

WINDSOR DRAKE

# AI in Cybersecurity Valuations: Q2 2026

JUNE 2026

Windsor Drake · Market Intelligence

## AI as the Valuation Engine

Across the AI-in-cybersecurity niche the blended median has settled near **11x NTM Revenue (WD estimate)**, roughly **1.7x** the broader cyber median of about 6.5x.

- AI-native security assets command a **30% to 50%** premium over comparable non-AI software (market reporting).
- The premium is now conditional on demonstrated revenue and outcomes, not narrative.
- Acquirers reward measurable analyst productivity and cost-to-defend reduction.
- Quality of AI, not the AI label, decides where in the range an asset prints.

## Demand Fundamentals

Security spending re-accelerated, and the AI line items grow fastest of all.

- Global information-security end-user spend reaches **\$244.2B in 2026**, up **13.3%** (Gartner).
- The **AI-amplified security market** grows from **\$49B (2025) to \$160B (2029)** (Gartner).
- Over **75%** of enterprises will use AI-amplified cyber products by 2028, up from under 25% (Gartner).
- **Cloud security** is the fastest-growing subsegment at **28.8%** in 2026 (Gartner).

Sources: Gartner; Bain & Company; Federal Reserve; Windsor Drake analysis. See appendix.

## The Capability Bifurcation

Headline averages mask a profound split between AI-native platforms and legacy tooling.

- **Model and LLM security** clears **20x to 35x**, the ceiling of the cycle.
- **AI SOC and security copilots** clear **16x to 26x** on scarce, proven autonomy.
- **AI-native cloud, detection and data security** sit at **12x to 20x**.
- **Legacy, non-AI security tools** compress to **4x to 8x** as capability is absorbed.

## Macro Backdrop: Rates Higher for Longer

Monetary policy is no longer the tailwind it was in 2025, so secular demand carries the premium.

- The Fed funds range holds at **3.50% to 3.75%**, maintained at the April 2026 FOMC (Federal Reserve).
- Goldman Sachs has shifted to expecting **no further 2026 cuts**, with markets pricing a June hold.
- Higher discount rates pressure long-duration multiples, sharpening the focus on profitable growth.
- Board-level cyber mandates and AI risk keep the demand base structurally defensive.

## Incumbents Buy AI Defence

Platform incumbents are decisively buying, rather than building, their AI security layers.

- **Google / Wiz** (\$32B) closed **March 2026**, the largest pure-play cyber deal on record.
- **Palo Alto Networks / CyberArk** (\$25B) closed **February 2026**, identity for the AI-agent era.
- **Palo Alto Networks / Protect AI** (about \$700M) anchors the new Prisma AIRS AI-security platform.
- **Cisco / Robust Intelligence** and **Check Point / Lakera** extend the model-security land grab.

## Private AI-Native Premium

Private rounds for AI-native security continue to clear public marks decisively.

- **Cyera** (AI data security) raised at a **\$6B** valuation in mid-2025, rising toward **\$9B** since.
- **Abnormal Security** (AI email defence) reached a **\$5.1B** valuation on its Series D.
- **Prophet Security** raised **\$30M** for fully autonomous SOC investigation (Accel, Bain Capital Ventures).
- Capital concentrates at the top of the AI quality curve as buyer demand outpaces supply.

Sources: S&P Global Market Intelligence; CB Insights; Bain & Company; SEC filings. See appendix.

## Strategic Buyers Dominate

Hyperscalers and platform incumbents now define the upper bound of AI-security pricing.

- The market has split into three camps: **autonomous SOC, assisted copilot and platform consolidation**.
- **Autonomous SOC:** CrowdStrike and SentinelOne; **copilot:** Microsoft and Fortinet.
- **Consolidation:** Palo Alto Networks and Zscaler assemble end-to-end AI security platforms.
- Capability bolt-ons under \$1B dominate by volume; mega-deals set the ceiling.

## IPO Window & Private Capital

The listing window reopened selectively, and PE capital remains abundant but disciplined.

- **Netskope** listed on Nasdaq in **September 2025**, raising **\$908M** at a \$7.3B valuation (SEC filings).
- **SailPoint** re-listed in **February 2025**, raising **\$1.38B** at a \$12.8B valuation.
- Global PE dry powder of about **\$1.3T** keeps pressure on platform asset prices (Bain).
- Bain notes tech deal value fell about **70%** from Q4 2025 to Q1 2026 on valuation uncertainty.

