



# Tenable Cyber Exposure Study – Maintaining Data Protection Controls

Last Revised: July 17, 2025



## Table of Contents

<b>Introduction</b>	<b>3</b>
<b>Requirements for Data Protection</b>	<b>4</b>
Encryption of Data at Rest	6
Encryption of Data in Transit	8
Removable Media Controls	19
<b>Verifying Data Protection Controls</b>	<b>24</b>
<b>Encryption Benefits</b>	<b>32</b>
<b>Learn More</b>	<b>33</b>



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



---

# Requirements for Data Protection


---

Compliance requirements vary among different industries and geographic locations. New legislation and industry regulations are continually developed that change the standards for compliance audits in these industries. Familiarity with multiple compliance standards is necessary, even if they do not seem to be required at the moment. Changing legislation or shifts in an organization's business offerings require that managers keep abreast of audit criteria in other industries. The goal of compliance requirements is to avoid breaches of regulatory, statutory, or contractual obligations related to information security and of any security requirements. This section provides an overview of three of the common security compliance requirements: HIPAA, ISO 27001, and PCI DSS. These requirements are a small sample of many security compliance initiatives that have overlapping controls. Please refer to the Tenable Research [Audits](#) page for a list of audit files that address many of these compliance initiatives.

## HIPAA Overview

The [Health Insurance Portability and Accountability Act \(HIPAA\)](#) provides a set of rules for the protection and privacy of electronic Patient Health Information (ePHI) for U.S. citizens. The HIPAA rules apply to Covered Entities and Business Associates of Covered Entities. Covered Entities are those who perform the functions of processing data for the release and transmission of funds for medical services and include:

- **Health Plans** – entities that provide or pay for the cost of medical care
- **Health Care Clearinghouses** – organizations that process health care transactions for providers and insurers
- **Health Care Providers** – professionals trained and licensed to give, bill and be paid for health care services and do so via electronic transactions
- **Business Associates of Covered Entities** – organizations that serve in a support capacity for Covered Entities and may not necessarily be in the health care business. Examples of Business Associates include:
  - Attorneys
  - Accountants

- 
- 
- Consultants
  - Data Aggregators
  - Vendors

## ISO 27001 Overview

[ISO 27001](#) is a collection of standards set by the [International Organization for Standardization \(ISO\)](#), an independent international organization with a [membership](#) of 167 national standards bodies. Organizations use these standards to guide their Information Security Management System (ISMS) in a manner that reduces risk to the Confidentiality, Availability, and Integrity (CIA) of data.

Many organizations choose to obtain certification from an accredited ISO certification registrar, who audits the program and submits evidence documents to the ISO governing body. The certification process includes a primary audit, followed by a secondary audit that evaluates the effectiveness of the organization's Information Security Management System (ISMS) and determines if the controls meet all the requirements of the standard. Once the process is complete, the ISO certification registrar issues one of the following: a certification; a conditional certification; or a rejection. The ISO governing body sets the standard, but the accredited ISO certification registrar issues the certification. The ISO certification registrar must be objective and impartial, which means they cannot write documentation or provide consulting services to help the organization address gaps. Accreditation is not mandatory, but provides independent confirmation of competence, which helps large organizations negotiate Service Level Agreements (SLAs) with third parties.

## PCI DSS Overview

The [Payment Card Industry Data Security Standard \(PCI DSS\)](#) is a comprehensive set of security standards established by the founding members of the PCI Security Standards Council, including Visa, American Express, Discover Financial Services and MasterCard. The PCI DSS is intended to provide a common baseline to safeguard sensitive cardholder data for all bankcard brands and is used by e-commerce vendors who accept and store credit card data. The PCI DSS specifies a variety of high-level guidelines for running a secure network that leads to variations in how auditors interpret these recommendations.

The PCI DSS mandates [12 high-level requirements](#) that e-commerce organizations must perform to be considered in compliance with the standard. Such organizations must also have a



comprehensive vulnerability audit of any internet-facing system that handles credit card transactions. This vulnerability audit is required to look for the following items:

- Any vulnerability with a CVSS score of 4 or larger
- Any cross-site scripting or SQL injection type of vulnerability
- Any evidence of outdated SSL encryption

## Encryption of Data at Rest

The [NIST Special Publication 800-111](#), "Guide to Storage Encryption Technologies for End User Devices," provides guidance for encrypting data at rest. Data at rest is data that is not in motion and may or may not require encryption, depending on the requirements for securing that data. For example, encryption is required for mobile devices, but may not be for servers and desktops which have other data protection controls in place. Encryption requirements for servers and desktops may be required by specific compliance requirements, depending on the sensitivity of the data. This section describes how to use [Tenable Compliance & Audit Files](#) to assess various Operating Systems and platforms for encryption of data at rest.

The following audit files contain encryption checks for data at rest. There are additional audit files that can be used to assess various platform versions:

- CIS\_Apple\_macOS\_12
- CIS\_Juniper\_OS
- CIS\_Kubernetes\_v1.6.1
- CIS\_MS\_Windows\_10\_Enterprise\_Bitlocker
- CIS\_MS\_Windows\_10\_Enterprise\_Level\_1\_Bitlocker
- CIS\_MS\_Windows\_10\_Enterprise\_Level\_2\_Bitlocker
- CIS\_MS\_Windows\_10\_Enterprise\_Level\_1\_Bitlocker\_Next\_Generation\_Windows\_Security
- CIS\_MS\_Windows\_10\_Enterprise\_Level\_2\_Bitlocker\_Next\_Generation\_Windows\_Security
- CIS\_OSX\_10.11
- DISA\_STIG\_Apple\_iOS\_12\_v1r2-AirWatch
- DISA\_STIG\_Apple\_iOS\_12\_v1r2-MobileIron



- DISA\_STIG\_MSSQL\_2016\_Database
- DISA\_STIG\_Samsung\_Android\_7\_with\_Knox\_2.x\_v1r1-AirWatch
- DISA\_STIG\_Samsung\_Android\_7\_with\_Knox\_2.x\_v1r1-MobileIron

As shown below, the *CIS\_MS\_Windows\_10\_Enterprise\_Level\_1\_Bitlocker* audit file contains a check to ensure that hardware-based encryption is enabled for fixed drives. The description is the audit check name, which becomes the Plugin Name in Tenable Security Center. The Cross References that this audit check maps to are also listed at the bottom in the *reference* section.

```
<custom_item>
  type : REGISTRY SETTING
  description : "18.9.11.1.10 Ensure 'Configure use of hardware-based encryption for fixed data drives' is set to 'Enabled'"
  info : "This policy setting allows you to manage BitLocker's use of hardware-based encryption on fixed data drives and specify which encryption algorithms it can use with hardware-based encryption. Using hardware-based encryption can improve performance of drive operations that involve frequent reading or writing of data to the drive."

You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption and whether you want to restrict the encryption algorithms and cipher suites used with hardware-based encryption.

Note: The 'Choose drive encryption method and cipher strength' policy setting does not apply to hardware-based encryption. The encryption algorithm used by hardware-based encryption is set when the drive is partitioned. By default, BitLocker uses the algorithm configured on the drive to encrypt the drive. The 'Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' option enables you to restrict the encryption algorithms that BitLocker can use with hardware encryption. If the algorithm set for the drive is not available, BitLocker will disable the use of hardware-based encryption.

Encryption algorithms are specified by object identifiers (OID). For example:

AES 128 in CBC mode OID: 2.16.840.1.101.3.4.1.2
AES 256 in CBC mode OID: 2.16.840.1.101.3.4.1.42

The recommended state for this setting is: Enabled.

Rationale:

From a strict security perspective the hardware-based encryption may offer the same, greater, or less protection than what is provided by BitLocker's software-based encryption depending on how the algorithms and key lengths compare.

Impact:

Hardware-based encryption can improve performance of both read and write operations to the storage drive."
  solution : "To establish the recommended configuration via GP, set the following UI path to Enabled:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Configure use of hardware-based encryption for fixed data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

BitLocker will use hardware-based encryption with the encryption algorithm set for fixed drives. If hardware-based encryption is not available, BitLocker software-based encryption will be used instead."
  reference : "800-53|RA-2,CSCv6|13.2,CSCv7|13.6,CSCv8|3.6,CSF|ID.AM-5,CSF|ID.RA-4,CSF|ID.RA-5,GDPR|32.1.b,GDPR|32.1.d,HIPAA|164.306(a)(1),ITSG-33|RA-2,LEVEL|BLA,NESA|M2.2.1,NESA|T1.3.1,QCSC-v1|6.2,QCSC-v1|11.2"
  see_also : "https://workdoen.ch.cisecurity.org/sites/3330"
  value_type : POLICY_DWORD
  value_data : "1"
  reg_key : "HKLM\SOFTWARE\Policies\Microsoft\FVE"
  reg_item : "FDVHardwareEncryption"
  reg_option : CAN_NOT_BE_NULL
</custom_item>
```

