

Windows 11 Endpoint Security Hardening Lab

Author: Kerolos Saeed

Date: December 28, 2025

Environment: Windows 11 Home (Local Machine)

1. Lab Objective

The objective of this lab is to **verify, configure, and document endpoint security controls** on a Windows 11 system.

This lab focuses on **malware protection, ransomware mitigation, encryption, and security updates**, aligning with **CompTIA A+ Core 2 (220-11202) Security Domain** and real-world IT support practices.

2. Tools & Technologies Used

- Windows 11 Security (Microsoft Defender)
 - Microsoft Defender Antivirus
 - Windows Device Encryption (BitLocker integration)
 - OneDrive (Ransomware recovery support)
-

3. Security Controls Verified

3.1 Microsoft Defender Antivirus

The following antivirus protections were verified as **enabled and functioning**:

- Real-time protection: **ON**
- Cloud-delivered protection: **ON**
- Dev Drive protection: **ON**
- Security intelligence: **Up to date**

A **Quick Scan** was executed to validate malware detection functionality.

Scan Results:

- Files scanned: **43,609**
- Threats detected: **0**
- Scan completed successfully

Security Impact:

Real-time and cloud-based protection help detect and block malware, ransomware, spyware, and other threats before they can execute.

3.2 Ransomware Protection (Controlled Folder Access)

Ransomware protection was reviewed and confirmed:

- Controlled Folder Access: **ON**
- Protected folders enabled
- Block history available for review
- Application allow-list option available

Security Impact:

Controlled Folder Access prevents unauthorized applications from modifying critical files, helping mitigate ransomware encryption attacks.

3.3 Device Encryption

Device encryption settings were verified under Windows Privacy & Security:

- Device Encryption: **ON**
- BitLocker drive encryption integration available
- Recovery key management option visible

Security Impact:

Encryption protects data **at rest**, ensuring files remain unreadable if the device is lost or stolen.

3.4 Security Updates

Security intelligence updates were verified:

- Defender security intelligence version confirmed
- Last update timestamp verified
- Automatic update process functioning

Security Impact:

Up-to-date security intelligence ensures protection against the latest malware signatures and attack techniques.

4. Results Summary

Security Feature	Status
Real-Time Antivirus	Enabled
Cloud Protection	Enabled
Ransomware Protection	Enabled
Device Encryption	Enabled

Security Updates	Up to Date
Malware Scan	Completed (No Threats)

5. Skills Demonstrated

- Endpoint security verification
 - Malware protection validation
 - Ransomware mitigation controls
 - Data-at-rest encryption awareness
 - Security posture assessment
 - Documentation and reporting
-

6. Relevance to IT & Cybersecurity Roles

This lab reflects **real tasks performed by:**

- IT Support / Help Desk
- SOC Tier 1 Analysts
- System Administrators

It demonstrates hands-on familiarity with **Windows endpoint protection**, a core responsibility in enterprise environments.

7. Conclusion

In this lab, Windows 11 endpoint security controls were successfully verified and documented. The system was confirmed to be protected against malware, ransomware, and unauthorized access, with encryption and security updates enabled to support defense-in-depth.

8. Screenshots

(

Ransomware protection

Protect your files against threats like ransomware, and see how to restore files in case of an attack.



Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.



On

[Block history](#)

[Protected folders](#)

[Allow an app through Controlled folder access](#)

Ransomware data recovery

You may be able to recover files in these accounts in case of a ransomware attack.

OneDrive - Personal

keroloss506@gmail.com

Free account with individual file recovery.

[View files](#)

Virus & threat protection updates

Security intelligence is up to date.

Last update: 12/28/2025 1:37 AM

Protection updates

Privacy & security > Device encryption

Device encryption helps protect your files and folders from unauthorized access in case your device is lost or stolen. [More about device encryption](#)

Device encryption

Encrypt data on this device to help protect from offline, unauthorized access

On

Related

BitLocker drive encryption

Manage your encryption settings using BitLocker



Find your BitLocker recovery key



Related support

Help with Device encryption



[Enabling Device Encryption on your device](#)

 Get help

 Give feedback

1:37 AM

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Dev Drive protection

Scans for threats asynchronously on Dev Drive volumes to reduce performance impact.

On

[See volumes](#)
[Learn more](#)

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Help improve Windows Security
[Give us feedback](#)

Change your privacy settings
View and change privacy settings for your Windows 11 Home device.
[Privacy settings](#)
[Privacy dashboard](#)
[Privacy Statement](#)



Protection updates

View information about your security intelligence version, and check for updates.

Security intelligence

Microsoft Defender Antivirus uses security intelligence to detect threats. We try to automatically download the most recent intelligence to protect your device against the newest threats. You can also manually check for updates.

Security intelligence version: 1.443.371.0
Version created on: 12/27/2025 7:02 PM
Last update: 12/27/2025 11:24 PM

 Checking for updates...

Home

- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control
- Device security
- Device performance & health
- Family options
- Protection history

Settings

Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 12/27/2025 2:11 AM (quick scan)
0 threats found.
Scan lasted 3 minutes 11 seconds
43609 files scanned.

[Quick scan](#)

[Scan options](#)

[Allowed threats](#)

[Protection history](#)

Virus & threat protection settings

No action needed.

[Manage settings](#)

Virus & threat protection updates

Security intelligence is up to date.
Last update: 12/27/2025 11:24 PM

[Protection updates](#)

Have a question?
[Get help](#)

Who's protecting me?
[Manage providers](#)

Help improve Windows Security
[Give us feedback](#)

Change your privacy settings
View and change privacy settings for your Windows 11 Home device.
[Privacy settings](#)
[Privacy dashboard](#)
[Privacy Statement](#)

- Microsoft Defender overview
- Ransomware protection settings
- Device encryption status
- Malware scan results