Verkada

Solution Overview

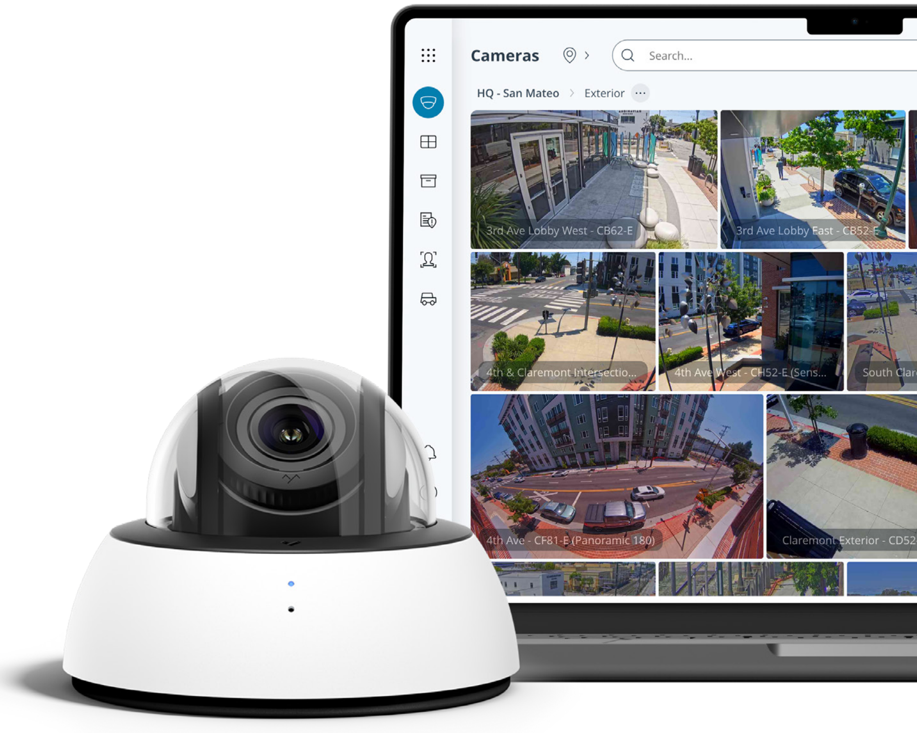
Verkada for PCI Compliance

Meet PCI Compliance With Verkada

90+ days of local and cloud-based storage - No NVRs/DVRs

Detailed user audit logs and modern data encryption standards

Proactive alerts to let users know when something is wrong


Cameras
Search...
HQ - San Mateo
Exterior
3rd Ave Lobby West - CB62-E
3rd Ave Lobby East - CB52-E
4th & Claremont Intersectio...
4th Ave West - CH52-E (Sens...
South Clar
4th Ave - CF81-E (Panoramic 180)
Claremont Exterior - CD52

Get a Live Demo

at verkada.com/demo

Background

The Payment Card Industry Data Security Standard (PCI DSS) outlines a set of requirements mandated by major credit card providers for organizations that handle their transactions. Administered by the Payment Card Industry Security Standards Council, the standard was established to strengthen protections of cardholder data and to reduce fraud.

How Verkada Helps

Updated as part of PCI DSS version 4.0, Requirement 9 outlines steps that organizations should take to restrict physical access to cardholder data. Included under this requirement are guidelines that organizations must take to limit and monitor physical access to systems in the cardholder data environment, such as points of sale (POS) systems. Requirement 9 includes such things as:

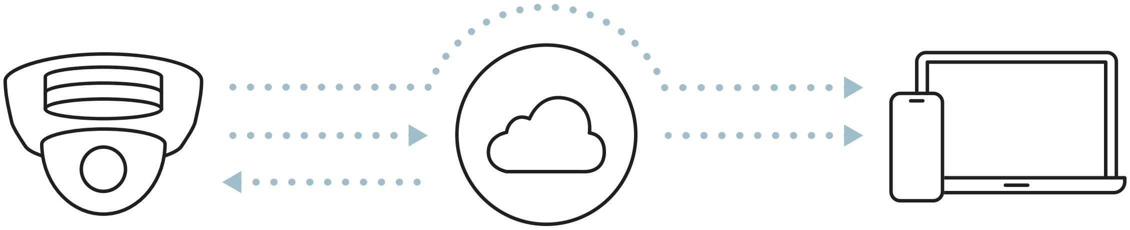
PCI Requirements 9: Physical Security Guidelines

