Cloud Security (CSPM/CWPP) Valuations: Q2 2026

Q2 2026 finds cloud security in a state Windsor Drake characterises as a structural premium: an enduring valuation premium underwritten by secular cloud migration rather than cyclical exuberance. Cloud security is the fastest-growing cyber subsegment, expanding **28.8%** in 2026 against a sector growing 13.3% (Gartner), and Windsor Drake's working benchmark for scaled cloud security platforms sits near **14x NTM revenue**. That combination of growth and a stable benchmark, more than any single number, is the story of the quarter.

Beneath the benchmark sits a profound and widening split. Headline ranges mask a divide between AI-native platforms and legacy point tools. AI-native cloud-native application protection platform (CNAPP) leaders trade at **20x to 32x revenue** in private rounds, broad CNAPP platforms at **14x to 22x**, and legacy point cloud tools at **6x to 10x** as their capability is absorbed into larger platforms. Capital is concentrating at the top of the quality curve as standalone CSPM and CWPP tools consolidate into unified CNAPP buying decisions.

The macro backdrop is a cautious tailwind. The Federal Reserve funds range holds at **3.50% to 3.75%** after the April 2026 FOMC, with the March dot plot signalling one further cut in 2026, though the committee is divided and April 2026 CPI rose 3.8% year on year, the highest since 2023. Demand fundamentals are exceptionally strong: Gartner sizes cloud security posture management (CSPM) at **$4.7B in 2025**, reaching **$16.2B by 2030**, and the combined cloud security market at **$32.4B by 2029**. 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 CNAPP, posture and identity platforms are valued like premium cloud infrastructure while legacy point tools face continued scrutiny.

What multiples are cloud security companies trading at?

The Q2 2026 valuation picture turns on a single divide: AI-native architecture, CNAPP platform breadth and recurring revenue quality on one side; legacy point-tool architecture and standalone delivery on the other. Scaled cloud security platforms cluster near Windsor Drake's **14x NTM revenue** benchmark, with public cloud-software proxies trading **11x to 19x**, but the spread between the top and bottom of the table is the widest in the niche's history. Investors are paying up for agentless, identity-aware platforms, AI-driven detection, and durable multi-module attach economics.

CNAPP, CSPM and AI-native platforms are valued on architecture and platform breadth. Legacy point tools, 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 history.

Table 1. Cloud Security Valuation Multiples by Niche, Q2 2026

Niche	EV/Revenue Range	YoY Trend	Primary Driver
AI-Native CNAPP	20.0x - 32.0x	Rising	Category-defining cloud-native architecture
Broad CNAPP Platforms	14.0x - 22.0x	Strengthening	Hyperscaler M&A, platform breadth
CSPM (Posture)	12.0x - 18.0x	Rising	Fastest-growing security category
DSPM / Cloud Data Security	10.0x - 16.0x	Rising	AI governance, regulatory mandates
CIEM / Cloud Identity	10.0x - 15.0x	Rising	Identity as the cloud perimeter
CWPP (Workload)	10.0x - 15.0x	Strengthening	Runtime-first detection
Container & Kubernetes Security	9.0x - 14.0x	Stable	Cloud-native adoption, supply chain
Legacy Cloud Tools	6.0x - 10.0x	Compressing	Platform absorption, commoditisation

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

Niche dynamics driving the dispersion

CNAPP and CSPM have re-rated upward as hyperscalers and platform incumbents compete for category-defining assets; Google's $32B Wiz acquisition anchors the upper bound, and the cloud-adjacent Palo Alto Networks acquisition of CyberArk for $25B repriced cloud identity. CIEM, CWPP and DSPM multiples remain healthy on platform consolidation and AI-governance demand, while container security increasingly prices as a CNAPP module rather than a standalone category. Legacy point tools move the other way, compressing as capability is absorbed into broader platforms and valued against a software premium they cannot match.

