
Akamai
Financial Services Regulatory Compliance
5 key business objectives

Table of contents

Akamai

Improved compliance capabilities in financial services can lead to a better customer experience, greater productivity, and resilient growth.

In the fast-paced world of financial services, staying compliant and maintaining operational resilience are critical. This ebook offers a structured approach to simplifying compliance, boosting productivity, enhancing the customer experience, managing security costs effectively, and building resilience and trust. While compliance alone doesn't ensure total security, it remains a top priority for executive teams because failed audits can lead to business disruptions and have serious financial impacts.

Compliance assessments are notoriously time-consuming and resource-intensive for security teams. The shift to perimeterless digital environments and the rise of remote work have only added to the challenge. Financial institutions must isolate their environments and ringfence regulated assets to meet standards like the Payment Card Industry Data Security Standard (PCI DSS), the Digital Operational Resilience Act (DORA), and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system. This ebook provides insights and strategies to help a financial institution navigate these complexities and achieve the following **5 key business objectives**:

1. **Simplify compliance**
2. **Boost productivity**
3. **Enhance customer service**
4. **Manage security and compliance costs effectively**
5. **Build resilience and trust**

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 to do business.

Our clients include:

All top **20** brokerages

17 of the top **20** banks

7 of the top **10** fintech companies

1

Simplify compliance

By dividing networks into smaller perimeters and isolating individual workloads, microsegmentation solutions can narrow the scope of compliance environments, streamline regulatory audits, and restrict access to sensitive information while delivering unparalleled visibility into network traffic and data flows.

Reduced scope of compliance environments

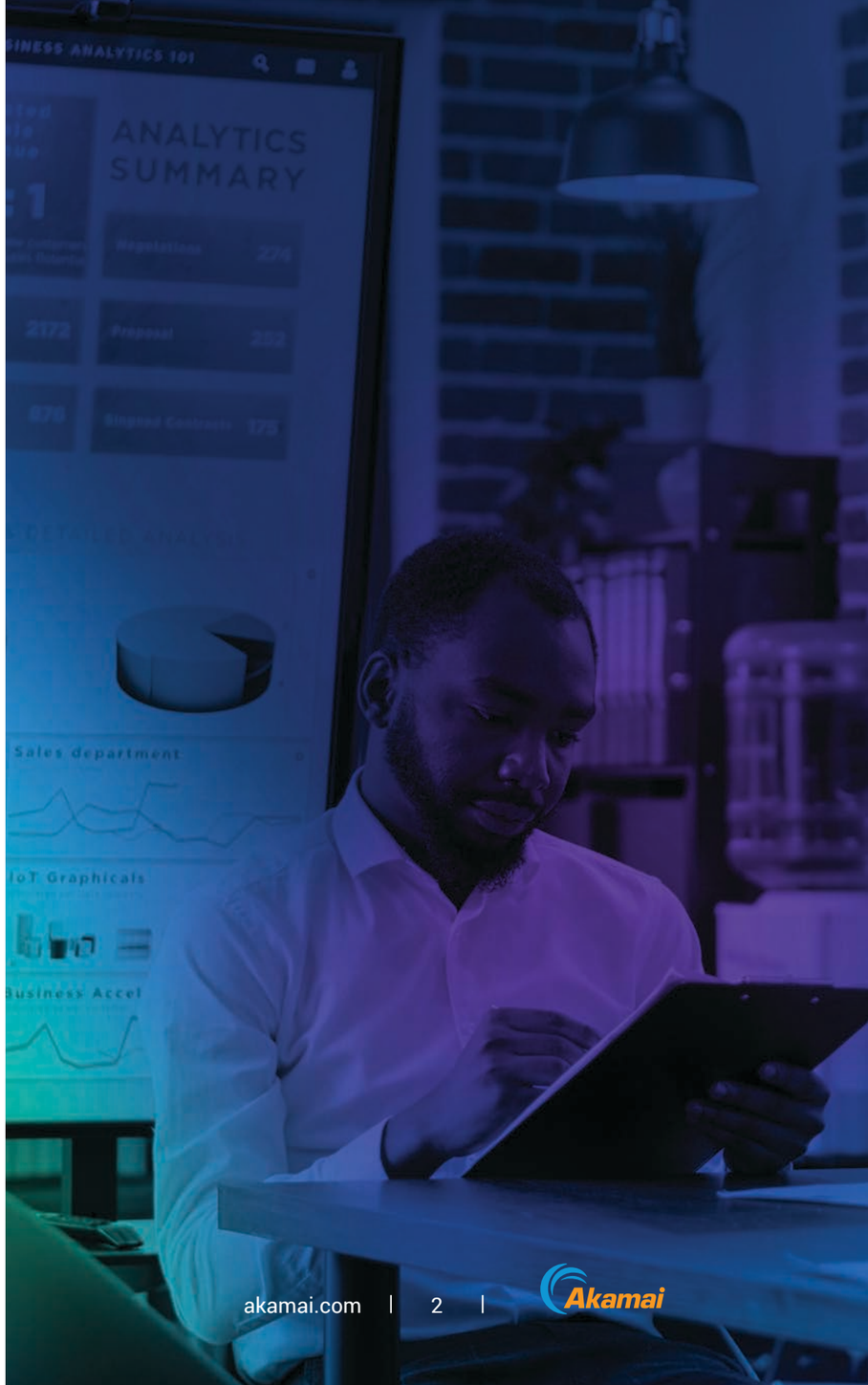
Segmenting compliance-related data from other IT assets significantly minimizes the scope of compliance efforts, reducing cost and complexity. Financial institutions can focus their compliance activities on specific segments of the network, making the process more efficient and less resource-intensive.

