Endpoint Security (EDR/XDR) Valuations: Q2 2026

Q2 2026 finds the endpoint security market in a state Windsor Drake characterises as barbelled: a durable valuation premium for scaled, AI-native platforms at one end, and compressed pricing for legacy antivirus and pure-services managed detection at the other. Endpoint Protection Platforms are the single largest information-security category, at **$17.8B in 2026 and growing 14.5%** (Gartner), and the segment is set to add **$14.2B** in spend by 2030, the largest dollar increase of any security category. The demand is structural; the dispersion in how it is valued is the story of the quarter.

The spread is the widest in the cohort's history. Scaled AI-native extended detection and response (XDR) leaders trade near **18x to 20x NTM revenue**, AI-native endpoint detection and response (EDR) rounds clear **12x to 18x**, while pure-play managed detection and response (MDR) and legacy antivirus sit at **3x to 6x** as platforms absorb capability. Windsor Drake estimates the blended public endpoint multiple near **8.0x**, but that single number conceals two very different markets. Capital is concentrating at the top of the quality curve.

The macro backdrop is restrictive rather than supportive. The Federal Reserve funds range holds at **4.25% to 4.50%**, unchanged since December 2024, and the FOMC has now held for five consecutive meetings; the March 2026 dot plot signals only limited easing in 2026, with most participants projecting no or one cut (Federal Reserve). Elevated discount rates continue to weigh on long-duration software, yet durable endpoint demand has sustained premium multiples for the best assets. Against that backdrop the consolidation engine runs hot: CrowdStrike crossed **$5.51B ARR, up 24%**, by April 2026 (filings), and Sophos, backed by Thoma Bravo, acquired Secureworks for **$859M** to create the largest pure-play MDR provider.

This report sets out institutional-grade analysis for navigating that split market, one in which AI-native detection and telemetry scale are valued like premium infrastructure while signature-based antivirus and undifferentiated managed services face continued scrutiny.

What multiples are endpoint security companies trading at?

The Q2 2026 valuation picture turns on a single divide: AI-native architecture, telemetry scale and platform breadth on one side; signature-based detection, single-product tools and services-heavy economics on the other. Windsor Drake estimates the blended public endpoint multiple near **8.0x NTM revenue**, but the spread between the top and bottom of the table is the widest in a decade. Investors are paying up for AI-native detection, security-data-lake economics and durable platform attach.

Scaled XDR, AI-native EDR and identity-aware endpoint platforms are valued on architecture and platform breadth. Legacy antivirus, pure-play managed services and single-product tools, by contrast, remain under scrutiny as platform incumbents absorb capability and Microsoft Defender's bundling compresses mid-market pricing. The gap between cohorts is wider than at any point in the past decade.

Table 1. Endpoint Security Valuation Multiples by Segment

Segment	EV/Revenue Range	YoY Trend	Primary Driver
Scaled AI-Native XDR	15.0x - 22.0x	Strengthening	Telemetry scale, Rule of 40, AI-native detection
AI-Native EDR (Next-Gen)	12.0x - 18.0x	Rising	Behavioural detection, legacy AV displacement
Identity-Aware Endpoint	10.0x - 15.0x	Rising	Zero-trust adoption, modern work surface
Device & Asset Telemetry	9.0x - 14.0x	Rising	Exposure management, data-lake adjacency
Mid-Market XDR / EDR	8.0x - 12.0x	Stable	SOC consolidation, attach economics
Next-Gen EPP	6.0x - 10.0x	Stable	Largest category by spend, commoditising base
MDR (Software-Attached)	5.0x - 8.0x rev	Stable	Software attach, delivery margin
Pure-Play MDR / MSSP	3.0x - 5.0x rev	Compressing	Services discount vs software
Legacy AV / Signature	3.0x - 5.0x	Compressing	Platform absorption, commoditisation

Source: Windsor Drake analysis of Gartner, CB Insights and public company filings.

Segment dynamics driving the dispersion

Scaled XDR has re-rated upward as platform incumbents compete to consolidate the security operations centre. CrowdStrike, reporting **$5.51B ARR (+24%)** and record Q1 net new ARR of **$256M (+32%)** for the quarter ended April 2026 (filings), trades near 18x to 20x NTM revenue on its expanding security-data-lake thesis. SentinelOne sits at the other end of the public cohort, near 3.5x to 4x revenue, despite **$1.16B ARR (+23%)**, illustrating that scale and Rule of 40 performance, not category membership, separate the winners. Legacy antivirus and pure-play managed-services multiples move the other way, compressing as capability is absorbed into broader platforms and as services-heavy revenue is valued against a software premium it cannot match.