## 1. Rule of 40, AI-Adjusted

Revenue Growth % plus EBITDA Margin % at or above 40% remains the baseline for a premium multiple, but AI inference cost is reshaping the math (Bain).

- Bain finds Rule-of-40 outperformers carry roughly **double** the EV/Revenue of those below the line.
- Frame AI infrastructure spend as a path to operating leverage, not a permanent margin drag.

## 2. AI-Native Architecture

AI-native design decouples detection and response from analyst headcount, and the market pays for it.

- AI-native security commands a **30% to 50%** premium over comparable non-AI software.
- Show non-linear margin expansion as the customer base scales, not pilots.

## 3. Prove Autonomy with Outcomes

For AI SOC and copilots, buyers now price demonstrated autonomy, not roadmaps.

- Quantify investigations handled, false-positive reduction and mean-time-to-respond gains.
- Top autonomous-SOC assets clear **16x to 26x**; assisted tooling sits lower.

## 4. Model & Agent Security Is the New Surface

Securing AI itself, models, LLMs and autonomous agents, is the fastest-emerging premium category.

- Enterprises spend roughly **17x more on AI tools than on securing AI** (Gartner), a clear demand gap.
- Protect AI, Robust Intelligence and Lakera show incumbents paying up for security-for-AI capability.

## 5. Public Market Discipline

Private marks are converging with public benchmarks, so pricing discipline applies even to private rounds.

- The public-to-private spread has narrowed materially since 2023 (PitchBook; CB Insights).
- Justify any private premium with growth, retention and a genuine AI-native posture.

## 6. Buyer-Readiness Discipline

With about **\$1.3T** of dry powder and strategics setting the AI-security ceiling, the prepared asset captures competitive tension.

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

# Founder FAQs: Valuations, Timing & Strategy

WINDSOR DRAKE

The questions AI-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 platforms in SOC automation, detection, identity and model security, **EV/EBITDA** for mature or services-heavy operators, and a recurring-revenue lens (NRR, NDR, ARR growth) for any SaaS-delivered AI-security asset. Always reference the correct AI-in-cyber cohort, never the broad cyber average.

## Q3 Why does the Rule of 40 still matter for AI security?

It remains the single best predictor of a premium multiple. Bain finds Rule-of-40 outperformers carry roughly double the EV/Revenue of companies below the line. AI inference cost is pressuring the rule, so Bain now discusses a 'Rule of 30' for AI-native players reinvesting hard; the market rewards a credible path back to operating leverage.

## Q5 When is the optimal time to run a process?

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

## Q7 Is the IPO window a viable alternative to M&A?

It has reopened but remains selective. **Netskope** (September 2025, \$908M raised, \$7.3B valuation) and **SailPoint** (February 2025, \$1.38B raised) reset expectations. The window favours scaled, profitable assets with a credible AI-native narrative and a clear path to durable profitability.

## Q2 What are the key segment ranges right now?

Model and LLM security (AI-SPM) leads at **20x to 35x NTM revenue**; AI SOC and security copilots at **16x to 26x**; AI-native cloud and detection at **12x to 20x**; AI data security and governance at **12x to 20x**; AI identity and agent security at **11x to 17x**; AI email defence at **10x to 16x**; legacy non-AI tools at **4x to 8x**.

## Q4 How do public and private valuations compare?

The historical private premium has compressed as public comparables anchor late-stage rounds. Genuine AI-native private companies still raise at clear premiums (Cyera near a \$6B valuation in 2025, rising since), but generic late-stage assets without a real AI-native architecture see flatter marks and become prime strategic or PE targets.

## Q6 Who are the most active buyers today?

**Hyperscalers** (Google, Microsoft) and **platform incumbents** (Palo Alto Networks, CrowdStrike, Cisco, Check Point) drove the defining deals of 2025 to 2026. **PE platforms** with about \$1.3T of dry powder pursue mid-market roll-ups, and corporate venture arms seed the model-security frontier.

