Windows Endpoint Security Hardening Report

Client Deliverable – v1.0
Prepared by: Joshua Rodriguez
Date: December 3, 2025

---

1. Executive Summary

This report documents the security hardening of a Windows 11 endpoint. The objective of the project was to assess the device's baseline security posture, apply industry-standard hardening controls, verify Microsoft Defender Antivirus and Firewall configurations, review account protections, strengthen reputation-based protection settings, and confirm hardware-based security features including core isolation.

This hardening process improves protection against malware, network intrusion attempts, malicious applications, phishing attacks, and unauthorized access.

---

2. System Overview

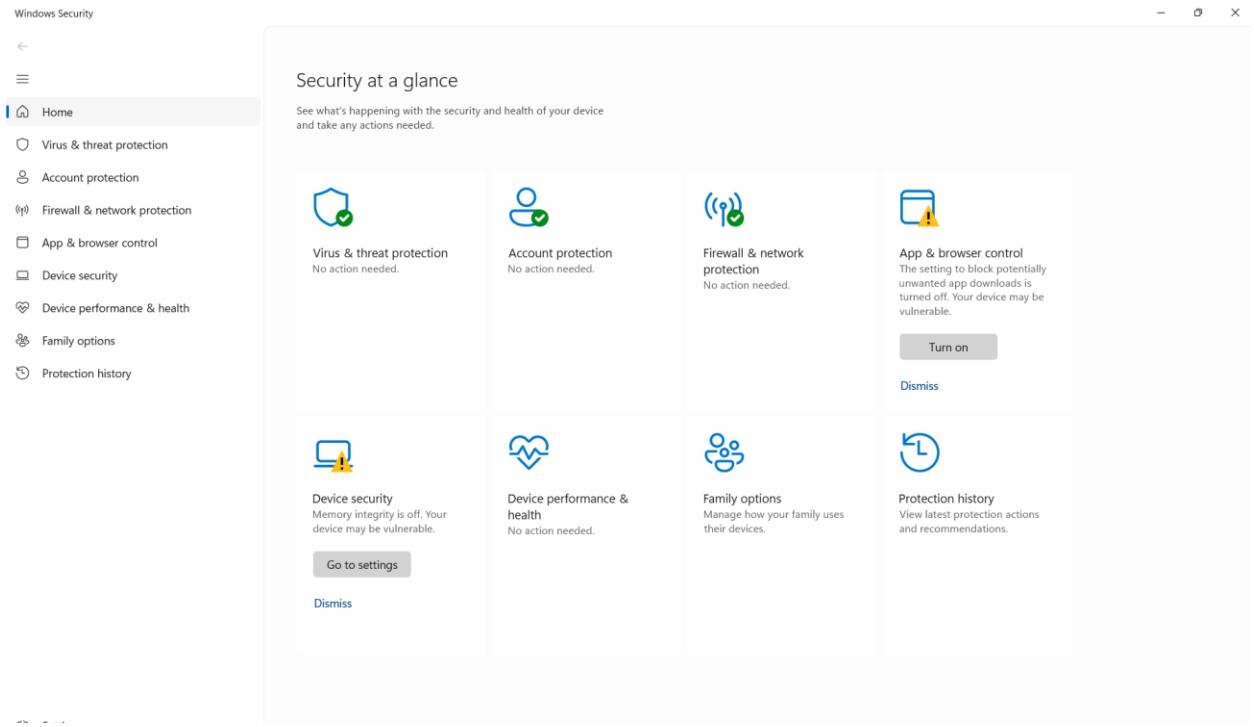
Category	Details
Operating System	Windows 11 Home
Version	24H2
Device Type	Laptop
Security Stack	Microsoft Defender Antivirus, Microsoft Defender Firewall, SmartScreen, Core Isolation

---

3. Baseline Security Posture

An initial review of the Windows Security dashboard was conducted to assess the current state of the endpoint's defenses.

