WHITE PAPER

Turn Compliance into a Competitive Advantage with Akamai Security

A four-pillar approach to boost security and prepare for audits

Focus on four security pillars to pave the way to compliance

Today, organizations worldwide find themselves navigating an increasingly challenging maze of regulations — from GDPR and HIPAA to PCI DSS and a growing array of regional mandates. But demonstrating compliance readiness isn't just about satisfying regulators — it's become essential for maintaining trust with customers and internal stakeholders like senior leaders and the board.

Indeed, the implications of compliance failures extend far beyond direct regulatory penalties. The costs of non-compliance include business disruption during the investigation and remediation stages, reputational damage, and increased legal exposure. If an organization falls afoul of compliance mandates, it can lead to lost revenue through customer churn and significant operational costs as resources are diverted to remediation rather than innovation. In 2024, the 35 largest breaches globally racked up $3 billion in penalties, and 23 of them cited violations tied to the European Union's General Data Protection Regulation (GDPR) rules as the cause, according to Forrester.

In the past, security teams addressed compliance as regulations emerged. But now, with technology advancing rapidly and attacks growing larger and more intense, compliance needs to be part of the discussion as they evaluate tools and maturity models. Teams need to ask themselves: "How will my security choices today help me meet compliance requirements now and in the future?"

At Akamai, we help customers answer that question by focusing the conversation on four pillars of security best practice that also naturally advance key areas of compliance readiness. Those pillars are:

- Achieve visibility across the IT estate
- Prevent lateral movement (across networks, apps, and APIs)
- Prevent unauthorized access
- Protect sensitive customer data and account information

The result yields a clear competitive advantage. Organizations are not only more secure; they are better prepared to clear regulatory hurdles. In being more secure and compliant, they are also better able to gain the trust of customers and internal leadership.

Pillar 1

Achieve visibility across the IT estate

The foundation of compliance readiness begins with comprehensive visibility across all digital assets. Organizations cannot protect what they cannot see, and regulators increasingly require evidence of complete asset inventory, continuous monitoring, and threat awareness.

It's not so easy. A recent Forrester study found that more than half (52%) of financial firms agree/strongly agree that they lack full visibility into their IT estate. Unfortunately, the stakes of non-compliance are high — for any industry. The number of organizations paying more than US$100,000 in regulatory fines jumped nearly 20% between 2023 and 2024.

For many organizations, the challenge with visibility lies in monitoring network traffic and APIs. Here are a few regulations and standards calling for a clear view into risk:

- The Payment Card Industry Data Security Standard (PCI DSS) contains guidance to confirm that an enterprise's software securely uses the functions of external components, such as APIs that transmit payment data from a mobile app to a bank's system.
- Standards such as the International Organization for Standardization (ISO) IEC 27001 require segregating data and data processing facilities in the event that an attacker breaks into the network.
- The Data Security Law of the People's Republic of China requires robust security controls to secure access to customers' personal information through technologies that exchange sensitive data across different IT systems.

Many companies have tools or processes that can meet some of these requirements. However, as they expand to hybrid computing environments and across geographies, monitoring becomes far more difficult. That's especially true for APIs. According to Akamai research, only 27% of security professionals who have full API inventories actually know which of their APIs return sensitive data — down from an already-concerning 40% in 2023.

Ultimately, organizations need to know where their sensitive data is and what's accessing it in order to know where to focus their security efforts. That requires visibility into:

- Which assets are communicating with the network (with real-time and historical views), including Layer 7 processes and edge traffic, across hybrid cloud and on-premises environments
- API inventory, including shadow and zombie APIs, showing where they integrate with traffic sources and code
- Client-side JavaScript — which is particularly important for the most recent PCI DSS requirements

Akamai's portfolio can help security teams gain the visibility they need.

Akamai Guardicore Segmentation can identify and visualize assets communicating within the network across the IT estate, including Layer 7 process, hash, and command line details. It also offers historical visibility for attestation during compliance audits to prove in-scope assets have not been compromised. North–south and east–west traffic visualizations also show where access is happening.

API Security provides a real-time inventory of APIs that organizations require for compliance and can help identify where and when unencrypted data might be flowing through APIs.

App & API Protector delivers application-level visibility, including API inventory, detection of sensitive data exposure, and real-time traffic analysis.

Client-Side Protection and Compliance provides the visibility into client-side scripts required by PCI DSS v4.

One healthcare organization implemented Akamai Guardicore Segmentation to address HIPAA and SOC 2 compliance requirements. It delivered valuable views into traffic flows between different apps. The security team could inspect granular details beyond Layer 4 logs: user IDs, command-line inputs, and even service correlations.

Pillar 2

Prevent lateral movement

Like security teams themselves, many regulators accept that even with a strong security posture, a breach can happen, and they seek assurances that businesses can limit the damage done in the event it does. For example:

- GDPR Article 32 requires "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident."
- PCI DSS v4 similarly requires organizations to "Implement firewalls to protect credit card holder's data and ensure the firewalls are configured to restrict connections among trusted and untrusted networks."
- **The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001** calls for the segregation of information and data-processing facilities to protect the confidentiality, integrity, and availability of information.

