Microsoft Defender vs. CrowdStrike: The "Free with Microsoft" Decision

Unvarnished Reviews Research

This report synthesizes data from 4,600+ verified user reviews and practitioner community posts collected from G2, TrustRadius (644 head-to-head reviews), PeerSpot, Spiceworks, Reddit practitioner communities including r/sysadmin and r/netsec, Microsoft Learn community forums, and Stack Overflow. Pricing data reflects vendor pricing pages, Microsoft licensing documentation, and enterprise procurement analysis current as of June 2026. Full research methodology at unvarnishedreviews.com/methodology. Research Notes available on request at editorial@unvarnishedreviews.com.

The Verdict Up Front

Microsoft Defender for Endpoint is a legitimately capable enterprise EDR platform that has improved substantially since 2022. For organizations on M365 E5, it is included at zero incremental cost, and for many organizations with moderate threat profiles, properly configured Defender P2 is sufficient. Independent real-world analysis puts Defender catching 90%-95% of threats, strong protection for the majority of enterprise environments. Its most honest documented limitation: analyst experience. Hands-on POC analysis from security practitioners describes Defender as carrying "hidden costs" of analyst frustration, unreliable alerts, and time spent navigating a scattered console, costs that don't appear on the license comparison sheet.

CrowdStrike Falcon is the market-leading dedicated EDR platform, positioned furthest right and highest on the 2026 Gartner Magic Quadrant for Endpoint Protection for the seventh consecutive year. Independent real-world analysis puts CrowdStrike catching 95%-98% of threats. Its cost advantage over Defender is not in licensing, it costs $60-$185/device/year on top of existing Microsoft investment. Its advantage is in analyst efficiency, detection consistency across non-Windows platforms, and the depth of OverWatch managed threat hunting.

A notable market signal: both platforms are losing PeerSpot mindshare in the EPP category as of June 2026, CrowdStrike from 10.8% to 6.0% and Defender from 10.7% to 6.8% year-over-year. SentinelOne and other challengers are gaining ground. The market is more competitive than either incumbent's marketing suggests.

Platform Ratings at a Glance

Platform	PeerSpot	TrustRadius (head-to-head)	G2 EPP
CrowdStrike Falcon	8.4 / 10	Preferred for detection depth	4.7 / 5
Microsoft Defender for Endpoint	8.2 / 10	Preferred for Microsoft-stack value	4.4 / 5

PeerSpot's 0.2-point gap reflects genuine detection and operational depth differences between dedicated EDR and integrated platform security. TrustRadius's 644 head-to-head reviews show a nuanced picture: CrowdStrike is preferred by organizations prioritizing detection sophistication; Defender is preferred by organizations prioritizing Microsoft stack integration and cost consolidation. Microsoft Defender for Endpoint is the #1 ranked solution in PeerSpot's Anti-Malware Tools category and #2 in endpoint security software, a strong position that reflects its scale of

deployment even if not its detection ceiling.

The Licensing Reality: "Free with Microsoft" Requires Precision

The most important section for any organization evaluating this comparison. The licensing structure specifically determines whether Defender is "free", and the answer depends entirely on which Microsoft plan the organization holds.

What changed in September-October 2025: Microsoft introduced new optional Defender Suite add-ons for Business Premium customers and removed Business Premium as a prerequisite for purchasing the Defender Suite. This created significant confusion in IT communities, practitioners on Microsoft Learn and Spiceworks documented difficulty understanding which products were included, which were add-ons, and which required separate licensing. The practical implication: if you believe your Microsoft licensing includes Defender EDR capabilities, verify the exact plan and tier before assuming coverage.

The licensing map (current as of June 2026):

License	Defender Included	EDR Capability
M365 Business Basic/Standard	No Defender for Endpoint	None
M365 Business Premium	Defender for Business (not Defender for Endpoint)	Limited, not equivalent to P2
M365 E3	Defender for Endpoint P1	No EDR, prevention only
M365 E5	Defender for Endpoint P2	Full EDR
E3 + E5 Security add-on	Defender for Endpoint P2	Full EDR
Standalone Defender P2	Defender for Endpoint P2	Full EDR, $5.20/user/month

The Business Premium distinction: Microsoft Defender for Business, included in Business Premium, is not the same product as Microsoft Defender for Endpoint P2. Defender for Business has a simplified configuration designed for organizations under 300 employees without dedicated security staff. It lacks advanced hunting, custom detection rules, and the threat analytics depth of Defender for Endpoint P2. Organizations on Business Premium that believe they have enterprise EDR coverage equivalent to Defender for Endpoint P2 do not.

