



Solution Overview

# Verkada for PCI Compliance





## Meet PCI Compliance With Verkada



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



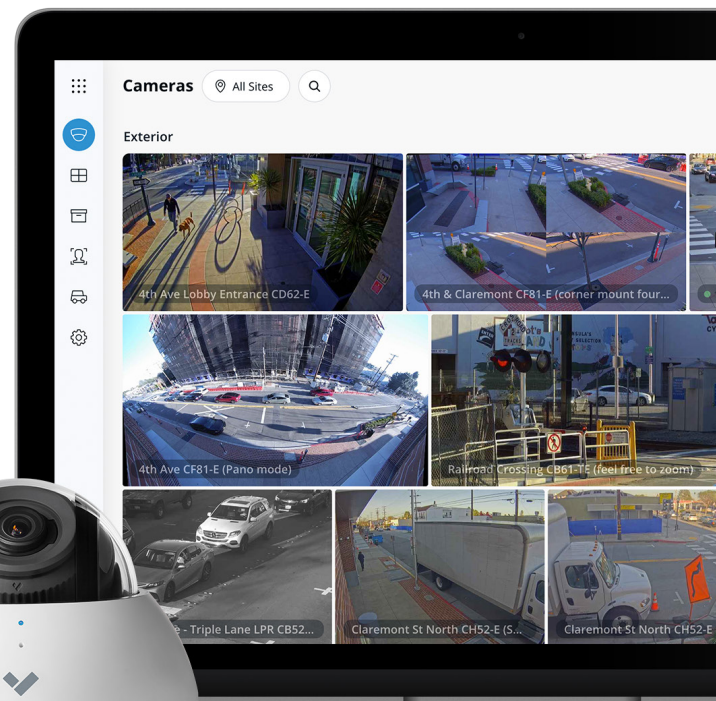
Detailed user audit logs and modern  
data encryption standards



Proactive alerts to let users know  
when something is wrong

Get a Live Demo

at [verkada.com/demo](https://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 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. Requirement 9 includes such things as:

## PCI Requirements 9: Physical Security Guidelines

PCI Requirement	Verkada Support
<b>9.1.1</b> 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.
<b>9.1.1.b</b> Ensure cameras are protected from tampering or disabling	✓ Verkada cameras automatically detect and report tampering using physical-motion sensors and computer vision techniques.
<b>9.2</b> 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.
<b>9.3</b> Control physical access for onsite personnel	✓ Easily search recorded video to identify who passed through points of ingress; review Verkada user session logs to identify which employees have accessed the building and where.



## Verkada's hybrid cloud architecture



### No NVR or DVRs

Industrial-grade onboard storage saves up to 365 days of continuous video<sup>1</sup>

### 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 Support
<b>2.1</b> 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.
<b>10.1</b> Implement audit trails	✓ Verkada automatically logs all user access and sessions.
<b>10.4</b> Synchronize all critical system clocks and times with time synchronization technology	✓ Verkada systems accurately record date and time, using the industry-standard Network Time Protocol (NTP).
<b>10.5</b> Prevent unauthorized changes to audit logs	✓ Verkada audit logs cannot be tampered with or altered.
<b>10.5.3</b> Audit log backup	✓ All Verkada audit logs are backed up into geographically redundant data centers.
<b>10.6</b> 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 connections, on any device.
<b>10.7</b> 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.