ManageEngine

ManageEngine's guide for PCI DSS compliance

Table of contents

Disclaimer

What is PCI DSS v4?

PCI DSS stands for Payment Card Industry Data Security Standard. It is a set of processes and practices designed to ensure the safe and secure transfer of payment card data. It is a global standard developed by major credit banks to ensure the security of credit card holder data.

This standard applies to all organizations that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD), or could impact the security of the cardholder data environment (CDE), which includes businesses that collect sensitive data to authenticate cardholders or authorize payment transactions.

Complying with PCI DSS is not a one time event. Organizations are expected to comply with the latest version of the standard, and will need to regularly review and update their organizational processes and operations to ensure continued compliance.

The latest version of PCI DSS version 4, was released in March 2022. PCI DSS v3.2.1 is valid through March 31, 2024, after which version 4 will supersede it.

The PCI DSS v4 structure

To be PCI DSS compliant, an organization needs to meet several operational and technical security requirements that applies to the CDE. The people, processes, and systems that interact with, or could impact the payment card information, make up the CDE.

PCI DSS 4.0, the latest version of PCI DSS, consists of 12 requirements spread across six main objectives. These requirements aim to help organizations maintain a secure cardholder data environment and, in turn, prevent cardholder data theft. Organizations are expected to comply with these 12 requirements in order to ensure compliance with the standard.

Objectives	Requirements
Build and maintain a secure network and systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components
Protect account data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a vulnerability management program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement strong access control measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Log and monitor all access to system, components and cardholder data 11. Test security of systems and networks regularly
Maintain an information security policy	12. Support information security with organizational policies and programs

How can ManageEngine help you comply with the PCI DSS v4 requirements?

ManageEngine's suite of IT management solutions will help you meet the technical requirements for PCI DSS and, in turn, support compliance with this standard.

Requirement 1

Install and maintain network security controls

Monitor and control network traffic to and from the cardholder environment with the help of network security controls (NSCs), such as firewalls and other network security technologies.

01

Requirement sections:

1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.

1.2 NSCs are configured and maintained.

1.3 Network access to and from the cardholder data environment is restricted.

1.4 Network connections between trusted and untrusted networks are controlled.

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
1.1	Ensure processes and mechanisms for installing and maintaining network security controls are defined and understood.	**Firewall Analyzer:** Gain real-time visibility into network security controls and analyze firewall logs to ensure that security policies are being enforced effectively. This solution also provides automated compliance reporting capabilities that help demonstrate adherence to regulatory requirements mentioned in the PCI DSS. **OpManager:** Identify and mitigate security threats in real time with the help of the extensive network monitoring capabilities provided in this network management solution. Its security module delivers visibility into network vulnerabilities, unauthorized access attempts, and policy violations, which help define and maintain network security controls. **Patch Manager Plus:** Automate the patch management process and ensure security patches are installed promptly across all endpoints in the network. The solution also provides detailed reports on patch compliance which helps demonstrate adherence to the PCI DSS requirements related to maintaining security controls. **Log360:** Detect and respond to security incidents with the help of this SIEM solution. It provides log monitoring, real-time alerting and reporting capabilities that help define and maintain network security controls.
1.2.1	Confirm configuration standards for NSC rulesets are defined, implemented and maintained.	**Firewall Analyzer:** Gain comprehensive visibility into firewall rules and policies to help maintain configuration standards for NSC rulesets. This solution also provides automated compliance reporting capabilities that demonstrate adherence to PCI DSS requirements related to NSC ruleset configurations. **OpManager:** Monitor NSC rulesets in real time to identify and respond to policy violations promptly. This network management solution also provides reporting capabilities that can help demonstrate compliance with PCI DSS v4 requirements related to NSC ruleset configuration. **NetFlow Analyzer:** Gain proper visibility into network traffic flows to identify and manage NSC rulesets more effectively. The solution also delivers reporting capabilities that help demonstrate adherence to PCI DSS v4 requirements related to NSC ruleset configuration. **EventLog Analyzer:** Identify and respond to NSC ruleset violations promptly using advanced analytics and reporting capabilities provided by this log management and SIEM solution. This solution also provides real-time alerting and automated compliance reporting which demonstrates adherence to PCI DSS v4 requirements related to NSC ruleset configuration.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
1.2.2	Verify that all changes to network connections and configurations of NSCs are approved and managed in accordance with the change control process (defined in Requirement 6.5.1.).	**Firewall Analyzer:** Gain real-time visibility into firewall rules and policies, which, in turn, helps identify changes to network connections and NSC configurations. The solution also provides automated change management capabilities that help ensure that all changes are approved and managed in accordance with PCI DSS v4 requirements. **OpManager:** Monitor NSC configurations in real time to identify unauthorized changes promptly. This solution also provides change management capabilities that help ensure that changes to network connections and NSCs are approved and managed in accordance with PCI DSS v4 requirements. **ServiceDesk Plus:** Manage changes to network connections and NSC configurations more effectively with the help of the change management capabilities provided by this IT service management solution. It also provides approval workflow, change tracking, and audit capabilities that help ensure compliance with PCI DSS v4 requirements. **Endpoint Central:** Ensure that all changes to endpoints are approved and managed in accordance with PCI DSS v4 requirements with the help of the patch management and configuration management capabilities provided by this endpoint management solution. It also provides approval workflow, change tracking, and reporting capabilities that help demonstrate compliance with this requirement.
1.2.3	Establish that an accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	**OpManager:** Create an accurate network diagram that shows all connections between the CDE and other networks with the help of network discovery and mapping capabilities provided by this network management solution. Real-time monitoring of network devices and interfaces is also provided to help organizations ensure that the diagram remains accurate over time. **Network Configuration Manager:** Maintain an accurate network diagram with the help of the configuration and change management capabilities provided by this network configuration management solution. It also provides automated backup and comparison of device configurations to help organizations ensure that the diagram reflects the current state of the network. **Applications Manager:** Identify and map all applications and services that are connected to the CDE with the help of the discovery and dependency mapping capabilities provided by this application performance monitoring solution. Also, real-time monitoring and alerting, that helps organizations ensure that any changes to the network are reflected in the diagram, are provided.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
1.2.4	**Ensure an accurate dataflow diagram(s) is maintained that:** • Shows all account data flows across systems and networks. • Is updated as needed upon changes to the environment.	**Firewall Analyzer:** Identify all account data flows across systems and networks with the help of the log analysis and reporting capabilities provided by this solution. It also provides detailed reports on network traffic, including the source and destination of data flows, to help organizations create an accurate data-flow diagram. **OpManager:** Create a data-flow diagram that shows all account data flows across systems and networks with the help of the network discovery and mapping capabilities provided by this network management solution. Real-time monitoring of network devices and interfaces, to help organizations ensure that the diagram remains accurate over time, is also provided. **Applications Manager:** Identify all applications and services that process account data using the discovery and dependency mapping capabilities provided by this application performance monitoring solution. It also provides real-time monitoring and alerting, to help organizations ensure that any changes to the data-flow are reflected in the diagram promptly.
1.2.5	Confirm all services, protocols and ports allowed are identified, approved, and have a defined business need.	**Firewall Analyzer:** Identify all services, protocols, and ports allowed across the network with the help of the log analysis and reporting capabilities provided by this solution. To help organizations identify any unauthorized services, protocols, or ports, a detailed reported on network traffic is also provided, which includes the source and destination of data flows. **OpManager:** Identify all network services and ports in use with the help of the network discovery and mapping capabilities provided by this network management solution. It also provides real-time monitoring of network devices and interfaces, helping organizations ensure that only authorized services and ports are in use. **Vulnerability Manager Plus:** Identify unauthorized services, protocols, or ports with the help of the vulnerability scanning and assessment capabilities provided by this vulnerability management solution. Remediation guidance and reporting that helps organizations ensure that only authorized services, protocols, and ports are in use, is also provided. **Log360:** Identify unauthorized services, protocols, or ports with the help of the log analysis and correlation capabilities provided by this security information and event management (SIEM) solution. It provides real-time alerts and reports on security events across the network, helping organizations detect and respond to any security incidents promptly.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
1.2.6	Verify that security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, so that the risk is mitigated.	**Firewall Analyzer:** Define and implement security features for all services, protocols, and ports in use with the help of the firewall policy management capabilities provided by this solution. It also provides recommendations on firewall rule changes to reduce the attack surface and enforce compliance with industry standards, including PCI DSS. **Patch Manager Plus:** Mitigate security risks associated with insecure services, protocols, and ports with the help of the patch deployment capabilities provided by this patch management solution. To help organizations ensure that all security patches are up to date, real-time visibility into the patch status of network devices and software is also provided. **Endpoint Central:** Mitigate security risks associated with insecure services, protocols, and ports with the help of the endpoint protection capabilities provided by this endpoint management solution. It also provides antivirus, firewall, and intrusion prevention capabilities, to help organizations protect their endpoints against cyberthreats. **Log360:** Detect and respond to security incidents associated with insecure services, protocols, and ports with the help of the log analysis and correlation capabilities provided by this unified log management and SIEM solution. Real-time alerts and reports on security events, which help organizations monitor and manage their network security posture, is also provided.
1.2.7	Establish that configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	**Firewall Analyzer:** Monitor firewall configurations continuously with the help of this solution to ensure its effectiveness in protecting the network. The solution also generates reports and alerts when firewall policies are changed, to help organizations identify any deviations from security policies and standards. **EventLog Analyzer:** Detect and respond to security incidents with the help of the real-time event log analysis provided by this solution. It also monitors configuration changes and provide alerts when NSCs are modified, making it easier for organizations to track and verify that their NSCs are relevant and effective. **Log360:** Detect and respond to security incidents by monitoring and analysis network logs in real time using this unified log management and SIEM solution. It also generates reports and alerts for configuration changes, making it easier for organizations to monitor and verify the effectiveness and relevance of their NSCs.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
1.2.8	Ensure configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	**Firewall Analyzer:** Ensure NSC configurations are consistent with active network configurations with the help of real-time firewall configuration change management capabilities provided by this solution. It also provides a centralized repository to manage and track firewall configuration files, to make it easier for organizations to ensure they are secured from unauthorized access. **EventLog Analyzer:** Detect and respond to security incidents with the help of the real-time event log analysis capability provided by this solution. It also monitors configuration changes and provide alerts when NSC configurations are modified, to make easier for organizations to track and verify that the configurations are consistent with active network configurations. **Network Configuration Manager:** Manage network configurations and ensure they are consistent with the NSC configurations with the help of the centralized repository provided by this solution. It also automates configuration backups and provide alerts for configuration changes, making it easier for organizations to keep their NSC configurations up to date and secured from unauthorized access.
1.3.1	Confirm that inbound traffic to the CDE is restricted: • To only traffic that is necessary. • All other traffic is specifically denied.	**Firewall Analyzer:** Ensure real-time monitoring and management of inbound traffic to the CDE. This solution is used to configure firewall rules that restrict inbound traffic to only necessary traffic and deny all other traffic. The solution provides a centralized dashboard to monitor and manage firewall rules, making it easier for organizations to ensure that their inbound traffic is restricted appropriately. **EventLog Analyzer:** Detect and respond to security incidents with the help of real-time event log analysis capability provided by this solution. It can be used to monitor inbound traffic to the CDE and provide alert when unauthorized traffic is detected, and also provide analysis of the inbound traffic patterns to help identify potential security risks. **Network Configuration Manager:** Manage network configurations and ensure that inbound traffic is restricted appropriately with the help of the centralized network configuration management repository provided by this solution. It can be used to configure network devices, such as routers and switches to restrict inbound traffic, to only necessary traffic and deny all other traffic. The solution also provides a dashboard to monitor and manage network configurations, making it easier for organizations to ensure that their inbound traffic is restricted appropriately.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
1.3.2	Verify that outbound traffic from the CDE is restricted: • To only traffic that is necessary. • All other traffic is specifically denied.	**Firewall Analyzer:** Ensure real-time firewall monitoring and analysis, including traffic flows and rule usage. Organizations can use this solution to identify all outbound traffic from the CDE and create firewall rules to allow only necessary traffic. **OpManager:** Guarantee network performance monitoring and traffic analysis. Organizations can use this solution to monitor outbound traffic from the CDE and identify any unusual traffic patterns or unauthorized connections. **Network Configuration Manager:** Ensure configuration management and automation for network devices, including firewalls. Organizations can use this solution to enforce firewall policies and ensure that only necessary outbound traffic is allowed.
1.3.3	Ensure NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, are: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	**Firewall Analyzer:** Monitor and analyze network traffic across NSCs and wireless networks, ensuring that only authorized traffic is allowed into the CDE. **Access Manager Plus:** Control access to the CDE by implementing role-based access controls, multi-factor authentication, and other security features.
1.4.1	Confirm that NSCs are implemented between trusted and untrusted networks.	**Firewall Analyzer:** Identify trusted and untrusted networks, and enforce firewall policies that segment these networks. The solution also generates reports that demonstrate compliance with PCI DSS requirements. **OpManager:** Monitor network traffic and identify devices that might require NSCs. The solution also helps enforce NSC policies and generates reports for compliance purposes. **Access Manager Plus:** Control access to the CDE by enforcing strict access controls and implementing network segmentation controls. The solution also helps enforce MFA for users accessing the CDE.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
1.4.2	**Verify that inbound traffic from untrusted networks to trusted networks is restricted to:** • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.	**Firewall Analyzer:** Identify authorized system components and enforce firewall policies that restrict inbound traffic to those components. The solution also monitors traffic and generates alerts when unauthorized traffic is detected. **OpManager:** Monitor network traffic and identify unauthorized traffic. This solution also helps enforce policies to restrict inbound traffic from untrusted networks. **Access Manager Plus:** Control access to system components that are authorized to provide publicly accessible services, protocols, and ports. The solution also helps enforce policies to restrict inbound traffic from untrusted networks.
1.4.3	Establish that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	**Firewall Analyzer:** Identify and block traffic with forged source IP addresses. This solution also generates alerts and reports to help identify and investigate potential spoofing attacks. **OpManager:** Monitor network traffic and identify potential spoofing attacks. The solution also helps enforce policies to block traffic from known spoofed sources. **EventLog Analyzer:** Detect and respond to spoofing attacks by analyzing network logs and identifying suspicious activity. This solution also helps generate alerts and reports to help investigate potential attacks.
1.4.4	Ensure that the system components that store cardholder data are not directly accessible from untrusted networks.	**Firewall Analyzer:** Identify system components that store cardholder data, and enforce firewall policies that restrict access to these components from untrusted networks. **OpManager:** Monitor network traffic and identify potential access to system components that store cardholder data from untrusted networks. The solution also helps enforce policies to restrict access to these components. **Access Manager Plus:** Control access to system components that store cardholder data, and ensure that they are not directly accessible from untrusted networks.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
1.4.5	Confirm that the disclosure of internal IP addresses and routing information is limited to only authorized parties.	**Firewall Analyzer:** Monitor and control access to internal IP addresses and routing information. The solution also generates alerts and reports to help identify potential unauthorized access to this information. **OpManager:** Monitor and control access to internal IP addresses and routing information. This solution also helps enforce policies to restrict access to this information. **Access Manager Plus:** Control access to internal IP addresses and routing information, and ensure that only authorized parties have access to this information.
1.5.1	**Verify that security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the internet) and the CDE as:** • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	**Endpoint Central:** Define and enforce security policies on desktops and laptops that connect to both untrusted networks and the CDE. The solution also ensures that security controls are actively running on all computing devices and prevents users from altering security controls without management authorization. **Mobile Device Manager Plus:** Enforce security controls on both company- and employee-owned devices that connect to both untrusted networks and the CDE. This solution also defines specific configuration settings to prevent threats from being introduced into the entity's network.

