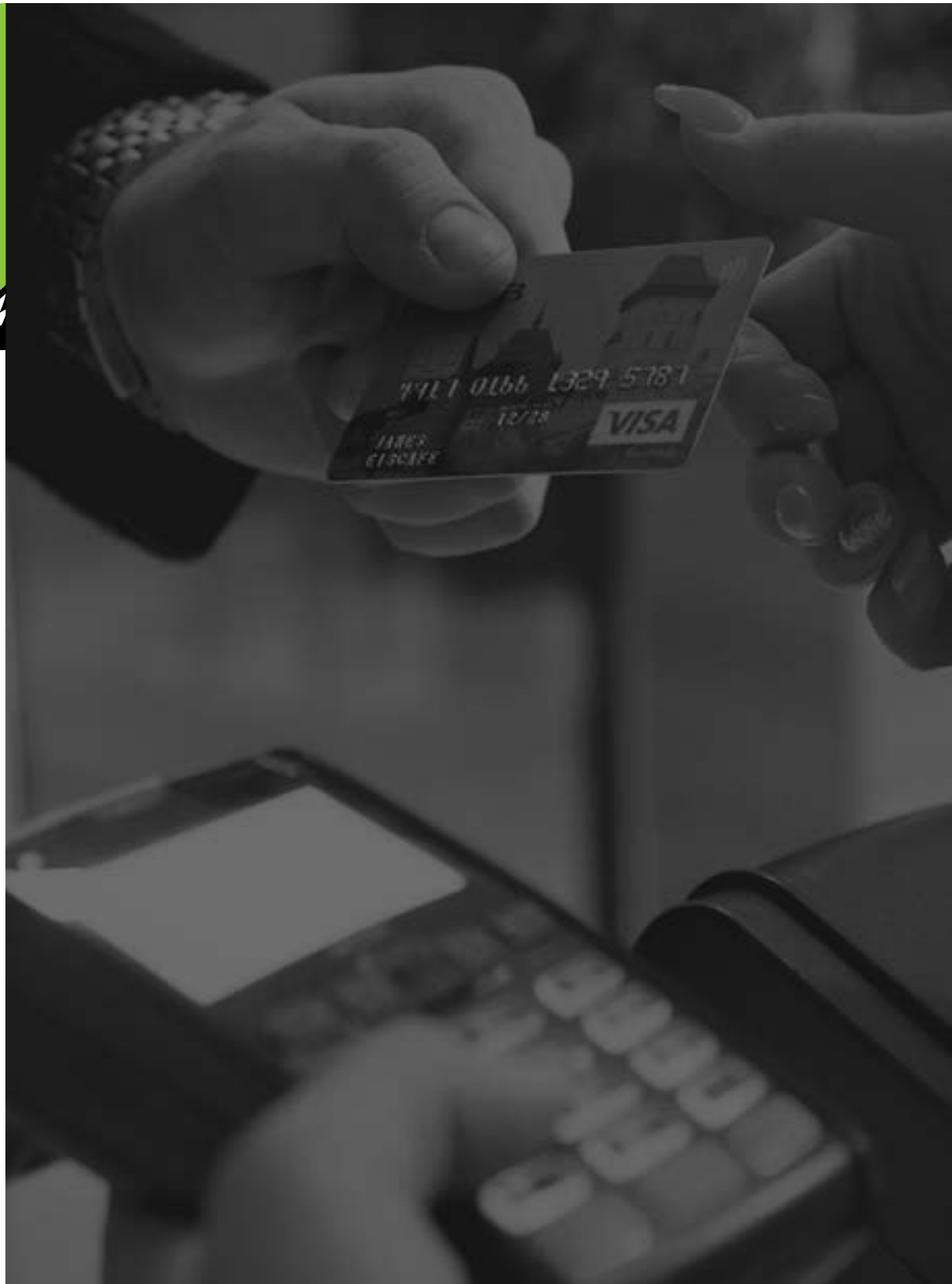
PCI DSS Compliance

Using RidgeBot Security Validation

RIDGE SECURITY



Overview

Continuous Validation with Automated Attacks; Detailed Steps to Resolve and Lock Down Vulnerabilities

The digital transformation of worldwide economic, business and government operations has seen rapid growth in security defense technologies such as encryption, Next-gen firewalls, filtering methods, malware screening, multi-factor authentication, and surveillance.