The audit check displayed below is from the *CIS\_Apple\_macOS\_12.0\_Monterey* audit file. The Cross References are highlighted for this check, which ensures FileVault is Enabled.



```
<custom_item>
  type      : CMD EXEC
  description : "2.5.1.1 Ensure FileVault Is Enabled"
  info      : "FileVault secures a system's data by automatically encrypting its boot volume and requiring a password or recovery key to access it.

FileVault may also be enabled using command line using the fdesetup command. To use this functionality, consult the Der Flounder blog for more details:
https://derflounder.wordpress.com/2015/02/02/managing-yosemites-filevault-2-with-fdesetup/ https://derflounder.wordpress.com/2019/01/15/
unlock-or-decrypt-your-filevault-encrypted-boot-drive-from-the-command-line-on-macos-mojave/

Rationale:

Encrypting sensitive data minimizes the likelihood of unauthorized users gaining access to it.

Impact:

Mounting a FileVault encrypted volume from an alternate boot source will require a valid password to decrypt it."
  solution  : "Perform the following to enable FileVault:
Graphical Method:

Open System Preferences

Select Security & Privacy

Select FileVault

Select Turn on FileVault

Additional Information:

FileVault may not be desirable on a virtual OS. As long as the hypervisor and file storage are encrypted the virtual OS does not need to be. Rather than checking if
the OS is virtual and passing the control regardless of the encryption of the host system the normal check will be run. Security officials can evaluate the
comprehensive controls outside of the OS being tested."
  reference : "800-171|3.5.2,800-53|IA-5(
1),800-53|RA-2,CSCv7|13.6,CSCv7|14.8,CSCv8|3.6,CSCv8|3.11,CSF|ID.AM-5,CSF|ID.RA-4,CSF|ID.RA-5,CSF|PR.AC-1,GDPR|32.1.b,GDPR|32.1.d,HIPAA|164.306(
a)(1),HIPAA|164.312(a)(2)(1),HIPAA|164.312(d),ITSG-33|IA-5(
1),ITSG-33|RA-2,LEVEL|1A,NESA|M2.2.1,NESA|T1.3.1,NESA|T5.2.3,QCSC-v1|5.2.2,QCSC-v1|6.2,QCSC-v1|11.2,QCSC-v1|13.2,SWIFT-CSCv1|4.1"
  see_also  : "https://workbench.cisecurity.org/rules/3644"
  cmd       : "/usr/bin/fdesetup status"
  expect    : "FileVault[\\s]+is[\\s]+0n"
</custom_item>
```

## Encryption of Data in Transit

Data in transit is considered to be data that is moving across a network. The NIST Special Publication titled [“Guidelines for the Selection, Configuration, and Use of Transport Layer Security \(TLS\) Implementations”](#) provides guidance to cryptographically protect data in transit. This Special Publication provides guidance for the selection and configuration of TLS protocol implementations, leveraging Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms. This section discusses dashboard templates and [plugins](#) related to encryption of data in transit, such as certificates and protocols.

The *Data Protection - Certificate Status* Tenable Security Center dashboard component template uses many of the plugins described in this section to display certificate information for scanned assets.

### Data Protection - Certificate Status

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





**Certificate Information:** Displays the SSL certificate information.

- [10863](#) | SSL Certificate Information

## SSL Certificate Information Detection in Tenable Vulnerability Management

### Findings

Host Vulnerabilities | Cloud Findings | Host Audits | Web Application Vulnerabilities

< | Advanced | 🔍 Plugin ID: is equal to 10863 | Severity: is equal to Info | Search by Assets

Apply

Select Filters | Clear All

▼ Plugin ID

is equal to

10863

▼ Severity

is equal to

☐ Critical

☐ High

☐ Medium

☐ Low

☒ Info

☐ > 1000 Host Vulnerabilities

	PLUGIN ID	SEVERITY	LAST UPDATED ↓	NAME	IPV4 ADDRESS	ASSET
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:20 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:20 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:20 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:20 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:20 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:20 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:14 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:14 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:14 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 08:14 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 03:09 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 03:09 AM	SSL Certificate Information		
<input type="checkbox"/>	10863	Info	06/08/2022 at 03:09 AM	SSL Certificate Information		

**Protocol Detection:** The remote service encrypts traffic using a protocol with known weaknesses.

- [8184](#) | TLS v1.2 Traffic Negotiation Detection
- [8185](#) | TLS v1.1 Traffic Negotiation Detection
- [8549](#) | SSLv3 Protocol Detection
- [9129](#) | SSLv2 Client Connection Request
- [20007](#) | SSL Version 2 and 3 Protocol Detection
- [56984](#) | SSL / TLS Versions Supported
- [84470](#) | TLS Version 1.0 Protocol Detection (PCI DSS)
- [104743](#) | TLS Version 1.0 Protocol Detection
- [121010](#) | TLS Version 1.1 Protocol Detection
- [136318](#) | TLS Version 1.2 Protocol Detection
- [138330](#) | TLS Version 1.3 Protocol Detection



- [139414](#) | TLS Version 1.1 Protocol Detection (PCI DSS)
- [700105](#) | TLS 1.0 Detection
- [700106](#) | TLS 1.1 Detection
- [700107](#) | TLS 1.2 Detection
- [700108](#) | TLS 1.3 Detection
- [700110](#) | TLS 1.1 Detection (UDP)
- [700111](#) | TLS 1.2 Detection (UDP)
- [700112](#) | SSL/TLS Detection
- [700113](#) | SSL/TLS Detection (UDP)

Note: There are several non-informational plugins that detect deprecated TLS and SSL protocols, such as the following:

- [132675](#) | SSL/TLS Deprecated Ciphers Unsupported
- [157288](#) | TLS Version 1.1 Protocol Deprecated

Note: The results from the following plugins can often help find hidden services running TLS.

- [22964](#) | Service Detection (HTTP Banner)
- [25221](#) | Remote listeners enumeration (Linux / AIX)
- [83875](#) | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
- [110483](#) | Unix / Linux Running Processes Information

## **TLS Version 1.x Detection in Tenable Vulnerability Management**



Findings

Host Vulnerabilities

Cloud Findings

Host Audits

Web Application Vulnerabilities

< ▾

Advanced

🔍

Plugin ID: is equal to 104743...

×

Search by Assets

Apply

Select Filters

Clear All

▼ Plugin ID

is equal to

104743, 84470, 121010, 139414, 136318, 138330

< ▾

> 1000 Host Vulnerabilities

1 to 50 of Many ▼

	PLUGIN ID	SEVERITY ▼	LAST UPDATED	NAME	IPV4 ...	ASSET	CVSSV3 BASE SC...
<input type="checkbox"/>	104743	<div><div>🔥</div>Medium</div>	06/06/2022 at 03:09 AM	TLS Version 1.0 Pr...			6.5
<input type="checkbox"/>	104743	<div><div>🔥</div>Medium</div>	02/24/2022 at 03:09 AM	TLS Version 1.0 Pr...			6.5
<input type="checkbox"/>	104743	<div><div>🔥</div>Medium</div>	06/08/2022 at 03:09 AM	TLS Version 1.0 Pr...			6.5
<input type="checkbox"/>	104743	<div><div>🔥</div>Medium</div>	06/08/2022 at 03:09 AM	TLS Version 1.0 Pr...			6.5
<input type="checkbox"/>	104743	<div><div>🔥</div>Medium</div>	12/24/2021 at 03:06 AM	TLS Version 1.0 Pr...			6.5
<input type="checkbox"/>	104743	<div><div>🔥</div>Medium</div>	06/08/2022 at 03:09 AM	TLS Version 1.0 Pr...			6.5

**Certificate Issues & Concerns:** Checks for common issues or concerns with certificates. Some issues, such as no certificate, Common Name, or Subject are not required, but offer broader compatibility if used. Other items, such as Self-Signed certificates, may present larger concerns if used in production environments.