Requirement 2

Apply secure configurations to all system components

Ensure you reduce your attack surface by applying and maintaining secure configurations for all systems and components. Prevent the use of default passwords and settings to thwart attackers from using them to gain access to employee or customer records.

02

Requirement sections:

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.

2.2 System components are configured and managed securely.

2.3 Wireless environments are configured and managed securely.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
2.1.1	**Ensure all security policies and operational procedures that are identified in Requirement 2 are:** • Documented. • Kept up to date. • In use. • Known to all affected parties.	**ADManager Plus:** Manage and document security policies and operational procedures related to Active Directory (AD). The solution also provides detailed reports on policy changes and user activities related to AD. **ServiceDesk Plus:** Manage and document security policies and operational procedures related to IT service management. This solution also helps automate policy enforcement and track policy violations. **ADAudit Plus:** Monitor and report on changes made to security policies and operational procedures related to AD. The solution also generates alerts and notifications for policy violations and unauthorized access attempts.
2.2.1	**Confirm that configuration standards are developed, implemented, and maintained to:** • Cover all system components. Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	**Patch Manager Plus:** Ensure that all system components are up to date with the latest security patches, which is a critical aspect of maintaining secure configuration standards. **Vulnerability Manager Plus:** Scan for known security vulnerabilities across all system components and track their remediation. This solution also provides industry-accepted system hardening standards and vendor hardening recommendations to ensure that configuration standards are consistent with best practices. **Endpoint Central:** Enforce configuration standards on endpoints by setting and verifying compliance policies. The solution also automates the deployment of updates and patches, making it easier to keep systems up to date with the latest security standards.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
2.2.3	**Verify that primary functions requiring different security levels are managed as:** • Only one primary function exists on a system component, or • Primary functions with differing security levels that exist on the same system component are isolated from each other, or • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	**Access Manager Plus:** Manage access controls and permissions for different primary functions on a system component. This solution enables administrators to set up role-based access controls (RBAC) and segregation of duties (SoD) policies, which helps ensure that different functions are isolated from each other. **Firewall Analyzer:** Monitor network traffic and identify any attempts to access primary functions with differing security levels on the same system component. The solution also helps enforce network segmentation and access controls to ensure that different functions are isolated from each other. **Password Manager Pro:** Manage privileged accounts and ensure that only authorized users have access to primary functions with differing security levels. This solution also enforces password policies and two-factor authentication (2FA) to ensure that access controls are strong enough to protect sensitive data.
2.2.4	Ensure only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	**Firewall Analyzer:** Ensure that only necessary services, protocols, daemons, and functions are enabled on firewall devices. The solution provides reports on the services and ports that are open on the firewall and alert administrators when any new services or ports are added. **EventLog Analyzer:** Monitor servers, workstations, and network devices for any suspicious activity related to enabled services, protocols, daemons, and functions. This solution delivers real-time alerts and notifications on any unauthorized changes made to these settings. **Endpoint Central:** Enforce policies related to enabled services, protocols, daemons, and functions on endpoints. The solution provides capabilities to remotely disable or remove any unnecessary or unauthorized software, services, or protocols from the endpoints. **Patch Manager Plus:** Keep systems up to date with the latest security patches for known vulnerabilities in enabled services, protocols, daemons, and functions. This solution delivers reports on the patch status of the systems and automates the deployment of patches to ensure that all systems are secured. **Access Manager Plus:** Ensure that only authorized users have access to enabled services, protocols, daemons, and functions on network devices. The solution provides granular access controls and real-time alerts on any unauthorized access attempts.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
2.2.5	**If any insecure services, protocols, or daemons are present, then:** • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	**Vulnerability Manager Plus:** Identify insecure services, protocols, and daemons that are running on the network. **Log360:** Collect and analyze logs from different sources to identify any insecure services, protocols, or daemons being used. **Firewall Analyzer:** Manage firewall rules and block any insecure services, protocols, or daemons. **Endpoint Central:** Manage the configuration of devices on the network and ensure that any insecure services, protocols, or daemons are removed or disabled. **Patch Manager Plus:** Identify and apply patches to devices in the network to fix any vulnerabilities associated with insecure services, protocols, or daemons.
2.2.6	Establish system security parameters that are configured to prevent misuse.	**ADAudit Plus:** Configure password policies and track password policy changes. This solution also monitors and provides alerts on any changes to security settings, such as changes to password policies or lockout settings. **EventLog Analyzer:** Monitor and track user activity, including failed logins and account lockouts. The solution monitors and delivers alerts on any changes to security settings, such as changes to password policies or lockout settings. **Endpoint Central:** Enforce password policies on endpoints, including password complexity and expiration settings. This solution helps organizations implement security settings, such as screen lock timeout values and automatic logout settings. **Patch Manager Plus:** Keep systems up to date with the latest security patches and updates, which helps prevent security misconfigurations and vulnerabilities.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
2.2.7	Confirm that all non-console administrative access is encrypted using strong cryptography.	**Password Manager Pro:** Gain access to a secure, centralized repository for storing and managing privileged account passwords, along with robust access controls and audit trails. The solution supports encryption of all communication between the client and the server using SSL/TLS, ensuring that all non-console administrative access is encrypted. **OpManager:** Gain real-time visibility into network performance and security. This solution supports encryption of all communication between the client and server using SSL/TLS, ensuring that all non-console administrative access is encrypted. **Firewall Analyzer:** Monitor and analyze firewall logs, providing insights into network traffic and security threats. The solution supports encryption of all communication between the client and server using SSL/TLS, ensuring that all non-console administrative access is encrypted.

Requirement 3

Protect stored account data

Don’t store card holder data unless it is necessary for your business operations. If you are storing data, ensure that you use necessary protection methods such as encryption, truncation, masking, and hashing of account data. Also make sure that all cryptographic keys and encryption tools are documented, recorded, and protected.

Requirement sections:

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

3.2 Storage of account data is kept to a minimum.

3.3 Sensitive authentication data (SAD) is not stored after authorization.

3.4 Access to displays of full primary account number (PAN) and ability to copy cardholder data are restricted.

3.5 PAN is secured wherever it is stored.

3.6 Cryptographic keys used to protect stored acount data are secured.

3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key life cycle are defined and implemented.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
3.1.1	**Ensure all security policies and operational procedures that are identified in Requirement 3 are:** • Documented. • Kept up to date. • In use. • Known to all affected parties.	**ServiceDesk Plus:** Create, manage, and share documents related to security policies and operational procedures. The solution enables you to create and manage documents in a central repository, set up document review and approval workflows, and automate document distribution to all affected parties. **ADAudit Plus:** Monitor and audit all changes made to security policies and operational procedures. This solution provides real-time alerts and notifications whenever a change is made, enabling you to take immediate action to address any issues. **EventLog Analyzer:** Generate reports and audit trails related to security policies and operational procedures. The solution delivers detailed reports on policy compliance, policy violations, and user activity, enabling you to identify and address any issues quickly.
3.2.1 (3.2.1.a , 3.2.1.b, 3.2.1.c)	Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement. Investigate files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy. Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.	**DataSecurity Plus:** Identify sensitive data and implement data retention policies based on compliance requirements. This solution also monitor data access and track data modifications to ensure data integrity. **ADAudit Plus:** Track file and folder access, user activity, and system logs to identify any unauthorized access or modification of data. The solution also generates reports on data retention policies and data disposal processes. **Log360:** Monitor log files from various sources and identify any suspicious activity related to data retention and disposal. This solution also generates reports on data retention policies and disposal processes. **EventLog Analyzer:** Monitor event logs from various sources to identify any unauthorized access or modification of data. The solution also generates reports on data retention policies and data disposal processes.
3.3.1	Ensure that SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	**Password Manager Pro:** Securely manage and store all sensitive authentication data, such as passwords, digital certificates, and SSH keys. The solution also provides a secure password vault, where sensitive information is securely stored and shared among authorized personnel. The system can be configured to remove SAD upon completion of the authorization process automatically.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
		Key Manager Plus: Manage and store digital keys and certificates securely.This solution tracks the entire life cycle of keys and certificates, including generation, renewal, revocation, and archival. This solution can be configured to automatically remove SAD upon completion of the authorization process. **EventLog Analyzer:** Collect, analyze, and store log data from various sources, including servers, applications, and network devices. The system can be configured to automatically remove SAD from log data upon completion of the authorization process. Additionally, the solution has built-in alerting and reporting capabilities that help organizations to identify and respond to security threats quickly.
3.3.1.2	Confirm that the card verification code is not retained upon completion of the authorization process.	**EventLog Analyzer:** Track the card verification code by monitoring and alerting on access to files containing cardholder data, as well as detecting and alerting on any attempts to access the code. **ADManager Plus:** Enforce secure password policies and automate the process of resetting passwords. This solution reduces the risk of the card verification code being retained by users or applications. **Password Manager Pro:** Store and manage passwords and other sensitive data securely, and ensure that the card verification code is not retained after completion of the authorization process. **DataSecurity Plus:** Identify and protect sensitive data by providing real-time alerts on unauthorized access to cardholder data, and monitoring and reporting on file access activity.
3.3.1.3	Verify that the personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	**Password Manager Pro:** Manage passwords and PINs securely by providing an encrypted vault to store sensitive information. The solution enables you to enforce password policies, track usage, and audit access to the stored information. **Key Manager Plus:** Manage cryptographic keys and certificates securely. This solution provides a centralized console to manage keys and certificates, automate key rotation, and track usage. **EventLog Analyzer:** Detect and respond to unauthorized access attempts by monitoring system logs. The solution alerts you in real-time when unauthorized access attempts are detected, and provide forensic analysis tools to investigate security incidents. **Firewall Analyzer:** Enforce network security policies and prevent unauthorized access to systems. This solution provides detailed reports on firewall activity and traffic patterns, enabling you to identify and block unauthorized traffic.