Despite advances in these defensive technologies, networks, hosts and applications are continuously under attack by increasingly creative and sophisticated methods. Breaches are continually growing in number, size, and the damage inflicted by the attackers.

Industry Trends

Traditional defensive security mechanisms have failed to adequately protect networks, data centers, hosts, and applications from infiltration, attacks, and breaches. The effectiveness of traditional defensive security mechanisms pivots mainly on the concept of border security—while increasingly, industry trends in SaaS, IaaS, cloud computing, IoT, virtualization, and mobility have blurred or erased borders in networks and computer processing and storage systems.

Security posture is also distressed because, while attacks have escalated in number, subtlety, and precision, IT resources for security measures, audits, and protective activities, have tightened.

Penetration Testing

Rapidly increasing threat incidence and sophistication have made it imperative to harden security postures with active, offensive methods. Posturing that does not supplant, but is an addition to traditional defensive measures—such as penetration testing that probe for vulnerabilities. Address vulnerabilities before exploitation.

Breach Prevention Traditional Defense 2002	Post Breach Detection 2012	Pre-Breach Offensive Defense 2020

Penetration testing is an expensive, resource-intensive, disruptive, and often manual process executed periodically (for example, annually). Testing may happen only when there is an upcoming audit or other collateral need to gain or reaffirm compliance with one of the many worldwide standards and regulations regarding financial, personal, health, or additional sensitive information. Your environment is vulnerable during the often lengthy periods in between audits doing scheduled pen-testing validation.

Automated Continuous Validation with RidgeBot

RidgeBot is an intelligent robot that provides low-cost, continuous, automated security validation services to harden your security posture ongoing and deliver always-on compliance monitoring. It has built-in collective real-time knowledge of the latest threats, vulnerabilities, exploits, and state-of-the-art AI/ML-assisted hacking methods and techniques. It scales as needed and runs as a VM, on an appliance, or as SaaS.

RidgeBot automates penetration testing, making it an ongoing high-use tool integral to your security policy and procedures instead of an expensive one-time test exercise. RidgeBot is your personal robot assistant that details how and where a hacker can successfully compromise your assets. It recommends step-by-step instructions on how to build and maintain your assets in a secure, protected manner.

RidgeBot does much more than a pen-test: it auto-discovers assets and then proceeds to probe them continuously, iteratively, fully automated, at scale, and exploits the vulnerabilities found. In its report, it alerts you to the ranked short-list of dangerous, successfully exploited vulnerabilities as well as a list of lower-priority, non-exploited vulnerabilities. Your network is always locked down, always patch-up-to-date, always ready for audit, always ready to submit proof of security posture—all at minimal cost and human intervention.

RidgeBot provides the following key capabilities:

- **Discovery:** Automatically crawls through your environment to identify and document types of assets (including networks, hosts, applications, plug-ins, images, IoT devices, and mobile devices) and the attack surfaces of those assets.
- **Scanning:** Mine assets and attack surfaces for vulnerabilities by leveraging Ridge Security's leading-edge Threat Intelligence Platform—a collective vulnerability knowledge database—that includes more than 2-billion pieces of security intelligence data, 100 million attack libraries, and 150K exploit libraries.
- **Exploit:** AI/ML-assisted attack techniques/modes automatically exploit vulnerabilities found. Document findings, along with remediation recommendations in accurate, reliable, and usable reports. AI/ML algorithms draw on an expert knowledge base to guide RidgeBot in attack-path-finding and path-selection. Launch iterative attacks based on learning along the path, achieving much broader test coverage and more in-depth inspection than traditional pen-test methods.
- **Post-exploit Risk Prioritization:** RidgeBot visualizes the kill-chain and quantifies risks based on multiple factors to give organizations a detailed and specific ranking of the most dangerous vulnerabilities. RidgeBot's analytics drastically reduce the manual work required to rank and remediate vulnerabilities, focusing on specific exploitable vulnerabilities (a single-digit percentage).

