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 (220-1202) 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.

---

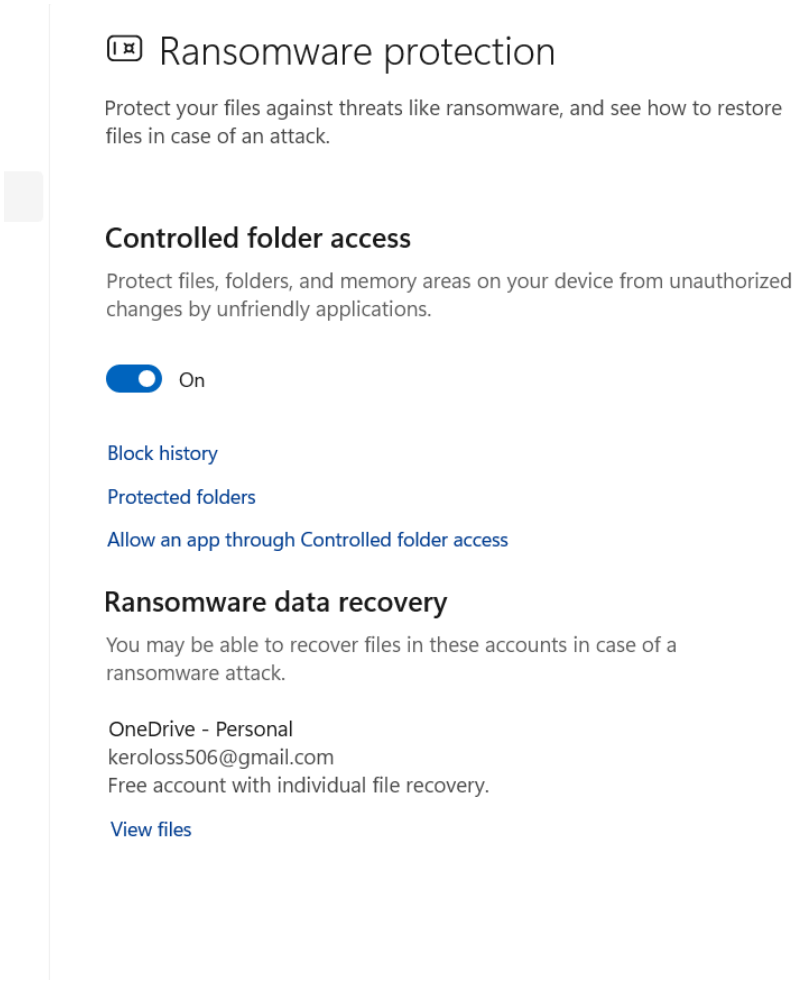
7. Conclusion

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

(

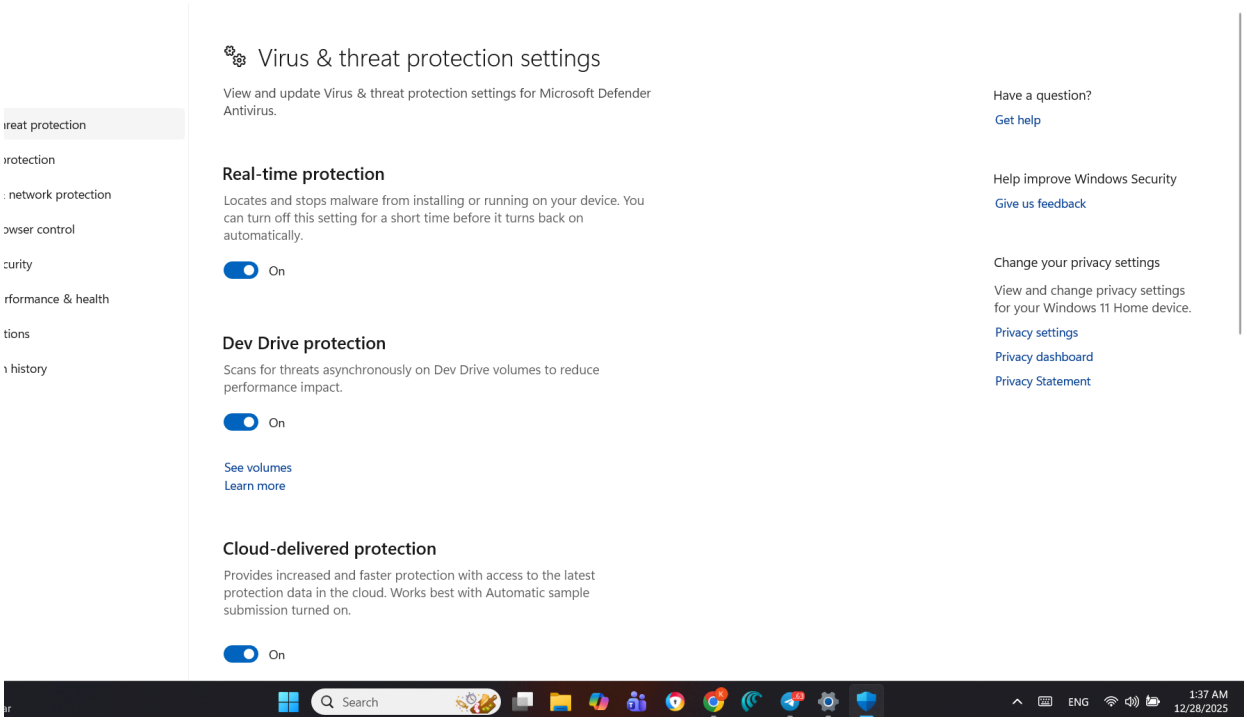


Virus & threat protection updates

Security intelligence is up to date.