Requirement 4

Protect cardholder data with strong cryptography during transmission over open, public networks

Prevent compromise of cardholder data during transmission over misconfigured wireless networks by encrypting the data before it is transmitted, encrypting the session over which the data is transmitted, or both. Use strong cryptography to ensure greater assurance in preserving cardholder data.

Requirement sections:

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.

4.2 PAN is protected with strong cryptography during transmission.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
4.1.1	Ensure all security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**ADAudit Plus:** Document policy violations and changes to critical systems and applications with the help of real-time alerts. This solution also helps generate audit reports necessary for this PCI DSS requirement. **Password Manager Pro:** Ensure that the security policies are up to date by enforcing strong password policies. An additional capability which helps in meeting this requirement is the centralized management of privileged passwords. **Access Manager Plus:** Ensure that security policies and procedures are in use by providing real-time monitoring and control of user access to critical systems and applications. **Log360:** Ensure that the security policies and procedures are known to all affected parties by providing real-time alerts and reports for security incidents and policy violations. The solution provides customizable dashboards and reports for compliance audits.
4.2.1	Confirm that strong cryptography and security protocols are implemented to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	**Key Manager Plus:** Secure the encryption keys used to protect PAN data during transmission with the help of centralized key management capabilities. This solution also helps organizations automate the generation, rotation, and revocation of encryption keys, and maintain a centralized repository of keys for easy management and auditing. **Firewall Analyzer:** Detect and prevent unauthorized access and data breaches with the help of real-time monitoring and network traffic analysis capabilities. The solution also helps organizations monitor network traffic for sensitive data such as PAN, and implement granular policies to prevent unauthorized access or transmission of this data over public networks. **OpManager:** Identify and address vulnerabilities in the network infrastructure that could expose sensitive data such as PAN to unauthorized access with this solution's network monitoring and management capabilities. This solution also monitors network devices and services for security issues, and provides alerts and reports to help administrators identify and address potential security threats quickly.
4.2.2	Verify that PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	**Exchange Reporter Plus:** Identify email messages that contain sensitive data such as PAN with the help of this solution's email traffic analysis and monitoring capabilities. The solution also provides encryption and decryption capabilities to secure sensitive data transmitted via email. **Endpoint Central:** Provide secure instant messaging capabilities for internal communication within an organization. The solution provides encryption and decryption capabilities to secure sensitive data transmitted via instant messaging. **ADManager Plus:** Deliver chat-based communication capabilities for IT administrators to communicate with each other. This solution also provides encryption and decryption capabilities to secure sensitive data transmitted via chat.

Requirement 5

Protect all systems and networks from malicious software

Use anti-malware solutions to protect your systems and networks from current and evolving malware threats. Make it a practice to keep your anti-virus software updated, conduct periodic scans for system vulnerabilities, and audit your logs so that you're able to keep a close watch for threats.

Requirement sections:

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

5.2 Malicious software (malware) is prevented, or detected and addressed.

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
5.1.1	**Ensure that all security policies and operational procedures that are identified in Requirement 5 are:** • Documented. • Kept up to date. • In use. • Known to all affected parties.	**ServiceDesk Plus:** Document and manage organizational IT policies and operational procedures. The solution provides a centralized platform for creating and maintaining documentation related to IT service management, including policies, procedures, and standard operating procedures (SOPs). **Endpoint Central:** Enforce security policies and operational procedures. This solution enables centralized configuration management, patch management, and software deployment, which are essential for ensuring that systems are configured in accordance with policies and procedures. **ADSelfService Plus:** Provides self-service password reset and account unlock capabilities. While not directly addressing documentation, it supports the "awareness" aspect of Requirement 5.1.1 by empowering users to manage their account credentials effectively. Additionally, organizations utilize ManageEngine solutions to send automated reminders or notifications regarding policy updates to affected parties
5.2.1	Establish an anti-malware solution(s) that is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	**Endpoint Central:** Deploy anti-malware software on all system components and configure policies to ensure that they are regularly updated and managed. The solution also provides a comprehensive endpoint management solution that includes anti-malware capabilities. **Endpoint DLP Plus:** Provide multi-layered endpoint protection that includes anti-malware capabilities, as well as features such as intrusion detection and prevention, firewall, and device control. This solution also delivers real-time threat detection and remediation capabilities to ensure that endpoints are protected against malware threats. **Patch Manager Plus:** Ensure that all software and operating systems are up to date with the latest security patches using the automated patch management capability. This helps prevent vulnerabilities that can be exploited by malware. **Log360:** Monitor and detect suspicious activities on endpoints and network devices with the help of log management and analysis capabilities. The solution alerts administrators of malware activity, enabling them to respond quickly and prevent further infection. **EventLog Analyzer:** Provide real-time security event monitoring, correlation, and threat intelligence capabilities which enables administrators to detect and respond to malware threats in real time, thereby minimizing the risk of a successful attack.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
5.2.2	Confirm that the deployed anti-malware solution(s): Detects all known types of malware. Removes, blocks, or contains all known types of malware.	**Endpoint Central:** Detect and remove malware from endpoints with the help of endpoint management capabilities and the anti-malware module provided in the solution. This also provides real-time protection against malware threats, and can be configured to automatically quarantine or delete infected files. **Patch Manager Plus:** Provide automated patch management capabilities for Windows, macOS, and Linux systems. In addition to patching vulnerabilities, the solution can also be configured to scan for malware and remove it from endpoints. **Firewall Analyzer:** Detect and block malware traffic with the help of this solution's firewall log analysis capabilities. This solution also includes a malware detection engine that identifies malware signatures and alerts administrators when malware is detected. **EventLog Analyzer:** Detect malware activity in endpoints and servers with the help of this solution's log management and analysis capabilities. It can also be configured to alert administrators when malware is detected and to automatically quarantine infected systems.
5.2.3.1	Verify that the frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**Vulnerability Manager Plus:** Perform targeted risk analysis by scanning the network and identifying vulnerabilities in the system components. The solution also generates a risk score and suggests remediation actions. **Log360:** Monitor the logs of system components and detect anomalies that could indicate a malware attack. This solution also provides real-time alerts and automated responses to contain the threat. **Endpoint Central:** Manage the security of endpoints by enforcing security policies, deploy patches, and control access to sensitive data. The solution also delivers reports on the security posture of the endpoints which can be used for risk analysis.
5.3.1	Ensure that the anti-malware solution(s) is kept current via automatic updates.	**Endpoint Central:** Ensure centralized patch management for endpoints, including anti-malware updates. This solution supports automatic updates for anti-malware solutions and enables administrators to configure patch deployment schedules.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
		Patch Manager Plus: Provides automated patch management for Windows, macOS, and Linux systems. The solution supports the deployment of third-party patches, including anti-malware updates. **Vulnerability Manager Plus:** Scan endpoints for vulnerabilities, including missing patches and outdated anti-malware solutions. This solution automates patch management and provides reports on patch status and compliance. **Endpoint DLP Plus:** Ensure endpoint protection, including anti-malware, firewall, and intrusion prevention capabilities. The solution includes automatic updates for the anti-malware solution(s) and
5.3.2.1	If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1	**Endpoint Central:** Provide automated malware scanning for Windows systems. The frequency of scans can be configured through policies and can be customized to meet the organization's needs. **Vulnerability Manager Plus:** Identify vulnerabilities in the organization's systems and prioritize them based on their risk level. This information is used for targeted risk analysis and determine the frequency of malware scans. **Patch Manager Plus:** Keep the organization's systems up to date with the latest security patches, which helps prevent malware infections. This solution automates the scanning of systems to detect missing patches and deploy them as needed.
5.3.3	For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, or • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	**Endpoint Central:** Manage and secure endpoints, including those that may be used to access removable electronic media. It includes an anti-malware solution that performs automatic scans of connected devices and also accomplishes continuous behavioral analysis of endpoints to detect and block malware in real time. **Patch Manager Plus:** Keep endpoints current with the latest security patches and updates, which helps prevent malware infections. The solution includes automated patch deployment and vulnerability scanning capabilities to help identify and remediate potential vulnerabilities that could be exploited by malware.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
5.3.4	Confirm that the audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	**Log360:** Provides real-time log management and SIEM capabilities, allowing organizations to collect, analyze, and archive logs from various sources, including anti-malware solutions. It also generates alerts based on predefined rules and thresholds, making it easier to identify and respond to potential security incidents. **EventLog Analyzer:** This solution provides log management, SIEM, and file integrity monitoring capabilities. It helps organizations meet the audit logging requirements of PCI DSS by collecting logs from anti-malware solutions and other sources, correlating events to identify potential threats, and generating reports for compliance audits. **Endpoint Central:** Ensure that anti-malware solutions are installed and updated on all endpoints. This solution can also collect and centralize logs from endpoints, including those generated by anti-malware solutions, and provide reports for compliance audits. **Patch Manager Plus:** Ensure that anti-malware solutions are updated with the latest security patches. It also collect and centralize logs from endpoints and generate reports for compliance audits. **OpManager:** Monitor the health and performance of anti-malware solutions and other security devices. It also generates alerts and reports for compliance audits, including audit logs for anti-malware solutions.
5.4.1	Verify that processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	**Access Manager Plus:** Protect against phishing attacks by requiring additional authentication factors or by flagging suspicious login attempts for further investigation with the help of MFA and risk-based authentication (RBA) capabilities. **Log360:** Identify phishing attacks in real time with the help of the threat detection capabilities. The solution monitors network traffic and alert security teams when suspicious activity are detected, including phishing attempts. **Endpoint Central:** Prevent phishing attacks using the endpoint protection and vulnerability management capabilities. This solution helps ensure that endpoints are secure and up to date, reducing the risk of successful phishing attacks. **Patch Manager Plus**: Identify and patch vulnerabilities that could be exploited in a phishing attack with the help of vulnerability scanning and patch management capabilities.

Requirement 6

Develop and maintain secure systems and software

Identify software and system vulnerabilities and apply appropriate security patches. Vulnerabilities related to custom software can be avoided by applying software life cycle (SLC) processes and secure coding techniques.