- [35297](#) | SSL Service Requests Client Certificate
- [45410](#) | SSL Certificate 'commonName' Mismatch
- [45411](#) | SSL Certificate with Wrong Hostname
- [51356](#) | Well-known SSL Certificate Used in Remote Device
- [56284](#) | SSL Certificate Fails to Adhere to Basic Constraints / Key Usage Extensions
- [56471](#) | SSL Certificate Chain Not Sorted
- [56472](#) | SSL Certificate Chain Contains Unnecessary Certificates
- [57571](#) | SSL Certificate Chain Analysis
- [57582](#) | SSL Self-Signed Certificate
- [121008](#) | SSL / TLS Certificate Known Hard Coded Private Keys
- [139546](#) | Improper Check for Certificate Revocation (FG-IR-19-144)
- [139547](#) | Improper Check for Certificate Revocation (FG-IR-19-144)
- [159544](#) | SSL Certificate with no Common Name
- [159545](#) | SSL Certificate with no Subject

## Certificate Issues & Concerns displayed in Tenable Vulnerability Management



Findings

Host Vulnerabilities

Cloud Findings

Host Audits

Web Application Vulnerabilities

< ▾

Advanced

🔍

Plugin ID: is equal to 159544... ×

Search by Assets

Apply

☐ 952 Host Vulnerabilities

Select Filters

Clear All

Plugin ID ▾

is equal to ▾

159544, 159545, 57582, 45410, 45411, 56471, 56472, 57571, 56284, 51356, 35297, 121008, 139546, 139547

PLUGIN ID	SEVERITY ↓	LAST UPDATED	NAME	IPV4 ADDRESS	ASSET	CVSSV3 BASE SCORE	VPR
<input type="checkbox"/> 121008	🔴 High	06/08/2022 at 03:09 AM	SSL / TLS Certificate Known Hard Coded Private Keys			7.5	3.6
<input type="checkbox"/> 121008	🔴 High	06/08/2022 at 03:09 AM	SSL / TLS Certificate Known Hard Coded Private Keys			7.5	3.6
<input type="checkbox"/> 121008	🔴 High	06/08/2022 at 03:09 AM	SSL / TLS Certificate Known Hard Coded Private Keys			7.5	3.6
<input type="checkbox"/> 139547	🔴 High	06/08/2022 at 03:09 AM	Improper Check for Certificate Revocation (FG-IR-19-144)			7.4	
<input type="checkbox"/> 57582	🟡 Medium	03/10/2022 at 04:11 AM	SSL Self-Signed Certificate				
<input type="checkbox"/> 57582	🟡 Medium	06/08/2022 at 03:09 AM	SSL Self-Signed Certificate				
<input type="checkbox"/> 45411	🟡 Medium	04/12/2022 at 03:12 AM	SSL Certificate with Wrong Hostname			5.3	



Findings								
Host Vulnerabilities Cloud Findings Host Audits Web Application Vulnerabilities								
<div>Advanced Plugin ID: is equal to 15901, ... Search by Assets</div>								
794 Host Vulnerabilities								
PLUGIN ID	SEVERITY	LAST UPDATED	NAME	IPV4 ADDRESS	ASSET	CVSSV3 BASE SCORE		
15901	Medium	06/08/2022 at 08:20 AM	SSL Certificate Expiry			5.3		
15901	Medium	06/08/2022 at 03:09 AM	SSL Certificate Expiry			5.3		
15901	Medium	06/08/2022 at 03:09 AM	SSL Certificate Expiry			5.3		
15901	Medium	06/08/2022 at 03:09 AM	SSL Certificate Expiry			5.3		
15901	Medium	06/08/2022 at 03:09 AM	SSL Certificate Expiry			5.3		
42981	Info	06/08/2022 at 03:09 AM	SSL Certificate Expiry - Future Expiry					

**Certificate Weaknesses:** Certificates that contain weak RSA keys, RSA keys with fewer than 2048 bits, are using a weak hashing algorithm, or are susceptible to spoofing.

- [35291](#) | SSL Certificate Signed Using Weak Hashing Algorithm
- [42053](#) | SSL Certificate Null Character Spoofing Weakness
- [60108](#) | SSL Certificate Chain Contains Weak RSA Keys
- [73459](#) | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits (PCI DSS)
- [86067](#) | SSL Certificate Signed Using SHA-1 Algorithm
- [95631](#) | SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Findings								
Host Vulnerabilities Cloud Findings Host Audits Web Application Vulnerabilities								
<div>Advanced Plugin ID: is equal to 60108, ... Search by Assets</div>								
117 Host Vulnerabilities								
PLUGIN ID	SEVERITY	LAST UPDATED	NAME	IPV4 ADD...	ASSET	CVSSV3 ...	VPR	
35291	High	06/08/2022 at 03:09 AM	SSL Certificate Signed Using Weak Hashing Algorithm			7.5	5.1	
35291	High	11/26/2021 at 03:07 AM	SSL Certificate Signed Using Weak Hashing Algorithm			7.5	5.1	
35291	High	03/15/2022 at 03:11 AM	SSL Certificate Signed Using Weak Hashing Algorithm			7.5	5.1	
35291	High	06/08/2022 at 03:09 AM	SSL Certificate Signed Using Weak Hashing Algorithm			7.5	5.1	
35291	High	06/08/2022 at 03:09 AM	SSL Certificate Signed Using Weak Hashing Algorithm			7.5	5.1	
35291	High	06/08/2022 at 03:09 AM	SSL Certificate Signed Using Weak Hashing Algorithm			7.5	5.1	

Tenable provides dashboard component templates in Tenable Security Center to identify deprecated cryptographic protocols of data in transit, such as the *Encryption - Cryptographic Compliance Concerns* component in the image below.



## Encryption - Cryptographic Compliance Concerns

70 Items

1 to 5 of 70

Page 1 of 14

PLUGIN ID	NAME	SEVERITY	TOTAL
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium	2440
65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	681
35291	SSL Certificate Signed Using Weak Hashing Algorithm	Medium	665
69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Low	312
70658	SSH Server CBC Mode Ciphers Enabled	Low	291

The *Encryption - Cryptographic Compliance Concerns* Tenable Security Center dashboard component template uses the filter combination below, as shown in the following two images:

- **Plugin Name** **Regex Match** `(\skey\s)([Kk]eys\s)([Cc]rypto)(AES)(\sDES\s)(TripleDES)([Pp][Gg][Pp])([Cc]ipher)([Hh]ash)(\sPIN\s)([Ss][Ss][Ll])([Tt][Ll][Ss])`
- **Severity:** Critical, High, Medium, Low

## Component Configuration for Encryption - Cryptographic Compliance Concerns:

Data

Type

Vulnerability

Query

Select a Query

Source

Cumulative

Tool

Vulnerability Summary

Filters

Plugin Name

Regex Match (\skey\s)([Kk]eys\s)([Cc]rypto)(AES)(\sDES\s)(Triple DES)([Pp][Gg][Pp])([Cc]ipher)([Hh]ash)(\sPIN\s)([Ss][Ss][Ll])([Tt][Ll][Ss])

Severity

Critical, High, Medium, Low

+ Add Filter



## Details when clicking View Data from the Encryption - Cryptographic Compliance Concerns component:

Vulnerabilities

Vulnerability Summary

<

Apply

Customize

Clear All

Load Query

Plugin Name

Regex Match

(\skey\s)|(\sKkey\s)|(\sCc|crypto)|(\sAES)|(\sDES\s)|(\sTripleDES)|(\sPp)|(\sGg)|(\sPp)|(\sCc|ipher)|(\sH|th|ash)|(\sPIN\s)|(\sSs)|(\sL)|(\sTt)|(\sLJ)|(\sSs)