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

Niche	Premium Driver	Principal Risk
AI-Native CNAPP	Agentless, identity-aware architecture	Hyperscaler capability build-out
CSPM	Fastest-growing category, posture wedge	Commoditisation into CNAPP suites
CWPP	Runtime-first detection context	Agent overhead, open-source competition
Container & Kubernetes	Cloud-native adoption, supply chain	Absorption into CNAPP platforms
CIEM	Identity as the cloud perimeter	Workforce IGA commoditisation
DSPM	AI governance and compliance mandates	Hyperscaler platform absorption
Legacy Cloud Tools	Installed-base cash flow	Commoditisation, platform displacement

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

How are cloud 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 CNAPP 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 multi-module 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 each ten-point improvement in the score added about **1.1x EV/Revenue** in Q4 2025, up from 0.8x a year earlier; cloud security leaders that clear the bar materially command the premium tier. The metric has become a stronger valuation driver as operational efficiency, not raw growth, separates winners.

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 cloud 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, Cloud Security, Q2 2026

Performance Tier	Rule of 40 Score	Avg EV/Revenue	Premium vs Median
Top Quartile (AI-Native Leaders)	Above 50	18x to 32x and above	+50% to +100%
Rule of 40 Met	40 to 50	12x to 18x	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 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 cloud security companies target 5:1 or better. Payback expectations have tightened, with investors looking for customer-acquisition cost recovered inside twelve months. For CNAPP 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 CSPM, CWPP, CIEM and DSPM. Top-tier platforms routinely deliver these metrics; sub-scale point tools rarely do.

A credible path to profitability

For any cloud security asset valued above fourteen times revenue, the market now expects a believable path to durable EBITDA profitability within 12 to 18 months. Public proxies set the template: Palo Alto Networks delivered a **37.6%** free cash flow margin in fiscal 2025 while growing next-generation security ARR **33% to $6.33B**, and CrowdStrike posted record net-new ARR alongside FY26 revenue of $4.81B. There is little tolerance for perpetual growth narratives that never demonstrate operating leverage, especially where AI infrastructure cost is pressuring the margin profile of the entire cohort.

What is driving cloud 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 cloud security valuation from a mispriced one. The headline arithmetic is a roughly **+2.0x** net expansion from a 2024 baseline of about 12x to the Q2 2026 benchmark of 14x: AI-native demand, hyperscaler M&A, CNAPP consolidation and easing rates outweigh a combined 1.0x drag from AI infrastructure cost, point-tool compression and macro risk.

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

Factor	Driver	Effect on Multiples	Notable Examples
Expansion	AI-native demand	Premium for agentless, AI architecture	Wiz, Upwind, runtime CWPP
Expansion	Hyperscaler M&A	Re-rating for category-defining platforms	Google / Wiz, Prisma Cloud
Expansion	CNAPP consolidation	Multi-module attach lifts platform value	CSPM plus CWPP plus CIEM plus DSPM
Expansion	Rate normalisation	Lower discount rates lift growth assets	Cloud-native platforms
Compression	AI infrastructure cost	Margin drag pressures Rule of 40	Mid-cap cloud security names
Compression	Point-tool compression	Platform absorption compresses pricing	Standalone CSPM, legacy tools
Compression	Geopolitical and rate risk	Cross-border deal friction	Israel, EU-exposure

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

Geographic variation

Location still matters for cloud security 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 is the global cloud security innovation hub: Wiz, Orca Security, Aqua Security, Upwind and Sysdig all carry Israeli roots, and the Wiz exit is the largest Israeli technology exit on record. Europe trades at a fragmentation discount but offers regulatory moats from NIS2 and DORA, while APAC continues to expand on growing enterprise cloud budgets.

Table 5. Geographic Variation, Cloud Security, Q2 2026

Region	Share of Activity	Posture	Key Drivers
North America	~50%	Premium	Hyperscaler M&A, deep public-market liquidity
Israel	~22%	Innovation	CNAPP pipeline, premium US strategic exits
Europe	~16%	Value	NIS2 and DORA moats; fragmentation discount
APAC & RoW	~12%	Growth	Expanding enterprise cloud security budgets

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

Public and private markets converge selectively

One of the defining features of the quarter is the selective convergence of public and private cloud security multiples. Generic private cloud tools have converged on public marks near the mid-teens, but AI-native CNAPP rounds reprice upward on hypergrowth, sustaining a premium of roughly 10x for the very best assets. Wiz approached a $1B annual recurring revenue run-rate before its sale, and Upwind raised at a $1.5B valuation on 900% revenue growth. Generic late-stage private companies without a clear AI-native architecture are seeing flat marks, and are increasingly prime candidates for strategic M&A or a PE take-private.

