Verkada

Descripción general de la solución

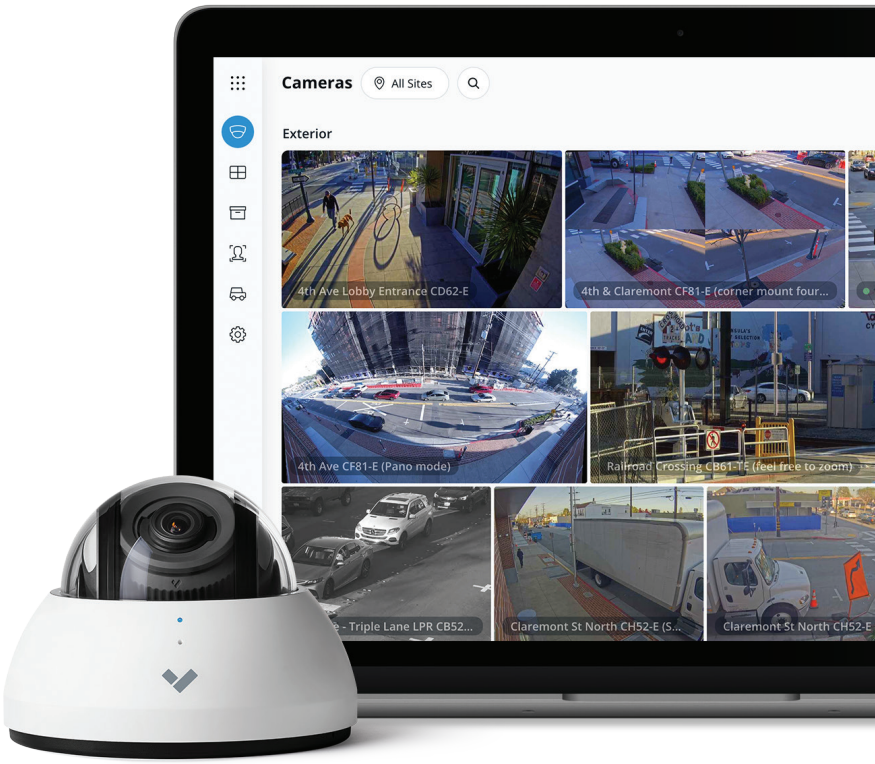
Verkada para el cumplimiento de PCI

Conozca el cumplimiento de PCI con Verkada

Más de 90 días de almacenamiento local y basado en la nube: sin NVR/DVR

Registros de auditoría detallados de usuarios y estándares modernos de cifrado de datos

Alertas proactivas para informar a los usuarios cuando algo está mal



Obtenga una demostración en vivo

en verkada.com/demo

Antecedentes

La Norma de Seguridad de Datos de la Industria de las Tarjetas de Pago (PCI DSS) describe un conjunto de requisitos exigidos por los principales proveedores de tarjetas de crédito para las organizaciones que gestionan sus transacciones. Administrado por el Consejo de Normas de Seguridad de la Industria de las Tarjetas de Pago, la norma se estableció para fortalecer las protecciones de los datos de los titulares de las tarjetas y reducir el fraude.

El cumplimiento de las directrices PCI se realiza anualmente y, según la organización en particular, se verifica de tres maneras:

1. Por un asesor de seguridad calificado externo.
2. Por un asesor de seguridad interno con credenciales específicas para organizaciones que manejan grandes volúmenes de transacciones.
3. Por un cuestionario de autoevaluación (normalmente para organizaciones que gestionan volúmenes más pequeños de transacciones).

Acerca del requisito PCI 9

Actualizado como parte de la versión 3.0 de PCI DSS, el requisito 9 describe las medidas que deben tomar las organizaciones para restringir el acceso físico a los datos de los titulares de tarjetas. Este requisito incluye pautas que las organizaciones deben adoptar para limitar y monitorear el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta, como sistemas de puntos de venta.

PCI DSS recomienda implementar mecanismos de control de acceso de entrada o cámaras de videoseguridad para cumplir con este requisito (o ambos). Además, requiere que las empresas:

- Verifiquen que existen cámaras de video o mecanismos de control de acceso (o ambos) para monitorear los puntos de entrada y salida de las zonas delicadas.
- Verifiquen que las cámaras de video (o los controles de acceso) estén protegidas contra manipulaciones o desactivaciones.
- Revisen los datos recopilados y los relacionen con otras entradas.
- Almacenen datos de video (o registros de acceso) durante al menos tres meses.

