FIELD CISO ADVISORY

STRATEGIC FORSIGHT,
HUMAN WISDOM

FIELD SECURITY REPORT

MICROSOFT DEFENDER FOR ENDPOINT ONBOARDING

RESEARCHED AND TESTED BY:
Nipun Juneja
Tanish Bhandari

JULY 2025

EXECUTIVE SUMMARY

- FieldCISO Advisory Services evaluated Microsoft Defender for Endpoint (MDE) Plan 1 — included with Microsoft 365 E3 — for onboarding across Windows Server (2025, 2022, 2012 R2) and Windows client (7 Enterprise SP1, 8.1, 10, 11) systems.

- Modern systems (Windows 10, 11, Server 2025) onboarded seamlessly using a single script.

- Windows Server 2022 required manual installation of Microsoft Defender Antivirus via PowerShell for full functionality.

- Windows Server 2012 R2, which is only partially supported via the Microsoft Monitoring Agent (MMA), required undocumented updates provided by Microsoft support — after a 7–8 day response period — to complete onboarding successfully.

- Windows 7 Enterprise SP1 and 8.1, claimed as supported in Microsoft's documentation, could not be onboarded despite full patching and support intervention.

- Findings highlight significant discrepancies in Microsoft's documentation for legacy systems.

- Organizations with a mix of legacy and modern operating systems will only be able to fully leverage Microsoft Defender for Endpoint on modern, fully updated systems, and should prioritize these for effective deployment.

INTRODUCTION AND DEPLOYMENT INSIGHTS

Microsoft Defender for Endpoint (MDE) is an enterprise-grade security platform designed to provide advanced threat protection, detection, and response capabilities across Windows operating systems. As organizations maintain diverse environments with both modern and legacy systems, understanding the practical challenges of onboarding MDE is critical for effective endpoint security.

This report, prepared by FieldCISO Advisory Services, examines the onboarding experience across Windows Server 2025, 2022, 2012 R2, and Windows 7 Enterprise SP1, 8.1, 10, and 11, focusing on the requirement for fully patched systems, the complexities of legacy system support via the Microsoft Monitoring Agent (MMA), and discrepancies between Microsoft’s documentation and real-world outcomes. The findings aim to assist enterprises in navigating MDE deployments in mixed operating system environments.

METHODOLOGY

ONBOARDING PROCESS

1. Tools Used:

- Modern systems (Windows 10, 11, Server 2025, 2022): Onboarding script from the Microsoft Defender portal, executed via PowerShell or Microsoft Endpoint Configuration Manager (MECM).
- Legacy systems (Windows 7 Enterprise SP1, 8.1, Server 2012 R2): Microsoft Monitoring Agent (MMA) with manual prerequisite installations.
- Windows Server 2022: Manual installation of Microsoft Defender Antivirus via PowerShell due to the absence of a pre-installed antivirus solution.

2. Prerequisites: All systems were fully patched with the latest cumulative updates, including SHA-2 support and TLS 1.2 configurations, as per Microsoft's documentation. For Server 2012 R2, additional undocumented updates were applied following Microsoft support guidance.

3. Connectivity: Connectivity to the Microsoft Defender portal was verified using device inventory and health status checks in the portal.

4. Data Collection: Onboarding logs, Defender portal alerts, and system event logs were monitored to identify errors, delays, or failures.

5. Support Interaction: Microsoft support was contacted for onboarding issues with Windows 7 Enterprise SP1, 8.1, and Server 2012 R2 to resolve persistent failures.

6. Licensing: Licensing: A valid Microsoft 365 E3 license was used during testing, which includes access to Microsoft Defender for Endpoint Plan 1. This allowed us to evaluate core threat detection, suitable for baseline enterprise endpoint security scenarios.