Severity

Select All

Critical

High

Medium

Low

Info

70 Results

[Jump to Vulnerability Detail](#)

[Export](#)

[Save](#)

[More](#)

<input type="checkbox"/>	PLUGIN ID	NAME	FAMILY	SEVERITY	TOTAL
<input type="checkbox"/>	1010187	3.10 Secure MySQL Keyring - keyring_hashicorp_store_path	N/A	High	29
<input type="checkbox"/>	80101	IPMI v2.0 Password Hash Disclosure	General	High	8
<input type="checkbox"/>	1005590	Use Secure Protocols When Possible - 'ssh key rsa = 2048'	N/A	High	6
<input type="checkbox"/>	1005599	TACACS+ Authentication - 'tacacs-server key is configured'	N/A	High	6
<input type="checkbox"/>	1005827	1.7.3 Ensure 'SSL AES 256 encryption' is set for HTTPS access	N/A	High	6
<input type="checkbox"/>	1007353	2.3.11.4 Ensure 'Network security: Configure encryption types allowe...	N/A	High	5
<input type="checkbox"/>	1002847	5.3.4 Ensure password hashing algorithm is SHA-512	N/A	High	4
<input type="checkbox"/>	1006434	6.6.12 Ensure SHA512 is used to hash local passwords	N/A	High	3
<input type="checkbox"/>	1006526	6.7.4 Ensure Authentication Keys are used for all NTP Servers	N/A	High	3
<input type="checkbox"/>	1007436	18.8.28.7 Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	N/A	High	3
<input type="checkbox"/>	1007763	18.9.45.5.1 Ensure 'Enable file hash computation feature' is set to 'En...	N/A	High	3
<input type="checkbox"/>	1006541	6.10.1.7 Ensure Only Suite B Ciphers are set for SSH - ciphers restricti...	N/A	High	2
<input type="checkbox"/>	1010530	6.7.5 Ensure Authentication Keys are used for all NTP Servers	N/A	High	2

The *SSL/TLS Discovery - SSL/TLS Vulnerabilities By Type* dashboard component template in the Tenable Security Center feed displays a count of systems with SSLv2, SSLv3, and TLS discovered actively with Nessus and passively with Nessus Network Monitor.

SSL/TLS Discovery - SSL/TLS Vulnerabilities By Type			
	Systems	Active	Passive
SSLv2	14	30	0
SSLv3	277	698	27
TLS 1.0 (Deprecated)	2088	2492	0
TLS 1.1	2116	4991	13
TLS 1.2	2183	4866	1279
TLS 1.3	6	12	0

The following images show detailed results of the cells in the *Systems* column of the *SSL/TLS Discovery - SSL/TLS Vulnerabilities by Type* Tenable Security Center dashboard component displayed above. The *Systems* column displays the number of systems that meet the search criteria, rather than the total number of vulnerabilities that meet the search criteria. The *Active* and *Passive* columns display the number of vulnerabilities that meet the search criteria. These columns use the



Plugin ID filters for only Active or Passive plugins, respectively. The *Systems* column uses both Active and Passive plugins to show all systems that meet the criteria.

### SSLv2 [Systems Column]:

- *Plugin ID* =  
20007,56984,84470,104743,22964,25221,83875,110483,121010,136318,138330,139414,8185,8184,8549,9129,700105,700106,700107,700108,700110,700111,700112,700113
- *Vulnerability Text* **contains** sslv2,SSL 2.0,SSL version 2

Vulnerabilities

Vulnerability Summary

<

Apply

+ Customize

× Clear All

Load Query

Plugin ID

=

20007,56984,84470,1

Vulnerability Text

Contains

sslv2,SSL 2.0,SSL version 2

2 Results

[Jump to Vulnerability Detail](#)

[Export](#)

[Save](#)

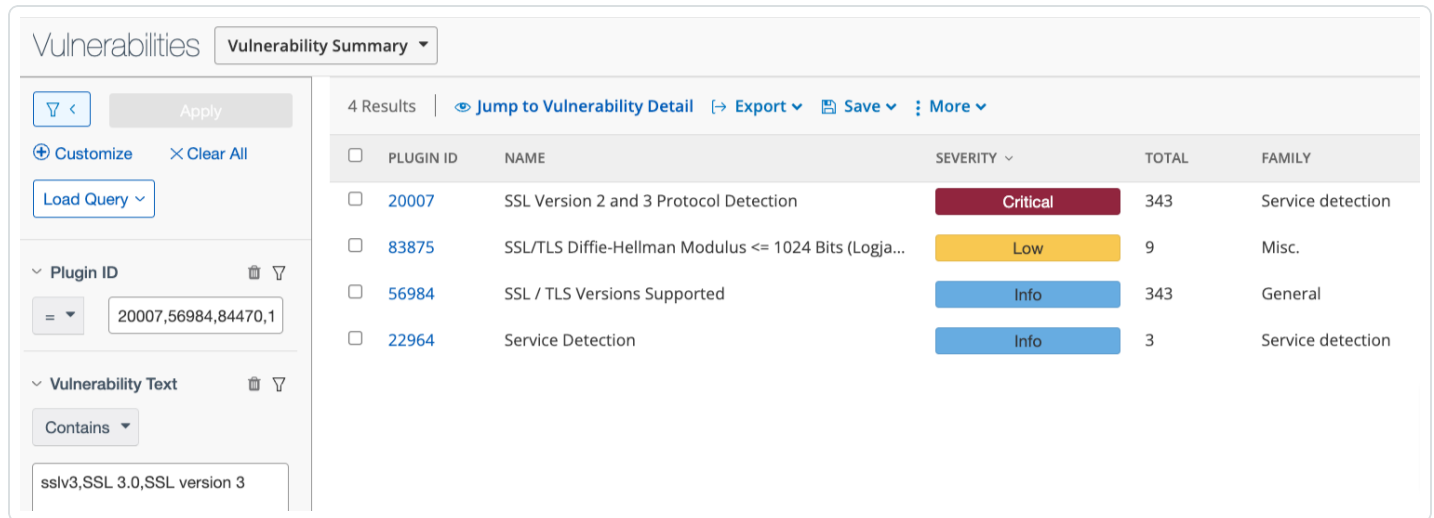
[More](#)

<input type="checkbox"/>	PLUGIN ID	NAME	SEVERITY	TOTAL	FAMILY
<input type="checkbox"/>	20007	SSL Version 2 and 3 Protocol Detection	Critical	14	Service detection
<input type="checkbox"/>	56984	SSL / TLS Versions Supported	Info	16	General

### SSLv3 [Systems Column]:

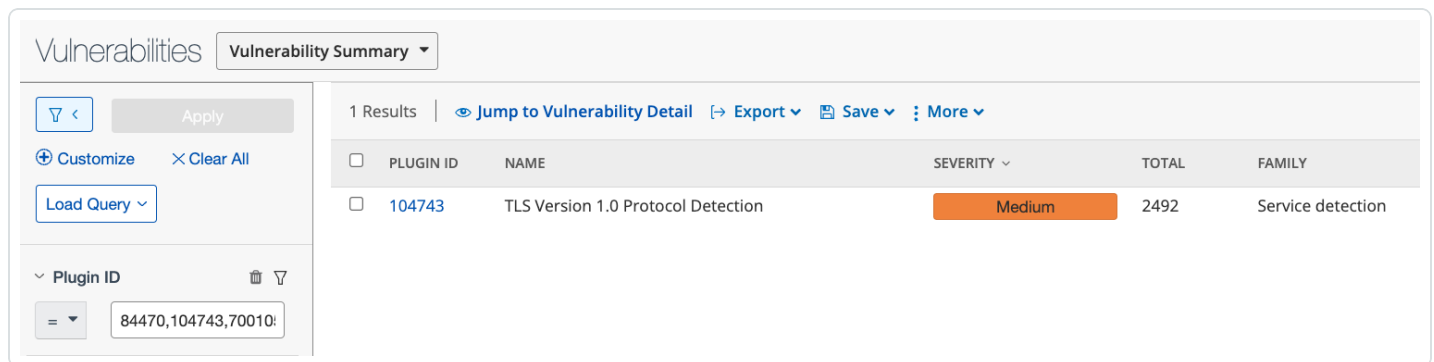
- *Plugin ID* =  
20007,56984,84470,104743,22964,25221,83875,110483,121010,136318,138330,139414,8185,8184,8549,9129,700105,700106,700107,700108,700110,700111,700112,700113
- *Vulnerability Text* **contains** sslv3,SSL 3.0,SSL version 3





