Akamai

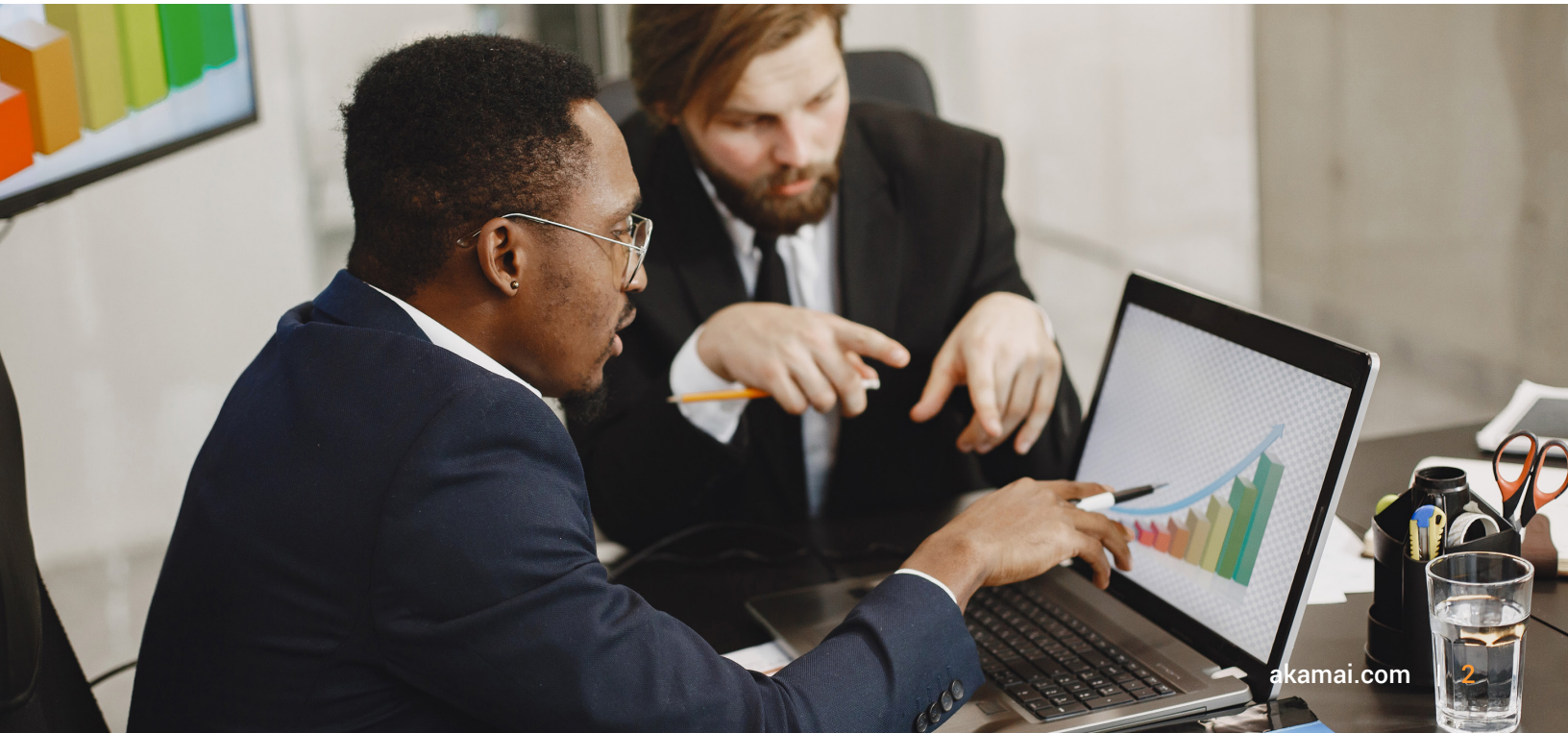
WHITE PAPER

Securing Financial Services with Comprehensive Compliance and Resilience

Cybersecurity strategies for emerging risks and evolving responses

The financial services industry faces constant pressure to evolve, driven by innovation and an ever-tightening regulatory landscape. On one hand, digital innovation presents immense opportunities for enhanced customer experience and a competitive edge. On the other hand, increased regulatory scrutiny, stricter enforcement actions, and reduced compliance timelines challenge institutions to maintain compliance without compromising security.

Digital evolution has also expanded the attack surface, exposing financial institutions to complex cyberthreats. These challenges are compounded by limited visibility into their infrastructure, applications, assets, and users. In such an environment, institutions must find proactive ways to adapt while ensuring the safety and resilience of their operations.