ONBOARDING EXPERIENCE BY OPERATING SYSTEMS

The following table summarizes the onboarding experiences across tested operating systems, all fully patched to meet MDE requirements, with CyberEase Ratings assigned by FieldCISO Advisory Services (1–5 stars, 5 being the best, 1 being the worst):

On boarding experience comparison

Operating System	Onboarding Method	Official Support	Notes/Challenges	CyberEase Rating
Windows 11	MDE Portal Script	Yes	Seamless onboarding; completed in approximately 20 minutes; full EDR and antivirus integration.	★★★★★ (5/5)
Windows 10	MDE Portal Script	Yes	Smooth onboarding; completed in approximately 25 minutes; no issues post-patching.	★★★★★ (5/5)
Windows Server 2025	MDE Portal Script	Yes	Beta version; completed in approximately 30 minutes; required latest cumulative updates.	★★★★☆ (4/5)
Windows Server 2022	MDE Portal Script + Manual AV Install	Yes	No pre-installed antivirus; required manual PowerShell installation; approximately 40 minutes.	★★★☆☆ (3/5)
Windows Server 2012 R2	MMA	Partial	Onboarding succeeded only after undocumented updates from Microsoft support; approximately 1.5 h	★★☆☆☆ (2/5)
Windows 7 SP1	MMA	Claimed (Failed)	Failed to onboard despite full patching and Microsoft support; certificate and connectivity issues.	★☆☆☆☆ (1/5)
Windows 8.1	MMA	Claimed (Failed)	Failed to onboard despite full patching and Microsoft support; similar connectivity errors.	★☆☆☆☆ (1/5)

WINDOWS 11 AND 10:

- **Process:** Onboarding was straightforward using the MDE portal script after applying all available patches, including the latest cumulative updates. Devices appeared in the Defender portal within 10 minutes, with full integration of endpoint detection and response (EDR) and Microsoft Defender Antivirus.
- **Challenges:** Minor connectivity issues were resolved by allow listing MDE service URLs (e.g., *.dm.microsoft.com) in firewall configurations.
- **CyberEase Rating:** ★★★★★ (5/5) – Exceptional ease of onboarding with minimal configuration and rapid portal visibility.

WINDOWS SERVER 2025:

- **Process:** Onboarding via the MDE portal script was efficient after applying the latest cumulative updates for the beta version. Devices were visible in the Defender portal within 15 minutes.
- **Challenges:** Minor delays due to beta status required firewall adjustments for MDE URLs.
- **CyberEase Rating:** ★★★★☆ (4/5) – Highly efficient, with slight delays due to beta-related updates.

WINDOWS SERVER 2022:

- **Process:** Lacked a pre-installed antivirus solution, requiring manual installation of Microsoft Defender Antivirus via PowerShell (Install-WindowsFeature -Name Windows-Defender). After installation and full patching (e.g., KB5044284), the MDE script executed successfully, with devices visible in the Defender portal within 15 minutes.
- **Challenges:** The additional antivirus installation step extended onboarding time to approximately 40 minutes.
- **CyberEase Rating:** ★★★☆☆ (3/5) – Functional but hindered by the need for manual antivirus installation.

WINDOWS SERVER 2012 R2:

- **Process:** Partially supported via MMA, requiring .NET Framework 4.5, KB5005292 (unified solution update), and TLS 1.2 configuration. Initial attempts following Microsoft's documentation failed. After a 7–8 day response from Microsoft support, undocumented update links were provided, enabling successful onboarding. Post-onboarding, MDE functioned as intended, though in passive mode, limiting some features.
- **Challenges:** The process took approximately 1.5 hours per device, with significant delays due to reliance on support for undocumented updates.
- **CyberEase Rating:** ★★☆☆☆ (2/5) – Onboarding achieved but required extensive effort and undocumented updates.

WINDOWS 7 ENTERPRISE SP1 AND 8.1:

- **Process:** Despite Microsoft's documentation claiming support via MMA, onboarding failed even after applying all recommended updates (e.g., KB3140245 for SHA-2, TLS 1.2 registry changes). Microsoft support was engaged but could not resolve persistent errors, including certificate issues and connectivity failures (e.g., "Failed to initialize security client"). Both systems remained non-functional with MDE.
- **Challenges:** Extensive troubleshooting, including registry modifications and firewall adjustments, was ineffective, highlighting outdated documentation and compatibility barriers.
- **CyberEase Rating:** ★☆☆☆☆ (1/5) – Complete failure to onboard, rendering MDE unusable.

