



Tenable Cyber Exposure Study - PCI DSS v4.0

Last Revised: October 21, 2024

Table of Contents

PCI DSS v4.0 Overview	3
How Tenable Helps	6
Control Objective 1: Build and Maintain a Secure Network and Systems	8
PCI Requirements Under This Objective Supported by Tenable	8
Cloud Environments	14
Control Objective 2: Protect Account Data	16
PCI Requirements Under This Objective Supported by Tenable	16
Compliance Audit Files	17
Secure Sockets Layer	18
Web Application Scanning	21
Control Objective 3: Maintain a Vulnerability Management Program	22
PCI Requirements Under This Objective Supported by Tenable	22
Web Application Scanning	22
Tenable Security Center	23
Tenable Vulnerability Management	25
Antivirus	26
Control Objective 4: Implement Strong Access Control Measures	31
PCI Requirements Under This Objective Supported by Tenable	31
Control Objective 5: Regularly Monitor and Test Networks	36
PCI Requirements Under This Objective Supported by Tenable	36
Tenable Web App Scanning	40
Control Objective 6: Maintain an Information Security Policy	42
PCI Requirements Under This Objective Supported by Tenable	42
References	43

PCI DSS v4.0 Overview

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all organizations that accept, process, store, or transmit credit card information maintains a secure environment. The PCI DSS standard was developed by the PCI DSS Council. The council is made up of credit card companies such as Visa, MasterCard, American Express, Discover, and JCB. PCI DSS version 3.2.1 was officially retired on March 31, 2024 and version 4.0 became the industry standard moving forward. On March 31, 2025 all version 4.0 requirements will become mandatory.

Note: On June 11, 2024 PCI DSS v4.0.1 was released. This latest release is a “limited revision of PCI DSS v4.0” which includes corrections for typographical and other minor errors. There are no new requirements, and no requirements have been added or removed. Additional information on the summary of changes can be found in the References section at the end of this document.

PCI-DSS has 12 main requirements and more than 300 sub-requirements. These 12 requirements are technical and operational. The requirements are organized into six control objectives, and cover areas such as network security, password management, data protection, and access control.

PCI DSS v4.0.x has the following six control objectives:

1. Build and Maintain a Secure Network and Systems
2. Protect Account Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Compliance with PCI DSS is required for any organization that stores, processes, or transmits cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This requirement includes all entities involved in payment processing - merchants, processors, acquirers, issuers, and other service providers. Cardholder data and sensitive authentication data are defined as:

Cardholder Data

**Sensitive
Authentication Data**

Primary Account Number (PAN)	Full track data (magnetic stripe data or chip equivalent on a chip)
Cardholder Name	Card verification code
Expiration Date	PINs/PIN blocks
Service Code	

Depending on the number of transactions an organization processes annually and the specific payment brand involved, there are four different levels of compliance validation requirements, commonly known as classifications:

- PCI Level 1 - Businesses processing over 6 million transactions annually
- PCI Level 2 - Businesses processing 1 to 6 million transactions annually
- PCI Level 3 - Businesses processing 20,000 to 1 million transactions annually
- PCI Level 4 - Businesses processing less than 20,000 transactions annually

Currently, PCI Level 1 requires an annual report be conducted by a Qualified Security Assessor (QSA), or an Internal Security Assessor (ISA). A QSA will typically visit the organization to conduct an audit, while the ISA can be a member of the organization, who is properly trained to conduct an assessment, and act as a liaison to external auditors. PCI Level 1 is the strictest of all classifications. Any organization, regardless of classification, is subject to an external audit, even if the organization is not a PCI Level 1 merchant.

In addition, all PCI Level merchants also require the following:

- Vulnerability Scanning to be completed Quarterly. Tenable's PCI ASV (Approved Scanning Vendor) streamlines the quarterly external vulnerability scan submission and dispute process as required by PCI 11.3.2. With pre-configured scan templates and an efficient evidence/dispute resolution process, Tenable can quickly prepare an Attestation of Scan Compliance (AOSC) for merchants and service providers.
- Annual or Semi-annual Penetration Test, as required by PCI 11.4.3, depending on the organizational PCI requirements (Note: Not required for PCI Level 3 or PCI Level 4 Merchants, however these organizations would benefit from conducting a penetration test, as least

annually)

- Completion of a Self-Assessment Questionnaire (SAQ). Note: There are different types of SAQ depending on the scope of the audit. See PCI DSS documentation for more information.
- Completion of an Attestation of Compliance (AOC). This form states you have complied with the required standards to satisfy PCI DSS requirements.
- PCI Requirement 11.3.1 makes vulnerability scanning mandatory at least once every three months, and recommends more frequent scanning depending on network complexity.

Organizations can best determine their level of PCI compliance by coordinating with their service provider.

Failure to comply with PCI DSS can result in fines imposed by credit card companies, restriction or limitations on processing payments, and reputational damage arising from security breaches.

Therefore organizations handling credit card information are strongly encouraged to adhere to PCI DSS standards to protect cardholder data and maintain trust with their customers.

How Tenable Helps

The Tenable solution starts with a foundation of [Tenable Security Center](#) or [Tenable Vulnerability Management](#), for compliance and vulnerability scanning, which include internal and external scanning templates to meet the mandatory PCI scanning requirements of PCI DSS Requirement 11.3.1. Both solutions provide the ability to gather security data from across your organization using sources such as active and passive monitoring. Next building upon the foundation by adding [Tenable PCI ASV](#), to meet the external vulnerability scanning requirements. Tenable (an Approved Scanning Vendor) can quickly prepare a compliant scan report for merchants and service providers with PCI ASV, streamlining the quarterly external vulnerability scan submission and dispute process as required by PCI DSS. Finally, [Tenable Web App Scanning](#), as a dedicated PCI web app scan, to be combined with Tenable PCI ASV, as needs require the identification of vulnerabilities for public facing applications.

As part of the Vulnerability Management solution, Tenable provides audit files which contain cross references to a wide range of benchmarks, standards, and frameworks. In the following example, a Center for Internet Security (CIS) audit file is utilized in a scan against a Debian server running software version 9.7. Reviewing a single response for policy check CIS 3.5.2.1 - Ensure IPv6 default deny firewall policy, 25 other cross references are mapped, including PCI-DSSv4.0 Requirement 1.5.1. This CIS audit check applies to all the listed cross references, including PCI-DSS 1.5.1. The significance of this specific audit check is if IPv6 is enabled on a system, IP tables should be configured. A default deny-all policy on all connections ensures that any unconfigured network usage will be rejected. If not configured properly, and failure of the check is recorded, as shown here:

tenable Vulnerability Management | Findings > Finding Details

Quick Actions ?

← Back to Findings

3.5.2.1 Ensure IPv6 default deny firewall policy - Chain INPUT

HOST AUDITS **FAILED**

Description
 A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
 Rationale:
 More

Audit File
 CIS_Debian_Linux_9_Server_v1.0.1_L1.audit

Solution
 Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

 More

See Also
<https://workbench.cisecurity.org/files/2619>

Audit Discovery
 FIRST SEEN 10/22/2023 at 09:02 PM
 LAST AUDIT 08/12/2024 at 07:07 AM

Reference Information

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6()
CSCV7	9.4
CSF	DE CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPRA	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Asset Affected | View Asset Details

Asset Information

ASSET ID	[REDACTED]
NAME	[REDACTED]
IPV4 ADDRESS	[REDACTED]
OPERATING SYSTEM	Linux Kernel 4.9.0-8-amd64 on Debian 9.7
SYSTEM TYPE	general-purpose
PUBLIC	No

Policy Value

```
cmd: /sbin/ip6tables --list | /bin/grep 'Chain INPUT'
expect: "Chain INPUT \(policy DROP\)"
system: Linux
```

Actual Value

```
The command '/sbin/ip6tables --list | /bin/grep 'Chain INPUT'' returned :
Chain INPUT (policy ACCEPT)
```

Asset Scan Information

FIRST SEEN	10/22/2023 at 09:01 PM
LAST SEEN	08/12/2024 at 07:07 AM
LAST AUTHENTICATED SCAN	08/12/2024 at 07:07 AM
LAST LICENSED SCAN	08/12/2024 at 07:07 AM
SOURCE	Nessus Scan

Additional Information

NETWORK	Default
---------	---------

This embedded cross reference data is utilized to present and report compliance information within Tenable Vulnerability Management and Tenable Security Center using a variety of dashboards and reports highlighted in this guide.

For more information related to cross references, review the Cyber Exposure Study: [Host Audit Data](#)

Note: This document only presents solutions for portions of PCI DSS version 4 that can be measured and validated using automated processes. There are many policy specific items with the PCI DSS rules and guidelines that require organizations to manually create, develop, or review documented procedures, interview personnel, validate training, or examine procedures. These items can not be tested and therefore will not be referenced in this document.

Control Objective 1: Build and Maintain a Secure Network and Systems

This objective includes installing and maintaining firewalls, and firewall configurations to protect cardholder data, and not using vendor supplied credentials (default credentials) for system passwords or security parameters. This control objective covers the following PCI DSS requirements:

Requirement 1: Install and maintain network security controls

Requirement 2: Apply secure configurations to all system components

The PCI Security Standards Council defines network security controls (NSCs) as firewalls and other network security technologies, which typically control network traffic between two or more logical or physical network segments (or subnets) based on predefined policies or rules. Traditionally, this function has been provided by firewalls, but may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technologies.

PCI Requirements Under This Objective Supported by Tenable

Requirement 1: Install and maintain network security controls

Firewalls, routers, and cloud virtual networks are configured with access control lists to control network traffic flowing inbound and outbound from the CDE. Ensure only acceptable ports, and protocols are being used. Configuration standards may outline what is acceptable and permitted on the network.

Examine configuration settings for all NSCs and verify that only approved services, protocols, and ports are in use. Compromises often occur due to insecure services such as telnet and FTP. Unsecure or unmanaged ports, services, and protocols can not only give attackers a point of entry, but they are additionally often overlooked and unpatched. By identifying all ports, protocols, and services, entities can ensure that unnecessary ports, protocols, and services that do not have a defined business need are disabled or removed.

Any network configuration setting changes are identified. Changes should not introduce misconfigurations, insecure services, or unauthorized network connections. Changes include the addition, removal, or modification of any connection, and include changes to the component and the components security functionality.

Security controls are implemented on any computing device, including company and employee owned devices, (desktops, laptops, tablets, smart phones, and any other mobile computing device) that connects to both untrusted networks (including the internet) and the CDE. Ensure that security controls are implemented and running, (firewall software or other endpoint protection solutions). Split Tunneling is a VPN technology that supports VPN clients to send only specific traffic over the VPN, while the rest travels over the local network to the internet. This setting is often used with remote workers or associated with remote sites. Split Tunneling is very dangerous, as the malicious users are given the ability to maneuver over the VPN tunnel and gain access to protected resources. Because of the risk exposed when split tunneling, the PCI requirement suggests strictly prohibiting the use of split tunneling of all employee-owned, corporate-owned, and mobile devices.