Screenshot:



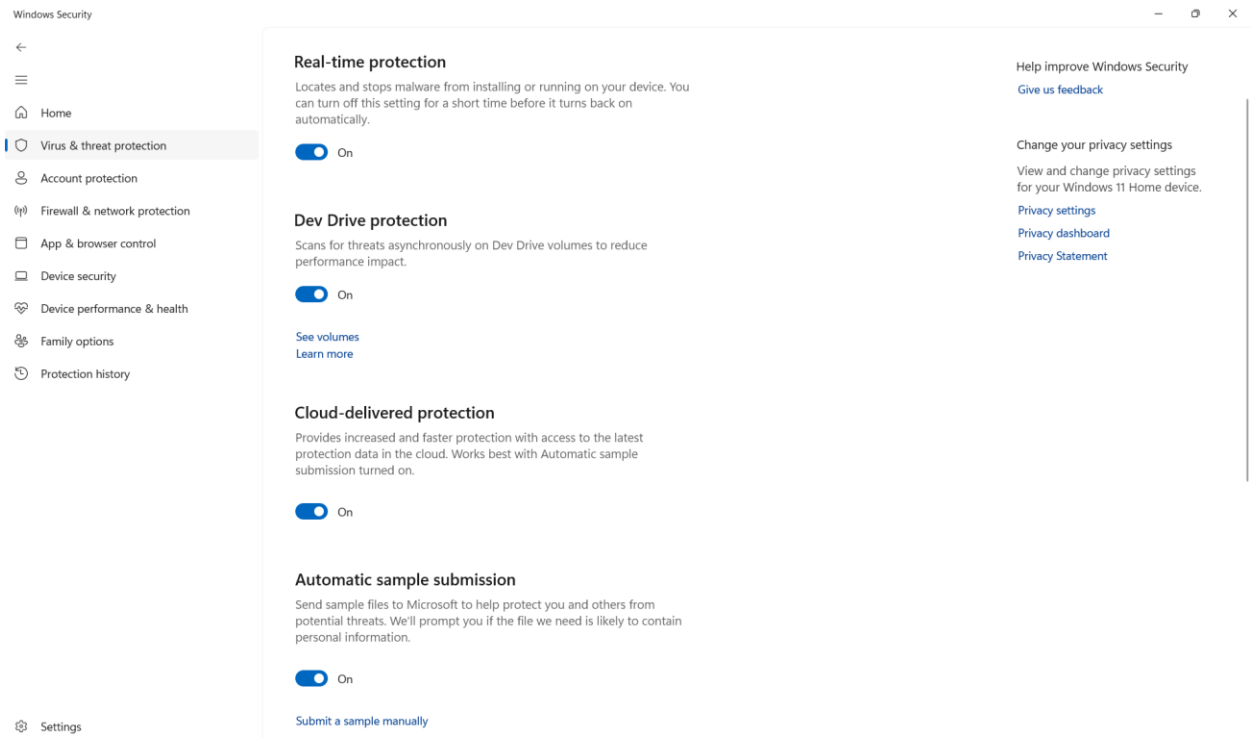
---

4. Security Enhancements Performed

4.1 Antivirus & Threat Protection

Actions completed:

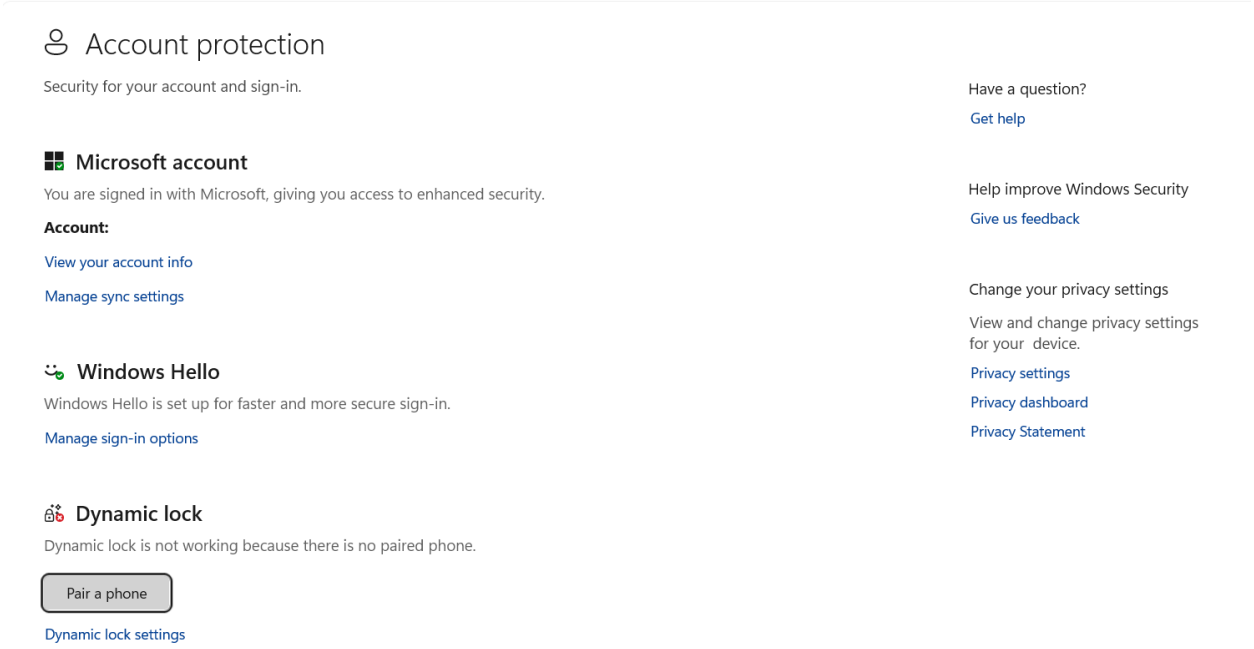
- Verified Microsoft Defender Antivirus was enabled and active.
- Enabled:
  - Real-time protection
  - Cloud-delivered protection
  - Automatic sample submission
  - Tamper Protection
- Reviewed threat history to confirm no active threats.
- (Optional): Performed a quick scan to validate system health.