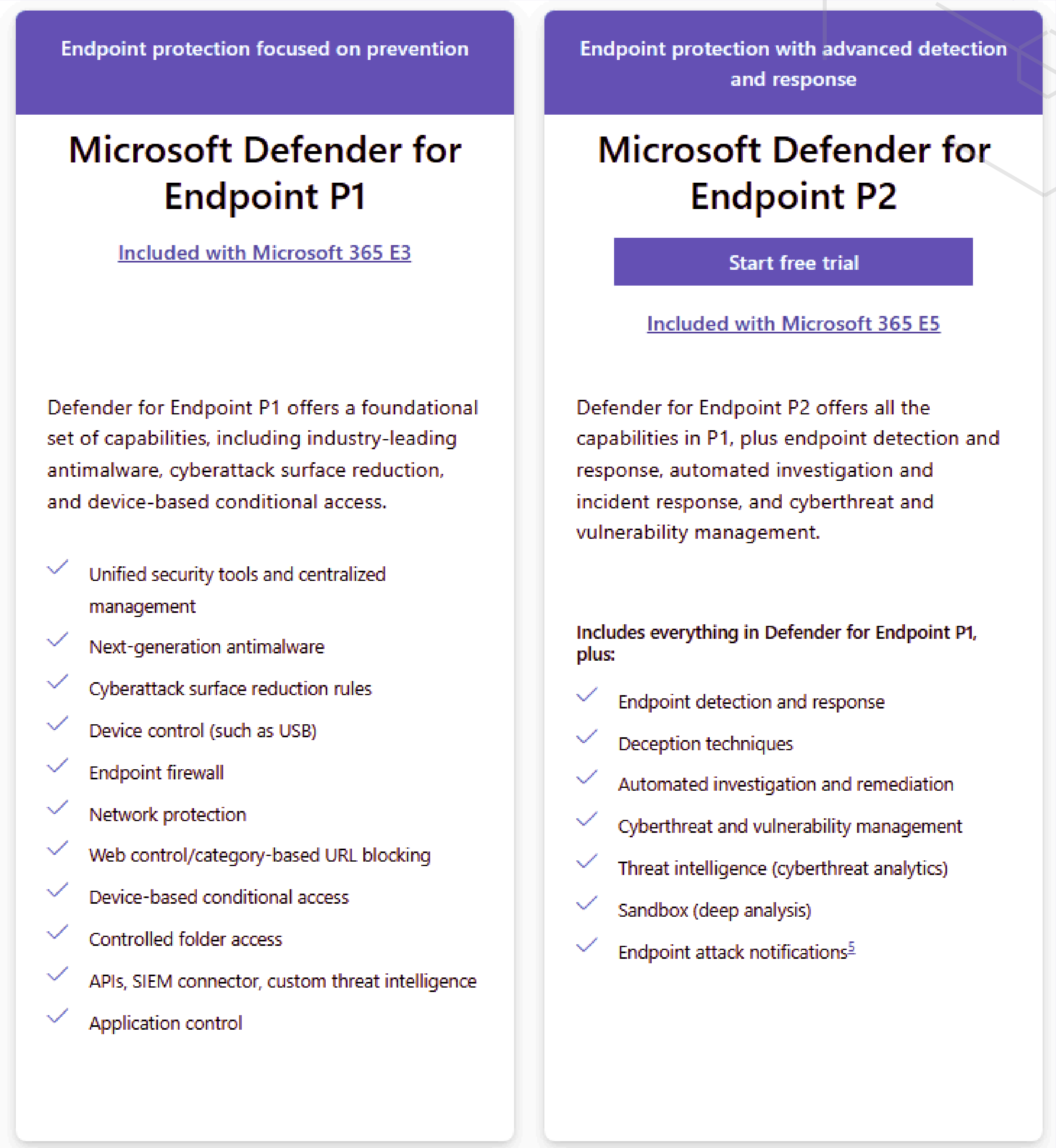
HOW DO WE CALCULATE CYBEREASE RATINGS?