Requirement sections:

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

6.2 Bespoke and custom software are developed securely.

6.3 Security vulnerabilities are identified and addressed.

6.4 Public-facing web applications are protected against attacks.

6.5 Changes to all system components are managed securely.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
6.2.1	**Bespoke and custom software are developed securely, and are:** • Based on industry standards and best practices for secure development. • In accordance with PCI DSS. For example, secure authentication and logging. • Incorporating consideration of information security issues during each stage of the software development life cycle.	**ADAudit Plus:** Monitor and audit custom applications and scripts with the help of pre-built reports. The solution helps to identify if the custom applications are compliant with the security standards and best practices, and provides real-time alerts on any unauthorized access or changes made to the custom applications. **Applications Manager:** Identify and resolve security issues in custom software with the help of this application performance monitoring (APM) solution. It also provides visibility into the performance of custom applications and identifies issues related to security vulnerabilities. **Firewall Analyzer:** Monitor the security of custom applications by analyzing firewall logs. This solution also provides real-time alerts on any security breaches and helps to identify the root cause of the issue. **Log360:** Identify and mitigate security risks in custom software by analyzing logs. This solution provides real-time alerts on any security breaches and helps to identify the root cause of the issue. **Patch Manager Plus:** Identify and mitigate security vulnerabilities in custom software by managing and deploying patches. The solution provides comprehensive reports on the status of patches, and helps to identify any gaps in the security posture of the custom software. **Vulnerability Manager Plus:** Ensure vulnerability scanning and management solutions for custom software. It helps to identify and prioritize vulnerabilities in custom software and provides guidance on how to remediate the issues.
6.2.2	**Ensure software development personnel working on bespoke and custom software are trained at least once every 12 months as:** • On software security relevant to their job function and development languages. • With secure software design and secure coding techniques. • Including, if security testing tools are used, on how to use the tools for detecting vulnerabilities in software.	**ADAudit Plus:** Get reports on the activities of software development personnel, including changes made to source code and other development artifacts. This solution helps identify security vulnerabilities introduced during the development process and provide insights into training needs. **Firewall Analyzer:** Enforce secure coding practices by blocking access to known insecure code libraries or prohibiting the use of certain coding practices. **Vulnerability Manager Plus:** Identify vulnerabilities in the custom software and recommend remediation steps. The solution helps development personnel learn about specific vulnerabilities and how to address them in future development efforts. **Log360:** Track changes made to security testing tools and provide reports on how they are being used by development personnel. This solutions helps identify areas where additional training might be needed.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
6.2.4	**Confirm that software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to:** • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.	**ADAudit Plus:** Track and report on all SQL injection attempts in real time, as well as monitor and audit database access and activity. **Firewall Analyzer:** Analyze and detect SQL injection attacks by examining database traffic and generating alerts. **EventLog Analyzer:** Detect and alert on buffer overflow attacks by monitoring system logs and identifying anomalies in network traffic. **ADSelfService Plus:** Enforce password policies and complexity requirements to prevent brute-force attacks on user accounts. **Key Manager Plus:** Enforce strong encryption protocols and ciphers, and manage cryptographic keys and certificates. **Password Manager Pro:** Automate the rotation of passwords and enforce password complexity requirements to ensure secure cryptographic implementation. **Application Manager:** Perform comprehensive application monitoring and get real-time alerts on application performance, availability, and security issues. **Firewall Analyzer:** Protect web applications from XSS, CSRF, and other attacks by filtering incoming traffic and blocking malicious requests.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
6.3.1	Security vulnerabilities are identified and managed as: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software. For example, operating systems and databases are covered.	**Vulnerability Manager Plus:** Provides vulnerability assessment and management capabilities. The solution helps you scan the network for vulnerabilities, and render a risk score for each vulnerability based on industry best practices. It also provides recommendations for remediation. **Patch Manager Plus:** Manage patches for various third-party software, including operating systems and databases. This solution scans the network for missing patches and provides a risk score for each missing patch. It also provides recommendations for patching. **Log360:** Provides real-time threat intelligence and log management capabilities. The solution helps organizations identify new security vulnerabilities using industry-recognized sources for security vulnerability information, including alerts from international and national CERTs. **Firewall Analyzer:** Identify and manage security vulnerabilities in the firewall. This solution provides real-time alerts for firewall rule changes and generates reports on vulnerabilities in firewall rules.
6.3.2	Verify that an inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	**AssetExplorer:** Maintain an inventory of all software assets, including bespoke and custom software, and third-party software components. The solution provides complete details about the software, including version information, license details, and other relevant information. This information is used to identify and track vulnerabilities and apply patches as required. **Endpoint Central:** Identify vulnerabilities in both third-party and custom software. This solution provides an integrated patch management system that automatically deploys patches to systems in the network. It also creates custom software packages for bespoke applications, and ensures that they are included in the patch management system. **Patch Manager Plus:** Maintain an inventory of all software assets, including bespoke and custom software, and third-party software components. The solution scans the network to identify vulnerabilities and provide a comprehensive report that includes details about the software, the associated vulnerabilities, and recommended patches. It also deploys patches automatically, ensuring that all systems are up-to-date. **Vulnerability Manager Plus:** Identify vulnerabilities in both third-party and custom software. This solution scans the network to identify vulnerabilities and provide a comprehensive report that includes details about the software, the associated vulnerabilities, and recommended patches. It also provides details about the severity of the vulnerability, enabling organizations to prioritize patching efforts.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
6.3.3	**Ensure all system components are protected from known vulnerabilities by installing applicable security patches and updates as:** • Critical or high-security patches and updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches and updates are installed within an appropriate time frame as determined by the entity. For example, within three months of release.	**Patch Manager Plus:** Automate the patch management process for operating systems, third-party applications, and custom software. The solution provides support for over 850 third-party applications, including Adobe, Java, and Microsoft products. The tool also enables organizations to test patches before deployment, schedule patch deployments, and view patch compliance reports to ensure timely patching of critical vulnerabilities. **Vulnerability Manager Plus:** Identify and remediate vulnerabilities in the IT infrastructure. The tool scans for vulnerabilities across operating systems, web applications, databases, and network devices. This solution also provides risk-based prioritisation of vulnerabilities based on the National Vulnerability Database (NVD) and Common Vulnerability Scoring System (CVSS) scores, that enables organizations to prioritize critical or high-risk vulnerabilities for patching. **Endpoint Central:** Automate patch deployment for desktops, laptops, and servers running Windows, macOS, and Linux operating systems. The solution supports patching for third-party applications, including Adobe, Java, and Microsoft products, and enables organizations to test patches before deployment, schedule patch deployments, and view patch compliance reports.
6.4.1	**For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as:** • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods : • At least once every 12 months and after significant changes. • By an entity that specializes in application security. • Including, at a minimum, all common software attacks in Requirement 6.2.4. • All vulnerabilities are ranked in accordance with Requirement 6.3.1. • All vulnerabilities are corrected. • The application is re-evaluated after the corrections.	**Firewall Analyzer:** Detect and prevent web-based attacks by installing this solution in front of public-facing web applications. It can actively run and update to detect new threats and vulnerabilities. The solution generates audit logs, and is configured to either block web-based attacks or generate an alert that is immediately investigated. **Application Manager:** Review public-facing web applications using manual or automated application vulnerability security assessment tools or methods. This solution performs automated vulnerability scans on web applications, and provides a detailed report of vulnerabilities. It also provides real-time monitoring and alerting for web applications.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
	or • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as: • Installed in front of public-facing web applications to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	**Log360:** Generate audit logs for public-facing web applications. The solution collects logs from various sources, including web servers and web application firewalls, and generate reports on attacks and vulnerabilities detected.
6.4.2	**For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:** • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	**OpManager:** Automate compliance checks and implement configuration changes for network devices. This solution also enables users to ensure that only the required services and protocols are enabled on their systems. **ADAudit Plus:** Monitor and audit AD configuration changes. The solution tracks and alerts administrators about any unauthorized changes to system configurations and ensures that industry-accepted hardening standards are followed. **EventLog Analyzer:** Collect and analyze system logs, and alert users to any changes to security parameters, and ensures that insecure services, protocols, and daemons are disabled or removed. **Password Manager Pro:** Provides a secure vault for storing and managing privileged passwords. This solution enables administrators to change default passwords, enforce password policies, and automate password rotation, thus ensuring that system passwords and passphrases are not vendor-supplied defaults.
6.4.3	**All payment page scripts that are loaded and executed in the consumer's browser are managed as:** • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary.	**Firewall Analyzer:** Monitor web traffic to detect and block suspicious requests to payment pages. The solution also generates reports on web traffic and alerts administrators of any unauthorized scripts or suspicious activity on payment pages.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
6.5.1	**Confirm that changes to all system components in the production environment are made according to established procedures that include:** • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.	**ServiceDesk Plus:** Establish and enforce change management processes for IT systems. This solution enables you to define workflows and approval processes for change requests, and provides visibility into the status of changes. You can also use this solution to document the reasons for changes and their security impact. **ADManager Plus:** Automate AD change management. Set up workflows to automate the approval and implementation of AD changes, ensuring that they are documented and approved before being implemented. This solution also enables you to track changes and generate reports to verify that changes have been made in accordance with established procedures. **OpManager:** Monitor changes in IT systems and applications. It provides real-time visibility into the performance of IT systems and applications, enabling you to identify potential issues before they become problems. You can also use the solution to track changes and verify that they have been made in accordance with established procedures. **Firewall Analyzer:** Monitor changes to firewall rules and configurations. It provides real-time alerts when changes are made, enabling you to quickly identify and respond to unauthorized changes. This solution has reporting and auditing capabilities, which enables you to track changes and ensure that they are made in accordance with established procedures.
6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and the documentation is updated as applicable.	**ADAudit Plus**: Ensure that all changes made to systems and networks are tracked and audited. This solution provides reports on changes made to user accounts, group policies, and other system configurations. By monitoring and auditing all changes, this solution helps ensure that all applicable PCI DSS requirements are in place after a change. **EventLog Analyzer:** Monitor and analyze log data from systems and networks to ensure that all PCI DSS requirements are being met. The solution alert administrators of potential security issues and generates reports on compliance with specific PCI DSS requirements. **Firewall Analyzer:** Monitor and analyze firewall logs to ensure that all traffic is being filtered and that all PCI DSS requirements are being met. This solution also generates reports on firewall activity to ensure compliance with specific PCI DSS requirements. **OpManager:** Monitor and manage network devices to ensure that all PCI DSS requirements are being met. The solution provides alerts on potential security issues and generates reports on compliance with specific PCI DSS requirements.

Requirement 7

Restrict access to system components and cardholder data by business need to know

Apply access control rules and mechanisms to prevent unauthorized access to critical systems, applications, and data. Limit access and grant privileges based on the requirement and job responsibilities.

07

Requirement sections:

7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

7.2 Access to system components and data is appropriately defined and assigned.

7.3 Access to system components and data is managed via an access control system(s).

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	**ADManager Plus:** Manage user accounts, permissions, and group memberships across multiple directories and systems. The solution automates user provisioning, deprovisioning, and permission changes based on predefined workflows, policies, and business rules. It also generates reports and audit trails to track changes and monitor access. **Password Manager Pro:** Control and monitor access to privileged accounts and resources. This solution provides a centralized vault to store and rotate passwords, SSH keys, and certificates. It also enforces granular access controls, session recordings, and approval workflows to ensure accountability and compliance. **Firewall Analyzer:** Enforce access policies and secure network endpoints. The solution can monitor network traffic, identify and block unauthorized devices and users, and quarantine infected systems. It also integrates with AD or LDAP to enforce RBAC and comply with regulatory requirements.
7.2.3	Ensure that required privileges are approved by authorized personnel.	**Access Manager Plus:** Provides a centralized platform for managing access to critical systems and data. It enables administrators to create and manage roles, assign permissions, and establish workflows for access requests and approvals.
7.2.4	Verify that all user accounts and related access privileges, including third-party and vendor accounts, are reviewed: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	**ADAudit Plus:** Perform regular user account reviews by providing predefined reports that detail user account activity, access history, and changes made to user accounts. These reports can be scheduled to run automatically and sent to the appropriate personnel for review. Additionally, this solution also helps raise alerts to notify administrators when there are changes to user accounts, or when an account is inactive for a certain period. **Access Manager Plus:** Ensure that user access is appropriate based on job function by providing granular access controls, and the ability to create policies that define access privileges based on job roles.The solution provides automated access review workflows that helps organizations streamline the review process and ensure that access privileges remain appropriate. **Identity Manager Plus:** Manage third-party and vendor accounts by providing automated workflows for onboarding and offboarding vendor accounts. This solution helps organizations enforce access controls and policies for third-party and vendor accounts, and provide reports that detail the activity and access history of these accounts.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
7.2.5	All application and system accounts and related access privileges are assigned and managed: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.	**Password Manager Pro:** Manage privilege access to critical systems and applications by providing secure storage, management, and retrieval of passwords. The solution enables you to enforce password policies and automatically change passwords to ensure that access is limited to those who require it. **Access Manager Plus:** Ensure granular access controls and role-based access to critical systems and applications. This solution enables you to create access policies based on user roles, groups, and devices to ensure that users have access only to the systems and applications they need. **ADManager Plus:** Automate the process of assigning and managing user accounts and access privileges in AD. The solution enables you to create templates for user account creation and automatically assign privileges based on the user's role.

