The Beginner's Guide to PCI-DSS Compliance with Kitecyber

Discover how Kitecyber helps your organisation map and meet the 12 PCI-DSS requirements by protecting cardholder data (CHD) and electronic cardholder data environments (CDE) across endpoints, networks, SaaS/cloud, and user access, preventing loss, misuse, and unauthorised disclosure.

What is PCI-DSS?

The Payment Card Industry Data Security Standard (PCI-DSS) is the global security standard for organisations that store, process, or transmit cardholder data. It defines 12 core requirements (technical + operational) to protect cardholder data and requires ongoing validation and audit.

Who must comply with PCI-DSS?

Any organisation that accepts, processes, stores, or transmits payment card data, including merchants, payment service providers, and their sub-processors and vendors, must comply with PCI-DSS and usually validate compliance annually.

Key GDPR Requirements

- Install and maintain firewalls to protect cardholder data.
- Do not use vendor defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus/anti-malware
- Develop and maintain secure systems and applications (patching).
- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes (scans, pen tests, file integrity, wireless)
- Maintain an information security policy for all personnel (risk assessments, training, incident response).

How Kitecyber helps map to PCI-DSS: product & feature summary

Kitecyber's core modules — **DLP, Unified Endpoint Management (UEM), UEBA, Data Classification, Secure Web Gateway (SWG), and ZTNA** — provide complementary controls that reduce PCI scope, prevent cardholder data leakage, enforce least-privilege access, and produce audit-ready evidence.

Below is a requirement-by-requirement mapping showing which Kitecyber product(s) apply and exactly how they help.

PCI-DSS Requirements Mapped to Kitecyber Products & Features

PCI-DSS Requirement	Mapped Kitecyber Product(s)	How Kitecyber Helps
1. Install and maintain a firewall configuration to protect cardholder data	SWG, ZTNA, DLP	SWG enforces network egress/ingress policies; ZTNA isolates CDE with microsegmentation; DLP inspects outbound traffic for CHD patterns.
2. Do not use vendor-supplied defaults for system passwords and other security parameters	UEM, Compliance	UEM enforces strong password policies, disables default accounts, and validates device posture; compliance checks flag insecure configurations.
3. Protect stored cardholder data	Data Classification, DLP, UEM	Data Classification discovers & tags CHD; DLP blocks unencrypted storage or unauthorised saving of PAN; UEM enforces full-disk encryption.
4. Encrypt transmission of cardholder data across open, public networks	SWG, ZTNA, DLP	SWG enforces TLS; ZTNA provides secure authenticated tunnels; DLP blocks cleartext transmissions of CHD.
5. Use and regularly update anti-virus software or programs	UEM, UEBA, Endpoint Threat Integration	UEM manages AV deployment & updates; UEBA detects malware-like behaviours; integration ensures visibility into endpoint threats.
6. Develop and maintain secure systems and applications (patching)	UEM, UEBA	UEM automates OS & app patching; UEBA detects suspicious activity post-vulnerability; logs provide patch compliance evidence.
7. Restrict access to cardholder data by business need-to-know	ZTNA, DLP, Data Classification	ZTNA enforces least-privilege access; Data Classification ensures only authorised workflows surface CHD; DLP applies contextual access policies.
8. Assign a unique ID to each person with computer access	ZTNA, UEM, Audit Logs	ZTNA integrates with SSO/MFA; UEM enforces device-user binding; audit logs tie every CHD event to a unique user ID.
9. Restrict physical access to cardholder data	UEM, DLP	UEM enforces disk encryption, remote wipe & lock; DLP blocks USB/physical data exfiltration; posture checks enforce location-based restrictions.
10. Track and monitor all access to network resources and cardholder data	DLP, UEBA, SWG, ZTNA	DLP logs CHD access attempts; UEBA correlates anomalies; SWG & ZTNA provide session-level logs; all exportable to SIEM.
11. Regularly test security systems and processes	UEBA, DLP, UEM	UEBA validates detection rules during tests; DLP runs in test/policy simulation mode; UEM provides patch and config validation for scans.
12. Maintain an information security policy for all personnel	DLP, UEM, UEBA	DLP & UEBA generate incident reports for training & awareness; UEM enforces baseline compliance; workflows track policy attestation.

Next steps

1. **Request a demo** to see a PCI-DSS mapping tailored to your environment (scope reduction plan + DLP policies).
2. **Run a discovery assessment** to find where PAN & CHD live today and estimate your remediation effort.

Practical outcomes for CMMC readiness

Scope reduction

Data Classification + DLP identify and isolate CUI to minimize systems in-scope.

Scope reduction

Data Classification + DLP identify and isolate CUI to minimize systems in-scope.

Scope reduction

Data Classification + DLP identify and isolate CUI to minimize systems in-scope.

KITE CYBER

Kitecyber, 691 S Milpitas Blvd, Ste 217, Milpitas, CA 95035

Email: info@kitecyber.com

Website: www.kitecyber.com

LinkedIn Twitter YouTube