Tenable has published several audit files that have checks for split-tunneling in Juniper and Cisco devices:

- DISA_Juniper_SRX_Services_Gateway_VPN_v2r2_STIG.audit
- DISA_STIG_Cisco_IOS_XE_Router_RTR_v2r9.audit
- DISA_Juniper_EX_Series_Switches_Router_v1r3_STIG.audi
- DISA_STIG_Cisco_IOS_XE_Switch_RTR_v2r5.audit
- DISA_STIG_Cisco_IOS-XR_Router_RTR_v2r4.audit

Requirement 2: Apply secure configurations to all system components

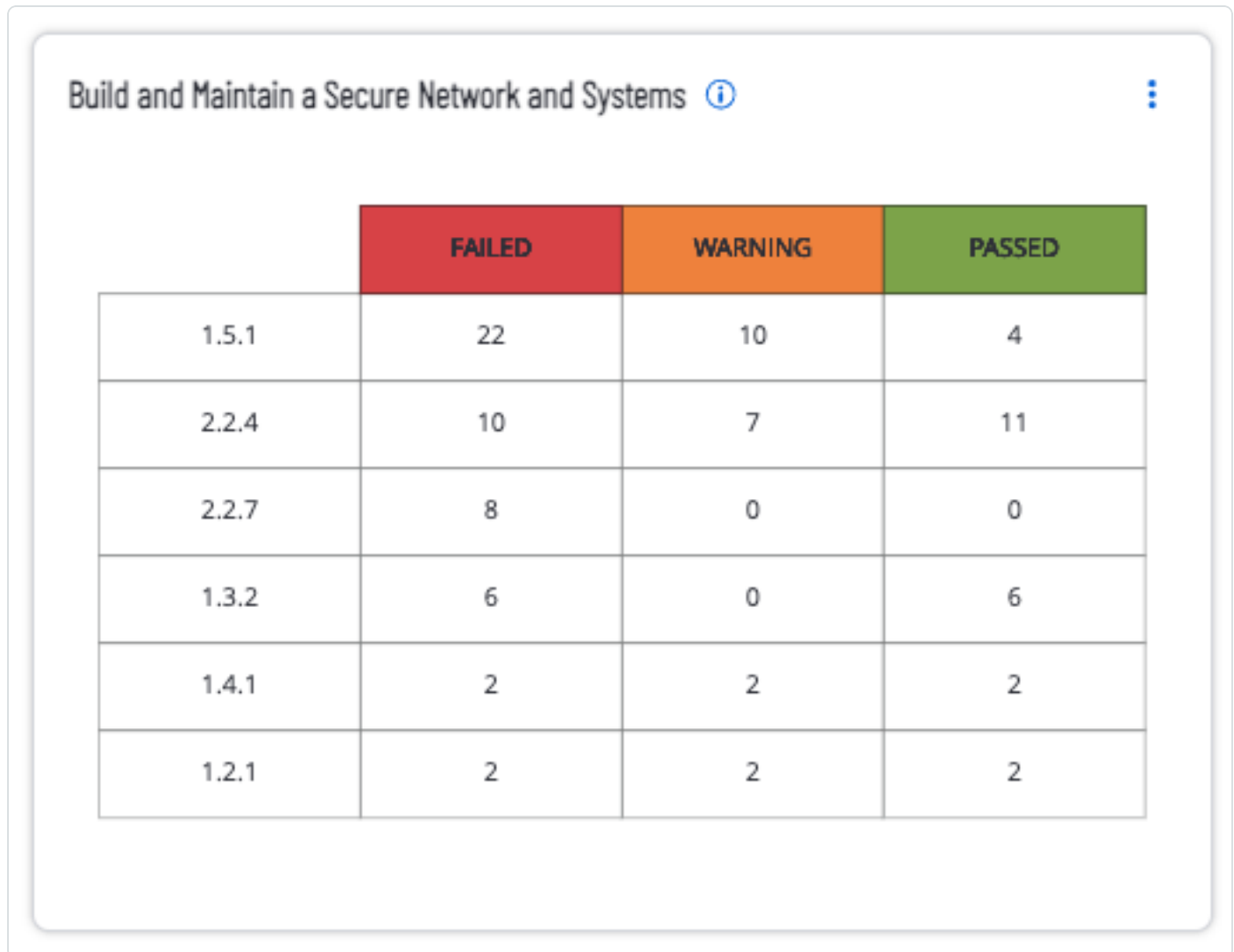
Default passwords are well known allowing bad actors (both external and internal) often use default passwords and other default vendor settings to compromise systems. Changing default passwords, removing unnecessary software, accounts, and services, reduces the attack surface.

Many operating systems and applications have known weaknesses by default. System configuration standards should be analyzed, and verified as being updated as new vulnerabilities are identified and immediately after a system is connected to a production environment. Keeping up to date with current industry standards will help maintain secure configurations. Numerous security organizations such as Center for Internet Security (CIS), International Organization for Standardization (ISO), and the National Institute of Standards and Technology (NIST), have established standards, recommendations, and system hardening guidelines.

Organizations should ensure that only necessary services, protocols, daemons, and functions are enabled on systems. Unnecessary functionality may include scripts, drivers, features, subsystems, file systems, interfaces (both USB and Bluetooth), as well as unnecessary web servers. Encrypted

communications should be used, and all clear text protocols should be avoided (HTTP, Telnet, etc). Certificates should be trusted, using strong encryption methods, and should not fall back to weaker insecure protocols or methods. Wireless Access Points, if used, should not have default encryption keys, SNMP defaults, or vendor defaults.

For Tenable Vulnerability Management the Build and Maintain a Secure Network and Systems widget provides details on each of the compliance controls for the compliance family group being referenced.



	FAILED	WARNING	PASSED
1.5.1	22	10	4
2.2.4	10	7	11
2.2.7	8	0	0
1.3.2	6	0	6
1.4.1	2	2	2
1.2.1	2	2	2

This widget focuses on the category Build and Maintain a Secure Network and Systems, which covers topics within PCI requirement 1 and 2. Both of these requirements cover installing and maintaining a firewall configuration to protect cardholder data, and the use of vendor supplied default credentials. This widget provides the count of audit checks according to the checks result.

The compliance control reference number is followed by a count, and compliance result for the compliance control displaying a count of passed, failed, and warning.

Compliance results are a product of Tenable Compliance audit files. Audit files contain tests for file permissions, configurations and access control. Audit files compare an organization's configuration to a secure standard, such as those available by the Center for Internet Security (CIS). A wide variety of audit files can be [downloaded here](#).

Clicking on the cell within the matrix, allows the user to drill down into the compliance data, opening the findings page and displaying the results (1). In this instance drilling down into the failed items under Requirement 1.5.1, the analysis is presented with the 22 failed compliance concerns. Selecting the first item opens a details pane (2), for that particular finding. The detail pane includes an overview as well as the actual audit output.

The screenshot shows the Tenable Vulnerability Management interface. At the top, there's a navigation bar with 'tenable Vulnerability Management' and 'Findings'. Below that, there are tabs for 'Vulnerabilities', 'Cloud Misconfigurations', 'Host Audits', and 'Web Application Findings'. A search filter is applied: '(Compliance Framework is equal to PCI-DSSv4.0 AND Compliance Family Name is equal to "Build and Maintain a Secure Network and Systems" AND Last Audited within last 90 days) AND Result is equal to Failed AND Compliance Control is equal to 1.5.1'. A table lists findings, with the first one selected. A red arrow labeled '1' points to the first row of the table. A second red arrow labeled '2' points to the details pane for the selected finding.

Audit Name	Audit File	Result	Asset Name	State	Asset Tags	Actions
<input checked="" type="checkbox"/> 3.5.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Failed	demoio-gcp-prod-us-east4-debian9-1.c...	Active	Cody: SaITest	
<input type="checkbox"/> 3.3.1 Ensure TCP Wrappers is installed	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Failed	demoio-gcp-prod-us-east4-debian9-1.c...	Active	Cody: SaITest	
<input type="checkbox"/> 3.5.2.1 Ensure IPv6 default deny firewall policy - Chain INPUT	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Failed	demoio-gcp-prod-us-east4-debian9-2.c...	Active	Cody: SaITest	
<input type="checkbox"/> 3.5.1.1 Ensure default deny firewall policy - Chain INPUT	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Failed	demoio-gcp-prod-us-east4-debian9-2.c...	Active	Cody: SaITest	

3.5.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT

Asset Information

NAME: [REDACTED]
IPV4 ADDRESS: [REDACTED]
OPERATING SYSTEM: Linux Kernel 4.9.0-8-amd64 on Debian 9.7
SYSTEM TYPE: general-purpose
NETWORK: Default
DNS (FQDN): [REDACTED]

Asset Scan Information

FIRST SEEN: 10/22/2023 at 09:01 PM
LAST SEEN: 08/12/2024 at 07:07 AM
LAST AUTHENTICATED SCAN: 08/12/2024 at 07:07 AM
LAST LICENSED SCAN: 08/12/2024 at 07:07 AM

Host Audit Information

AUDIT NAME: 3.5.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT
AUDIT FILE: CIS_Debian_Linux_9_Server_v1.0.1_L1.audit
BENCHMARK: CIS Debian 9 v1.0.1
BENCHMARK SPECIFICATION NAME: CIS Debian 9
BENCHMARK VERSION: 1.0.1
PLUGIN NAME: Unix Compliance Checks
RESULT: Failed
STATE: ACTIVE

Audit Discovery

FIRST SEEN: 10/22/2023 at 09:02 PM

Overview | Audit Output

Description

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to write list acceptable usage than to black list unacceptable usage.

