WINDSOR DRAKE

Endpoint Security (EDR/XDR) Valuations: Q2 2026

JUNE 2026

Windsor Drake · Market Intelligence

Executive Summary: The Barbelled Endpoint

WINDSOR DRAKE

Endpoint's Software Premium

Endpoint Protection Platforms are the single largest information-security category at **$17.8B in 2026, growing 14.5%** (Gartner), yet pricing is barbelled.

- Endpoint will add **$14.2B** in spend by 2030, the largest dollar increase of any security category (Gartner).
- The market pays for AI-native detection and platform breadth, not signature-based antivirus.
- Scaled AI-native XDR leaders clear **15x to 22x** revenue while legacy AV sits at **3x to 5x**.
- Quarter-to-quarter multiple volatility has compressed versus the 2022 to 2024 cycle.

The Platform Divergence

Headline averages mask a barbell between scaled AI-native platforms and single-product tools.

- Scaled AI-native XDR (CrowdStrike-class) trades near **18x to 20x NTM revenue** (Windsor Drake analysis).
- Sub-scale and single-product EDR sit at **8x to 12x** as platforms absorb capability.
- Pure-play MDR and legacy AV clear **3x to 6x** revenue.
- Capital concentrates at the top of the quality curve as platform consolidation accelerates.

Demand Fundamentals

Endpoint demand is a board-level mandate, reinforced by zero-trust and disclosure regulation.

- Global information-security end-user spend reaches **$244.2B in 2026, up 13.3%** (Gartner).
- Endpoint Protection grows **14.5%** in 2026, leading all security categories in dollar terms (Gartner).
- Zero-trust mandates and NIS2 reporting turn endpoint telemetry into a compliance obligation.
- CrowdStrike crossed **$5.51B ARR (+24%)** by April 2026, advancing toward $10B ending ARR (filings).

Macroeconomic Backdrop

Monetary policy is restrictive, and durable endpoint demand has absorbed the headwind.

- Fed funds range holds at **4.25% to 4.50%**, unchanged since December 2024 (Federal Reserve).
- The FOMC has held for five consecutive meetings; the March 2026 dot plot signals limited 2026 easing (Federal Reserve).
- Elevated discount rates pressure long-duration software, yet premium endpoint multiples have held.
- The next Summary of Economic Projections lands at the June 2026 FOMC (Federal Reserve).

Sources: Gartner; Federal Reserve; company filings; Windsor Drake analysis. See appendix.

Executive Summary: Capital and Consolidation

WINDSOR DRAKE

Platform Consolidation

Scale and platform breadth define the endpoint cycle and set the Q2 2026 backdrop.

- CrowdStrike posted record Q1 net new ARR of **$256M (+32% YoY)** for the quarter ended April 2026 (filings).
- Endpoint incumbents are buying capability in browser, identity, SaaS posture and data telemetry.
- Microsoft Defender's bundling pressures standalone endpoint pricing across the mid-market.
- The broad cyber megadeal backdrop (Google / Wiz $32B; PANW / CyberArk $25B) frames buyer ambition.

AI Premium

AI-native detection has become the primary, measurable driver of endpoint value.

- Autonomous, LLM-assisted SOC tooling decouples detection from analyst headcount.
- CrowdStrike's roll-ups (**SGNL, Seraphic, Pangea, Onum**) extend Falcon into adjacent AI-native layers.
- **SentinelOne's** emerging solutions reached roughly **half of total ARR** by April 2026 (filings).
- Buyers pay for measurable analyst-productivity gains, not pilots.

Strategic Buyers and PE

Both strategic platforms and financial sponsors are deploying capital into endpoint.

- Strategic platforms drive the majority of endpoint M&A by value (Windsor Drake analysis).
- Global PE dry powder of roughly **$3.7T** sustains pressure on cash-generative MDR and EPP assets (McKinsey; Bain).
- **Sophos** (Thoma Bravo) acquired **Secureworks** for **$859M**, creating the largest pure-play MDR (company releases).
- PE treats MDR and managed endpoint as buy-and-build roll-up categories.

Public Markets and Private Capital

The listing window is narrow; the leading private MDR assets remain well funded.

- CrowdStrike and SentinelOne anchor public endpoint comps at opposite ends of the scale curve.
- **Arctic Wolf**, valued near **$4.4B**, remains a leading MDR IPO candidate awaiting the rate window (PitchBook).
- Cyber venture funding reached about **$18B in 2025**, the highest in three years (CB Insights; Crunchbase).
- Endpoint and network saw weaker standalone venture interest as capital shifted to platforms (CB Insights).

Sources: Gartner; CB Insights; Federal Reserve; company and SEC filings. See appendix.

Key Founder Takeaways: Q2 2026

WINDSOR DRAKE

1. Rule of 40 Achievement

Revenue Growth % plus EBITDA Margin % at or above 40% is the non-negotiable baseline for a premium endpoint multiple, and the market prices it harder each quarter (Bain; McKinsey).

- Public software clearing the rule posts a median **10.7x EV/Revenue** (Bain).
- AI infrastructure cost is pressuring the rule; track the score monthly at board level.

2. Platform Coherence

Single-product EDR is being absorbed; platforms that span endpoint, identity, cloud and data are the winners.

- Scaled XDR leaders clear **15x to 22x NTM revenue**; single-product tools sit far lower.
- Codify how the asset slots into a CISO's SOC consolidation roadmap.

3. Net Revenue Retention

Land-and-expand economics are scrutinised more heavily than topline growth; durable retention beats raw acquisition.

- Top endpoint platforms sustain **NRR above 115%**; CrowdStrike holds **97% gross retention** (filings).
- Document the multi-module attach motion (identity, exposure, SIEM) that drives retention.

4. AI-Native Detection

AI is no longer optional; the autonomous SOC is now a primary driver of deal size, buyer interest and multiple expansion.

- AI-native detection that decouples response from analyst headcount commands the cohort's top multiples.
- Show measurable SOC analyst productivity gains, not pilots.

5. Public Market Discipline

Public endpoint comps are barbelled and private marks reference them, so pricing discipline is required even for private rounds.

- CrowdStrike trades near **18x to 20x** revenue versus SentinelOne near **3.5x to 4x** (WD analysis).
- Justify any premium with scale, Rule of 40 and AI-native posture, not category labels.

6. Buyer-Readiness Discipline

With roughly **$3.7T** of dry powder and strategics driving the majority of endpoint M&A by value, the prepared asset captures competitive tension.

- Clean financials, audited SOC 2 and FedRAMP posture, defensible data room.
- Map specific capability gaps for each of your top five strategic acquirers.

Source: Windsor Drake advisory methodology. See appendix.

Founder FAQs: Valuations, Timing & Strategy

WINDSOR DRAKE

The questions endpoint security founders ask most, answered against the Q2 2026 market.

Q1 Which valuation metric applies to my business?

Use **EV/Revenue** for high-growth, AI-native XDR, EDR and identity-aware endpoint platforms; **EV/EBITDA** for mature, cash-generative MDR and managed-endpoint operators; and a recurring-revenue lens (NRR, GRR, ARR growth) for any SaaS-delivered endpoint asset. Always reference the correct endpoint cohort, never a broad cyber average.

Q2 What are the key endpoint segment ranges right now?

Scaled AI-native XDR platforms lead at **15x to 22x NTM revenue**; AI-native EDR at **12x to 18x**; identity-aware endpoint at **10x to 15x**; device and asset telemetry at **9x to 14x**; mid-market XDR/EDR at **8x to 12x**; next-gen EPP at **6x to 10x**; software-attached MDR at **5x to 8x revenue** or **12x to 18x EBITDA**; legacy AV at **3x to 5x**.

Q3 Why is the Rule of 40 so critical?

It is the single best predictor of a premium multiple in software. Public software clearing the rule earns a median **10.7x EV/Revenue** versus far less below the line (Bain). For endpoint specifically, a scaled clearer like CrowdStrike trades near **18x to 20x NTM revenue** on durable rule-of-40 performance, while sub-scale tools that miss it sit in the low single digits.

Q4 How do public and private valuations compare?

The public endpoint cohort is barbelled, with CrowdStrike near **18x to 20x** and SentinelOne near **3.5x to 4x** (WD analysis). The historical private premium has compressed toward **1x to 2x**, and public comparables now anchor late-stage private rounds for all but the most differentiated AI-native assets.

Q5 When is the optimal time to run a process?

After demonstrating **4 to 6 quarters** of predictable performance, while still holding 12 to 18 months of runway. Negotiating from a position of strength, rather than necessity, is what captures the scarcity premium in a strategic-buyer-dominated endpoint market.

Q6 Who are the most active buyers today?

Platform incumbents (CrowdStrike, Palo Alto Networks, Microsoft, SentinelOne) drive capability M&A in browser, identity, SaaS posture and telemetry. **PE platforms** with roughly $3.7T of dry powder execute MDR and managed-endpoint roll-ups; Thoma Bravo's Sophos / Secureworks deal is the template. Hyperscalers mostly partner rather than buy endpoint.

Q7 Is an IPO a viable alternative to M&A?

For endpoint it is narrow. The scaled pure-plays (CrowdStrike, SentinelOne) are already public, so the listing question centres on private MDR leaders. **Arctic Wolf**, valued near $4.4B, is the most-watched candidate but has signalled it is waiting for a friendlier rate and tech-multiple window (PitchBook). The window favours scaled, profitable assets with a credible AI-native narrative.

Q8 How do we maximise our multiple, and should we expect earn-outs?

Clear the **Rule of 40**, sustain **NRR above 115%**, hold premier certifications (SOC 2, FedRAMP High, ISO 27001) and codify autonomous-SOC value. Expect **earn-outs** to bridge AI-capability or scale gaps; structures typically pay over 12 to 24 months on revenue and integration milestones.

