AKAMAI SOLUTION BRIEF

Preparing Financial Institutions for PCI DSS Compliance with Akamai

With PCI DSS v4.0 bringing the most significant changes to payment card industry security standards since 2004, financial institutions must adapt swiftly to remain compliant. This comprehensive framework, established by the PCI Security Standards Council, mandates rigorous measures to protect cardholder data. Akamai's solutions empower financial institutions to meet these evolving requirements through advanced security features, continuous monitoring, and robust penetration testing. Our tools are designed to streamline compliance, safeguard customer information, and assist your institution for readiness by PCI's March 2025 deadline.

Unified compliance: Simplifying PCI DSS with one provider

For financial institutions, PCI DSS compliance involves not only employee training and corporate policies but also sophisticated security software to meet most of the requirements. Given the comprehensive nature of these requirements, this often means working with multiple providers. Some requirements might necessitate a firewall, while others cover identity management. Financial institutions that can find a single provider with integrated technology will benefit from a simplified audit process and enhanced security for their customers' financial information. Adopting robust cybersecurity solutions that address these requirements as part of a broader security strategy can result in cost savings and reduced complexity in the long run. Akamai's portfolio of solutions comprehensively addresses existing and upcoming PCI DSS requirements, providing a seamless experience for financial institutions.

Addressing scope

A significant challenge for financial institutions seeking to meet PCI DSS requirements is the issue of scope. Applications and network environments that are considered "in scope" by PCI can be complex, spanning different types of infrastructure, technology, and locations. As financial institutions have embraced cloud infrastructure and SaaS-based applications, this hybrid environment of on-premises and on-demand services adds an additional layer of complexity. For financial institutions, including those with autoscaling ecommerce businesses, understanding the location of a given workload at any time can be particularly challenging.

Financial institutions have turned to internal firewalls, VLANs, and access control lists to address the challenge of scope. However, these legacy applications often struggle to keep pace with hybrid environments, introducing additional complexity, downtime, and operational overhead while leaving security gaps.

Benefits

- **Streamline security and compliance workflows**
- **Cut audit burdens with dedicated PCI capabilities**
- **Receive and log actionable PCI compliance alerts**
- **Protect sensitive financial data**
- **Boost operational efficiency and cut compliance costs**

Akamai Guardicore Segmentation delivers visibility into the cardholder data environment (CDE) and its boundaries — a crucial step in the compliance process. This visibility helps financial institutions meet multiple requirements in PCI DSS and provides comprehensive oversight of their network. For example:

- Requirement 1.2.3 demands that organizations have a diagram of their network. Akamai Guardicore Segmentation's dashboard displays all links between the CDE and other networks, helping financial institutions meet this requirement.
- Requirement 1.2.4 demands that organizations maintain a data flow diagram that shows how account data moves across systems and networks. Akamai Guardicore Segmentation's dashboard aids financial institutions in validating this requirement by displaying the necessary connections.

Addressing controls

- Requirement 1.2.5 specifies the necessity to identify, approve, and have a clear business justification for all permitted services, protocols, and ports. Akamai Guardicore Segmentation helps financial institutions meet this requirement by implementing policies that are universally enforced, determining which protocols or services are permitted and which are not.

Addressing client-side protection

Financial institutions that accept payment card data aren't only responsible for their own environments. The use of JavaScript in modern web development has introduced innovation and consistency, but it has also created challenges for payment card processors. JavaScript's decentralized client-side execution and third-party dependencies make it extremely difficult for financial institutions to monitor and manage. Attackers have exploited this blind spot by injecting harmful code into websites on the client side to steal sensitive data. These types of attacks — including web skimming, formjacking, and Magecart — have grown in popularity, leading to new requirements around client-side protections and script monitoring.

PCI DSS v4.0 will require financial institutions to track, inventory, and justify all JavaScript executing on their public-facing website's payment pages. Under requirement 6.4.3, they will need to assure the behavioral integrity and authorization of all scripts, as well as provide an inventory of these scripts with written justification of their individual necessity. Additionally, under requirement 11.6.1, financial institutions need to detect and respond to any unauthorized changes made on their payment pages. Authorized personnel must be alerted to any modification, including indicators of compromise, changes, additions, or deletions, to HTTP headers and payment page content by the consumer's browser.

> “
>
> With Akamai Guardicore Segmentation, we have significantly reduced our attack surface with none of the costs and delays associated with upgrading legacy firewalls.
>
> **– Dave Wigley,**
> **CISO, Daiwa Capital Markets Europe**

In summary, PCI DSS v4.0 requires financial institutions to:

- Maintain an inventory and justification of every script executed on payment pages
- Ensure all scripts are authorized and performing the actions they are intended to
- Establish detection, alerting, and response mechanisms to address unauthorized changes to scripts, protection tampering, and data exfiltration on payment pages

Akamai Client-Side Protection & Compliance provides broad support to help financial institutions meet requirements 6.4.3 and 11.6.1 of PCI DSS v4.0. It automatically tracks and inventories scripts on payment pages, boosting their integrity and authorization. Security teams can easily justify the purpose of scripts executing on payment pages with predefined justifications and automated rules. The solution also monitors for changes in HTTP headers and payment page protections to defend against page tampering. A comprehensive dashboard and dedicated PCI alerts make it easy to rapidly respond to compliance-related events and provide auditing evidence.

Protecting against attacks

Protecting cardholder data is a core principle of PCI DSS, but as web apps and APIs proliferate, they can also become entry points for attackers. To comply with PCI DSS, financial institutions need strong protections against malware, zero-day attacks, and other efforts that can lead to data leakage.

Akamai App & API Protector with the Malware Protection module can help financial institutions protect themselves against payment card information data leakage by scanning files at the edge of the network before they can get inside and start spreading malware. APIs can introduce new vulnerabilities that attackers seeking payment card data will exploit. Many financial institutions can't even account for all their APIs, let alone attest that they are secure. Any API that receives or transmits cardholder data falls under the scope of PCI DSS, meaning financial institutions need to monitor API development and authentication and secure these APIs.

Akamai API Security automates the continuous discovery of APIs across your environment. It assigns a risk score to the API and endpoint by comparing APIs to existing documentation and notifying security, developer, and API teams of misconfigurations and vulnerabilities. This continuous automation means that vulnerabilities are assessed when you finalize updates to your API estate.

Conclusion

While the ultimate goal of implementing PCI DSS controls is to protect cardholder data, thus safeguarding your customers and your business, financial institutions still need to satisfy auditors. This is where a single provider offers distinct advantages. With both real-time and historical views of your network, you can more quickly and easily satisfy many aspects of your audit. Moreover, working with a single provider with demonstrated leadership in the sector — and a stable of customers that have successfully met PCI DSS requirements — can lead to smoother implementations, faster audits, and ongoing compliance support. Akamai's comprehensive visibility and integrated solutions help financial institutions streamline compliance efforts and fortify their defenses against evolving threats.

To learn more, visit akamai.com or contact your Akamai sales team.