### TLS 1.0 (Deprecated) [Systems Column]:

- *Plugin ID* = 84470,104743,700105
- *Vulnerability Text* **Contains** TLSv1



### TLS 1.1 [Systems Column]:

- *Plugin ID* =  
20007,56984,84470,104743,22964,25221,83875,110483,121010,136318,138330,139414,8185,8184,8549,9129,700105,700106,700107,700108,700110,700111,700112,700113
- *Vulnerability Text* **Contains** TLSv1.1



Vulnerabilities

Vulnerability Summary

Apply

Customize

Clear All

Load Query

Plugin ID

=

20007,56984,84470,1

Vulnerability Text

Contains

TLSv1.1

6 Results

[Jump to Vulnerability Detail](#)

[Export](#)

[Save](#)

[More](#)

<input type="checkbox"/>	PLUGIN ID	NAME	SEVERITY	TOTAL	FAMILY
<input type="checkbox"/>	121010	TLS Version 1.1 Protocol Detection	Medium	2293	Service detection
<input type="checkbox"/>	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logja...	Low	362	Misc.
<input type="checkbox"/>	56984	SSL / TLS Versions Supported	Info	2296	General
<input type="checkbox"/>	22964	Service Detection	Info	38	Service detection
<input type="checkbox"/>	25221	Remote listeners enumeration (Linux / AIX)	Info	1	Service detection
<input type="checkbox"/>	110483	Unix / Linux Running Processes Information	Info	1	General

## TLS 1.2 [Systems Column]:

- *Plugin ID* =  
20007,56984,84470,104743,22964,25221,83875,110483,121010,136318,138330,139414,8185,8184,8549,9129,700105,700106,700107,700108,700110,700111,700112,700113
- *Vulnerability Text* **Contains** TLSv1.2

Vulnerabilities

Vulnerability Summary

Apply

Customize

Clear All

Load Query

Plugin ID

=

20007,56984,84470,1

Vulnerability Text

Contains

TLSv1.2

5 Results

[Jump to Vulnerability Detail](#)

[Export](#)

[Save](#)

[More](#)

<input type="checkbox"/>	PLUGIN ID	NAME	SEVERITY	TOTAL	FAMILY
<input type="checkbox"/>	56984	SSL / TLS Versions Supported	Info	2406	General
<input type="checkbox"/>	136318	TLS Version 1.2 Protocol Detection	Info	2315	Service detection
<input type="checkbox"/>	22964	Service Detection	Info	143	Service detection
<input type="checkbox"/>	25221	Remote listeners enumeration (Linux / AIX)	Info	1	Service detection
<input type="checkbox"/>	110483	Unix / Linux Running Processes Information	Info	1	General

## TLS 1.3 [Systems Column]:

- *Plugin ID* =  
20007,56984,84470,104743,22964,25221,83875,110483,121010,136318,138330,139414,8185,8184,8549,9129,700105,700106,700107,700108,700110,700111,700112,700113
- *Vulnerability Text* **Contains** TLSv1.3



Vulnerabilities

Vulnerability Summary

<

>

Apply

Customize

Clear All

Load Query

Plugin ID

=

20007,56984,84470,1

Vulnerability Text

Contains

TLsv1.3

2 Results

[Jump to Vulnerability Detail](#)

[Export](#)

[Save](#)

[More](#)

<input type="checkbox"/>	PLUGIN ID	NAME	SEVERITY	TOTAL	FAMILY
<input type="checkbox"/>	56984	SSL / TLS Versions Supported	Info	6	General
<input type="checkbox"/>	138330	TLS Version 1.3 Protocol Detection	Info	6	Service detection

## Removable Media Controls

Data stored on removable media is susceptible to unauthorized disclosure and needs to be secured. Removable media, by design, is designed to be portable and is particularly susceptible to data loss. This section describes security concerns for removable media and how Tenable products can determine if controls are in place that align with the organization's policy on removable media.

Removable media has both "read" and "write" access controls. Many organizations restrict write access to prevent data from being written to removable media. Exceptions may be made on a case by case basis.

If write access is permitted, encryption can be enforced at the file or device level, depending on the solutions in place and the company policy. The [NIST Special Publication 800-111](#), "Guide to Storage Encryption Technologies for End User Devices," provides guidance for encrypting data on removable media.

Data Loss Prevention controls can be used to prevent particular types of data (such as credit card numbers) from being written to removable media, even if write access is permitted.

The following image displays an audit check from the *CIS\_MS\_Windows\_10\_Enterprise\_Bitlocker* audit file, which ensures that hardware-based encryption for removable data drives is enabled.



```
<custom_item>
  type : REGISTRY SETTING
  description : "18.9.11.3.10 Ensure 'Configure use of hardware-based encryption for removable data drives' is set to 'Enabled'"
  info : "This policy setting allows you to manage BitLocker's use of hardware-based encryption on removable data drives and specify which encryption algorithms it can use with hardware-based encryption. Using hardware-based encryption can improve performance of drive operations that involve frequent reading or writing of data to the drive."

You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption and whether you want to restrict the encryption algorithms and cipher suites used with hardware-based encryption.

Note: The 'Choose drive encryption method and cipher strength' policy setting does not apply to hardware-based encryption. The encryption algorithm used by hardware-based encryption is set when the drive is partitioned. By default, BitLocker uses the algorithm configured on the drive to encrypt the drive. The 'Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' option enables you to restrict the encryption algorithms that BitLocker can use with hardware encryption. If the algorithm set for the drive is not available, BitLocker will disable the use of hardware-based encryption.

Encryption algorithms are specified by object identifiers (OID). For example:

AES 128 in CBC mode OID: 2.16.840.1.101.3.4.1.2
AES 256 in CBC mode OID: 2.16.840.1.101.3.4.1.42

The recommended state for this setting is: Enabled.

Rationale:

From a strict security perspective the hardware-based encryption may offer the same, greater, or less protection than what is provided by BitLocker's software-based encryption depending on how the algorithms and key lengths compare.

Impact:

Hardware-based encryption can improve performance of both read and write operations to the storage drive."
  solution : "To establish the recommended configuration via GP, set the following UI path to Enabled:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Configure use of hardware-based encryption for removable data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

BitLocker will use hardware-based encryption with the encryption algorithm set for removable drives. If hardware-based encryption is not available, BitLocker software-based encryption will be used instead."
  reference : "800-53|RA-2,CSCv6|13.2,CSCv7|13.6,CSCv8|3.6,CSF|ID.AM-5,CSF|ID.RA-4,CSF|ID.RA-5,GDPR|32.1.b,GDPR|32.1.d,HIPAA|164.306(a)(1),ITSG-33|RA-2,LEVEL|BLA,NESA|M2.2.1,NESA|T1.3.1,QCSC-v1|6.2,QCSC-v1|11.2"
  see_also : "https://workbench.cisecurity.org/files/3350"
  value_type : POLICY_DWORD
  value_data : "1"
  reg_key : "HKLM\SOFTWARE\Policies\Microsoft\FVE"
  reg_item : "RDVHardwareEncryption"
  reg_option : CAN_NOT_BE_NULL
</custom_item>
```

Unix-based systems support file system mount options that can provide additional security controls, such as 'nodev,' 'noexec,' and 'nosuid,' as described below:

- **nodev** – Restricts character and blocks special devices from being accessed on the filesystem. Character and block special devices are those that permit access to a file that is attached to a device that is not part of the file system, such as a USB drive. Use the 'nodev' mounting option for filesystems that contain sensitive data to prevent data exfiltration. Removable media containing character or block special devices could be used to bypass security controls by allowing non-root users to access sensitive device files such as /dev/kmem or raw disk partitions.
- **noexec** – Prevents executable files from running on a file system. Use the 'noexec' option for removable media to prevent malware from being run when the media is attached to the system.



- **nosuid** – Disables the ability to elevate privileges on a file system. Use the 'nosuid' option for world-writable file systems and removable media.