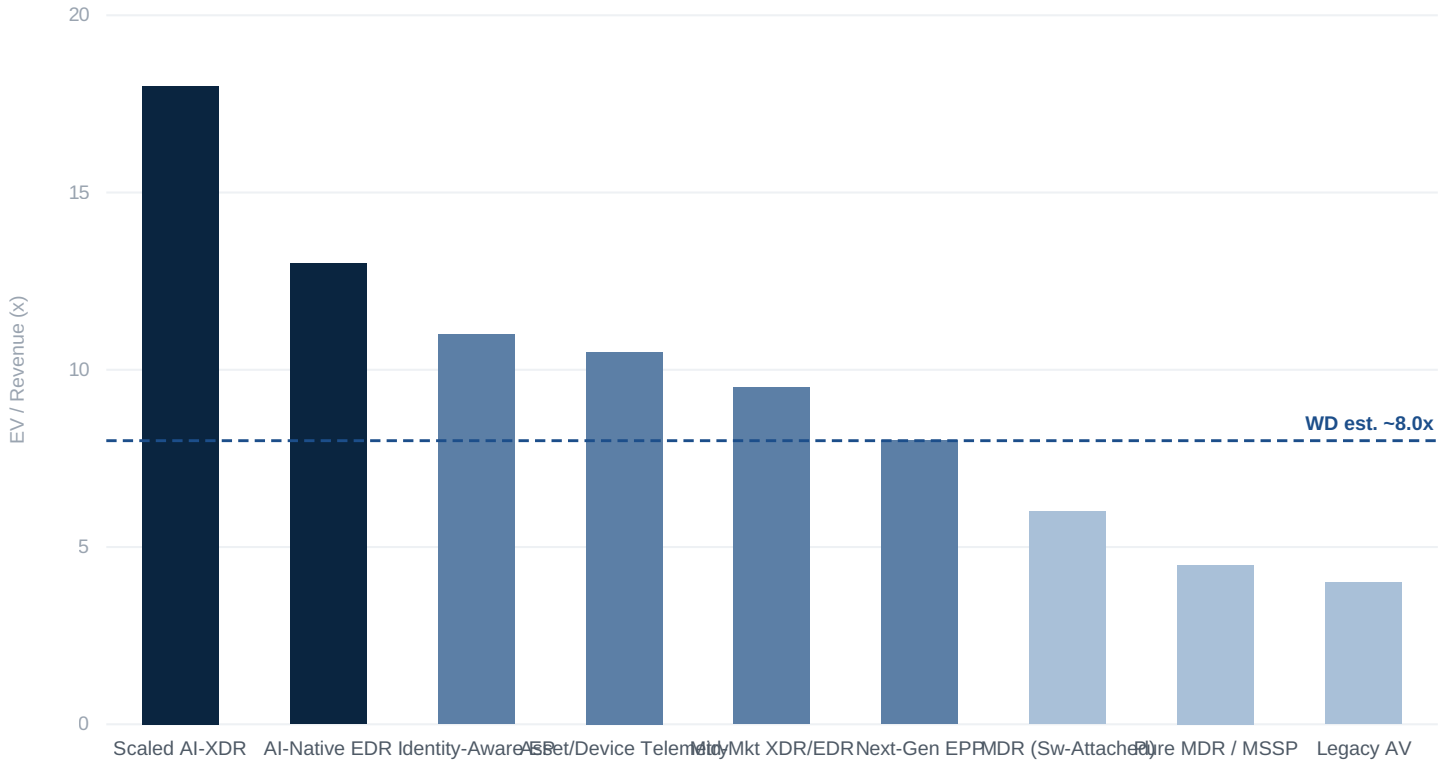
Source: Windsor Drake advisory methodology. See appendix.

Q2 2026 Valuation Landscape Overview

WINDSOR DRAKE

Premium multiples cluster in scaled AI-native XDR; legacy AV and pure-play MDR stay compressed.

Median EV / Revenue Multiple by Endpoint Segment (x)



Barbell, not bell curve: the gap between scaled AI-native XDR (15x to 22x) and legacy AV and pure-play MDR (3x to 6x) is the defining feature of the endpoint market, driven by AI-native architecture, telemetry scale and platform attach.

SEGMENT MEDIAN BENCHMARK

~8.0x

Windsor Drake house estimate of the blended public endpoint multiple, synthesising the cited comps.

SCALED XDR PREMIUM

18x to 20x

CrowdStrike-class AI-native XDR leaders command the cohort's highest revenue multiples (WD analysis).

ENDPOINT SPEND GROWTH, 2026

+14.5%

Gartner forecast growth for Endpoint Protection Platforms, the largest security category in dollar terms.

Key Driver

Disciplined pricing has replaced 2021 enthusiasm: acquirers reward AI-native detection, telemetry scale and platform breadth, not topline growth or category labels alone.

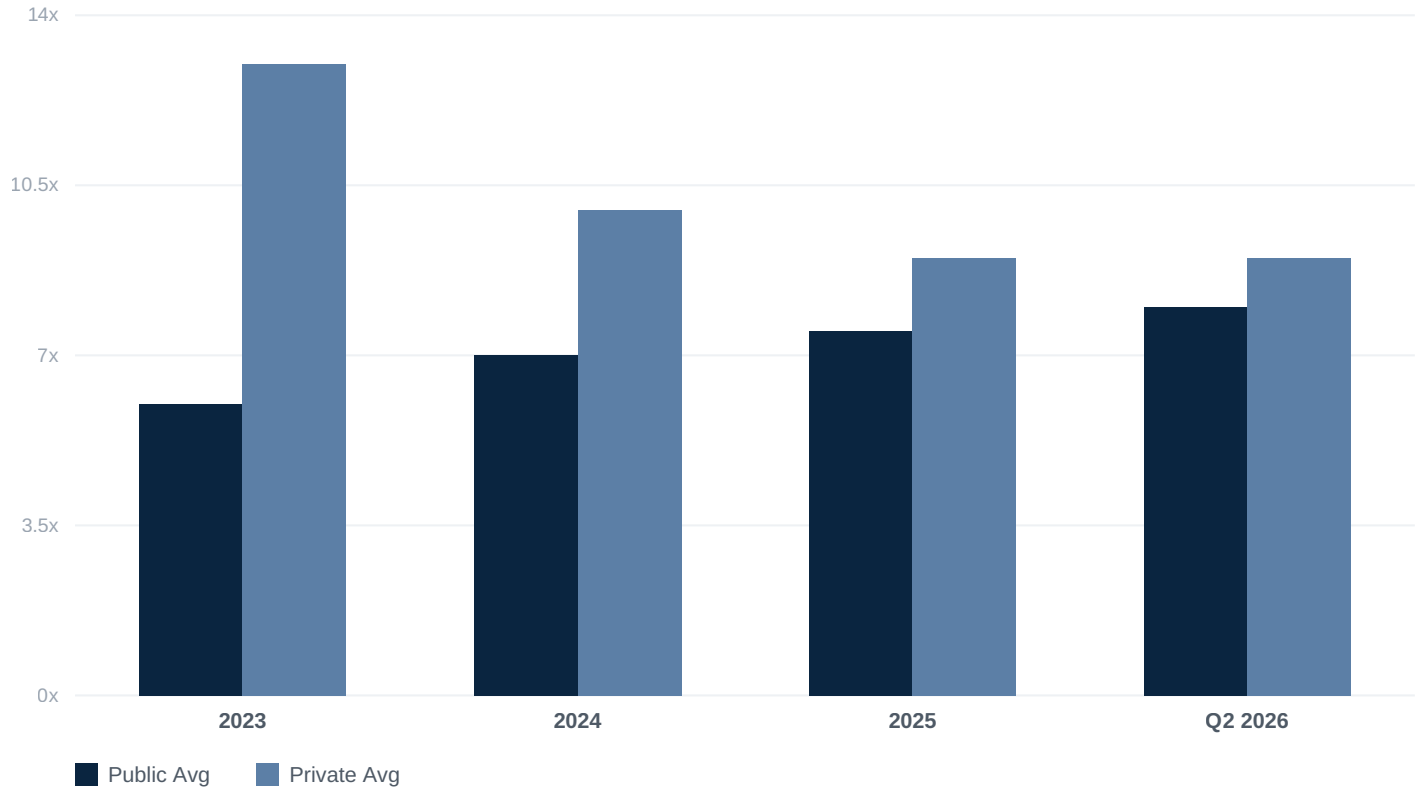
Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

Public vs Private Market Convergence

WINDSOR DRAKE

The private premium compressed sharply through 2023 to 2025, and now holds only for differentiated AI-native assets.

Average EV / Revenue Multiple, Public vs Private (x)



PUBLIC / PRIVATE SPREAD

~1.0x

Down from about 7x in 2023, with most of the gap closed by 2025 (Windsor Drake analysis).

DIFFERENTIATED PRIVATE TAIL

12x to 18x

AI-native EDR and autonomous-SOC rounds still clear blended public marks decisively.

PUBLIC BENCHMARK ANCHOR

~8.0x

Public comparables now cap late-stage private round pricing for non-differentiated assets.