The dynamic regulatory landscape

In recent years, the evolving threat landscape and increasing complexity of cyberattacks have led to the introduction of new regulatory frameworks aimed at bolstering the cybersecurity and operational resilience of financial institutions. Regulations such as the EU's Digital Operational Resilience Act (DORA) and the Network and Information Security Directive (NIS2) have placed a renewed focus on safeguarding critical financial infrastructure and ensuring that institutions can withstand, respond to, and recover from cyber incidents.

Additionally, frameworks such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR) have heightened the importance of protecting customer data and maintaining robust security controls across all digital interactions. These regulatory demands create a challenging environment for financial institutions as they must continuously adapt to new rules while managing rising cyber risks in a dynamic threat landscape.

This regulatory pressure necessitates a dual focus on both compliance and cybersecurity, requiring financial institutions to enhance their operational resilience, improve visibility into their digital assets, and mitigate evolving threats.

Key challenges for financial institutions: Visibility and compliance

Gaps in visibility, gaps in compliance

Financial institutions often struggle with visibility into their infrastructure, users, and applications, leading to significant security and compliance failures. According to a recent Forrester study, commissioned by Akamai:

- 88% of financial institutions have faced at least one material impact event in the past 18 months, with 60% incurring remediation costs due to noncompliance
- More than one-third of financial institutions lack confidence in their ability to promptly detect and respond to vulnerabilities, risking noncompliance and fines
- More than 25% of institutions do not have a full view of their environment concerning current and upcoming regulations, and 50% struggle to report on users, assets, infrastructure, and applications to compliance teams and auditors

Operational silos and tooling gaps

Limited visibility is further exacerbated by fragmented tooling, internal silos, and staffing challenges. For example:

- 69% of institutions report that limited staff and expertise contributed to material impact events and noncompliance issues over the past 18 months
- 61% note that ineffective or piecemeal security tooling is a challenge, and 52% say their tools fail to provide an integrated view of users, assets, infrastructure, and applications
- Increased vendor complexity also amplifies risk; institutions that use multiple vendors for visibility are more likely to experience material impact events

Global perspectives on compliance challenges

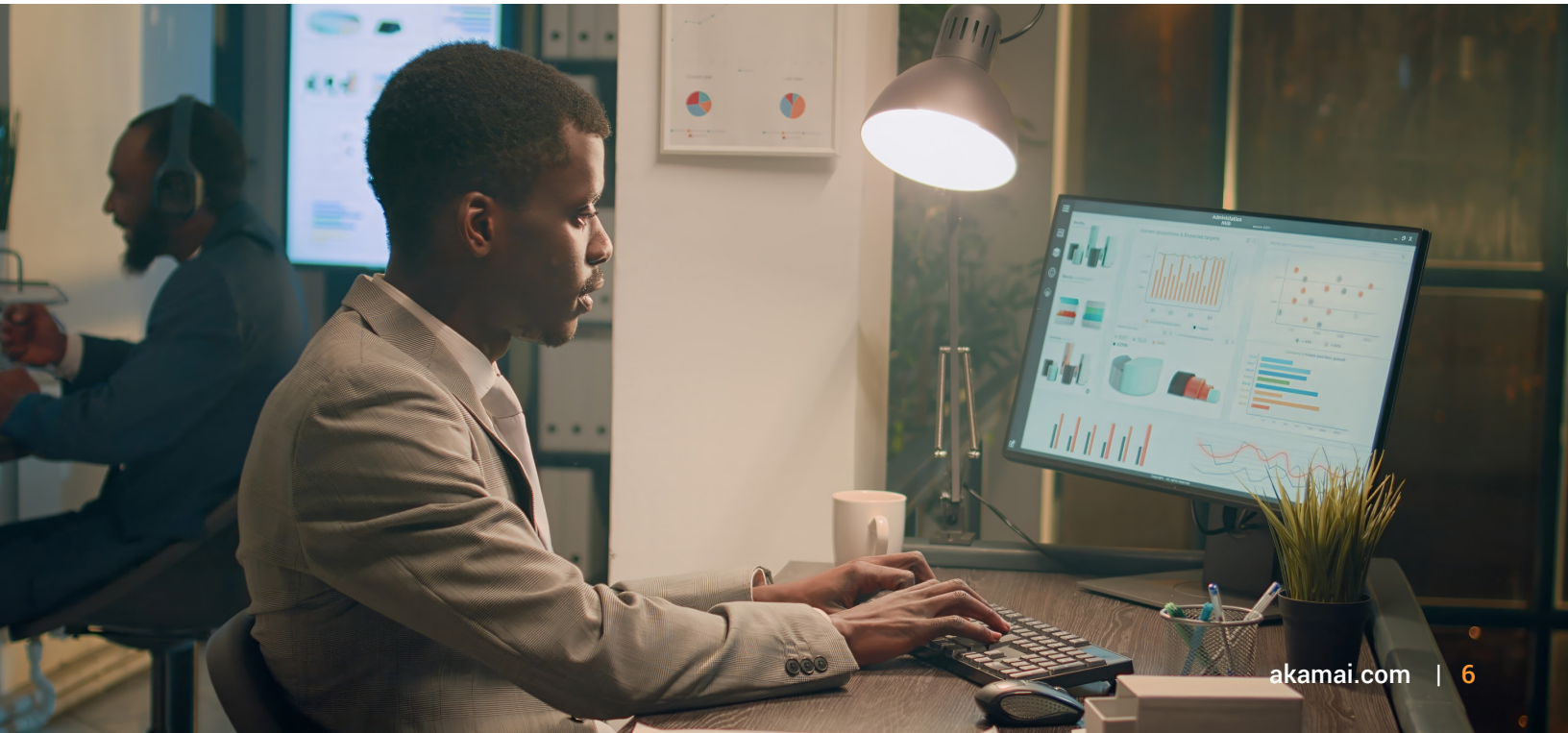
Geopolitical uncertainty and political upheaval directly impact banking industry regulation. During uncertain times, regulatory authorities face differing jurisdictional responsibilities and administrative focus areas, which can sometimes result in conflicting mandates and overlapping rules. This complexity can lead to challenges regarding enforcement and can limit opportunities for information exchange and operational synergies. Without these synergies, silos can emerge, causing multiple lines of business to maintain redundant, inconsistent customer-level data that requires enterprise-level reconciliation.

