RAPID7

PCI DSS V3.2 EXPLAINED

How to Achieve Compliance with the Payment Card Industry Data Security Standard (PCI DSS)

TABLE OF CONTENTS

WHAT IS PCI DSS?

Negative media coverage, a loss of customer confidence, and the resulting loss in sales can cripple a business. As a result, all entities that handle credit cardholder information are being challenged to adopt more effective data protection measures.

The Payment Card Industry Data Security Standard (PCI DSS) was created to protect credit cardholder data, and it is now on version 3.2, released in April 2016. The PCI DSS version 3.2 encompasses twelve requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. These requirements are grouped into six major categories, shown to the right.

In total, the PCI DSS has six domains, twelve requirements, and 200 detailed sub-requirements. Page 12 of this compliance guide provides a breakdown of PCI requirements in detail.

The PCI Security Standards Council (SSC) owns, develops, maintains, and distributes the PCI DSS. The SSC also provides oversight of external on-site Qualified Security Assessors (QSA) and Internal Security Assessors (ISA) to validate compliance, the qualification of PCI Forensic Investigators (PFI) that act on compromised cases, and the certification of Approved Security Vendors (ASV) to perform external vulnerability scans and deliver an Attestation of Compliance.

In order to safeguard credit cardholder personal information, the five major payment card brands have endorsed PCI DSS: Visa, MasterCard, Discover Financial Services, American Express, and
JCB International.

The PCI DSS requirements are grouped into six major categories:

Build and maintain a secure network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

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

Protect cardholder data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

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

Requirement 6: Develop and maintain secure systems and applications

Implement strong access control measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Identify and authenticate access to system components

Requirement 9: Restrict physical access to cardholder data

Regularly monitor and test networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an information security policy

Requirement 12: Maintain a policy that addresses information security for all personnel

WHO NEEDS TO BE PCI COMPLIANT AND WHY?

As a global standard, the PCI DSS applies to any entity worldwide that stores, processes or transmits credit cardholder data. This includes financial institutions, merchants and service providers in all payment channels.

- Financial institutions include banks, insurance companies, lending agencies, and brokerages.
- Merchants include restaurants, retailers (brick-and-mortar, mail/telephone order, e-commerce), transportation operators, and virtually any point-of-sale that processes credit cards across all industries.
- Examples of service providers include transaction processors, payment gateways, customer service entities, (i.e. call centers), managed service providers, web hosting providers, data centers, and Independent Sales Organizations.

The five major payment card brands enforce PCI compliance validation by requiring merchant banks to meet specific auditing and reporting criteria for their respective merchants and service providers. Each payment card brand has its own compliance program to uphold the PCI standard by enforcing PCI auditing and reporting requirements that must be met by the acquiring banks for merchants (also called merchant banks) in order to provide access to their payment network. See page 5 for a breakdown of the payment card brand requirements for merchants and service providers.

The merchant bank then needs to produce evidence that merchants using their bank, along with any service providers used by those merchants, are in fact PCI compliant. This chain of liability at each level is designed to protect credit cardholder data by using PCI DSS to mitigate the risk of data breaches in the rapidly evolving threat landscape.

COMPLIANCE VALIDATION TOOLS AND REQUIREMENTS

Any organization that needs to be PCI compliant must definitively prove their compliance with standards and practices in place. Thankfully, PCI has a number of available tools to help validate compliance. In this next section, we'll review some of these compliance validation tools and what PCI requirements they help fulfill.

Approved Scanning Vendor (ASV) network vulnerability scans

This tool has been specifically designed to help organizations meet one particular requirement of PCI DSS (11.2.2):

> Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).

PCI requires external vulnerability scans to be performed on a quarterly basis by security companies qualified by the PCI Council (PCICo)—Approved Scanning Vendors.

The scope of the external vulnerability scan must include all externally accessible system components that are part of the cardholder data environment (CDE). It should also include any externally facing component that provides a path to the CDE.

The scan customer is responsible for defining the scope of the external vulnerability scan. If an account data compromise occurs via an externally facing system component not included in the scan, the scan customer is responsible.

ASVs validate any IP addresses found during the scan with the customer to determine whether or not they should be included within the scope of the assessment.

ASV scan reports consist of three parts:

1. An attestation of compliance—a declaration of global compliance
2. An executive summary—provides component compliance summary information
3. A detailed vulnerability report—detailed list of vulnerabilities found

Organizations can obtain a passing result on their network vulnerability scan when the scan report does not contain:

- High- or medium-severity vulnerabilities
- Automatic failures (as defined by the PCICo)

To be considered compliant, an organization must conduct four consecutive passing ASV scans within twelve months.

Notes:

- A passing scan report may require multiple iterative scans.
- Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed.
- Additional documentation may be required to verify that non-remediated vulnerabilities are in the process of being addressed.

Self-assessment questionnaire

The self-assessment questionnaire (SAQ) allows organizations to evaluate their compliance with PCI DSS. This is a useful tool to determine, document, and modify alignment with the standard.

There are as many SAQ versions as there are merchant types. There are five kinds of merchant types for PCI: A, B, C-VT, C, and D. Each SAQ covers only the PCI sections and requirements relevant to the specific merchant type.