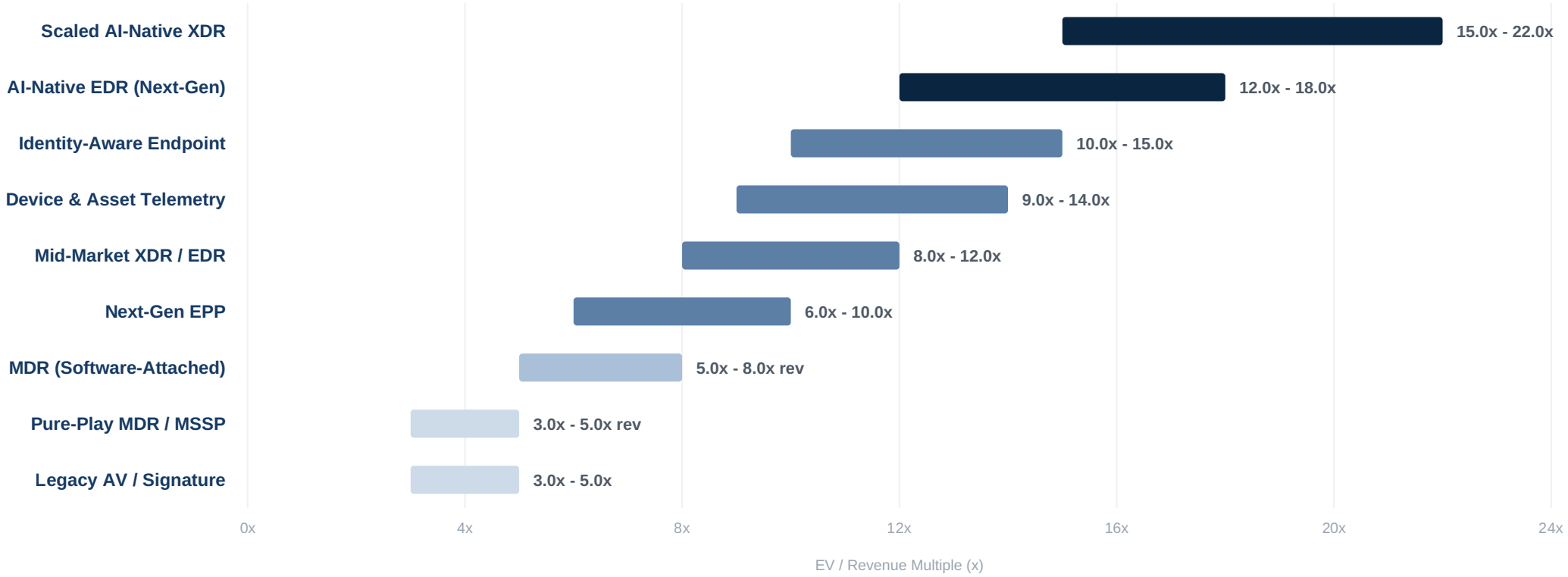
Selective convergence: the public-to-private spread narrowed from about 7x in 2023 to roughly 1x in 2026. Scaled AI-native XDR still prints far above the blended mean, repricing the very top of the cohort while sub-scale private endpoint marks have gone flat.

Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

Exit Valuation Multiples by Endpoint Segment

WINDSOR DRAKE

A sharp barbell persists between scaled AI-native platforms (15x to 22x) and pure-services or legacy stacks (3x to 5x).



KEY OBSERVATION

The market is paying for AI-native detection and telemetry scale, not for category labels. The multiple gap between scaled XDR platforms and legacy antivirus reflects the structural shift from signature-based agents to software-delivered, identity-aware, autonomous defence.

Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

Valuation Multiple Drivers: Expansion vs. Compression

WINDSOR DRAKE

Net expansion to roughly 8.0x is driven by AI-native detection, platform consolidation and zero-trust mandates, partly offset by AI margin drag, legacy commoditisation and restrictive rates.

NET EXPANSION OF +1.0X

AI-native detection, platform breadth and zero-trust regulation outweigh a combined 0.9x drag from AI infrastructure cost, legacy AV commoditisation and a higher-for-longer rate path. The bridge reflects Windsor Drake analysis of the cited institutional data.

Source: Windsor Drake analysis of Gartner, Bain and Federal Reserve data. See appendix.

Capital Markets: Listing Benchmarks & Public Comps

WINDSOR DRAKE

Scaled endpoint pure-plays are already public; the listing question now centres on private MDR leaders.

CrowdStrike (Nasdaq)

The public benchmark for scaled, profitable endpoint, reporting **$5.51B ARR (+24%)** as of April 2026 (filings).

- Q1 FY27 revenue of **$1.39B (+26%)** and record Q1 net new ARR of **$256M (+32%)** (filings).
- Record free cash flow of **$468M** in the quarter; non-GAAP subscription gross margin **81%**.
- Trades near **18x to 20x NTM revenue**, the cohort ceiling (Windsor Drake analysis).
- Advancing toward **$10B** ending ARR on Falcon Flex and platform attach.

SentinelOne (NYSE)

The scale-and-profitability discount case, reporting **$1.16B ARR (+23%)** as of April 2026 (filings).

- Q1 FY27 revenue of **$277M (+21%)**; non-GAAP gross margin **77%** (filings).
- Emerging solutions reached roughly **half of total ARR**, broadening beyond core EDR.
- Trades near **3.5x to 4x revenue**, a steep discount to CrowdStrike (WD analysis).
- Illustrates how scale and Rule of 40 separate the cohort, not category.

Arctic Wolf (Private)

The most-watched MDR IPO candidate, valued near **$4.4B** (PitchBook).

- Leading managed-detection-and-response operator with broad mid-market reach.
- Acquired **Sevco Security** (asset and device telemetry) in February 2026 (PitchBook).
- Leadership has signalled it is awaiting a friendlier rate and multiple window.
- A successful listing would reset the public comp set for managed endpoint.

Microsoft Defender (Incumbent)

Named a Leader in the **2026 Gartner Magic Quadrant for Endpoint Protection** (Gartner).

- Defender for Endpoint bundling pressures standalone EPP and EDR pricing.
- Sets a high free-or-bundled baseline that pure-plays must out-innovate.
- Reinforces that differentiation, not breadth alone, sustains premium multiples.
- Frames the buy-versus-build calculus for every mid-market endpoint vendor.

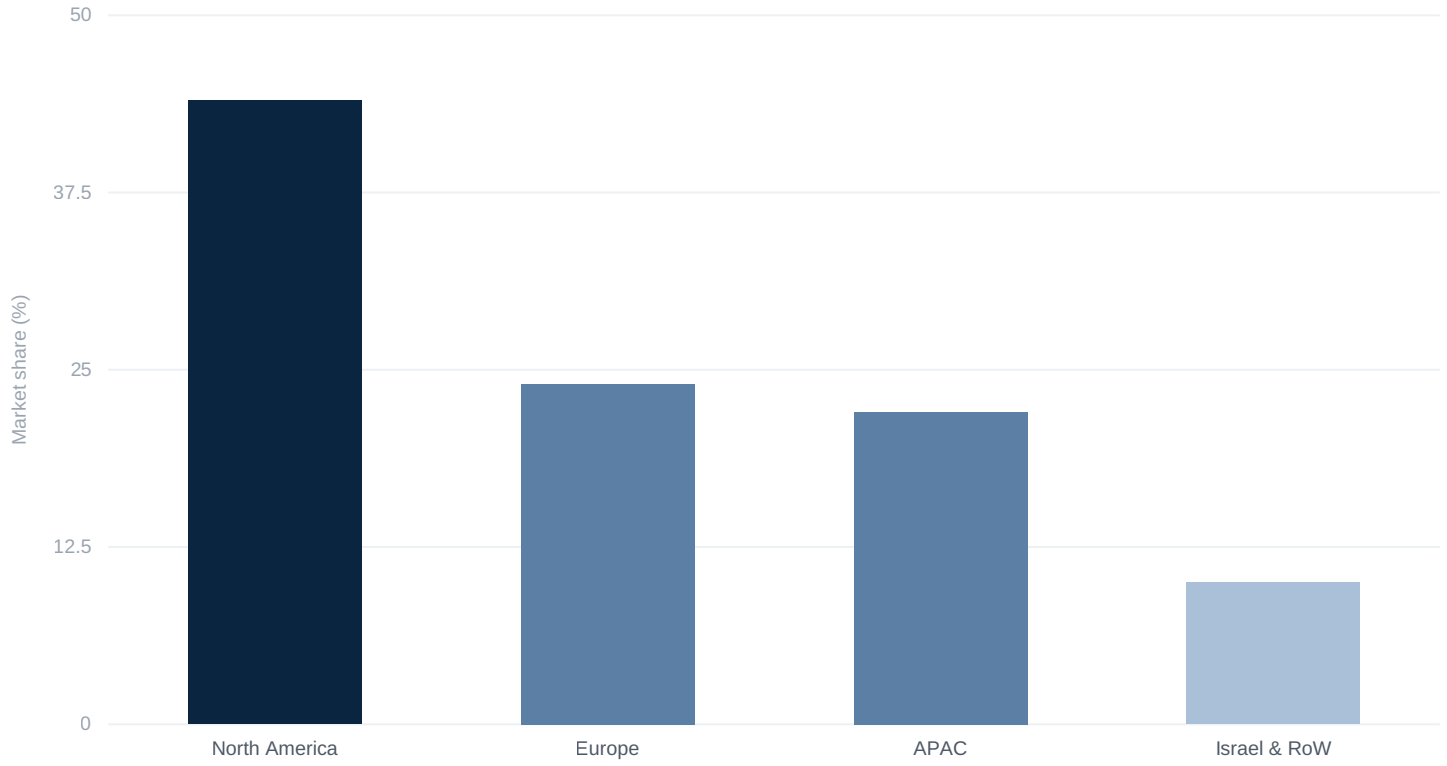
Sources: Gartner; company and SEC filings; PitchBook. See appendix.

Geographic Valuation Variations

WINDSOR DRAKE

North America commands an endpoint premium; Israel anchors innovation and Europe offers a fragmentation discount.

Share of Global Cybersecurity Market by Region (%)



NORTH AMERICA

Premium

About 44% of the global cybersecurity market, deepest exit liquidity and the scaled endpoint platforms.

EUROPE

Discount

About 24% share; NIS2 and DORA moats, offset by a fragmented endpoint vendor landscape.

ISRAEL & APAC

Growth

Israel and APAC together drive about 32% of share; Israel remains a dominant endpoint venture pipeline.

Valuation gap: North America commands the endpoint premium, home to CrowdStrike, Microsoft, Tanium and Arctic Wolf. Israel remains a dense endpoint-innovation hub (SentinelOne heritage, Cybereason). Europe (Sophos, Bitdefender, ESET) trades at a fragmentation discount that US acquirers are arbitraging.

