PCI DSS Compliance

Meeting Full Compliance with Kognitive Konnect SD-WAN

The **Payment Card Industry Data Security Standard (PCI DSS)** is a globally recognized framework of information security controls designed to protect cardholder data — including account numbers, cardholder names, CVV codes, and authentication information — across any system that stores, processes, or transmits payment card information.

Originating in 2004 through collaboration between the major credit card brands, PCI DSS defines **12 core requirements** that ensure secure network design, system management, and data protection practices — regardless of point-of-sale (POS) type, application, or network infrastructure.

Kognitive Konnect™ SD-WAN is a cloud-native, multi-tenant platform that delivers software-defined connectivity, routing, and integrated Layer 7 security services with complete orchestration and automation. By providing segmentation, encryption, and continuous monitoring, Kognitive enables organizations to achieve and maintain PCI DSS compliance across distributed retail, hospitality, and financial environments.

The current PCI DSS: v4.0.1 requirements can be downloaded for free at the PCI Security Standards Council download center.

Securing POS and Retail Networks

Kognitive's Konnect SD-WAN architecture places security and segmentation directly at the branch and edge — where POS systems and user devices connect to the internet. Through **native security** and **zero-trust access controls** with **centralized logging and orchestration**, Kognitive enables each site to meet PCI DSS network isolation and encryption requirements without additional hardware.

- **Unified SD-WAN and Security Fabric**: Each Kognitive Edge appliance provides routing, firewall, VPN, and policy management in one device — reducing network complexity and attack surface.
- **Centralized Management via Kognitive Cloud**: Secure, role-based management with change tracking, user audit history, and multi-tenant isolation.
- **Zero-Trust Access & Multi-WAN Encryption**: Dynamic VPN tunnels automatically encrypts data and application traffic across Starlink, 5G, or wired links.
- **Segmentation for PCI Scope Control**: Logical separation of POS, guest Wi-Fi, and corporate traffic using VLANs and policy-based routing keeps cardholder data isolated from non-PCI systems.
- **Continuous Monitoring**: The Security Dashboard provides threat analytics, firewall and IPS events, and network telemetry to detect anomalies in real time.

The 12 Core PCI DSS Requirements

PCI DSS 4.0.1 Requirement		Kognitive capabilities to enable compliance
Build and Maintain a Secure Network and Systems		
1	**Install and Maintain Network Security Controls**	Kognitive Konnect includes a Next-Generation Firewall (NGFW) and stateful packet inspection engine that delivers zone-based segmentation for POS, guest, and operational networks. Security and WAN policies are centrally managed through Kognitive Cloud, which maintains a full audit trail of all configuration changes. Role-Based Access Control (RBAC) ensures only authorized users can modify security configurations.
2	**Apply Secure Configurations to All System Components**	During provisioning, Kognitive devices and the Konnect Cloud require unique credentials and enforce strong password policies. MFA is supported for administrative users.
Protect Account Data		
3	**Protect Stored Account Data**	No cardholder data is stored on the system or components.
4	**Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks**	Kognitive Konnect uses MPK-VPN (Multipath Konnect VPN) tunnels and TLS 1.2+ encryption. The platform supports IPsec tunneling with AES-256-GCM ciphers and SHA-2 integrity validation. All WAN traffic between edge sites, hubs, and cloud services can be encrypted, ensuring confidentiality and integrity of transmitted data.
Maintain a Vulnerability Management Program		
5	**Protect All Systems and Networks from Malicious Software**	While PCI antivirus requirements primarily apply to endpoints, Kognitive provides network-layer malware defense through Intrusion Prevention (IPS) and Talos-based threat signature updates. The IPS engine blocks malicious payloads and DoS attacks before they reach the LAN or POS devices.
6	**Develop and Maintain Secure Systems and Software**	Kognitive maintains a secure development lifecycle (SDLC) for all software components and delivers regular firmware updates as well as automatic security updates for Kognitive Cloud. Regular patching and vulnerability remediation are part of Kognitive's product maintenance program.
Implement Strong Access Control Measures		
7	**Restrict Access to System Components and Cardholder Data by Business Need to Know**	Identity Access Management (IAM) and RBAC in Kognitive Cloud restrict system access by user role, organization, or tenant. POS and payment applications can be isolated into dedicated VLANs or VRFs, ensuring cardholder data paths are logically separated from guest or operational networks. No cardholder data is stored or entered directly into any Kognitive system.
8	**Identify Users and Authenticate Access to System Components**	Kognitive's hierarchical RBAC model assigns unique credentials to each administrative user. User and configuration actions are logged, timestamped, and auditable in Kognitive Cloud.
9	**Restrict Physical Access to Cardholder Data**	Physical security of POS devices and local edge hardware remains the responsibility of the merchant.
Regularly Monitor and Test Networks		
10	**Log and Monitor All Access to System Components and Cardholder Data**	Kognitive Cloud provides centralized logging and analytics for firewall, VPN, and system events. All administrative access and configuration changes are retained with immutable audit logs. Logs can be exported to third-party SIEMs or compliance tools for PCI audit visibility.
11	**Test Security of Systems and Networks Regularly**	Kognitive conducts continuous vulnerability scanning, penetration testing, and threat-signature validation on its platform. Customers should complement this with periodic PCI-mandated scans of their own cardholder-data environments.
Maintain an Information Security Policy		
12	**Support Information Security with Organizational Policies and Programs**	Kognitive maintains a comprehensive Information Security Policy aligned with ISO 27001 and SOC 2 Type II frameworks (certifications in progress). Customers are responsible for maintaining their internal PCI policies governing staff access and operational processes.

Compliance Without Complexity

Achieving and maintaining PCI DSS compliance requires a comprehensive, layered approach to network security. Kognitive Konnect SD-WAN provides organizations with the tools to secure payment data from edge to cloud through unified policy control, zero-trust segmentation, and continuous monitoring.

By integrating encryption, identity management, and automated threat detection into a single platform, Kognitive enables retailers, hospitality providers, and financial institutions to reduce complexity and meet PCI DSS v4.0.1 requirements with confidence.

For more information visit www.kognitive.net or contact sales@kognitive.net.