Cybersecurity Valuations: Q2 2026

Q2 2026 finds global cybersecurity in a state Windsor Drake characterises as a re-anchored premium: an enduring valuation premium underwritten by secular demand rather than cyclical exuberance. The sector's median public multiple has settled near **6.0x to 6.5x NTM Revenue**, roughly **25%** above the broader software median, and that stability, more than any single number, is the story of the quarter.

Beneath the benchmark sits a profound and widening split. Headline averages mask a profound divide between platforms and point tools. Cloud security and SASE leaders trade at **14x to 22x NTM revenue**, AI-native private rounds clear **20x to 30x**, and legacy network and managed-security operators sit at **5x to 8x** as capability is absorbed by larger platforms. Capital is concentrating at the top of the quality curve as middle-market exits surge.

The macro backdrop is constructive. The Federal Reserve funds range holds at **3.50% to 3.75%** after the March 2026 FOMC, with the March dot plot signalling one further cut in 2026 and easing the cost of capital for long-duration software assets. Demand fundamentals are exceptionally strong: Gartner forecasts global information-security end-user spending at **$244B in 2026, up 13.3%**, with AI security nearly doubling from **$25.9B to $51.3B** and cloud security growing **28.8%** year on year. Capital markets are reopening in parallel, and Google's **$32B** acquisition of Wiz, closed in March 2026, confirmed that hyperscaler buyers will pay record prices for category-defining cloud-native security assets.

This report sets out institutional-grade analysis for navigating that split market, one in which AI-native cloud and identity platforms are valued like premium infrastructure while legacy services and network operators face continued scrutiny.

What multiples are cybersecurity companies trading at?

The Q2 2026 valuation picture turns on a single divide: AI-native architecture, platform breadth and recurring revenue quality on one side; legacy delivery models, point-tool architecture and services-heavy economics on the other. The broad public-cyber median clusters near **6.0x to 6.5x NTM revenue**, a roughly **25%** premium to broader software, but the spread between the top and bottom of the table is the widest in a decade. Investors are paying up for cloud-native, identity-aware platforms, AI-driven detection, and durable platform attach economics.

Cloud security, identity and AI-native platforms are valued on architecture and platform breadth. Legacy network security, managed services and box-shipping models, by contrast, remain under scrutiny as platform incumbents and hyperscalers absorb capability and compress pricing. The gap between cohorts is wider than at any point in the past decade.

Table 1. Cybersecurity Valuation Multiples by Subsector, Q2 2026

Subsector	EV/Revenue Range	YoY Trend	Primary Driver
AI-Native Security Platforms	20.0x - 30.0x	Rising	Category-defining AI architecture
Cloud Security & SASE	14.0x - 22.0x	Strengthening	Hyperscaler M&A, cloud-native pull
Identity & Access (IAM)	12.0x - 16.0x	Rising	Zero-trust adoption, agent identity
Endpoint / XDR Platforms	10.0x - 15.0x	Stable	SOC consolidation, data-lake economics
DevSecOps & AppSec	9.0x - 14.0x	Rising	AI code surface expansion
Data Security / DSPM	8.0x - 13.0x	Rising	AI governance, regulatory mandates
GRC & Cyber Risk SaaS	7.0x - 12.0x	Stable	SEC and NIS2 compliance demand
Network Security (Legacy)	5.0x - 8.0x	Compressing	Platform absorption, commoditisation
Managed Security Services	3.0x - 5.0x	Stable	Services-revenue discount vs software

Source: Windsor Drake analysis of PitchBook, CB Insights and S&P Global Market Intelligence data.