4.2 Account Protection (Identity Security)

Items reviewed:

- Microsoft account linked (email omitted for privacy).
- Windows Hello PIN configured for secure sign-in.
- Dynamic Lock not configured (optional feature).
- Status confirmed as “No actions needed.”



4.3 Firewall & Network Protection

The following items were reviewed and configured:

- Firewall enabled for ALL profiles (Private, Public).
- Public profile inbound rules configured more restrictively for untrusted networks.

Private network

Networks at home or work, where you know and trust the people and devices on the network, and where your device is set as discoverable.

Active private networks

Not connected

Microsoft Defender Firewall

Helps protect your device while on a private network.

On

Public network

Networks in a public place such as an airport or coffee shop, and where your device is set as not discoverable.

Active public networks

Microsoft Defender Firewall

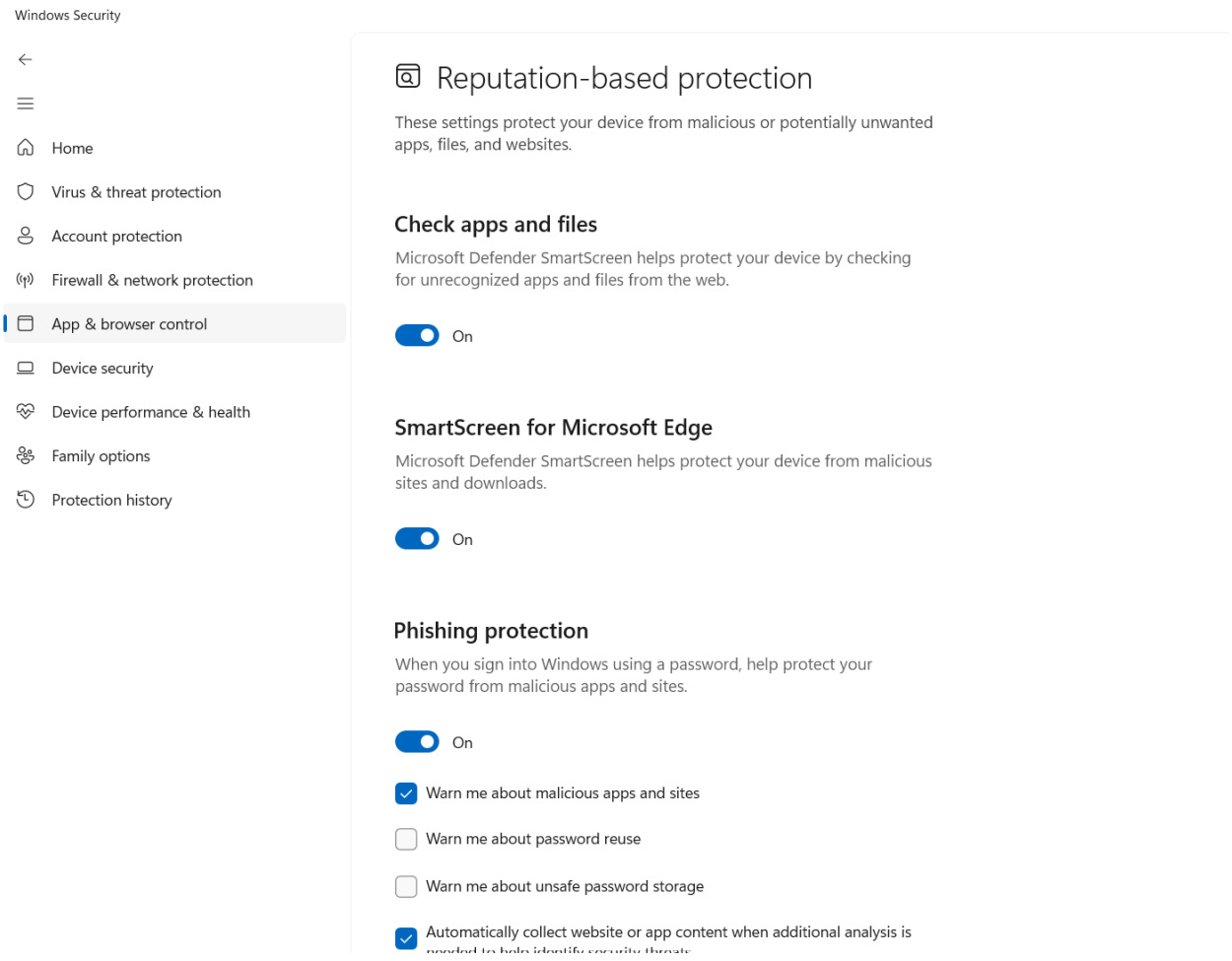
Helps protect your device while on a public network.