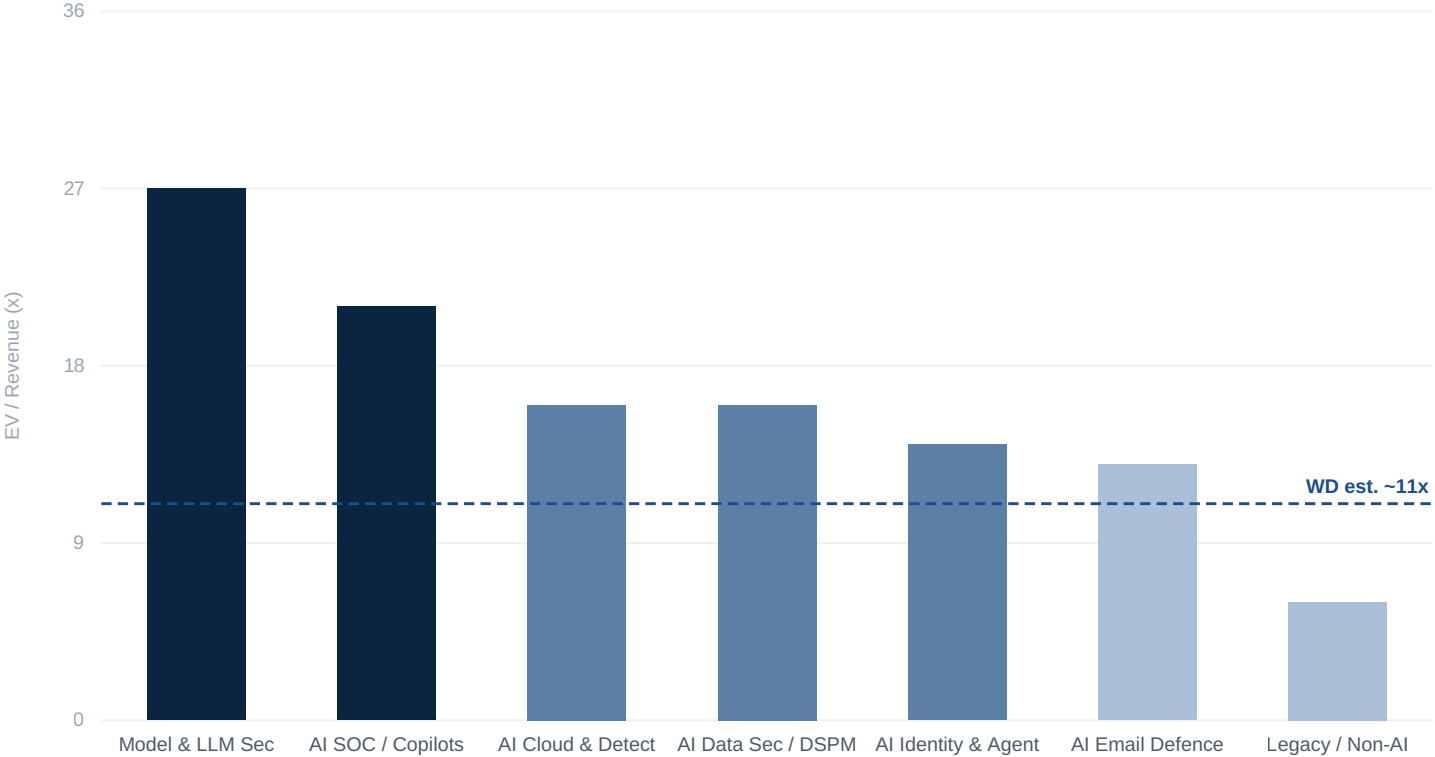
## Q8 How do we maximise our multiple, and should we expect earn-outs?

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

# Q2 2026 Valuation Landscape Overview

Premium multiples cluster in model security and autonomous SOC; legacy, non-AI tooling stays compressed.

Median EV / Revenue Multiple by AI-Security Segment (x)



NICHE MEDIAN BENCHMARK

**~11x**

WD estimate for the AI-in-cyber blended median, roughly 1.7x the broader cyber median of about 6.5x.

AI-NATIVE PREMIUM

**+30% to 50%**

Premium that AI-native security commands over comparable non-AI software (market reporting).

AI-AMPLIFIED SECURITY, 2026

**Fast-growth**

Gartner sees the AI-amplified security market rising from \$49B in 2025 to \$160B by 2029.

**Key Driver**

Disciplined exuberance has replaced 2021 enthusiasm: acquirers reward demonstrated AI outcomes, autonomy and AI-native architecture, not the AI label or topline growth alone.

