AI in Cybersecurity Valuations: Q2 2026

Q2 2026 finds the application of artificial intelligence to cybersecurity in a state Windsor Drake characterises as a premium re-anchored on proof. Across the AI-in-cybersecurity niche, autonomous SOC platforms, AI security copilots, AI-native threat detection and response, AI for identity and email security, and the securing of models and large language models, the blended median has settled near **11x NTM Revenue (Windsor Drake estimate)**, roughly **1.7x** the broader cybersecurity median of about 6.5x. AI-native security commands a **30% to 50%** premium over comparable non-AI software, but that premium is now conditional on demonstrated revenue and outcomes rather than narrative.

Beneath the benchmark sits a profound and widening split. Securing AI itself, model and LLM security, clears **20x to 35x revenue**, the ceiling of the cycle, and AI SOC and security copilots clear **16x to 26x** on scarce, proven autonomy. AI-native cloud, detection and data-security platforms sit at **12x to 20x**, while legacy, non-AI security tooling compresses to **4x to 8x** as capability is absorbed by larger platforms. Capital is concentrating at the very top of the AI quality curve.

The macro backdrop is no longer the tailwind it was in 2025. The Federal Reserve funds range holds at **3.50% to 3.75%**, maintained at the April 2026 FOMC, and Goldman Sachs has shifted to expecting no further cuts in 2026, with markets pricing a June hold. Higher discount rates pressure long-duration multiples, so secular demand now carries the premium. That demand is exceptional: Gartner forecasts global information-security end-user spending at **$244.2B in 2026, up 13.3%**, projects the **AI-amplified security market rising from $49B in 2025 to $160B by 2029**, and expects over **75%** of enterprises to use AI-amplified cyber products by 2028, up from under 25%. Incumbents are responding through M&A: Google's **$32B** Wiz close, Palo Alto Networks' **$25B** CyberArk close and its roughly **$700M** Protect AI purchase confirm that platform buyers will pay record prices to own AI-native and security-for-AI capability.

This report sets out institutional-grade analysis for navigating that split market, one in which security-for-AI and autonomous SOC platforms are valued like premium infrastructure while legacy, non-AI tooling faces continued scrutiny.

What multiples are AI-in-cybersecurity companies trading at?

The Q2 2026 valuation picture turns on a single divide: demonstrated AI capability, AI-native architecture and recurring revenue quality on one side; AI-washed positioning, legacy delivery models and services-heavy economics on the other. The blended niche median clusters near **11x NTM revenue**, a roughly **1.7x** premium to the broader cyber median, but the spread between the top and bottom of the table is the widest in the sector's history. Investors are paying up for proven autonomy, security-for-AI capability and defensible training data.

Model security, autonomous SOC and AI-native detection are valued on capability and platform breadth. Legacy, signature-based tools and services-heavy 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 niche's short history. Windsor Drake calibrates these ranges against its proprietary index of **236 verified and reported transactions** spanning 2020 to 2026, refreshed each quarter and supplemented by current-quarter AI-security research.

Table 1. AI-in-Cybersecurity Valuation Multiples by Segment, Q2 2026

Segment	EV/Revenue Range	YoY Trend	Primary Driver
Model & LLM Security (AI-SPM)	20.0x - 35.0x	Rising	Scarcity, security-for-AI demand
AI SOC & Security Copilots	16.0x - 26.0x	Rising	Demonstrated autonomy, analyst leverage
AI-Native Cloud & Detection	12.0x - 20.0x	Strengthening	Hyperscaler M&A, cloud-native pull
AI Data Security & Governance	12.0x - 20.0x	Rising	AI governance, regulatory mandates
AI Identity & Agent Security	11.0x - 17.0x	Rising	Identity as the AI-agent control plane
AI Email & Social-Eng Defence	10.0x - 16.0x	Stable	GenAI phishing and deepfake threat
Legacy / Non-AI Security Tools	4.0x - 8.0x	Compressing	Platform absorption, commoditisation

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

Segment dynamics driving the dispersion

Model and LLM security has re-rated upward as incumbents compete for security-for-AI capability; Palo Alto Networks' Protect AI purchase, Cisco's Robust Intelligence acquisition and Check Point's Lakera deal anchor strategic appetite, and Gartner's observation that enterprises spend roughly 17x more on AI tools than on securing AI frames the demand gap. Autonomous SOC multiples remain healthy on demonstrated outcomes, with CrowdStrike and SentinelOne anchoring the public cohort. AI-native cloud detection re-rated after Google's $32B Wiz close. Legacy, non-AI tooling moves the other way, compressing as capability is absorbed into broader AI-security platforms.