Requirement 8

Identify users and authenticate access to system components

Implement and manage strong identification and authentication measures to grant access to user rights and privileges. Establish and manage identities and verify them with the help of authentication factors, including MFA, to strengthen the security of your CDE.

Requirement sections:

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's life cycle.

8.3 Strong authentication for users and administrators is established and managed.

8.4 MFA is implemented to secure access into the CDE.

8.5 MFA systems are configured to prevent misuse.

8.6 Use of application and system accounts and associated authentication factors is strictly managed.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.1.1	**Ensure all security policies and operational procedures that are identified in Requirement 8 are:** • Documented. • Kept up to date. • In use. • Known to all affected parties.	**ServiceDesk Plus:** Create and manage policies and procedures in a structured and organized manner, and track policy and procedure changes, ensuring that they are kept up to date. This solution provides a centralized platform for documenting security policies and operational procedures. **ADAudit Plus:** Audit and report on all changes made to AD, including changes to security policies and operational procedures in real time. The solution tracks policy and procedure changes, and ensures that they are being followed by all affected parties. **Log360:** Ensure centralized log collection, analysis, and reporting for all IT systems and applications. This solution enables organizations to monitor policy and procedure compliance by generating alerts and reports on policy violations. **Endpoint Central:** Enforce security policies on all endpoints, including desktops, laptops, and mobile devices. This solution enables organizations to manage security policies and procedures centrally and ensure that they are being followed by all users.
8.2.1	Confirm that all users are assigned a unique ID before access to system components, or that cardholder data is allowed.	**ADManager Plus:** Manage AD user accounts and permissions from a central location. The solution includes a user creation wizard that automates the process of assigning unique IDs to new users. **Password Manager Pro:** Store and manage passwords, including those associated with user accounts in a secure vault. This solution helps ensure that each user has a unique ID and password before being granted access to sensitive systems or data. **Access Manager Plus:** Access multiple applications with a single set of credentials with the help of this solution's single sign-on (SSO) capabilities. The solution also helps ensure that each user has a unique ID and password before accessing any system components or cardholder data.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.2.2	**Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as:** • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	**Password Manager Pro:** Store shared credentials in a centralized password vault. The vault is protected by MFA and granular access controls. This solution automatically rotates passwords for shared accounts on a regular basis to prevent unauthorized access. This ensures that the password is changed immediately after the exceptional circumstance has ended. The solution also helps maintain detailed audit trails of all password-related activities, including who accessed which password, when, and from where, helping organizations track all actions taken with shared credentials and ensuring that every action is attributable to an individual user. Additionally, this solution enables users to request access to shared credentials through a customizable access request workflow. The workflow ensures that every access request is explicitly approved by management and that individual user identity is confirmed before granting access.
8.2.4	**Verify that addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as:** • Authorized with the appropriate approval. • Implemented with only the privileges specified on the	**ADManager Plus:** Enforce password policies across AD environments. The solution includes options to specify password length requirements, require the use of both numeric and alphabetic characters, and prevent the use of easily guessable passwords. **Password Manager Pro:** Enforce password policies across an entire IT infrastructure. This solution includes options to specify password strength requirements and prevent the use of weak passwords. **ADSelfService Plus:** Educate users on the importance of strong passwords and encourage them to choose strong passwords. The solution includes a password strength meter that provides feedback to users on the strength of their chosen passwords.
8.2.5	Establish that access for terminated users is immediately revoked.	**ADManager Plus:** Automate user provisioning and deprovisioning, when an employee is terminated ensuring their account is automatically disabled or deleted based on predefined rules and workflows. This solution enables mass deprovisioning of user accounts, which can save time and ensure that all accounts associated with a terminated user are disabled. **Identity Manager Plus:** Manage the life cycle of user accounts, including provisioning, deprovisioning, and access review. This solution allows for role-based access control and enables organizations to set up approval workflows for granting access to sensitive systems and data. It also provides reports on user activity, which can be used to monitor for any unauthorized access attempts.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.2.6	Ensure inactive user accounts are removed or disabled within 90 days of inactivity.	**ADManager Plus:** Create an automated workflows that helps identify and disable inactive user accounts. Administrators can configure actions such as disabling accounts or sending notifications to account owners when their accounts are inactive for a specified period of time. **ADAudit Plus:** Receive reports on inactive user accounts to identify and disable them. The solution can be configured to generate reports on accounts that have not been used to log in to the system for a specified period of time.
8.2.7	Confirm accounts used by third parties to access, support, or maintain system components via remote access are managed as: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.	**Remote Access Plus:** Secure remote access to endpoints and servers. This solution enables organizations to create granular policies to control access, set up MFA, and monitor all remote access activities in real time. **Access Manager Plus:** Control access to applications and resources by third-party vendors. The solution enables MFA, granular control over user access, and provides real-time monitoring of user activities. **Password Manager Pro:** Ensure secure management of passwords for privileged accounts used by third-party vendors. This solution provides password rotation, automatic discovery of privileged accounts, and MFA.
8.2.8	Verify that if a user session has been idle for more than 15 minutes, the user is required to reauthenticate to reactivate the terminal or session.	**ADAudit Plus:** Get real-time alerts and reports on user logon activities. Organizations can monitor user activity and set up alerts to notify them if a user session has been idle for more than 15 minutes. The solution helps configure policies to log off idle users automatically after a certain period of time. **ADManager Plus:** Configure session timeout policies to enforce user reauthentication after a certain period of inactivity. This ensures that unauthorized users do not gain access to sensitive data even if a user forgets to log off their session.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.3.1	**Establish that all user access to system components for users and administrators is authenticated via at least one of the following authentication factors:** • Something you know, such as a password or passphrase. Something you have, such as a token device or smart card. • Something you are, such as a biometric element like a facial or iris scan, or a fingerprint.	**ADSelfService Plus:** Enable users to reset their forgotten or expired passwords, and unlock their accounts by themselves. The solution also supports MFA, including one-time passwords and biometrics, to provide secure authentication for remote access. **Password Manager Pro:** Manage privileged accounts, enabling organizations to implement strong password policies, and manage access to critical systems and applications via a centralized platform. **Access Manager Plus:** Enable users to access multiple applications using a single set of credentials with the help of the SSO capabilities. The solution also supports MFA, including biometrics, to provide secure access to critical systems and applications. **Log360:** Monitor user activity and detect anomalies that might indicate a security breach using real-time threat detection and log management capabilities. **EventLog Analyzer:** Detect security threats and compliance violations in real time with the help of real-time log analysis and event correlation capabilities.
8.3.2	Ensure strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	**ADSelfService Plus:** Provide end-users with a secure way to reset their forgotten passwords, change their passwords, and update their personal information.The solution uses strong cryptography to encrypt all user authentication factors during transmission and storage. **Password Manager Pro:** Provide IT administrators with a secure and centralized way to manage privileged accounts and passwords. This solution uses strong cryptography to encrypt all sensitive information related to authentication, such as passwords and authentication tokens, during transmission and storage. **Key Manager Plus:** Enable a secure and centralized way to manage encryption keys and digital certificates. The solution uses strong cryptography to ensure that all sensitive information related to authentication is kept secure and unreadable during transmission and storage.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.3.3	Confirm that user identity is verified before modifying any authentication factor.	**Password Manager Pro:** Centrally manage and store all their privileged account passwords. This solution includes features such as 2FA, session recording, and access control to ensure that user identities are verified before making any changes to authentication factors. **ADManager Plus:** Provides a comprehensive solution for managing AD user accounts. The solution includes features such as user provisioning, deprovisioning, and modification, as well as self-service password reset and 2FA. **ADSelfService Plus:** This solution provides self-service password reset and account unlock capabilities to end users. This solution includes features such as MFA, help desk delegation, and policy enforcement to ensure that user identities are verified before making any changes to authentication factors. **Mobile Device Manager Plus:** Provides mobile device management capabilities for iOS, Android, and Windows devices. The solution includes features such as mobile application management, device security, and compliance enforcement, as well as 2FA to ensure that user identities are verified before making any changes to authentication factors.
8.3.4	Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.	**ADAudit Plus:** Monitor user logons in real time and alert administrators when there are repeated failed logon attempts. This solution provides automatic account lockout and password reset capabilities. **Password Manager Pro:** Enforce password policies, monitor password usage, and implement account lockout policies to prevent unauthorized access. **ADSelfService Plus:** This solution provides MFA options, including SMS and email-based authentication, which helps prevent brute-force attacks. The solution also enables organizations to enforce strong password policies and set account lockout thresholds.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.3.5	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	**Password Manager Pro:** Centrally manage and store all their privileged account passwords. The solution includes features such as password policies, password resets, and scheduled password changes to ensure that passwords are set and reset for each user as required by PCI DSS. **ADManager Plus:** This solution provides a comprehensive solution for managing AD user accounts. It includes features such as password policies, password resets, and scheduled password changes to ensure that passwords are set and reset for each user as required by PCI DSS. **ADSelfService Plus:** The solution delivers self-service password reset capabilities to end-users. It includes features such as password policies, password resets, and password expiration notifications to ensure that passwords are set and reset for each user as required by PCI DSS.
8.3.6	If passwords and passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the this minimum level of complexity: • A minimum length of 12 characters (or if the system does not support 12 characters, a minimum length of eight characters). • Contains both numeric and alphabetic characters.	**ADSelfService Plus:** Enforce strong password policies and complexity requirements such as minimum length, use of special characters, and regular password changes. It also supports the implementation of 2FA to strengthen authentication processes beyond passwords. Using this solution, administrators can configure password policies and deploy them to all users to ensure password complexity requirements are met. **Password Manager Pro:** Securely store and manage privileged account passwords and enforce password complexity policies for those accounts. Administrators can define and enforce password policies such as minimum length, use of special characters, and regular password changes for privileged accounts. The solution also provides the capability to perform periodic password rotation and can generate strong, random passwords that meet the complexity requirements.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.3.7	Verify that individuals are not allowed to submit a new password and passphrase that is the same as any of the last four passwords and passphrases used.	**Password Manager Pro:** Centrally manages and stores all privileged account passwords. This solution includes features such as password policies, password history tracking, and password rotation to ensure that individuals are not allowed to submit a new password that is the same as any of the last four passwords used. **ADManager Plus:** The solution provides a comprehensive solution for managing AD user accounts. It includes features such as password policies, password history tracking, and password expiration notifications to ensure that individuals are not allowed to submit a new password that is the same as any of the last four passwords used. **ADSelfService Plus:** Enables self-service password reset capabilities for end users. This solution includes features such as password policies, password history tracking, and password expiration notifications to ensure that individuals are not allowed to submit a new password that is the same as any of the last four passwords used.
8.3.8	**Authentication policies and procedures are documented and communicated to all users including:** • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords and passphrases. • Instructions to change passwords and passphrases if there is any suspicion or knowledge that the password and passphrases have been compromised and how to report the incident.	**ADManager Plus:** Enforce password policies such as password length, complexity, and history, which are essential to comply with the requirement. The solution enables the definition and enforcement of custom password policies that match the organization's security standards. It also allows establishing automatic password expiration policies that require users to change their passwords after a specific period. This solution helps to notify users of impending password expirations. These notifications can customized to include password policies, recommendations for creating a strong password, and links to password reset portals. **Password Manager Pro:** Enable the users to reset or change their passwords without the help desk's intervention. Users can securely reset their passwords through a web-based portal or mobile app, eliminating the need for them to contact the help desk. This solution also provides reports on password usage, including passwords that are never or rarely used, passwords that have been reset, and passwords that are shared between multiple users. This feature can help you detect and mitigate security risks. **ADSelfService Plus:** Provides MFA solutions that deliver an additional layer of security to user authentication. Users can authenticate through various methods, such as mobile push notifications, soft tokens, SMS, and email, in addition to passwords. This solution helps to notify users of impending password expirations. These notifications can customized to include password policies, recommendations for creating a strong password, and links to password reset portals.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.3.9	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, or • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	**Password Manager Pro:** Centrally manage and store all privileged account passwords. The solution includes features such as password policies, password rotation, and password expiration notifications to ensure that passwords are changed at least once every 90 days. **ADManager Plus:** Provides a comprehensive solution for managing AD user accounts. This solution includes features such as password policies, password rotation, and password expiration notifications to ensure that passwords are changed at least once every 90 days. **Log360:** Delivers real-time log analysis and correlation capabilities that help organizations dynamically analyze the security posture of user accounts. This solution includes features such as user behavior analytics, anomaly detection, and automated threat response to ensure that real-time access to resources is automatically determined accordingly.
8.3.11	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	**ADManager Plus:** Manage user accounts and access rights in AD. Administrators can assign authentication factors such as smart cards or certificates to individual users and ensure that they are not shared among multiple users. This solution also provides options to enable strict password policies, force password resets, and detect weak passwords, helping to ensure strong authentication practices. **Password Manager Pro:** Provides a centralized platform for managing and controlling privileged access to critical systems and applications. The solution helps enforce the use of strong authentication factors such as 2FAand can also track and audit all access to privileged accounts.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.4.1	Ensure that MFA is implemented for all non-console access into the CDE for personnel with administrative access.	**Password Manager Pro:** Delivers MFA capabilities for privileged account access. This solution includes features such as one-time passwords (OTP), smart cards, and biometric authentication to ensure that only authorized individuals can access sensitive data. **ADManager Plus:** Provides a comprehensive solution for managing AD user accounts. The solution includes features such as MFA capabilities for remote access, session management, and user activity tracking to ensure that only authorized individuals can access sensitive data. **ADSelfService Plus:** Delivers self-service password reset capabilities to end-users, including MFA capabilities. This solution includes features such as OTP and biometric authentication to ensure that only authorized individuals can access sensitive data. **Log360:** Monitor and track user access to sensitive data using real-time log analysis and correlation capabilities provided by this solution. It includes features such as user behavior analytics, anomaly detection, and automated threat response to ensure that only authorized individuals can access sensitive data.
8.4.2	Confirm that MFA is implemented for all access into the CDE.	**ADSelfService Plus:** This solution provides a self-service portal for end users to manage their own authentication settings, including the ability to set up MFA for their accounts. This can include various factors, such as SMS-based one-time passwords, push notifications, or hardware tokens. **Password Manager Pro:** The solution includes support for a wide range of MFA options, including Google Authenticator, RSA SecurID, and YubiKey. It also enforces MFA for specific users or groups, and customizes the MFA policy for different scenarios. **AD360:** This solution includes a range of MFA options, including SMS-based one-time passwords, email-based codes, and soft token apps. It also includes support for hardware tokens, and can enforce MFA for all users accessing the CDE.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.4.3	**Verify that MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as:** • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.	**Password Manager Pro:** This solution provides MFA capabilities for privileged account access. It includes features such as OTP, smart cards, and biometric authentication to ensure that only authorized individuals can access sensitive data. **ADManager Plus:** The solution delivers a comprehensive solution for managing AD user accounts. It includes features such as MFA capabilities for remote access, session management, and user activity tracking to ensure that only authorized individuals can access sensitive data. **ADSelfService Plus:** This solution provides self-service password reset capabilities to end users, including MFA capabilities. It includes features such as OTP and biometric authentication to ensure that only authorized individuals can access sensitive data. **Log360:** The solution delivers real-time log analysis and correlation capabilities that can help organizations monitor and track user access to sensitive data. It includes features such as user behavior analytics, anomaly detection, and automated threat response to ensure that only authorized individuals can access sensitive data.
8.5.1	**Ensure that MFA systems are implemented as:** • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	**AD360:** Provides time-based one-time password (TOTP) authentication for AD, which is then resistant to replay attacks. This solution allows administrators to enable MFA for all users, including administrators, and can provide reports on all MFA bypass attempts.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
8.6.2	Confirm that passwords and passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration and property files, or bespoke and custom source code.	**Password Manager Pro:** Securely store and manage privileged passwords used for accessing critical applications, servers, and network devices. Passwords are encrypted and stored in a secure repository, and the solution supports automatic password resets, ensuring that hard-coded passwords are not used in scripts, configuration and property files, or source code. **Application Manager:** Ensure out-of-the-box support for monitoring application servers, databases, and middleware. The solution can detect and alert on hard-coded passwords in scripts and configuration files, helping to prevent their use. **Firewall Analyzer:** Gain visibility into network traffic and firewall logs, including identifying the use of hard-coded passwords in scripts and configuration files. The solution can generate reports and alerts on these events, enabling IT teams to take action to prevent their use.
8.6.3	**Verify that passwords and passphrases for any application and system accounts are protected against misuse as:** • Passwords and passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords and passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	**Password Manager Pro:** Enforce password policies, such as length, complexity, and expiration, for all stored passwords. This solution is a secure vault for storing and managing passwords and other sensitive information. It can also send notifications when passwords are about to expire or have been changed. **ADSelfService Plus:** Enable users to reset their passwords and unlock their accounts without IT assistance utilizing this self-service password management solution. It enforces password policies, such as complexity and expiration, and can notify users when their passwords are about to expire. **ADManager Plus:** Enforce password policies, including complexity and expiration, for all user accounts in AD. The solution also generates reports on password policy compliance and notifies users when their passwords are about to expire. **Exchange Reporter Plus:** Generate reports on password policy compliance, such as the complexity and expiration of user passwords, and notify users when their passwords are about to expire. This is a reporting and analysis solution for Microsoft Exchange Server.