This complexity is often exacerbated by older legacy systems with hard-coded business rules, which complicates efforts to automate compliance processes. The scattered organizational structures, data formats, and legacy system processes significantly complicate compliance tasks and increase costs.

Operational resilience gained prominence in 2017 as regulators from Europe, Singapore, Hong Kong, the United States, and beyond responded to a surge in cybersecurity incidents and ransomware attacks. Approaches vary by region. The EU and the United Kingdom lead with detailed and timely regulations, while the United States employs a collaborative but varied approach. Asia-Pacific demonstrates strong efforts in some areas but lacks consistency across jurisdictions. In Digital Empires: The Global Battle to Regulate Technology, Anu Bradford identifies three predominant regulatory frameworks: the American market-driven model, the Chinese state-driven model, and the European rights-driven model. These diverse approaches create a complex environment, requiring financial institutions to understand and adapt to regional nuances and regulatory requirements.

Regulators worldwide, including the Monetary Authority of Singapore (MAS), the European Central Bank (ECB), the Office of the Superintendent of Financial Institutions (OSFI) in Canada, the Federal Financial Institutions Examination Council (FFIEC) in the United States, and the Australian Prudential Regulation Authority (APRA) with its newest CPS 230 standard, are increasingly scrutinizing corporate networks to ensure that only authorized users and applications can communicate. This shift from traditional perimeter defense to microsegmentation and Zero Trust architecture reflects the global trend toward tighter security controls.

For example, APRA's CPS 230 standard, which focuses on the operational resilience of financial institutions, underscores the importance of maintaining robust procedures to withstand and recover from disruptions. Additionally, the latest FFIEC Information Technology Examination Handbook devotes an entire section to application programming interfaces (APIs), explaining how "… broken, exposed, or compromised APIs can be exploited by malicious actors and used in data breaches." The handbook describes a range of security controls to help financial institutions safeguard APIs, protect confidential data, and defend against attacks. Whether in Europe, the United States, or Asia, financial institutions must adapt to this evolving landscape by ensuring that communication is strictly controlled and monitored.



Specific regulations

DORA

DORA is a significant piece of European legislation that sets a stronger regulatory rule book for financial entities by requiring an enhanced digital operational resilience framework that covers financial entities and their information and communication technology (ICT) third-party providers. DORA will come into force on January 17, 2025.

PCI-DSS v4.0

PCI DSS is a set of security standards that applies to any organization that accepts, processes, stores, or transmits credit card data. The latest version, PCI DSS v4.0, was released in March 2022, and full compliance is required by March 2025. This standard is globally recognized for enforcing payment card data security and preventing breaches.

NIS2 Directive

The NIS2 Directive provides EU-wide legislation on cybersecurity, updating the previous NIS Directive. It aims to create a common level of cybersecurity across the EU, harmonizing measures and approaches to secure digital infrastructure against cyberattacks.