The *Data Protection - Removable Media noexec, nosuid, nodev* Compliance Tenable Security Center dashboard component template uses the following filters:

- *Plugin Type*: Compliance
- *Plugin Name* **Regex Match** (nodev.\*[Rr]emovable [Mm]edia)([Rr]emovable [Mm]edia.\*nodev)(noexec.\*[Rr]emovable [Mm]edia)([Rr]emovable [Mm]edia.\*noexec)(nosuid.\*[Rr]emovable [Mm]edia)([Rr]emovable [Mm]edia.\*nosuid)

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

The following image displays an audit check from the *CIS\_CentOS\_8\_Server* audit file, which displays the mount options that are used on the file system.

Note: This is a manual check, requiring a review of the output by IT staff who are familiar with the correct settings for the system. See "Manual Review Required" in the *expect* section of the image.

```
<custom_item>
  system : "Linux"
  type   : CMD_EXEC
  description : "1.1.18 Ensure nodev option set on removable media partitions"
  info    : "The nodev mount option specifies that the filesystem cannot contain special devices.

Rationale:

Removable media containing character and block special devices could be used to circumvent security controls by allowing non-root users to access sensitive device files such as /dev/kmem or the raw disk partitions.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance."
  solution : "Edit the /etc/fstab file and add nodev to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the fstab(5) manual page for more information."
  reference : "800-171|3.4.2,800-53|CM-6,CSCv6|3.1,CSCv7|5.1,CSF|PR.IP-1,GDPR|32.1.b,HIPAA|164.306(a)(1),ITSG-33|CM-6,LEVEL|1M,SWIFT-CSCv1|2.3"
  see_also  : "https://workbench.cisecurity.org/files/3148"
  cmd       : "/bin/mount"
  expect    : "Manual Review Required"
  severity  : MEDIUM
</custom_item>
```



Tenable provides dashboard component templates in the Tenable Security Center feed, such as the *Removable Media and Content Audits - CDROM, Floppy, Other Storage Audit* component shown below.

#### 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

In Tenable Security Center, the audit check name corresponds to the Plugin Name, so searches can be performed using the *Plugin Name* filter. For example, the search below can be used in Tenable Security Center to find results from audit scans [also called compliance scans] with check names containing 'removable media' and 'nodev' from various audit files.

- *Plugin Name* **Regex Match** (nodev.\*[Rr]emovable [Mm]edia)([Rr]emovable [Mm]edia.\*nodev)
- *Plugin Type*: compliance

### Vulnerabilities

Vulnerability Summary ▾

🔍 <

Apply

⊕ Customize

✕ Clear All

Load Query ▾

▼ Plugin Name

Regex Match ▾

(nodev.\*[Rr]emovable [Mm]edia)([Rr]emovable [Mm]edia.\*nodev)

▼ Plugin Type

☐ Active

☒ Compliance

4 Results

[👁 Jump to Vulnerability Detail](#) [↔ Export ▾](#) [📄 Save ▾](#) [⋮ More ▾](#)

PLUGIN ID	NAME	SEVERITY ▴	TOTAL
1009023	1.1.21 Ensure nodev option set on removable media partitions	Info	1
1010611	1.1.20 Ensure nodev option set on removable media partitions	Info	2
1006861	1.1.22 Ensure nodev option set on removable media partitions	Medium	4
1001822	1.1.18 Ensure nodev option set on removable media partitions	High	5

- 22 -



In the Tenable Vulnerability Management *Host Audits Findings*, the *Audit Name* filter can be used to display results from various audit files. For example, the search below displays any scan results from audit checks containing "Removable Media."

- *Audit Name is equal to* \*Removable media\*

The screenshot shows the Tenable.io interface for finding audit results. The 'Findings' section is active, and the 'Host Audits' tab is selected. The search filters are set to 'Audit Name: is equal to \*Removable media\*' and 'State: is equal to Active, Resurfaced'. The results table shows 19 Host Audits.

ASSET NAME	AUDIT NAME	AUDIT FILE	RE...	LAST AUDITED	ACTIONS
d...	1.1.20 Ensure noexec option set on removable media partitions	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Fa	05/22/2022 at 07:10 A...	⋮
d...	1.1.18 Ensure nodev option set on removable media partitions	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Fa	05/22/2022 at 07:10 A...	⋮
d...	1.1.19 Ensure nosuid option set on removable media partitions	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Fa	05/22/2022 at 07:10 A...	⋮
d...	1.1.20 Ensure noexec option set on removable media partitions	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Fa	05/22/2022 at 07:04 A...	⋮
d...	1.1.18 Ensure nodev option set on removable media partitions	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Fa	05/22/2022 at 07:04 A...	⋮
d...	1.1.19 Ensure nosuid option set on removable media partitions	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit	Fa	05/22/2022 at 07:04 A...	⋮
ai...	2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interac...	CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker_...	Error	05/17/2022 at 04:17 PM	⋮
ji...	2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interac...	CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker_...	Error	05/16/2022 at 04:05 PM	⋮
sc...	2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interac...	CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker_...	Error	05/16/2022 at 03:54 PM	⋮
sf...	2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interac...	CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker_...	Error	05/16/2022 at 03:51 PM	⋮
ai...	2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interac...	CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker_...	Error	05/16/2022 at 03:48 PM	⋮
jo...	2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interac...	CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker_...	Error	05/16/2022 at 03:45 PM	⋮



## Verifying Data Protection Controls

The [National Institute of Standards \(NIST\) Special Publication 800-53](#) provides comprehensive guidance for a secure infrastructure. This section describes NIST guidance for data protection controls and how Tenable solutions help validate that appropriate encryption controls are implemented within the organization.

The [NIST Cybersecurity Framework \(CSF\)](#) is a control framework, whose high level controls align with [ISO 27001](#), [NIST SP 800-53](#), and others. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. Many regulating bodies accept evidence documentation of compliance with the NIST CSF as assurance that the organization has effective controls in place to meet their security requirements. The HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework is an example of alignment with NIST.

Tenable audit checks contain a **reference** field that points to specific controls in a standard (ISO 27001), framework (NIST Cybersecurity Framework), or regulation (HIPAA) and is used by nearly all plugins. Any external reference can be identified using the Cross References field. References can be used to search or filter in Tenable Security Center. For example, the following References define requirements for the encryption of data at rest:

- 800-171 - 3.13.16
- 800-53 - SC-28

Security Requirement 3.13.16 in the NIST Special Publication 800-171 Revision 2 provides guidance to protect the confidentiality of Controlled Unclassified Information (CUI) at rest and maps to Security Control SC-28 of [NIST Special Publication 800-53](#), which provides guidance for *Protection of Information at Rest*. Security Requirements specify what action needs to be taken. For example, HIPAA requires that Personal Health Information (PHI) be encrypted when traversing internal networks. Security controls specify how to meet the requirement, such as "enable switch to switch encryption on internal network segments."

Data at rest is data that is stored on a device and not in process or transmission. Encryption requirements for data at rest depend on the sensitivity of the data and other protection controls that may be in place. For example, data stored on mobile devices has a greater risk since the device is exposed to unsecured networks. Data stored on secure servers in a protected data center has a





lower risk of unauthorized access. NIST Special Publication 800-171 provides recommended requirements to protect the confidentiality of controlled unclassified information.