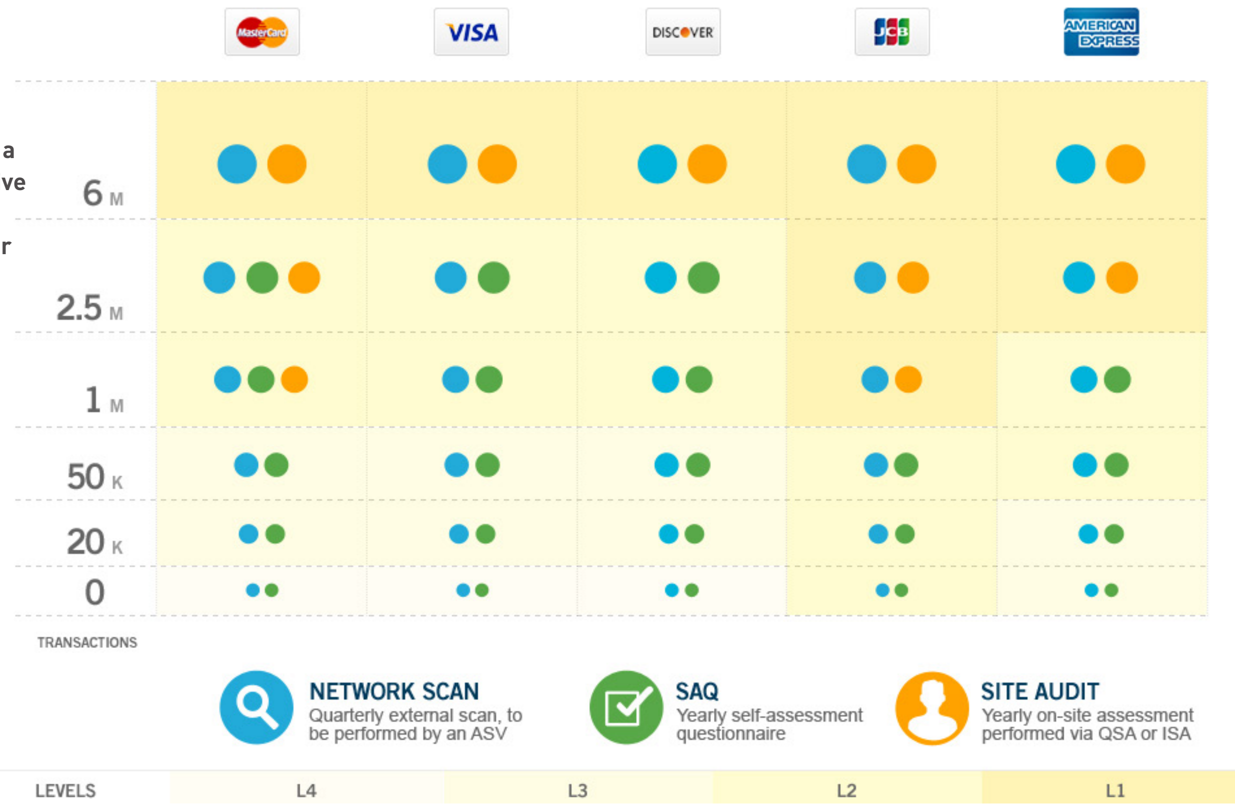
Each SAQ version has two parts:

1. Questions correlating to the PCI DSS requirements
2. Attestation of Compliance (AOC) or self-certification that a company is eligible to complete that specific SAQ

Rapid7 is a certified Approved Scanning Vendor (ASV) by the PCI Security Standards Council, authorizing us to help you achieve compliance with PCI DSS.

VALIDATION REQUIREMENTS FOR MERCHANTS

This chart gives a global perspective on validation requirements for merchants from each payment card brand. The requirements here are organized by level, from 1 through 4.



On-site audit

Organizations perform this thorough assessment internally in order to validate their adherence to the PCI standard.

Such assessments must be conducted by qualified external (QSAs) or internal security auditors (ISAs) trained and approved by PCICo.

If internal individuals are used, the key thing is that they must belong to an internal audit organization. For obvious conflicts of interest reasons, IT staff or information security staff must not perform the assessment.

To complete the on-site audit, organizations must:

- Validate the scope of the cardholder data environment
- Verify of all technical and procedural documentation
- Confirm that each PCI DSS requirement has been met
- Evaluate, accept, or reject compensating controls
- Produce a Report on Compliance (ROC)

Payment card brand-specific notes and recommendations:

MasterCard
Level 1 merchants: Annual on-site assessment can be executed by Internal Qualified Staff (ISA) if they have attended PCI SSC ISA Training and passed the accreditation program every year.

Level 2 merchants:

- Effective June 30, 2012, level 2 merchants that choose to complete an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC ISA Training and pass the associated accreditation program annually in order to continue the option of self-assessment for compliance validation.
- Alternatively, level 2 merchants may, at their own discretion, complete an annual on-site assessment conducted by a PCI SSC approved Qualified Security Assessor (QSA), rather than complete an annual self-assessment questionnaire.

Level 4 merchants: Consult acquirer for more information on completing the network scan and SAQ.

