AKAMAI SOLUTION BRIEF

PCI DSS v4.0 in the Games Industry: An Overview

Introduction to PCI DSS v4.0

The Payment Card Industry Data Security Standard (PCI DSS) v4.0 is the latest iteration of the security standards designed to protect cardholder data and ensure the security of payment systems. Released in March 2022, PCI DSS v4.0 introduces new requirements and enhances existing measures to address evolving cyberthreats and technological advancements.

Relevance to the games industry

The games industry, which has grown exponentially in recent years, often involves complex online payment systems, in-game purchases, subscriptions, and microtransactions. With millions of transactions occurring daily, the need for stringent data security is paramount. Compliance with PCI DSS v4.0 is crucial for game developers, publishers, and platform providers to protect users' sensitive information and maintain trust.

Key aspects of PCI DSS v4.0 in games

Enhanced security controls and data protection

- **Increased flexibility:** PCI DSS v4.0 offers more flexibility in how companies meet their security objectives, allowing for customized controls that fit unique business models like those in the games industry. This is particularly important for developers who may operate across different platforms (mobile, console, PC) and need adaptable security measures.
- **Multi-factor authentication:** The requirement for multi-factor authentication (MFA) is emphasized, ensuring that only authorized personnel have access to sensitive payment systems. In games that often have their back-end systems and customer accounts targeted, MFA can mitigate unauthorized access.
- **Isolation of cardholder data:** Microsegmentation allows games companies to isolate environments that handle cardholder data from other parts of the network. By strictly controlling communication among these segments, the risk of unauthorized access or data breaches is significantly reduced.
- **Granular access control:** With microsegmentation, access to each segment can be tightly controlled based on specific roles, tasks, or devices. This ensures that only authorized personnel can access sensitive payment data, which is a core requirement of PCI DSS.

Why Akamai?

Industry knowledge
Decades of experience working with game companies

Real-time monitoring
Microsegmentation, Zero Trust Network Access, and MFA monitoring of network traffic

Distributed cloud
Lower latency, faster transactions, and better game experience

Improved network security and compliance

- **Minimized attack surface:** By breaking down the network into microsegments, the attack surface is minimized. Even if an attacker gains access to one part of the network, microsegmentation can prevent the threat actor from moving laterally to more sensitive areas, such as those containing payment data.
- **Real-time monitoring and response:** Microsegmentation solutions often include advanced monitoring tools that provide real-time visibility into traffic within each segment. This capability is crucial for detecting and responding to potential threats quickly, helping to maintain continuous PCI compliance.

Focus on continuous compliance

- **Ongoing risk assessment:** PCI DSS v4.0 encourages continuous monitoring and regular risk assessments. This approach aligns well with the dynamic nature of game platforms, where new features, updates, and expansions are frequent. Regular assessments help identify potential vulnerabilities introduced by such changes.
- **Security awareness training:** The standard emphasizes the need for security awareness across all employees. In the games industry, where creative and development teams might not traditionally focus on security, this requirement ensures that everyone is informed about the importance of protecting cardholder data.

Continuous monitoring and threat detection

- **Real-time monitoring:** Zero Trust involves continuous monitoring of all network traffic, user activity, and device interactions. This aligns with PCI DSS requirements for regular monitoring and testing of networks to identify and respond to threats quickly. In the games industry, where threats can emerge rapidly and unexpectedly, real-time monitoring helps ensure that any suspicious activity is immediately flagged and addressed.
- **Behavioral analysis:** Zero Trust systems often incorporate behavioral analysis to detect anomalies in user or device behavior. This adds an extra layer of security, as it can identify potential threats even from users who have passed initial authentication checks. This is crucial in games, where compromised accounts could lead to unauthorized purchases or access to player data.

Scalability and flexibility

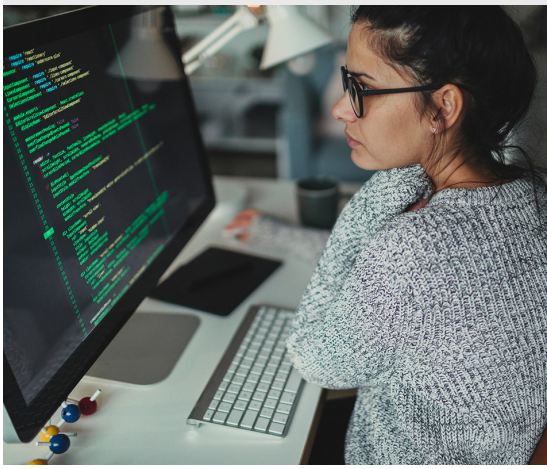
- **Adapting to growing game networks:** As game platforms expand and new features or payment methods are introduced, microsegmentation allows for scalable security controls. New segments can be created and secured without disrupting the entire network, ensuring that PCI compliance is maintained as the platform evolves.
- **Integration with DevOps practices:** In the games industry, where continuous development and deployment are common, microsegmentation can be integrated into DevOps pipelines. This ensures that security is built into the development process, and any new segments created during updates or expansions are compliant with PCI DSS.

