WHITE PAPER

PCI DSS 4.0 Compliance and Continuous Security Validation Using RidgeBot®

RIDGE SECURITY

Executive Summary

PCI DSS version 4.0 represents a fundamental shift in how organizations approach payment card security. While retaining the original 12 high-level requirements, PCI DSS 4.0 emphasizes security objectives, continuous risk management, and demonstrable effectiveness of controls over static, checklist-based compliance.

RidgeBot® by Ridge Security enables organizations to meet and exceed PCI DSS 4.0 requirements through continuous, automated, and risk-based security validation. By safely simulating real-world attacks across networks, systems, applications, and cloud environments, RidgeBot® provides continuous assurance that security controls are operating as intended and that exploitable vulnerabilities are identified and remediated before attackers can leverage them.

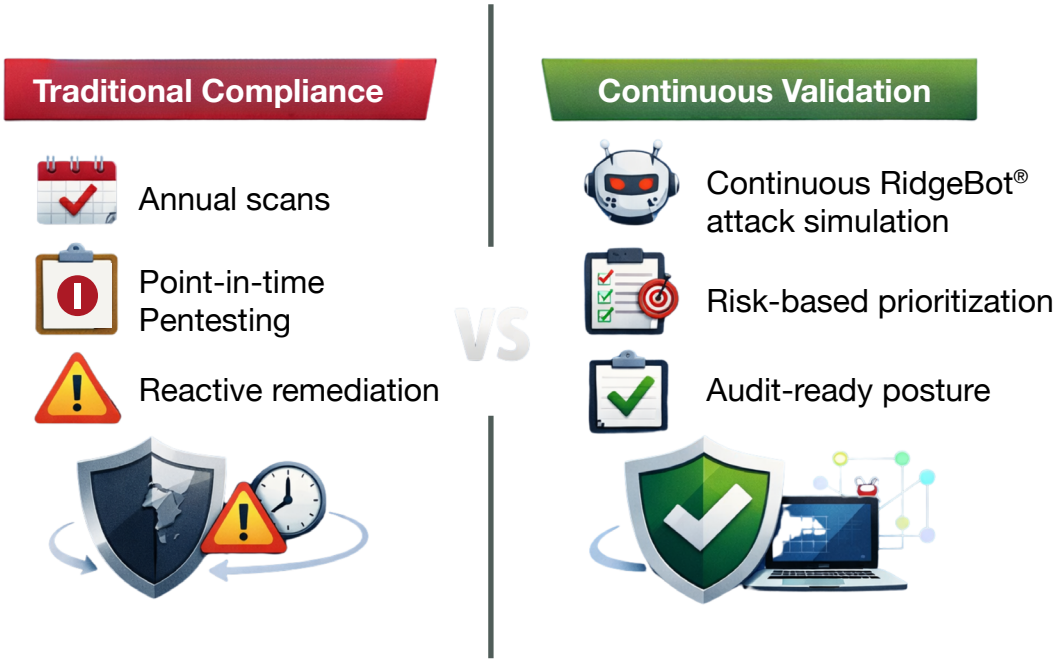
Industry Context:
From Periodic Compliance to Continuous Security

Modern payment environments are highly dynamic, incorporating cloud infrastructure, SaaS platforms, APIs, mobile devices, and remote access. Traditional point-in-time assessments such as annual penetration tests or quarterly scans are insufficient to address continuously evolving attack surfaces.

PCI DSS 4.0 responds to this reality by requiring organizations to:

- Continuously validate security controls
- Perform ongoing risk analysis
- Demonstrate security outcomes, not just control presence

RidgeBot® operationalizes these principles through continuous, automated offensive security validation.



RidgeBot® Overview:
Automated Offensive Security Validation

RidgeBot is an autonomous penetration testing and security validation platform that continuously discovers assets, identifies vulnerabilities, safely exploits attack paths, and prioritizes risk based on real-world impact.

Key capabilities include:
- Continuous asset discovery and attack surface mapping
- AI-assisted vulnerability exploitation
- Risk-weighted prioritization of exploitable findings
- Actionable remediation guidance
- Audit-ready reporting aligned to compliance requirements

RidgeBot, as a software solution, operates on a virtual appliance, physical appliance, or cloud deployment and integrates seamlessly into enterprise and cloud environments.

PCI DSS 4.0 Overview

The Payment Card Industry Data Security Standard (PCI DSS) 4.0 applies globally to all entities that store, process, or transmit cardholder data or sensitive authentication data. PCI DSS 4.0 introduces:

- Outcome-based security objectives
- Support for customized and compensating controls
- Stronger authentication and credential requirements
- Expanded requirements for vulnerability management, risk analysis, and continuous monitoring

Organizations must demonstrate that security controls are effective over time, not merely implemented.

Supporting PCI DSS 4.0 Customized Approaches

PCI DSS 4.0 allows organizations to meet requirements using customized controls when traditional approaches are impractical, provided that risks are assessed and security objectives are achieved.

RidgeBot® supports customized approaches by:

- Validating control effectiveness through real-world attack simulation
- Demonstrating exploitability or resistance of systems
- Providing repeatable, defensible evidence for auditors

PCI DSS 4.0 Requirements and RidgeBot® Alignment

Requirement 1
Install and Maintain Network Security Controls

Organizations must define, implement, and continuously maintain network security controls that restrict traffic based on business need.

RidgeBot® Support:
- Discovers network assets and exposed services;
- Validates firewall and segmentation effectiveness through attack simulation
- Identifies misconfigurations and unauthorized access paths

Requirement 2
Apply Secure Configurations to All System Components

Systems must be securely configured, hardened, and inventoried.