Subsector dynamics driving the dispersion

Cloud security and identity have re-rated upward as hyperscalers and platform incumbents compete for category-defining assets; Google's $32B Wiz acquisition and Palo Alto Networks' $25B CyberArk deal anchor the upper bound. Endpoint and XDR multiples remain healthy on platform consolidation, with CrowdStrike trading near 22x NTM revenue on its expanding security data-lake thesis. Network security and 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. Subsector Valuation Drivers and Principal Risks, Q2 2026

Subsector	Premium Driver	Principal Risk
Cloud Security & SASE	Cloud-native architecture, hyperscaler M&A	Hyperscaler capability build-out
Identity & Access (IAM)	Zero-trust adoption, AI agent identity	Workforce IAM commoditisation
Endpoint / XDR	Platform breadth, data-lake economics	AI margin pressure on Rule of 40
DevSecOps & AppSec	AI-generated code surface expansion	Open-source competition
Data Security & DSPM	AI governance, compliance mandates	Platform absorption by hyperscalers
Managed Security	Software attach, scale consolidation	Services discount vs software peers
Network Security	Cash flow, installed-base monetisation	Commoditisation, platform displacement

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

How are cybersecurity 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 posture 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; cybersecurity leaders such as CrowdStrike clear that bar materially, trading near **22x NTM revenue**. Each ten-point gain in the score is now worth roughly an additional turn of revenue in the public cyber 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 talks about a 'Rule of 30' alternative for AI-native players. The implication for cyber founders is to track the score monthly with board-level visibility, and to demonstrate AI investment as a path to operating leverage rather than a permanent margin drag.

Table 3. Rule of 40 Performance Tiers, Cybersecurity, Q2 2026

Performance Tier	Rule of 40 Score	Avg EV/Revenue	Premium vs Median
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 cyber companies target 5:1 or better. Payback expectations have tightened, with investors looking for customer-acquisition cost recovered inside twelve months for SaaS-delivered cyber 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-product expansion engine. Top-tier public cyber companies routinely deliver these metrics; sub-scale point tools rarely do.

A credible path to profitability

For any cyber asset valued above ten times revenue, the market now expects a believable path to durable EBITDA profitability within 12 to 18 months. SentinelOne's Q1 FY26 reset, growing ARR **24% to $948M** while delivering a **20%** free cash flow margin, is the template the market now expects: 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 cybersecurity 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 cyber valuation from a mispriced one. The headline arithmetic is a roughly **+0.75x** net expansion from a 2024 baseline of about 5.5x to the Q2 2026 median of 6.25x: AI integration, platform breadth and easing rates outweigh a combined 0.9x drag from AI infrastructure cost, network commoditisation and geopolitical risk.

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

Factor	Driver	Effect on Multiples	Notable Examples
Expansion	AI integration	Premium for AI-native architecture	Cloud, identity, agent security
Expansion	Platform consolidation	Re-rating for category-defining platforms	Wiz, CyberArk, CrowdStrike
Expansion	Rate normalisation	Lower discount rates lift growth assets	Cloud, identity, DevSecOps
Expansion	Regulation tailwind	Compliance demand widens buying centre	DSPM, GRC SaaS, AI governance
Compression	AI infrastructure cost	Margin drag pressures Rule of 40	Mid-cap public cyber names
Compression	Network commoditisation	Platform absorption compresses pricing	Legacy firewalls, network sec
Compression	Geopolitical risk	Cross-border deal friction	EU, Israel, China-exposure

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

Geographic variation

Location still matters for cybersecurity valuation. North America commands a clear innovation and exit-liquidity premium, anchored by hyperscaler M&A activity and the deepest public-market liquidity in cyber. Israel remains the global cyber innovation hub on technical talent density and a deep startup pipeline, and Israeli-built IP routinely captures premium exit pricing through US strategic acquisitions. Europe 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 cyber budgets and government-driven mandates.