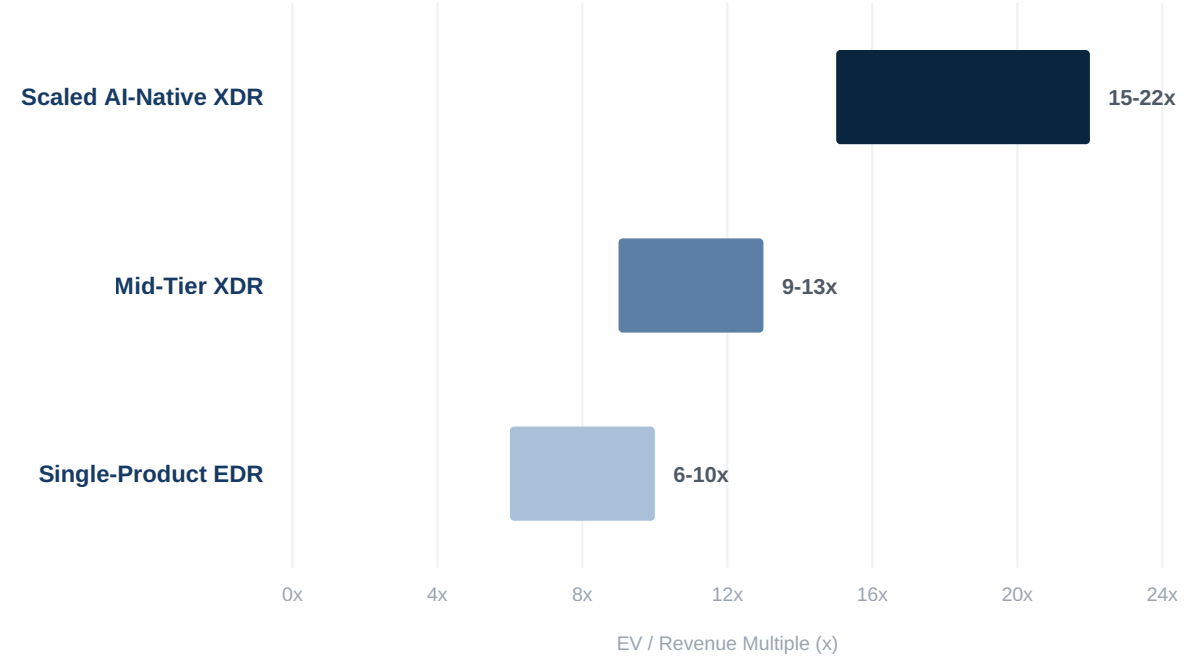
Sources: Gartner; S&P Global Market Intelligence; Windsor Drake analysis. See appendix.

Scaled XDR Platforms: The Premium Cohort

WINDSOR DRAKE

AI-native detection, telemetry scale and platform breadth underwrite the cycle's highest endpoint multiples.

EV / Revenue Multiple Range (x)



Valuation Drivers

Scale Defensibility

CrowdStrike crossed **$5.51B ARR (+24%)** with record Q1 net new ARR of $256M, and trades near 18x to 20x NTM revenue on platform reach and rule-of-40 performance, anchoring the top of the cohort.

Data-Lake Economics

Scaled XDR platforms are valued as security data lakes that anchor adjacent SIEM, identity and exposure workloads, expanding the addressable wallet per endpoint and lifting net revenue retention.

Buyer Priorities

Platform incumbents acquire AI-driven detection (browser, SaaS posture, identity, data telemetry) to compound their telemetry and policy advantages rather than build it slowly in-house.

KEY OBSERVATION

CrowdStrike's roll-ups of Adaptive Shield, SGNL, Seraphic, Pangea and Onum illustrate the capability-compounding pattern that sustains premium XDR multiples.

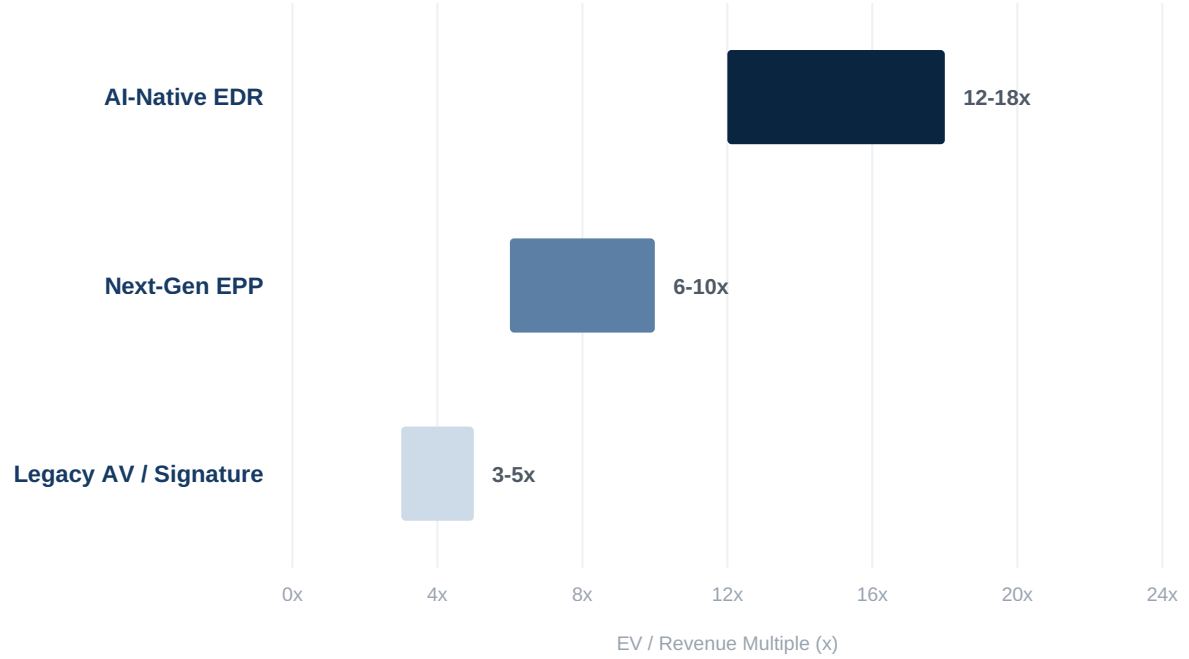
Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

EDR & Next-Generation Endpoint Protection (EPP)

WINDSOR DRAKE

Endpoint Protection is the largest security category by spend, but value accrues to AI-native, platform-attached EDR.

EV / Revenue Multiple Range (x)



Valuation Drivers

Legacy Displacement

Signature-based antivirus is being displaced by behavioural, AI-native EDR. The replacement cycle is durable, but pricing power sits with the platforms doing the displacing, not the incumbents being displaced.

Consolidation into XDR

Standalone EDR is increasingly absorbed into XDR and the broader SOC stack, compressing multiples for single-product tools while lifting platforms that own the telemetry and the response workflow.

Microsoft Bundling Pressure

Microsoft, a Leader in the 2026 Gartner Magic Quadrant for Endpoint Protection, bundles Defender aggressively, setting a low baseline that pure-play EPP and EDR vendors must out-innovate to defend price.

KEY OBSERVATION

Endpoint Protection is the single largest security category at **$17.8B, growing 14.5% in 2026 (Gartner)**, yet the premium accrues to AI-native, platform-attached EDR rather than commodity EPP.

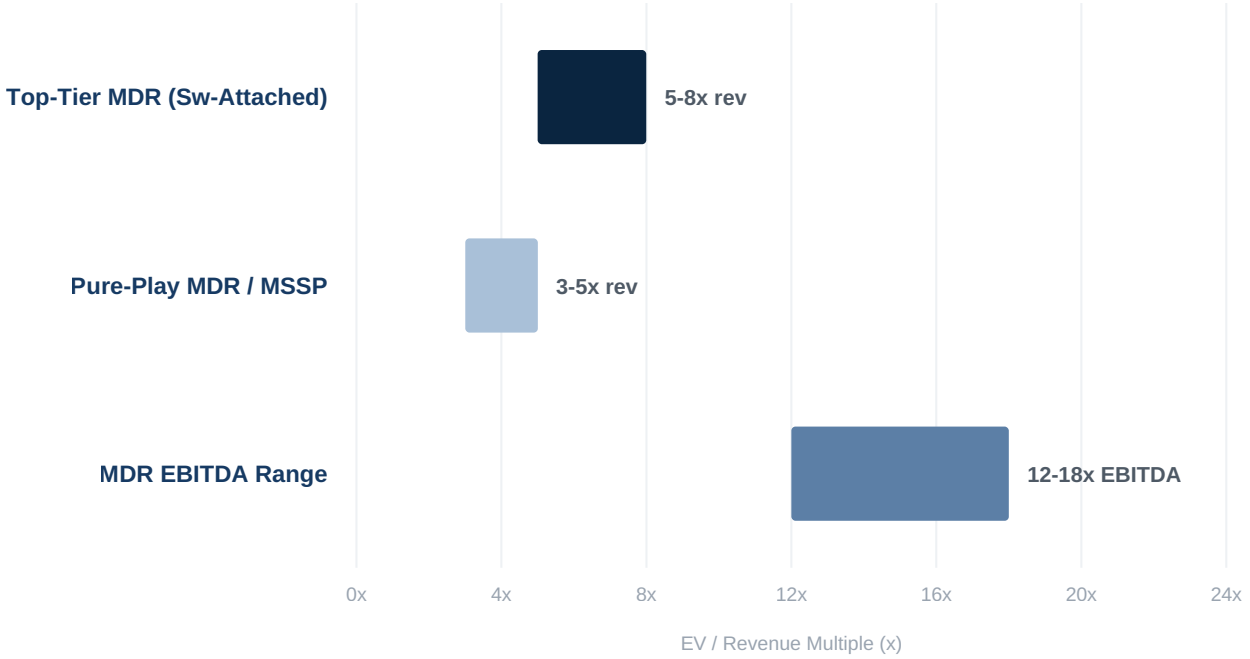
Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

Managed Detection & Response (MDR)

WINDSOR DRAKE

Managed endpoint demand is structural, but pure-services multiples stay compressed versus software-attached operators.

EV / Revenue Multiple Range (x)



KEY OBSERVATION

Software-attached MDR earns a clear revenue-multiple premium versus pure-services MSSP, the sharpest expression of the segment's bifurcation.

Valuation Drivers

Scale Economics

Sophos (Thoma Bravo) acquired **Secureworks** for **$859M** to become the largest pure-play MDR provider, serving about 28,000 organisations on the Taegis platform. Scale drives delivery margin and recurring-revenue density.

