FIELD SECURITY REPORT · APRIL 2026

SentinelOne vs MDE

Singularity Control vs Defender for Endpoint

Evaluated under Microsoft 365 E3 (Plan 1)

AUTHOR
Tanish Bhandari

PEER REVIEWED BY
Vatsal Sharma
Devesh Taneja

MDE LICENSE TESTED
Microsoft 365 E3 (Plan 1 / P1)

Table of Contents

01 Executive Summary

02 Purpose & Scope

03 Methodology

04 Market Position & External Validation

05 Detection & Remediation Efficacy

06 Onboarding Experience & OS Coverage

07 Performance & System Impact

08 Manageability & Operational Features

09 Total Cost, Risk & Integration

10 Conclusions & Recommendations

SECTION 01

EXECUTIVE SUMMARY

SentinelOne Singularity Control

Delivers stronger autonomous detection and remediation including full rollback, particularly on legacy OS families and mixed or hardware-constrained environments.

Microsoft Defender for Endpoint Plan 1 - E3 License

Included with Microsoft 365 E3/A3/G3, MDE P1 provides next-generation antivirus, attack surface reduction, centralized portal management, incident and alert visibility, reporting, and limited manual response actions. It does

not

include Automated Investigation & Remediation (AIR), Live Response, device timeline, advanced hunting, custom detections, or threat analytics. Those capabilities require MDE Plan 2 - available as a standalone add-on or part of Microsoft 365 E5.

Tradeoffs

MDE's ecosystem advantages (identity, Intune, Azure integration) are balanced against a larger resource footprint and more complex onboarding for legacy devices. SentinelOne provides autonomous endpoint protection, lower resource overhead, and simpler cross-OS coverage.

RECOMMENDATION

Adopt **SentinelOne** as the primary EDR/EPP for high-risk, heterogeneous, and legacy workloads where autonomous remediation, rollback, lower endpoint overhead, and simpler onboarding are priorities. Retain MDE P1 where Microsoft-native core protection is sufficient and risk is lower. If the organisation wants Microsoft investigation and response capabilities comparable to SentinelOne, MDE Plan 2 or Microsoft 365 E5 must be evaluated separately - including the licensing impact for servers.

TOP-LINE SUPPORTING EVIDENCE

SentinelOne's leadership in the Gartner 2025 Magic Quadrant is reinforced by Forrester's 2025 Total Economic Impact study, quantifying a 353% ROI and substantial operational savings through automation and reduced breach risk. Customers reported up to $3 million in savings from legacy tool consolidation and over 300 analyst hours saved monthly. The Forrester TEI study is vendor-commissioned and should be validated against internal pilot metrics.

353%	300+	$3M	6mo
Forrester ROI (S1 TEI)	Analyst hrs/mo saved	Legacy tool savings	Payback period

PURPOSE, SCOPE & METHODOLOGY

Purpose & Scope

Objective: Identify the EPP that best matches our operational risk profile across malware detection and remediation (including fileless and zero-day threats), performance and resource overhead, operational manageability, integration with existing Microsoft investments and SIEM/SOAR tools, and 3-year TCO and compliance considerations.

Scope: Internal lab tests using 50 malware samples on **Windows 11 Enterprise** (modern) and **Windows Server 2012 R2** (legacy), combined with vendor documentation and public benchmark references. MDE was evaluated exclusively under a **Microsoft 365 E3 license (Plan 1)**.

Methodology

DATASET & ENVIRONMENT

- **50 samples:** ransomware, file-based malware, credential stealers, and keyloggers (mid-to-high severity)
- **OSes:** Windows 11 Enterprise and Windows Server 2012 R2
- **Process:** Controlled sandbox and live endpoint validation; cross-check of vendor console activity logs and post-incident artifact collection

EVALUATION CRITERIA

- Detection rate and speed
- Remediation completeness including persistence cleanup
- RAM/CPU utilisation under idle and active threat conditions
- Onboarding duration and complexity across OS families
- Analyst effort required post-detection

Test Limitations: The 50-sample malware set provides a controlled internal comparison. Results should be treated as directional and validated through a wider pilot using real enterprise telemetry, false positive rates, alert volumes, analyst effort, containment time, and remediation completeness.