PCI DSS Overview

The Payment Card Industry Data Security Standard (PCI DSS) strives to improve the overall security of electronically stored, processed, and transmitted data and transactions found in enterprise and government distributed networks and data centers. The PCI DSS standard helps merchants and financial institutions understand and implement security policies, technologies, and ongoing processes to protect payment systems from breaches and theft of payment card data.

PCI DSS applies worldwide to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data.

Type of Requirement: Financial industry standard.

Geographic Applicability: Worldwide.

Ownership: The PCI DSS standard was formed in 2006 by a consortium of financial payment companies (American Express, Discover, JCB International, MasterCard, and Visa) forming the PCI Security Standards Council (PCI SSC) who fines any business for data breaches that expose payment card transactions or data.

Compliance Verification and Enforcement: Evidence of compliance is submitted to the PCI SSC. Periodic vulnerability scans are required by an Approved Scanning Vendor (ASV). Breaches and evidence of non-compliance are fined.

More information: https://www.pcisecuritystandards.org/pci_security/

PCI DSS Goals and Requirements

There are 12 PCI DSS requirements—structured into 6 distinct goals—with which an organization must comply.

Goal	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system pass words and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly up date anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know. 8. Identify and authenticate access to system compo-nents. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

PCI DSS Requirements

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

1. Protect stored cardholder data.
2. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

1. Protect all systems against malware and regularly update anti-virus software or programs.
2. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

1. Restrict access to cardholder data by business need-to-know.
2. Identify and authenticate access to system components.
3. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

1. Track and monitor all access to network resources and cardholder data.
2. Regularly test security systems and processes.

Maintain an Information Security Policy

1. Maintain a policy that addresses information security for all personnel.

OVERVIEW

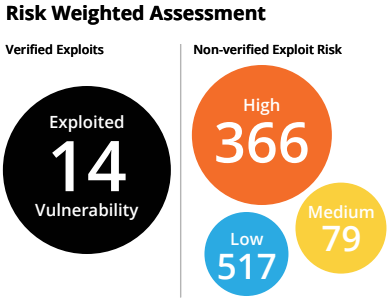
How RidgeBot Can Help

RidgeBot helps find non-compliant issues in your assets and guides how to resolve the exposure immediately. Moreover, RidgeBot continually maintains a security posture that is always in compliance with PCI DSS and other standards and regulations.

Some of RidgeBot's key benefits to your organization's security posture include:

Improve and Simplify Security Activities and Process

- Discover, inventory, and document system components, assets, and attack surfaces. Because RidgeBot is fully automated, you can do this continuously or at much more frequent intervals than previous periodic manual processes.
- Reports help document vulnerabilities found, exploited, remediated, and validated.
- Reports provide clear risk-ranking to focus manual remediation activity on the highest risk vulnerabilities.
- RidgeBot's flexibility allows you to run attack testing from inside and outside your environment.
- Ridge Security's Threat Intelligence Platform knowledge base ensures that you are always up to date with industry-leading security vulnerability information.



- Run RidgeBot attacks and scans as a standard part of your ongoing security policy.

Continuous Security Validation

- RidgeBot provides no-cost iterative, continuous hardening, and asset inventory. You can run different scans periodically or continuously—because it is fully automated, no manual intervention is required until a vulnerability is reported.
- Continuous monitoring and asset discovery protect against hacker intrusion caused by an employee (or any other person) accidentally or maliciously connecting untrusted or unplanned IoT, wireless, or other unauthorized devices to the environment.
- Scan reports provide a shortlist of must-fix exploitable vulnerabilities to document and resolve. Report output ensures all software patches and updates needed to resolve dangerous vulnerabilities are installed on all affected assets.