While most organizations have some form of firewall, limiting lateral movement once a malicious actor is inside the network requires a greater level of control. This makes microsegmentation, preferably software-defined, a key tool in achieving compliance. Akamai is well-positioned to address the lateral movement concerns of auditors.

Akamai Guardicore Segmentation provides the limits on lateral movement that organizations need to stay compliant. Out-of-the-box policy templates facilitate rapid enforcement for compliance-related initiatives with granular Layer 7 controls. And because it's software-defined, it can provide the same level of granular protection no matter where assets reside. Additionally, its ability to identify apps communicating within the network and communication attempts between segmented zones gives auditors another level of confidence in your ability to mitigate threats.

Attackers are finding new opportunities for lateral movement, thanks to the proliferation of APIs — particularly API endpoints that are vulnerable to Broken Object Level Authorization (BOLA) attacks. Threat actors can manipulate object IDs in API requests to enable lateral movement in the network. Once inside, threat actors can bypass authorization, escalate privileges, and gain access to customer data.

Akamai API Security can flag APIs that expose sensitive data without the proper authentication and identify APIs with weak or misconfigured access controls that could lead to unauthorized data access and lateral movement. The integration with Akamai Web Application Firewall (WAF) also allows API Security to block malicious threats in real time.

One Akamai customer, a global financial services organization, implemented API Security because it was struggling with unknown APIs in its environment. The deployment dramatically reduced its API sprawl and improved compliance, as Akamai API Security classifies sensitive data to help satisfy regulations like GDPR, HIPAA, and more. During regulatory audits, these implementations serve as direct evidence that the company has taken appropriate technical measures.

Today's AI threats are tomorrow's regulatory hurdles

Today, any examination of an organization's cybersecurity defenses must address the specter of AI. The rapid proliferation of AI-powered applications, large language models (LLMs), and generative-AI-linked APIs have introduced new vulnerabilities that many organizations are not yet aware of. Examples of these kinds of applications include AI-powered chatbots, retail recommendation engines, health diagnostic tools, and risk decision engines. Meanwhile, threat actors are taking advantage of AI to launch more sophisticated attacks.

And anywhere threats to business operations and the public emerge, regulation is likely to follow.

Organizations looking to protect their investments in AI, their data, and their customers are looking to Akamai for help. As a security provider with a strong track record of meeting the visibility, lateral movement, and access control requirements of today, Akamai has proactively invested in meeting the AI requirements of tomorrow. Akamai has developed advanced AI capabilities to strengthen its security solutions and has now introduced a solution to help organizations protect their own AI investments.

Akamai Firewall for AI provides comprehensive security for AI-driven applications by identifying and mitigating AI-specific threats and attacks that traditional security tools aren't designed to address. Firewall for AI's purpose-built protections include:

- **Prompt injection defense** — protects against attackers manipulating AI models through deceptive inputs
- **Data loss prevention (DLP)** — detects and blocks sensitive data leaks in AI-generated responses, as well as protects against receiving sensitive data in the requests
- **Toxic and harmful content filtering** — flags hate speech, misinformation, and offensive content before delivery
- **Adversarial AI security** — protects against remote code execution, model backdoors, and data-poisoning attacks
- **Denial-of-service mitigation** — mitigates AI-driven DoS attacks by controlling excessive query usage and model overload

Additionally, Firewall for AI can help organizations comply with existing privacy, safety, and security guidelines. By enforcing AI-specific security policies, businesses can mitigate risks related to data protection regulations, ethical AI usage, and corporate governance mandates.

Pillar 3

Prevent unauthorized access

Controlling access to sensitive systems and data represents a cornerstone of compliance across virtually all regulatory frameworks. Organizations must understand their app and API security posture and prevent unauthorized access and abuse. That demands authenticating users appropriately, authorizing access on a need-to-know basis, and maintaining detailed records of all access activities.

For full access control that satisfies regulatory requirements, organizations must address three key challenges. Akamai's security portfolio can help deliver in-depth defenses that address each of them:

1. **Gain a comprehensive understanding of their app and API security posture**

Akamai's App & API Protector allows organizations to enforce traffic policies across all environments in which they're running, while Akamai API Security can alert an organization to any unusual activity and unauthorized data access or misconfigurations, all of which are key considerations for auditors. Meanwhile, Akamai Guardicore Segmentation can track all apps communicating within the network and establish a baseline for activity.

2. **Monitor user behavior and limit access to sensitive information**

Akamai Guardicore Segmentation limits access within the network based on user identity while **App & API Protector** enforces traffic policies with AI-powered threat detection to prevent breaches. Finally, **Client-Side Protection & Compliance** monitors JavaScript execution behavior to mitigate client-side attacks.

3. **Detect and limit fraudulent activity**

API Security can help by detecting anomalous API behavior and misconfigured authentication controls to block high-risk attacks. Akamai Guardicore Segmentation protects the network by flagging and blocking suspicious connections that might indicate fraudulent activity. App & API Protector detects and mitigates threats identified by OWASP to further reduce the risk of fraud.