Solution

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP  
# iptables -P OUTPUT DROP  
# iptables -P FORWARD DROP
```

The specific PCI-DSSv4 requirements referenced in this widget are: 1.4.3 | 2.2.2 | 1.5.1 | 1.2.1 | 1.3.1 | 2.2.3 | 1.4.2 | 1.4.5 | 2.2.4 | 1.4.1 | 1.3.2 | 1.1.2 | 2.2.7.

Dashboards such as the Compliance Benchmarks by Category dashboards, available for:

- [Microsoft Security Compliance Toolkit \(MSCT\)](#)
- [Tenable Best Practices \(TNS\)](#)

- [Defense Information Systems Agency \(DISA\)](#)
- [Center for Internet Security \(CIS\)](#)

The screenshot displays a Tenable Vulnerability Management interface with four main dashboard panels, each showing compliance benchmarks by plugin category. The panels are:

- Computer:** Shows benchmarks for DISA, TNS, and MSCT. The MSCT table includes columns for PASSED, FAILED, and WARNING.
- Network:** Shows benchmarks for MSCT with columns for FAILED, WARNING, and PASSED.
- Application:** Shows benchmarks for MSCT with columns for WARNING, ERROR, PASSED, and FAILED.
- Cloud:** Shows benchmarks for MSCT with columns for WARNING, ERROR, PASSED, and FAILED.

Each dashboard includes a table of results and a 'Jump to Dashboard' button. The interface also features a sidebar with category filters and a top navigation bar with 'Quick Actions' and 'CE' icons.

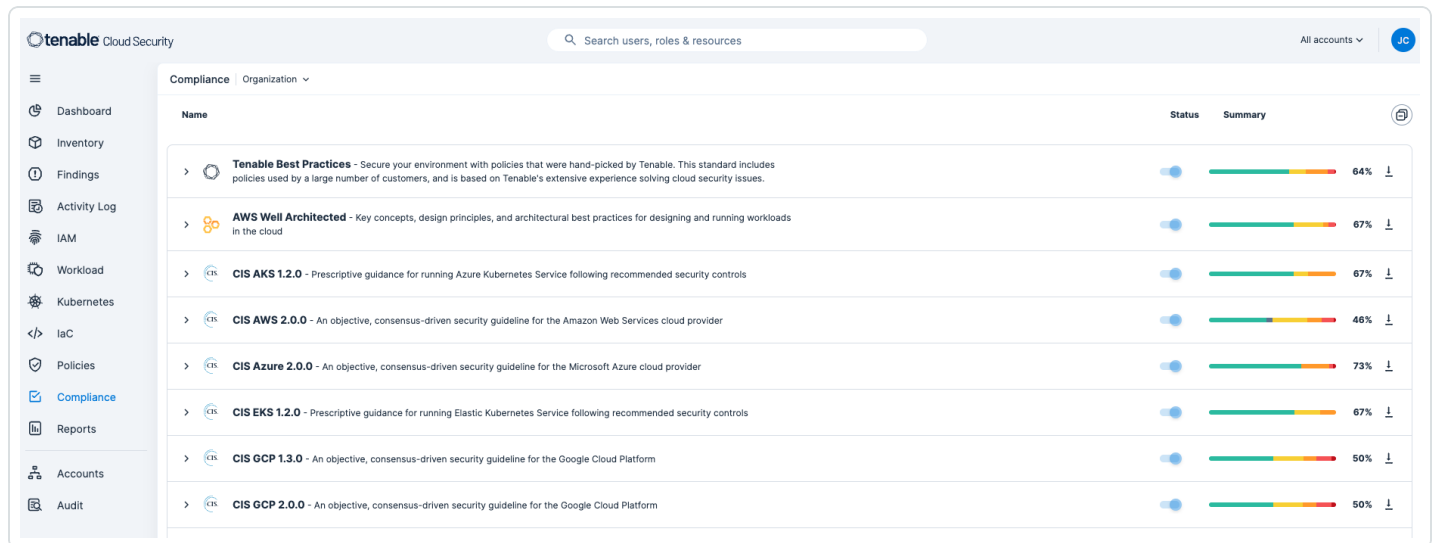
These dashboards for Tenable Vulnerability Management focus on best practice checks for the following four categories, Computer, Network, Application, and Cloud. This information allows organizations to review information related to secure systems configuration and systems hardening related to a specific set of compliance standards. Similarly, the [CIS Audit Summary Dashboard](#) for Tenable Security Center provides compliance results for numerous devices.

Cloud Environments

Cloud services are an integral part of business operations, offering scalability, flexibility, and accessibility. Cloud environments store vast amounts of sensitive data, including personal information, financial records, intellectual property, and proprietary business data. Ensuring robust security measures protects this information from unauthorized access, breaches, or theft.

Protecting cloud environments is vital for protecting data, ensuring compliance with regulatory requirements, maintaining operational continuity, managing risks, and optimizing business efficiency. Tenable Cloud Security provides out-of-the-box, continuously updated support for all major compliance frameworks, and best practices. Tenable Cloud Security provides the ability to create customized frameworks to meet the exact needs of your organization. Using customized reports, communicate with stakeholders on internal compliance, external audit and daily security activities.

Compliance reporting is available by navigating to the Compliance tab. On the Compliance dashboard, analysts have the option to select the appropriate compliance benchmark from the list. By default, this dashboard reports compliance details for all Benchmarks combined if no option is selected.



The screenshot displays the Tenable Cloud Security interface. The top navigation bar includes the Tenable logo, a search bar for users, roles, and resources, and a user profile icon labeled 'JC'. The left sidebar contains a menu with options: Dashboard, Inventory, Findings, Activity Log, IAM, Workload, Kubernetes, IaC, Policies, Compliance (highlighted), Reports, Accounts, and Audit. The main content area is titled 'Compliance | Organization' and features a table of benchmarks. Each row includes a name, a status indicator (a blue circle), a progress bar, a percentage, and a downward arrow icon.

Name	Status	Summary
Tenable Best Practices - Secure your environment with policies that were hand-picked by Tenable. This standard includes policies used by a large number of customers, and is based on Tenable's extensive experience solving cloud security issues.		64% ↓
AWS Well Architected - Key concepts, design principles, and architectural best practices for designing and running workloads in the cloud		67% ↓
CIS AKS 1.2.0 - Prescriptive guidance for running Azure Kubernetes Service following recommended security controls		67% ↓
CIS AWS 2.0.0 - An objective, consensus-driven security guideline for the Amazon Web Services cloud provider		46% ↓
CIS Azure 2.0.0 - An objective, consensus-driven security guideline for the Microsoft Azure cloud provider		73% ↓
CIS EKS 1.2.0 - Prescriptive guidance for running Elastic Kubernetes Service following recommended security controls		67% ↓
CIS GCP 1.3.0 - An objective, consensus-driven security guideline for the Google Cloud Platform		50% ↓
CIS GCP 2.0.0 - An objective, consensus-driven security guideline for the Google Cloud Platform		50% ↓

To view details, analysts can drill down into any of the findings. In this example, drilling down into the **CIS AWS 2.0.0** item provides details on the root account.

- Dashboard
- Inventory
- Findings
- Activity Log
- IAM
- Workload
- Kubernetes
- IaC
- Policies
- Compliance
- Reports
- Accounts
- Audit

Compliance Organization

Name	Status	Summary										
Tenable Best Practices - Secure your environment with policies that were hand-picked by Tenable. This standard includes policies used by a large number of customers, and is based on Tenable's extensive experience solving cloud security issues.		64%										
AWS Well Architected - Key concepts, design principles, and architectural best practices for designing and running workloads in the cloud		67%										
CIS AKS 1.2.0 - Prescriptive guidance for running Azure Kubernetes Service following recommended security controls		67%										
CIS AWS 2.0.0 - An objective, consensus-driven security guideline for the Amazon Web Services cloud provider		46%										
1. Identity and Access Management		43%										
1.4 Ensure no root user account access key exists The root user account is the most privileged user in an AWS account. AWS Access Keys provide programmatic access to a given AWS account. It is recommended that all access keys associated with the root user account be removed.		100%										
<table border="1"><thead><tr><th>Platform</th><th>Policy</th><th>Failed Resources</th><th>Scanned Resources</th><th>Summary</th></tr></thead><tbody><tr><td>aws</td><td>RootUser.has.access.key</td><td>0 rootUsers</td><td>2 root users</td><td></td></tr></tbody></table>	Platform	Policy	Failed Resources	Scanned Resources	Summary	aws	RootUser.has.access.key	0 rootUsers	2 root users			
Platform	Policy	Failed Resources	Scanned Resources	Summary								
aws	RootUser.has.access.key	0 rootUsers	2 root users									
1.5 Ensure MFA is enabled for the "root user" account The root user account is the most privileged user in an AWS account. Multi-factor Authentication (MFA) adds an extra layer of protection on top of a username and password.		0%										
1.7 Eliminate use of the root user for administrative and daily tasks The root user has unrestricted access to and control over all resources in the AWS account. It is highly recommended that the use of this account be avoided for everyday tasks.		100%										

Control Objective 2: Protect Account Data

This includes protecting stored cardholder data, encrypting transmission of cardholder data across networks, and ensuring encryption keys are stored properly. This control objectives covers the following PCI DSS requirements:

Requirement 3: and passively detected assets

Requirement 4: Asset discovery statistics

Note: Notes related to Requirement 3. This requirement is related to the controls around account data that is printed or stored in any form. Account data is both cardholder data and sensitive authentication data. While this requirement is not supported by Tenable directly, the recommended practice here is to keep storage of account data to a minimum. Do not store sensitive authentication data (SAD) after authorization. Restrict the display of the full primary account number (PAN) and cardholder data. And secure the PAN, account data, and any cryptographic keys used to protect the data when they are stored.

PCI Requirements Under This Objective Supported by Tenable

Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks

Requirement 4 applies only to the transmissions of PAN unless specifically called out in an individual requirement. PAN transmissions can be protected by encrypting the data before transmission, or by encrypting the session over which the data is transmitted or both. PCI DSS v4 does not require that strong cryptography be applied at both the data level and the session level, but they do recommend both.

At the session level, system configurations should be verified to ensure strong cryptography and security protocols are implemented, and that keys and/or certificates that can not be verified are rejected. Some protocol implementations, such as SSL, SSH v1.0, and earlier versions of TLS have known vulnerabilities. Entities should be aware of industry defined depreciation dates for the cipher suites that are in use. Certificates should be verified to ensure integrity of all secure connections.

For Tenable Vulnerability Management the Protect Account Data widget provides details on each of the compliance controls for the compliance family group being referenced.

Protect Account Data - PCI-DSSv4.0 (Explore) ⓘ

	FAILED	PASSED
4.2.1	57	42
3.5.1	14	14
3.3.2	14	14

This widget focuses on the category Protect Account Data, which covers topics within PCI requirement 3 and 4. Both of these requirements cover protecting stored cardholder data, and the encrypted transmission of cardholder data. This widget provides details on each of the compliance controls for the compliance family group being referenced. The compliance control reference number is followed by a count, and compliance result for the compliance control. The specific controls being referenced are: 4.2.1 | 3.5.1 | 3.3.2 | 3.2.1

Compliance Audit Files

Additionally, audit files such as the TNS File Analysis - Credit Card Number audit file contains a number of file content checks. Files such as pdf, docx, txt, xls and more, are searched using this audit file for major credit cards (American Express, Discover, Maestro, MasterCard, VISA, UnionPay) and any potential credit card number, CVV or PIN. This .audit file searches the first 50k bytes looking for valid credit card numbers using regular expressions. Since potential credit card data may be found only the last four digits of the number are shown in the output. An example is shown below:

```
<item>
  type      : FILE_CONTENT_CHECK
  description : "PII - Determine if a file contains a valid American Express credit card number."
  file_extension : "pdf" | "doc" | "xls" | "xlsx" | "xlsm" | "xlsb" | "xml" | "ltx" | "ltxm" | "docx"
  | "docm" | "dotx" | "dot" | "txt"
  regex     : "([^\0-9-]|^)(3[47][0-9]{2}(|-|)[0-9]{6}(|-|)[0-9]{5})([^\0-9-]|$)"
  expect    : "American Express" | "CCAX" | "amex" | "credit" | "AMEX" | "CCN"
  max_size  : "50K"
  only_show : "4"
  regex_replace : "\3"
</item>
```

Secure Sockets Layer

SSL and TLS are both cryptographic protocols which provide data encryption between network devices. The National Institute of Standards and Technology has stated that Secure Sockets Layer (SSL) v3.0 is no longer acceptable for protection of data due to inherent weakness within the protocol. As such, no version of SSL meets the PCI DSS definition of "strong cryptography."

SSL remains a common component of web security to encrypt data being transmitted between a browser and website, ensuring that sensitive information, such as login information and payment details are protected from eavesdropping. Therefore organizations should assess all their SSL/TLS implementations. Dashboards such as the [Maintaining Data Protection Controls](#) for Tenable Security Center, contain components which report on SSL/TLS, Encryption, Certificate Status, and more, assisting organizations in demonstrating to third parties and regulatory bodies that sensitive data is protected in accordance with Data Loss Prevention requirements.

tenable.sc Dashboard Solutions Analysis Scans Reporting Assets Workflow Users

Maintaining Data Protection Controls Refresh All Switch Dashboard Options

Encryption - Cryptographic Compliance Concerns

88 Items | 1 to 5 of 88 | Page 1 of 18

PLUGIN ID	NAME	SEVERITY	TOTAL
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium	2438
65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	680
35291	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	668
69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Low	313
70658	SSH Server CBC Mode Ciphers Enabled	Low	291

Last Updated: 4 hours ago

Removable Media and Content Audits - CDROM, Floppy, Other Storage Audit Checks

Passed	Manual	Failed
BitLocker	BitLocker	BitLocker
CDROM	CDROM	CDROM
Remote Storage	Remote Storage	Remote Storage
Removable Media	Removable Media	Removable Media
Removable Storage	Removable Storage	Removable Storage
floppy	floppy	floppy

Last Updated: 9 minutes ago

Data Protection - Data at Rest - Encryption Compliance

6 Items | 1 to 5 of 6 | Page 1 of 2

NAME	SEVERITY	TOTAL
6.14 Ensure Configuration File Encryption is Set	High	3
18.9.67.3 Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	High	2
1.5.9 Ensure NIST FIPS-validated cryptography is configured - rpm	High	1
1.5.9 Ensure NIST FIPS-validated cryptography is configured - proc	High	1
1.5.9 Ensure NIST FIPS-validated cryptography is configured - grub	High	1

Last Updated: 4 hours ago

Data Protection - Confidentiality of Protected Information Concerns

10 Items | 1 to 5 of 10 | Page 1 of 2

NAME	SEVERITY	TOTAL
18.8.53.1.2 Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) - Disabled	High	1
2.3.7.6 Ensure 'interactive logon: Number of previous logons to cache (in case domain controller is ...	High	1
18.8.37.1 Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) - E...	High	1
18.8.28.4 Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) - ...	High	1
18.3.1 Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS onl...	High	1

Last Updated: 22 hours ago

SSL/TLS Discovery - SSL/TLS Vulnerabilities By Type

	Systems	Active	Passive
SSLv2	14	30	0
SSLv3	277	698	27
TLS 1.0 (Deprecated)	2087	2491	0
TLS 1.1	2115	4989	13
TLS 1.2	2182	4870	1279
TLS 1.3	6	12	0

Last Updated: 9 minutes ago

Windows File Contents Audit Results - Compliance Summary

	Passed	Manual Check	Failed
Check Count	0	0	0
Check Ratio	0	0	0
System Count	0	0	0
System Ratio	0	0	0

Last Updated: 9 minutes ago

Unix File Contents Audit Results - Compliance Summary

	Passed	Manual Check	Failed
Check Count	0	0	0
Check Ratio	0	0	0
System Count	0	0	0
System Ratio	0	0	0

Last Updated: 9 minutes ago

Data Protection - Certificate Status

Certs Found	Expired Certs	Certs Expiring Soon	Untrusted SSL Certs	Self-Signed Certs	Weakness
2217	108	334	2197	2135	581

Last Updated: 3 hours ago

Data Protection - Removable Media noexec, nosuid, nodev Compliance

12 Items | 1 to 6 of 12 | Page 1 of 2









NAME	SEVERITY	TOTAL
1.1.18 Ensure nodev option set on removable media partitions	High	5
1.1.19 Ensure nosuid option set on removable media partitions	High	5
1.1.20 Ensure noexec option set on removable media partitions	High	5
1.1.22 Ensure nodev option set on removable media partitions	Medium	4
1.1.23 Ensure nosuid option set on removable media partitions	Medium	4
1.1.24 Ensure noexec option set on removable media partitions	Medium	4

Last Updated: 27 minutes ago

Tenable Vulnerability Management widgets such as the **SSL Certs That are Expired or Soon-to-Expire** and the **SSL -TLS Insecure Communications Issues and Info** widgets, list assets that have SSL Certificates that have already expired or will soon expire and current SSL and TLS insecure communication exposures in the environment respectively.



SSL - TLS Insecure Communications Issues and Info (Explore) ⋮

Updated 5/20/2024

Plugin Name	First Value of Severity	Count
SSL Certificate Cannot Be Trusted	 Medium	123
SSL Self-Signed Certificate	 Medium	84
SSL RC4 Cipher Suites Supported...	 Low	81
SSL 64-bit Block Size Cipher Sult...	 Medium	78
TLS Version 1.0 Protocol Detection	 Medium	64
TLS Version 1.1 Protocol Depreca...	 Medium	60
SSL Medium Strength Cipher Sult...	 High	57
SSL Expired Certificate Detection	 Medium	37

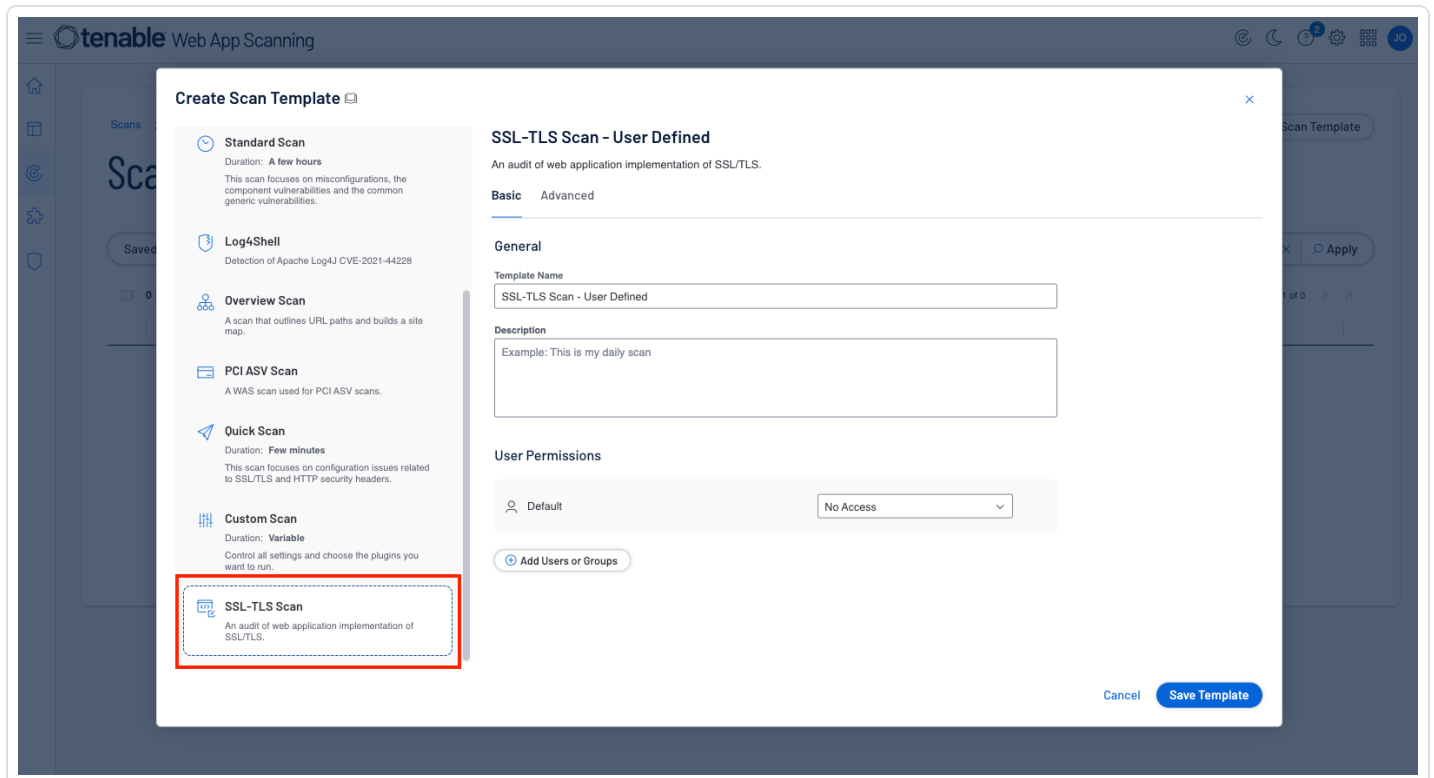
SSL Certs That are Expired or Soon-to-Expire (Explore) ⋮

Updated 5/20/2024

Plugin Name	First Value of Severity	Count
SSL Certificate Expiry	 Medium	27
SSL Certificate Chain Contains Ce...	 Info	9
SSL Certificate Expiry - Future Ex...	 Info	9

Web Application Scanning

Tenable Web App Scanning contains a predefined scan policy which allows for deep analysis of the SSL configuration of a web server on the public internet. This scan result provides insight into the organization's SSL/TLS configuration based on industry standards.



Control Objective 3: Maintain a Vulnerability Management Program

This objective focuses on proactively updating antivirus software, maintaining secure systems and applications, and implementing strong access control methods. All systems that are susceptible to malware are protected with antivirus software. All antivirus software should be kept up to date. Malware detection scans are run periodically, and all infected systems should be remediated. Patches and updates should be installed within one month of release for critical systems. Maintaining a strong vulnerability management program ensures that security concerns are addressed before they can be exploited, safeguarding cardholder data and meeting PCI DSS compliance standards.

This control objectives covers the following PCI DSS requirements:

Requirement 5: Protect all systems and networks from malicious software.

Requirement 6: Develop and maintain secure systems and software.

PCI Requirements Under This Objective Supported by Tenable

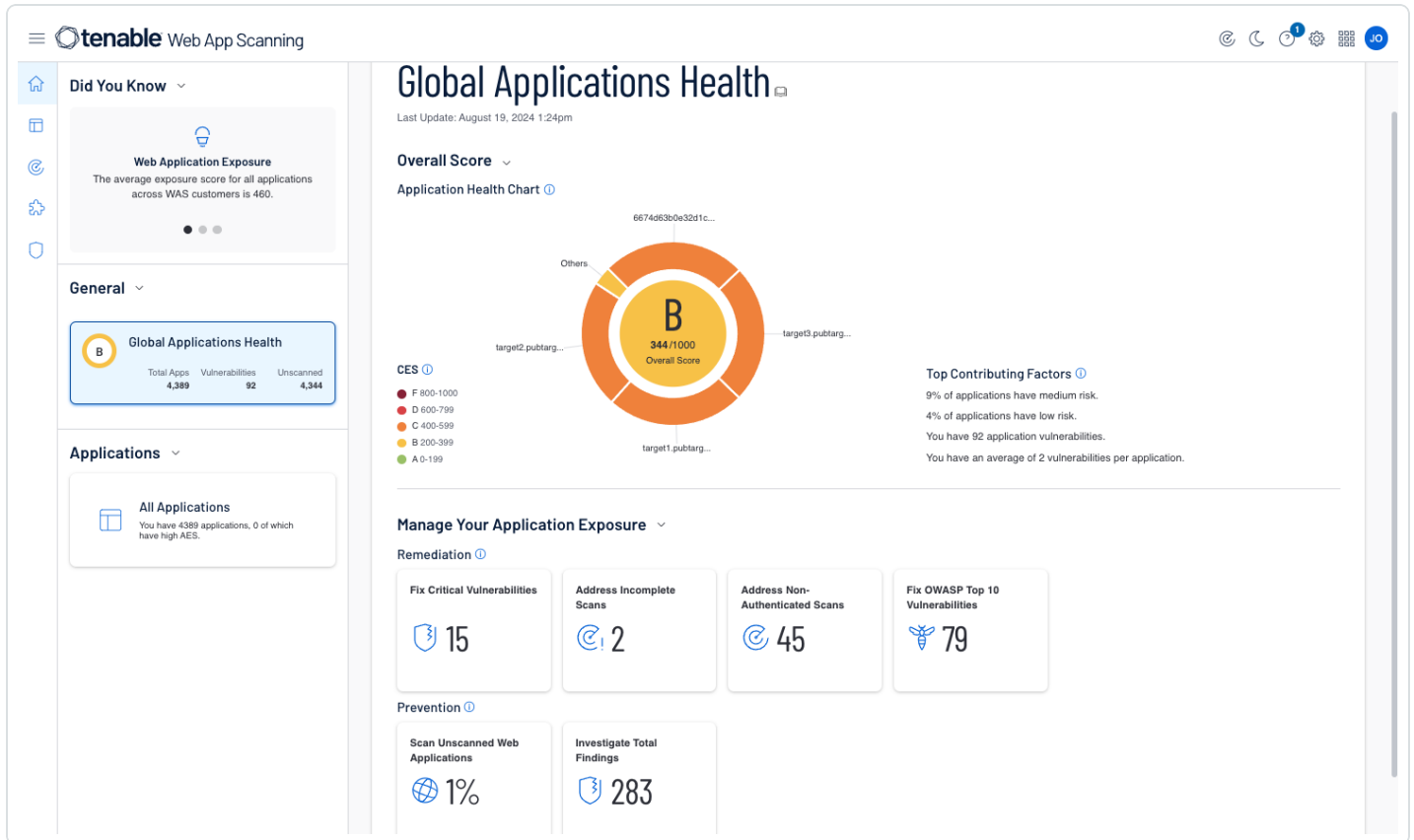
PCI Requirement 5: Protect All Systems and Networks from Malicious Software

Malicious software, often referred to as malware is any software that is designed to harm, exploit, or otherwise compromise the confidentiality, integrity, or availability of a computer system, network, or device. Included are a variety of tactics such as viruses, ransomware, spyware, and adware. Malware can enter the environment through many business approved activities, such as email, or the approved use of storage devices. Using antivirus or anti-malware software, combined with a robust vulnerability scanning program helps address these concerns. Performing periodic scanning or continuous monitoring of the environment will help ensure that previously undetected malware is identified. Scans should include all systems in the CDE.