Which valuation metric should apply?

Selecting the right metric is what separates a professional cloud 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 or capability-heavy bolt-on assets.

EV/Revenue: the growth metric

EV/Revenue suits high-growth cloud security assets with recurring revenue that are reinvesting ahead of profitability, including CNAPP, CSPM, CWPP, CIEM and DSPM 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 services revenue earned on a delivery-margin model.

EV/EBITDA: the profitability metric

EV/EBITDA fits mature, slower-growth cloud security businesses where cash flow is the primary value driver, such as PE-owned mid-market software and services-heavy operators. It remains rare in cloud security, where most leaders are valued on revenue, but it becomes relevant as growth moderates and a buyer underwrites cash generation rather than expansion.

ARR, NRR and strategic premium

For SaaS-delivered cloud 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 cloud security processes, typically **25% to 30%**, are applied on top of underlying revenue multiples where platform and capability synergies can be concretely underwritten; the Google / Wiz transaction illustrates the upper bound of those premiums, clearing roughly 32x forward to 43x trailing ARR.

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

Niche	Primary Metric	Typical 2026 Range	Key Adjustment
AI-Native CNAPP	EV/Revenue	20x to 32x	Category-defining premium
Broad CNAPP Platforms	EV/Revenue	14x to 22x	Rule of 40, AI-native posture
CSPM (Posture)	EV/Revenue	12x to 18x	Category growth, attach motion
CIEM / Cloud Identity	EV/Revenue	10x to 15x	Platform pull, agent identity
CWPP (Workload)	EV/Revenue	10x to 15x	Runtime context, retention
Container & Kubernetes	EV/Revenue	9x to 14x	CNAPP module convergence
Mature / PE-Owned Cloud Sec	EV/EBITDA	12x to 22x EBITDA	Cash flow, scale

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 cloud 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; Bain finds each ten-point gain added about 1.1x EV/Revenue in Q4 2025. 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 the CNAPP platform, not the point tool

Standalone CSPM and CWPP are being absorbed. Target net revenue retention above **115% to 120%** through multi-module attach across posture, workload, identity and data, and codify how the asset slots into a cloud-platform consolidation roadmap. CNAPP platform leaders clear **14x to 22x 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 cloud security value, not a talking point. Present specific use cases across posture, runtime detection, entitlement and data security, and quantify the analyst productivity gains and false-positive reduction with hard return-on-investment numbers. Private AI-native CNAPP platforms command roughly **20x to 32x** 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 **$1.3T** of PE dry powder in the system, the prepared asset captures the competitive tension. Run a structured gap analysis of potential acquirers, hyperscalers and platform incumbents alike, and map your capabilities directly to each buyer's declared cloud security 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 hyperscaler demand, AI-native premia and stable pricing still holds is, in practice, preparing in the current cycle.

Sources

- Gartner, Forecast: Information Security End-User Spending Worldwide
- Gartner, Forecast Analysis: Cloud Security (CSPM, CWPP, CASB), Worldwide
- Gartner, Top Cybersecurity Trends 2026 and Cloud Security Forecast
- McKinsey & Company, Global Private Markets Report 2026
- Bain & Company, 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
- S&P Global Market Intelligence, Global M&A by the Numbers: Q1 2026
- PitchBook, Q1 2026 Global M&A Report and cloud security comparables
- CB Insights, State of Cybersecurity Venture Funding
- Crunchbase, Cybersecurity Startup Investment 2025
- KPMG, Venture Pulse Q4 2025
- Federal Reserve, FOMC statement and Summary of Economic Projections
- U.S. Bureau of Labor Statistics, Consumer Price Index Summary
- Alphabet Inc., Form 8-K, Wiz acquisition close (Mar 2026)

- Netskope Inc., SEC Form S-1 / 424B and IPO pricing (Sep 2025)
- World Economic Forum, Global Cybersecurity Outlook 2026