Software Attach

MDR operators that own underlying EDR, XDR and telemetry trade at meaningful premia to pure resellers; embedded software lifts gross margin, contract stickiness and the achievable revenue multiple.

PE Roll-Up Engine

Sponsors with roughly **$3.7T** of dry powder treat MDR as a buy-and-build category, pricing on EBITDA with multiple-arbitrage upside as scale compounds. Arctic Wolf, valued near $4.4B, leads the independent cohort.

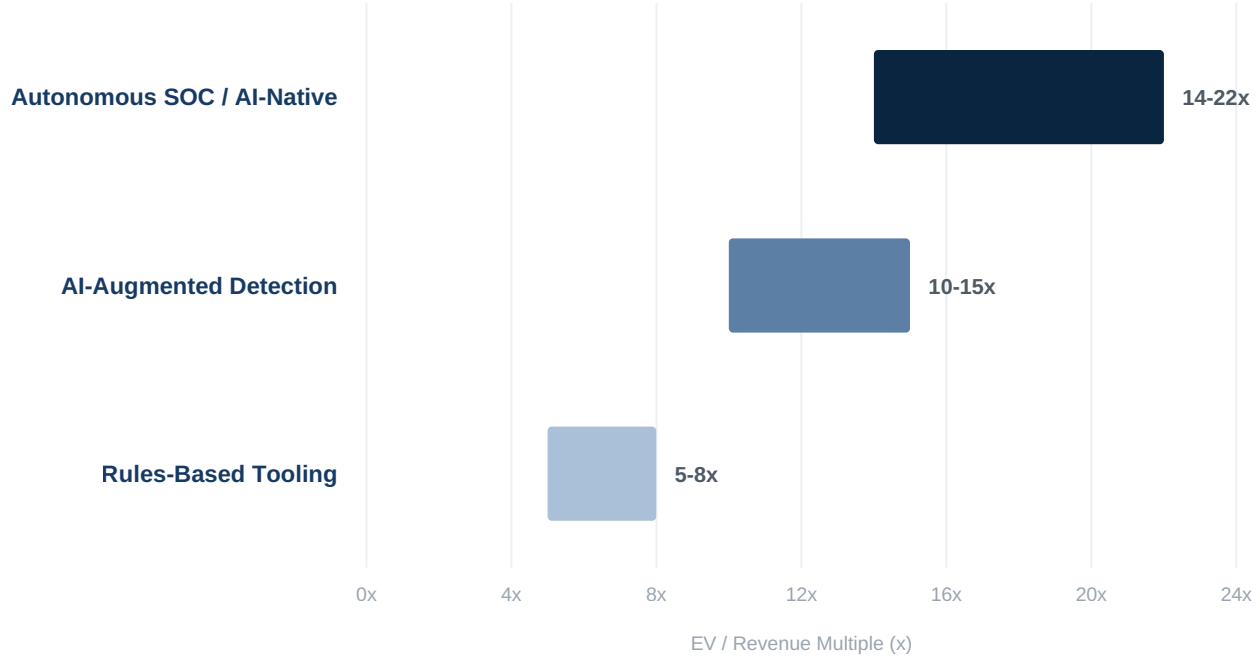
Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

AI-Native Endpoint & the Autonomous SOC

WINDSOR DRAKE

Detection and response decoupled from analyst headcount is the fastest re-rating driver across the endpoint stack.

EV / Revenue Multiple Range (x)



Valuation Drivers

Headcount Decoupling

LLM-assisted triage and automated response cut the marginal cost to defend an endpoint, demonstrating non-linear margin expansion as the install base scales and lifting the Rule of 40 score that gates premium multiples.

Telemetry Advantage

Proprietary endpoint telemetry trains detection models that rivals cannot easily replicate, creating a compounding data moat that grows with sensor count and event history.

Buyer Priorities

CrowdStrike (Charlotte AI, plus SGNL and Seraphic) and SentinelOne (Purple AI) are buying and building autonomous-SOC capability, treating defensive AI as core infrastructure rather than an experiment.

KEY OBSERVATION

SentinelOne's emerging solutions reached roughly **half of total ARR** by April 2026 (filings), evidence that AI-native and adjacent modules now drive the growth narrative.

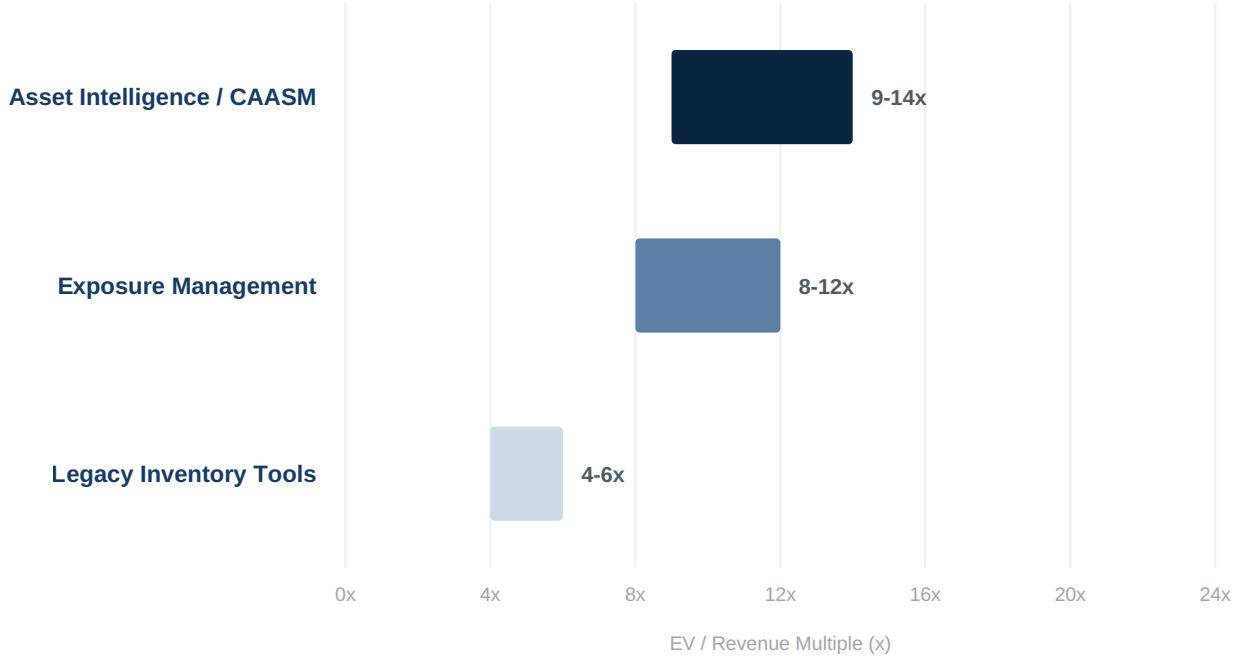
Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

Device, Asset & Endpoint Telemetry

WINDSOR DRAKE

Asset intelligence and exposure management compound the XDR data-lake thesis as high-value adjacencies.

EV / Revenue Multiple Range (x)



Valuation Drivers

Device Sprawl

AI agents, unmanaged devices and shadow assets are expanding the endpoint estate, driving demand for continuous asset discovery, classification and device telemetry as a foundation for any zero-trust programme.

Exposure Convergence

Asset intelligence is converging with exposure and vulnerability management into a single buying decision, rewarding platforms that unify the device inventory with the detection and response stack.

Buyer Priorities

Arctic Wolf's acquisition of **Sevco Security** in February 2026 and CrowdStrike's exposure-management push show incumbents pricing telemetry as a cloud-and-endpoint adjacency, not a standalone tool.

VALUATION DRIVER

Device and endpoint telemetry assets compound the scaled XDR multiple structure as adjacencies that deepen the data moat.

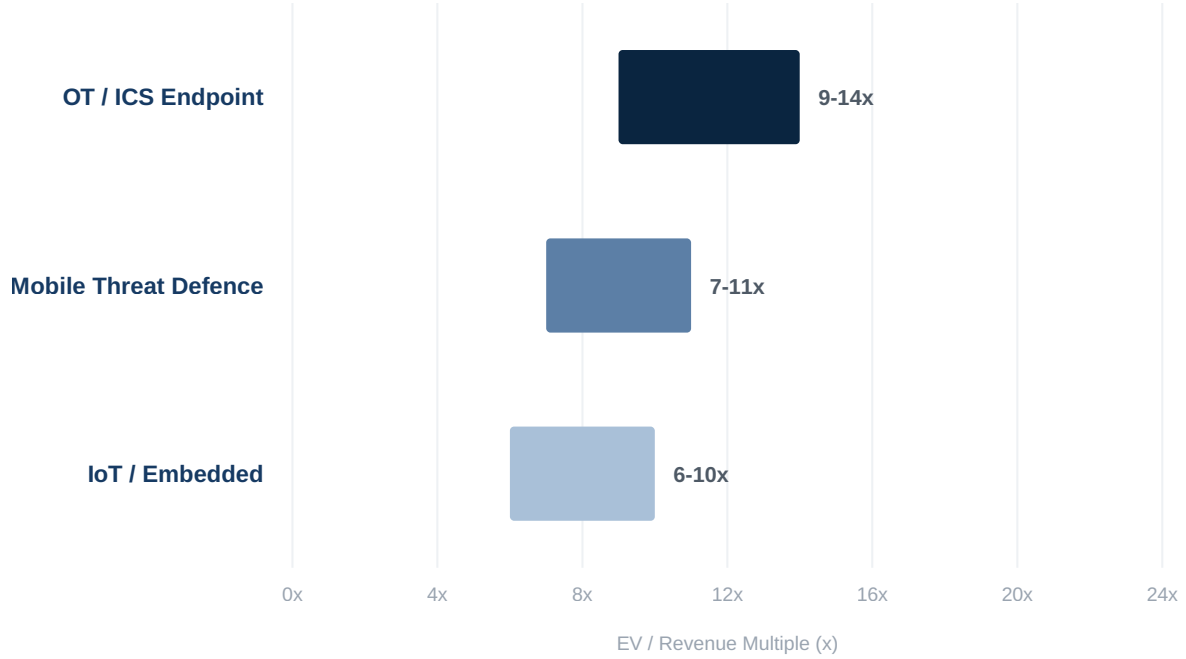
Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

Mobile, IoT & OT Endpoint

WINDSOR DRAKE

The endpoint definition is widening to phones, devices and industrial systems, opening a regulated, premium-priced frontier.

