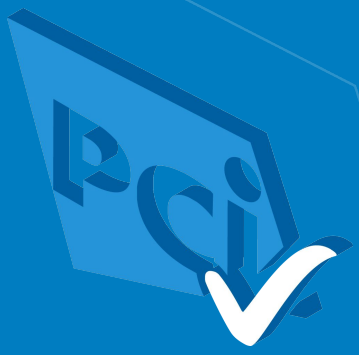
okta

Your PCI DSS Compliance Journey with Okta



Payment Card Industry Data Security Standards (PCI DSS) are designed to reduce risk of debit and credit card data loss. The standard's controls suggest how data loss can be prevented, detected and how to react if a potential data loss does occur. Among other controls, this standard requires strong multi-factor authentication to access servers and software handling credit card data, use of strong encryption, and ensuring that only authorized employees have access to credit card data.

In 2018, Okta announced our commitment to support customers who use Okta to protect cardholder data environments by releasing Okta's PCI DSS SAQ-D AOC. Now Okta is going a step further: Okta's PCI DSS SAQ-D has now been assessed by a QSA and is available to download. To access the PCI DSS SAQ-D AOC, Okta administrators of current customers must login to the Okta Help Center. Prospective customers interested in accessing the AOC should reach out to their Okta representative.

In this document, we'll share more information on these assessments and also discuss how you can use the Okta Identity Cloud to comply with PCI DSS v3.2.

PCI DSS: Background and Goals

To protect cardholder data around the globe, the PCI Council works with "merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments." Their work helps both these institutions understand and implement standards for security policies -- including processes to protect payment systems from breaches -- as well as vendors implement standards for creating secure payment solutions.

PCI DSS outlines 12 requirements for payment card security. These requirements can be complex and difficult to maintain, especially for larger organizations. We've grouped these requirements into six easy-to-understand goals:

GOAL 1

Safeguard cardholder data by implementing and maintaining a firewall

1. Install and maintain a firewall configuration to protect cardholder data as firewalls restrict incoming and outgoing network traffic through rules and criteria configured by your organization.
2. Focus on hardening your organization's systems and assets, e.g not using vendor-supplied defaults for system passwords and other security parameters help in reducing the risk of the known.

GOAL 2

Protect Cardholder Data

Cardholder data or customer account data need to be adequately protected when stored at rest (in the database) and when in transit. Implementing strong access control and making use of approved encryption techniques can help you protect your customer's cardholder data.

GOAL 3

Maintain a Vulnerability Management Program

Every organization should protect all systems against malware. Regularly updating the anti-virus software or programs and implementing secure system development techniques help in maintaining a bug free environment.

GOAL 4

Implementing Strong Access Control Measures

Implement strong access control measures, logical and physical, based on business justification or on a need-to-know basis to help reduce the inherent risk of data loss.

GOAL 5

Regularly Monitor and Test Networks

Track and monitor all access to network resources and cardholder data and regularly test security systems and processes help by preventing unauthorized access to cardholder data stored in your environment.

GOAL 6

Maintain an Information Security Policy

Maintain a policy that addresses information security for all personnel and make a central location for everything PCI, from running scans to employee guidelines, and more. This can help delegate PCI DSS specific responsibilities within your organization and also act as a guidance space for everything PCI.

Meeting PCI DSS Goals with Okta

Okta is a service provider for its customers who are in scope of PCI DSS requirements. The Okta Identity Cloud, including core IDaaS solutions like Single Sign-On (SSO), Lifecycle Management for provisioning, Multi-factor Authentication (MFA) as well as more recently released Advanced Server Access (ASA) and Okta Access Gateway (OAG), when implemented and configured correctly, can help Okta's customers meet PCI DSS requirements. Let's look at features of these products and how they can help you achieve PCI DSS goals.

Okta Identity Cloud (IDaaS)

The Okta Identity Cloud includes features such as user identity management, SSO login, Active Directory (AD) and lightweight directory access protocol (LDAP) integration, along with centralized provisioning and de-provisioning of users, multi-factor authentication, mobile identity management, and flexible policies for organization security and control. You can use a combination of these features to restrict access to your cardholder data based on business justifications maintained within your systems.