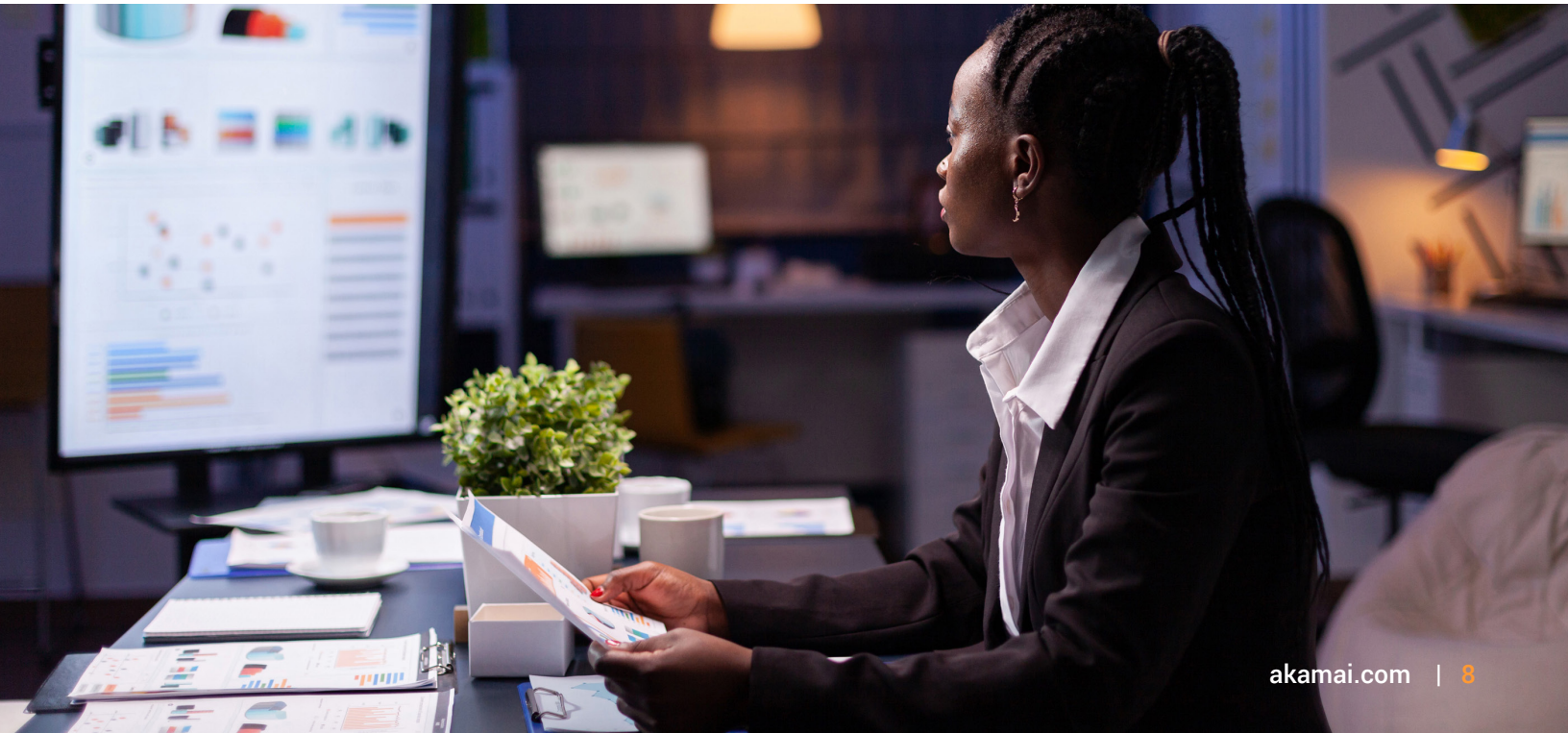
Data privacy regulations

With growing data privacy regulations — such as the GDPR in the EU and the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), in the United States — financial institutions need a flexible IT platform to meet new regulatory data requirements. Akamai safeguards customer data, accelerates breach investigations, adapts to regulatory changes, and provides process visibility and auditability.

The threat landscape and its impact

The threat landscape for financial institutions is constantly evolving, with cyberthreats such as distributed denial-of-service (DDoS) attacks, ransomware, phishing, and data breaches posing significant challenges. These threats not only disrupt operations but also have severe financial and reputational impacts. DDoS attacks have become increasingly sophisticated, often serving as smoke screens for more malicious activities like ransomware attacks. The Akamai Prolexic platform, for example, successfully thwarted the largest DDoS attack against a major U.S. financial institution, underscoring the need for robust defense mechanisms. Ransomware attacks exploit vulnerabilities to encrypt critical data and demand ransom for decryption.

The financial losses and operational disruptions caused by such attacks can be substantial. Financial institutions must deploy advanced threat detection and incident response capabilities to mitigate these risks effectively. Phishing and social engineering attacks are also prevalent, tricking employees into revealing sensitive information or credentials, which can lead to unauthorized access to systems. Continuous employee training and robust email security measures are essential to combat these threats. Data breaches result in the exposure of sensitive customer information, leading to financial losses, regulatory penalties, and damage to reputation. Implementing strong encryption, access controls, and monitoring solutions are critical to safeguard data integrity.