PCI Requirement	Verkada Supports
9.2 Physical access controls are in place to manage entry into facilities and systems containing cardholder data.	Cloud-managed access controls help enable customers to limit physical access to CDE systems to authorized personnel, protecting sensitive information and helping prevent unauthorized changes or theft. Organizations can implement physical security controls at critical entry points while managing access schedules, roles, and alerts through an intuitive platform.
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both).	Unconstrained by NVRs/DVRs, Verkada systems are fully modular and scalable. Deploy cameras to monitor sensitive areas like data closets, or multiple access control devices to help protect critical entry points. Devices can be centrally managed across multiple locations for seamless scalability and control.
9.2.1.1.b Verify monitoring devices or mechanisms are protected from tampering or disabling.	Verkada cameras automatically detect and report tampering using physical-motion sensors and computer vision techniques.
9.2.1.1.c Verify that collected data from video cameras and/or physical access control mechanisms is reviewed and correlated with other entries. Collected data is stored for at least three months.	The integration between access control and cameras allows for easy correlation of access events with video footage. Video data can be stored on-device for up to 365 days and archived to cloud-based storage indefinitely, exceeding the three-month requirement.

PCI Requirement	Verkada Supports
9.3 Physical access for personnel and visitors is authorized and managed.	Verkada provides a unified solution for managing physical access for personnel and visitors: • **Access Control:** Streamline authorization and management with SCIM integration, automated onboarding, and credential provisioning. Admins can swiftly manage user permissions, including issuing or revoking mobile or physical credentials. • **Visitor Management:** Verkada Guest enables seamless visitor check-in, color-coded badge printing, and optional background checks. Visitor access can be managed through native integrations with access control and video-verified with cameras, helping ensure visitors are authorized, identifiable, and escorted when required.
9.3.1.b Observe identification methods, such as ID badges, and processes to verify that personnel in the CDE are clearly identified.	Verkada's access control and credential management tools help organizations clearly identify personnel in the CDE: • **Badge Design and Printing:** Customize ID badges in Verkada Command using existing profiles and configurations. Color-coded badges distinguish personnel roles and streamline identification. • **Automated Credential Management:** SCIM integration with systems like Okta and Azure AD synchronizes user access levels, enabling automated onboarding, badge provisioning, and deprovisioning. • **Versatile Access Methods:** Issue secure mobile credentials or 128-bit encrypted NFC cards to personnel for convenient and traceable access.
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job functions. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	Verkada streamlines access revocation with SCIM integration, automatically removing physical access when a user's status changes in systems like Azure AD. Admins can also suspend users temporarily or permanently delete them, revoking access permissions and disabling physical credentials such as access cards or mobile credentials.
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	Verkada Guest combines seamless visitor experiences with enhanced security controls. • **Visitor Authorization and Identification:** Visitors can pre-register, check in via touchless options, and receive color-coded badges that clearly differentiate them from personnel. Badges include expiration settings to prevent unauthorized reuse. • **Controlled Access and Escorting:** Verkada integrates with access control systems, allowing admins to remotely unlock doors for approved visitors while maintaining visibility with live video monitoring and guest logs. • **Enhanced Security Features:** Optional background checks provide added visibility into visitor risks, supporting compliance and security measures.

PCI Requirement	Verkada Supports
9.3.2.c Observe the use of visitor badges or other identification to verify that the badge or other identification does not permit unescorted access to the CDE.	With Verkada Guest, features like color-coded badge printing make it easy to distinguish between visitors and employees. Optional background checks help identify risks, while admins can monitor and restrict visitor activity with integrated cameras and access controls.
9.3.2.d Observe visitors in the CDE to verify that: • Visitor badges or other identification are being used for all visitors. • Visitor badges or identification easily distinguish visitors from personnel.	With Verkada Guest, tailored check-in templates and branded badges allow visitors to be easily distinguished from personnel. Each badge can be tailored to include visitor type and host details.
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	In addition to self sign-out options through Verkada Guest, Verkada Access Control's Credential Auto-Deactivate can automatically disable unused physical badges after a specified period to minimize the risk of unauthorized access.
9.3.4 Visitor logs are used to maintain a physical record of visitor activity both within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months unless otherwise restricted by law.	Verkada Guest simplifies visitor logging by capturing detailed records, including visitor names, organizations, check-in and check-out times, and authorizing personnel. Logs can be retained for over three months and exported for audits. Integrated video and access control provide visibility into visitor activity to support record management. With customizable workflows, branded badges, and expiration settings for credentials, visitors can be clearly identified and tracked.