Okta captures a comprehensive set of events and states including user import, application assignment, activation and deactivation, Okta or application login, and application configuration change. The data is captured in real time and maintained historically to support both interactive troubleshooting as well as detailed reporting.

By maintaining a detailed set of logs and fine-grained access configurations, the IT admin or internal control testers can regularly test the security policies and processes because of the detailed view available based on access restrictions. In addition, Okta maintains an industry standard vulnerability management programs which provide additional assurances of safekeep of sensitive information managed by Okta.

Okta Access Gateway (OAG)

Traditional web applications pre-date modern standards like SAML and OpenID Connect, so they often use legacy authentication methods to grant end users access. Historically, providing Single Sign-On and centralized access management for end users across these legacy applications required a Web Access Management (WAM) product. These on-premise software tools could be expensive to maintain and complex to deploy. With the Okta Access Gateway (OAG), organizations can protect both on-premise and cloud apps from a single Identity Provider.

The Okta Access Gateway acts as a broker between Okta and on-premises resources. On the on-premises side, it connects to apps using the legacy patterns they natively support. On the cloud side, the gateway connects each application to Okta using the secure standards broadly adopted by SaaS platforms, thereby extending IDaaS services to on-premise solutions.

Like all of Okta's products, OAG captures events such as access requests, access approvals and denials, event details, etc. and provides structured logs which can be delivered to a third-party security information and event management (SIEM) tool via the Okta Integration Network.

In addition to the above, using OAG in the PCI DSS environment also augments the use of stronger authentication mechanisms such as biometric authentication or authentication using push for legacy web apps.

Okta Advanced Server Access (ASA)

Okta Advanced Server Access (ASA) extends least privilege access controls to infrastructure resources in the cloud or on-premises, specifically Linux and Windows servers via Secure Shell (SSH) and Remote Desktop Protocol (RDP), respectively.

A key mechanism to protecting access to cardholder data is to restrict access to the systems where it is stored. Server access is traditionally gated by an SSH Key or RDP username/password combination for Linux and Windows, respectively. These credentials hold administrative privileges in themselves, and are traditionally protected via a secure vault service or Privileged Access Management (PAM) product. These methods carry significant operational burden, and are prone to error via credential theft and misuse.

Okta ASA delivers a modern, identity-first approach to server access that replaces the use of shared admin accounts and static credentials with short-lived, tightly scoped Client Certificates minted on-demand. Every login attempt via SSH or RDP is independently authenticated by the Okta platform, with the ability to inject multi-factor authentication (MFA) inline. Once authenticated, the user is authorized as a function of the role-based access controls (RBAC) associated with the target server. Within ASA, a grouping of servers and their respective RBAC are known as Projects. Only users who have been explicitly assigned to a Project are authorized to access the enrolled servers.

Additional command-level controls can be implemented for Linux servers in the form of sudo entitlements. Administrators can create commands, or a group of commands, and explicitly assign to a group on the server, further restricting actions that can be performed on systems that carry cardholder data.

Every server enrolled with ASA runs a local server agent which performs local account and entitlement management. The server agent also captures all login events, which are outputted as structured logs to the backend API that contain user and device metadata for PCI audits. This data may be delivered to a third-party security information and event management (SIEM) tool for further analysis.

Resources

For more information about Okta security and compliance, including leveraging Okta for PCI DSS compliance, please use the following resources:

Okta security and compliance resources:

- PCI DSS Responsibility Matrix (available in the Okta Help Center; interested organizations who are not currently Okta customers should reach out to their Okta representative)
- Okta Security Technical Whitepaper
- Not All Cloud Services Are Built Alike—Okta's High Availability Architecture

Okta Identity Cloud resources:

- Okta Identity Cloud overview
- Okta Advanced Server Access (ASA) overview
- Okta Access Gateway (OAG) overview

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 6,000 applications, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work. For more information, visit us at www.okta.com or follow us on www.okta.com/blog.