Verkada

Solution Overview

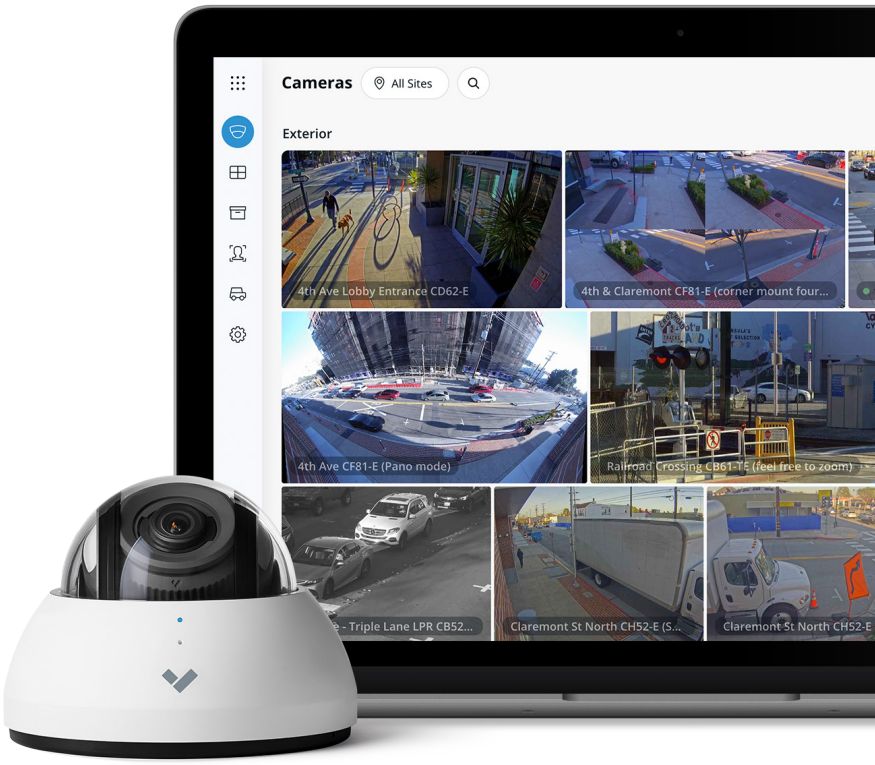
Verkada for PCI Compliance

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



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.

Compliance with PCI guidelines is performed annually and, depending on the particular organization, is verified in one of three ways:

1. By an external Qualified Security Assessor (QSA)
2. By an Internal Security Assessor who has specific credentials for organizations handling large volumes of transactions
3. By Self-Assessment Questionnaire (SAQ) — typically for organizations handling smaller volumes of transactions

About PCI requirement 9

Updated as part of PCI DSS version 3.0, 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.

PCI DSS recommends deploying entry access control mechanisms or video security cameras to meet this requirement (or both). Additionally, they require companies to:

- Verify that either video cameras or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas
- Verify that video cameras (or access controls) are protected from tampering or disabling
- Review collected data and correlate with other entries
- Store video data (or access logs data) for at least three months

Beyond the requirements specific to physical security, PCI DSS outlines a range of measures that organizations must take to ensure the network and data security of their facilities.

Verkada's video surveillance technology is designed specficially to meet the high uptime and stringent data security requirements for the modern enterprise.

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
- HTTPS/SSL data encryption (in transit)
- RSA + AES data encryption (at rest)
- Automatic firmware updates

PCI Requirement 9: Physical Security Guidelines

PCI Requirement	Met by Verkada?	Notes
9.1.1 Use either cameras or access control, or both, in every computer room, data center and other physical areas with systems in the cardholder data environment	✓	Unconstrained by NVRs/DVRs, Verkada systems are fully modular and scalable. You can install a single camera to cover a data closet, for example, and centrally manage thousands of cameras across many locations.
9.1.1.b Ensure cameras are protected from tampering or disabling	✓	Verkada cameras automatically detect and report tampering using physical-motion sensors and computer vision techniques.
9.2 Develop procedures to distinguish between personnel and visitors	✓	Verkada makes it possible to search video on motion and detect unusual or unexpected activity. When these incidents occur, users can receive proactive alerts informing of the time and place, as well as the incident detected.
9.3 Control physical access for onsite personnel	✓	Easily search recorded video to identify specifically who passed through points of ingress; review Verkada user session logs to identify which employees have accessed the system.

Other PCI Requirements

PCI Requirement	Met by Verkada?	Notes
2.1 Do not use vendor default passwords	✓	Verkada systems do not have vendor provided default passwords; SAML/OAuth and 2-factor authentication, are available as standard options.
10.1 Implement audit trails	✓	Verkada automatically logs all user access and sessions.
10.4 Synchronize all critical system clocks and times with time synchronization technology	✓	Verkada systems always have the correct date and time, using the industry-standard Network Time Protocol (NTP).
10.5 Prevent unauthorized changes to audit logs	✓	Verkada audit logs cannot be tampered with or altered.
10.5.3 Audit log backup	✓	All Verkada audit logs are backed up into geographically redundant data centers.
10.6 Review logs and security events to identify unusual activity	✓	Verkada enables authorized administrators to regularly review live and recorded video, as well as user sessions data, over secure connection on any device.
10.7 Retain audit logs for 1 year	✓	Verkada audit logs are stored securely in geographically redundant data centers and may be configured to retain data for 12 months.