

# CIS Control 10: Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

## Why is this CIS Control Critical?

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques.

Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, and removable media. Malware often relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives. Modern malware is designed to avoid, deceive, or disable defenses.

Malware defenses must be able to operate in this dynamic environment through automation, timely and rapid updating, and integration with other processes like vulnerability management and incident response. They must be deployed at all possible entry points and enterprise assets to detect, prevent spread, or control the execution of malicious software or code.

---

## 10.1: Deploy and Maintain Anti-Malware Software

Deploy and maintain anti-malware software on all enterprise assets.

Asset Type	Security Function	Implementation Groups
Devices	Detect	1, 2, 3

## Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

# Inputs

- 1. GV1 : Enterprise asset inventory
- 2. GV5 : Authorized software inventory
- 3. GV3 : Configuration standards

# Operations

- 1. Use GV1 to identify and enumerate assets capable of supporting anti-malware software:  
GV30 (M1)
- 2. Use GV5 to identify authorized anti-malware software: GV31
- 3. For each asset identified in Operation 1, use the output of Operation 2
  - 1. Identify and enumerate assets with at least one authorized anti-malware software installed: GV32 (M2)
  - 2. Identify and enumerate assets with only unauthorized anti-malware software installed (M3)
  - 3. Identify and enumerate assets without any anti-malware software installed (M4)
- 4. For each asset with a least one authorized anti-malware software installed from Operation 3.1, use GV3 to check configurations
  - 1. Identify and enumerate assets with properly configured anti-malware software (M5)
  - 2. Identify and enumerate assets with improperly configured anti-malware software (M6)

# Measures

- M1 = Count of assets capable of supporting anti-malware software
- M2 = Count of assets with at least one authorized anti-malware software installed
- M3 = Count of assets with only unauthorized anti-malware software installed
- M4 = Count of assets without any anti-malware software installed
- M5 = Count of assets with properly configured authorized anti-malware software installed
- M6 = Count of assets with improperly configured authorized anti-malware software installed

# Metrics

## Coverage

Metric	The percentage of assets with properly configured authorized anti-malware installe
Calculation	<span>M5 / M1</span>

# 10.2: Configure Automatic Anti-Malware Signature Updates

Configure automatic updates for anti-malware signature files on all enterprise assets.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

## Dependencies

- Safeguard 10.1: Deploy and Maintain Anti-Malware Software

## Inputs

- GV30** : Assets capable of supporting anti-malware software
- GV31** : Assets with at least one authorized anti-malware software installed
- GV3** : Configuration standards

## Operations

- For each asset in Input 2 **GV31** , check configurations **GV3** to determine if anti-malware software is configured to automatically update signature files
  - Identify and enumerate assets properly configured for automatic updates (M2)
  - Identify and enumerate assets not properly configured for automatic updates (M3)

## Measures

- M1 = Count of **GV30**
- M2 = Count of assets configured to automatically update signature files
- M3 = Count of assets not configured to automatically update signature files

## Metrics

### Coverage

Metric	The percentage of assets properly configured to automatically update signature file
Calculation	<b>M2 / M1</b>

# 10.3: Disable Autorun and Autoplay for Removable Media

Disable autorun and autoplay auto-execute functionality for removable media.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

## Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

## Inputs

1. GV1: Enterprise asset inventory
2. GV3: Configuration standards

## Operations

1. Use GV1 to identify and enumerate enterprise assets capable of performing autorun, autoplay, and auto-execute functions (M1)
2. Check the configurations GV3 of each asset identified in Operation 1 to see if the autorun, autoplay, and auto-execute functions are disabled
  1. Identify and enumerate properly configured assets (M2)
  2. Identify and enumerate improperly configured assets (M3)

## Measures

- M1 = Count of assets capable of performing autorun, autoplay, and auto-execute functions
- M2 = Count of assets properly configured to disable functions
- M3 = Count of assets not properly configured to disable functions

## Metrics

## Compliance

Metric	The percentage of assets properly configured to disable autorun, autoplay, and auto
Calculation	<span>M2 / M1</span>

# 10.4: Configure Automatic Anti-Malware Scanning of Removable Media

Configure anti-malware software to automatically scan removable media.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