Top cyberthreats that impact financial institutions

Zero-day threats

Zero-day attacks are particularly dangerous for financial institutions, targeting previously unknown software vulnerabilities. These attacks can escalate quickly, with thousands of exploitation attempts occurring within hours of discovery. Financial institutions need multilayered defenses and real-time visibility across their entire environment for rapid detection and response. Solutions should offer a "single pane of glass" for granular visibility across all assets and infrastructure, including legacy systems and modern operating environments like operational technology (OT) and the Internet of Things (IoT). Vulnerabilities in software like SolarWinds, Log4j, and OpenSSL emphasize the need for surgical control to ringfence systems, mitigate risk, and block malicious activity during investigations. Reducing exposure windows and eliminating security gaps helps institutions stay ahead of these volatile threats without disrupting production applications.

DDoS attacks

DDoS attacks pose significant risks to financial institutions by overwhelming networks with malicious traffic, causing service disruptions and financial losses. Often used as distractions for more harmful activities like ransomware, DDoS attacks can cripple operations. Akamai's Prolexic platform successfully mitigated one of the largest DDoS attacks against a major U.S. financial institution. To defend against such threats, financial institutions require robust, multilayered defenses that are capable of handling large-scale attacks without disrupting critical services. A resilient infrastructure is essential to minimize operational downtime and ensure uninterrupted service availability.

Ransomware

Ransomware remains a persistent threat to financial institutions, with attackers encrypting critical data and demanding ransom for its release. However, the real danger lies in ransomware's ability to spread laterally across systems, leading to widespread operational failure. To mitigate these risks, institutions must focus on reducing the initial attack vector, such as limiting exposed servers and ensuring proper patch management. Network segmentation and ringfencing can limit propagation paths and prevent ransomware from spreading. Regular data backups are crucial for minimizing downtime and data loss, ensuring swift recovery and business continuity after an attack.

Phishing and social engineering

Phishing and social engineering attacks continue to exploit employees in financial institutions, leading to unauthorized access and compromised data. Attackers often trick employees into revealing sensitive information or unknowingly installing malware. To counter these threats, financial institutions must implement continuous employee education, advanced email filtering, and strict access control protocols. Ongoing training programs help employees stay vigilant against evolving phishing techniques, protecting both internal systems and customer data from compromise. Advanced email security and proactive monitoring are essential to mitigate these risks.

API attacks

APIs have increasingly become a key target for cybercriminals as financial institutions rely on them to drive innovation and facilitate transactions. Poorly secured APIs can allow attackers to access sensitive data or initiate fraudulent transactions. Ensuring comprehensive API security is essential for maintaining trust and adhering to regulatory standards like DORA. Akamai's API security solutions offer real-time monitoring, auditing, and threat detection to prevent unauthorized access, ensuring the protection of critical infrastructure and sensitive data. With APIs becoming an integral part of financial services, securing them is critical for reducing the attack surface and ensuring compliance.

Brand impersonation

Brand impersonation is a growing threat in the financial services sector, with cybercriminals creating fraudulent websites or social media profiles that mimic those of legitimate financial institutions. These fake sites trick customers into providing personal and financial information, which is then sold on the dark web or used to drain accounts. To combat brand impersonation, financial institutions must adopt proactive measures, including continuous monitoring, rapid takedown services, and customer education about the risks. Protecting brand reputation is critical, as brand impersonation erodes trust, which is essential for maintaining customer relationships in today's digital economy.

Akamai's role in compliance

Akamai's portfolio of services can help financial institutions defend against these threats while navigating regulatory challenges effectively. Akamai's solutions include:

Akamai API Security

API Security provides comprehensive visibility into API activity, enabling institutions to discover, monitor, and audit API behavior using real-time analytics to detect and respond to threats and abuse. This is crucial for protecting sensitive data and ensuring compliance with regulations that govern data security and privacy.

Akamai Guardicore Segmentation

Microsegmentation helps isolate critical applications and workloads, which reduces the risk of lateral movement within the network. This containment strategy is vital for maintaining operational resilience and compliance with stringent regulatory standards.

Akamai Edge DNS

Edge DNS provides high availability and performance for DNS services, protecting on-premises, cloud, and hybrid DNS infrastructure. This solution is essential for maintaining service continuity and protecting against large-scale cyberthreats.

Akamai App & API Protector

App & API Protector combats Layer 7 attacks with comprehensive protections. This includes defense against DDoS, bots, and the OWASP top 10 security risks exploits, ensuring robust security for web applications and APIs.