KEY DEFINITIONS

Term	Definition
Detected	Product generated an alert or prevention event
Quarantined	Malicious file blocked or moved to quarantine
Remediated	Product removed or reversed malicious activity including persistence mechanisms and associated artifacts

Term	Definition
Manual Cleanup Required	Analyst intervention needed to remove scheduled tasks, registry keys, services, or other persistence artifacts after the initial product response

MARKET POSITION & EXTERNAL VALIDATION

SENTINELONE SINGULARITY

- Leader in Gartner 2025 Magic Quadrant for Endpoint Protection Platforms
- Forrester 2025 TEI: 353% ROI, 6-month payback period
- Unified autonomous architecture across all major OS families
- Consistent protection in hybrid enterprise environments
- Faster mean-time-to-remediate confirmed in operational reviews

MICROSOFT DEFENDER FOR ENDPOINT

- Leader in Gartner 2025 Magic Quadrant for Endpoint Protection Platforms
- Processes ~84 trillion daily security signals
- Deep integration with Microsoft 365, Azure AD, and Intune ecosystem
- Full XDR capabilities at Plan 2 / E5 tier only
- E3/P1 is limited to prevention and basic manual response

External Benchmarks: Our findings are directionally consistent with public MITRE ATT&CK Enterprise Evaluation observations for 2024. MITRE results are referenced as external validation and not a direct substitute for internal pilot testing.

Both Vendors Hold Gartner Leader Status in 2025

Both SentinelOne and Microsoft are Leaders in the 2025 Gartner Magic Quadrant for Endpoint Protection Platforms, reflecting strong execution and product vision. The distinction in this evaluation lies not in market recognition but in **capability at the tested license tier** - MDE E3/P1 (prevention-focused) versus SentinelOne Singularity Control (full EDR with autonomous remediation).

Key Point: This report compares SentinelOne Singularity Control (full EDR) against MDE Plan 1 (E3) - not E5 vs SentinelOne. Both vendors hold Gartner Leader status, but the capability gap at the tested license tier is where the material differences lie.

SECTION 05

DETECTION & REMEDIATION EFFICACY

License Context: MDE results reflect the E3/Plan 1 license. MDE P1 performs AV quarantine and supports limited manual response (isolate device, stop process, quarantine file). It does **not** include AIR. All persistence cleanup in the MDE column was performed manually by SOC analysts.

OS / Scenario	Tested	SentinelOne: Detection / Remediation	MDE P1: Detection / AV Quarantine	Notes
Windows 11 Enterprise	50	**46 detected / 45 remediated**	**43 detected / 41 quarantined**	SentinelOne left 1 artifact for manual review. MDE P1 quarantined 41 via Windows Defender AV. No AIR available - SOC analysts manually cleaned scheduled tasks and registry entries. AIR is a Plan 2 only capability.
Windows Server 2012 R2	50	**43 detected / 40 remediated**	**36 detected / 28 quarantined**	SentinelOne missed 3 samples. MDE P1 failed to detect 14/50 - a significant gap. Without AIR or Live Response, all post-quarantine cleanup was manual. High risk exposure on legacy servers.

46/50
S1 Detections (Win 11)

43/50
MDE Detections (Win 11)

43/50
S1 Detections (2012 R2)

36/50
MDE Detections (2012 R2)

Observations

On Windows 11: Both platforms perform comparably on detection. The more significant difference is on remediation. SentinelOne autonomously investigates and rolls back threats. MDE was tested under E3/Plan 1, which supports manual response actions like file quarantine and device isolation but does not include AIR. Deeper cleanup around registry keys, scheduled tasks, and persistence artifacts fell to the SOC team rather than being handled by the platform.

On Windows Server 2012 R2: SentinelOne maintains strong coverage while MDE shows a notable drop - 14 out of 50 samples undetected. This aligns with the practical complexity of onboarding legacy OSes to the MDE pipeline. The MMA-based onboarding path for older platforms introduces capability limitations that directly impact detection quality.

OPERATIONAL IMPACT SUMMARY

92%
S1 Remediation (Win 11)

56%
MDE Quarantine (2012 R2)

0%
MDE P1 Auto-Remediation

ONBOARDING EXPERIENCE & OS COVERAGE

Microsoft MDE P1 - Onboarding Results

Operating System	Method	Support	Notes	Rating
Windows 11	MDE Portal Script	Yes	Seamless; ~20 min. Core endpoint protection, AV, ASR, alert/incident visibility, limited manual response. Full P2-level EDR not available under E3.	★★★★★
Windows 10	MDE Portal Script	Yes	Smooth; ~25 min; no issues post-patching.	★★★★★
Server 2025	MDE Portal Script	Yes	~30 min; required latest cumulative updates.	★★★★☆
Server 2022	Portal Script + Manual AV	Yes	No pre-installed AV; required manual PowerShell install; ~40 min.	★★★☆☆
Server 2012 R2	MMA / Modern Unified Solution	Partial	Succeeded only after undocumented updates from Microsoft support; ~1.5 hours. Server coverage may require separate Defender for Servers license.	★★☆☆☆
Windows 7 SP1	MMA	Claimed (Failed)	Failed to onboard in test environment despite full patching and Microsoft support assistance. Certificate and connectivity issues. Treat as high operational risk.	★☆☆☆☆
Windows 8.1	MMA	Claimed (Failed)	Failed to onboard in test environment. Similar connectivity errors. Treat as high operational risk.	★☆☆☆☆