When protecting systems and networks is paramount, Tenable has a comprehensive security solution that provides continuous visibility, critical context and actionable intelligence. These products provide purpose built PCI compliance dashboards, Assurance Report Cards (ARCs) to assist organizations in monitoring ongoing compliance with PCI DSS.

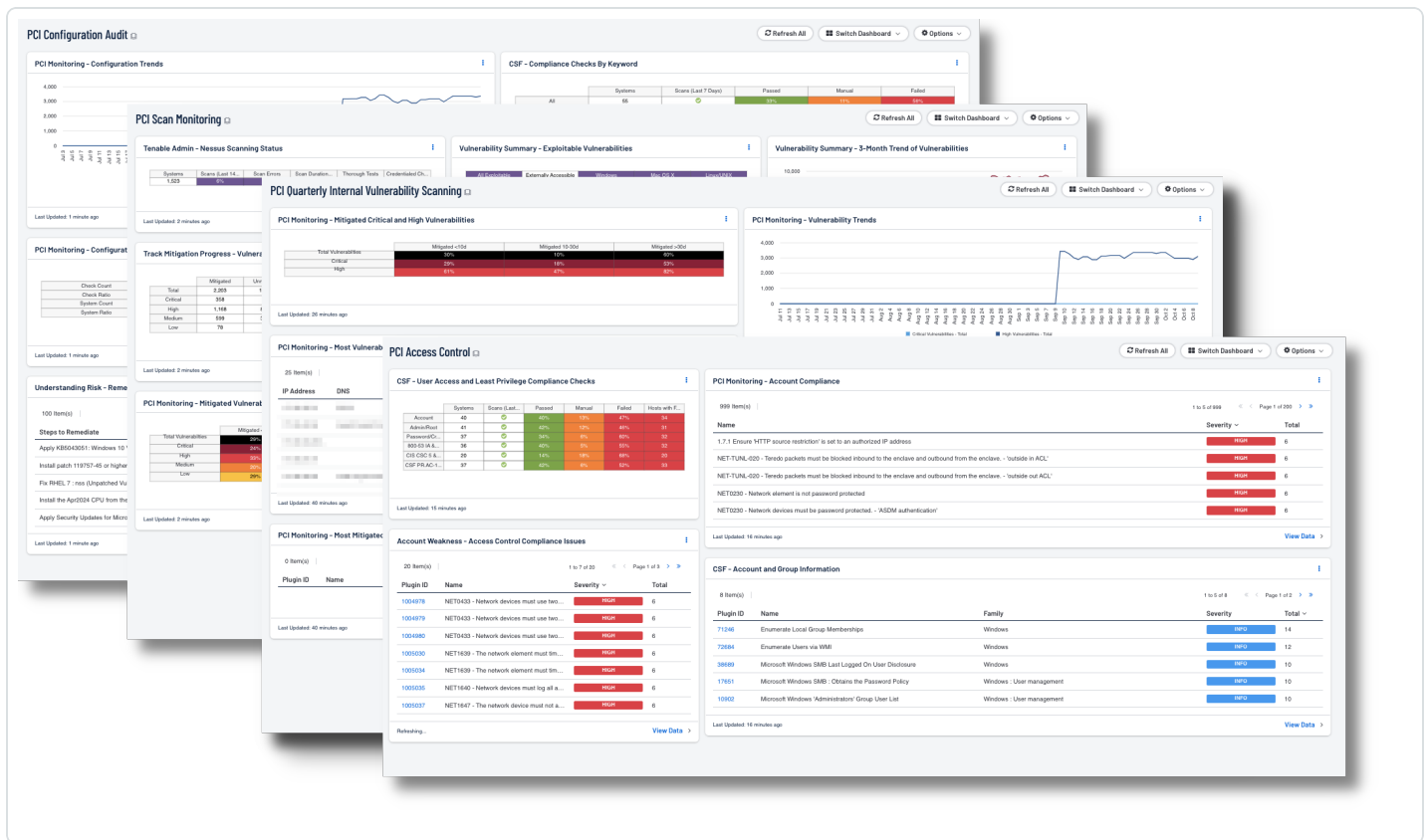
Web Application Scanning

Tenable Web App Scanning provides comprehensive vulnerability scanning for modern web applications. Accurate vulnerability coverage minimizes false positives and false negatives to ensure that security teams understand the true security risks in their web applications. Tenable Web App Scanning provides safe external scanning so that production web applications do not experience disruptions or delays. Information presented allows organizations to categorize findings and remediate vulnerabilities quickly.



Tenable Security Center

There are a series of PCI dashboards for Tenable Security Center that assist in supporting an organization's PCI compliance journey. These dashboards focus on PCI control objectives. The information contained within the dashboards provide insight to help organizations secure their systems against vulnerabilities that could lead to data breaches.



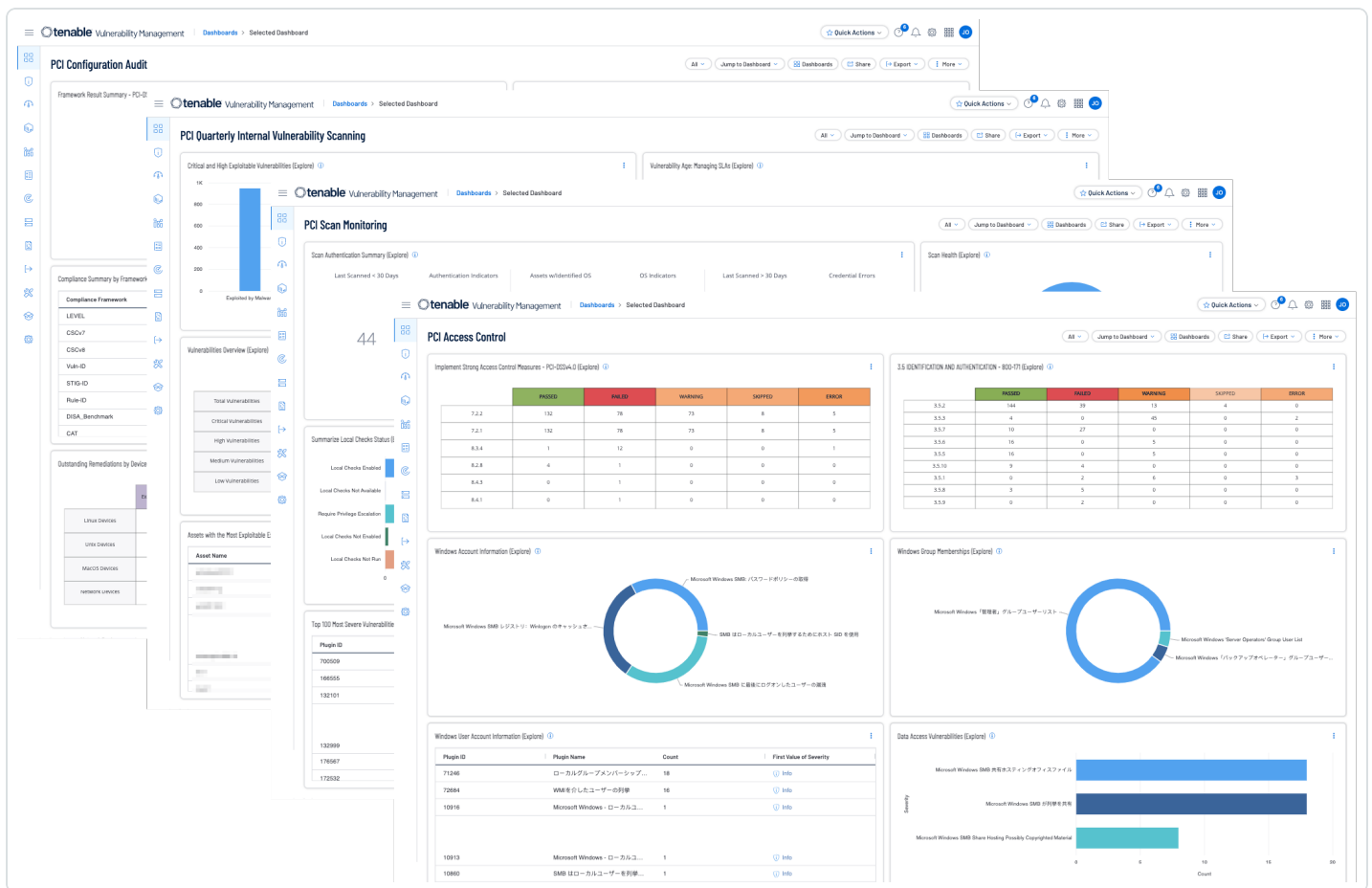
Within the Access Control dashboard, user account focused widgets are provided to help analysts see activities detected in the organization around user accounts. All user accounts such as regular user accounts and administrative accounts should be monitored for unusual activity. Multiple industry recommendations from standards such as PCI and NIST CyberSecurity Framework (CSF) are provided to help analysts see potential malicious indicators around user accounts. Examples of these indicators, such as privilege changes and group membership changes, alert analysts as changes may not be expected and should be validated. Analysts can use these widgets to help determine what typical activity should be on a network and then be more aware of when abnormal activity takes place within the organization.

The PCI Scan Monitoring dashboard provides security teams with detailed insight into their organization and vulnerability management posture. Vulnerabilities are filtered by severity and exploitability to identify at-risk hosts. Detailed information about remediation opportunities and risk issues are presented. Indicator matrices alert to the detection of specific exploitable vulnerabilities and patch management details. Nessus scans are monitored for progress and errors, and vulnerability trend data is presented. By effectively monitoring the network for vulnerabilities and remediation options, security teams can better ensure network integrity and security.

The PCI Configuration Audit dashboard presents extensive data about the configuration status of the network based on the available data. The dashboard can be used to gain insight into all configuration results, or can be modified to focus exclusively on the results related to the cardholder data environment (CDE). Organizations can configure repositories or asset lists in order to tailor the focus of the dashboard.

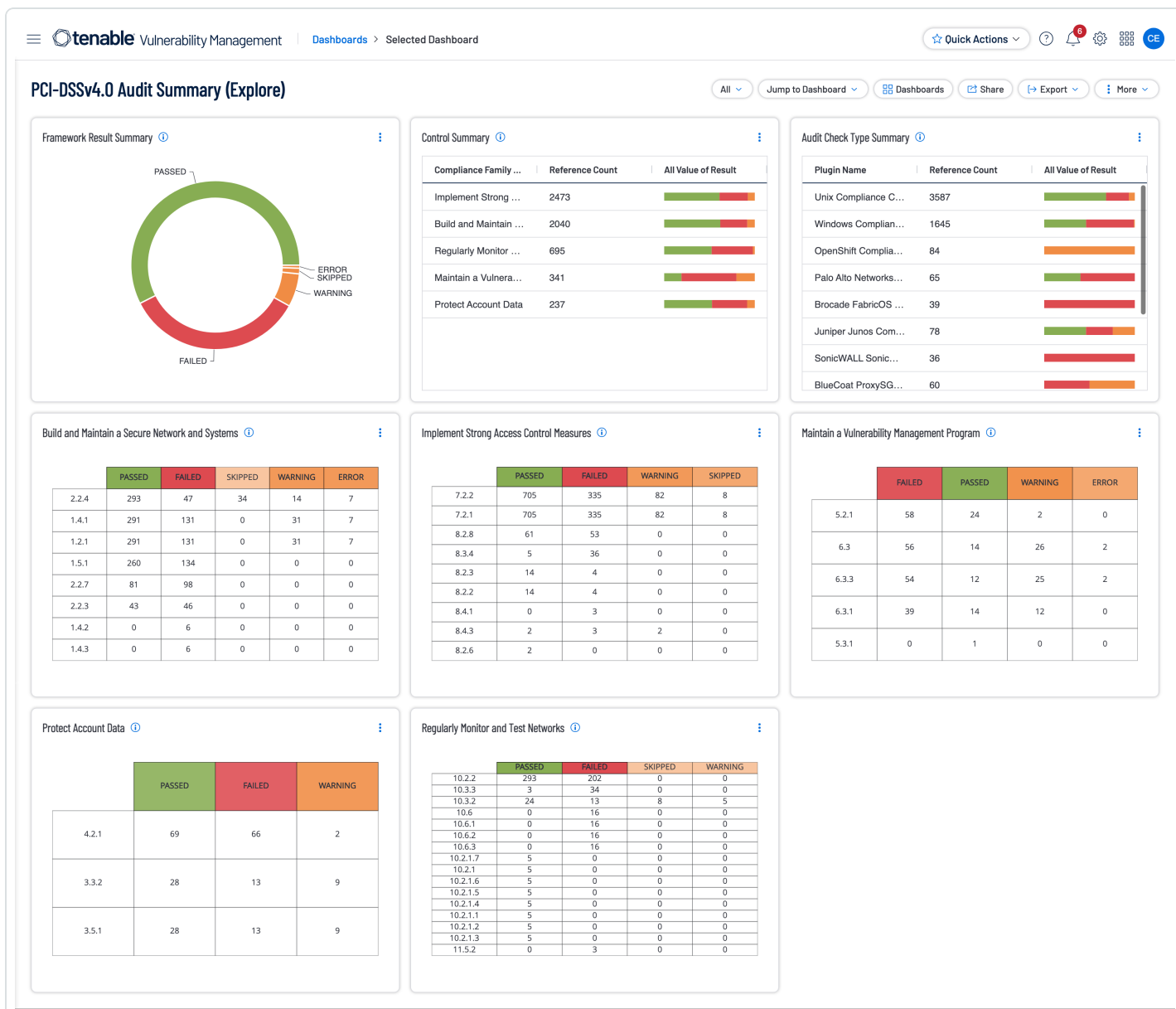
The PCI Quarterly Internal Vulnerability Scanning dashboard presents extensive data about the vulnerability status of the network based on the available data. The dashboard can be used to gain insight into all vulnerability results, or can be modified to focus exclusively on the results related to the cardholder data environment (CDE). Organizations can configure repositories or asset lists in order to tailor the focus of the dashboard.

A similar series of dashboards exist for Tenable Vulnerability Management.



Tenable Vulnerability Management

Tenable Vulnerability Management PCI-DSSv4.0 Audit Summary dashboard.



Antivirus

There are a number of plugins available which detect if an antivirus product is installed, running, and up-to-date. These include:

- [24232](#) BitDefender Check
- [20284](#) Kaspersky Anti-Virus Check
- [12107](#) McAfee Anti Virus Check
- [21608](#) NOD32 Antivirus System Check

- [12106](#) Norton Anti Virus Check
- [12215](#) Sophos Anti Virus Check
- [20283](#) Panda Antivirus Check
- [21725](#) Symantec Anti Virus Corporate Edition Check
- [16192](#) Trend Micro Anti Virus Check
- [24344](#) Windows Live OneCare AntiVirus Check

PCI Requirement 5.3 requires that anti-malware mechanisms and processes are active, maintained, and monitored. For anti-malware solutions to be effective, they need to be functional, and have the latest updates and signatures. The above plugins only report an issue if a problem is found with the detected antivirus solution. Nessus also has plugin #[16193](#) which aggregates the results from these and other plugins. This is useful if you are in a multiple anti-virus solution environment and just want to find hosts that have a solution installed and operational. While the individual product detect plugins only report an issue if a problem is found with the detected antivirus solution, plugin [16193](#) reports if a system does have a known working anti-virus solution. Further details can be viewed by reviewing the plugin output. In this example, the plugin output for 16193 displays the antivirus application, file path, version, antivirus engine version, and antivirus signature version.

The screenshot shows the Nessus Findings interface. At the top, there are tabs for 'Vulnerabilities', 'Cloud Misconfigurations', 'Host Audits', and 'Web Application Findings'. A search filter is applied: 'Plugin ID: is equal to 16193'. Below the search bar, a table lists findings. The first finding is highlighted, showing 'Antivirus Software Check' with a severity of 'Info' and a state of 'New'. A red arrow points from this finding to the detailed view below.

Antivirus Software Check

Asset Information

- NAME: [REDACTED]
- IPV4 ADDRESS: [REDACTED]
- OPERATING SYSTEM: Microsoft Windows Server 2022 Standard Build 20348
- SYSTEM TYPE: general-purpose
- NETWORK: Default
- DNS (FQDN): [REDACTED]

Additional Information

- CLOUD MISCONFIGURATIONS: 0
- ASSET SCAN INFORMATION: FIRST SEEN 10/31/2023 at 09:25 AM, LAST SEEN 10/31/2023 at 09:25 AM, LAST AUTHENTICATED SCAN 10/31/2023 at 09:25 AM

Vulnerability Information

- SEVERITY: Info
- PLUGIN ID: 16193
- PORT: 445
- PROTOCOL: TCP
- LIVE RESULT: No
- DISCOVERY: FIRST SEEN 10/31/2023 at 09:25 AM, LAST SEEN 10/31/2023 at 09:25 AM, VULNERABILITY AGE 293 Days

Overview Plugin Output

Plugin Output

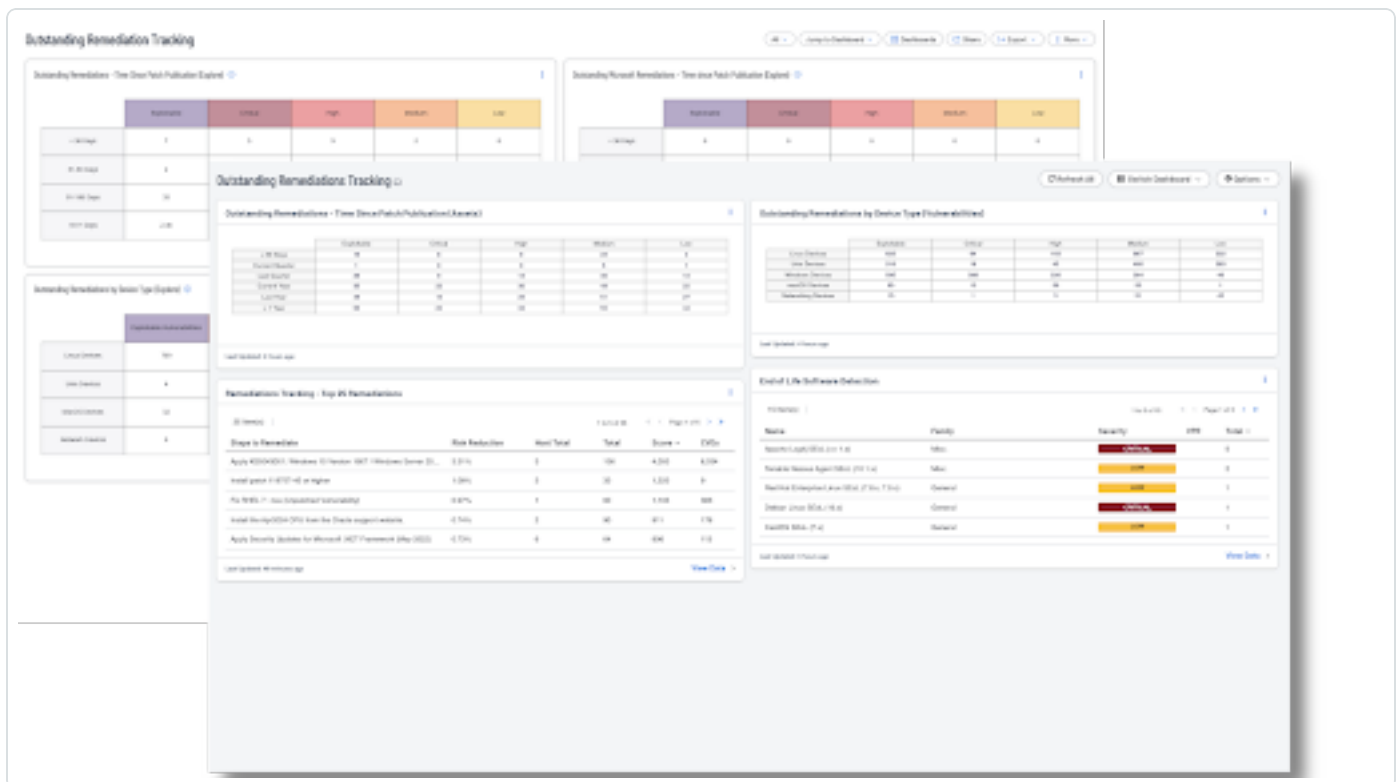
```
Forefront_Endpoint_Protection :
A Microsoft anti-malware product is installed on the remote host :
Product name       : Windows Defender
Path               : C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23090.2008-0\
Version            : 4.18.23090.2008
Engine version     : 1.1.23090.2007
Antivirus signature version : 1.399.1352.0
Antispyware signature version : 1.399.1352.0
```

Requirement 6: Develop and Maintain Secure Systems and Software

Bad actors are always searching for vulnerabilities which can provide an easy method for gaining access to systems and networks. Keeping systems updated and patched mitigate the majority of these potential entryways. PCI DSS requires that all system components have all the appropriate software patches installed to protect against the exploitation and compromise of account data. Appropriate patches are defined by PCI DSS as those patches which have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.

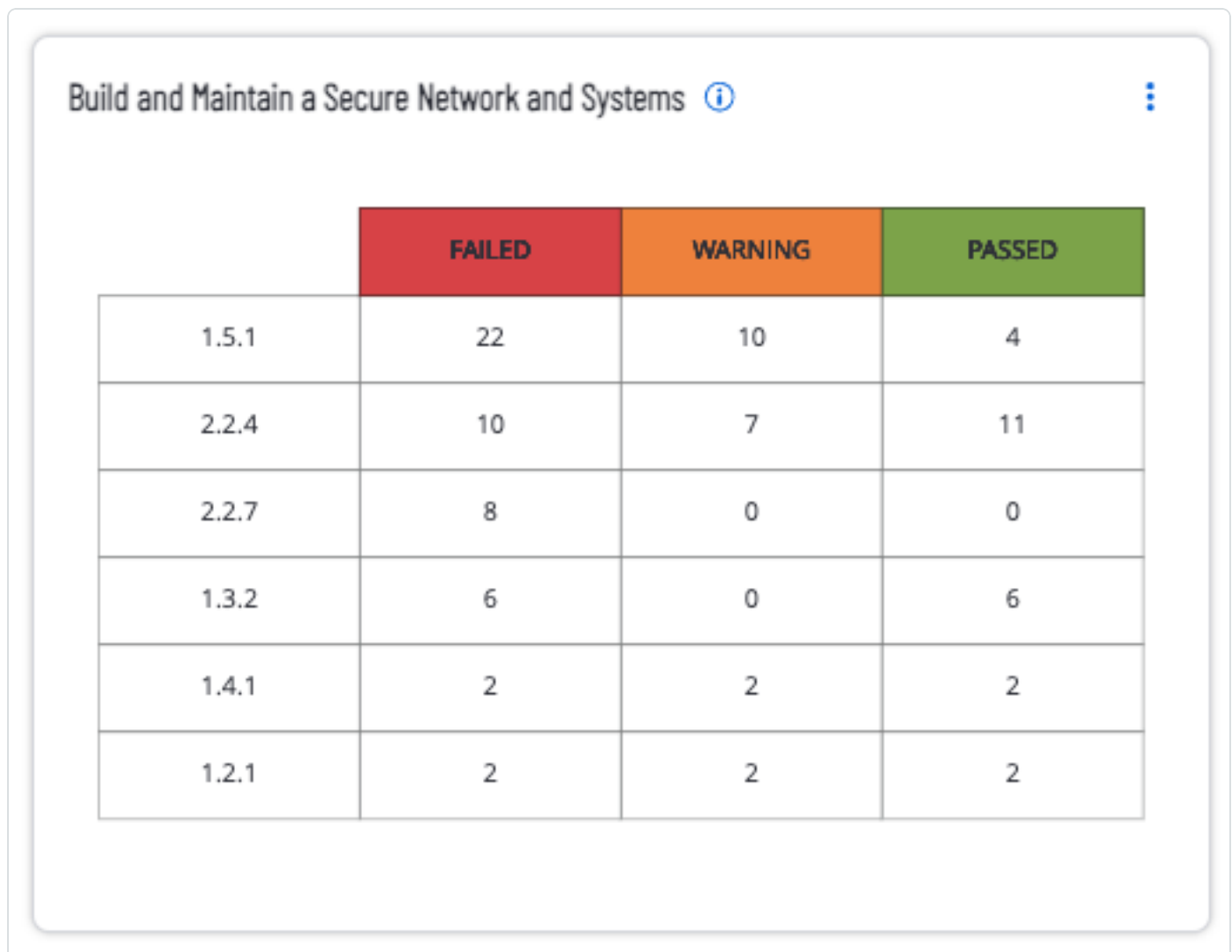
Prioritizing patches for critical infrastructure will ensure that high priority systems and devices are protected from vulnerabilities as quickly as possible after a vendor releases an update. Public facing websites are primary targets for attackers and should be tested for vulnerabilities on a regular basis.