The server licensing gap: Defender for Endpoint licensing covers user endpoints. Servers require separate Defender for Endpoint licensing or Defender for Servers (part of Microsoft Defender for Cloud). This is the most commonly missed cost in Defender deployments, and unmanaged servers consistently represent the largest security exposure in enterprise environments.

Technical Performance: What the Data Shows

Real-world detection benchmark: Independent hands-on POC analysis comparing both platforms against actual enterprise environments puts Defender for Endpoint catching approximately 90%-95% of threats and CrowdStrike catching approximately 95%-98%. This gap is meaningful for organizations facing advanced persistent threats and sophisticated attackers, less meaningful for organizations whose primary threat profile is commodity malware, phishing, and opportunistic ransomware.

The Defender AI-agent detection capability (2026): As of 2026, Microsoft Defender for Endpoint is the only EDR in the market with AI-agent-aware detection, specifically capable of detecting threats from compromised AI agents accessing enterprise systems. As agentic AI adoption accelerates across enterprise environments, this capability becomes increasingly relevant as a forward-looking differentiator that CrowdStrike has not yet matched.

MITRE ATT&CK; context: Microsoft achieved 100% detection coverage in the 2024 MITRE ATT&CK; Enterprise Evaluation. CrowdStrike did not participate in the 2024 evaluation. Neither vendor participated in the 2025 evaluation. The 2024 data is the most current independent benchmark available, and Microsoft's result, while strong, reflects controlled evaluation conditions, not the real-world 90%-95% detection rate that practitioners document in production environments.

The "free isn't free" reality from POC experience: Practitioners who have run head-to-head evaluations consistently document that Defender's hidden operational cost, analyst time spent on alert noise, console navigation complexity, and configuration maintenance, partially offsets the licensing cost advantage. One practitioner analysis states directly: "Microsoft E5 looks 'free' because you're already paying for it. But the hidden cost is analyst frustration, unreliable alerts, and the time spent navigating a scattered console. The cheapest tool isn't always the cheapest solution."

What Users Actually Report

Microsoft Defender: What Works

TrustRadius and PeerSpot reviewers consistently identify three areas of genuine strength: native Windows integration, Microsoft ecosystem convergence, and cost consolidation for E5 organizations.

The Defender XDR platform, correlating signals across endpoint, identity (Entra ID), email (Defender for Office 365), and cloud (Defender for Cloud Apps) in a single console, is specifically called out as a genuine architectural advantage for Microsoft-first organizations. PeerSpot reviewers at financial services firms specifically describe the rich telemetry data and in-depth threat identification as competitive with dedicated EDR platforms when properly configured.

The 2026 AI-agent-aware detection capability is a forward-looking differentiator that practitioners are beginning to flag as meaningful as agentic AI workloads increase enterprise attack surface.

Microsoft Defender: What Doesn't Work

Configuration complexity is the primary documented complaint. Practitioners consistently note that Defender requires meaningful technical expertise to configure at its full detection ceiling. The gap between Defender in default configuration and Defender properly tuned for EDR is substantial, organizations that deploy and assume it is running at full capability without dedicated configuration investment are not getting the protection the license implies.

Alert noise and false positive rate are specifically cited in Gartner's own customer research as areas where Defender's "initial deployment, configuration optimization and relatively slow pace of support issue resolution may degrade the overall customer experience." The signal-to-noise ratio in Defender XDR requires ongoing tuning that dedicated EDR platforms handle more automatically.

Cross-platform consistency. TrustRadius data shows Defender deployments are 100% Windows, but 39% also protect macOS and 35% protect Linux. Practitioner reviews consistently rate Defender's non-Windows coverage as less mature than its Windows-native capabilities. Organizations with significant macOS or Linux fleets encounter meaningful

coverage gaps.

The 2025-2026 licensing change confusion. The September-October 2025 Microsoft licensing restructuring, new add-ons, removal of Business Premium prerequisite, generated documented confusion in practitioner communities. Organizations should verify their current Defender capability tier before assuming their security posture has not been affected by these changes.

CrowdStrike: What Works

TrustRadius and PeerSpot enterprise reviewers consistently praise CrowdStrike for three things: detection consistency across operating systems, console clarity for SOC analysts, and the depth of OverWatch managed threat hunting. Practitioners describe the Falcon console as genuinely more intuitive for incident investigation than Defender XDR, a meaningful operational advantage for security teams that live in the console daily.

