A practical guide to understanding and verifying anti-malware functionality across platforms.

python-docx

Windows & Linux Anti-malware System

Lalit Mangale

2025

Windows & Linux Anti-malware System: Functionality and Verification Guide

Table of Contents

[Scope 1](#_Toc196470522)

[1. Introduction 2](#_Toc196470523)

[2. Windows Antimalware System: Microsoft Defender Antivirus 2](#_Toc196470524)

[2.1. Test Detection with EICAR File 2](#_Toc196470525)

[2.2. Reviewing Logs and Events 3](#_Toc196470526)

[2.3. Command-Line Checks Using PowerShell 3](#_Toc196470527)

[2.4. Verify Defender Definitions Are Updated 5](#_Toc196470528)

[3. Linux Antimalware System: ClamAV 5](#_Toc196470529)

[3.1. Update Your System 5](#_Toc196470530)

[3.2. Install ClamAV and ClamAV Daemon 5](#_Toc196470531)

[3.3. Update Virus Definitions 6](#_Toc196470532)

[3.4. Scan Your System 6](#_Toc196470533)

[3.5. Automatically Remove Infected Files 7](#_Toc196470534)

[3.6. Start Real-Time Scanning (Checking Running status) 7](#_Toc196470535)

[4. EICAR: 8](#_Toc196470536)

[5. Paid Antivirus Options for Windows and Linux: 8](#_Toc196470537)

# Scope

This document provides a comprehensive approach to verifying the operational status and functionality of antimalware systems on both Windows and Linux platforms. It covers both manual and automated techniques, introduces the relevant tools (Windows Defender for Windows, ClamAV for Linux), and includes a Proof of Concept (PoC) section with actionable examples. The guide is ideal for system administrators, security auditors, and technical professionals responsible for endpoint protection.

# 1. Introduction

Cyber threats evolve rapidly, and ensuring that antimalware solutions are functioning correctly is critical for maintaining endpoint security. Both Windows Defender (built into modern Windows systems) and ClamAV (a lightweight, open-source Linux antivirus) provide foundational protection.  
  
This document outlines the verification process for each platform's antimalware tools, focusing on real-time monitoring, system logs, command-line status checks, and malware test files.

# 2. Windows Antimalware System: Microsoft Defender Antivirus

## 2.1. Test Detection with EICAR File

The EICAR test file is a widely accepted method for verifying antivirus functionality without introducing actual malware.

Steps:  
1. Open Notepad or any plain text editor.  
2. Paste the following line: (signature file)  
 X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\*  
3. Save the file with the .txt extension.  
4. Defender should automatically detect and either quarantine or remove the file.  
5. A notification should appear in the system tray.

|  |  |
| --- | --- |
|  |  |
| **Type in Notepad** | **Save as .txt format** |
| **Threat (.txt) file detected by Win Defender** | **Threat Quarantine by Win Defender** |

## 2.2. Reviewing Logs and Events

Open Windows Security > Virus & threat protection to review scan history, quarantined items, and protection logs. For detailed logs, go to Event Viewer > Applications and Services Logs > Microsoft > Windows > Windows Defender.

## 2.3. Command-Line Checks Using PowerShell

Use the following command to check Defender’s detailed status:  
Get-MpComputerStatus

|  |
| --- |
|  |

This show:

RealTimeProtechtionEnable: True/False

AntiSpywareSignatiureVersion: 1.427.385.0

QuickScanStartTime : 23-04-2025 13:00:16

QuickScanEndTime : 23-04-2025 13:01:05

**Note : we can conform that AntiSpywareSignatiureVersion from** [**HERE**](https://www.microsoft.com/en-us/wdsi/defenderupdates)

## 2.4. Verify Defender Definitions Are Updated

Use the following command to check version info: Powershell   
Get-MpComputerStatus | Select-Object -Property AMEngineVersion, AMProductVersion, AVSignatureVersion, NISSignatureVersion

|  |
| --- |
|  |

# 3. Linux Antimalware System: ClamAV

## 3.1. Update Your System

Run: sudo apt update && sudo apt upgrade

|  |
| --- |
| **Update your Linux Machine by following Command** |

## 3.2. Install ClamAV and ClamAV Daemon

Run: sudo apt install clamav clamav-daemon

|  |
| --- |
| **Install ClamAV in your machine** |

## 3.3. Update Virus Definitions

Run: sudo freshclam

|  |
| --- |
| **Update Virus Database (if you use VM or Dual Boot Please turn off Windows Defender)** |

## 3.4. Scan Your System

Run: sudo clamscan -r /(mention your Path)

|  |
| --- |
| **Threat Found : EICAR file** |

## 3.5. Automatically Remove Infected Files

Run: sudo clamscan --remove -r / (Mention your Patch)

|  |
| --- |
| **Threat removed successfully** |

## 3.6. Start Real-Time Scanning (Checking Running status)

Run: sudo systemctl status clamav-daemon

|  |
| --- |
| **ClamAV running status check: Active** |

# 4. EICAR:

The **EICAR Standard Anti-Virus Test File** is a harmless file developed by the **European Institute for Computer Antivirus Research (EICAR)**. It’s designed to allow IT professionals to safely test antivirus software without using actual malware.

**🧾 Key Points:**

* The file is **100% safe** and cannot harm your computer.
* Visit the official EICAR website: <https://www.eicar.org/>

# 5. Paid Antivirus Options for Windows and Linux:

|  |  |  |  |
| --- | --- | --- | --- |
| **Antivirus Software** | **Supported OS** | **Features** | **Ideal For** |
| **Bitdefender Total Security** | Windows, Linux | Multi-layer malware protection, anti-phishing, cloud-based AI detection | Home & small businesses |
| **ESET NOD32 / Smart Security** | Windows, Linux | Lightweight, fast scanning, UEFI & ransomware protection | Personal use, technical users |
| **Kaspersky Premium** | Windows, Linux | Web filtering, privacy tools, real-time protection | Families, professionals |
| **McAfee Total Protection** | Windows, Linux | Identity theft protection, VPN, device management | Home & multi-device households |
| **Norton 360** | Windows | Full system protection, cloud backup, VPN, dark web monitoring | General home users |
| **Sophos Antivirus** | Linux | Heuristic scanning, command-line and central management | Servers, IT admins |
| **Trend Micro Server Protect** | Linux | Server-focused AV, real-time scanning, admin dashboards | Enterprise Linux environments |
| **Kaspersky Endpoint Security** | Linux | Behaviour monitoring, policy control, enterprise integration | Corporate Linux systems |
| **Bitdefender Gravity Zone** | Windows, Linux | Endpoint security, ransomware protection, centralized management | Businesses, IT teams |