Más allá de los requisitos específicos de seguridad física, PCI DSS describe una serie de medidas que las organizaciones deben tomar para garantizar la seguridad de la red y los datos de sus instalaciones.

La tecnología de videoseguridad de Verkada está diseñada específicamente para cumplir con los estrictos requisitos de alto tiempo de actividad y seguridad de datos para las empresas modernas.

Arquitectura de nube híbrida de Verkada

Sin necesidad de NVR o DVR
El almacenamiento incorporado de grado industrial ahorra hasta 365 días de video continuo[1].

Fácil de adaptar
Se adapta al ancho de banda disponible y admite miles de cámaras en una cantidad ilimitada de ubicaciones.

Gestión centralizada
La moderna plataforma permite el acceso seguro en cualquier dispositivo desde cualquier lugar del mundo.

Solución Verkada

Verkada ofrece una solución tecnológica que simplifica el proceso de cumplimiento con los requisitos de seguridad física de PCI. A diferencia de los sistemas CCTV tradicionales, Verkada elimina equipos obsoletos como NVR, DVR y servidores locales. El resultado es un diseño de sistema que permite contar con estándares modernos de seguridad de datos y funcionalidades de software innovadoras de manera predeterminada.

Aspectos destacados del producto

- Sin NVR/DVR ni servidores.
- Más de 90 días de almacenamiento de video en la cámara.
- Copia de seguridad opcional en la nube.
- Detección y búsqueda de movimiento.
- Detección de manipulaciones y alertas.
- Registros de auditoría detallados de usuarios.
- Cifrado de datos HTTPS/SSL (en tránsito).
- Cifrado de datos RSA + AES (en reposo).
- Actualizaciones automáticas de firmware.

Requisito PCI 9: Directrices de seguridad física

Requisito PCI	¿Se cumple con Verkada?	Notas
9.1.1 Utilizar cámaras o control de acceso, o ambos, en cada sala de computadoras, centro de datos y otras áreas físicas con sistemas en el entorno de datos del titular de la tarjeta.	✓	Al no estar limitados por los NVR/DVR, los sistemas Verkada son totalmente modulares y ajustables. Puede instalar una sola cámara para cubrir un armario de datos, por ejemplo, y gestionar de forma centralizada miles de cámaras en muchas ubicaciones.
9.1.1.b Asegurarse de que las cámaras estén protegidas contra manipulaciones o desactivaciones.	✓	Las cámaras de Verkada detectan y denuncian automáticamente la manipulación mediante sensores de movimiento físico y técnicas de visión artificial.
9.2 Desarrollar procedimientos para distinguir entre el personal y los visitantes.	✓	Verkada permite buscar videos en movimiento y detectar actividades inusuales o inesperadas. Cuando se producen estos incidentes, los usuarios pueden recibir alertas proactivas que informan la hora y el lugar, así como del incidente detectado.
9.3 Controlar el acceso físico para el personal en el sitio.	✓	Busque fácilmente videos grabados para identificar específicamente quién pasó por los puntos de ingreso; revise los registros de sesión de usuario de Verkada para identificar qué empleados han accedido al sistema.

Otros PCI Requisitos

Requisito PCI	¿Se cumple con Verkada?	Notas
2.1 No utilizar contraseñas predeterminadas del proveedor.	✓	Los sistemas de Verkada no tienen contraseñas predeterminadas proporcionadas por el proveedor. SAML/OAuth y la autenticación de 2 factores están disponibles como opciones estándar.
10.1 Implementar registros de auditoría.	✓	Verkada registra automáticamente todos los accesos y sesiones de los usuarios.
10.4 Sincronizar todos los relojes y las horas importantes del sistema con la tecnología de sincronización horaria.	✓	Los sistemas Verkada siempre tienen la fecha y la hora correctas, utilizando el protocolo de tiempo de red estándar de la industria.
10.5 Impedir cambios no autorizados en los registros de auditoría.	✓	Los registros de auditoría de Verkada no se pueden manipular ni alterar.
10.5.3 Copia de seguridad del registro de auditoría.	✓	Todos los registros de auditoría de Verkada están respaldados en centros de datos geográficamente redundantes.
10.6 Revisar registros y eventos de seguridad para identificar actividades inusuales.	✓	Verkada permite a los administradores autorizados revisar regularmente el video en vivo y grabado, así como los datos de las sesiones de usuario, a través de una conexión segura en cualquier dispositivo.
10.7 Conservar los registros de auditoría durante un año.	✓	Los registros de auditoría de Verkada se almacenan de forma segura en centros de datos geográficamente redundantes y se pueden configurar para guardar datos durante 12 meses.