SentinelOne Singularity - Onboarding Results

Operating System	Method	Support	Notes	Rating
Server 2025	Single Executable	Yes	Seamless; <5 min; full console integration.	★★★★★
Server 2022	Single Executable	Yes	Seamless; <5 min; full console integration.	★★★★★
Windows 11 Enterprise	Single Executable	Yes	Seamless; <3 min; fully automated.	★★★★★
Windows 10 Enterprise	Single Executable	Yes	Seamless; <3 min; fully automated.	★★★★★
Server 2012 R2	Single Executable	Yes	Required 4 manual Windows updates per installer guidance; <10 min with smooth integration.	★★★★☆

Operating System	Method	Support	Notes	Rating
Windows 7 Enterprise	Single Executable	Yes	Required 4 manual Windows updates; <10 min with smooth integration.	★★★★☆
Windows 8.1 Enterprise	Single Executable	Yes	Required 4 manual Windows updates; <10 min with smooth integration.	★★★★☆

SECTION 07

PERFORMANCE & SYSTEM IMPACT

Metric	SentinelOne (observed / vendor)	Microsoft MDE P1 (observed / vendor)
RAM Usage (Idle)	~100-150 MB (lightweight single agent)	~200-300 MB (MsMpEng and associated components)
CPU - Active Threat / Scan	Spikes ~15-20%	Spikes ~30-40%; higher impact under heavy scan workloads
Install / Update Behaviour	Single executable, centralized update control, agent rollback support from console	Updates via Intune/SCCM/Windows Update; older OSes rely on MMA with limited rollback automation

Implication: SentinelOne's lower resource footprint is favorable for older hardware and performance-sensitive server workloads. The roughly 2x RAM difference at idle is material on endpoints with constrained memory - particularly the Windows Server 2012 R2 systems in scope.

Agent Lifecycle Control

The July 2024 CrowdStrike Falcon outage highlighted the operational risk of uncontrolled content and agent updates. SentinelOne's policy-driven upgrade model addresses this directly.

SENTINELONE UPDATE CONTROLS

- **Smart Policies:** Latest agent for test, n-1 for production, n-2 as fallback
- **Fixed Version Pinning:** Lock critical systems to a specific agent version
- **Maintenance Windows:** Schedule updates for low-impact periods
- **Content updates** are separate from version upgrades and can be toggled or delayed
- All upgrades via console - no system restart required in most cases

MDE P1 UPDATE CONTROLS

- Agent lifecycle depends on Windows Update, Intune, or SCCM
- Legacy OS (2012 R2 and older) rely on MMA with limited automation
- Less granular version pinning compared to SentinelOne
- Rollback options more limited at the P1 tier

SECTION 08

MANAGEABILITY & OPERATIONAL FEATURES

Deployment & Lifecycle

SENTINELONE

- Single agent across all supported OS families
- Supports update rings and phased rollouts
- One-click rollback from console
- Strong cross-OS management APIs
- Simpler onboarding for legacy endpoints including Windows 7 and Server 2012 R2

MDE P1 (E3)

- Deeply integrated with Intune and SCCM for modern devices
- Agent lifecycle depends on Windows Update, Intune, or SCCM
- Older OSes require MMA onboarding - complex and can fail in practice
- E3/P1 portal is simplified: no device timeline, no Live Response

Threat Hunting & Analyst Tools

SENTINELONE - STORYLINE & PURPLE AI

Graphical attack narrative (Storyline) shortens investigation time and clarifies process and file lineage. Purple AI accelerates threat hunting, root cause analysis, and response - reducing both MTTD and MTTR significantly.

MDE P1 (E3) - WHAT IS AND IS NOT AVAILABLE

Under the E3/P1 license, the Defender portal provides incident and alert visibility, device management, reporting, and basic manual response actions. The following are **not available at this tier:**

- No full device timeline (deep EDR investigation view is Plan 2 only)
- No Live Response console
- No full advanced hunting across all data tables (30-day KQL hunting is Plan 2 only)
- No custom detection rules
- No Automated Investigation and Remediation (AIR)

SOC Impact: SOC teams on E3/P1 must account for this gap. A significant portion of investigation work that MDE P2 automates will fall back to manual analyst effort, increasing alert triage time and remediation cost.