Verkada's hybrid cloud architecture



No NVR or DVRs
Industrial-grade onboard storage saves up to 365 days of continuous video[1]

Easy to scale
Bandwidth friendly and supports thousands of cameras across unlimited locations

Centralized management
Modern platform enables secure access on any device from anywhere in the world

Verkada Solution

Verkada offers a technology solution that simplifies the process of meeting PCI physical security requirements. Unlike traditional CCTV systems, Verkada eliminates outdated equipment such as NVRs, DVRs and on-premise servers. The result: a system design that enables modern data security standards and innovative software capabilities by default.

Product Highlights

- No NVRs/DVRs or servers
- 90+ days of on-camera video storage
- Optional cloud backup
- Motion detection and search
- Tamper detection and alerts
- Detailed user audit logs
- TLS 1.2 (or greater) data encryption (in transit)
- RSA + AES data encryption (at rest)
- Automatic firmware updates

Other PCI Requirements

In addition, Verkada also helps customers meet their PCI cyber security requirements as follows:

PCI Requirement	Verkada Supports
2.2 Do not use vendor default passwords	Verkada systems do not have vendor-provided default passwords; SAML/OAuth and multi-factor authentication (MFA) are available as standard options.
8.2 Strict Management of User and Administrator Accounts	Verkada's Role-Based Access Control (RBAC) enables granular access assignments within the Verkada system, helping limit users and administrators to only the permissions necessary for their roles. Audit logs provide visibility into Verkada customer account actions, tracking changes to user access throughout the account lifecycle.
8.3 Strong Authentication for Users and Administrators	Verkada supports strong authentication for its physical security systems with MFA options, including Passkeys, TOTP, HOTP, magic email links, and SMS codes for Verkada system users. These measures add an extra layer of security to prevent unauthorized access of Verkada systems.
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.	Verkada's centralized management allows Verkada system admins to monitor and manage MFA configurations of Verkada systems, reducing risks associated with misuse. Audit logs provide insights into MFA-related actions within Verkada systems, supporting traceability for adjustments or breaches.
8.6 Use of application and system accounts and associated authentication factors is strictly managed.	With SSO integrations, role-based access, and comprehensive audit logs, Verkada enables efficient management of its application and system accounts connected to Verkada systems. Verkada's audit log feature captures user and device activities that occur within the Verkada Command platform. For example, user permissions and modifications of access roles are recorded, supporting accountability and compliance with physical access requirements.
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	Verkada's audit log feature captures user and device activities that occur within the Command platform.
10.3 Audit logs are protected from destruction and unauthorized modifications.	Verkada audit logs are safeguarded with detailed user activity tracking and modern encryption standards, helping reduce the risk of tampering and preserving their integrity.

PCI Requirement	Verkada Supports
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	Verkada's audit logs capture detailed records of user and device actions across the platform: • **Comprehensive Activity Tracking:** Audit logs record events like user logins, changes to user permissions, camera access, and video viewing activities, tying each action to a specific user or device with timestamps and IP addresses. • **Centralized and Per-Camera Logs:** Admins can efficiently review and filter logs at both the organizational and camera levels, streamlining audits and anomaly detection. • **Exportable Reports:** Audit logs can be exported as CSV files for detailed analysis and reporting.
10.5 Audit log history is retained and available for analysis.	Verkada audit logs are stored in geographically redundant data centers and may be configured to retain data for 12 months.
10.6 Time-synchronization mechanisms support consistent time settings across all systems.	Verkada systems accurately record date and time, using the industry-standard Network Time Protocol (NTP).
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.	Verkada offers system health alerts that enable administrators to detect and respond to downtime or issues promptly. 24/7 technical support is available via phone, chat, and email to help troubleshoot and resolve potential system issues.

***Requirement 8: Identify Users and Authenticate Access to System Components**

Verkada systems can help support to compliance with this requirement by offering physical access controls and user identification tools for protected facilities. Features such as SCIM integration, Single Sign-On (SSO), role-based access control (RBAC), and multi-factor authentication (MFA) available within the Verkada systems help manage access to physical environments protected by them. However, Verkada does not provide support for the management or authentication of broader PCI system components or application accounts that access cardholder data.