DevOps/SecOps Software Development and Release Testing

- Use RidgeBot during the software development process. Help ensure that dangerous coding practices that introduce vulnerabilities never ship in new releases of software.
- Use RidgeBot to harden software patches, software upgrades, new devices, and any configuration changes before pushing them into the production environment.

Security Posture Validation

- Continuously and iteratively attack the production environment. Maintain a security posture and discover misconfigurations in wireless or defensive security appliances or services such as firewall rules or UTM appliances.
- Continuously monitor and harden login credentials on sensitive assets.

Compliance Audit

- Continuous asset discovery scanning and attack and exploitation attempts (and the reports issued) mean your environment is always audit-ready.
- Use RidgeBot reports to submit evidence of vulnerabilities probed, remediated, and resolved.

Security Incident Response

- Scan reports containing recommended solutions for each vulnerability found, provide critical information to your security incident response/escalation team.
- Risk ranking of vulnerabilities feeds into the priorities and procedures for incident response.
- RidgeBot AI/ML exploitation attacks provide forensic capabilities to investigate the origin and path taken by a breach and step-by-step guidance on how to resolve the entry point vulnerability.

RidgeBot includes several template scans, as well as the flexibility to customize your own scans completely. The system templates include:

- **Full Scan**: This test launches numerous attack techniques used by real-world hackers. Based on threat intelligence and an exploit knowledge base, RidgeBot profiles assets, mines vulnerabilities, and launches attacks against target assets, which may be internal or external to your environment, in a private or public environment.
- **Weak Password Scan**: This test launches direct or iterative attacks based on sensitive information collected via weak credential or unauthorized access vulnerabilities. Attack targets include Redis, Elasticsearch, ActiveMQ, database, web login, and other applications.
- **Struts 2 Scan**: This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using the Struts 2 framework.
- **Weblogic Scan**: This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using Weblogic middleware.
- **Web Scan**: This test launches cyberattacks against target websites, web applications, and all related attack surfaces, gaining control of the target website for self-developed and contact management system-based websites.
- **Host Scan**: This test launches direct or iterative attacks from inside a corporate network to validate the security system's response to an internal threat. Target systems include all network-accessible internal hosts and servers.

SPECIFIC REQUIREMENTS

How RidgeBot Can Help

PCI Req 1: Install and maintain a firewall configuration to protect cardholder data.

1.1 Establish and implement firewall and router configuration standards. Formalize testing whenever configurations change; that identify all connections between the cardholder data environment and other networks (including wireless); that document various technical settings for each implementation; review of configuration rule sets at least every six months.

1.2 Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment.

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

1.4 Install personal firewall software or equivalent on any devices (company and private) that connect to the Internet when outside the network and access the cardholder data environment.

USING RIDGEBOT TO COMPLY

- Run a scan against any firewall or router where the configuration or software image has changed—run the scan in a staged environment before deploying to the production network. Rerun the test against the production environment (hosts, web servers, and clients behind the changed firewall or router) with exploitation turned on for the vulnerabilities found.
- Run a scan against any software-firewalled or software-secured hosts or client devices.
- Run a scan from all "untrusted" networks, such as the Internet, to gain entry into the secured environment.

PCI Req 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

2.1 Always change [ALL] vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network, including wireless devices connected to the cardholder data environment or used to transmit cardholder data.

2.2 Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

2.3 Encrypt all non-console administrative access using strong cryptography.

2.4 Maintain an inventory of system components that are in scope for PCI DSS.

2.5 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data.