Akamai Client-Side Protection & Compliance

Akamai assists with PCI compliance and protects websites against JavaScript attacks. This helps safeguard sensitive customer data as part of financial institutions' compliance programs.

Akamai Prolexic

Prolexic protects infrastructure from DDoS attacks. It offers robust defense mechanisms to ensure uptime and reliability, even during large-scale attacks.

Akamai Bot Manager

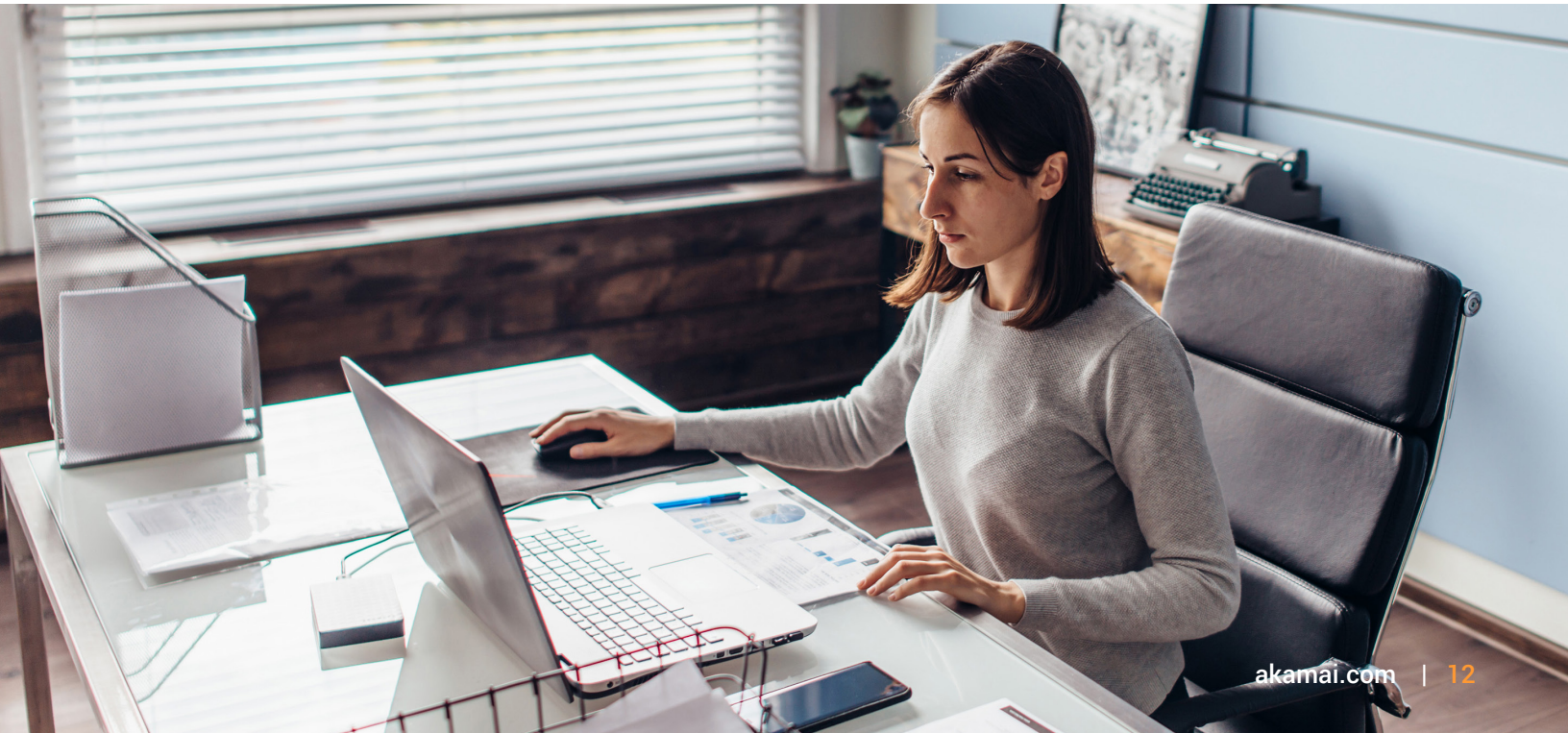
Bot Manager provides advanced bot management designed to detect and mitigate sophisticated bad bots while allowing good bots so that legitimate traffic is not hindered to maintain a seamless user experience.

Akamai Account Protector

Account Protector detects and mitigates account takeover, account opening abuse, and credential stuffing. This is crucial for protecting customer accounts and maintaining trust.

Akamai Content Protector

Content Protector helps stop scrapers from stealing content and lowering conversion rates so proprietary content remains secure and financial institutions can maintain their competitive edge.