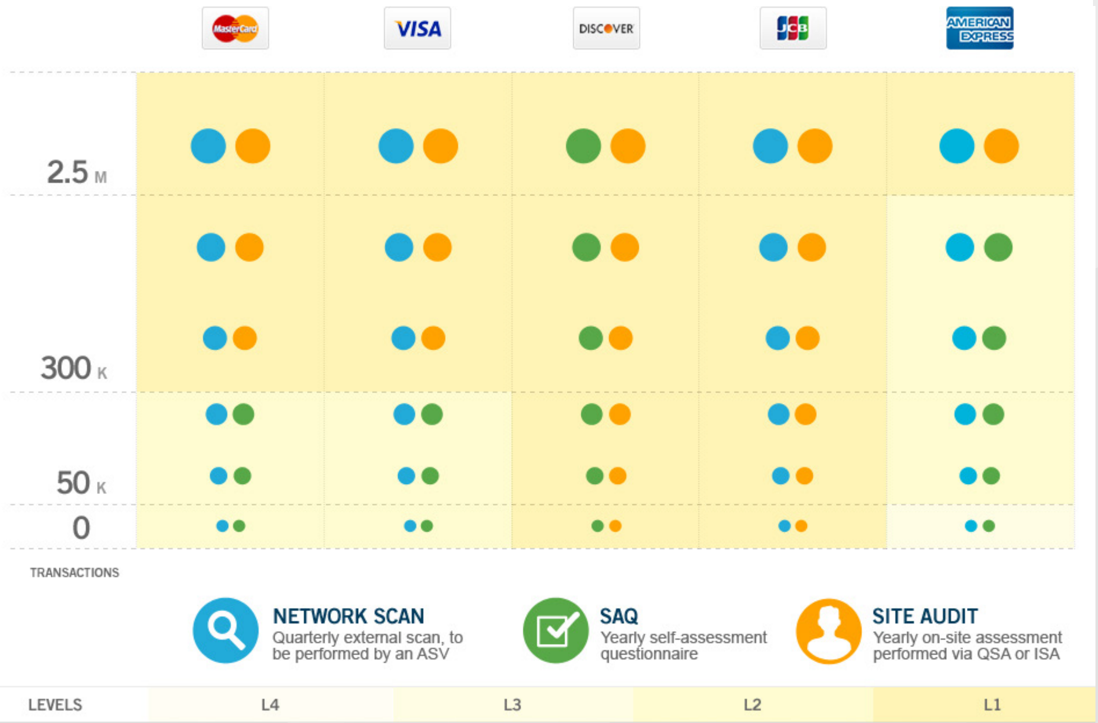
Visa
Network scans and SAQs for level 4 merchants are recommended. Compliance validation requirements are set by acquirers.

American Express and **Discover**
Network scans and SAQs for level 3 merchants (American Express) or level 4 (Discover) are not mandatory but strongly recommended.

JCB
Network scans for level 1 or level 2 merchants are not required if your organization does not handle cardholder data and transaction data via the internet or an internet-accessible network.

VALIDATION REQUIREMENTS FOR SERVICE PROVIDERS

This chart gives a global perspective on validation requirements for service providers from each payment card brand. The requirements here are organized by level, from 1 through 4.



Payment card brand-specific notes and recommendations:

MasterCard

- Level 1 service providers definition: All Third Party Processors (TPPs) and all Data Storage Entities (DSEs) with more than 300,000 total combined MasterCard and Maestro transactions annually.
- Level 2 service providers definition: All Data Storage Entities (DSE) with less than 300,000 total combined MasterCard and Maestro transactions annually.
- A DSE or Data Storage Entity is an entity other than a member, merchant, Independent Sales Organization (ISO), or Third Party Processor (TPP) that stores, transmits, and/or processes MasterCard account data for or on behalf of a merchant, ISO, or TPP.

Visa

- Level 1 service provider definition: VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 Visa transactions annually.
- Level 2 service provider definition: Any service provider that stores, processes and/or transmits less than 300,000 Visa transactions annually.

JCB

- For all service providers: Network scans and site audits are not required if your organization does not handle cardholder data and transaction data via the internet or an internet-accessible network.

American Express

- For level 3 service providers: Network scans and SAQs are not mandatory but strongly recommended.

Discover

- For all service providers: Discover authorizes use of either an annual on-site review by QSA or an annual SAQ.

HOW RAPID7 CAN HELP

Rapid7 has extensive experience partnering with financial institutions, merchants, and service providers globally such as Stein Mart, Trader Joe's, LendingTree, and E*TRADE FINANCIAL. Rapid7 is a certified Approved Scanning Vendor (ASV) by the PCI Security Standards Council, authorizing us to help you achieve compliance with the PCI Data Security Standard (DSS). Rapid7 can perform an independent, quarterly ASV vulnerability scan and produce the certified documentation for your records to satisfy PCI DSS Requirement 11.2. In addition, Rapid7 helps meet Report on Compliance (ROC) Audits through our trusted partner Qualified Security Assessors (QSAs).

Rapid7 InsightVM is a threat exposure management solution that helps organizations to find and fix vulnerabilities, misconfigurations, and exposures from the endpoint to the cloud.

In the context of PCI DSS version 3.2, InsightVM and Nexpose helps covered entities to:

- Perform quarterly internal and external vulnerability scanning of their environment.
- Implement secure configuration policies based on industry standards like CIS and DISA STIG.
- Identify and prioritize vulnerabilities based on threat exposure and asset criticality.
- Audit system access, authentication, and other security controls to detect policy violations.
- Automatically detect and scan new devices as they enter the network.
- Create, assign, track, and verify remediation tasks.
- Demonstrate compliance and communicate progress with reports, analytics, and live dashboards.

Rapid7 Metasploit is a penetration testing solution that provides risk assessment through the controlled simulation of a real world attack.