USING RIDGEBOT TO COMPLY

- Run a weak password scan against all assets to document and resolve login credential vulnerabilities.
- Run a full scan with exploitation turned on for the vulnerabilities found. The AI/ML exploitation engine uses Ridge Security's industry-leading knowledge base on attack methods and techniques.
- Run a scan specifically targeting encryption-related vulnerabilities such as Pulse Secure SSL VPN Arbitrary File Read Vulnerability (CVE-2019-11510), OpenSSL End of Life Detection on Linux, Splunk Enterprise Multiple OpenSSL Vulnerabilities, and Debian Security Advisory DSA 1726-1 (python-crypto).
- Run an asset discovery scan to ensure all assets and attack surfaces are identified and documented in the system components inventory. Iteratively running this scan will immediately discover any changes in the presence of assets.
- Make continuous RidgeBot scans part of your security policy and procedures.
- Run a scan against any provider- or cloud-hosted assets and services.

PCI Req 3: Protect stored cardholder data.

REQUIREMENT

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data without the proper cryptographic keys, the data is unreadable and unusable to that person.

3.1 Minimize cardholder data storage by implementing data retention and disposal policies, procedures, and processes.

3.2 Do not store sensitive authentication data after authorization (even if it is encrypted).

3.3 Mask PAN (Primary Account Number) when displayed to the first six and last four digits.

3.4 Render PAN, at minimum, unreadable anywhere it is stored.

3.5 Protect cryptographic keys used for cardholder data from disclosure and misuse.

3.6 Document and implement all appropriate key management processes and procedures for cryptographic keys used to encrypt cardholder data.

USING RIDGEBOT TO COMPLY

- Run an asset discovery scan to identified and inventoried all assets that hold cardholder data. Ensure the proper assessment of these data storage assets.
- Run a weak password scan against all assets that hold cardholder data to document and resolve login credential vulnerabilities.

PCI Req 4: Encrypt transmission of cardholder data across open, public networks.

REQUIREMENT

Sensitive cardholder data must be encrypted during transmission over networks easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targeted by malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

4.1 Use strong cryptography and security protocols such as SSL/TLS, IPSEC, and IEEE 802.11ix to safeguard sensitive cardholder data during transmission over open, public networks (e.g., Internet, wireless, GSM, GPRS). WEP was prohibited for new implementations after 31 March 2009 and for existing implementations after 30 June 2010.

4.2 Never send unencrypted PANs by end-user messaging technologies.

USING RIDGEBOT TO COMPLY

- Run a scan specifically targeting encryption-related vulnerabilities.
- Run an asset discovery scan to ensure all wireless assets and attack surfaces are identified. Run a weak password scan against all wireless assets to document and resolve login credential vulnerabilities.

PCI Req 5: Protect all systems against malware and regularly update anti-virus software or programs.

REQUIREMENT

Malware—including viruses, worms, and Trojans—enters the network during many business-approved activities (e-mail, Internet, mobile devices, storage devices) that exploit system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware—for current and evolving software threats.

5.1 Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).

5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

USING RIDGEBOT TO COMPLY

- Run a full scan iteratively against all assets and attack surfaces to find, document, and correct any vulnerabilities that a hacker can exploit to inject malware into the environment.

PCI Req 6: Develop and maintain secure systems and applications.

REQUIREMENT

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Vendor-provided security patches fix many of these vulnerabilities. All systems must have appropriate software patches to protect against exploitation by malicious individuals and software.

6.1 Identify security vulnerabilities using reputable outside sources for security vulnerability information and assign a risk ranking to newly discovered security vulnerabilities.

6.2 Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches.

6.3 Develop internal and external software applications in accordance with PCI DSS based on industry best practices and incorporate information security throughout the software development life cycle.

6.4 Follow change control procedures for all changes to system components.

6.5 Develop all web applications based on secure coding guidelines and review custom application code to identify coding vulnerabilities.

6.6 Protect all public, web-facing applications against known attacks with annual reviews of code. Install a Web application firewall in front of public-facing Web applications.

