Verkada

Présentation de la solution

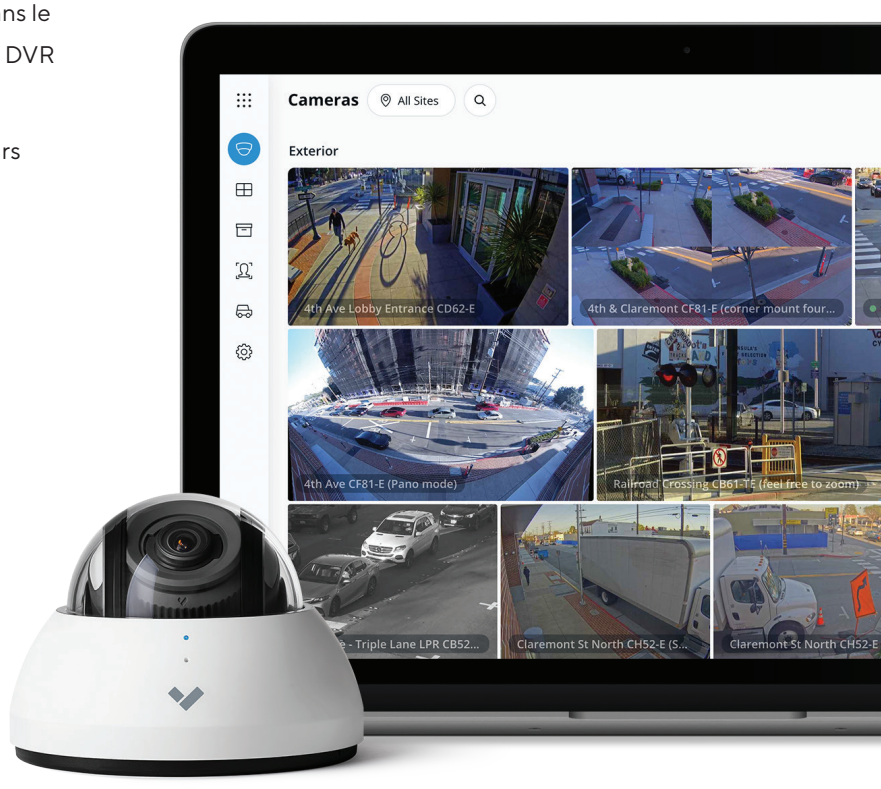
La conformité PCI chez Verkada

Répondez aux exigences de la norme PCI avec Verkada

Plus de 90 jours de stockage local et dans le cloud : oubliez les enregistreurs NVR et DVR

Journaux d'audit détaillés des utilisateurs et respect des normes modernes de chiffrement des données

Alertes proactives pour informer les utilisateurs en cas de problème



Participez à une démonstration

sur verkada.com/fr/demo

Contexte

La norme de sécurité de l'industrie des cartes de paiement (PCI DSS) regroupe un ensemble d'exigences imposées par les principaux fournisseurs de cartes de crédit aux organisations qui gèrent leurs transactions. Administrée par le Conseil des normes de sécurité de l'industrie des cartes de paiement, cette norme a été créée pour renforcer la protection des données des titulaires de carte et réduire la fraude.

La conformité aux exigences de la norme PCI est vérifiée chaque année et, en fonction de l'organisation concernée, de trois manières différentes :

1. Par un évaluateur de sécurité qualifié (QSA) externe
2. Par un évaluateur de sécurité interne (ISA) qui possède les qualifications nécessaires pour les organisations traitant d'importants volumes de transactions
3. Par un questionnaire d'auto-évaluation (SAQ), généralement pour les organisations qui traitent de petits volumes de transactions

À propos de l'exigence n° 9 de la norme PCI

Mise à jour dans le cadre de la version 3.0 de la norme PCI DSS, l'exigence n° 9 décrit les mesures que les organisations doivent prendre pour restreindre l'accès physique aux données des titulaires de cartes. Cette exigence donne des directives aux organisations pour limiter et contrôler l'accès physique aux systèmes dans l'environnement des données des titulaires de cartes, tels que les systèmes de points de vente.

La norme PCI DSS recommande de déployer des mécanismes de contrôle d'accès aux entrées ou des caméras de vidéosurveillance (ou les deux) pour répondre à cette exigence. De plus, elle oblige les entreprises à :

- Vérifier que les caméras de vidéosurveillance ou les mécanismes de contrôle d'accès (ou les deux) sont opérationnels pour surveiller les points d'entrée et de sortie dans les zones sensibles
- Vérifier que les caméras de vidéosurveillance (ou les mécanismes de contrôle d'accès) sont protégés contre toute tentative de sabotage ou de désactivation
- Analyser les données collectées et les corréler avec d'autres indicateurs
- Conserver les données vidéo (ou les données des journaux d'accès) pendant au moins trois mois

Outre les exigences spécifiques à la sécurité physique, la norme PCI DSS prévoit un ensemble de mesures que les organisations doivent prendre pour garantir la sécurité du réseau et des données de leurs installations.