Streamlined compliance efforts and audit processes

Microsegmentation simplifies the job of complying with audit requests and processes by reducing the scope of compliance environments and making it easier to demonstrate compliance. This streamlined approach not only saves time but also enhances accuracy in meeting regulatory requirements.

Protected APIs

Implementing robust API security measures, as outlined in the latest Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook, helps financial institutions safeguard APIs, protect confidential data, and defend against attacks. This is crucial for maintaining compliance with stringent API security regulations.



2

Boost productivity

Unified security management

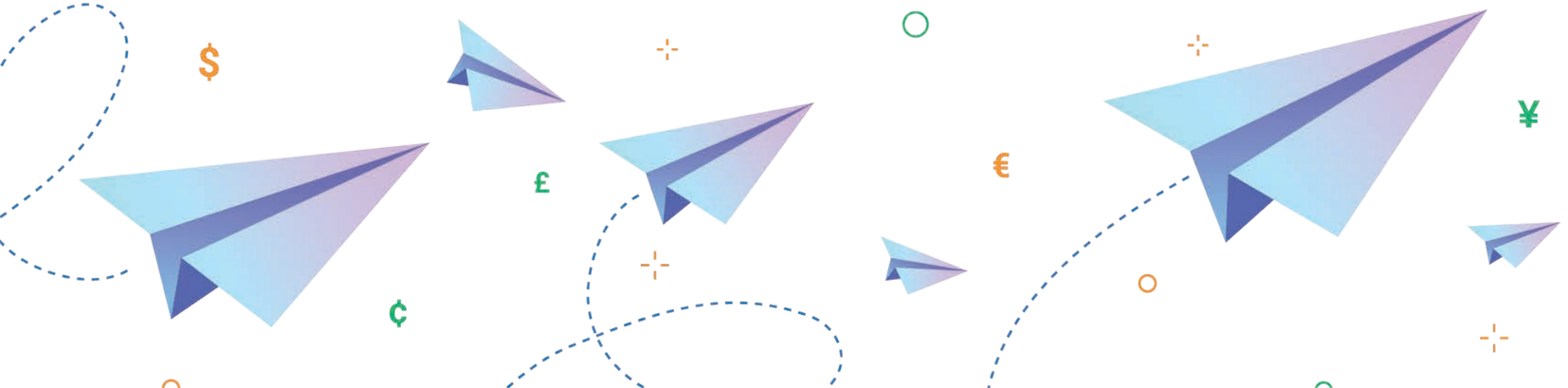
Consolidating security management with Akamai's unified platform reduces the time spent managing multiple security solutions and improves operational efficiency. This approach allows security teams to focus on strategic initiatives rather than operational firefighting.

Proactive threat hunting

Enhancing productivity through proactive threat hunting identifies and neutralizes threats before they impact operations, ensuring smoother business continuity. Akamai's advanced threat detection and mitigation capabilities allow for efficient resource allocation.

Advanced API protection

By using runtime protection capabilities powered by artificial intelligence (AI) and machine learning (ML), financial institutions can detect and block advanced API attacks in real time, which can thwart sophisticated threat actors and enhance overall productivity.



3

Enhance customer support

Seamless user access

Ensuring a seamless and secure customer experience with Akamai's edge security solutions protects user data and maintains high performance, regardless of the user's location. Improved service availability through distributed denial-of-service (DDoS) protection and load balancing ensures continuous service, which is crucial for maintaining customer trust and satisfaction.