USING RIDGEBOT TO COMPLY

- Run a full scan with exploitation turned on for the vulnerabilities found as a regular part of the software development, software validation, and change control processes and procedures.
- Run continuous and iterative full scans with exploitation turned on for the vulnerabilities found against all production web servers and applications. The AI/ML exploitation engine uses Ridge Security's industry-leading knowledge base on attack and hardening actions.
- Run a full scan against any updated software or patches to ensure no new vulnerabilities are introduced before putting the software update in your production environment.
- Run an access scan to ensure appropriate access controls exist to separate your software development/test environments from production environments.

PCI Req 7: Restrict access to cardholder data by business need to know.

REQUIREMENT

Access critical data only by authorized personnel, systems, and processes that must be in place. Limit access based on need-to-know and according to job responsibilities.

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

7.2 Establish an access control system for systems' components with multiple users that restricts access based on a user's need-to-know. Set to "deny all" unless specifically allowed.

7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

USING RIDGEBOT TO COMPLY

- Run a weak password scan against all assets to document and resolve login credential vulnerabilities.
- Run a scan against access control systems and devices to ensure these cannot be compromised to allow a hacker to erase or alter logs.

PCI Req 8: Identify and authenticate access to system components.

REQUIREMENT

Assign a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions and can be tracked and traced.

8.1 Assign all users a unique user name before allowing them to access system components or cardholder data.

8.2 Employ at least one of these to authenticate all users: password or passphrase; or two-factor authentication (such as token devices, smart cards, biometrics, or public keys).

8.3 Secure all individual non-console administrative access and all remote access using multi-factor authentication.

8.4 Document and communicate authentication policies and procedures, such as strong passwords and not reusing passwords, to all users.

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods.

8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, or certificates), assign the use of these mechanisms to an individual, not a group.

8.7 All access to databases containing cardholder data (including access by applications, administrators, and all other users) is restricted.

USING RIDGEBOT TO COMPLY

- Run a weak password scan against all assets containing cardholder data to document and resolve login credential vulnerabilities.

PCI Req 9: Restrict physical access to cardholder data.

REQUIREMENT

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

9.2 Develop procedures to help personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.

9.3 Control physical access for onsite personnel to sensitive areas.

9.4 Use a visitor log to maintain a physical audit trail of visitor information and activity.

9.5 Store media back-ups in a secure location, preferably off-site.

9.6 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.

9.7 Maintain strict control over the storage and accessibility of media that contains cardholder data.

9.8 Destroy media containing cardholder data when it is no longer needed for business or legal reasons.

9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.

USING RIDGEBOT TO COMPLY

- Run an access scan to ensure that all systems or devices used to control, log, or surveil physical entry to premises or places where physical media or backups of cardholder data are stored. Secure weak credentials or other software/malware vulnerabilities where a hacker can access physical entry (instead of denying it), erase or alter logs, video surveillance, or audit trail information.

PCI Req 10: Track and monitor all access to network resources and cardholder data.

REQUIREMENT

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

10.1 Establish a process for linking all access to system components to each user, especially access done with administrative privileges.

10.2 Implement automated audit trails for all system components for reconstructing access events.

10.3 Record audit trail entries for all system components for each access event.

10.4 Synchronize all critical system clocks and times.

10.5 Secure audit trails so they cannot be altered.

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.

USING RIDGEBOT TO COMPLY

- Run an access scan to ensure that all systems or devices used to control, log, or surveil physical entry to premises or places where physical media or backups of cardholder data are stored. Systems or devices must be secure from weak credentials or other software/malware vulnerabilities. As we know, a hacker can get access to allow physical entry (instead of denying it) or to erase or alter logs, video surveillance, or audit trail information.
- Scan reports can document security failures and the steps taken to resolve them. A subsequent scan (after remediation) can confirm that a specific detected vulnerability is no longer present in the system or device where the failure initially occurred.
- A forensic scan—after a security incident has occurred in logging or surveillance systems or devices—can also determine where and how the breach occurred.

PCI Req 11: Regularly test security systems and processes.