In the context of PCI DSS version 3.2, Metasploit helps covered entities to:

- Perform internal and external penetration tests on their network.
- Validate the effectiveness of network segmentation controls.
- Test access and authentication control systems and policies.
- Simulate password attacks to identify weak and shared credentials.
- Prioritize critical risks with closed-loop vulnerability validation.

- Simulate phishing campaigns to measure security awareness.
- Manage and document vulnerability exceptions and false positives/accepted risk

Rapid7 AppSpider is an application security solution that dynamically assesses web, mobile, and cloud applictions for vulnerabilities across all modern technologies.

In the context of PCI DSS version 3.2, AppSpider helps covered entities to:

- Automatically simulate attacks to test web applications.
- Identify gaps in compliance with best practices for secure software development.
- Integrate application security testing throughout the software development lifecycle.
- Continuously monitor applications for changes.
- Automatically generate targeted WAF/IPS rules.
- Identify web application vulnerabilities that allow unauthorized or insecure access.

Rapid7 InsightIDR is a SaaS SIEM powered by user behavior analytics, complete with both pre-built compliance dashboards and detections across the entire attack chain.

In the context of PCI DSS version 3.2, InsightIDR helps covered entities to:

- Securely centralize and store all log files from an existing network and security stack (e.g. Firewall, Authentication Logs, any event source) and correlate network behavior to the users and assets behind them.
- Audit the separation between development/test and production environments.
- Monitor access to cardholder data to ensure the user’s job requires access.
- Expose risky user behavior, including shared user accounts, non-expiring passwords, and anomalous administrative activity.
- Accelerate investigations with the ability to combine log search, real-time user activity, and endpoint artifacts together on a visual timeline.
- Track user authentications and admin activity across local, domain, and cloud services.
- Monitor disabled users and service accounts across on-premise and cloud systems to identify compromised credentials and lateral movement.
- Audit access to restricted assets.
- Alert the security team on top attack vectors behind breaches, including stolen credentials, phishing, and malware.

Rapid7 InsightOps is an IT Operations solution that automatically combines live log and asset data from across your infrastructure into one central and searchable location, so you can easily access the insight you need, when you need it.

In the context of PCI DSS version 3.2, InsightOps helps covered entities to:

- Confirm that there are no shared accounts and that normal and elevated administrative privileges are linked to individual, trackable users.
- Ensure audit trails exist for all individual accesses to cardholder data, administrative and root access actions, creation and deletion of system-level objects, and invalid logical access attempts.
- Record audit trail entries for all system components for each event, including event type, date and time, origination of event, and more.

Rapid7 offers a variety of **Advisory Services** to help organizations accelerate security improvement through industry-leading methodologies and experts who understand the attacker mindset.

In the context of PCI DSS version 3.2, the Rapid7 Advisory Services team helps covered entities to:

- Assist in completing the appropriate PCI Self-Assessment Questionnaire (SAQ) and documenting security policies and procedures.
- Develop and manage a vulnerability management program.
- Perform penetration testing on networks, applications, and users (social engineering).
- Build a penetration testing methodology.
- Perform a security program assessment to determine if security policies and procedures are being followed in actual day-to-day operations, identify gaps in their security program against PCI DSS, and provide guidance on developing missing control policies and procedures.
- Provide customizable security awareness training to users.
- Build an incident response plan and simulate breach scenarios to increase readiness.
- Detect and analyze threats in real-time, then investigate and remediate incidents.

RAPID7 SOLUTIONS FOR PCI DSS VERSION 3.2 COMPLIANCE

This section details the PCI DSS version 3.2 security requirements and how Rapid7 products and services help organizations become and remain compliant.

PCI DSS V3.2		InsightVM	Metasploit	AppSpider	InsightIDR	InsightOps	Consulting Services
Requirement 1	Install and maintain a firewall configuration to protect cardholder data	x	x	-	x	-	x
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters	x	x	x	-	-	x
Requirement 3	Protect stored cardholder data	-	-	-	x	-	x
Requirement 4	Encrypt transmission of cardholder data across open, public networks	x	-	x	-	-	x
Requirement 5	Protect all systems against malware and regularly update antivirus software or programs	x	-	-	x	-	x
Requirement 6	Develop and maintain secure systems and applications	x	x	x	x	-	x
Requirement 7	Restrict access to cardholder data by business need to know	x	-	x	x	-	x
Requirement 8	Identify and authenticate access to system components	x	x	x	x	-	x
Requirement 9	Restrict physical access to cardholder data	-	-	-	-	-	x
Requirement 10	Track and monitor all access to network resources and cardholder data	-	-	-	x	x	x
Requirement 11	Regularly test security systems and processes	x	x	x	x	-	x
Requirement 12	Maintain a policy that addresses information security for all personnel	-	-	-	x	-	x

Requirement 1 - Install and maintain a firewall configuration to protect cardholder data

1.1	Establish firewall and router configuration standards that include: approval, testing, and review processes; network connectivity and dataflow diagrams; description of groups, roles, and responsibilities; and business justification for use of all services, protocols, and ports allowed.
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in 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 on any portable computing devices (including company and/or employee-owned) that connect to the internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

Use Rapid7 InsightVM or Nexpose to:

- Manage baseline configuration policies and settings for auditing firewalls, routers, switches, hubs, ports, and network services. (Requirement 1.1)
- Generate a comprehensive mapping of network devices and services in order to detect devices and services that may allow connections between an untrusted network and any system components in the cardholder environment. (Requirement 1.1)
- Scan and monitor firewalls and routers for vulnerabilities and compliance with baseline configuration policies and settings. (Requirement 1.2)
- Detect configuration violations that allow unauthorized connections between cardholder data environments and untrusted networks. (Requirement 1.2)
- Integrate with Project Sonar to detect previously unknown externally facing devices. (Requirement 1.3)
- Verify that Windows firewall is enabled and configured to actively run on all workstations. (Requirement 1.4)

Use Rapid7 Metasploit to:

- Automatically test firewalls for open ports that allow outbound traffic and verify that egress filtering policies are effective at blocking traffic. (Requirements 1.2, 1.3)

Use Rapid7 InsightIDR to:

- Aggregate, search, and automatically attribute firewall log activity to the users behind them. (Requirement 1.5)

Use Rapid7 Consulting Services to:

- Recommend best practices to optimize network security components, including firewall and router configuration standards. (Requirements 1.1, 1.2)

- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirements 1.3, 1.4, 1.5)

Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters

2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
2.2	Develop configuration standards for all system components. Assure that these standards 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 security policies and operational procedures for managing vendor defaults and other security parameters 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. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.

Use Rapid7 InsightVM or Nexpose to:

- Automatically scan systems to identify vendor-supplied default passwords and accounts. (Requirement 2.1)

- Implement secure configuration policies and settings based on industry standards like CIS and DISA STIG, and automatically scan and monitor systems for compliance. (Requirement 2.2)

- Verify that each server only has a single critical role installed, default credentials have been changed, and unnecessary services and functionality are disabled. (Requirement 2.2)

- Assign custom asset tags to all devices in scope for PCI DSS, and assemble an inventory of all software and services on these devices. (Requirement 2.4)

Use Rapid7 Metasploit to:

- Scan ports to determine if there are multiple primary functions with differing security levels coexisting on the same server that should instead be implemented on separate servers. (Requirement 2.2)

- Determine if any non-console administrative access tools, including browser-based management tools, are not encrypted. (Requirement 2.3)

Use Rapid7 AppSpider to:

- Dynamically scan web applications for vulnerabilities, including HTTP authentication over insecure channel. (Requirement 2.3)

Use Rapid7 Consulting Services to:

- Evaluate configuration of all non-console administrative access to ensure appropriate use of encryption in security controls, and identify vulnerabilities that could lead to tampering with encryption keys in files and other encryption controls. (Requirement 2.3)
- Build and maintain system inventory. (Requirement 2.4)
- Create or validate security policies and operational procedures. (Requirement 2.5)
- Evaluate and recommend if shared hosting providers meet requirements defined in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers. (Requirement 2.6)

Requirement 3 - Protect stored cardholder data

3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures, and processes.
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.
3.4	Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: one-way hashes based on strong cryptography; truncation; index tokens and pads; strong cryptography with associated key-management processes and procedures.
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.

Use Rapid7 InsightIDR to:

- Monitor which users access critical systems or restricted network zones that may hold cryptographic keys, providing you with an access audit trail. (Requirement 3.5.1)

Use Rapid7 Consulting Services to:

- Identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirements 3.2 to 3.5)
- Evaluate key management processes and procedures for encryption of cardholder data, and provide recommendations as part of Rapid7 PCI Gap Analysis. (Requirement 3.6)
- Evaluate and document cardholder data policies and operational procedures associated with these requirements. (Requirement 3.7)

Requirement 4 - Encrypt transmission of cardholder data across open, public networks

4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.
4.2	Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.

Use Rapid InsightVM or Nexpose to:

- Identify all open ports and monitor traffic over secured and unsecured ports, including any evidence that any web applications, software enterprise applications, or databases are not using the ports assigned as secure ports for transmitting secure cardholder data. (Requirement 4.1)

Use Rapid7 AppSpider to:

- Dynamically scan web applications for vulnerabilities, including sensitive data transported over an unencrypted channel. (Requirement 4.1)

Use Rapid7 Consulting Services to:

- Recommend best practices to optimize data security, including end-user messaging policies. Identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirements 4.1, 4.2)
- Evaluate and document transmission encryption policies and operational procedures associated to these requirements. (Requirement 4.3)

Requirement 5 - Protect all systems against malware and regularly update antivirus software or programs

5.1	Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).
5.2	Ensure that all antivirus mechanisms are current, actively running, and capable of generating audit.
5.3	Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.

Use Rapid7 InsightVM or Nexpose to:

- Automatically generate a comprehensive mapping of all assets, including applications such as antivirus software, and verify that antivirus software has been deployed to all workstations. (Requirement 5.1)

- Scan all systems for vulnerabilities and misconfigurations, including versioning and patch levels, and verify that antivirus software and definitions are up to date on all workstations. (Requirement 5.2)
- Verify that antivirus software is actively running on all workstations. (Requirement 5.3)

Use Rapid7 InsightIDR to:

- Scan all endpoints for malware and identify risky user behavior, including compromised user accounts, malicious lateral movement, and anomalous administrative activity. This endpoint visibility is accomplished by a combination of the included Insight Agent and endpoint scans. (Requirements 5.1, 5.2)
- Verify that antivirus software is actively running on all workstations. (Requirement 5.3)

Use Rapid7 Consulting Services to:

- Evaluate and document antivirus policies and operational procedures associated with these requirements. (Requirement 5.4)