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

Protection updates



Protection updates

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

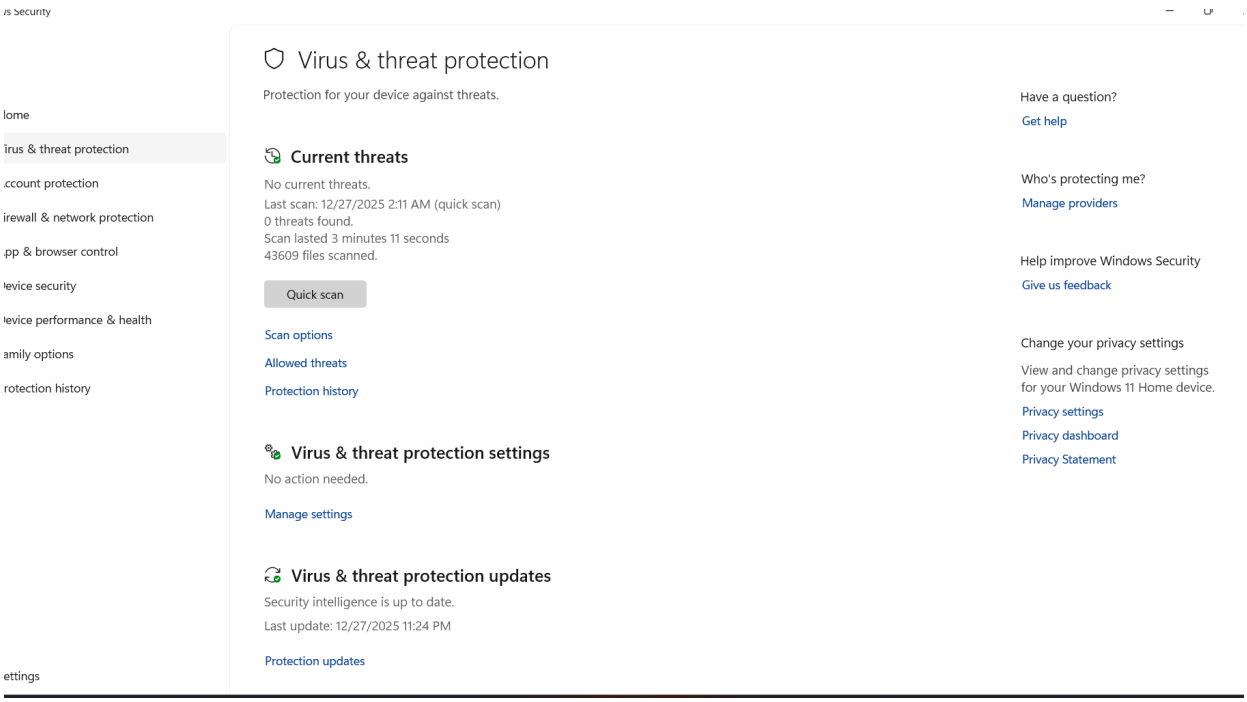
Security intelligence

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...

Cancel



)

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