NIS2 and securing access

The updated Network and Information Security Directive (NIS2) is designed to create a common level of cybersecurity across EU member states. Among the recent additions to NIS2 is that enterprises must build an information security management system that assesses people, policies, and technology to protect sensitive data and ensure operational resiliency. NIS2 also contains an increased emphasis on securing IT supply chains and third-party supplier relationships.

Pillar 4

Protect sensitive customer data and account information

The final pillar of a comprehensive regulatory readiness approach demands organizations have plans in place for sensitive data. Securing the data of customers, patients, partners, and more is at the heart of most security-focused regulations.

For example, Japan's Act on the Protection of Personal Information requires data protection impact assessments that can identify and mitigate risks for technologies that process large volumes of personal data or involve high-risk data processing activities.

For U.S. financial institutions, the Federal Financial Institutions Examination Council (FFIEC) requires controls that ensure APIs only allow access to specific data for authorized users via layered security — for example, monitoring, logging, and reporting.

Addressing this pillar begins with threat detection. Akamai's web application and API protection solution **App & API Protector** offers the first layer of defense, while **Akamai Guardicore Segmentation** monitors and segments north–south and east–west traffic. Akamai's **Bot Abuse & Protection portfolio of solutions** adds an additional layer of security against automated threats and human-based attacks.

However, to properly identify threats, organizations also need to understand the baseline behavior within their network. Here is how Akamai Security capabilities can provide these critical insights:

- Akamai API Security and Akamai Guardicore Segmentation, respectively, provide the baseline understanding of APIs and apps communicating within the network to flag any anomalous behavior.
- Adaptive Security Engine — a core technology of App & API Protector — learns attack patterns by using local and global data to make customer-specific adjustments to protections while adapting to future threats.
- Akamai Hunt, a managed threat-hunting service leveraging Akamai's expert research team, lets businesses take a more proactive approach to defense.

DORA and data security

The Digital Operational Resilience Act (DORA) is designed to help financial services organizations in EU member states withstand and recover from cyberattacks. With DORA, the sector has a binding, comprehensive risk management framework for information and communication technology (ICT). DORA Article 3 requires organizations to use ICT solutions and processes that:

- Minimize data-related risks, unauthorized access, and technical flaws
- Prevent data unavailability, data loss, and integrity and confidentiality breaches
- Ensure data transfer security

From compliance silo to competitive advantage

Effective compliance programs must demonstrate business impact beyond simply "checking the box" on regulatory requirements. Organizations implementing Akamai's compliance-focused security solutions have reported measurable improvements across three key dimensions.

Compliance cost reduction

Organizations with mature compliance programs typically spend less on compliance activities than those with ad-hoc approaches. Automating evidence collection through integrated security platforms can reduce audit preparation time significantly, as can consolidating point solutions onto a comprehensive platform.

Risk posture improvement

Beyond cost reduction, compliance improvements should deliver measurable risk reduction. Organizations implementing Akamai's segmentation solutions can restrict vulnerable lateral movement paths, directly addressing key compliance requirements while reducing organizational risk.

Comprehensive monitoring capabilities improve visibility that translates directly to risk reduction by eliminating blind spots where compliance violations might otherwise go undetected.

Operational efficiency

The third dimension of compliance impact involves operational efficiency improvements. Pre-approved controls and consistent security patterns can mean significantly faster security approvals for new applications. This improves developer satisfaction by reducing friction in security review processes and accelerating time-to-market for new applications.

Fine-tuning compliance

As regulatory requirements continue to evolve and organizations grow, they need a compliance approach that adapts. Akamai's integrated security portfolio provides the foundation for a compliance strategy that anticipates regulatory trends and scales with organizational growth.

- Configurable policy frameworks can adapt to new requirements without significant rearchitecting while extensible reporting capabilities can accommodate emerging evidence requirements as regulations evolve.
- Automated policy deployment for new assets ensures that compliance coverage extends automatically as the business expands.
- Centralized management capabilities maintain comprehensive visibility regardless of scale, while comprehensive API support enables automation of compliance processes to manage increasing complexity.

Additionally, organizations need to be proactive about establishing a regular cadence for reviewing regulations and updating their compliance controls accordingly. Akamai provides regular updates to our security solutions, specifically designed to address evolving compliance requirements, ensuring that customers maintain continuous compliance regardless of regulatory changes.

Conclusion: Compliance as a competitive differentiator

Effective compliance is no longer merely about satisfying regulatory requirements — it represents a strategic business imperative that directly impacts organizational performance, customer trust, and competitive positioning. No matter your industry or region, a proactive approach toward compliance ensures a strong and agile security posture.

By implementing an integrated security approach across the four pillars of compliance readiness — visibility across the IT estate, lateral movement prevention, unauthorized access prevention, and protection of sensitive customer data and account information — organizations can establish a sustainable compliance foundation that delivers measurable business value beyond regulatory satisfaction.

The organizations seeing the greatest success are those that have transformed compliance from a necessary cost of doing business into a strategic advantage that enables digital transformation while protecting what matters most — customer trust, data integrity, and business reputation.

Contact us to learn how Akamai can help your organization.

Contact us

 | Published 07/25