Requirement 6 - Develop and maintain secure systems and applications

6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
6.3	Develop internal and external software applications in accordance with PCI DSS (for example, secure authentication and logging) based on industry standards and/or best practices, and incorporate information security throughout the software development lifecycle.
6.4	Follow change control procedures for all changes to system components.
6.5	Address common coding vulnerabilities in software-development processes as follows: Train developers at least annually in secure coding techniques, including how to avoid common coding vulnerabilities; Develop applications based on secure coding guidelines.
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.
6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

Use Rapid7 InsightVM or Nexpose to:

- Prioritize vulnerabilities using an advanced scoring algorithm that takes into account the CVSS score, exploit and malware kit exposure, vulnerability age, and modify the risk score based on asset criticality. (Requirement 6.1)
- Scan all systems to ensure security patches and configurations are maintained based on user-specified parameters for all system components and software, including web applications, enterprise software, network components, and databases. (Requirement 6.2)

Use Rapid7 Metasploit Pro to:

- Identify and prioritize exploitable vulnerabilities. (Requirement 6.1)
- Simulate web application attacks to uncover weaknesses. (Requirements 6.2 to 6.6)

Use Rapid7 AppSpider to:

- Dynamically scan web, mobile, and cloud applications for vulnerabilities, and identify gaps in compliance against PCI DSS and industry best practices. (Requirements 6.3 to 6.6)
- Assess applications throughout the software development lifecycle by integrating with continuous integration, QA testing, and ticketing systems. (Requirement 6.3)
- Continuously monitor applications for changes to trigger a re-scan. Automatically generate targeted WAF/IPS rules to protect specific vulnerabilities against attacks. (Requirement 6.6)

Use Rapid7 InsightIDR to:

- Monitor multiple separated environments, define network zones and alert you if access policies are violated. As an example, an organization could prevent all users that are "developers" to access the network zone "PCI Production," ensuring InsightIDR alerts them on any such violations. (Requirements 6.4.1 and 6.4.2)

Use Rapid7 Consulting Services to:

- Perform penetration testing on web and mobile applications and deliver prioritized findings on compliance against PCI DSS and industry best practices. (Requirements 6.3 to 6.6)
- Recommend best practices for secure software development. Identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirements 6.3 to 6.6)
- Evaluate and document application security policies and operational procedures associated with these requirements. (Requirement 6.7)

Requirement 7 - Restrict access to cardholder data by business need-to-know

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(s) for systems components that restricts access based on a user's need to know, and is 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.

Use Rapid7 InsightVM or Nexpose to:

- Automatically monitor user access controls (including adherence to policies for role-based access) to ensure product users only have access to data that's relevant to them. (Requirement 7.2)

Use Rapid7 Metasploit to:

- Test access control systems and policies by simulating lateral movement and escalation of privilege type attacks. (Requirement 7.1 and 7.2)

Use Rapid7 AppSpider to:

- Dynamically scan web applications for vulnerabilities that allow unauthorized personnel to bypass access controls. (Requirement 7.2)

Use Rapid7 InsightIDR to:

- Flag systems in the cardholder data environment (CDE) as critical systems and alert you when suspicious authentications are detected (e.g. a user authenticating to the CDE that has never authenticated to it before, helping you enforce your policy). (Requirement 7.1)
- Flag systems in the cardholder data environment (CDE) as critical systems and alert whenever it sees any unusual authentications. You can set up different alerts for each CDE system based on who is allowed access to what system. Any user with an unexpected privilege escalation that could be used to access a CDE system will trigger an automatic alert. (Requirement 7.1.1)
- Monitor policy enforcement by alerting if any user violates these authentication policies. (Requirement 7.3)

Use Rapid7 Consulting Services to:

- Recommend best practices to optimize data security, including system access policies to limit access to system components and cardholder data to only those whose job role absolutely requires such access. (Requirements 7.1, 7.2)
- Evaluate and document access control policies and operational procedures, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirement 7.3)

Requirement 8 - Identify and authenticate access to system components

8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.
8.4	Document and communicate authentication policies and procedures 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, certificates, etc.), use of these mechanisms must be assigned to an individual account and not shared among multiple accounts, and physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted.
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.

Use Rapid7 InsightVM or Nexpose to:

- Audit system configuration settings for authentication controls, including number of login attempts, account lockout duration, password length, age and complexity, and other access control policies. (Requirements 8.1, 8.2)
- Verify that administrative credentials are not shared across multiple workstations or servers. (Requirement 8.5)

Use Rapid7 Metasploit Pro to:

- Use brute forcing, offline cracking, and pass-the-hash attacks to test for weak and shared passwords. (Requirements 8.2, 8.5)

Use Rapid7 AppSpider to:

- Dynamically scan web applications for vulnerabilities that allow unauthorized personnel access to a system or database without authentication. (Requirements 8.2, 8.7)

Use Rapid7 InsightIDR to:

- Alert if a user takes admin actions, whether on the endpoint, network, or across cloud services. All account modifications can be viewed in a single Administrator Activity view. (Requirement 8.1.2)
- Alert if any disabled Directory Services user attempts access to another account, including ActiveSync and cloud accounts such as Salesforce.com, Box.com, and Amazon Web Services. (Requirement 8.1.3)
- Define a network zone that a vendor should have access to and alert you if the credential is used outside of this zone. For example, if an account in the HVAC user group is used outside of the HVAC network zone, InsightIDR automatically alerts. InsightIDR also monitors VPN activity and detects unusual behavior, such as a vendor connecting from a different country. (Requirement 8.1.5)
- Alert on brute forcing and other password guessing attempts by running user behavior analytics on authentication logs and deception technology, such as honey users and honey credentials. (Requirement 8.1.6)
- Identify user account risk by highlighting accounts with non-expiring passwords, shared accounts, and administrators across local, domain, and cloud accounts. This actionable visibility exposes risk and improves security posture. (Requirements 8.2.4, 8.5)