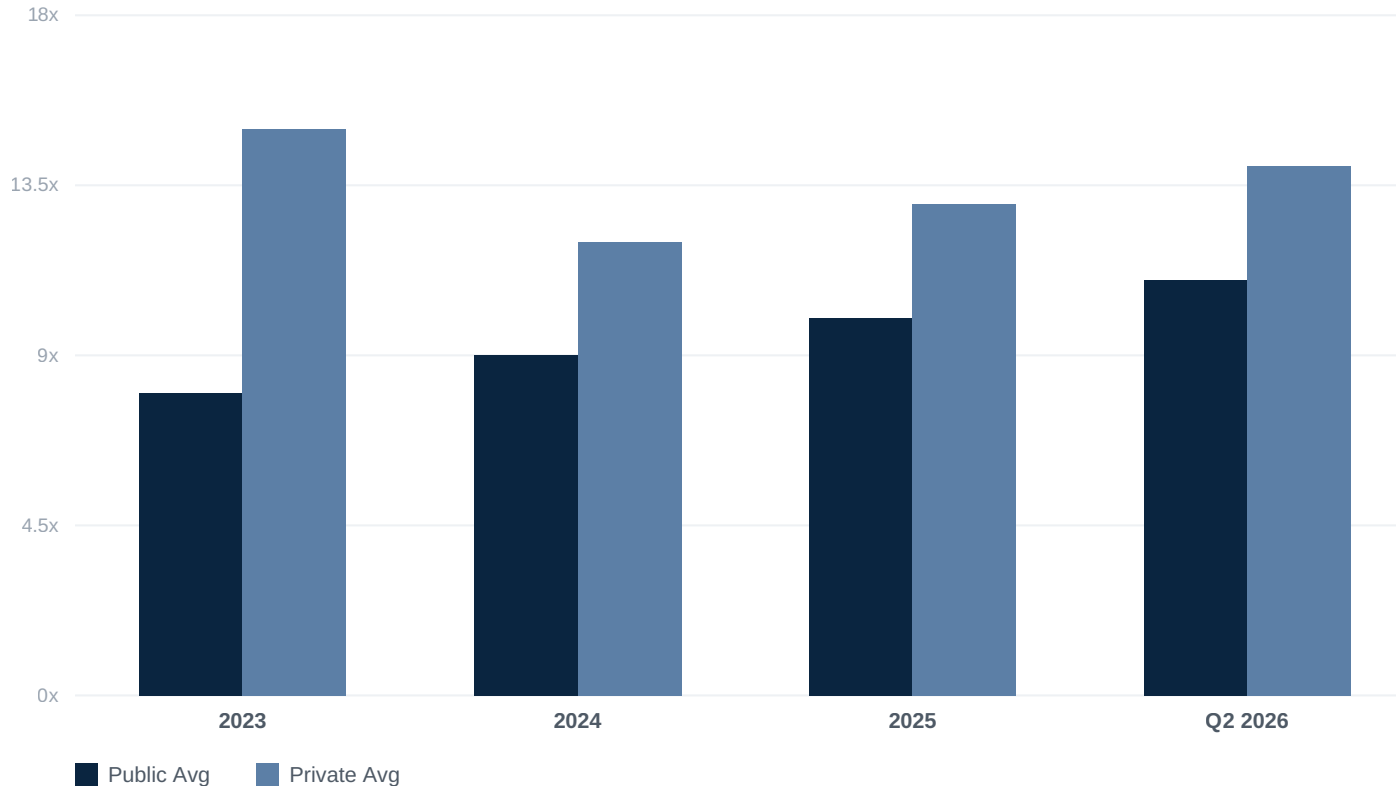
**AI-native bifurcation:** the gap between security-for-AI and autonomous SOC platforms (16x to 35x) and legacy, non-AI tooling (4x to 8x) is the defining feature of the niche, driven by proven autonomy, AI-native architecture and the scarcity of genuine AI talent.

Sources: PitchBook; CB Insights; S&P Global Market Intelligence; Windsor Drake analysis. See appendix.

# Public vs Private Market Convergence

The private premium has compressed as public comparables anchor late-stage rounds, but AI-native rounds still reprice the top of the cohort.

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



## PUBLIC / PRIVATE SPREAD

**~3.0x**

Down from about 7x in 2023, as public comparables anchor late-stage pricing (PitchBook; CB Insights).

## QUALITY PRIVATE TAIL

**20x to 35x**

AI-native model security and autonomous SOC rounds clear public marks decisively.