Tracking updates for the constantly changing landscape of assets is important to identify legacy code and asset footprint. The Outstanding Remediations Tracking dashboard, shown below for [Tenable Vulnerability Management](#) and [Tenable Security Center](#), focuses on legacy patches and assets to reduce management effort and reactive firefighting. Organizations can identify parts of their network that have been missed by patching cycles, or where traditional mitigation methods no longer apply.



The Maintain a Vulnerability Management Program widget for Tenable Vulnerability Management focuses on the category Maintain a Vulnerability Management Program, which covers topics within PCI requirement 5 and 6. Both of these requirements cover the need for maintaining a vulnerability

management program to protect systems against malware, and develop and maintain secure systems and applications. This widget provides details on each of the compliance controls for the compliance family group being referenced. The compliance control reference number is followed by a count, and compliance result for the compliance control. The specific controls being referenced are: 5.3.1 | 6.5.3 | 6.3 | 5.3.3 | 6.3.1 | 6.3.3 | 5.3.2 | 5.2.1



The screenshot shows a dashboard titled "Build and Maintain a Secure Network and Systems" with an information icon and a menu icon. Below the title is a table with four columns: a blank header column, "FAILED" (red), "WARNING" (orange), and "PASSED" (green). The table contains six rows of data for different PCI requirements.

	FAILED	WARNING	PASSED
1.5.1	22	10	4
2.2.4	10	7	11
2.2.7	8	0	0
1.3.2	6	0	6
1.4.1	2	2	2
1.2.1	2	2	2

For example, reviewing the details of the cell for failed checks, in the row for PCI Requirement 6.3, clicking within the cell will drill down into the details. The next screen presented is the findings page, shown below:

The image shows a Nessus 'Findings' page. At the top, there are tabs for 'Vulnerabilities', 'Cloud Resources', 'Hosts', and 'Hosts'. A filter bar is present with a dropdown set to 'Compliance Framework is equal to PCI-DSSv4.0 and Compliance Family Name is equal to Maintain a Vulnerability Management Program AND Last audit with last 90 days and Scan Method is not equal to Acceptable AND Result is equal to Failed AND Compliance Control is equal to 6.3'. Below the filter bar, there is a table of audit items. The first item, '1.2.5 Ensure updates, patches, and additional security software are installed', is selected and highlighted in blue. Red arrows point from this item back to the filter bar and from the 'Audit Output' tab in the detailed view to the terminal output. The detailed view includes sections for 'Host Information' (IP: 10.10.10.10), 'Host Audit Information' (CPE: CVE-2013-1234), and 'Audit Details' (Result: Failed). The 'Audit Output' tab shows the terminal output of the command 'yum check-update', which lists several updates available for packages like gcc, perl, and vim, leading to a failed result.

Checking the filters presented allows verification of the data being presented. In this case, Compliance Framework PCI-DSSv4.0, the PCI Objective is to Maintain a Vulnerability Management Program, Results are Failed audit items, and the PCI Requirement is 6.3. Selecting an Audit Item (1.2.5 Ensure updates, patches, and additional security software are installed) presents additional details at the bottom of the page, including the results from a yum check-update command. Nessus ran the command during the audit to check for updates to any installed packages. The results were captured and logged. Those results are available in the Audit Output tab. Since there are a number of updates that are available, this check has failed. Once updates are applied, this audit item will then be displayed in the pass column.

Control Objective 4: Implement Strong Access Control Measures

This objective ensures that access to cardholder data is restricted to only authorized users with a legitimate need. Access is to be controlled by business need-to-know, and each person with computer access is assigned a unique identifier (ID). Access is to be authenticated to all system components ensuring individual accountability. By regulating who has access to certain systems, networks, or files, organizations can reduce the risk of unauthorized actions, data breaches, or fraud. This control objectives covers the following PCI DSS requirements:

Requirement 7: Restrict access to system components and cardholder data by business need-to-know.

Requirement 8: Identify users and authenticate access to system components.

Requirement 9: Restrict physical access to cardholder data. **

Note: ** Notes related to Requirement 9. This requirement is related to the controls around physical access to cardholder data or systems that store, process, or transmit cardholder data. While this requirement is not supported by Tenable directly, the recommended practice here is to restrict data and access to authorized individuals only and remove systems or hard copies containing this data.

PCI Requirements Under This Objective Supported by Tenable

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

Controlling and restricting access to sensitive systems and devices is important for many reasons, especially in protecting cardholder data. Strong access control maintains the confidentiality and integrity of systems, and ensures that only authorized users can access sensitive data, such as financial records, personal information, and proprietary business information. By controlling who can perform certain actions within a system, strong access control prevents unauthorized modifications, deletions, or additions to data, maintaining the integrity and reliability of the systems and information. PCI DSS requires that access levels must be “need to know” and “least privilege”, providing the least amount of access, with minimum privileges to perform a job. These requirements apply to all service and user accounts for employees, contractors, consultants, and internal or external vendors and other third parties.

Requirement 8: Identify users and authenticate access to system components

PCI DSS states, two additional fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity. The identity aspect is the account identifier, such as a user, system, or application ID. The element that proves or verifies the identity is the authentication factor. Authentication factors are something you know, such as a password, something you have, such as a token or smart card, and something you are, such as a biometric element. These elements are based on industry standards and best practices. [NIST 800-63, Digital Identity Guidelines](#) provides additional information.

Tenable Identity Exposure helps organizations validate Active Directory and Entra ID environments for weakness, misconfigurations, and activity that can lead to damaging attacks. Such as removing inactive accounts not used for 90 days, verification of timeouts, or idle time, and Multi-Factor Authentication (MFA).

For more information on getting started with AD Security, and Tenable Identity Management, reference this [Identity and Access Control guide](#).

The Implement Strong Access Control Measures widget covers topics within PCI requirement 7 and 8.

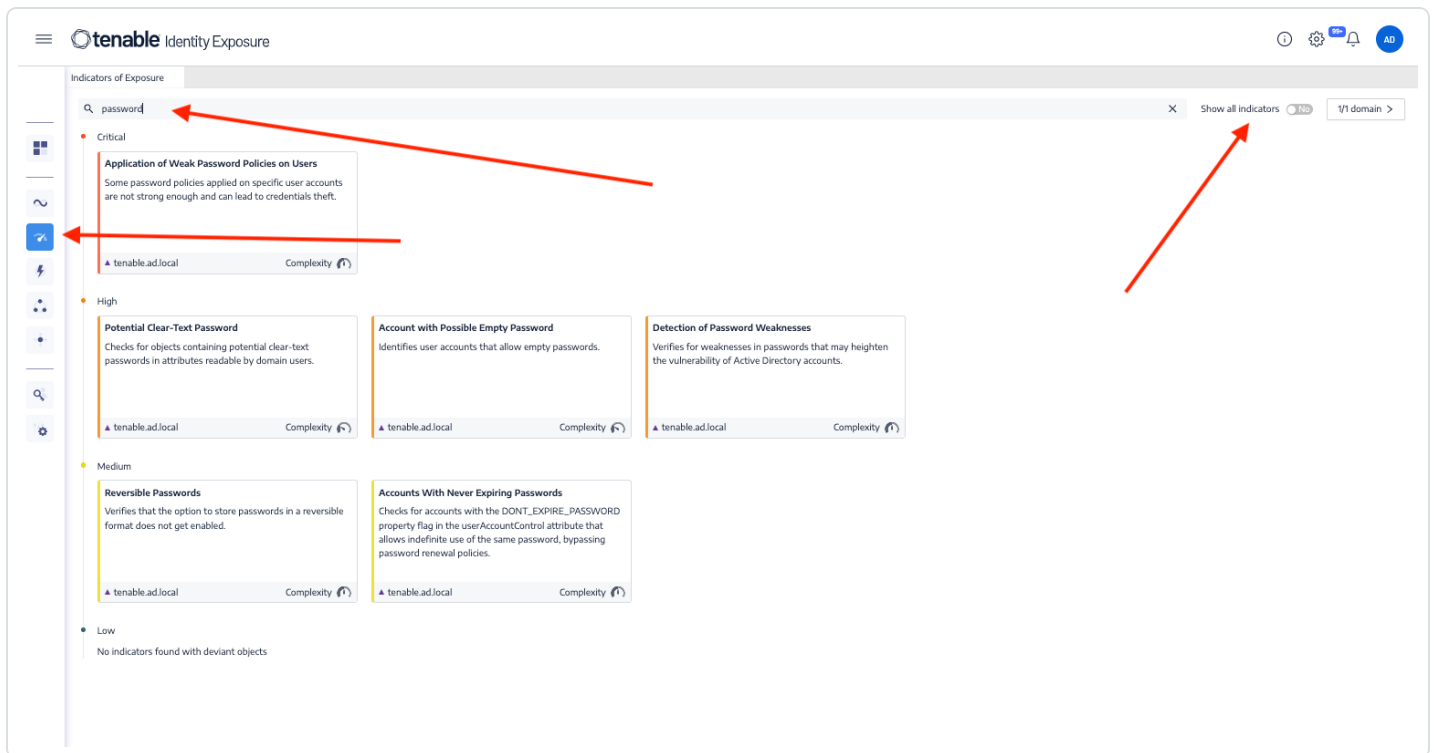
Implement Strong Access Control Measures ⓘ

	PASSED	FAILED	WARNING	SKIPPED	ERROR
7.2.2	289	206	64	8	0
7.2.1	289	206	64	8	0
8.2.8	35	37	0	0	0
8.3.4	1	26	0	0	1
8.2.3	16	6	0	0	0
8.2.2	16	6	0	0	0
8.4.3	0	0	2	0	0
8.4.1	0	0	2	0	0

Audit items checked and validated include, but not limited to: Ensuring accounts are secured, root accounts are secured, permissions to files related to authentication are correct, SELinux policies are configured (if appropriate for the system in question), and more.