Requirement 9

Restrict physical access to cardholder data

Set up security mechanisms to restrict physical access to cardholder data. This includes restricting entry into facilities and systems containing cardholder data.
Also, ensure that you physically protect all media containing the cardholder data and destroy it when your business no longer needs it.

Requirement sections:

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

9.3 Physical access for personnel and visitors is authorized and managed.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
9.2.1	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	**ADAudit Plus:** Monitor and track all user activity across the network, including access to sensitive systems and data. The solution provides real-time alerts and reports on user activity, helping organizations identify potential security threats and respond quickly to security incidents. **Access Manager Plus:** Gain granular access control and password management capabilities that can help secure physical access control systems. This solution can be used to enforce strong password policies, control access to sensitive areas, and monitor user activity to ensure compliance with PCI DSS requirements. **Log360:** Monitor and audit all log data from physical access control systems, such as badge readers and security cameras. The solution provides real-time alerts and reports on user activity, helping organizations identify potential security threats and respond quickly to security incidents. **EventLog Analyzer:** Monitor and analyze logs from all systems and devices in the network, including physical access control systems. This solution delivers real-time alerts and reports on user activity, to help identify potential security threats and respond quickly to security incidents.
9.4.1	Ensure all media with cardholder data is physically secured.	**ADAudit Plus:** Track all file and folder activity on Windows servers and workstations, including access attempts, modifications, and deletions. This helps organizations monitor and secure sensitive cardholder data that is stored on these systems. The solution is an IT security and compliance management solution that provides comprehensive auditing and reporting capabilities. **Key Manager Plus:** Control access to sensitive data, including cardholder data using this web-based key management solution. It can securely store encryption keys and digital certificates, and provide granular access control over who can access them. This helps ensure that cardholder data is only accessible by authorized personnel. **Mobile Device Manager Plus:** Secure mobile devices that may contain cardholder data. The solution helps enforce security policies, such as password requirements and data encryption, on mobile devices to help prevent unauthorized access to sensitive data.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
9.4.2	Confirm that all media with cardholder data is classified in accordance with the sensitivity of the data.	**Log360:** Identify and classify cardholder data stored in logs, and apply appropriate security measures to protect it. This solution provides real-time log management and analysis for IT infrastructure. **ADAudit Plus:** Identify and classify cardholder data stored on these systems, and apply appropriate security measures to protect it. The solution provides real-time audit trails for all changes made to AD, Windows servers, and workstations. **DataSecurity Plus:** Identify and classify cardholder data stored in the network with the help of this solution's data discovery and classification capabilities. It monitors access to sensitive data and provides alerts when unauthorized access is detected.

Requirement 10

Log and monitor all access to system components and cardholder data

Implement log monitoring and management practices to ensure that all logs related to system components and the CDE are collected and analyzed. Ensure you protect these audit logs from unauthorized modifications because these logs help detect and alert you of anomalies and suspicious activities, as well as support forensic analysis of events.

Requirement sections:

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.5 Audit log history is retained and available for analysis.

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
10.2.1	Ensure that audit logs are enabled and active for all system components and cardholder data.	**EventLog Analyzer:** Collect, analyze, and archive logs from various sources, including servers, applications, network devices, and security solutions. The solution generates real-time alerts on security events, including attempts to access cardholder data. **ADAudit Plus:** Track and audit all user and administrator activities in AD, Azure AD, Windows servers, and workstations. This solution produces detailed audit reports, including user logon and logoff events, file access, and permission changes. **Log360:** Monitor and analyze logs from a wide range of sources, including servers, applications, network devices, and security solutions. The solution generates real-time alerts on security events, including attempts to access cardholder data. **Firewall Analyzer**: Monitor and analyze logs from their firewalls. This solution produces real-time alerts on security events, including attempts to access cardholder data.
10.2.1.1	Verify that audit logs capture all individual user access to cardholder data.	**Log360:** Ensure centralized log management and monitoring. The solution collects logs from various sources, including servers, applications, and network devices, and stores them in a secure and tamper-proof manner. It also supports real-time log monitoring and alerting, and notifies immediately of any suspicious or unauthorized access to cardholder data.
10.2.1.2	Establish that audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	**EventLog Analyzer:** Collect and analyze logs from various sources, including servers, applications, and network devices. This solution can correlate logs from different sources to provide a complete picture of user activity and system events. It also generates real-time alerts and reports based on log data, making it easier to detect and investigate any suspicious activity. This solution also monitors administrative access to systems and applications, including interactive use of application or system accounts. It alerts administrators in real-time when an administrative user performs an action that is outside of their normal behavior.
10.2.1.3	Ensure audit logs capture all access to audit logs.	**EventLog Analyzer:** Gain access to audit trails. This solution provides audit trails for all actions taken by privileged users. Administrators can view the audit trails to investigate any suspicious activity or identify potential security issues.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
10.2.1.4	Confirm that audit logs capturez all invalid logical access attempts.	**EventLog Analyzer:** Generate detailed reports on all invalid access attempts, identify patterns and trends, and quickly identify and respond to potential security incidents. Additionally, the solution can also provide insights into user behavior, such as excessive login attempts, which can help organizations identify potential insider threats.
10.2.1.5	**Verify that audit logs capture all changes to identification and authentication credentials including, but not limited to:** • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	**ADAudit Plus:** Ensure real-time auditing and alerting for AD, Azure AD, and Windows servers. This solution can be configured to capture all changes to user accounts, including the creation of new accounts, elevation of privileges, and any changes, additions, or deletions to accounts with administrative access. **Log360:** Provides comprehensive log management and SIEM capabilities, enabling organizations to collect, manage, and analyze audit logs from a wide range of sources, including Windows and Unix servers, network devices, databases, and more.
10.2.1.7	Establish that audit logs capture creation and deletion of system-level objects.	**ADAudit Plus:** Ensure real-time auditing of AD, including tracking changes to objects such as users, groups, and computers. The solution provides reports and alerts for critical events, such as changes to privileged accounts or modifications to security policies. **EventLog Analyzer:** Provides centralized log management for Windows and Unix/Linux servers, as well as network devices such as routers, switches, and firewalls. This solution captures and analyzes logs from a wide range of sources, including system-level objects such as files, folders, and registry keys. **OpManager:** Delivers network and server monitoring, including real-time alerts for critical events such as system-level object creation or deletion. The solution also tracks changes to system configurations, including changes to network devices and server settings.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
10.2.2	**Ensure audit logs record the following details for each auditable event:** • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	**EventLog Analyzer:** Collect, analyze, and correlate log data from different sources, including servers, network devices, and applications. This solution generates reports and alerts based on specific criteria, such as failed login attempts, changes to user accounts, and access to sensitive data. **ADAudit Plus:** Audit Windows Active Directory and other IT systems to track user activity, generate reports, and alert on suspicious events. The solution helps organizations meet other PCI DSS requirements related to user access control and authentication. **Log360:** Collect, analyze, and archive log data from different sources, including servers, network devices, and applications. This solution provides real-time alerts and reports based on specific criteria, such as failed login attempts, changes to user accounts, and access to sensitive data. Additionally, it delivers automated responses to security threats, such as blocking IP addresses and disabling user accounts.
10.3.1	Confirm that read access to audit logs files is limited to those with a job-related need.	**Log360:** Provides a centralized platform for collecting and analyzing logs from various sources. The solution enables you to configure access controls so that only authorized personnel can view the logs. **ADAudit Plus:** Provides real-time monitoring and reporting of AD changes. This solution allows you to configure alerts and notifications for specific events, and restricts access to audit logs based on user roles and responsibilities. **EventLog Analyzer:** Provides comprehensive event log management and analysis. The solution enables you to configure user-specific access controls for audit logs and provides detailed reports on user access to logs.
10.3.2	Verify audit log files are protected to prevent modifications by individuals.	**Log360:** Protect audit logs from tampering by providing secure storage and access controls for audit log files. The solution provides real-time alerts and notifications for suspicious activity, helping organizations quickly identify and respond to any potential threats to the integrity of audit log files.
10.3.3	Establish that audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	**EventLog Analyzer:** Collect, analyze, and store logs from various sources, including network devices, servers, and applications. You can configure this solution to automatically collect and store audit logs in a secure, centralized location, such as a dedicated log server or storage appliance.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
10.4.1	**Ensure that the following audit logs are reviewed at least once daily:** • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).	**Log360:** Ensure real-time log monitoring, analysis, and management. This solution includes a user-friendly dashboard that enables personnel to easily review audit logs and identify potential security incidents. ManageEngine also provides training and certification programs for Log360 users to help them build the necessary skills to effectively analyze and interpret log entries.
10.4.1.1	Confirm that automated mechanisms are used to perform audit log reviews.	**Log360:** This comprehensive log management and SIEM solution enables you to collect, analyze, and correlate logs from various sources in real time. It has built-in automation features that enable you to automate log review processes, alert you about security events and potential security threats. The solution also features prebuilt compliance reports that help you demonstrate compliance with PCI DSS. **EventLog Analyzer:** This log management and SIEM solution helps with automated log reviews. This solution enables you to collect, analyze, and correlate logs from various sources in real time, and it provides built-in automation features that help with log review processes. It features prebuilt compliance reports that help you demonstrate compliance with PCI DSS.
10.4.1.1	Confirm that automated mechanisms are used to perform audit log reviews.	**Log360:** This comprehensive log management and SIEM solution enables you to collect, analyze, and correlate logs from various sources in real time. It has built-in automation features that enable you to automate log review processes, alert you about security events and potential security threats. The solution also features prebuilt compliance reports that help you demonstrate compliance with PCI DSS. **EventLog Analyzer:** This log management and SIEM solution helps with automated log reviews. This solution enables you to collect, analyze, and correlate logs from various sources in real time, and it provides built-in automation features that help with log review processes. It features prebuilt compliance reports that help you demonstrate compliance with PCI DSS.