## PUBLIC BENCHMARK ANCHOR

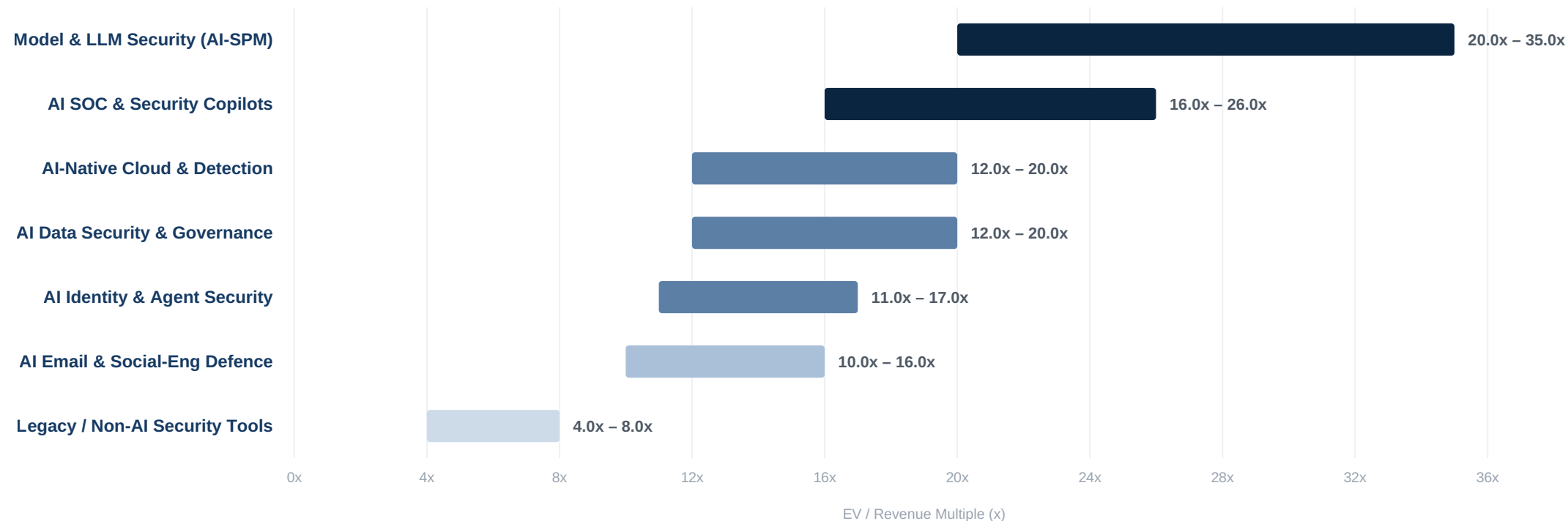
**~11x**

Public AI-security comparables now cap late-stage private pricing for non-AI-native assets.

**Selective convergence:** the public-to-private spread narrowed from about 7x in 2023 to about 3x in 2026, but AI-native model-security and autonomous-SOC rounds still print far above the mean, repricing the very top of the private cohort.

# Exit Valuation Multiples by AI-Security Segment

A sharp bifurcation persists between security-for-AI and autonomous SOC (16x to 35x) and legacy, non-AI tooling (4x to 8x).



## KEY OBSERVATION

The market is paying for proven AI capability and AI-native architecture, not category labels. The multiple-point gap between security-for-AI assets and legacy tooling reflects the structural shift from human-scaled, signature-based defence to autonomous, model-driven security.

# Valuation Multiple Drivers: Expansion vs. Compression

Net expansion to roughly 11x is driven by AI capability premia, platform consolidation and governance demand, partly offset by higher rates and AI infrastructure cost.



## NET EXPANSION OF +2.5X

AI capability premia, platform breadth and AI-governance demand outweigh a combined 1.5x drag from higher-for-longer rates, AI infrastructure cost and point-tool commoditisation. The bridge reflects Windsor Drake analysis of the cited institutional data.

# Capital Markets: IPO Window & Listing Benchmarks

WINDSOR DRAKE

The 2024 to 2025 listing class reopened the window selectively; scale, profitability and AI posture now gate access.

## Netskope (Nasdaq)

Listed September 2025 at **\$19 per share**, raising **\$908M** at a **\$7.3B** valuation (SEC filings).

- Sold 47.8 million shares; the largest cybersecurity IPO of 2025.
- Confirmed that SASE and AI-driven cloud security command public-market appetite.
- Reopened the cyber listing window alongside Circle, Figma and CoreWeave.
- Set the bar for scaled, AI-positioned platforms targeting a listing.