Both of these requirements cover the need to restrict access to cardholder data by business need to know, identify and authenticate access to system components, and restrict physical access to cardholder data. This widget provides details on each of the compliance controls for the compliance family group being referenced. The compliance control reference number is followed by a count, and compliance result for the compliance control. The specific controls being referenced are: 8.3.1 | 8.2.2 | 7.2.1 | 8.2.3 | 7.2.2 | 8.4.3 | 8.2.1 | 8.3.4 | 8.2.8 | 8.2.6 | 8.4.1

Tenable Identity Exposure measures security maturity of the AD infrastructure through Indicators of Exposure assigning severity levels to the flow of events that are being monitored and analyzed. Alerts are triggered when security regressions are detected. To view these indicators select the Indicators of Exposure icon from the navigation pane. All Indicators of Exposure can be displayed by toggling the Show all indicators to Yes, or a keyword can be typed into the search pane. In the following example indicators based on the keyword "password" are displayed.



Selecting a result presents a series of details allowing the analyst to view:

- **Information** - Which provides an executive summary, including known attack tools, affected domains, and relevant documentation.
- **Vulnerability Details** - More in-depth information about the misconfiguration.
- **Deviant Objects** - This information highlights misconfigurations in AD that may contribute to broader attacks.
- **Recommendations** - Provides guidance on effective configuration strategies to minimize the attack surface.



Name
Application of Weak Password Policies on Users

Severity
Critical

Status
Not compliant

Latest detection
16:32:20, 2024-03-08

Information Vulnerability details Deviant objects Recommendations

EXECUTIVE SUMMARY

Weak password policies increase the risk of password theft through generic techniques.

DOCUMENTS

- AD DS: Fine-Grained Password Policies
- Configuring Password Policies

ATTACKER KNOWN TOOLS

No tools listed for this indicator.

VULNERABILITY DETAILS

Some privileged users, Windows machines



Name
Application of Weak Password Policies on Users

Severity
Critical

Status
Not compliant

Latest detection
16:32:20, 2024-03-08

Information Vulnerability details Deviant objects Recommendations

DEVIANT OBJECTS

Type an expression.

Type	Object
<input type="checkbox"/>	SYSDVOL
<input type="checkbox"/>	SYSDVOL GptTmpl.inf



Name
Application of Weak Password Policies on Users

Severity
Critical

Status
Not compliant

Latest detection
16:32:20, 2024-03-08

Information Vulnerability details Deviant objects Recommendations

EXECUTIVE SUMMARY

Password policies for user accounts should enforce strong passwords using more than 7 characters and symbols.

DETAILS

Review the password policy of your supervised Active Directory domains to impose complex passwords for various groups of users.

Starting with Windows Server 2008, you can create and assign Password Settings Objects (PSO) objects to users or groups of users to allow for a more refined password policy than for previous Windows versions. Tenable recommends that you use PSO objects instead of the old Default Domain Policy GPO to manage password policies.

To apply these PSO objects it is necessary to raise the level of functionality of the forest to Windows Server 2008 if it is not already done.

TO DEFINE AND ASSIGN A PSO OBJECT TO A GROUP OF USERS, FOLLOW THE PROCEDURES BELOW:

1. Run the *ADSI Edit* tool (either from the MMC snap-in or from the server manager tools) with administrative rights.
2. In the *Select a well-known Naming Context* drop-down box, select *Default Naming Context*, and then click *OK*.
3. Expand *Adsiedit*.
4. Expand *Default Naming Context*.
5. Expand the distinguished name of your domain, e.g. *DC=contoso,DC=com*.
6. Expand the System container, e.g. *CN=System,DC=contoso,DC=com*.
7. Right-click *Password Settings Container*, and select *New* then *Object...*
8. In the *Create Object Editor* tab, select the *msDS-PasswordSettings* attribute, and then click *Next*.
9. Fill the *Common-Name* input box with the chosen name of the PSO object: *password policy for administrators*.
10. Fill the *Password Settings Precedence* input box with the application priority of the PSO object, in the case of multiple objects applying to the same group. The lowest value (or the lowest GUID if two PSOs have the same precedence value) being the highest priority. The lowest value starts with 1.
11. Fill the *Password reversible encryption status for user accounts* input box with the value *False*.
12. Fill the *Password History Length for user accounts* input box with the value *5*.
13. Fill the *Password complexity status for user accounts* input box with the value *True*.
14. Fill the *Minimum Password Length for user accounts* input box with the value *12*.
15. Fill the *Minimum Password Age for user accounts* input box with the minimum time (in days) before a user can change its password.

Select current page 0/2 object sel

Control Objective 5: Regularly Monitor and Test Networks

This includes monitoring all systems/network access and regularly testing systems security and processes. This control objectives covers the following PCI DSS requirements:

Requirement 10: Log and monitor all access to system components and cardholder data.

Requirement 11: Test security of systems and networks regularly.

PCI Requirements Under This Objective Supported by Tenable

Requirement 10: Log and monitor all access to system components and cardholder data

Audit logs are required which capture all individual user access to cardholder data. PCI DSS requirements highlight the criticality of having a process or system that links user access to system components accessed. Log mechanisms which record relevant events are an important component in detecting unauthorized access and potential breaches. Systems should have synchronized clocks to ensure that log entries are consistent and accurately reflect the timing of events.

By keeping logs and monitoring them, organizations not only meet regulatory compliance, they can quickly identify and respond to potential security incidents and breaches. In the event of a data breach, logs provide a crucial understanding of what happened, how the breach may have happened, and the impact of the breach. While Tenable does not directly collect and store system logs, there are several checks that assist organizations with this requirement.

The Regularly Monitor and Test Networks widget within the PCI-DSSv4.0 Audit Summary dashboard covers topics within PCI requirement 10 and 11.

Regularly Monitor and Test Networks ⓘ

	FAILED	PASSED	WARNING	SKIPPED
10.2.2	168	98	1	0
10.3.3	34	3	0	0
10.6.3	13	0	0	0
10.6.2	13	0	0	0
10.6.1	13	0	0	0
10.6	13	0	0	0
10.3.2	9	8	2	8

Both of these requirements cover tracking and monitoring all access to network resources and cardholder data, and the regular testing of security systems and processes. This widget provides details on each of the compliance controls for the compliance family group being referenced. The compliance control reference number is followed by a count, and compliance result for the compliance control. The specific controls being referenced are: 10.2.2 | 10.6.2 | 11.5.2 | 10.2.1 | 10.6.1 | 10.2.1.7 | 10.2.1.5 | 10.3.2 | 10.2.1.2 | 10.4.1.1 | 10.6.3 | 10.2.1.4 | 10.6 | 10.5.1 | 10.2.1.1 | 10.2.1.3 | 10.3.3 | 10.2.1.6

Requirement 11: Test Security of Systems and Networks Regularly

PCI DSS requires that vulnerabilities are identified and assigned a risk ranking based on industry best practices and consideration of potential impact. Continuous vulnerability scanning is essential for maintaining a robust security posture, adapting to changes, ensuring compliance, and effectively managing and mitigating risks.

Tenable assigns an Asset Criticality Rating (ACR) to each asset based on indicators of business value and criticality. ACR is based on several key metrics such as business purpose, asset type,