Use Rapid7 Consulting Services to:

- Provide customizable security awareness training to users, including password security and policy training. (Requirement 8.4)

- Recommend best practices to optimize data security, including usage of multi-factor authentication for remote access to the network, secure dial-in service, terminal access controls with tokens, or VPNs with individual certificates. (Requirements 8.2, 8.3, 8.6, 8.7)
- Evaluate and document authentication control policies and operational procedures, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirement 8.8)

Requirement 9 - Restrict physical access to cardholder data

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 easily distinguish between on-site personnel and visitors.
9.3	Control physical access for on-site personnel to the sensitive areas.
9.4	Implement procedures to identify and authorize visitors.
9.5	Physically secure all media.
9.6	Maintain strict control over the internal or external distribution of any kind of media.
9.7	Maintain strict control over the storage and accessibility of media.
9.8	Destroy media 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.

Use Rapid7 Consulting Services to:

- Perform social engineering testing to verify the effectiveness of physical access controls, then present detailed findings and prioritized remediations. (Requirements 9.1, 9.3, and 9.5 to 9.9)
- Review existing policies, procedures, and tools in use for securing the physical access to cardholder data. Recommend best practices for physical access security measures to limit and monitor physical access to systems in the cardholder environment. (Requirements 9.2, 9.4, 9.10)
- Evaluate and document physical access controls, identify gaps in your security program, and determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirement 9.10)

Requirement 10 - Track and monitor all access to network resources and cardholder data

10.1	Implement audit trails to link all access to system components to each individual user.
10.2	Implement automated audit trails for all system components to reconstruct events.
10.3	Record at least the following audit trail entries for all system components.

10.4	Using time-synchronization technology, 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 (for example, online, archived, or restorable from backup).
10.8	Additional requirement for service providers: Implement a process for timely detection and reporting of failures of critical security control systems.
10.9	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.

Use Rapid7 InsightIDR to:

- Aggregate all authentication and network logs and directly correlate the activity to the users behind them. This provides full visibility on authentications to all systems. (Requirement 10.1)
- Securely centralize, search, and visualize all log data on the Insight platform. This provides a reliable audit trail as the logs can no longer be altered by the organization or an attacker, whether it be an external or insider threat. (Requirements 10.2, 10.3)
- Record a full audit trail for all authentications to all systems, viewable by user and by asset. The security team can search across all log files, including authentication logs, for easy incident investigation. (Requirement 10.2.1)
- Real-time visibility into administrators across local, domain, and cloud, as well as a history of administrative activity across the ecosystem. First time administrative actions are logged as notable behavior, and alerts are generated on anomalous admin activity. (Requirements 10.2.2, 10.2.5)
- Track all authentication attempts, both successful and invalid ones. These kinds of metrics can be easily reported on via pre-built PCI dashboard cards. (Requirements 10.2.4, 10.3.4)
- Scan endpoint systems and alert on log file deletion, a common attacker behavior to hide one's tracks. (Requirement 10.2.6)
- During incident investigations, the security team can bring together log search, real-time user activity, and system activity into a single timeline. This is a big step forward from parsing disparate log files, jumping between multiple solutions, and tedious retracing of user activity, including normalizing timestamps and building Excel timelines. (Requirement 10.3.3)
- Log where authentications came from, enabling incident responders to follow the trail through the network. (Requirement 10.3.5)
- Record the assets that users authenticated to, and alert on anomalous lateral movement. (Requirement 10.3.6)
- Synchronize timestamps across disparate log sources for a trustworthy string of events. (Requirement 10.4)
- Provide log management through direct integrations with event sources or integrating with an existing SIEM solution. The logs are securely sent to the Rapid7 Insight Platform and are available

for search and custom compliance cards. InsightIDR is only accessible using unique credentials provided to each member of the security team, and it is separate from the organization's security systems. (Requirements 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.7)

- Store all logs for at least one year and keep them immediately searchable for a minimum of ninety days. (Requirement 10.7)
- Consume all logs, create user behavior baselines, and alert on anomalies and malicious behavior. (Requirement 10.6)
- Get real-time visibility into all logs and alerts about suspicious access to critical systems that deviate from baseline behavior. Accounts, assets, and network zones that are defined as critical in the risk management strategy can be configured in InsightIDR to detect policy violations. (Requirement 10.6.2)

Use Rapid7 InsightOps to:

- Collect logs from any source, in any format, including servers, applications, Active Directory, databases, firewalls, DNS, VPNs, AWS, and other cloud services. (Requirements 10.1 and 10.2)
- Secure log centralization from any source, in any format. (Requirement 10.5)
- Generate ad hoc and custom reports to share with your team or auditors, and schedule recurring reports that are automatically saved to your reports archive for compliance. (Requirement 10.7)
- Receive immediate alerts when server, application, or service performance is impacted and regularly review performance using live dashboards and scheduled reports. (Requirements 10.6 and 10.8)

Use Rapid7 Consulting Services to:

- Recommend best practices to optimize their incident detection and response program, including auditing processes, logging and threat detection technologies, and an incident response plan (Requirements 10.3 to 10.4, 10.6, 10.8)
- Get a fully managed service for continuous threat detection to identify suspicious activity or anomalous behavior in real-time, then investigate and remediate incidents. (Requirement 10.6)
- Evaluate and document network monitoring policies and operational procedures, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirement 10.9)

Requirement 11 - Regularly test security systems and processes

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 on a quarterly basis.
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, and product upgrades).
11.2.1	Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved. Scans must be performed by qualified personnel.