RidgeBot® Support:
- Continuous asset discovery and configuration exposure detection
- Identification of default credentials, weak configurations, and legacy services
- Validation of secure administrative access

Requirement 3
Protect Stored Account Data

Cardholder data must be minimized, protected, and rendered unreadable where stored.

RidgeBot® Support:
- Identifies systems storing sensitive data
- Tests access paths to encrypted and unencrypted data
- Validates credential and privilege controls protecting data stores

Requirement 4
Protect Cardholder Data with Strong Cryptography During Transmission

Sensitive data must be protected during transmission over open and public networks.

RidgeBot® Support:
- Detects weak or deprecated encryption protocols
- Identifies exposed services and insecure transmission paths
- Validates wireless and remote access security

Requirement 5
Protect All Systems and Networks from Malicious Software

Organizations must deploy and maintain anti-malware controls and detection mechanisms.

RidgeBot® Support:
- Identifies exploitable vulnerabilities that enable malware delivery
- Simulates post-exploitation attack paths used by real malware campaigns
- Prioritizes remediation based on exploit success

Requirement 6
Develop and Maintain Secure Systems and Software

Security must be integrated throughout the system and software lifecycle.

RidgeBot® Support:
- Continuous vulnerability identification and exploitation validation
- Verification of patch effectiveness
- Security validation for new releases, updates, and configuration changes

Requirement 7
Restrict Access to System Components and Cardholder Data by Business Need-to-Know

Access must be limited to authorized users and processes.

RidgeBot® Support:
- Tests privilege escalation paths
- Identifies excessive permissions and lateral movement opportunities
- Validates access control enforcement

Requirement 8
Identify and Authenticate Access to System Components

Strong authentication, including multi-factor authentication (MFA), is required.

RidgeBot® Support:
- Tests credential strength and reuse
- Validates MFA enforcement and bypass resistance
- Identifies exposed authentication services

Requirement 9
Restrict Physical Access to Cardholder Data

Physical access to systems and media must be controlled and monitored.

RidgeBot® Support:
- Validates security of systems controlling physical access
- Identifies exploitable weaknesses in access control systems

Requirement 10
Log and Monitor All Access to System Components and Cardholder Data

Logging and monitoring must support timely detection and investigation.

RidgeBot® Support:
- Identifies exploitable paths to tamper with logs or monitoring systems
- Provides forensic visibility into attack paths
- Supports incident response investigations

Requirement 11
Test Security of Systems and Networks Regularly

Security controls must be tested continuously.

RidgeBot® Support:
- Continuous automated penetration testing
- Internal and external attack simulation
- Coverage far exceeding minimum testing frequencies

Requirement 12
Support Information Security with Organizational Policies and Programs

Organizations must maintain security governance, risk management, and incident response processes.

RidgeBot® Support:
- Continuous risk validation aligned to policy requirements
- Evidence generation for audits and risk assessments
- Support for incident response and remediation suggestions

PCI DSS 4.0 Outcome-Based Compliance Model

Continuous Audit Readiness and Reporting

RidgeBot® generates detailed, auditor-ready reports documenting:

- Assets tested
- Vulnerabilities identified and exploited
- Risk prioritization
- Remediation actions and validation results

This enables organizations to remain continuously audit-ready under PCI DSS 4.0.

Appendix A
PCI DSS 4.0 Requirement Mapping to RidgeBot® Capabilities

This appendix maps RidgeBot®'s API testing capabilities to the OWASP API Security Top 10.

PCI DSS 4.0 Requirement	Security Objective	RidgeBot® Validation Evidence
Req. 1 – Network Security Controls	Prevent unauthorized network access	Firewall and segmentation attack-path validation reports
Req. 2 – Secure Configurations	Reduce attack surface	Asset discovery, weak/default configuration findings
Req. 3 – Stored Data Protection	Protect cardholder data	Access-path validation to sensitive data stores
Req. 4 – Cryptography in Transit	Prevent data interception	Encryption weakness detection and validation
Req. 5 – Malware Protection	Prevent malware execution	Exploit simulations enabling malware delivery
Req. 6 – Secure Systems & Software	Reduce exploitable vulnerabilities	Continuous vulnerability exploitation validation
Req. 7 – Access Restriction	Enforce least privilege	Privilege escalation and lateral movement testing
Req. 8 – Authentication	Ensure strong identity controls	MFA validation and credential abuse testing
Req. 9 – Physical Security	Protect physical systems	Testing of systems managing physical access
Req. 10 – Logging & Monitoring	Enable detection & response	Log tampering and attack-path forensic analysis
Req. 11 – Continuous Testing	Maintain ongoing security	Automated continuous penetration testing
Req. 12 – Security Governance	Sustain security program	Policy-aligned risk validation evidence

Conclusion

PCI DSS 4.0 represents a decisive shift toward continuous, outcome-driven security. RidgeBot® enables organizations to operationalize PCI DSS 4.0 requirements through automated, continuous, and risk-based security validation, delivering defensible audit evidence and materially reducing breach risk.

By aligning offensive security validation with PCI DSS 4.0 objectives, RidgeBot® empowers organizations to move beyond compliance and achieve resilient payment security.

About Ridge Security

Ridge Security is a leader in Adversarial Exposure Validation and is dedicated to developing innovative cybersecurity solutions designed to protect organizations from advanced cyber threats. Ridge Security's flagship product RidgeBot® incorporates advanced artificial intelligence to deliver automated exposure validation continuously. With a focus on automation, intelligence, and actionable insights, Ridge Security enables security teams to stay ahead of emerging threats.

Ridge Security Technology Inc.
https://ridgesecurity.ai/

Follow us online