PeerSpot reviewers specifically call out CrowdStrike's behavior-based insights and AI integration as delivering "full visibility and streamlined threat detection", with the product consistently described as one that "just works" for security teams that need it to function without significant ongoing configuration investment.

CrowdStrike: What Doesn't Work

Licensing complexity and add-on accumulation remain the platform's most consistent complaint across TrustRadius and PeerSpot. Falcon Go and Pro do not include EDR, organizations that believe they have enterprise EDR at entry-level pricing do not. Each advanced capability is a separate subscription module that accumulates.

The July 2024 outage remains present in every practitioner evaluation, though its acute impact has faded. Most customers stayed with CrowdStrike. The architectural update architecture risk is now a standard evaluation criterion that was not present before the incident.

Support at standard tiers is a recurring complaint, practitioners report AI-driven responses and slow escalation to qualified engineers for complex issues. Premium support options resolve most issues but add cost.

Pricing Reality (June 2026)

Microsoft Defender for Endpoint

- M365 E5: ~$57/user/month (includes Defender P2, zero incremental cost for EDR)
- E5 Security add-on to E3: ~$12/user/month (adds Defender P2)
- Standalone Defender P2: $5.20/user/month
- Defender for Servers (server coverage): separate licensing under Defender for Cloud

CrowdStrike Falcon

Tier	Price	EDR
Falcon Go	$59.99/device/year ($5/device/month)	No
Falcon Pro	$99.99/device/year	No
Falcon Enterprise	$184.99/device/year	Yes
Falcon Complete MDR	$200-$400/device/year	Yes + managed response

The incremental cost calculation for E5 organizations: Adding CrowdStrike Falcon Enterprise on top of existing E5 costs $184.99/device/year ($15.42/device/month). For a 500-device organization, that's $92,495/year above existing M365 investment. The question is whether the incremental detection improvement, from the 90%-95% Defender range to the 95%-98% CrowdStrike range, justifies that investment given the organization's specific threat profile.

The MSSP factor: Practitioners consistently recommend that to get full value from either platform, organizations without a dedicated SOC should engage an MSSP for the response component. Both platforms have managed detection and response options, CrowdStrike Falcon Complete, Microsoft Defender Experts for XDR, that add cost but address the 24/7 analyst coverage gap that most mid-market organizations cannot staff internally.

The Decision Framework

Defender is likely sufficient if:

- Your organization is on M365 E5 (verified, not assumed) and has properly configured P2
- Your environment is predominantly Windows-centric
- Your threat profile is moderate, commodity malware, phishing, opportunistic ransomware
- You have IT staff to configure and tune Defender to its full capability before assuming coverage
- You are using Defender XDR to correlate across Entra ID, Defender for Office 365, and Defender for Cloud Apps, capturing the ecosystem convergence value
- You have verified server coverage under a separate Defender for Servers license

CrowdStrike is justified if:

- Your threat profile is elevated, financial services, healthcare, critical infrastructure, or organizations with prior targeted incidents
- You have a staffed SOC or MSSP relationship that will leverage CrowdStrike's detection depth and OverWatch
- Your environment includes significant non-Windows assets requiring uniform EDR coverage quality
- You have assessed the July 2024 outage architectural risk and have a documented remediation plan
- You have modeled the full incremental cost, not just comparing license to zero

The most common mistake:

Deploying Microsoft Defender P2 without configuring it properly, then comparing its default-state detection to CrowdStrike's tuned deployment. Defender at default configuration is not Defender at full capability. Before concluding CrowdStrike is necessary, conduct a genuine Defender P2 evaluation with dedicated configuration investment, including attack surface reduction rules, automated investigation settings, and threat hunting activation.

The Bottom Line

The "free with Microsoft" argument for Defender is real, but only for verified E5 organizations, and only when the platform is properly configured. The 2025-2026 Microsoft licensing changes have made the "what do I actually have" question more complex, not less. Every organization that assumes Defender coverage should verify the exact plan and tier.

CrowdStrike's detection depth, threat intelligence scale, and managed hunting capability remain genuinely superior to Defender in independent evaluations. The 90%-95% vs. 95%-98% detection rate gap is real. For organizations with elevated threat profiles and staffed security operations, the investment is defensible.

For most organizations on E5 with moderate threat profiles and properly configured Defender P2: the incremental cost of CrowdStrike is difficult to justify. For organizations with elevated threat profiles, significant non-Windows environments, or mature SOC functions, CrowdStrike delivers detection depth that Defender does not match.

The question is not which platform is technically superior. It is whether your organization's specific threat profile justifies the incremental cost, and whether your Defender deployment is actually configured to its capability ceiling before that question is answered.