11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the PCI Security Standards Council. Perform rescans as needed, until passing scans are achieved.
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.
11.3	Implement a methodology for penetration testing.
11.3.1/2	Perform external/internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification.
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; 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.

Use Rapid7 InsightVM or Nexpose to:

- Automatically scan the network for all wireless access points. (Requirement 11.1)
- Perform regular internal vulnerability scans, detect and scan new devices as they enter the network, and prioritize vulnerabilities based on threat exposure and asset criticality. Create, assign, and track remediation tasks, then verify that critical vulnerabilities have been remediated. (Requirement 11.2)

Use Rapid7 Metasploit to:

- Perform internal and external penetration tests either in preparation for the official security assessment or for the audit itself. (Requirement 11.3)
- Automatically test the effectiveness of network segmentation controls. (Requirement 11.3.4)

Use Rapid7 AppSpider to:

- Automatically simulate web application attacks to test for application-layer vulnerabilities in accordance with PCI DSS Requirement 6.5. (Requirement 11.3)

Use Rapid7 InsightIDR to:

- Identify malicious behavior earlier in the attack chain, the steps required to breach a company. Through a combination of user behavior analytics and deception technology, InsightIDR detects the top attack vectors behind breaches, including phishing, compromised credentials, and malware. (Requirement 11.4)

Use Rapid7 Consulting Services to:

- Perform Wireless Security Audits to test identify security best practices to prevent unauthorized use of your Wireless LAN (802.11). Conduct penetration testing and perform wireless reconnaissance to locate rogue unsecured access points. (Requirement 11.1)
- Get a fully managed vulnerability management service to perform quarterly internal network vulnerability scans, with concise reporting and remediation guidance. (Requirement 11.2)
- Perform quarterly external network vulnerability scans. Rapid7 is a certified Approved Scanning Vendor (ASV) by the PCI Security Standards Council and can perform quarterly external vulnerability scans and produce certified documentation to satisfy this requirement. (Requirement 11.2.2)
- Develop a penetration testing methodology based on industry-accepted approaches, and perform internal and external penetrations tests. (Requirement 11.3)
- Evaluate and document security assessment policies and operational procedures, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies. (Requirement 11.6)

Requirement 12 - Maintain a policy that addresses information security for all personnel

12.1	Establish, publish, maintain, and disseminate a security policy.
12.2	Implement a risk-assessment process.
12.3	Develop usage policies for critical technologies and define 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 to an individual or team information security management responsibilities.
12.6	Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)
12.8	Maintain and implement policies and procedures to managed service providers with whom cardholder data is shared, or that could affect the security of cardholder data.
12.9	Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.

Use Rapid7 Metasploit to:

- Simulate phishing campaigns to measure effectiveness of a security awareness program. (Requirement 12.6)

Use Rapid7 InsightIDR to:

- Track each device and its associated users, automatically identifying primary users for each asset. Through integration with Active Directory, InsightIDR provides information about each user for easy contact by the security team. (Requirement 12.3.4)
- Visibility into external vendor authentications onto VPN, including authentication times and assets involved. InsightIDR also monitors disabled and service accounts and automatically alerts on anomalous behavior. (Requirement 12.3.9, 12.5.4)
- Real-time detection of top attack vectors behind breaches. Log file data, real-time user activity, and endpoint artifacts can be brought together on a single visual timeline, accelerating incident investigations. (Requirement 12.5.2)
- Aggregate, search, and attribute logs and alerts from Intrusion Detection/Prevention Systems (IDS/IPS) and firewalls to the users and assets behind them. For example, with one search, the security team can identify the users generating the most IDS/IPS alerts. (Requirement 12.10.5)

Use Rapid7 Consulting Services to:

- Assist in writing the documentation to meet annual PCI DSS requirements, such as the applicable Self-Assessment Questionnaire (SAQ), and formal security policy documentation. (Requirement 12.1)
- Perform a formal risk assessment to identify critical threats and vulnerabilities. (Requirement 12.2)
- Provide a customizable security awareness training program for all personnel on the importance of securing cardholder data. (Requirement 12.6)
- Evaluate and document security policies and operational procedures associated with these requirements. (Requirements 12.3, 12.4 , 12.8)
- Build an incident response plan and simulate breach scenarios to increase readiness. (Requirement 12.10)

ABOUT RAPID7

With Rapid7 (NASDAQ: RPD), security and IT professionals gain the clarity and confidence they need to protect against risk and drive innovation Rapid7 analytics transform data into answers, eliminating blind spots and giving customers the insight they need to securely develop and operate today's sophisticated IT infrastructures, networks, and applications, Rapid7 solutions include vulnerability management, penetration testing, application security, incident detection and response, SIEM and log management, and offers managed and consulting services across its portfolio. To learn more about Rapid7 or get involved in our threat research, www.rapid7.com.