Table 2. Segment Valuation Drivers and Principal Risks, Q2 2026

Segment	Premium Driver	Principal Risk
Scaled AI-Native XDR	Telemetry scale, platform attach	AI margin pressure on Rule of 40
AI-Native EDR	Behavioural detection, AV displacement	Absorption into XDR platforms
Identity-Aware Endpoint	Zero-trust adoption, modern work surface	Identity-vendor commoditisation
Device & Asset Telemetry	Exposure management, data-lake adjacency	Feature absorption by incumbents
MDR (Managed)	Software attach, scale consolidation	Services discount vs software peers
Next-Gen EPP	Largest category by spend	Microsoft Defender bundling pressure
Legacy AV / Signature	Installed-base cash flow	Commoditisation, platform displacement

Source: Windsor Drake analysis of Gartner and S&P Global Market Intelligence research.

How are endpoint security companies valued in 2026?

Valuation in 2026 has coalesced around a disciplined framework built on AI-native architecture, recurring revenue quality and a credible route to platform breadth. The growth-at-all-costs playbook is gone. In its place is a multi-factor model in which the Rule of 40 is table stakes, AI-native detection is now a measurable premium driver, and platform attach economics decide where in the multiple range an asset prints.

The Rule of 40 mandate

The Rule of 40, where revenue growth plus EBITDA margin reaches at least 40%, is the primary filter for a premium multiple. Bain finds that public software clearing the rule posts a median **10.7x EV/Revenue** versus far less below the line; endpoint leaders such as CrowdStrike clear that bar materially, trading near **18x to 20x NTM revenue**. Each ten-point gain in the score is now worth roughly an additional turn of revenue in the public endpoint cohort.

AI infrastructure cost is, however, pressuring the rule across the cohort. Bain has noted that some software companies and their investors may need to settle for smaller margins as they reinvest to stay competitive with AI-native rivals, and now discusses a 'Rule of 30' alternative for AI-native players. The implication for endpoint founders is to track the score monthly with board-level visibility, and to demonstrate that autonomous-SOC investment is a path to operating leverage rather than a permanent margin drag.

Table 3. Rule of 40 Performance Tiers, Endpoint Security, Q2 2026

Performance Tier	Rule of 40 Score	Avg EV/Revenue	Premium vs Benchmark
Top Quartile (Scaled Leaders)	Above 50	12x to 22x and above	+50% to +100%
Rule of 40 Met	40 to 50	8x to 12x	Healthy premium
Near Miss	30 to 39	5x to 7x	Modest discount
Bottom Quartile	Below 30	3x to 5x	Deep discount

Source: Windsor Drake analysis of McKinsey and Bain & Company software value-creation research.

Unit economics under scrutiny

An LTV/CAC ratio above 3:1 is now the minimum, and the strongest endpoint companies target 5:1 or better. Payback expectations have tightened, with investors looking for customer-acquisition cost recovered inside twelve months for SaaS-delivered endpoint assets. For platform-attach motions, **net revenue retention above 115% to 120%** has become essential, evidence not merely of satisfied customers but of a working multi-module expansion engine across identity, exposure and SIEM. CrowdStrike's **97% gross retention** (filings) sets the benchmark; sub-scale point tools rarely match it.

A credible path to profitability

For any endpoint asset valued above ten times revenue, the market now expects a believable path to durable cash generation. CrowdStrike's record free cash flow of **$468M** in the quarter ended April 2026, alongside 24% ARR growth, is the template the market rewards: high growth combined with demonstrable cash discipline. There is little tolerance for perpetual growth narratives that never demonstrate operating leverage, especially in an environment where AI infrastructure cost is pressuring the margin profile of the entire cohort.

What is driving endpoint security valuations this quarter?

Valuations in Q2 2026 reflect an interplay of expansionary forces and compressive market realities. Reading those drivers correctly is what separates a defensible endpoint valuation from a mispriced one. The headline arithmetic is a roughly **+1.0x** net expansion from a 2024 baseline of about 7.0x to the Q2 2026 blended benchmark of 8.0x: AI-native detection, platform consolidation and zero-trust mandates outweigh a combined 0.9x drag from AI infrastructure cost, legacy antivirus commoditisation and a higher-for-longer rate path.