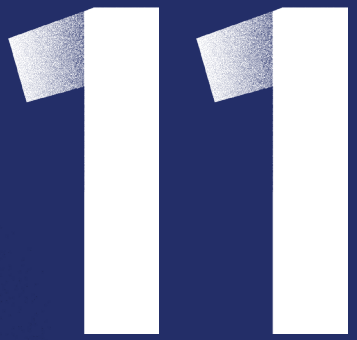
Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
10.4.2	Verify that logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	**EventLog Analyzer:** Collect and analyze logs from various sources including servers, databases, network devices, and applications. With its log analysis and reporting capabilities, the solution helps identify security incidents and anomalies in the logs generated by these systems.
10.4.2.1	Establish the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**Log360:** Identify and prioritize risks and perform regular log reviews with the help of the log management, log analysis, and log forensics capabilities provided by this solution. It provides automated alerts and notifications to help organizations quickly respond to potential threats, and reduces the time it takes to detect and respond to security incidents. **Vulnerability Manager Plus:** Identify vulnerabilities in the IT infrastructure and prioritize them based on the level of risk they pose to the organization. By addressing vulnerabilities promptly, organizations can reduce the risk of security incidents and ensure that log reviews are conducted on a regular basis. **Analytics Plus:** Gain access to data visualization and reporting capabilities that help organizations track and monitor their compliance with PCI DSS requirements, including those related to log reviews.
10.4.3	Ensure that exceptions and anomalies identified during the review process are addressed.	**Log360:** Provide real-time alerts and notifications for any unusual activity detected in the audit logs. This solution enables security teams to quickly identify and investigate potential threats, and take appropriate actions to mitigate them.
10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	**EventLog Analyzer:** Collect, store, and analyze log data from various sources in real time. The solution can retain logs for up to seven years, and it provides prebuilt compliance reports for PCI DSS, as well as alerts and dashboards to monitor critical events. **Log360:** Collect and store logs from various sources and supports retention policies that help organizations comply with PCI DSS requirements. This solution provides several prebuilt compliance reports, including PCI DSS, and also generates custom reports to meet specific audit requirements.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
10.6.1	Confirm that system clocks and time are synchronized using time-synchronization technology.	**OpManager:** This solution includes a time-synchronization feature that ensures all clocks in the network are synchronized to a common time source. This tool also generates reports to confirm that time synchronization is occurring as expected. **EventLog Analyzer:** The solution can automatically synchronize the time on all devices in the network and ensure that all events are recorded with accurate timestamps. The tool also produces reports on the accuracy of the timestamps, providing evidence that the system is meeting this requirement.
10.6.2	**Verify that systems are configured to the correct and consistent time as follows:** • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on • International Atomic Time (TAI) or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).	**AD360:** This solution can help with time synchronization across AAD domain environments, ensuring that all systems within the domain receive accurate and consistent time information. It supports time synchronization with external time servers, enabling organizations to configure AD domain controllers to use a designated central time server(s). **Applications Manager:** Monitor time synchronization across distributed systems and ensure that systems are configured to the correct time. The solution provides features for monitoring time drift and can alert administrators if time discrepancies are detected.
10.6.3	Establish that time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	**Endpoint Central:** Manage time settings on endpoints, including configuring time synchronization with Network Time Protocol (NTP) servers and setting up automatic time zone detection. This solution provides auditing and reporting capabilities to track changes to time settings. **ADManager Plus:** Manage time settings in AD environments, including configuring time synchronization and auditing changes to time settings. **EventLog Analyzer:** Monitor and analyze log data related to time settings and synchronization, including tracking changes to time settings and monitoring for unauthorized access to time data. **Access Manager Plus:** Enforce access controls and permissions related to time data, including restricting access to only authorized personnel and monitoring access to time data through audit logs and reports.

Requirement 11

Test security of systems and networks regularly

Perform penetration and vulnerability testing to identify, prioritize, and address internal and external security vulnerabilities. Carry out wireless analyzer scans to detect and identify all authorized and unauthorized wireless access points. Keep track of file modifications and network intrusions.



Requirement sections:

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

11.5 Network intrusions and unexpected file changes are detected and responded to.

11.6 Unauthorized changes on payment pages are detected and responded to.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
11.3.2	**Ensure external vulnerability scans are performed as follows:** • At least once every three months. • By a PCI Security Standards Council (PCI SSC) Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	**Vulnerability Manager Plus:** Identify and remediate vulnerabilities in an organization's network using this solution. It includes support for scanning web applications and external IP addresses, making it a suitable tool for external vulnerability scanning. This solution generates reports that demonstrate compliance with external scanning requirements. **Site24x7:** This is a cloud-based monitoring solution that includes support for external network and web application monitoring. The solution scans external IPs and domains for open ports, SSL/TLS vulnerabilities, and other common vulnerabilities, and can be configured to perform regular scans and send alerts when new vulnerabilities are discovered. It generates reports that demonstrate compliance with external scanning requirements.
11.3.2.1	**Confirm that external vulnerability scans are performed after any significant change as follows:** • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a Qualified Security Assessor (QSA) or an ASV.	**Vulnerability Manager Plus:** Perform regular external vulnerability scans and also scans to detect significant changes. This solution uses the CVSS to score vulnerabilities and provides a list of prioritized vulnerabilities to be remediated. It provides detailed reports to help meet the PCI DSS compliance requirements.
11.4.1	**A penetration testing methodology is defined, documented, and implemented by the entity, and includes:** • Industry-accepted penetration testing approaches. Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4.	**Vulnerability Manager Plus:** This solution provides comprehensive vulnerability assessment and management capabilities, including automated vulnerability scanning, reporting, and remediation workflows. The solution supports network-layer and application-layer penetration testing, as well as coverage for the entire CDE perimeter and critical systems. **Application Manager Plus:** The solution delivers application performance management capabilities, including application-layer penetration testing to identify vulnerabilities in the software development life cycle. This solution supports coverage for critical systems and the retention of penetration testing results and remediation activities for at least 12 months.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
	• Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.	**Firewall Analyzer:** The solution provides firewall management capabilities, including the validation of segmentation and scope-reduction controls. It detects and alerts on anomalies in network traffic, including potential intrusion attempts. **Log360:** This solution delivers log management and SIEM capabilities, including the review and consideration of threats and vulnerabilities experienced in the last 12 months. It assists with identifying exploitable vulnerabilities and security weaknesses found during penetration testing.
11.4.3	Verify that external penetration testing is performed: • Per the entity's defined methodology. • At least once every 12 months. • After any significant infrastructure or application upgrade or change. • By a qualified internal resource or qualified external third-party. • Organizational independence of the tester exists (not	**Application Manager:** Conduct application-layer penetration testing to identify the vulnerabilities listed in Requirement 6.2.4. **OpManager:** Ensure network-layer penetration testing that encompasses all components that support network functions as well as operating systems. **Vulnerability Manager Plus:** Identify and remediating vulnerabilities found during penetration testing. The solution provides a risk score to prioritize remediation efforts. **Log360:** Retain penetration testing results and remediation activities results for at least 12 months. **EventLog Analyzer:** Monitor and alert on suspicious activities during penetration testing, to ensure that testing is done in a controlled manner.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
11.4.4	**Establish that exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as :** • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.	**Vulnerability Manager Plus:** Identify vulnerabilities in your network, servers, and endpoints. It provides risk-based prioritization, remediation guidance, and reports to help you identify and fix vulnerabilities quickly. **Patch Manager Plus:** Automate the patching process across multiple operating systems and applications. This ensures that all systems are up-to-date with the latest security patches, reducing the risk of exploitation. **ServiceDesk Plus:** Track and manage incidents related to exploitable vulnerabilities and security weaknesses. This solution provides a centralized platform for documenting, prioritizing, and resolving security incidents. **Log360:** Detect security incidents and breaches by collecting and analyzing log data from various sources in your network. This solution generates reports on security incidents and assist in the incident response process. **OpManager:** Simulate attacks and identify vulnerabilities in your network. The solution helps you create a report of vulnerabilities found and remediation actions taken.
11.5.1	**Ensure intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as:** • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines. baselines, and signatures are kept up to date.	**Firewall Analyzer:** This solution delivers visibility into network traffic at the perimeter of the CDE, including identifying suspicious activity and alerts for potential intrusions. **EventLog Analyzer:** The solution provides real-time monitoring and analysis of logs from critical systems within the CDE, alerting personnel to potential threats and intrusions. **Log360:** This solution delivers real-time monitoring and analysis of logs from critical systems within the CDE, including identifying suspicious activity and alerts for potential intrusions. **Network Configuration Manager:** The solution enables organizations to maintain up-to-date intrusion-detection and prevention engines, baselines, and signatures, as required by the PCI DSS standard.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
11.5.2	**Confirm that a change-detection mechanism (for example, file integrity monitoring tools) is deployed:** • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	**DataSecurity Plus:** Provides real-time file auditing and change monitoring for Windows and NetApp file servers. This solution helps organizations meet this requirement by: • Tracking all changes made to files and folders, including modifications, deletions, and additions. It alerts administrators in real time when critical files are modified. • Scheduling file comparisons to ensure that critical files have not been modified. Administrators can specify the frequency and files to compare, and the solution will generate an alert if there are any discrepancies. • Provide detailed reports on file and folder changes. Reports can be generated on a weekly basis to meet the requirement for critical file comparisons.