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

Segment	Premium Driver	Principal Risk
Model & LLM Security	Scarcity, incumbent buy-side demand	Nascent revenue, fast commoditisation
AI SOC & Copilots	Proven autonomy, analyst leverage	AI infra cost, autonomy trust gap
AI-Native Cloud & Detection	Cloud-native architecture, hyperscaler M&A	Hyperscaler capability build-out
AI Data Security & DSPM	AI governance, compliance mandates	Platform absorption by hyperscalers
AI Identity & Agent Security	Agent identity control plane	Workforce IAM commoditisation
AI Email Defence	GenAI phishing and deepfake demand	Bundling by email providers
Legacy / Non-AI Tools	Cash flow, installed base	Commoditisation, AI displacement

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

How are AI-in-cybersecurity companies valued in 2026?

Valuation in 2026 has coalesced around a disciplined framework built on demonstrated AI outcomes, 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, proven autonomy and security-for-AI capability are measurable premium drivers, and platform attach economics decide where in the multiple range an asset prints.

The Rule of 40, AI-adjusted

The Rule of 40, where revenue growth plus EBITDA margin reaches at least 40%, remains the primary filter for a premium multiple. Bain finds that Rule-of-40 outperformers carry EV/Revenue multiples roughly double those of companies below the line, and achieve shareholder returns as much as 15% above the S&P 500. AI infrastructure cost is, however, pressuring the rule across the cohort. Bain notes that AI inference and model-access costs introduce real variable expense into previously high-margin software, and now discusses a 'Rule of 30' alternative for AI-native players reinvesting hard to compete. The implication for AI-security 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, AI in Cybersecurity, Q2 2026

Performance Tier	Rule of 40 Score	Avg EV/Revenue	Premium vs Median
Top Quartile (Scaled Leaders)	Above 50	17x to 35x	Substantial premium
Rule of 40 Met	40 to 50	12x to 17x	Healthy premium
Near Miss	30 to 39	8x to 11x	Modest discount
Bottom Quartile	Below 30	4x to 8x	Deep discount

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

Unit economics under scrutiny

An LTV/CAC ratio above 3:1 is now the minimum, and the strongest AI-security companies target 5:1 or better. Payback expectations have tightened, with investors looking for customer-acquisition cost recovered inside twelve months for SaaS-delivered 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 AI expansion engine. Top-tier AI-security companies routinely deliver these metrics; sub-scale point tools rarely do.

A credible path to profitability

For any AI-security asset valued above ten times revenue, the market now expects a believable path to durable EBITDA profitability, especially given higher-for-longer rates. SentinelOne, approaching $1B ARR with about a 20% free cash flow margin on company reporting, illustrates the template the market rewards: high growth combined with demonstrable cash discipline. CrowdStrike, reporting FY26 ARR of $5.25B up 24% with record net-new ARR, shows the same at greater scale. There is little tolerance for perpetual growth narratives that never demonstrate operating leverage, particularly where AI infrastructure cost is pressuring the margin profile of the entire cohort.

What is driving AI-in-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 AI-security valuation from a mispriced one. The headline arithmetic is a roughly **+2.5x** net expansion from a 2024 baseline of about 8.5x to the Q2 2026 niche median of 11x: AI capability premia, platform consolidation and AI-governance demand outweigh a combined 1.5x drag from higher-for-longer rates, AI infrastructure cost and point-tool commoditisation.

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

Factor	Driver	Effect on Multiples	Notable Examples
Expansion	AI capability premium	Premium for proven AI outcomes	Model security, autonomous SOC
Expansion	Platform consolidation	Re-rating for category-definers	Wiz, CyberArk, Protect AI
Expansion	AI governance mandates	Compliance demand widens buying centre	DSPM, TRiSM, AI Act
Compression	Higher-for-longer rates	Lifts discount rate on long-duration assets	All high-growth software
Compression	AI infrastructure cost	Margin drag pressures Rule of 40	AI-native players reinvesting
Compression	Point-tool commoditisation	Platform absorption compresses pricing	Legacy, single-feature tools

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

Geographic variation

Location still matters for AI-security valuation. North America commands a clear innovation and exit-liquidity premium, anchored by hyperscaler and platform M&A and the deepest public-market liquidity in cyber. Israel remains the global AI-security innovation hub on technical talent density and a deep startup pipeline, and Israeli-built AI IP routinely captures premium exit pricing through US strategic acquisitions. Europe trades at a fragmentation discount but offers regulatory moats from the EU AI Act, 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	AI Act, NIS2 and DORA moats; fragmentation discount
APAC	~22%	Growth	Enterprise cyber budgets, government mandates
Israel & RoW	~10%	Innovation	AI 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 AI-security multiples. The historical private premium has compressed from roughly 7x in 2023 to about 3x in 2026, and

public comparables now act as a gravity anchor on late-stage rounds for most assets. AI-native model-security and autonomous-SOC companies still raise at genuine premiums of **20x to 35x revenue**, matching the highest public-market appetite, but generic late-stage private companies without a clear AI-native architecture are seeing flatter marks. Those companies are increasingly prime candidates for strategic M&A or a PE take-private outcome. Cyera's progression, raising at a $6B valuation in 2025 and rising toward $9B since, shows that the genuine AI-native tail still reprices upward.