The 800-53:SC-28 mapping aligns with the following regulatory controls:

- 800-171: NIST 800-171 (Standard)
- csf: [NIST Cybersecurity Framework \(CSF\)](#) (Framework)
- hipaa: [HIPAA](#) (Regulation applying a standard)
- isoiec-27001: [ISO 27001](#) (Standard)
- pci-dss: [PCI-DSS](#) (Standard)
- cobit5: [COBIT](#) (Standard)

Control mappings, shown as “reference” in the following audit check image, identify encryption algorithms and cipher suites that the audit check verifies. Audit checks can map to multiple controls across multiple standards. For example, the audit check shown in the image below verifies compliance with the following controls:

- NIST SP 800-53 - RA-2
- CIS Critical Security Controls (CSC) v6 - 13.2
- CSC v7 - 13.6
- CSC v8 -3.6
- CSF - ID.AM-5,ID.RA-4,ID.RA-5
- General Data Protection Regulation (GDPR) - 32.1, 32.1.d
- HIPAA - 164.306(a)(1)
- Overview of IT Security Risk Management: A Lifecycle Approach (ITSG-33) - RA-2
- LEVEL|BitLocker Automated (BLA)
- National Electronic Security Authority (NESA) - M2.2.1, T1.3.1
- QCSC-v1|6.2
- QCSC-v1|11.2"



```

<custom_item>
  type : REGISTRY_SETTING
  description : "18.9.11.3.13 Ensure 'Configure use of hardware-based encryption for removable data drives: Restrict crypto algorithms or cipher suites to the following:' is set to 'Enabled: 2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42'"
  info : "This policy setting allows you to manage BitLocker's use of hardware-based encryption on removable data drives and specify which encryption algorithms it can use with hardware-based encryption. Using hardware-based encryption can improve performance of drive operations that involve frequent reading or writing of data to the drive."

You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption and whether you want to restrict the encryption algorithms and cipher suites used with hardware-based encryption.

Note: The 'Choose drive encryption method and cipher strength' policy setting does not apply to hardware-based encryption. The encryption algorithm used by hardware-based encryption is set when the drive is partitioned. By default, BitLocker uses the algorithm configured on the drive to encrypt the drive. The 'Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' option enables you to restrict the encryption algorithms that BitLocker can use with hardware encryption. If the algorithm set for the drive is not available, BitLocker will disable the use of hardware-based encryption.

Encryption algorithms are specified by object identifiers (OID). For example:

AES 128 in CBC mode OID: 2.16.840.1.101.3.4.1.2
AES 256 in CBC mode OID: 2.16.840.1.101.3.4.1.42

The recommended state for this setting is: Enabled: 2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42.

Rationale:

From a strict security perspective the hardware-based encryption may offer the same, greater, or less protection than what is provided by BitLocker's software-based encryption depending on how the algorithms and key lengths compare.

Impact:

None - this value is ignored when the checkbox above it (Restrict encryption algorithms and cipher suites allowed for hardware-based encryption) is False (unchecked), as is required in Rule 18.9.11.3.12. If that checkbox is set to True (checked), then the encryption algorithms permitted on removable drives would be restricted to the specified object identifiers (OIDs)."
  solution : "To establish the recommended configuration via GP, set the following UI path to Enabled: 2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Configure use of hardware-based encryption for removable data drives: Restrict crypto algorithms or cipher suites to the following:

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Encryption algorithms and cipher suites are not restricted for hardware-based encryption on removable drives."
  reference : "800-53|RA-2,CSCv6|13.2,CSCv7|13.6,CSCv8|3.6,CSF|ID.AM-5,CSF|ID.RA-4,CSF|ID.RA-5,GDPR|32.1.b,GDPR|32.1.d,HIPAA|164.306(a)(1),ITSG-33|RA-2,LEVEL|BLA,NESA|M2.2.1,NESA|T1.3.1,QCSC-v1|6.2,QCSC-v1|11.2"
  see_also : "https://workbench.cisecurity.org/files/3350"
  value_type : POLICY_MULTI_TEXT
  value_data : "2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42"
  reg_key : "HKLM\SOFTWARE\Policies\Microsoft\FVE"
  reg_item : "RDVAllowedHardwareEncryptionAlgorithms"
  reg_option : CAN_NOT_BE_NULL
</custom_item>

```

The *Data Protection - Confidentiality of Protected Information* Concerns Tenable Security Center dashboard component template uses the Cross References mentioned above in the filters for the component, shown in the next two images:

- *Cross References* = 800-53|RA-2,CSCv6|13.2,CSCv7|13.6,CSCv8|3.6,CSF|ID.AM-5,CSF|ID.RA-4,CSF|ID.RA-5,GDPR|32.1.b,GDPR|32.1.d,HIPAA|164.306(a)(1),ITSG-33|RA-2,LEVEL|BLA,NESA|M2.2.1,NESA|T1.3.1,QCSC-v1|6.2,QCSC-v1|11.2
- *Plugin Type*: Compliance
- *Severity*: High, Medium



## Data Protection - Confidentiality of Protected Information Concerns

10 Items	1 to 5 of 10	Page 1 of 2
NAME	SEVERITY	TOTAL
5.2 Client Encryption	High	4
5.1 Inter-node Encryption	High	4
4.1 Ensure that logging is enabled. - logback.xml	High	4
4.1 Ensure that logging is enabled. - nodetool getlogginglevels	High	4
3.5 Ensure that Cassandra only listens for network connections on authorized interfaces	High	4

## Vulnerabilities

Vulnerability Summary

### Cross References

800-53|RA-2,CSCv6|13.2,CSCv7|13.6,CSv8|3.6,CSF|ID.AM-5,CSF|ID.RA-4,CSF|ID.RA-5,GDPR|32.1.b,GDPR|32.1.d,HIPAA|164.206(e)(1),ITSC

### Plugin Type

- ☐ Active  
☒ Compliance  
☐ Event  
☐ Passive

### Severity

- ☐ Select All  
☒ High  
☒ Medium

1589 Results | [Jump to Vulnerability Detail](#) | [Export](#) | [Save](#) | [More](#)

<input type="checkbox"/>	PLUGIN ID	NAME	SEVERITY	TOTAL
<input type="checkbox"/>	1010189	4.5 Ensure 'mysqld' is Not Started With '--skip-grant-tables'	High	28
<input type="checkbox"/>	1010176	1.2 Use Dedicated Least Privileged Account for MySQL Daemon/Service	High	27
<input type="checkbox"/>	1001812	1.1.3 Ensure nodev option set on /tmp partition	High	8
<input type="checkbox"/>	1001813	1.1.4 Ensure nosuid option set on /tmp partition	High	8
<input type="checkbox"/>	1001814	1.1.5 Ensure noexec option set on /tmp partition	High	8
<input type="checkbox"/>	1001815	1.1.8 Ensure nodev option set on /var/tmp partition	High	8
<input type="checkbox"/>	1001816	1.1.9 Ensure nosuid option set on /var/tmp partition	High	8
<input type="checkbox"/>	1001817	1.1.10 Ensure noexec option set on /var/tmp partition	High	8
<input type="checkbox"/>	1001832	1.3.2 Ensure filesystem integrity is regularly checked	High	8
<input type="checkbox"/>	1001979	5.1.2 Ensure permissions on /etc/crontab are configured	High	8
<input type="checkbox"/>	1001980	5.1.3 Ensure permissions on /etc/cron.hourly are configured	High	8
<input type="checkbox"/>	1001981	5.1.4 Ensure permissions on /etc/cron.daily are configured	High	8
<input type="checkbox"/>	1001982	5.1.5 Ensure permissions on /etc/cron.weekly are configured	High	8
<input type="checkbox"/>	1001983	5.1.6 Ensure permissions on /etc/cron.monthly are configured	High	8
<input type="checkbox"/>	1001984	5.1.7 Ensure permissions on /etc/cron.d are configured	High	8

The table below displays the Cross Reference display formats in Tenable Security Center and Tenable Vulnerability Management:

In Tenable Security Center, the Cross References are displayed in [Scan Results](#) and [Vulnerability Analysis](#) in the format Type:ID:

In Tenable Vulnerability Management, the Cross References are displayed in a



Reference Information table under [Host Audit Details:](#)