REQUIREMENT

Vulnerabilities are being discovered continually by malicious individuals and researchers, introduced by new software. System components, processes, and custom software need to be tested frequently to ensure security controls continue to reflect a changing environment.

11.1 Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points quarterly.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant network change.

11.3 Implement a methodology for penetration testing that includes testing based on industry-accepted penetration testing approaches (such as NIST SP800-115), coverage of the entire cardholder data environment perimeter and critical systems, and testing from both inside and outside the network.

11.4 Use IDS/IPS techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment and critical points in the environment, and alert personnel to suspected compromises.

11.5 Deploy a change-detection mechanism (such as file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.

USING RIDGEBOT TO COMPLY

- Run an asset discovery scan to ensure all wireless assets and attack surfaces are identified and documented.
- Run full scans, with exploitation turned on for found vulnerabilities, as a regular part of your policy and process for hardening new software during the software development process.
- Run full scans, with exploitation, turned on for found vulnerabilities, as a regular part of your policy and process for hardening software patches, software upgrades, new devices, and any configuration changes before pushing them live into the production environment.
- Run full scans, with exploitation, turned on for found vulnerabilities, as a regular part of your security posture policy to achieve ongoing monitoring and hardening of your production environment.
- RidgeBot's built-in AI/ML exploitation engine uses Ridge Security's industry-leading knowledge base of attack techniques and ensures that your assets are always hardened with the most up to date vulnerability intelligence.
- Running automated, continuous, iterative scans on your internal and external networks allow you to cost-effectively execute pen-test scans on an ongoing basis—far more frequently than the quarterly requirement in the standard and ensures always-on security monitoring and compliance.

PCI Req 12: Maintain a policy that addresses information security for all personnel.

REQUIREMENT

A firm security policy sets the whole entity's security tone and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

12.1 Establish, publish, maintain, and disseminate a security policy.

12.2 Implement a risk-assessment process, performed at least annually. Upon significant changes to the environment, identify critical assets, threats, and vulnerabilities, resulting in a formal documented analysis of risk.

12.3 Develop usage policies for critical technologies to define the proper use of these technologies.

12. 4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

12.5 Assign the responsibility to establish, document, and distribute security policies and procedures; monitor and analyze alerts; establish, document, and distribute incident responses and escalation to an individual or team-information security management team.

12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

12.7 Screen new hires before hiring to minimize the risk of attacks from internal sources.

12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect cardholder data security.

12.9 Service providers must acknowledge in writing that they are responsible for the security of cardholder data. This means data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer or the extent to which they could impact the security of the customer's cardholder data environment.

12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.11 Service providers are to perform reviews at least quarterly to confirm that personnel follows security policies and operational procedures.

USING RIDGEBOT TO COMPLY

- Make continuous asset discovery scans a regular part of your security policy, procedures, and documentation to inventory assets. Discover any new or changed devices in the environment that might pose new attack surfaces.
- Make continuous scans, with exploitation turned on for the vulnerabilities found, part of your security policy, procedures, documentation, and incident response actions.
- With exploitation turned on for the vulnerabilities found, make continuous scans part of your software or website development process. Also, run the testing process to harden software patches, software upgrades, new devices, and any configuration changes before pushing them into your production environment.
- Scan reports—which include recommended solutions for each vulnerability—provide critical information for your security incident response/escalation or forensics team to ensure timely and effective handling of all situations.

Company Profile

Ridge Security delivers ethical, efficient and affordable pen testing solutions to enterprises, small and large. We ensure our customers stay compliant, alerted and secure at all times in the cyber world. The management team has many years of networking and security experience. Ridge Security is located in the heart of Silicon Valley and is expanding into other areas including Latin America, Asia and Europe.

RidgeBot, a robotic penetration testing system, fully automates the testing process by coupling ethical hacking techniques to decision-making algorithms. RidgeBots locate, exploit and document business risks and vulnerabilities discovered during the testing process, highlighting the potential impact or damage.

Ridge Security Technology Inc.
www.ridgesecurity.ai