## SailPoint (Nasdaq)

Re-listed February 2025, raising **\$1.38B** at a **\$12.8B** valuation.

- Thoma Bravo-backed identity-security leader returning to public markets.
- Established AI-augmented identity governance as a public-market category.
- Demonstrated PE appetite to crystallise value via the listing route.
- Provided a fresh public comp for identity and agent-security assets.

## Rubrik & the 2024 Class

The 2024 listings proved enterprise appetite for AI-driven cyber resilience.

- Rubrik (NYSE, April 2024) anchored cyber-resilience and data security as a category.
- Reopened the broader cyber IPO pipeline after the 2022 to 2023 freeze.
- Confirmed appetite for ransomware-recovery and data-security infrastructure.
- Public investors now price AI-native architecture into IPO valuations.

## CrowdStrike & SentinelOne (Public Marks)

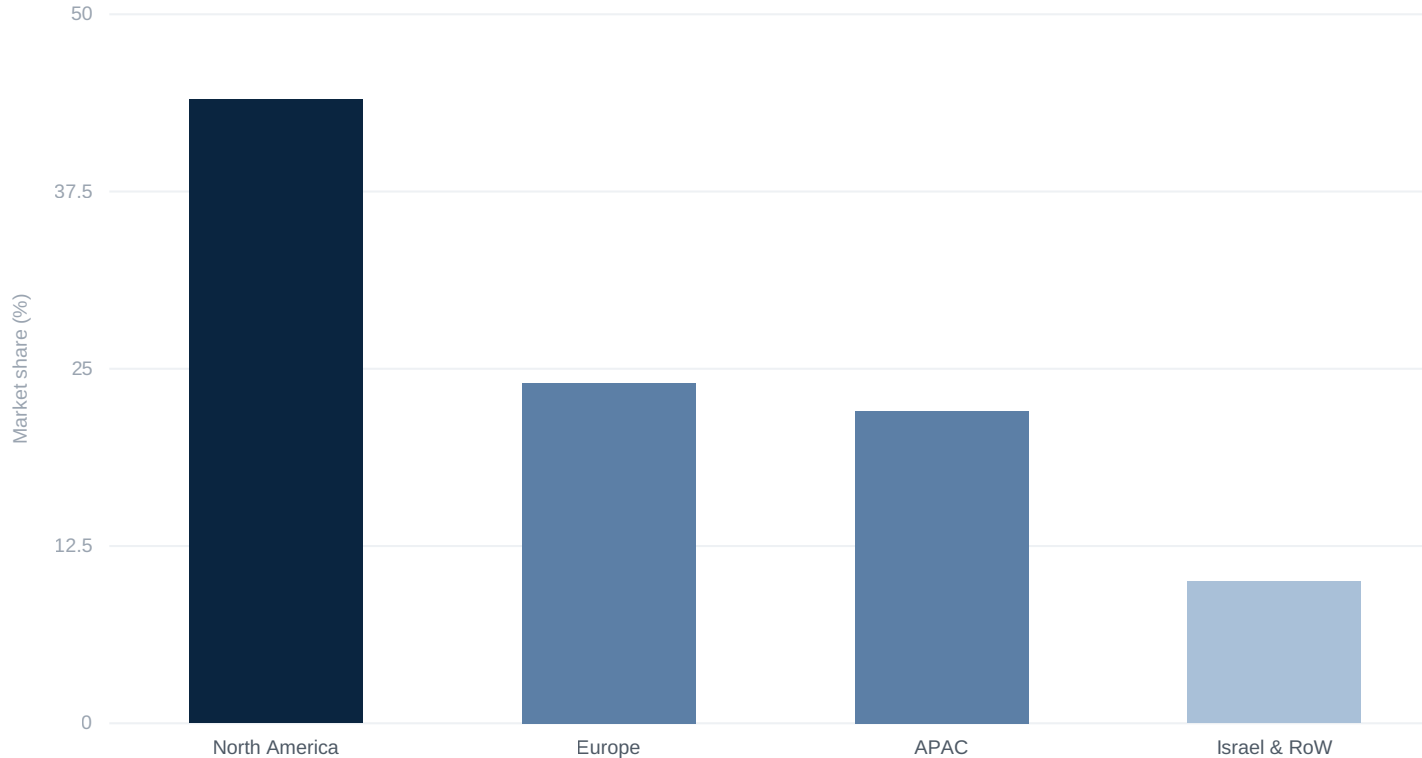
The scaled AI-SOC leaders set fresh marks via public trading and product cadence.