Requirement 12

Support information security with organizational policies and programs

Maintain an information security policy which clearly defines the security roles and responsibilities of all personnel, including employees, contractors, and consultants. You should also make it a practice to perform security-related programs on a regular basis like risk assessment, user awareness training, employee background checks, and incident management.

Requirement sections:

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

12.4 PCI DSS compliance is managed.

12.5 PCI DSS scope is documented and validated.

12.6 Security awareness education is an ongoing activity.

12.7 Personnel are screened to reduce risks from insider threats.

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

12.9 TPSPs support their customers' PCI DSS compliance.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

*Note: As per the PCI DSS document, the requirements are further divided into requirement sections and subsections.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
12.1.2	**Ensure that the information security policy is:** • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.	**ADManager Plus:** Create and manage policies for their Active Directory environment. Policies can be reviewed and updated on a regular basis to ensure that they remain relevant and effective. **EventLog Analyzer:** Monitor logs from various sources, including security devices, servers, applications, and operating systems. By analyzing these logs, organizations can identify changes to their environment that may require updates to their information security policy. **Patch Manager Plus:** Manage patches for various applications and operating systems. By keeping software up to date, organizations can reduce the risk of vulnerabilities that may require changes to their information security policy. **Vulnerability Manager Plus:** Scan the network for vulnerabilities that may pose a risk to the environment. By identifying and addressing these vulnerabilities, organizations can update their information security policy to reflect changes in their risk profile.
12.1.4	Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	**Log360:** This Security Information and Event Management (SIEM) solution provides a comprehensive view of security events and incidents across the entire network. It can help identify potential security issues and enable CISOs and other security professionals to take appropriate action to address them.

Requirement number	Requirement	ManageEngine solutions that helps you meet the requirement
12.3.1	**Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes:** • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyzes when needed, as determined by the annual review.	**Vulnerability Manager Plus:** Identify the assets that are being protected by performing regular vulnerability assessments. It provides detailed reports on the assets scanned, the vulnerabilities identified, and recommendations for remediation. **Log360:** Identify the threat(s) that the requirement is protecting against by providing real-time threat intelligence and monitoring. It analyzes logs from various sources and detects security threats and anomalies. This solution can also help in determining, and including justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. It automates compliance assessments and provides reports that help organizations understand their compliance posture and identify areas of risk. **ADAudit Plus:** Identify the factors that contribute to the likelihood and/or impact of a threat being realized. It provides detailed reports on user activity, file and folder activity, and server and workstation activity, enabling organizations to identify areas of risk. It can also help in reviewing each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. And provides comprehensive audit reports that help organizations identify areas of risk and comply with various regulatory standards.

ManageEngine solutions that helps with PCI DSS v4 compliance

Identity and access management solutions

Manage, govern, and secure digital identities and privileged access.

Exchange Reporter Plus: Reporting, auditing, and monitoring for hybrid Exchange and Skype
ADManager Plus: Active Directory, Microsoft 365, and Exchange management and reporting
ADSelfService Plus: Password self-service, endpoint MFA, and enterprise SSO
AD360: Integrated identity and access management
Identity Manager Plus: Secure SSO for enterprise applications
Password Manager Pro: Privileged account management
Key Manager Plus: SSH key and SSL certificate management
Access Manager Plus: Privileged session management

Enterprise service management solutions

Design, automate, deliver, and manage IT and business services.

ServiceDesk Plus: Full-stack ITSM suite with enterprise service management
AssetExplorer: ITAM with built-in CMDB

Security information and event management solutions

Secure your network from cyberattacks and ensure compliance.

Log360: Comprehensive SIEM with advanced threat mitigation and ML-driven UEBA
EventLog Analyzer: Log management, IT auditing, and compliance management
Firewall Analyzer: Firewall rule, configuration, and log management
ADAudit Plus: Active Directory auditing and reporting
DataSecurity Plus: File auditing, data loss prevention, and data risk assessment

Unified endpoint management and security solutions

Manage and secure desktops, servers, laptops, mobile devices, and web browsers.

Endpoint Central: Holistic unified endpoint management and security
Mobile Device Manager Plus: Comprehensive mobile device management
Remote Access Plus: Remote access and support
Patch Manager Plus: Automated multi-platform patch management
Vulnerability Manager Plus: Integrated threat and vulnerability management
Endpoint DLP Plus: Integrated data loss prevention software

IT operations management solutions

Monitor and manage your network, servers, and applications.

OpManager: Network and server performance monitoring
NetFlow Analyzer: Bandwidth monitoring and traffic analysis
Network Configuration Manager: Network change and configuration management
Applications Manager: Server and application performance monitoring
Site24x7: Full-stack monitoring for IT admins, DevOps, and SREs

Advanced IT analytics

Visualize IT data and gain actionable insights into IT operations.

Analytics Plus: AI-enabled IT analytics for enterprises

ManageEngine's checklist for PCI DSv4 compliance

ManageEngine solutions	Requirements they help meet											
	1. Install and maintain network security controls	2. Apply secure configurations to all system components	3. Protect stored account data	4. Protect cardholder data with strong cryptography during transmission over open, public networks	5. Protect all systems and networks from malicious software	6. Develop and maintain secure systems and software	7. Restrict access to system components and cardholder data by business need to know	8. Identify users and authenticate access to system components	9. Restrict physical access to cardholder data	10. Log and monitor all access to system, components and cardholder data	11.Test security of systems and networks regularly	12. Support information security with organizational policies and programs
ADManager Plus		✓	✓	✓		✓	✓	✓		✓		✓
ADSelfService Plus					✓	✓		✓				
Exchange Reporter Plus				✓				✓				
AD360								✓		✓		
Identity Manager Plus							✓	✓				
Password Manager Pro		✓	✓	✓		✓	✓	✓				
Key Manager Plus			✓	✓		✓		✓	✓			
Access Manager Plus	✓	✓		✓	✓		✓	✓	✓	✓		

ManageEngine solutions	Requirements they help meet											
	1. Install and maintain network security controls	2. Apply secure configurations to all system components	3. Protect stored account data	4. Protect cardholder data with strong cryptography during transmission over open, public networks	5. Protect all systems and networks from malicious software	6. Develop and maintain secure systems and software	7. Restrict access to system components and cardholder data by business need to know	8. Identify users and authenticate access to system components	9. Restrict physical access to cardholder data	10. Log and monitor all access to system, components and cardholder data	11.Test security of systems and networks regularly	12. Support information security with organizational policies and programs
ServiceDesk Plus	✓	✓	✓		✓	✓		✓			✓	
AssetExplorer						✓						
Log360	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
EventLog Analyzer	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓
Firewall Analyzer	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
ADAudit Plus		✓	✓	✓		✓	✓	✓	✓	✓		✓
DataSecurity Plus			✓						✓		✓	
Endpoint Central	✓	✓		✓	✓	✓		✓		✓		
Mobile Device Manager Plus	✓							✓	✓			

ManageEngine solutions	Requirements they help meet											
	1. Install and maintain network security controls	2. Apply secure configurations to all system components	3. Protect stored account data	4. Protect cardholder data with strong cryptography during transmission over open, public networks	5. Protect all systems and networks from malicious software	6. Develop and maintain secure systems and software	7. Restrict access to system components and cardholder data by business need to know	8. Identify users and authenticate access to system components	9. Restrict physical access to cardholder data	10. Log and monitor all access to system, components and cardholder data	11.Test security of systems and networks regularly	12. Support information security with organizational policies and programs
Remote Access Plus								✓				
Patch Manager Plus	✓	✓			✓	✓					✓	✓
Vulnerability Manager Plus	✓	✓			✓	✓				✓	✓	✓
Endpoint DLP Plus					✓							
OpManager	✓	✓		✓	✓	✓				✓	✓	
NetFlow Analyzer	✓											
Network Configuration Manager	✓										✓	
Applications Manager	✓					✓		✓		✓	✓	

ManageEngine solutions	Requirements they help meet											
	1. Install and maintain network security controls	2. Apply secure configurations to all system components	3. Protect stored account data	4. Protect cardholder data with strong cryptography during transmission over open, public networks	5. Protect all systems and networks from malicious software	6. Develop and maintain secure systems and software	7. Restrict access to system components and cardholder data by business need to know	8. Identify users and authenticate access to system components	9. Restrict physical access to cardholder data	10. Log and monitor all access to system, components and cardholder data	11.Test security of systems and networks regularly	12. Support information security with organizational policies and programs
Site24x7											✓	
Analytics Plus										✓		

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—more than 120 products and free tools—to manage all of your IT operations, from networks and servers to applications, your service desk, AD, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use. You can find our on-premises and cloud solutions powering the IT of over 280,000 companies around the world, including 9 of every 10 Fortune 100 companies.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize future opportunities.

Enterprise service management
Full-stack ITSM suite
IT asset management with a CMDB
Knowledge base with user self-service
Built-in and custom workflows
Orchestration of all IT management functions
Service management for all departments
Reporting and analytics

Identity and access management
Identity governance and administration
Privileged identity and access management
AD and Azure AD management and auditing
SSO for on-premises and cloud apps, with MFA
Password self-service and sync
Microsoft 365 and Exchange management and auditing
AD and Exchange backup and recovery
SSH and SSL certificate management

Unified endpoint management and security
Desktop and mobile device management
Patch management
Endpoint device security
OS and software deployment
Remote monitoring and management
Web browser security
Monitoring and control of peripheral devices
Endpoint data loss prevention

Take control of your IT.

Monitor, manage, and make the most of your IT infrastructure.

ManageEngine crafts comprehensive IT management software for your business needs

Available for
Enterprise IT | Managed service providers (MSPs)
As
Self-hosted on-premises
Self-hosted in public cloud (AWS, Azure)
Zoho Cloud-native

IT operations management
Network, server, and application performance monitoring
Bandwidth monitoring with traffic analysis
Network change and configuration management
Application discovery and dependency mapping
Cloud cost and infrastructure monitoring
End-user experience monitoring
DNS management
AIOps

Security information and event management
Unified SIEM for cloud and on-premises
AI-driven user and entity behavior analytics
Firewall log analytics
Data leak prevention and risk assessment
Regulatory and privacy compliance

Advanced IT analytics
Self-service IT analytics
Data visualization and business intelligence for IT
Hundreds of built-in reports and dashboards
Instant, flexible report creation
Out-of-the-box support for multiple data sources

Low-code app development
Custom solution builder

9 of every 10 Fortune 100 companies
trust us to manage their IT

Glossary

Term	Definition
2FA	Two-factor authentication
APIs	Application program interface
APM	Application performance monitoring
ASV	Approved Scanning Vendor
CDE	Cardholder data environment
CERTs	Computer emergency response teams
CHD	Cardholder data
CSRF	Cross-site request forgery
CVSS	Common Vulnerability Scoring System
IDS/IPS	Intrusion detection system/Intrusion prevention system
LDAP	Lightweight Directory Access Protocol
MFA	Multi-factor authentication
NSC	Network security controls
NTP	Network Time Protocol
NVD	National Vulnerability Database
OTP	One-time password
PAN	Primary account number
PCI SSC	PCI Security Standards Council
POI	Point of interaction
QSA	Qualified Security Assessor
RBA	Risk-based authentication
RBAC	Role-based access controls
SAD	Sensitive authentication data
SIEM	Security information and event management
SLC	Software life cycle
SMS	Short Message Service
SoD	Segregation of duties
SOPs	Standard operating procedures
SSH	Secure Shell or Secure Socket Shell
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSO	Single sign-on
TOTP	Time-based one-time password
TPSP	Third-party service provider
UTC	Coordinated Universal Time
XSS	Cross-site scripting

www.manageengine.com

ManageEngine ManageEngine ManageEngine