Proven success stories from our customers

Here are a few examples that offer valuable insights into our customers' experiences with how effectively Akamai supports regulatory compliance.

Large insurance organization

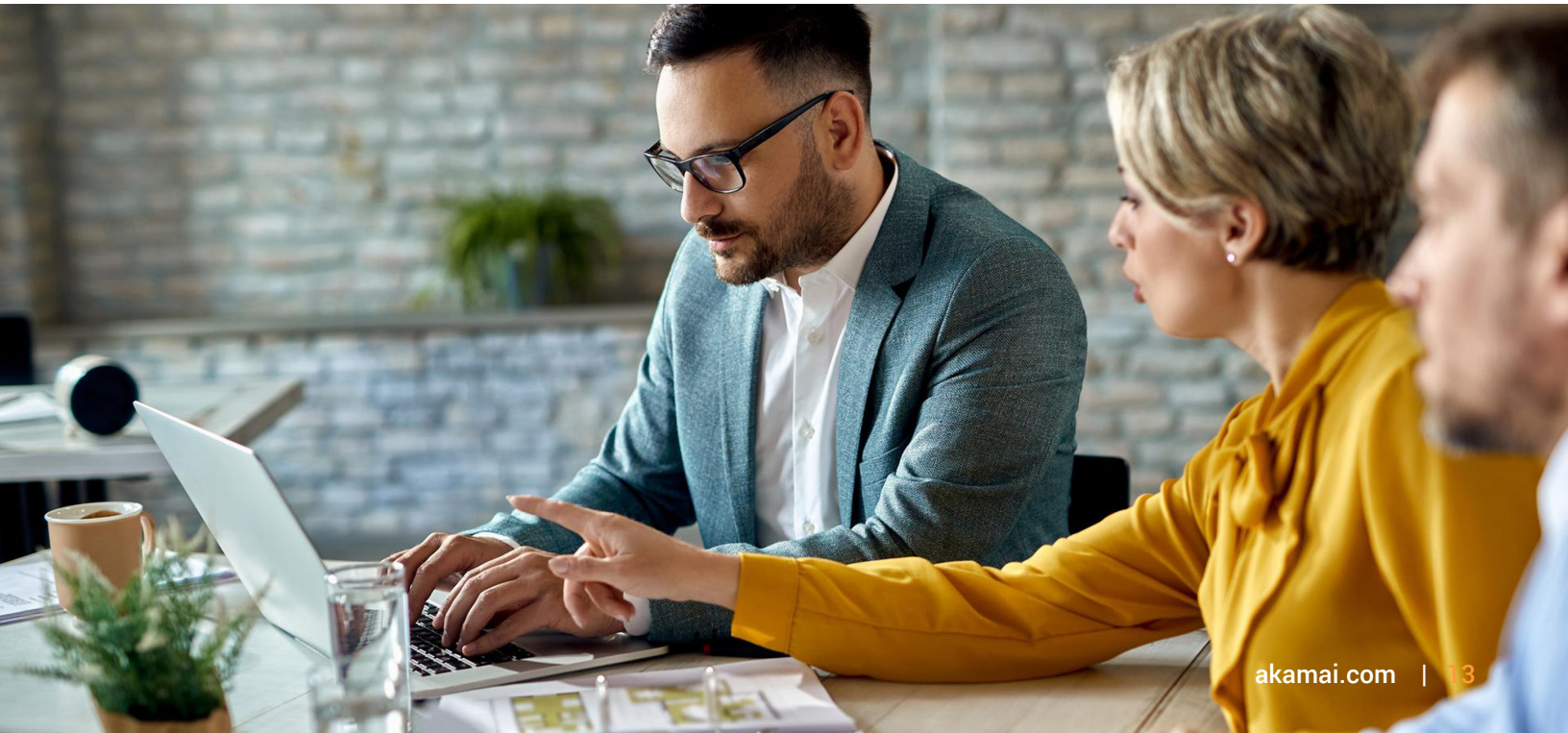
This customer story highlights how this insurer uses Akamai's solutions to enhance security and performance. Akamai's offerings help in mitigating DDoS attacks and securing APIs, which are crucial components for maintaining ICT risk management and incident response — key aspects of many compliance regulations.

CashFlows

By implementing Akamai's security solutions, CashFlows protects its cloud-hosted payment platform against threats like DDoS attacks. Maintaining the continuous availability and security of payment services aligns with ICT risk management and digital operational resilience testing requirements.

LANDBANK

As the largest government-owned bank in the Philippines, LANDBANK relies on Akamai to secure its online applications and protect against cyberthreats by simplifying its digital transformation. This example demonstrates how Akamai helps manage third-party risks and ensure robust incident management processes.



