure, powered by Akamai

To lead in Malaysia's rapidly evolving financial services landscape, institutions need infrastructure that can do more than defend against today's threats. It must also enable innovation, support digital expansion, and respond effectively to the unexpected. Whether enforcing verification, scaling across blended IT ecosystems, or navigating rising API threats, the most successful organizations will be those that combine long-term flexibility with responsive security controls.

Akamai's solutions are purpose-built to help financial institutions expand securely while staying resilient in the face of mounting cyber risk.

Rapid threat containment: Akamai Guardicore Segmentation uses microsegmentation and runtime protection to protect compromised systems and stop attacks from spreading across the network or cloud.

Scalability for digital growth: Akamai's distributed cloud platform allows financial institutions to roll out new services, integrate fintech partnerships, and expand cloud capabilities — all without compromising security.

Cloud adoption readiness: Akamai Guardicore Segmentation's unified policy engine and API Security's posture controls secure both cloud native workloads and legacy infrastructure, ensuring visibility across hybrid and multicloud platforms.

Proactive risk management: Akamai API Security and Akamai Guardicore Segmentation help institutions stay ahead of evolving threats, from surging API abuse to advanced ransomware, by embedding protection directly into their infrastructure.

Resilience against evolving risks: As threats become more advanced and persistent, response time and control are critical. Akamai's solutions help institutions prepare, adapt, and recover quickly — minimizing impact and protecting customer confidence.

Zero Trust frameworks: Akamai's Zero Trust architecture enforces continuous verification and strict access enforcement, limiting the blast radius of any incident and reducing exposure in a multi-environment infrastructure.

Top 5 benefits for Malaysian financial institutions

Modernizing cybersecurity isn’t just about reducing risk. For financial institutions in Malaysia, the right solution can also drive efficiency, support growth, and strengthen relationships with customers. Akamai’s platform delivers value across five key dimensions: scalability, trust, risk reduction, resilience, and efficiency.

1. Scalability

As financial institutions grow, Akamai scales with them to support mobile-first strategies, fintech expansion, and cloud adoption.

- Secures mobile apps, APIs, and hybrid workloads across platforms
- Flexible architecture adapts to emerging technologies and evolving operational needs
- No need to rip and replace existing infrastructure to add protection

2. Customer trust

Trust is earned through consistent, safe financial interactions. Akamai helps financial institutions deliver on that promise.

- Defends customer data at every layer of the stack
- Minimizes service disruptions that could impact brand reputation
- Reinforces institutional credibility in a competitive financial ecosystem

3. Reduced risk

Akamai helps institutions minimize their exposure by limiting how far attackers can move within the environment and how much data they can access.

- Microsegmentation and API protection shrink the attack surface by controlling access to sensitive systems and services
- Real-time detection and policy enforcement prevent threats from escalating into full-scale incidents

4. Enhanced resilience

Cyberattacks are inevitable, but downtime and data loss don’t have to be. Akamai’s solutions are designed to keep operations running even under pressure.

- Akamai Guardicore Segmentation isolates compromised systems, preventing lateral movement
- Akamai API Security and runtime protections maintain the integrity of customer-facing services
- Built-in redundancies and distributed architecture help ensure service continuity

5. Operational efficiency

Security doesn’t need to be a resource drain. Akamai helps reduce manual effort and complexity through intelligent automation and preconfigured tools.

- Automated API discovery accelerates visibility and reduces risk from shadow endpoints
- Policy templates streamline segmentation, reducing administrative overhead
- Unified controls simplify compliance tasks and make audits more manageable

Choosing the right cybersecurity partner

In today’s digital economy, cybersecurity isn’t just defense — it’s direction. The right partner helps financial institutions adapt, grow, and lead with confidence. In Malaysia, that means choosing teams who bring deep expertise, global scale, and fast, responsive support.

The qualifications that matter most:

- **Proven experience in financial services.** Look for providers that understand the complexities of ransomware containment, API protection, and hybrid infrastructure in a regulated environment.
- **A comprehensive portfolio.** Solutions should cover all critical areas (microsegmentation, API security, DDoS mitigation, and web application protection) to reduce complexity and close security gaps.
- **Scalability and reach.** The right partner should support growth in digital banking, fintech collaboration, and multicloud environments without sacrificing performance or visibility.
- **Ease of management.** Built-in automation, simplified deployment tools, and centralized policy management allow security teams to stay ahead without adding overhead.
- **Operational support and services.** Strong cybersecurity relies on both effective tools and expert guidance. Providers that offer dedicated service teams, technical account managers, and hands-on support for implementation, tuning, and incident response can help institutions stay secure and efficient. These services are especially important when internal teams are short-staffed or managing multiple priorities.

Why Akamai?

Akamai delivers on all these criteria and more.

- **Akamai Guardicore Segmentation** helps institutions gain deep visibility and block lateral movement, protecting critical assets from ransomware and other threats.
- **Akamai API Security** uncovers shadow APIs, blocks abuse, and secures digital transactions in real time.
- **Complementary offerings** like DDoS mitigation and WAAP provide end-to-end protection across the attack surface.
- Akamai is a **trusted critical provider to FS-ISAC** and secures **all of the top 10 global banking firms**, offering unmatched credibility in the financial sector.
- Its global platform is paired with regional expertise to deliver solutions that align with Malaysia’s regulatory and operational priorities.

Want to keep your systems secure and your customers confident? Let’s talk. Our team at Akamai is ready to help you build tailored solutions that protect your digital future and strengthen trust across Malaysia’s financial services landscape.

Contact Akamai today to learn more about our comprehensive security solutions.

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai’s cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X and LinkedIn. Published 08/25.