location, connectivity, capabilities, and third-party data. An ACR score is a range from 0-10. Low scores are not considered to be business critical, and high scores represent the organizations most critical, and have a greater business impact if compromised. Organizations that are also Tenable Lumin customers have the ability to adjust the default Tenable ACR value to more accurately reflect organizational risk.

Not all vulnerabilities pose the same risk. By combining ACR and VPR, prioritization efforts focus on the most critical vulnerabilities first.

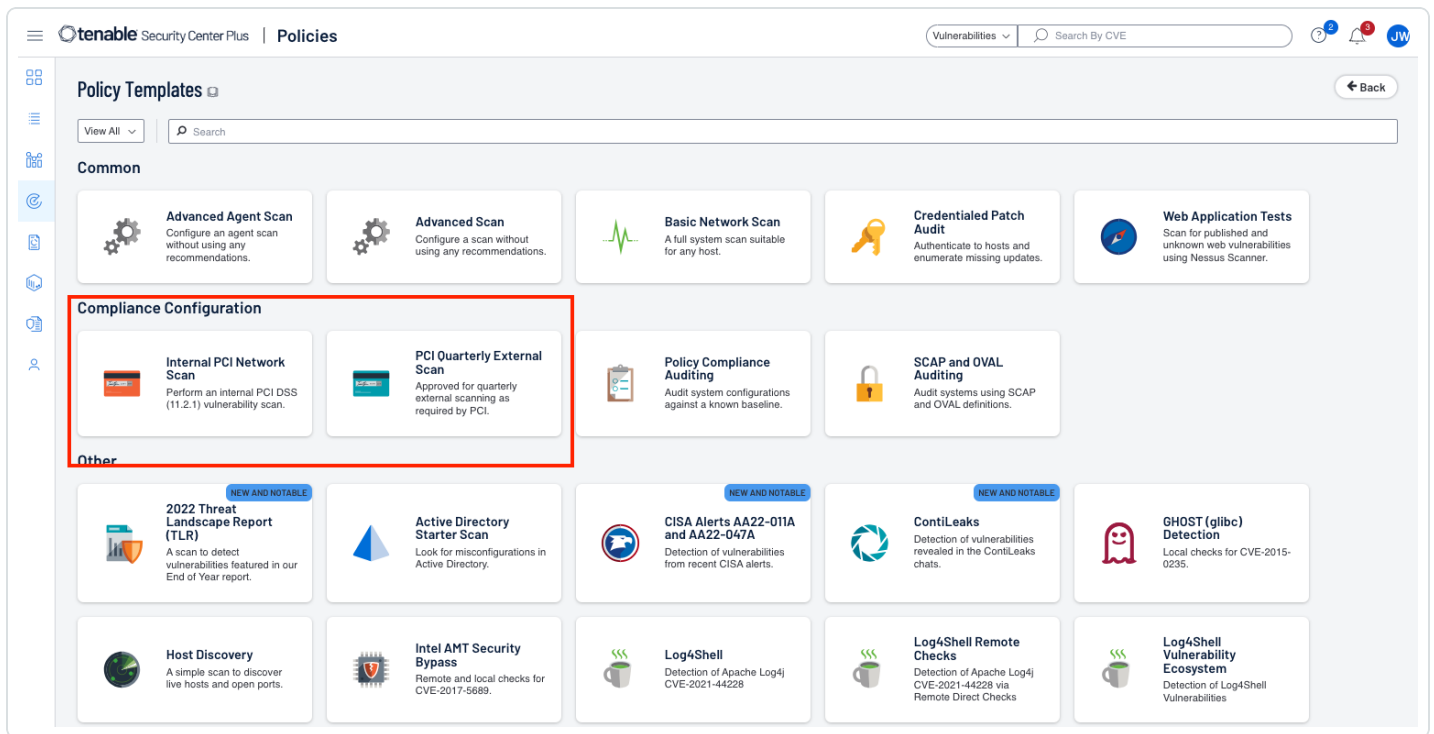
Organizations may also utilize CVSS and Severity ratings for risk prioritization. For more information on prioritization of vulnerabilities [reference this document](#).

For additional scanning under Requirement 11 organizations should utilize the pre-configured Nessus scan templates, available in Nessus, Tenable Security Center, and Tenable Vulnerability Management. These PCI scan templates allow organizations to get started quickly, with minimal configuration, however they can not be edited. When these scans are completed they can be submitted to Tenable's ASV Engineers for review. To maintain a set continuous scanning schedule, Nessus scans can be easily automated to run at specific times/days.

More information on this process can be found here: [Submitting Scans for PCI ASV Validation](#).

As a PCI Approved Scanning Vendor (ASV), Tenable offers two built-in scan policies designed for PCI scanning: 'PCI Quarterly External Scan' and 'Internal PCI Network Scan'. While only the 'PCI Quarterly External' policy is valid for official attestation, both policies can be used anytime for organizational scanning purposes. For official attestation, the PCI ASV add-on is required. The two policies differ in terms of settings and plugins included- the 'External' policy is designed for an 'outside-in' perspective of the target vector and therefore only executes remote checks, while the 'Internal' policy is better suited for scanning various connected devices within an organization's network.

Mandatory Requirement: PCI Requirement 11.3.1 requires that vulnerability scans be conducted at least once every three months, and that high risk and critical vulnerabilities are resolved. Rescans are to be conducted to verify that any identified high risk and critical vulnerabilities have been resolved. Tenable's PCI Scan policies assist organizations in meeting this requirement.



As the official External policy is approved and designed specifically in accordance with the specifications set forth by the PCI Security Standards Council, there is little customization possible with it- users are limited to adjusting the scan's performance settings to allow for proper analysis per the network's capabilities. No other customization to the External policy is permitted. The Internal policy, however, allows users to control the scan's Discovery, Assessment, Report, and Advanced settings, although plugins are not modifiable. Additionally, the Internal policy allows for the input of credentials to enable the local checks included in the scan's configuration.

A comparison between the two policies (default settings)

Setting	Internal	External
Use fast network discovery	enabled	disabled
Override firewall detection (for TCP port scanner)	automatic	soft
Credentialed access (local checks possible)	yes	no
Only use NTLMv2	yes	no
Paranoia level (Override normal accuracy)	normal	high

Perform thorough tests (slow)	disabled	enabled
CGI scanning	disabled	disabled
Only use credentials provided by the user	enabled	disabled
Elevate privileges	disabled	enabled
Test default accounts (slow)	disabled	enabled
Check for PCI DSS compliance	yes	yes
Enable Web Application tests	no	yes
Max simultaneous hosts per scan	30	20
Network timeout	5	15
Port scan range	default	1-65535

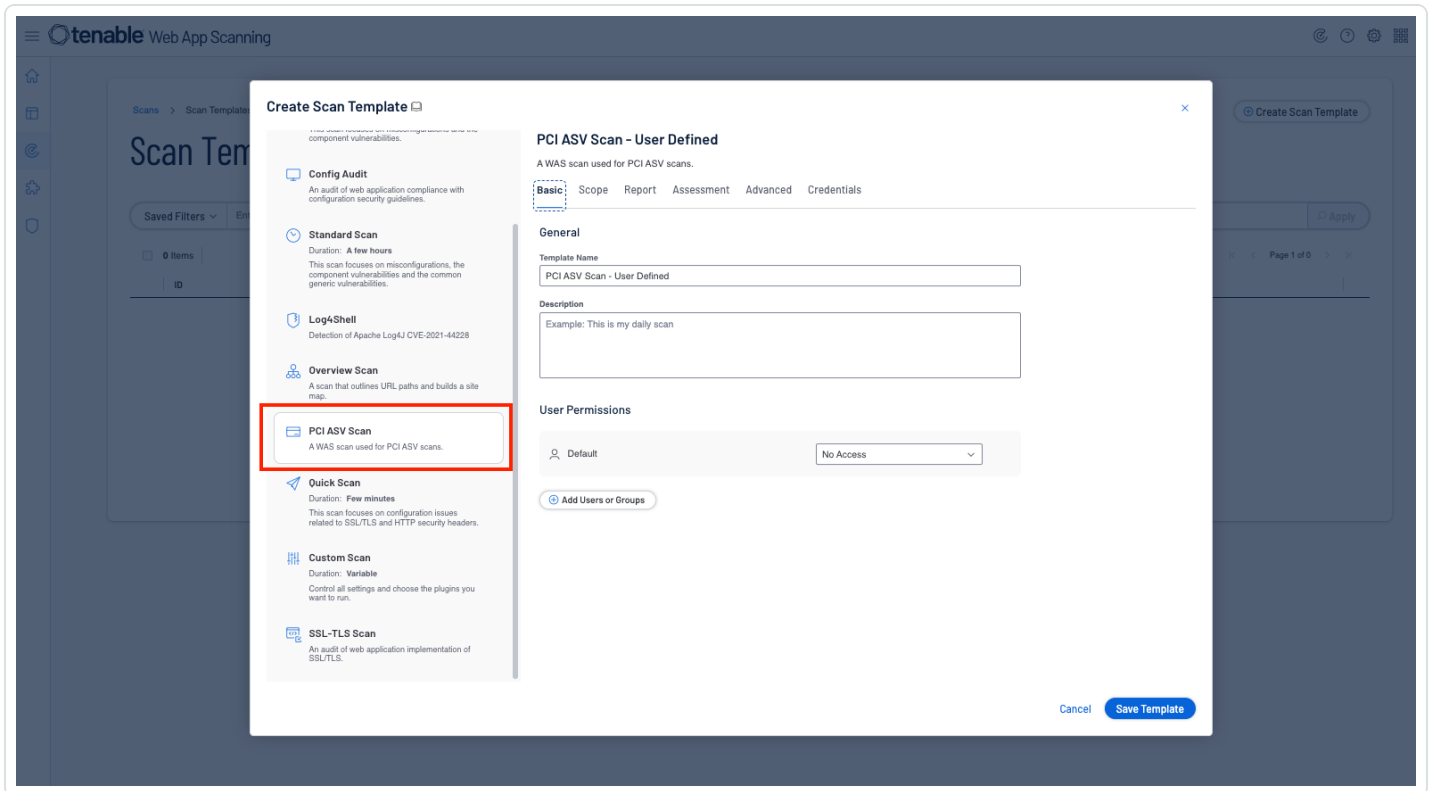
While the policies differ in terms of their various settings, the main idea for the external scan is that the policy demonstrates the publicly-visible attack vector currently present in the environment. The policy is meant to show what an attacker may be able to leverage from the external perspective, with the understanding that they would not be privy to valid authentication methods.

The settings that tend to make the biggest difference in the outcome of the two policies are the ability to authenticate with the Internal PCI policy and the increased paranoia in the External PCI policy. Use of credentials for the internal scan policy is preferred. Valid credentials allow the Internal policy to utilize a variety of local plugins, including the enumeration of missing patches. The increased paranoia of the External policy may result in some plugins reporting a vulnerability with lower confidence that would otherwise not be reported. Another key difference between the Internal and External PCI policies is how the port scanners operate. Especially if the Internal policy is provided with target credentials, the port scanner can enumerate the services running on the data plane, whereas the External policy will enumerate exposed ports, and can potentially enumerate the services running on the control plane.

Tenable Web App Scanning

Tenable Web Application Scanning contains a built-in PCI scan template. The PCI ASV Scan is a scan that assesses web applications for compliance with Payment Card Industry Data Security Standards (PCI DSS) for Tenable PCI ASV. (This scan also allows you to view and edit the Request

Redirect Limit. The default value for this limit is 3.) This scan template helps organizations who are using web servers or APIs meet the requirements for PCI 11.3.2.



Control Objective 6: Maintain an Information Security Policy

This includes maintaining a policy that addresses information security policies and procedures. PCI DSS Requirement 12 resides within this control objective. Requirement 12 ensures that organizations handling cardholder data have clear security policies in place, which are communicated, enforced, and updated on a regular basis. In addition to the establishing, publishing and maintaining of security policies, other Items that are evaluated in this requirement are employee training and awareness, are information security responsibilities.

By enforcing these requirements organizations ensure that security policies are in place but also actively maintained, communicated, and followed, reducing the risk of security incidents.

This control objectives covers the following PCI DSS requirements:

Requirement 12: Support information security with organizational policies and programs.

PCI Requirement 12.5.1 mandates that organizations have an inventory of system components that are in scope for PCI DSS. Maintaining a current list of all systems enables organizations to define which assets are in scope for PCI DSS. Recommended methods of maintaining the inventory list include databases, files, or inventory management tools.

PCI Requirements Under This Objective Supported by Tenable

As listed in PCI Requirement 12.5.1, a good practice is to keep an inventory of all assets. Those systems that are in scope for PCI DSS should be clearly identifiable among those assets.

Tenable products allow assets that have been identified to be tagged. Organizations can use tags to label assets, policies, credentials, or queries with a custom descriptor to improve filtering and object management. For example, you could add a tag named PCI DSS to label all of the assets that are in scope for PCI. Tenable Attack Surface Management continuously maps the Internet and discovers connections to your Internet-facing assets, whether internal or external to your networks, allowing organizations to discover unauthorized or unknown devices.

For more information regarding tagging assets reference these documents:

- [Tenable Security Center](#)
- [Tenable Vulnerability Management](#)
- [Tenable Attack Surface Management](#)

References

- [PCI Security Standards Council](#)
- [PCI DSS Prioritized Approach to PCI Compliance](#)
- [PCI DSS v4.0 Quick Reference Guide](#)
- [PCI DSS Summary of Changes from v4.0 to 4.0.1](#)
- [PCI DSS Summary of Changes from PCI DSS v3.2.1 to 4.0](#)