Table 4. Valuation Drivers, Expansion versus Compression, Q2 2026

Factor	Driver	Effect on Multiples	Notable Examples
Expansion	AI-native detection	Premium for autonomous-SOC architecture	CrowdStrike Charlotte AI, SentinelOne Purple AI
Expansion	Platform consolidation	Re-rating for SOC-complete platforms	Falcon roll-ups, Sophos / Secureworks
Expansion	Zero-trust mandates	Compliance demand widens buying centre	NIS2, DORA, federal zero-trust
Compression	AI infrastructure cost	Margin drag pressures Rule of 40	Sub-scale public endpoint names
Compression	Legacy AV commoditisation	Platform absorption compresses pricing	Signature antivirus, single-product EDR
Compression	Higher-for-longer rates	Elevated discount rates weigh on growth	Long-duration private endpoint assets

Source: Windsor Drake analysis of Gartner, Bain & Company and Federal Reserve data.

Geographic variation

Location still matters for endpoint valuation. North America commands a clear innovation and exit-liquidity premium, home to CrowdStrike, Microsoft, Tanium and Arctic Wolf and the deepest public-market liquidity in cyber. Israel remains a dense endpoint-innovation hub on technical talent (SentinelOne's heritage, Cybereason), and Israeli-built detection IP routinely captures premium exit pricing through US strategic acquisitions. Europe (Sophos, Bitdefender, ESET) trades at a fragmentation discount but offers regulatory moats from NIS2 and DORA that US acquirers are increasingly arbitraging. APAC continues to expand on growing enterprise budgets and government-driven mandates.

Table 5. Geographic Valuation Variation, Cybersecurity, Q2 2026

Region	Market Share	Posture	Key Drivers
North America	~44%	Premium	Scaled endpoint platforms, deep public-market liquidity
Europe	~24%	Value	NIS2 and DORA moats; fragmented endpoint vendor base
APAC	~22%	Growth	Enterprise budgets, government mandates
Israel & RoW	~10%	Innovation	Endpoint talent density, US strategic exits

Source: Windsor Drake analysis of Gartner and S&P Global Market Intelligence data.

Public and private markets converge

One of the defining features of the quarter is the selective convergence of public and private endpoint multiples. The historical private premium has compressed from roughly 7x in 2023 to about 1x in 2026, and public comparables now act as a gravity anchor on late-stage private rounds for most assets. Differentiated AI-native EDR and autonomous-SOC companies still raise at genuine premiums of **12x to 18x revenue**, but generic late-stage private endpoint companies without a clear AI-native architecture are seeing flat marks. Those companies are increasingly prime candidates for strategic M&A or a PE take-private outcome, a dynamic reinforced by roughly **$3.7T** of global private equity dry powder (McKinsey; Bain) and the **$18B** of cyber venture funding deployed in 2025 (CB Insights; Crunchbase).

Which valuation metric should apply?

Selecting the right metric is what separates a professional endpoint valuation from a careless one. Different corners of the endpoint market demand different lenses, and leaning too hard on a generic EV/Revenue multiple can badly misprice mature managed-services businesses or capability-heavy bolt-on assets.

EV/Revenue: the growth metric

EV/Revenue suits high-growth endpoint assets with recurring revenue that are reinvesting ahead of profitability, including scaled XDR, AI-native EDR and identity-aware endpoint platforms. The essential adjustment is for gross margin: a dollar of software revenue at an 80%-plus margin is not comparable to a dollar of managed-detection revenue earned on a delivery-margin model.

EV/EBITDA: the profitability metric

EV/EBITDA fits mature, slower-growth endpoint businesses where cash flow is the primary value driver, such as scaled MDR operators and PE-owned managed-endpoint platforms. Many companies once valued on revenue are now assessed on EBITDA as their growth rates moderate; for managed-detection platforms, **EBITDA multiples of 12x to 18x** are the relevant range.

ARR, NRR and strategic premium

For SaaS-delivered endpoint assets, an ARR and NRR lens overlays the EV/Revenue methodology: premium for NRR above 120% and gross retention above 90%, discount for concentration risk and short contract duration. Strategic premiums in endpoint processes, typically **25% to 30%**, are applied on top of underlying revenue or EBITDA multiples where platform and capability synergies can be concretely underwritten; the Sophos / Secureworks transaction, and CrowdStrike's capability roll-ups, illustrate where those premiums accrue.