## Dependencies

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 10.1: Deploy and Maintain Anti-Malware Software

## Inputs

1. GV30: Assets capable of supporting anti-malware software
2. GV32: Assets with at least one authorized anti-malware software installed
3. GV3: Configuration standards

## Operations

1. For each asset in Input 2 GV32, use configurations GV3 to identify if the software is configured to automatically scan removable media
  1. Identify and enumerate assets with properly configured software (M2)
  2. Identify and enumerate assets with improperly configured software (M3)

## Measures

- M1 = Count of GV30
- M2 = Count of assets with anti-malware properly configured to scan removable media
- M3 = Count of assets with anti-malware not properly configured to scan removable media

## Metrics

### Coverage

Metric	The percentage of assets with properly configured software to automatically scan r
Calculation	<span>M2 / M1</span>

 Read the Docs

 latest

# 10.5: Enable Anti-Exploitation Features

Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

## Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

## Inputs

1. GV1: Enterprise asset inventory
2. GV3: Configuration standards

## Operations



1. For each asset in GV1, use configuration standards GV3 to determine if it is properly configured to enable anti-exploitation features
  1. Identify and enumerate assets properly configured to enable anti-exploitation features (M2)
  2. Identify and enumerate assets not properly configured to enable anti-exploitation features (M3)

## Measures

- M1 = Count of GV1
- M2 = Count of assets properly configured to enable anti-exploitation features
- M3 = Count of assets not properly configured to enable anti-exploitation features

## Metrics

### Coverage

Metric	The percentage of assets properly configured to enable anti-exploitation features		
Calculation	<span>M2 / M1</span>	 Read the Docs	 latest



# 10.6: Centrally Manage Anti-Malware Software

Centrally manage anti-malware software.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

## Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 10.1: Deploy and Maintain Anti-Malware Software

## Inputs

1. **GV30**: Assets capable of supporting anti-malware software
2. **GV31**: Authorized anti-malware software

## Operations

1. For each authorized anti-malware software **GV31**, check if it is centrally managed
  1. Identify and enumerate anti-malware software that is centrally managed (M2)
  2. Identify and enumerate anti-malware software that is not centrally managed (M3)

## Measures

- M1 = Count of **GV31**
- M2 = Count of authorized anti-malware software that is centrally managed
- M3 = Count of authorized anti-malware software that is not centrally managed

## Metrics

### Coverage

Metric	The percentage of anti-malware centrally managed
Calculation	$M2 / M1$

# 10.7: Use Behavior-Based Anti-Malware So

 Read the Docs

 latest

Use behavior-based anti-malware software.

Asset Type	Security Function	Implementation Groups
Devices	Detect	2, 3

## Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

## Inputs

1. **GV1**: Enterprise asset inventory
2. **GV5**: Authorized software inventory
3. **GV3**: Configuration standards

## Operations

1. Use **GV1** to identify and enumerate assets capable of supporting behavior-based anti-malware software (M1)
2. Use **GV5** to identify authorized behavior-based anti-malware software
3. For each asset identified in Operation 1, use the output of Operation 2
  1. Identify and enumerate assets with at least one authorized behavior-based anti-malware software installed (M2)
  2. Identify and enumerate assets without any behavior-based anti-malware software installed (M3)
4. For each asset with a least one authorized behavior-based anti-malware software installed from Operation 3.1, use **GV3** to check configurations
  1. Identify and enumerate assets with properly configured behavior-based anti-malware software (M4)
  2. Identify and enumerate assets with improperly configured behavior-based anti-malware software (M5)

## Measures

- M1 = Count of assets capable of supporting behavior-based anti-malware software
- M2 = Count of assets with at least one authorized behavior-based anti-malware software installed
- M3 = Count of assets without any behavior-based anti-malware software installed
- M4 = Count of assets with properly configured authorized behavior-based anti-malware software installed
- M5 = Count of assets with improperly configured authorized behavior-based anti-malware software installed



# Metrics

## Coverage

Metric	The percentage of assets with properly configured authorized behavior-based anti-i
Calculation	<div>M4 / M1</div>