- **CrowdStrike** reported **FY26 ARR of \$5.25B (+24%)** with record net-new ARR (company reporting).
- Charlotte AI agentic analyst and AgentWorks anchor its autonomous SOC narrative.
- **SentinelOne** approaches \$1B ARR with about a 20% free cash flow margin (company reporting).
- The choice is now between listing for liquidity and selling for a strategic premium.

# Geographic Valuation Variations

North America commands an AI-security premium; Israel is the innovation engine; Europe offers regulatory-moat value.

Share of Global Cybersecurity Market by Region (%)



## NORTH AMERICA

### Premium

About 44% of the global cyber market, deepest exit liquidity and hyperscaler-driven AI-security pricing.

## EUROPE

### Discount

About 24% share; AI Act, NIS2 and DORA moats, offset by market fragmentation.

## ISRAEL & APAC

### Innovation

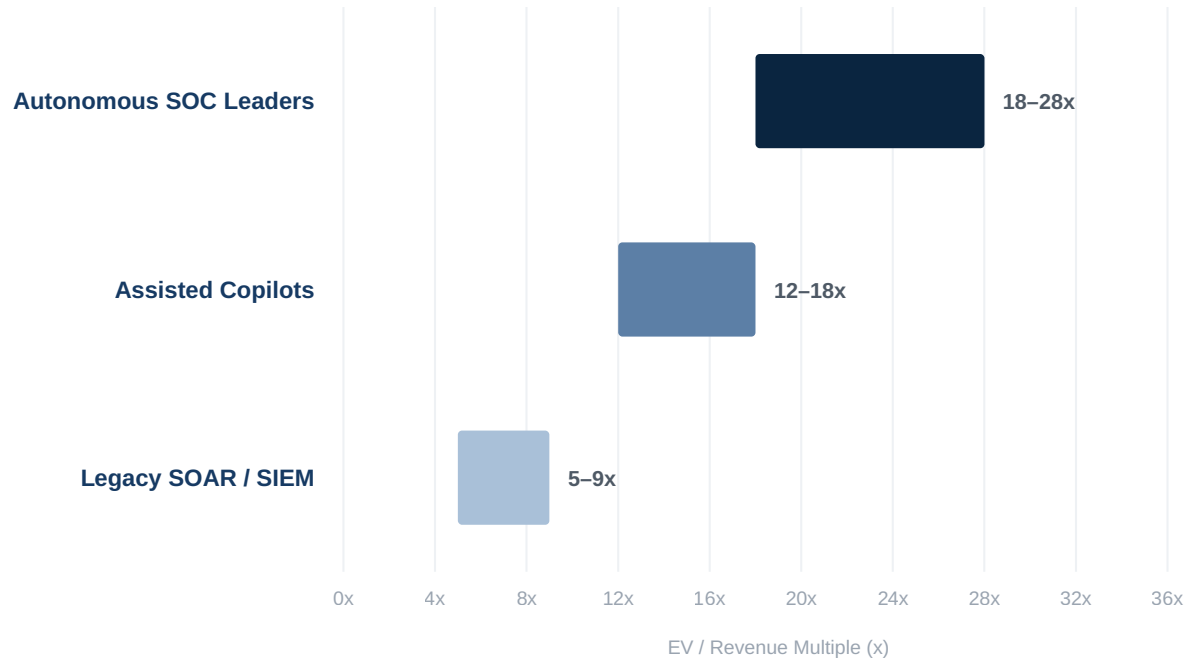
Israel and APAC drive about 32% of share; Israel remains the dominant AI-security venture pipeline.

**Valuation gap:** North America commands a premium, anchored by hyperscaler and platform M&A. Israel remains the global AI-security innovation hub on technical talent density. Europe trades at a regulatory-moat discount, sharpened by the EU AI Act, that US acquirers are increasingly arbitraging.

# AI SOC & Security Copilots: The Premium Cohort

Autonomy that decouples detection and response from analyst headcount underwrites some of the cycle's highest multiples.

EV / Revenue Multiple Range (x)



## Valuation Drivers

### Autonomy Premium

Buyers now pay for demonstrated autonomy, not roadmaps. Assets that show investigations handled end to end, large false-positive reductions and faster mean-time-to-respond clear the top of the range; pilots do not.