Personalized security policies

Implementing personalized security policies that adapt to individual user behaviors and needs enhances the overall customer experience while maintaining robust security. Akamai's solutions ensure that financial institutions can deliver a secure and personalized experience to their customers.

Real-time API monitoring

Auditing API behavior using real-time analytics enables financial institutions to swiftly detect and respond to threats to protect sensitive data and ensure a smooth and secure customer experience.

4

Manage security and compliance costs effectively

Scalable security solutions

Akamai's scalable security solutions grow with your business needs, providing cost-effective protection without the need for significant capital investment. This scalability ensures that financial institutions can effectively manage their security and compliance costs.

Reduced operational costs

Lowering operational costs by using Akamai's cloud-based services eliminates the need for maintaining expensive on-premises infrastructure. Akamai's comprehensive risk management framework helps identify, assess, and mitigate risks efficiently, which can reduce potential financial losses from security breaches.

Simplified compliance audits

By reducing the scope of compliance environments and making it easier to demonstrate compliance, Akamai's microsegmentation solutions simplify the audit process, saving time and reducing the overall cost of compliance management.

It also provides the agility today's financial institutions need so that they can quickly tweak interfaces, optimize visualizations, adjust business rules, and integrate new information. The result is a much more complete and adaptable solution that aligns with the pace of case-management demands.

5

Build resilience and trust

Enhanced operational resilience

Achieving a high level of digital operational resilience is critical for financial institutions to navigate the ever-evolving threat landscape. Akamai's solutions help institutions prevent, respond to, and recover from cybersecurity incidents, ensuring continuous operation and fostering customer trust.

Robust security measures

Regulators worldwide emphasize the need for robust cybersecurity measures. Akamai's comprehensive security portfolio aligns with these regulatory requirements, providing institutions with the tools necessary to maintain operational resilience and protect against advanced threats.

Trust and stability

Akamai's security solutions not only protect against current threats but also build a foundation of trust and stability. By embedding security into the core of their operations, financial institutions can ensure long-term resilience and maintain the confidence of their customers.

> Understanding your exposure and then being able to manage it is key. The visibility of what is going on in your environment is a huge risk identifier. By monitoring red team activity, we were able to quickly build policies to block common attack vectors.
>
> **– CISO, registered securities broker-dealer**

Global bank achieves SWIFT compliance in two weeks

External regulators required one of Akamai's clients, a global bank, to ringfence all its critical applications to meet the requirements of SWIFT, which is a secure process for transferring money between financial institutions. Typically, an application like this requires more than 100 servers deployed in different locations, including bare-metal and virtual servers. On average, this process would take a bank of its size between 8 and 12 months to plan and execute, because it would have to create a virtual local area network (VLAN) for the segment across multiple locations. Determining the dependencies of the SWIFT application and making sure the ruleset was correct would have only added to the timeline.

Meanwhile, the project would also require purchasing new firewall equipment. And because the SWIFT application is critical to the banking business, the bank cannot tolerate downtime. All in all, the segmentation project was expected to require a massive effort by many people.

With Akamai, however, the whole process took just one security engineer approximately two weeks to complete; it did not require any network changes and the bank avoided any application changes or downtime.

TIME SAVED
226–351 days

FTE REDUCTION
> 4 FTEs

ALL WHILE ENSURING
0 downtime
AND ENHANCED VISIBILITY

Saved time and enhanced visibility

A financial institution needed to ringfence its SWIFT application within a complex environment comprising bare-metal, VMware, and OpenStack infrastructure. Traditional segmentation methods were proving to be challenging, requiring 8 to 12 months and more than five full-time employees (FTEs) to complete, with additional issues of downtime and lack of visibility into applications and dependencies. By implementing Akamai Guardicore Segmentation, the institution completed SWIFT application mapping in hours, with automatically suggested and fine-tuned segmentation policies. There was no need for new hardware or firewalls, and the entire process was completed in two weeks with just one FTE.

Conclusion

Akamai provides comprehensive solutions that help financial institutions navigate the complex landscape of regulatory compliance and cybersecurity. By leveraging advanced technologies such as microsegmentation, financial institutions can achieve simplified compliance, enhance productivity, improve customer experience, manage security and compliance costs effectively, and build resilience and trust. Akamai's proven track record and innovative solutions make it an ideal partner for financial institutions that are looking to strengthen their security posture and ensure regulatory compliance.

Learn more about our solutions for financial services

Akamai security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale and visibility of our global platform, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision.

 | Support | | Published 09/24