What to look for in a technology partner

Choosing the right technology partner for threat monitoring and security solutions is crucial for financial institutions. Key factors to consider include:

Effective algorithms

Look for partners with sophisticated algorithms capable of detecting and mitigating complex threats

Strong signal detection

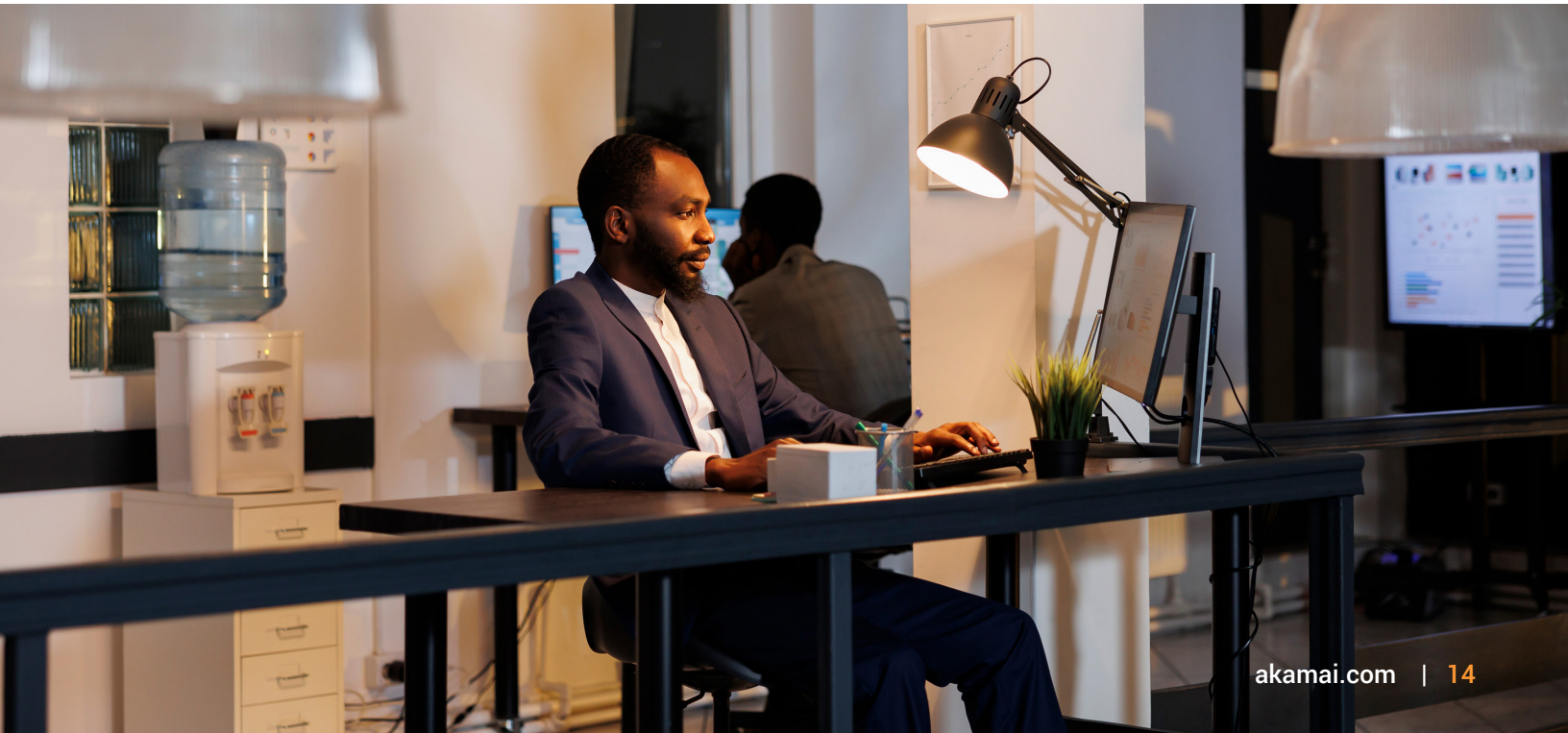
Ensure the partner has capabilities robust enough to identify subtle indicators of potential attacks

Experienced staff

Choose a partner with a proven track record and experienced personnel who understand the unique challenges of the financial services sector

Lower total cost of ownership

Opt for solutions that offer cost efficiency without compromising on security and performance



Commitment to operational excellence

Choose a vendor with a strong commitment to continuous improvement and operational excellence, which is essential for maintaining high standards of security

Single vendor for multiple solutions

Work with a single vendor that can provide multiple security solutions to simplify management and integration

Performance

Ensure that the solutions provided by the partner deliver high performance and do not degrade the user experience

Learn more about our solutions for financial services.

Akamai

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, formerly known as Twitter, and LinkedIn. Published 01/25.