### Reference Information

**800-171:** 3.5.7  
**800-53:** IA-5  
**CIP:** 007-6-R5  
**CN-L3:** 7.1.2.7(e)  
**CN-L3:** 7.1.3.1(b)  
**CSF:** PR.AC-1  
**HIPAA:** 164.308(a)(5)(ii)(D)  
**ISO/IEC-27001:** A.9.4.3  
**ITSG-33:** IA-5  
**LEVEL:** 1S  
**NESA:** T5.2.3  
**NIAv2:** AM19a  
**NIAv2:** AM19b  
**NIAv2:** AM19c  
**NIAv2:** AM19d  
**NIAv2:** AM22a  
**PCI-DSSv3.1:** 8.2.3  
**PCI-DSSv3.2:** 8.2.3  
**PCI-DSS:** 8.2.3  
**SANS-CSC:** 12-3  
**SANS-CSC:** 16-8  
**SWIFT-CSCv1:** 4.1  
**TBA-FIISB:** 26.2.1  
**TBA-FIISB:** 26.2.4  
**Cross References:** LEVEL:1S, 800-53:IA-5, CSF:PR.AC-1, ITSG-33:IA-5, HIPAA:164.308(a)(5)(ii)(D), ISO/IEC-27001:A.9.4.3, NESA:T5.2.3, SWIFT-CSCv1:4.1, CIP:007-6-R5, CN-L3:7.1.2.7(e),7.1.3.1(b), 800-171:3.5.7, NIAv2:AM19a,AM19b,AM19c,AM19d,AM22a, PCI-DSSv3.1:8.2.3, PCI-DSSv3.2:8.2.3, TBA-FIISB:26.2.1,26.2.4, auditFile:unix, PCI-DSS:8.2.3, SANS-CSC:12-3,16-8

**Failed**  
RESULT

**Active**  
FINDING STATE

#### Host Audit Information

AUDIT NAME	5.3.1 Ensure password creation requirements are configured - dcredit
AUDIT FILE	CIS_Debian_Linux_9_Server_v1.0.1_L1.audit
RESULT	Failed
STATE	ACTIVE

#### Audit Discovery

FIRST AUDIT	12/07/2021 at 07:03 AM
LAST AUDIT	06/08/2022 at 07:03 AM

#### Reference Information

800-171	3.5.2
800-53	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

The expected filter format syntax for searching, filtering, and querying in Tenable Security Center <XREF TYPE>|<XREF ID> uses a pipe, "|", rather than a colon, ":". In the GUI the XREF Type and ID are separated by a ":". Please note in the filter, you must use a pipe, "|". Using an example from above, 800-171 is the XREF Type, and 3.13.16 is the XREF ID. A search with proper syntax in Tenable Security Center that matches any item in the comma separated list is shown below, as used in the



Data Protection - Data at Rest - Encryption Compliance Tenable Security Center dashboard component template.

#### Data Protection - Data at Rest - Encryption Compliance

5 Items |

1 to 5 of 5

« < Page 1 of 1 > »

NAME	SEVERITY	TOTAL
6.14 Ensure Configuration File Encryption is Set	High	3
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
1.5.9 Ensure NIST FIPS-validated cryptography is configured - etc	High	1

Note: Spaces can be included or omitted after commas.

- *Cross References* = 800-171|3.13.16, 800-53|SC-28
- *Plugin Type*: Compliance
- *Severity*: Medium, High



Vulnerabilities

Vulnerability Summary

<

>

Apply

Customize

Clear All

Load Query

Cross References

=

800-171|3.13.16, 800-53|SC-28

Plugin Type

Active

Compliance

Event

Passive

Severity

Select All

Medium

High

6 Results

[Jump to Vulnerability Detail](#)

Export

Save

More

	PLUGIN ID	NAME	SEVERITY	TOTAL
<input type="checkbox"/>	1006529	6.14 Ensure Configuration File Encryption is Set	High	3
<input type="checkbox"/>	1011484	18.9.67.3 Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	High	2
<input type="checkbox"/>	1009460	1.5.9 Ensure NIST FIPS-validated cryptography is configured - rpm	High	1
<input type="checkbox"/>	1009461	1.5.9 Ensure NIST FIPS-validated cryptography is configured - grub	High	1
<input type="checkbox"/>	1009462	1.5.9 Ensure NIST FIPS-validated cryptography is configured - proc	High	1
<input type="checkbox"/>	1009463	1.5.9 Ensure NIST FIPS-validated cryptography is configured - etc	High	1

The following table displays valid Cross References that can be found in Tenable Vulnerability Management and Tenable Security Center:

Non-Compliance	Compliance
ALAS,ALSA,APPLE-SA,AUSCERT,BID,CERT,CERT-CC,CERT-FI,CERTA,CISA-KNOWN-EXPLOITED,CIS-NCAS,CISCO-BUG-ID,CISCO-SA,CISCO-SR,CLSA,CVE,CWE,DSA,EDB-ID,FEDORA,FLSA,FREEBSD,FreeBSD,GLSA,HP,HPSB,IAVA,IAVB,IAVT,ICS-ALERT,ICSA,JSA,MCAFEE-SB,MDKSA,MDVSA,MFSA,MGASA,MSFT,MSKB,MSVR,	800-171,800-53,8500.2,BSI-100-2,CAT,CCE,CCI,CCM-3,CIP,CIS_RECOMMENDATION,CN-L3,COBIT5,CSCV6,CSCV7,CSCV8,CSF,DISA_BENCHMARK,GDPR,GROUP-ID,HIPAA,ISOIEC-27001,ITSG-33,LEVEL,NESA,NIIV2,OPENSTACK,PCI,PCI-DSS,PCI-DSS-2.0,PCI-DSS-3.0,PCI-DSSV3.1,PCI-DSSV3.2,QCSC-V1,RULE-ID,SANS-CSC,STIG-ID,STIG-LEGACY,SWIFT-CSCV1,TBA-FIISB,VMWARE-ID,VMWARE-



Non-Compliance	Compliance
NSFOCUS,NessusID,OPENPKG-SA, OSVDB,OWASP,RHSA,RLSA,SECUNIA,SSA, SuSE,TLSA,TRA,TLSA,USN,VMSA,ZDI	PROFILE,VULN-ID

Below are some Cross Reference search examples that can be used in Tenable Security Center (xref refers to the Cross References filter):

- xref = 800-53|AC\*
  - Would be a match for AC-1, AC-2, etc.
- xref = 800-53|AC-1
  - Would be a match for AC-1, but not AC-11
- xref = 800-53|AC-1\*
  - Would be a match for AC-1, AC-11, AC-12, etc.
- xref = 800-53|SC-7 (5),800-53|SC-8
  - Would match 800-53|SC-7 (5) and 800-53|SC-8
- xref = 800-53|SC-7\*
  - Would match 800-53|SC-7 (5), 800-53|SC-7, 800-53|SC-71, etc.
- xref = 800-53|\*
  - Would match anything with 800-53 any xref ID
- xref = 800-53|\*7
  - Would match anything with XREF ID ending in 7
- xref = 800-53|S\*-7
  - Would match anything with XREF ID beginning with S and ending with "-7"



---

## Encryption Benefits

---

Encryption has garnered quite a lot of attention in recent years as cyber criminals have leveraged encryption to lock organizations out of their data through [ransomware attacks](#). Many companies have learned the hard way that encryption is very effective and difficult to break without the correct key. Organizations should take their cue from cyber criminals and leverage encryption themselves to protect their data from unauthorized access. Encryption costs very little to implement, but does require that a process be developed and implemented to manage encryption keys and ensure that multiple business owners have access to encryption keys. Encryption is required by many data protection regulations, such as PCI DSS and HIPAA, which levy heavy fines for violations. The migration to remote work requires an efficient, encrypted communication system, such as a VPN to protect data in transit.

Encrypting everything is not practical, since personnel still need to be productive. Developing a strategy for encryption can go a long way towards protecting data and saving the organization from costly data breaches and fines.





---

## Learn More

---

[COBIT \(An ISACA Framework\)](#)

[ISO About Us: Members](#)

[ISO/IEC 27001 Information Security Management](#)

[NIST Compliance FAQs: Federal Information Processing Standards \(FIPS\)](#)

[NIST Computer Security Resource Center \(CSRC\) Publications](#)

[NIST Cybersecurity Framework \(CSF\)](#)

[NIST Special Publication 800-52 Rev. 2 "Guidelines for the Selection, Configuration, and Use of Transport Layer Security \(TLS\) Implementations"](#)

[NIST Special Publication 800-53 Rev. 5 "Security and Privacy Controls for Information Systems and Organizations"](#)

[NIST Special Publication 800-111 "Guide to Storage Encryption Technologies for End User Devices"](#)

[PCI Document Library](#)

[Tenable Compliance and Audit Files Download](#)

[Tenable Host Audits Findings Details](#)

[Tenable Plugins Search](#)

[U.S. Department of Human & Health Services Health Information Privacy \(HIPAA\)](#)