On

4.4 App & Browser Control (SmartScreen & Reputation Protection)

Strengthened application and browser security by enabling:

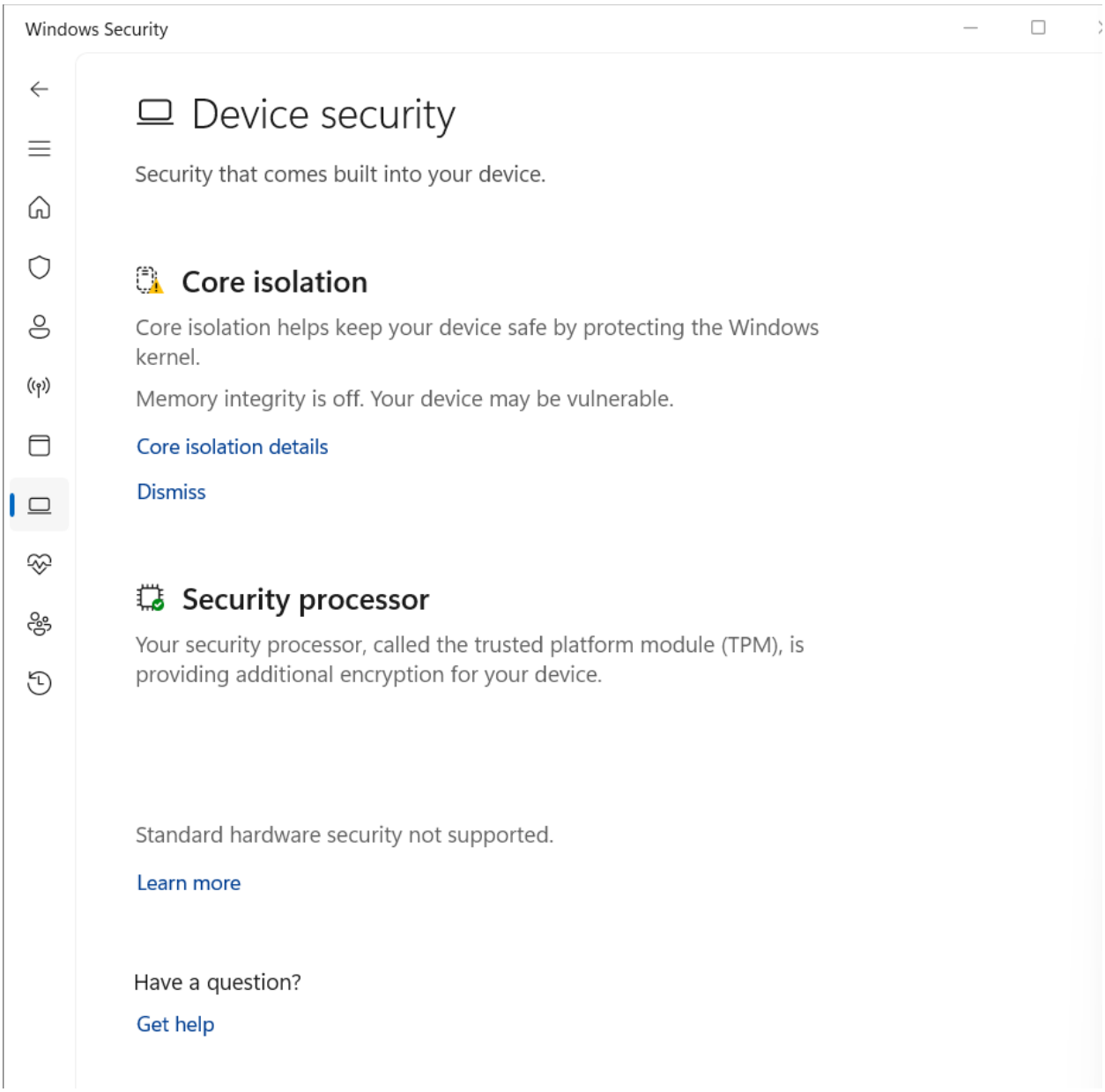
- Reputation-based protection
- SmartScreen for Microsoft Edge
- SmartScreen for Microsoft Store apps
- Potentially unwanted app (PUA) blocking