Akamai products for games companies

Security
Zero Trust Network Access, multi-factor authentication, segmentation, DNS firewall, threat hunting, Akamai App & API Protector

Cloud computing
Compute, containers, storage, databases

Content delivery
Akamai Download Delivery, Akamai API Acceleration, Akamai EdgeWorkers



Technological advancements and future-proofing

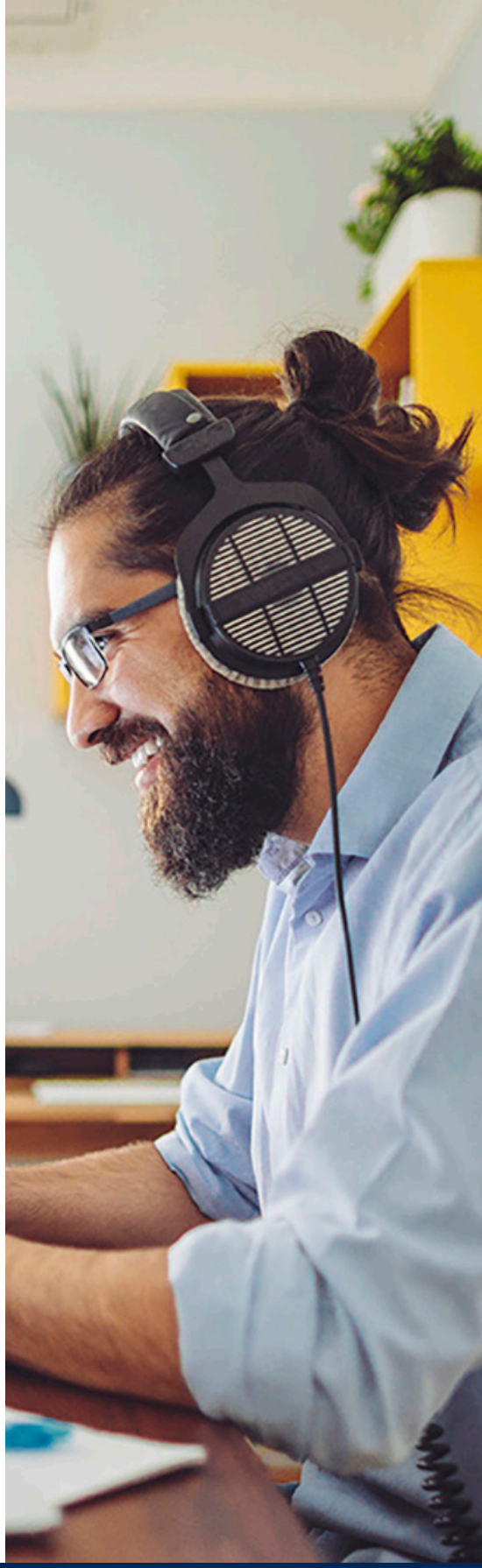
- **Cryptography and encryption:** PCI DSS v4.0 mandates stronger encryption standards, ensuring that cardholder data remains protected both in transit and at rest. Game companies, especially those that handle large volumes of microtransactions, need to implement robust encryption protocols to secure data against potential breaches.
- **Cloud security:** Many games companies use cloud services for storage and processing. PCI DSS v4.0 provides clearer guidelines on securing cloud environments, which is critical for the industry as it increasingly relies on cloud-based solutions for scalability and performance.

Increased focus on third-party risk management

- **Vendor management:** Games companies often work with third-party vendors for payment processing, customer support, and other services. PCI DSS v4.0 places a greater emphasis on managing the security of these third parties, ensuring that they also comply with PCI standards.

Conclusion

PCI DSS v4.0 represents a critical framework for ensuring the security of payment systems in the games industry. As the industry continues to grow and evolve, games companies must prioritize compliance to protect their users and maintain trust. By adopting the enhanced measures outlined in PCI DSS v4.0, games companies can safeguard cardholder data, mitigate risks, and ensure the long-term security of their platforms.



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