Each star represents a distinct criterion for evaluating the onboarding experience of endpoint security solutions:

- **1 Star:** Failed Onboarding Despite Claimed Support – The operating system is documented as supported, but onboarding fails despite applying all recommended updates and configurations, even with support intervention.
- **2 Stars:** Onboarding with Significant Effort – Onboarding succeeds, and the device appears in the console, but requires extensive effort, multiple installation steps, debugging, and support interaction for undocumented updates or information.
- **3 Stars:** Onboarding with Additional Configuration for Detection – Onboarding is achieved by running a setup process, but further manual changes (e.g., installing antivirus software) are required to enable malware detection functionality.
- **4 Stars:** Onboarding with Minor Documented Updates – Onboarding is successful and the device appears in the console, but requires installation of a few minor, easily available, and well-documented updates or configurations.
- **5 Stars:** Seamless Out-of-the-Box Onboarding – Onboarding is effortless, completed out-of-the-box with no prerequisites or post-installation configurations, and the device appears instantly in the console with full functionality.

CONCLUSIONS

- FieldCISO Advisory Services' evaluation of Microsoft Defender for Endpoint (MDE) onboarding demonstrates significant variations in deployment success across Windows operating systems.
- Modern systems, including Windows 10, 11, and Server 2025, exhibited exceptional onboarding efficiency, earning CyberEase Ratings of 4–5 stars due to seamless integration with the MDE portal script and minimal configuration requirements when fully patched.
- Windows Server 2022, while fully supported, received a moderate CyberEase Rating of 3 stars due to the additional step of manually installing Microsoft Defender Antivirus via PowerShell, which extended onboarding time.
- Windows Server 2012 R2, despite partial support, necessitated extensive effort and undocumented updates obtained through Microsoft support after a 7–8 day delay, resulting in a low CyberEase Rating of 2 stars.
- Windows 7 SP1 and 8.1, claimed to be supported in Microsoft's documentation, could not be onboarded despite full patching and support intervention, earning the lowest CyberEase Rating of 1 star.
- Microsoft's documentation for legacy systems is outdated and fails to address real-world compatibility challenges, significantly hindering onboarding efforts.
- Overall, MDE onboarding is highly effective for modern systems but severely limited by legacy system constraints, resulting in an overall CyberEase Rating of 3 stars.
- Organizations must prioritize modern, fully patched systems to ensure successful MDE deployment and anticipate significant obstacles with legacy environments.



Endpoint protection focused on prevention

Microsoft Defender for Endpoint P1

Included with Microsoft 365 E3

Defender for Endpoint P1 offers a foundational set of capabilities, including industry-leading antimalware, cyberattack surface reduction, and device-based conditional access.

- ✓ Unified security tools and centralized management
- ✓ Next-generation antimalware
- ✓ Cyberattack surface reduction rules
- ✓ Device control (such as USB)
- ✓ Endpoint firewall
- ✓ Network protection
- ✓ Web control/category-based URL blocking
- ✓ Device-based conditional access
- ✓ Controlled folder access
- ✓ APIs, SIEM connector, custom threat intelligence
- ✓ Application control

Endpoint protection with advanced detection and response

Microsoft Defender for Endpoint P2

Start free trial

Included with Microsoft 365 E5

Defender for Endpoint P2 offers all the capabilities in P1, plus endpoint detection and response, automated investigation and incident response, and cyberthreat and vulnerability management.

Includes everything in Defender for Endpoint P1, plus:

- ✓ Endpoint detection and response
- ✓ Deception techniques
- ✓ Automated investigation and remediation
- ✓ Cyberthreat and vulnerability management
- ✓ Threat intelligence (cyberthreat analytics)
- ✓ Sandbox (deep analysis)
- ✓ Endpoint attack notifications[5]

Image Source

STRATEGIC FORSIGHT, HUMAN WISDOM

Contact Us:

for further information contact:
tanish@fieldciso.com or
visit us at **fieldciso.com**

PEER REVIEWED BY:

Prateek Bhajanka and Devesh Taneja

DESIGNED BY:

Tanaa Chauhan