

Kiteworks bietet eine PCI DSS-konforme Plattform

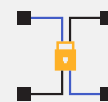
Robuste Sicherheitsfunktionen schützen Karteninhaberdaten

Der Payment Card Industry Data Security Standard (PCI DSS) umfasst eine Reihe von Sicherheitsstandards, die gewährleisten sollen, dass alle Unternehmen, die Kreditkarteninformationen akzeptieren, verarbeiten, speichern oder übertragen, über eine sichere Umgebung verfügen. Der Standard gilt für alle Unternehmen, die Karteninhaberdaten verwalten, unabhängig von Größe oder Transaktionsvolumen. Dies umfasst Branchen wie Einzelhandel, Banken, Finanzwesen, Versicherungen und jedes Unternehmen, das Zahlungen abwickelt. Nichtbeachtung kann zu erheblichen Geldstrafen, erhöhten Transaktionsgebühren, Reputationsschäden und sogar dem Verlust der Möglichkeit zur Abwicklung von Kreditkartenzahlungen führen. Die 12 wesentlichen Anforderungen des PCI DSS umfassen die Installation und Wartung von Netzwerksicherheitskontrollen, die Anwendung sicherer Konfigurationen auf Systemkomponenten, den Schutz gespeicherter Kontodaten und Karteninhaberdaten während der Übertragung, den Schutz der Systeme vor Malware, die Entwicklung sicherer Systeme und Software, Zugangsbeschränkungen, die Identifizierung von Benutzern, die Authentifizierung des Zugriffs, die Protokollierung und Überwachung, Sicherheitstests sowie die Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme. Kiteworks ist eine PCI DSS-konforme Plattform und unterstützt die Einhaltung dieses Standards. So funktioniert es:

Starke Sicherheitsbasis mit gehärteter virtueller Appliance

Sichere Netzwerk- und Systemanforderungen tragen gemeinsam dazu bei, eine robuste Sicherheitsbasis zu schaffen, indem Firewalls installiert und gewartet, Standardpasswörter vermieden, Malware bekämpft und sichere Systeme und Anwendungen entwickelt werden. Die Kiteworks-Plattform erfüllt die PCI DSS-Anforderungen für sichere Netzwerke und Systeme durch die Nutzung von AWS und den Einsatz von Single-Tenant Private Clouds zum Schutz von Karteninhaberdaten. Die Plattform arbeitet nach dem Prinzip des geringsten Privilegs, sodass nur notwendiger Datenverkehr zugelassen wird. Kiteworks ist eine vorgehärtete Appliance, bei der alle Verbindungen zum System über sichere Kanäle mit Verschlüsselung erfolgen. Schließlich werden alle Server mit Antiviren- und Schwachstellenabwehrmaßnahmen ausgestattet, und Änderungen an der Produktionsumgebung folgen einem dokumentierten Änderungsmanagementprozess, der eine Überprüfung und Genehmigung durch das Management erfordert. Zusammen bilden diese Funktionen eine solide Sicherheitsbasis für die Kiteworks-Plattform.

Highlights der Lösung



**Robuste
Zugangs-
kontrollen**



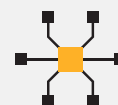
**Single-Tenant
Private Cloud**



**Doppelte Ver-
schlüsselung**



**Kundeneigene
Schlüssel**



**SIEM-
Integration**

Robuste Zugangskontrolle und Verschlüsselung schützen Daten

Anforderungen im Zusammenhang mit Datenschutz und Zugangskontrollen stellen sicher, dass sensible Daten geschützt und nur autorisiertem Personal zugänglich sind. Dies geschieht durch den Schutz gespeicherter Daten, die Verschlüsselung übertragener Daten, die Einschränkung des Zugriffs nach dem Need-to-Know-Prinzip, die Zuweisung eindeutiger IDs und die Beschränkung des physischen Zugriffs. Kiteworks schützt gespeicherte Karteninhaberdaten durch die Verschlüsselung der Daten mit AES-256 im ruhenden Zustand und mit TLS 1.3 während der Übertragung. Die Kunden sind für die Verwaltung ihrer eigenen Verschlüsselungsschlüssel verantwortlich. Der Zugang zu sensiblen Daten wird durch integrierte Authentifizierungsmechanismen und die Integration mit bestehenden Identitätsanbietern sowie durch granulare Zugangskontrollen geregelt. Jedem Benutzerkonto wird eine eindeutige ID zugewiesen, und die Kunden konfigurieren die Sicherheitsanforderungen für Passwörter. Dies stellt sicher, dass sensible Daten geschützt und nur autorisiertem Personal zugänglich bleiben.

Echtzeitüberwachung und Identifizierung potenzieller Lücken

Die abschließenden Anforderungen umfassen die Überwachung, das Testen und die Richtlinien, die Unternehmen dabei unterstützen, wachsam zu bleiben, potenzielle Sicherheitslücken zu identifizieren und eine Kultur des Sicherheitsbewusstseins und der Verantwortung zu fördern. Dies geschieht durch die Verfolgung und Überwachung des Zugriffs, regelmäßige Tests von Sicherheitssystemen und -prozessen sowie die Einhaltung einer für alle Mitarbeiter verbindlichen Informationssicherheitsrichtlinie. Die Plattform bietet SIEM-Integration und Log-Weiterleitung, und Audit-Logs erfassen in Echtzeit alle Benutzerzugriffe, Änderungen an Konten und Authentifizierungseinstellungen, wobei die Logdateien von vornherein unveränderlich sind. Kiteworks führt zudem regelmäßig Schwachstellen-Scans, Prämienprogramme und Tests durch Dritte durch. Diese Funktionen helfen Unternehmen, wachsam zu bleiben, potenzielle Sicherheitslücken zu identifizieren und eine Kultur des Sicherheitsbewusstseins und der Verantwortung unter den Mitarbeitern zu fördern.

Kiteworks ist eine PCI DSS-konforme Plattform, die ein umfassendes Set an Sicherheitsfunktionen zum Schutz von Karteninhaberdaten bietet. Die Plattform nutzt eine gehärtete virtuelle Appliance, sichere Datenverschlüsselung und robuste Zugangskontrollen, um sicherzustellen, dass sensible Informationen geschützt und nur autorisiertem Personal zugänglich sind. Kiteworks bietet zudem Echtzeitüberwachung und Log-Weiterleitung, um Unternehmen dabei zu helfen, wachsam zu bleiben und potenzielle Sicherheitslücken zu identifizieren. Mit regelmäßigen Schwachstellen-Scans, Prämienprogrammen und Penetrationstests durch Dritte stellt Kiteworks sicher, dass die Plattform sicher und konform mit den neuesten PCI DSS-Anforderungen bleibt. Durch den Einsatz von Kiteworks können Unternehmen eine sichere Umgebung für die Abwicklung von Kreditkartentransaktionen gewährleisten und gleichzeitig das Risiko von Datenschutzverletzungen und Strafen wegen Nichteinhaltung der Vorschriften minimieren.