Table 5. Geographic Valuation Variation, Cybersecurity, Q2 2026

Region	Market Share	Posture	Key Drivers
North America	~44%	Premium	Hyperscaler M&A, deep public-market liquidity
Europe	~24%	Value	NIS2 and DORA moats; fragmentation discount
APAC	~22%	Growth	Enterprise cyber budgets, government mandates
Israel & RoW	~10%	Innovation	Technical 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 cyber multiples. The historical private premium has compressed from roughly 7x in 2023 to about 2x in 2026, and public comparables now act as a gravity anchor on late-stage private rounds for most assets. AI-native and cloud-native private companies still raise at genuine premiums of **20x to 30x revenue**, matching the highest public-market appetite, but generic late-stage private cyber 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.

Which valuation metric should apply?

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

EV/Revenue: the growth metric

EV/Revenue suits high-growth cyber assets with recurring revenue that are reinvesting ahead of profitability, including cloud security, identity, DevSecOps and AI-native 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-services revenue earned on a delivery-margin model.

EV/EBITDA: the profitability metric

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

ARR, NRR and strategic premium

For SaaS-delivered cyber 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 cyber 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 Google / Wiz and PANW / CyberArk transactions illustrate the upper bound of those premiums.

Table 6. Valuation Methodology Matrix, Cybersecurity, Q2 2026

Subsector	Primary Metric	Typical 2026 Range	Key Adjustment
AI-Native Security Platforms	EV/Revenue	20x to 30x	Category-defining premium
Cloud Security & SASE	EV/Revenue	14x to 22x	Rule of 40, AI-native posture
Identity & Access (IAM)	EV/Revenue	12x to 16x	Platform pull, zero-trust
Endpoint / XDR Platforms	EV/Revenue	10x to 15x	Data-lake economics, NRR
DevSecOps & AppSec	EV/Revenue	9x to 14x	AI code surface, dev attach
Network Security (Legacy)	EV/EBITDA	10x to 16x EBITDA	Cash flow, installed base
Managed Security Services	EV/EBITDA	12x to 18x EBITDA	Scale, software attach

Source: Windsor Drake valuation methodology, calibrated to PitchBook and CB Insights comparables.

Key takeaways for founders

Translating the market picture into strategy means concentrating on six areas that consistently move cybersecurity 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 median. Make the score a board-level priority with monthly tracking, and demonstrate that AI 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-product attach. Document the specific motion that drives that retention, and codify how the asset slots into a CISO's consolidation roadmap. Platform leaders clear **12x to 22x NTM revenue**; point 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 cyber value, not a talking point. Present specific use cases across detection, response, identity and code security, and quantify the SOC analyst productivity gains and cost-to-defend reduction with hard return-on-investment numbers. Private AI-native security platforms command roughly **20x to 30x** revenue when the AI 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, healthcare and financial services. Present audited evidence in the data room before the first buyer engagement.

5. Map specific strategic buyers

With strategics deploying an estimated **92%** of cyber M&A capital in 2025 and **$1.1T** of PE dry powder in the system, the prepared asset captures the competitive tension. Run a structured gap analysis of potential acquirers 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, 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 capability premia and stable pricing still holds is, in practice, preparing in the current cycle.

Sources

- Gartner, Forecast: Information Security End-User Spending Worldwide
- Gartner, Top Cybersecurity Trends 2026 and AI Security Forecast
- McKinsey & Company, SaaS and the Rule of 40
- 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 and Cybersecurity)
- EY, M&A Activity Insights
- S&P Global Market Intelligence, Global M&A by the Numbers: Q1 2026
- PitchBook, Q1 2026 Global M&A Report and Cybersecurity IPO Watchlist
- CB Insights, State of Cybersecurity Venture Funding

- KPMG, Venture Pulse Q4 2025
- Federal Reserve, FOMC statement and Summary of Economic Projections
- World Economic Forum, Global Cybersecurity Outlook 2026
- Alphabet Inc., Form 8-K, Wiz acquisition close (Mar 2026)
- Palo Alto Networks, Form 8-K, CyberArk acquisition close (Feb 2026)
- Netskope Inc., SEC Form S-1 / 424B and IPO pricing (Sep 2025)