MANAGEABILITY AT A GLANCE

Single	n-2	0
S1 Agent Across All OS	Version Fallback Available	MDE P1 AIR Capabilities

SECTION 09

TOTAL COST, RISK & INTEGRATION CONSIDERATIONS

Licensing

MDE P1 - E3 LICENSE

- Included at no additional cost with Microsoft 365 E3/A3/G3 for eligible user endpoints
- Zero incremental cost for MDE on user devices already on E3
- **Server coverage is NOT included under E3 user licensing** - Windows Server 2012 R2 and other servers may require Defender for Servers or Defender for Endpoint Server licensing
- Full Plan 2 capabilities require MDE P2 add-on or upgrade to M365 E5

SENTINELONE SINGULARITY CONTROL

- Separate commercial licensing required
- Forrester TEI (2025): 353% ROI - vendor-commissioned, validate against internal metrics
- Up to $3M in legacy tool consolidation savings reported by customers
- Single agent covers workstations and servers under unified licensing

Risk Tradeoffs

MDE P1 / E3 Only: Lower incremental cost for existing E3 customers, but detection gaps on legacy OSes, higher analyst workload for manual remediation (no AIR), and higher resource footprint increase operational risk.

SentinelOne: Higher licensing cost but measurable operational gains - faster autonomous detection and remediation, fewer analyst hours, lower performance impact, and stronger legacy OS coverage. The cost delta should be measured against analyst time saved and breach risk reduced.

Financial Recommendation

Build a 3-year TCO that includes licensing costs, SOC analyst hours per alert triage, endpoint performance impact (user productivity), and migration/deployment costs. Ensure server workloads are separately scoped - do not assume E3 user licensing covers server endpoints. Use vendor TEI/Forrester studies as a baseline, but validate all figures with local pilot metrics.

CONCLUSIONS & RECOMMENDATIONS

Conclusions

SentinelOne

Demonstrated stronger detection and autonomous remediation - particularly on Windows Server 2012 R2 - and simpler, more resilient agent management. This materially reduces SOC workload and risk from legacy endpoint populations. Full rollback capability and lower resource footprint are additional operational advantages.

MDE P1 (E3)

A solid choice for heavily Microsoft-centric environments where core endpoint protection on modern Windows is sufficient. The E3/P1 license does not provide the EDR investigation, automated remediation, or advanced hunting capabilities needed to match SentinelOne. Legacy onboarding complexity and higher resource footprint are operational tradeoffs that must be factored in.

Actionable Recommendations

- **Pilot SentinelOne** in a phased rollout starting with legacy servers and high-risk desktops. Track detection rate, remediation completeness, agent stability, SOC alert volumes, and endpoint performance.
- **Keep MDE P1** active on devices where core Microsoft-native protection is sufficient for the risk profile. The current E3 license does not provide AIR, Live Response, device timeline, advanced hunting, or custom detections. To get MDE functionality comparable to SentinelOne, the organisation needs MDE Plan 2 as a standalone add-on or an upgrade to Microsoft 365 E5 - weigh that upgrade cost directly against SentinelOne licensing.
- **Coexistence planning:** Define whether Microsoft Defender Antivirus runs in active, passive, or disabled mode when SentinelOne is deployed - along with exclusions, alert routing, and SIEM integration ownership.
- **Measure ROI during pilot** using Forrester/TEI metrics as a baseline but validate with local numbers: alerts triaged, MTTR, user complaints, CPU/RAM delta.
- **Document onboarding playbooks** for legacy systems (MMA path vs SentinelOne agent) and rollback steps if an agent update causes an incident.

BOTTOM LINE

Based on internal test results, SentinelOne is the stronger choice for legacy servers, high-risk workloads, and mixed-OS environments. MDE P1 on E3 is appropriate where basic Windows AV protection is sufficient. Organisations wanting full Microsoft XDR capabilities must evaluate MDE P2/E5 as a separate upgrade and weigh that against SentinelOne's commercial licensing on a 3-year TCO basis.

Strategic Foresight, Human Wisdom

For questions about this report or to commission a field evaluation for your environment, reach out to the FieldCISO Advisory team.

CONTACT

vatsal@fieldciso.com · fieldciso.com

AUTHOR

Tanish Bhandari

PEER REVIEWED BY

Vatsal Sharma · Devesh Taneja