EV / Revenue Multiple Range (x)



Valuation Drivers

Expanding Definition

Endpoint now spans mobile, IoT and operational-technology assets, expanding the protectable surface well beyond servers and laptops and creating new, defensible niches for purpose-built vendors.

Critical-Infrastructure Mandates

NIS2, DORA and US critical-infrastructure rules turn OT and device monitoring from best practice into a compliance obligation, widening the buying centre and supporting premium pricing for regulated coverage.

Buyer Priorities

Scaled platforms extend their agents and telemetry to non-traditional endpoints to defend the consolidation thesis, acquiring specialist OT and mobile capability rather than building it from scratch.

KEY OBSERVATION

Regulatory mandates widen the non-traditional endpoint TAM faster than incumbents can build coverage, sustaining premium multiples for credible OT and mobile specialists.

Sources: Gartner; CB Insights; company and SEC filings; Windsor Drake analysis. See appendix.

Comparable Transaction Analysis Framework

WINDSOR DRAKE

A rigorous quality-of-revenue filter rather than broad endpoint category labels.

1. Select Peer Set

Identify genuinely comparable assets by architecture (AI-native vs signature-based), buyer (SOC vs IT operations vs MSSP), revenue model (consumption vs subscription) and autonomous-SOC posture, not by broad endpoint labels.

2. Normalise Metrics

Adjust KPIs to a pro-forma basis: normalise ARR for M&A, standardise NRR and GRR definitions, separate platform software from managed-services revenue, and reconcile reported and verified deal metrics.

3. Adjust for Structure

Account for deal-specific terms (earn-outs, stock-versus-cash mix, control premiums, and CFIUS / FDI overhang) that pull headline valuation away from underlying economic value.

255
WD INDEX TRANSACTIONS

2020-26
INDEX COVERAGE

Proprietary Transaction Index

Calibration draws on Windsor Drake's proprietary index of **255 verified and reported transactions (2020 to 2026)**, refreshed each quarter and supplemented by current-quarter endpoint research for segment-specific comps.

Quality-of-Revenue Filter

Peer selection prioritises recurring vs re-occurring revenue, gross margin profile (above 75% for software vs below 60% for managed services), and concentration risk across enterprise vs mid-market cohorts.

Rule of 40 Premium Adjustment

A specific premium layer is applied for top-decile efficiency performers; offsetting discounts are applied where AI infrastructure cost is depressing margin below the threshold.

Control Premium Calibration

Indications include a control-premium layer, typically **25% to 30%** in strategic endpoint processes, where platform and capability synergies can be concretely underwritten.

Source: Windsor Drake proprietary transaction database and methodology.

Strategic Acquirer Mapping by Endpoint Segment

WINDSOR DRAKE

Platform incumbents pursue capability roll-ups; PE concentrates on MDR and managed endpoint; hyperscalers mostly partner.

Segment	Hyperscalers / Strategics	Platform Incumbents	Private Equity
Scaled XDR / Platform	**MODERATE** Hyperscalers prefer to partner with scaled XDR rather than acquire it.	**HIGH** Incumbents extend platforms via capability M&A to defend the consolidation thesis.	**MODERATE** PE pursues take-privates of mid-tier XDR assets selectively.
EDR / Next-Gen EPP	**LOW** Microsoft builds Defender rather than buying EPP; hyperscalers rarely acquire.	**HIGH** XDR leaders absorb EDR and EPP capability to widen the protected surface.	**MODERATE** PE consolidates mid-market EPP and EDR into managed platforms.
MDR (Managed)	**LOW** Hyperscalers partner; they rarely acquire pure managed services.	**MODERATE** Incumbents bundle MDR to attach managed services to software.	**HIGH** PE primary buyer; the roll-up engine for MDR and managed-endpoint scale.
AI-Native Endpoint	**MODERATE** Hyperscalers acquire AI detection talent selectively for cloud security.	**HIGH** Incumbents buy autonomous-SOC and AI detection to compound telemetry moats.	**MODERATE** PE backs AI-native challengers as platform foundations.
Device / Asset Telemetry	**MODERATE** Hyperscalers fold asset intelligence into cloud and identity stacks.	**HIGH** Endpoint platforms add CAASM and exposure data to deepen the data lake.	**MODERATE** PE buys exposure and asset SaaS for buy-and-build theses.
Mobile / IoT / OT	**LOW** Hyperscalers partner on device coverage rather than acquire specialists.	**MODERATE** Platforms add OT and mobile capability to extend agent coverage.	**MODERATE** PE consolidates regulated OT and mobile niche vendors.

Platform Incumbents & Hyperscalers as Buyers

WINDSOR DRAKE

Endpoint platforms are using M&A to convert detection scale into a durable consolidation moat.

Strategic Motives: Buy vs. Build

The internal build cycle for AI-native detection, identity-aware policy and browser or SaaS-posture coverage is too slow to counter category-defining startups. That gap compels endpoint incumbents to acquire modern stacks outright, treating M&A as defensive modernisation rather than expansion.

Acquisition Patterns

Capability bolt-ons under $1B dominate by volume (CrowdStrike's SGNL, Seraphic, Pangea and Onum), often preceded by partnership or technology-integration de-risking. Larger managed-endpoint consolidation (Sophos / Secureworks, $859M) sits at the top of the pure-play range.

$5.51B
CROWDSTRIKE ARR, APR 2026

$859M
SOPHOS / SECUREWORKS

Semi-Autonomous Integration

A federated model preserves the target's product cadence and retains scarce detection-engineering talent, while platform-grade compliance and telemetry pipelines are overlaid at the backend.

Priority: AI-Native Detection

Top focus is autonomous-SOC and AI-driven detection deployable across the existing endpoint install base, lifting analyst productivity and net revenue retention.

Priority: Identity & Browser

Identity, browser and SaaS-posture telemetry extend the endpoint into the modern work surface; assets here are priced as platform pillars, not point tools.

Priority: Telemetry & Exposure

Device, asset and exposure telemetry are increasingly priority targets to deepen the security data lake and make endpoint platforms 'SOC-complete' for enterprise buyers.

Sources: company press releases; SEC filings; Windsor Drake analysis. See appendix.

Private Equity Acquisition Patterns

WINDSOR DRAKE

Record dry powder is creating intense deployment pressure on efficient, cash-generative endpoint and MDR assets.

Deployment Pressure

With roughly **$3.7T** of global dry powder to deploy, sponsors face acute pressure to transact (McKinsey; Bain). Cyber venture and growth funding reached about **$18B in 2025**, the highest in three years, even as capital concentrated in identity and security operations over standalone endpoint (CB Insights; Crunchbase).

Managed-Endpoint Roll-Up Thesis

MDR and managed endpoint are prime buy-and-build categories; Thoma Bravo's Sophos (Sophos / Secureworks, $859M) is the template, and independents such as Arctic Wolf (valued near $4.4B) anchor the next wave of sponsor interest.

~$3.7T
GLOBAL PE DRY POWDER

~$18B
CYBER VC FUNDING, 2025

Ideal Target Profile

Sponsors prioritise **Rule of 40** adherence, a recurring-revenue mix above 85%, and gross retention above 90%, the profile that supports leverage capacity in managed-endpoint roll-ups.

Value-Creation Playbook

Pricing optimisation, a mix-shift toward software-attached managed services, and buy-and-build consolidation of MDR, MSSP and verticalised endpoint software.

Aging-Portfolio Catalyst

Many PE software holdings now exceed a five-year hold, and as 2022 to 2024 vintage capital approaches its deployment deadline, sponsors are increasingly motivated to transact (McKinsey).

Deal Structure Trends

A preference for all-cash transactions for deal certainty, with earn-outs bridging gaps on unproven AI-native capability.

Sources: McKinsey & Company; Bain & Company; CB Insights. See appendix.

Competitive Moats Driving Premium Valuations

WINDSOR DRAKE

Endpoint valuations above 12x revenue are reserved for companies that can demonstrate structural defensibility.

Telemetry & Data Moats

ASSET VALUE: HIGH

Proprietary endpoint telemetry training detection models

- Creates a virtuous cycle of detection improvement that rivals cannot easily replicate.
- Powers unique threat-intelligence, behavioural and identity analytics capability.
- Compounds in value as the install base, sensor count and event history grow.
- **Action:** deepen first-party telemetry capture across every endpoint and device.

AI-Native Architecture

SCALE VALUE: HIGHEST

Detection and response decoupled from analyst headcount

- LLM-assisted triage and automated response cut the marginal cost to defend.
- Demonstrates non-linear margin expansion as the customer base scales.
- Directly lifts the Rule of 40 score that gates premium multiples.
- **Action:** integrate AI into core detection, response and identity workflows.

Certifications & Compliance

BARRIER VALUE: MED-HIGH

Hard-to-acquire certifications and regulated access

- FedRAMP High, IL5 and ISO 27001 are difficult, expensive and slow to obtain.
- Function as compliance-by-design, a structural barrier to mid-market entrants.
- Are increasingly central to government and critical-infrastructure theses.
- **Action:** invest early in certifications that gate the most defensible verticals.

Platform Attach

GROWTH VALUE: HIGH

Multi-module attach and identity-aware policy

- Each incremental module (identity, exposure, SIEM) raises NRR and churn cost.
- Drives structurally lower CAC and higher retention over time.
- Raises switching costs as endpoint, identity and data converge in one stack.
- **Action:** prioritise attach motion in the most strategic customer segments.