Table 6. Valuation Methodology Matrix, Endpoint Security, Q2 2026

Segment	Primary Metric	Typical 2026 Range	Key Adjustment
Scaled AI-Native XDR	EV/Revenue	15x to 22x	Telemetry scale, Rule of 40
AI-Native EDR (Next-Gen)	EV/Revenue	12x to 18x	AI-native posture, AV displacement
Identity-Aware Endpoint	EV/Revenue	10x to 15x	Zero-trust attach, NRR
Device & Asset Telemetry	EV/Revenue	9x to 14x	Exposure-management adjacency
Next-Gen EPP	EV/Revenue	6x to 10x	Growth quality, bundling exposure
MDR (Software-Attached)	EV/EBITDA	12x to 18x EBITDA	Software attach, scale
Legacy AV / Signature	EV/EBITDA	8x to 12x EBITDA	Cash flow, installed base

Source: Windsor Drake valuation methodology, calibrated to public company filings and CB Insights comparables.

These ranges are calibrated against Windsor Drake's proprietary transaction index of **255 verified and reported transactions (2020 to 2026)**, refreshed each quarter and supplemented by current-quarter endpoint research. Peer sets are filtered on architecture, buyer and revenue quality rather than broad endpoint labels, and private-market indications are adjusted for earn-outs and lack-of-marketability discounts, typically in the 20% to 30% range.

Key takeaways for founders

Translating the market picture into strategy means concentrating on six areas that consistently move endpoint security valuation in the current environment.

1. Clear the Rule of 40

Revenue growth plus EBITDA margin must reach at least 40%. No single metric predicts a valuation premium better, and top-quartile performers earn **50% to 100%** over the benchmark. Make the score a board-level priority with monthly tracking, and demonstrate that autonomous-SOC investment is a path to durable operating leverage rather than a permanent margin drag.

2. Build for platform attach, not point sale

Target net revenue retention above **115% to 120%** through multi-module attach across identity, exposure and SIEM. Document the specific motion that drives that retention, and codify how the asset slots into a CISO's SOC consolidation roadmap. Scaled platform leaders clear **15x to 22x NTM revenue**; single-product tools sit far lower, and the gap is widening as platforms absorb capability through M&A.

3. Make the AI-native case concrete

AI is now a measurable driver of endpoint value, not a talking point. Present specific use cases across detection, triage, response and identity, and quantify the SOC analyst productivity gains and cost-to-defend reduction with hard return-on-investment numbers. Differentiated AI-native EDR commands **12x to 18x** revenue when the autonomous-SOC case is real.

4. Invest in certifications and compliance

FedRAMP High, IL5, ISO 27001 and SOC 2 Type II are hard, expensive and slow to obtain, and that is precisely why they function as moats. Invest early in the certifications that gate the most defensible verticals, particularly federal, critical-infrastructure and financial services. Present audited evidence in the data room before the first buyer engagement.

5. Map specific strategic buyers

With strategics driving the majority of endpoint M&A by value and roughly **$3.7T** of PE dry powder in the system (McKinsey; Bain), the prepared asset captures the competitive tension. Run a structured gap analysis of potential acquirers, from platform incumbents to MDR roll-up sponsors, and map your capabilities directly to each buyer's declared strategic deficits before engaging the market.

6. Prepare for the current cycle

Listing thresholds now demand scale, growth, AI-native architecture and a clear path to profitability, the public window for endpoint is narrow, and private valuations are converging on public-market standards. A full process runs **12 to 18 months** end to end, so a founder who intends to engage the market while today's alignment of strategic-buyer demand, AI-native premia and barbelled pricing still holds is, in practice, preparing in the current cycle.

Sources

- Gartner, Forecast: Information Security, Worldwide and Forecast Analysis 2026
- Gartner, Magic Quadrant for Endpoint Protection Platforms 2026
- McKinsey & Company, Global Private Markets Report 2026
- Bain & Company, Hacking Software's Rule of 40 and AI Brings Headwinds and Tailwinds
- Bain & Company, Global Private Equity Report 2026
- PwC, Global M&A Industry Trends: 2026 Outlook (TMT)
- EY, M&A Activity Insights
- S&P Global Market Intelligence, Global M&A by the Numbers: Q1 2026
- CB Insights, State of Cybersecurity Venture Funding
- PitchBook, Arctic Wolf company profile and dry powder dashboard

- CrowdStrike Holdings, Q1 FY2027 and FY2026 financial results
- SentinelOne, Q1 FY2027 financial results
- Sophos and Thoma Bravo, Sophos completes Secureworks acquisition
- Microsoft, Leader in the 2026 Gartner Magic Quadrant for Endpoint Protection
- Federal Reserve, FOMC statement and Summary of Economic Projections (Mar 2026)
- World Economic Forum, Global Cybersecurity Outlook 2026