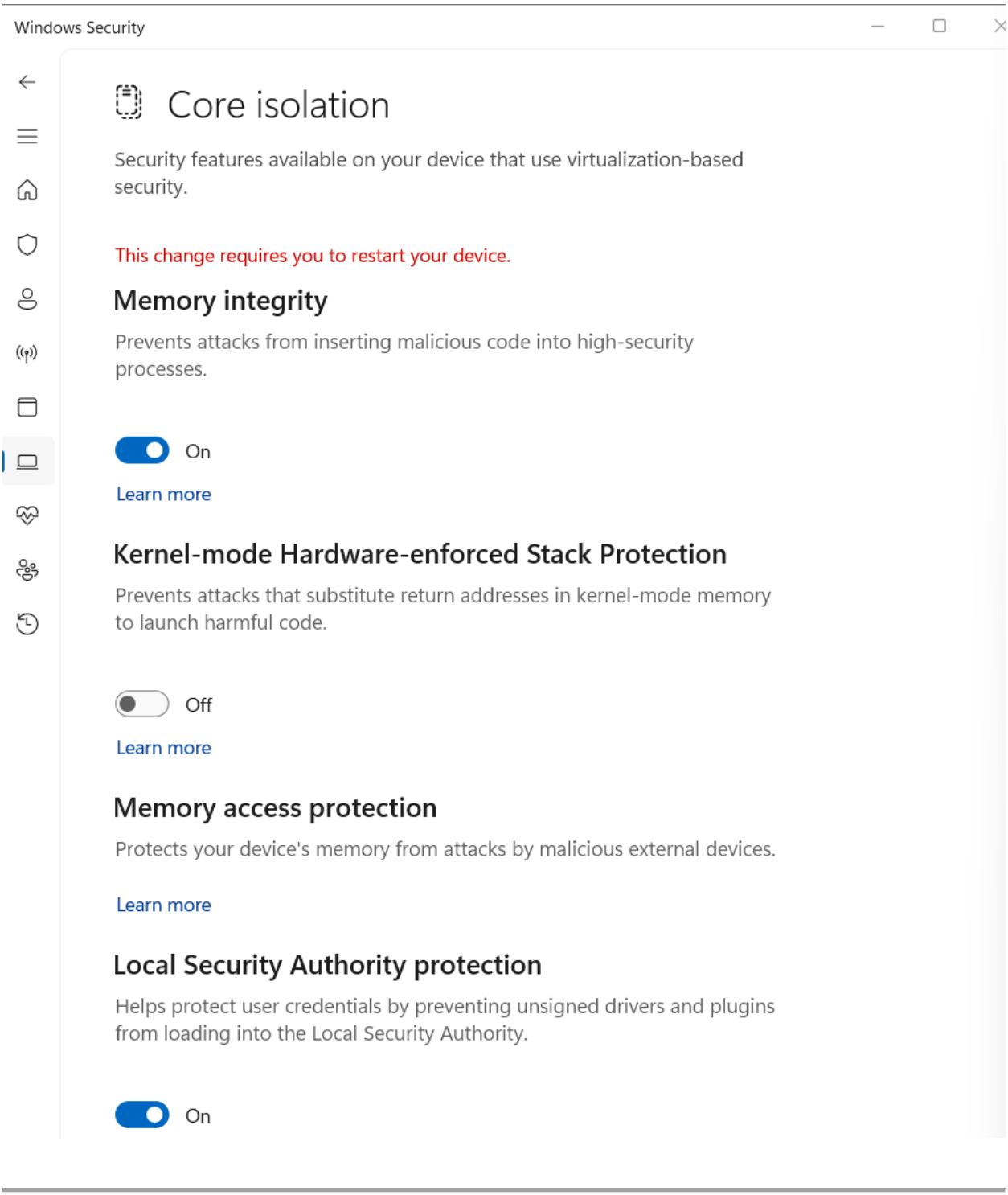


4.5 Device Security (Hardware Security)

Reviewed and verified:

- Secure Boot
- Core Isolation / Memory Integrity
- Virtualization-based security readiness


Windows Security
Device security
Security that comes built into your device.
Core isolation
Core isolation helps keep your device safe by protecting the Windows kernel.
Memory integrity is off. Your device may be vulnerable.
Core isolation details
Dismiss
Security processor
Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.
Standard hardware security not supported.
Learn more
Have a question?
Get help



4.6 PowerShell Verification

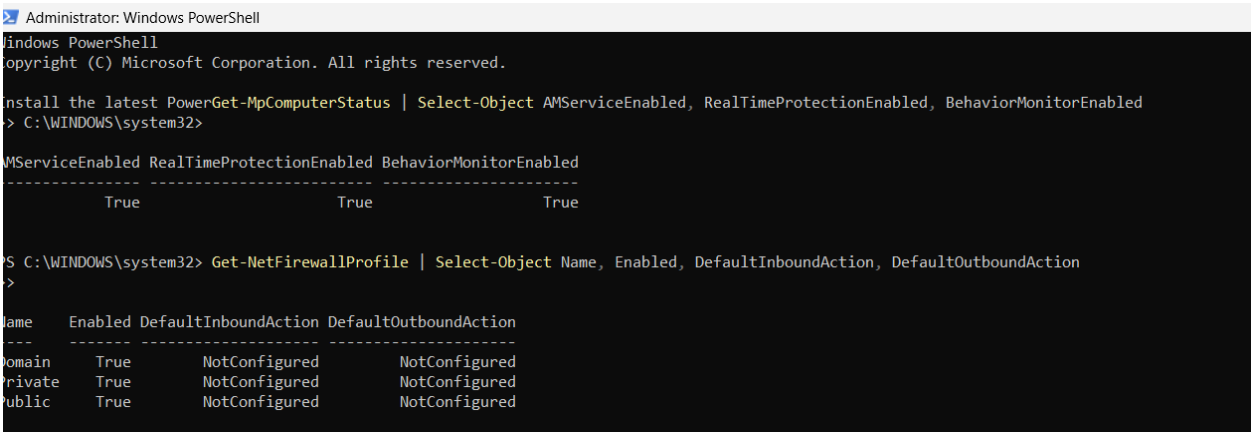
To confirm configuration integrity, PowerShell was used:

Commands:

```
Get-MpComputerStatus | Select-Object AMServiceEnabled,
RealTimeProtectionEnabled, BehaviorMonitorEnabled
Get-NetFirewallProfile | Select-Object Name, Enabled, DefaultInboundAction,
DefaultOutboundAction
```

These commands verified:

- Microsoft Defender services were enabled
- Real-time protection was active
- Firewall profiles were enabled
- Inbound/outbound actions followed secure defaults



---

5. Results Summary

After applying hardening steps, the endpoint now has:

- Fully enabled Microsoft Defender Antivirus
- Active SmartScreen filtering
- Firewalls enabled across all profiles
- Reputation-based protection and PUA blocking
- Hardware-based protections (core isolation, memory integrity)
- Verified system integrity through PowerShell

This brings the device's security posture in line with widely recommended baseline hardening guidelines.

---

6. Recommendations

To maintain strong security posture:

- Keep Windows and Microsoft Defender fully updated weekly
- Do not disable real-time protections unless performing trusted tasks
- Use a strong PIN or password with a linked Microsoft account
- Run routine quick scans weekly and full scans monthly
- Avoid installing unknown or unsigned applications
- Maintain SmartScreen and PUA blocking enabled
- Avoid connecting to untrusted Wi-Fi without a VPN

---

7. Conclusion

This endpoint has been successfully hardened using built-in Windows and Microsoft Defender security controls. The device is now significantly more resistant to malware, phishing attempts, network-based attacks, and unauthorized access.

This report can be used as a template for improving additional endpoints or designing client-level security policies.