La technologie de vidéosurveillance de Verkada est spécialement conçue pour répondre aux exigences élevées en matière de conservation et de sécurité des données des entreprises modernes.

Architecture cloud hybride de Verkada

Pas d'enregistreurs NVR ou DVR

Le stockage intégré de qualité industrielle permet de sauvegarder jusqu'à 365 jours de vidéo en continu[1]

Une évolutivité simplifiée

Peu gourmand en bande passante, le système prend en charge des milliers de caméras sur un nombre illimité de sites

Gestion centralisée

Accédez en toute sécurité à notre plateforme moderne depuis n'importe quel appareil et où que vous soyez

La solution Verkada

Verkada propose une solution technologique qui simplifie le processus de conformité aux exigences de sécurité physique de la norme PCI. Contrairement aux systèmes de vidéosurveillance traditionnels, le système Verkada élimine les équipements obsolètes tels que les enregistreurs NVR ou DVR et les serveurs sur site. Ainsi, la conception du système permet de respecter les dernières normes en matière de sécurité des données et d'utiliser des fonctionnalités logicielles innovantes par défaut.

Points forts du produit

- Aucun enregistreur NVR ou DVR ni aucun serveur
- Plus de 90 jours de stockage vidéo sur caméra
- Sauvegarde optionnelle dans le cloud
- Détection et recherche de mouvement
- Détection de sabotage et alertes
- Journaux d'audit détaillés des utilisateurs
- Chiffrement des données HTTPS/SSL (en transit)
- Chiffrement des données RSA et AES (au repos)
- Mises à jour automatiques des firmwares

Exigence n° 9 de la norme PCI : Directives relatives à la sécurité physique

Exigence de la norme PCI	Remplie par Verkada ?	Remarques
9.1.1 Utiliser des caméras ou des mécanismes de contrôle d'accès (ou les deux) dans chaque salle informatique, centre de données et toute autre zone physique donnant accès aux systèmes de l'environnement des données des titulaires de cartes	✓	Non limités par les enregistreurs NVR ou DVR, les systèmes Verkada sont entièrement modulaires et évolutifs. Ainsi, vous pouvez installer une seule caméra pour couvrir une armoire de données ou gérer de manière centralisée des milliers de caméras réparties sur plusieurs sites.
9.1.1.b S'assurer que les caméras sont protégées contre toute tentative de sabotage ou de désactivation	✓	Les caméras Verkada détectent et signalent automatiquement les actes de sabotage à l'aide de capteurs de mouvement physique et de techniques de vision par ordinateur.
9.2 Mettre en place des procédures pour distinguer le personnel des visiteurs	✓	Verkada permet d'effectuer des recherches vidéo basées sur le mouvement et de détecter toute activité inhabituelle ou inattendue. Lorsque de tels incidents se produisent, les utilisateurs peuvent recevoir des alertes proactives indiquant l'heure, le lieu et l'incident détecté.
9.3 Contrôler l'accès physique du personnel sur site	✓	Effectuez facilement des recherches dans les enregistrements vidéo afin d'identifier précisément les personnes qui sont passées par les points d'entrée. Examinez les journaux de session des utilisateurs de Verkada pour identifier les employés qui ont accédé au système.

Autres exigences de la norme PCI
Configuration matérielle et logicielle requise

Exigence de la norme PCI	Remplie par Verkada ?	Remarques
2.1 Ne pas utiliser les mots de passe par défaut du fournisseur	✓	Les systèmes Verkada ne fournissent pas de mots de passe par défaut ; la technologie SAML/OAuth et l'authentification à deux facteurs sont proposées comme options standard.
10.1 Mettre en place des pistes d'audit	✓	Verkada enregistre automatiquement tous les accès et toutes les sessions des utilisateurs.
10.4 Synchroniser toutes les horloges et heures cruciales du système à l'aide d'une technologie de synchronisation temporelle	✓	La date et l'heure des systèmes Verkada sont toujours correctes grâce au protocole NTP (Network Time Protocol).
10.5 Empêcher toute modification non autorisée des journaux d'audit	✓	Les journaux d'audit Verkada ne peuvent être ni falsifiés ni modifiés.
10.5.3 Sauvegarder les journaux d'audit	✓	Tous les journaux d'audit Verkada sont sauvegardés dans des centres de données géographiquement redondants.
10.6 Examiner les journaux et les événements de sécurité pour identifier toute activité inhabituelle	✓	Verkada permet aux administrateurs autorisés d'examiner régulièrement les séquences vidéo en direct et enregistrées ainsi que les données des sessions des utilisateurs via une connexion sécurisée sur n'importe quel appareil.
10.7 Conserver les journaux d'audit pendant 1 an	✓	Les journaux d'audit Verkada sont stockés en toute sécurité dans des centres de données géographiquement redondants et peuvent être configurés pour conserver les données pendant 12 mois.