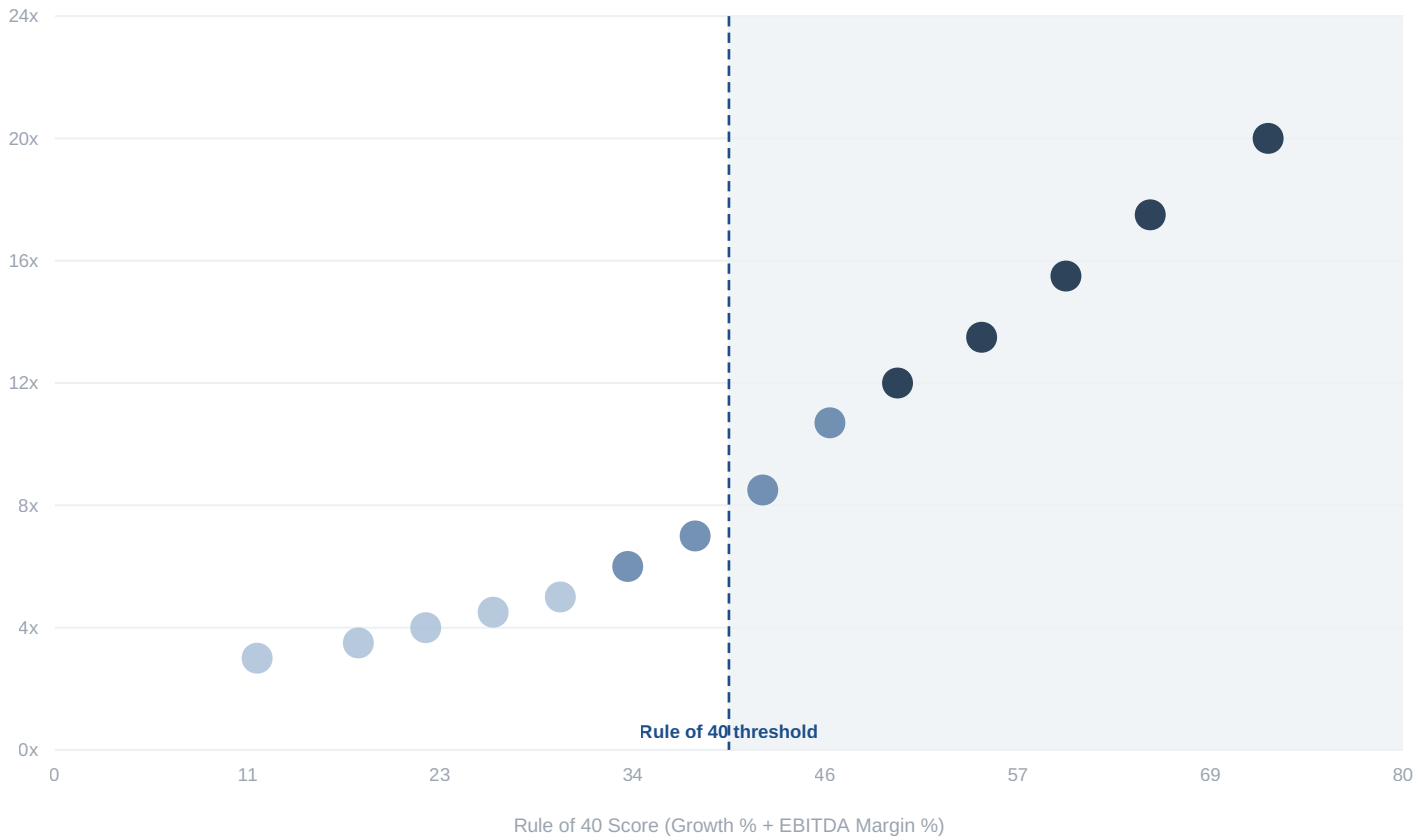
Source: Windsor Drake analysis. See appendix.

Rule of 40 Performance Distribution

WINDSOR DRAKE

Clearing the Rule of 40 unlocks a 50% to 100% valuation premium; AI infrastructure cost is pressuring the rule across the cohort.

EV / Revenue Multiple vs Rule of 40 Score



TOP QUARTILE (SCORE >50)

12x to 22x+

Scaled winners; the primary targets for premium strategic M&A and the public-market leaders.

RULE OF 40 MET (40 TO 50)

8x to 12x

A healthy growth and profit balance; credible IPO-ready candidates.

BELOW THRESHOLD (<40)

3x to 7x

Transition and value-trap zones; vulnerable to consolidation.

Public software that clears the Rule of 40 posts a median 10.7x EV/Revenue (Bain), and endpoint leaders such as CrowdStrike clear that bar materially, trading near 18x to 20x NTM revenue. AI infrastructure cost is pressuring the rule, leading some analysts to discuss a 'Rule of 30' alternative for AI-native players.

Sources: McKinsey & Company; Bain & Company; Windsor Drake analysis. See appendix.

Cross-Border M&A Considerations

WINDSOR DRAKE

Jurisdictional divergence is the primary deal risk, and the primary arbitrage, in endpoint security in 2026.

Regulatory Regimes

Heightened scrutiny of security and data infrastructure (CFIUS, FDI review), and divergence between EU AI Act compliance, NIS2, DORA and US frameworks, materially complicate tech-stack integration for endpoint telemetry and lengthen approval timelines.

Currency & WACC Impact

US acquirers are leveraging a strong dollar and premium domestic multiples to buy discounted European and Israeli endpoint assets; managing divergent regional rate environments is central to any debt-financed deal.

12-18mo
CROSS-BORDER CYCLE

+30-50%
LONGER CLEARANCE

Extended Timelines

Regulatory clearance for cross-border security deals now runs 30% to 50% longer than domestic transactions; ensure runway to withstand delay without losing leverage.

Milestone-Tied Earn-Outs

Regulatory earn-outs unlock tranches of consideration on specific authorisation transfers or data-sovereignty approvals, rather than on revenue alone.

Tax & Structure Efficiency

Establish efficient holding structures early; optimise repatriation and IP transfer pricing well before LOI discussions begin, particularly for Israeli-based endpoint IP.

Dual-Track & Local Partners

Run IPO readiness alongside the M&A process for competitive tension, and retain local management to navigate post-close regulatory nuance.

Sources: EY; PwC; Windsor Drake analysis. See appendix.

Exit Valuation Optimisation Strategies

WINDSOR DRAKE

Four levers that systematically de-risk the asset while amplifying its scarcity value.

1. Pricing Power & Margins

6 TO 12 MONTHS PRE-EXIT

Demonstrate defensible unit economics

- Shift from seat-based to **outcome and consumption pricing** where possible.
- Implement platform-tier upsell across endpoint, identity and exposure modules.
- Target a 15%-plus ARPU lift across the top customer cohorts.
- Evidence pricing elasticity with clean, auditable cohort data.

2. Revenue Quality

PREDICTABILITY

Engineer resilience into the revenue model

- Increase the recurring revenue mix to **85%+** of total.
- Improve Net Revenue Retention to **>120%** via module attach.
- Reduce concentration so the top 10 accounts are under 25%.
- Lengthen contract duration to extend revenue visibility.

3. Rule of 40 Efficiency

PREMIUM TIER

Prove scalable profitability

- Reallocate operating expense from low-ROI channels into R&D.
- Deploy AI to decouple analyst headcount from revenue growth.
- Achieve **above 40%** on growth plus EBITDA margin.
- Track the score monthly with board-level visibility.

4. Strategic Narrative

COMPETITIVE TENSION

Frame the asset as a platform enabler

- Position as SOC-complete platform infrastructure, not a point tool.
- Present quantified synergy cases covering revenue and cost.
- Map specific capability gaps for the top five strategic acquirers.
- Run a structured process to manufacture competitive tension.

Source: Windsor Drake advisory methodology. See appendix.

Positioning for Strategic Acquisition

WINDSOR DRAKE

Strategic value is driven by capability fit, integration ease and synergy density.

Capability Fit

Demonstrate unique IP and proprietary telemetry, identity or AI-native detection assets that fill a specific, declared buyer gap, making the buy-versus-build decision self-evident for the acquirer.

Integration Ease

Acquirers pay clear premiums for plug-and-play assets. Minimise critical dependencies, document APIs and event schemas thoroughly, and present clean, audited financials and security certifications.

Synergy Density

Quantify the revenue lift from cross-selling into the acquirer's endpoint base, and model the cost synergies from shared telemetry and infrastructure, to support a higher multiple.

Strategic Buyer Mapping

Run a structured gap analysis of potential acquirers and map your capabilities directly to each buyer's declared strategic deficits.

Proof-of-Integration

Develop technical materials that demonstrate speed-to-value within the acquirer's ecosystem, pre-empting the technical diligence phase.

Synergy Quantification

Explicitly model top-line and bottom-line impact in the management presentation to anchor the valuation conversation on hard numbers.

Comprehensive VDR Readiness

Build a defensive data room addressing regulatory, IP, customer-concentration and certification risk before the first buyer engagement.

Source: Windsor Drake advisory methodology. See appendix.

Timing the Exit: 12-18 Month Roadmap

WINDSOR DRAKE

A full process runs 12 to 18 months end to end. Founders who prepare in the current cycle meet the market while today's alignment of strategic-buyer demand, AI-native premia and barbelled pricing still holds.