Which valuation metric should apply?

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

EV/Revenue: the growth metric

EV/Revenue suits high-growth, AI-native assets with recurring revenue that are reinvesting ahead of profitability, including model security, AI SOC, AI-native detection and identity platforms. The essential adjustment is for gross margin and quality of AI: a dollar of software revenue at an 80%-plus margin with proven autonomy is not comparable to a dollar of services revenue or AI-washed positioning.

EV/EBITDA: the profitability metric

EV/EBITDA fits mature, slower-growth or services-heavy cyber businesses where cash flow is the primary value driver. Many companies once valued on revenue are now assessed on EBITDA as their growth rates moderate; for these operators, **EBITDA multiples of 12x to 22x** are the relevant range, with margin expansion and operating leverage the key value drivers.

ARR, NRR and strategic premium

For SaaS-delivered AI-security 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 AI-security 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 Palo Alto Networks / CyberArk transactions illustrate the upper bound of those premiums.

Table 6. Valuation Methodology Matrix, AI in Cybersecurity, Q2 2026

Segment	Primary Metric	Typical 2026 Range	Key Adjustment
Model & LLM Security (AI-SPM)	EV/Revenue	20x to 35x	Scarcity, capability premium
AI SOC & Security Copilots	EV/Revenue	16x to 26x	Proven autonomy, Rule of 40
AI-Native Cloud & Detection	EV/Revenue	12x to 20x	Cloud-native posture, data-lake
AI Data Security & Governance	EV/Revenue	12x to 20x	AI governance, compliance demand
AI Identity & Agent Security	EV/Revenue	11x to 17x	Agent identity, platform pull
AI Email & Social-Eng Defence	EV/Revenue	10x to 16x	Behavioural data moat, NRR
Legacy / Non-AI Tools	EV/EBITDA	12x to 22x EBITDA	Cash flow, installed base

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 AI-security valuation in the current environment.

1. Clear the Rule of 40, AI-adjusted

Revenue growth plus EBITDA margin must reach at least 40%. No single metric predicts a valuation premium better, and Bain finds outperformers carry roughly double the multiple of companies below the line. Make the score a board-level priority with monthly tracking, and demonstrate that AI infrastructure investment is a path to durable operating leverage rather than a permanent margin drag.

2. Prove autonomy and AI outcomes with data

AI is now a measurable driver of value, not a talking point. Instrument and publish the metrics buyers diligence: investigations handled end to end, false-positive reduction, mean-time-to-respond improvement and customer cost-to-defend reduction. Private AI-native security platforms command **16x to 35x** revenue when the AI case is real and quantified.

3. Build for platform attach, not point sale

Target net revenue retention above **115% to 120%** through multi-product AI attach. Document the specific motion that drives that retention, and codify how the asset slots into a CISO's AI-security consolidation roadmap. Platform leaders clear the top of the range; point tools sit far lower, and the gap is widening as platforms absorb capability through M&A.

4. Own the security-for-AI surface

Securing the enterprise's own AI, models, LLMs, pipelines and autonomous agents, is the fastest-emerging premium category. Gartner notes enterprises spend roughly 17x more on AI tools than on securing AI, and Protect AI, Robust Intelligence and Lakera show incumbents paying up to close that gap. Defensible IP in model detection, posture and runtime guardrails commands the cycle's richest multiples.

5. Map specific strategic buyers

With strategics setting the AI-security ceiling and about **$1.3T** 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 AI-security deficits before engaging the market.

6. Prepare in 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 and elevated AI-capability premia still holds is, in practice, preparing in the current cycle.

Sources

- Gartner, Forecast: Information Security and Risk Management, Worldwide; AI-amplified security
- Gartner, Worldwide AI Spending Forecast 2026 and Top Cybersecurity Trends 2026
- McKinsey & Company, Global Private Markets Report 2026 and software value creation
- Bain & Company, Hacking Software's Rule of 40 and AI Brings Headwinds and Tailwinds to the Rule of 40
- Bain & Company, Global Private Equity Report 2026
- PwC, Global M&A Industry Trends: 2026 Outlook (TMT)
- EY, M&A Activity Insights and 2026 Outlook
- S&P Global Market Intelligence, Global M&A by the Numbers: Q1 2026
- PitchBook, Q1 2026 Global M&A Report; AI and cybersecurity coverage
- CB Insights, State of AI and Cybersecurity Venture Funding
- KPMG, Venture Pulse Q4 2025
- Goldman Sachs, US rates outlook 2026
- Federal Reserve, FOMC statement (Apr 2026) and Summary of Economic Projections
- World Economic Forum, Global Cybersecurity Outlook 2026
- Alphabet Inc., SEC filings, Wiz acquisition close (Mar 2026)
- Palo Alto Networks, SEC filings and press, CyberArk close and Protect AI / Prisma AIRS
- Netskope Inc. and SailPoint, SEC Form S-1 / 424B and IPO pricing (2025)