Readiness & Hygiene
Q3 2026

- Audit completion to PCAOB standard
- AI governance and data-rights review
- Security certification refresh (SOC 2, FedRAMP)
- Clean up the cap table and option pool

KEY MILESTONE
Clean IP and security audit

Strategic Positioning
Q4 2026

- Launch dual-track process preparation
- Build the strategic buyer-targeting list
- Draft the CIM and management presentation
- Lock key-employee retention packages

KEY MILESTONE
Retention packages locked

Market Engagement
Q1 2027

- Fireside chats with priority strategics
- Solicit initial indications of interest
- Deliver management presentations
- Open the virtual data room

KEY MILESTONE
Competitive bid tension

Execution & Closing
Q2 2027

- Definitive agreement negotiation
- Regulatory filings (HSR, CFIUS, FDI)
- Confirmatory diligence support
- Closing and integration kickoff

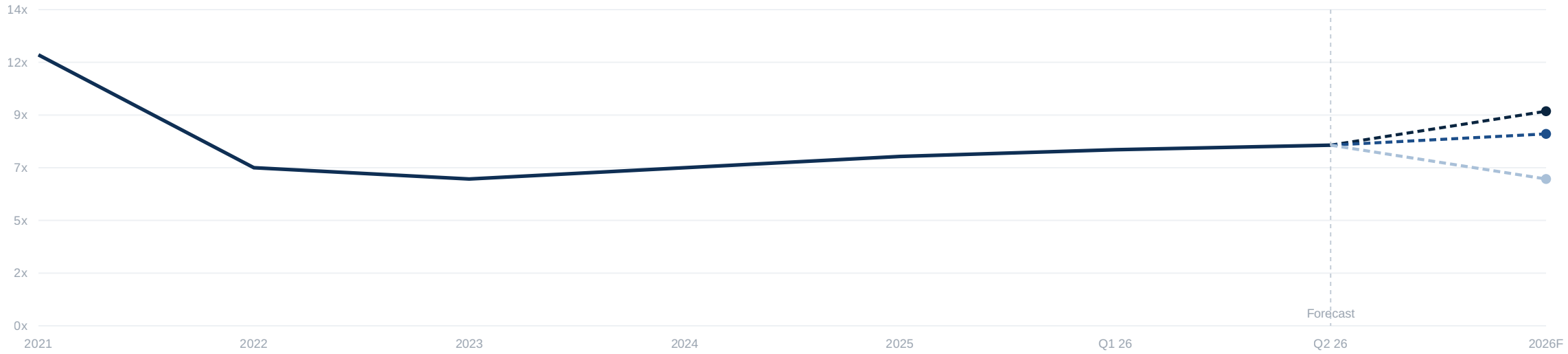
KEY MILESTONE
No-MAC event verification

Source: Windsor Drake advisory methodology. See appendix.

2026 Valuation Forecast Scenarios

WINDSOR DRAKE

With the blended endpoint benchmark near 8.0x, forward trajectories diverge on rates, AI pricing dynamics and the pace of platform consolidation.



BULL CASE — 9.5x

Key Drivers

- Fed delivers H2 2026 cuts
- Autonomous-SOC supercycle lifts multiples
- MDR roll-up bidding war intensifies

STRATEGY: ACCELERATE GROWTH

BASE CASE — 8.5x

Key Drivers

- Rates higher for longer, one cut
- Platform consolidation continues
- Barbell between XDR and AV persists

STRATEGY: BALANCE GROWTH & PROFIT

BEAR CASE — 6.5x

Key Drivers

- Inflation resurgence, no 2026 cuts
- AI cost compresses Rule of 40
- Legacy AV commoditisation accelerates

STRATEGY: CASH PRESERVATION

Source: Windsor Drake analysis; EY M&A Outlook; Federal Reserve projections. See appendix.

Emerging Opportunities & Buyer Trends

WINDSOR DRAKE

Capital is flowing into the connective infrastructure of an AI-first endpoint stack.

Autonomous SOC & AI Detection

Agentic, LLM-assisted detection and response is the fastest-emerging endpoint category, with both venture and strategic capital building toward an autonomous SOC that decouples defence from analyst headcount.

Device & Asset Telemetry

Continuous asset discovery and device telemetry (CAASM, exposure management) is in explosive demand; Arctic Wolf's Sevco acquisition shows incumbents treating it as a core endpoint adjacency.

Browser & Identity-Aware Endpoint

The browser and identity layer have become the new endpoint; CrowdStrike's Seraphic and SGNL acquisitions underline the strategic value of extending detection into the modern work surface.

Platform Capability Acquisitions

Endpoint incumbents prioritise AI-native detection, identity and telemetry capability over distribution, buying technology to make their platforms SOC-complete for enterprise buyers.

PE Managed-Endpoint Roll-Ups

Sponsors are consolidating fragmented MDR, MSSP and verticalised endpoint software to build scale and drive multiple expansion.

Regional Champions Go Global

European and Israeli endpoint leaders are acquiring or being acquired by North American platforms to capture premium valuations and access deeper capital markets.

Market Intelligence

Top-tier forecasts point to continued elevated cyber M&A in 2026. Record dry powder and capability-driven demand are chasing a supply of quality endpoint assets that has not kept pace.

Sources: McKinsey & Company; CB Insights; EY; Windsor Drake analysis. See appendix.

M&A Case Study: Sophos & Secureworks

WINDSOR DRAKE

The defining endpoint-services consolidation of the cycle, and the playbook it sets for founders.

The Managed-Endpoint Playbook

Sophos, backed by **Thoma Bravo**, acquired **Secureworks** for **$859M** in an all-cash transaction, creating the largest pure-play managed detection and response provider, serving about **28,000 organisations**. It confirms that scale buyers will pay up to consolidate managed endpoint and its underlying telemetry.

Strategic Rationale

- **MDR scale:** combining two large managed-endpoint operators drives delivery margin and recurring-revenue density.
- **Platform telemetry:** Secureworks' Taegis XDR platform and Counter Threat Unit deepen the combined detection data lake.
- **Sponsor thesis:** a PE-backed strategic executing buy-and-build at the top of the pure-play MDR range.

Implications for Founders

Software Attach Defines the Multiple

In managed endpoint, **owning the underlying software and telemetry** is what separates a premium revenue multiple from a services discount. Sophos paid for Taegis and the data, not headcount. Codify the software you own before a process begins.

Quantify Telemetry Synergies Pre-LOI

Headline value rests on **identifiable, underwritable telemetry and delivery synergies**. Vague strategic fit no longer moves valuation; rigorous synergy math, presented before the LOI, does.

Platform vs. Point Solution

Assets framed as **SOC-complete platforms** capable of absorbing bolt-ons trade at clear premiums to single-product tools. Integration readiness, clean APIs and a unified data model is itself a valuation lever, and the window to consolidate is narrowing as scale players combine.

Sources: company press releases; financial press. See appendix.

Valuation Methodology: Choosing the Right Metric

WINDSOR DRAKE

The right metric depends on business model, profitability profile and revenue mix.

EV / Revenue

10-22X+

High-growth AI-native endpoint

- Applied where profitability is suppressed by deliberate growth reinvestment.
- Software revenue (above 80% margin) is valued far above managed-services revenue.
- The Rule of 40 score dictates where in the range an asset sits.
- Best suited to scaled XDR, AI-native EDR and identity-aware endpoint platforms.

EV / EBITDA

12-18X

Mature & cash-generative

- Essential for mature MDR, scaled MSSP and PE-owned managed-endpoint operators.
- Many firms valued on revenue in 2024 are now assessed on EBITDA.
- Margin expansion and operating leverage are the key value drivers.
- Captures the cash-flow reality of consolidating managed-services segments.

ARR & NRR Lens

RECURRING FOCUS

SaaS-delivered endpoint assets

- Focus on ARR growth, NRR and gross retention as primary value drivers.
- Premium for NRR above 120% and gross retention above 90%.
- Discount for concentration risk and short contract duration.
- Most relevant for SaaS-delivered EDR, XDR and identity-aware endpoint.

Strategic Premium

+25-30%

Platform & capability fit

- Applied on top of underlying revenue or EBITDA multiples.
- Premiums accrue to AI-native detection and unique telemetry.
- Platform-integration potential can lift the premium materially.
- Synergy math should be modelled explicitly before LOI.

Source: Windsor Drake valuation methodology. See appendix.

Appendix: Sources & Methodology (Part 1)

WINDSOR DRAKE

Institution	Report / Source	Date
Gartner	*Forecast: Information Security, Worldwide (4Q25 Update); Forecast Analysis: Information Security, Worldwide, 2026*	Feb 2026
Gartner	*Magic Quadrant for Endpoint Protection Platforms 2026; Top Cybersecurity Trends 2026*	May 2026
McKinsey & Company	*Global Private Markets Report 2026*	Mar 2026
Bain & Company	*Hacking Software's Rule of 40; AI Brings Headwinds and Tailwinds*	2025
Bain & Company	*Global Private Equity Report 2026*	Feb 2026
PwC	*Global M&A Industry Trends: 2026 Outlook (TMT)*	Jan 2026
EY	*M&A Activity Insights: 2026 Outlook*	Apr 2026
S&P Global Market Intelligence	*Global M&A by the Numbers: Q1 2026*	Apr 2026
CB Insights	*State of Cybersecurity Venture Funding 2025*	2026
PitchBook	*Arctic Wolf company profile; Global Private Market Funds Dry Powder Dashboard 2026*	2026

Appendix: Sources & Methodology (Part 2)

WINDSOR DRAKE

Institution	Report / Source	Date
CrowdStrike Holdings	*Q1 FY2027 results (quarter ended Apr 30, 2026); FY2026 results*	Jun 2026
SentinelOne	*Q1 FY2027 results (quarter ended Apr 30, 2026)*	May 2026
Sophos / Thoma Bravo	*Sophos completes Secureworks acquisition (press releases)*	Feb 2025
Federal Reserve	*FOMC Statement (Mar 2026); Summary of Economic Projections (Mar 2026)*	2026
Microsoft	*Named a Leader in the 2026 Gartner Magic Quadrant for Endpoint Protection*	May 2026
Crunchbase	*Cybersecurity startup investment review 2025*	2026
World Economic Forum	*Global Cybersecurity Outlook 2026*	Jan 2026

VALUATION METHODOLOGY NOTES

Source Standard

Inputs are restricted to top-tier institutions: bulge-bracket banks, the major consultancies, elite data houses, and primary regulatory and filing sources. Boutique and market-report vendors are excluded.

Structural Adjustments

Private-market valuations are adjusted for earn-outs, liquidation-preference overhang and lack-of-marketability discounts, typically in the 20% to 30% range.

Peer Set & Normalisation

Peers are filtered on architecture (AI-native vs signature-based), buyer (SOC, IT operations, MSSP), revenue quality (above 85% recurring) and Rule of 40 profile. Financials are adjusted to a pro-forma basis excluding one-time items and stock-based compensation.

Synthesis & Attribution

Figures labelled as firm analysis or house estimate, including the roughly 8.0x blended endpoint benchmark and the public-comp multiple ranges, are the firm's own synthesis of the cited institutional data and public market pricing, presented as a house view rather than third-party consensus.