### Three Camps Emerge

The market has split into autonomous SOC (CrowdStrike, SentinelOne), assisted copilot (Microsoft, Fortinet) and platform consolidation (Palo Alto Networks, Zscaler), with autonomy commanding the richest multiples.

### Buyer Priorities

Platform incumbents acquire autonomous-SOC capability to lift net revenue retention and to convert their telemetry into a defensible, self-improving data and policy advantage.

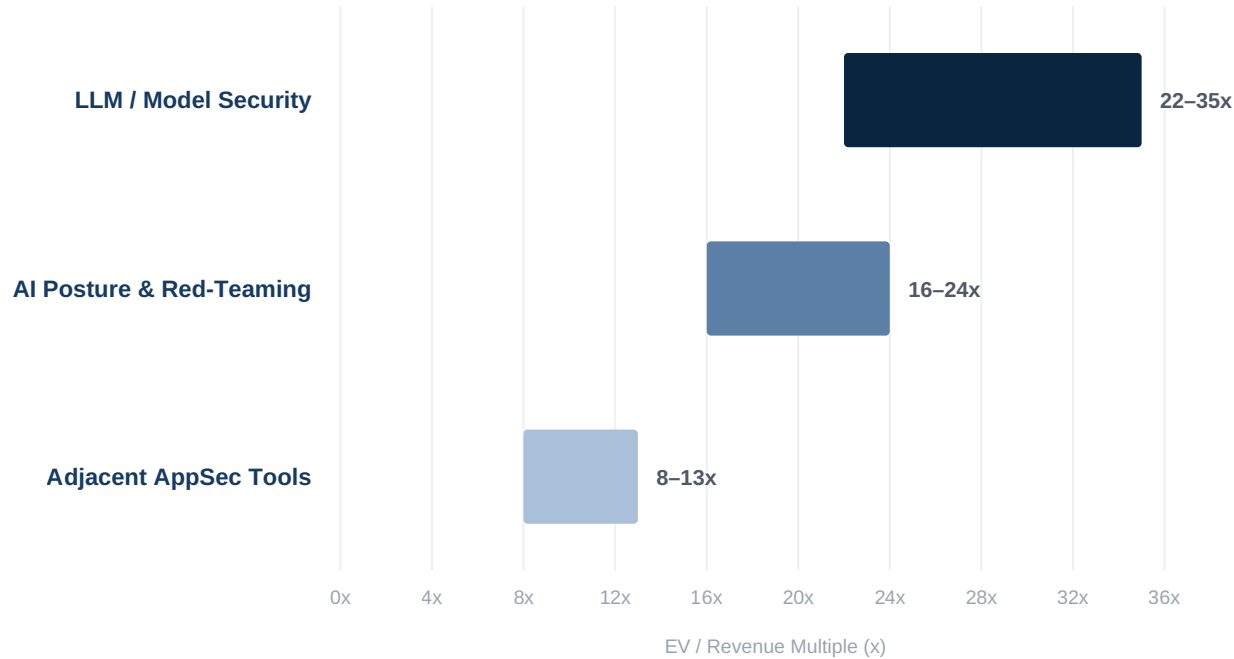
#### KEY OBSERVATION

**CrowdStrike** (Charlotte AI, AgentWorks) and **SentinelOne** (Purple AI Athena) anchor the public cohort; private autonomous-SOC entrants such as **Prophet Security** validate venture appetite for full autonomy.

# Model & LLM Security (AI-SPM): The Frontier

Securing AI itself, models, LLMs and pipelines, is the fastest-emerging category and the richest on a revenue-multiple basis.

EV / Revenue Multiple Range (x)



## Valuation Drivers

### Spend Gap as TAM

Gartner notes enterprises spend roughly **17x more on AI tools than on securing AI**. That gap is the bull case: model-security TAM expands as AI moves into production across the enterprise.

### Incumbents Buy In

Palo Alto Networks acquired **Protect AI** (about \$700M) to build Prisma AIRS, Cisco acquired **Robust Intelligence**, and Check Point acquired **Lakera**, repricing every comparable model-security asset.

### Scarcity & Multiples

Revenue bases are small and growth is explosive, so multiples are the highest in cyber. Pricing rewards defensible IP in model detection, red-teaming and runtime guardrails over breadth.

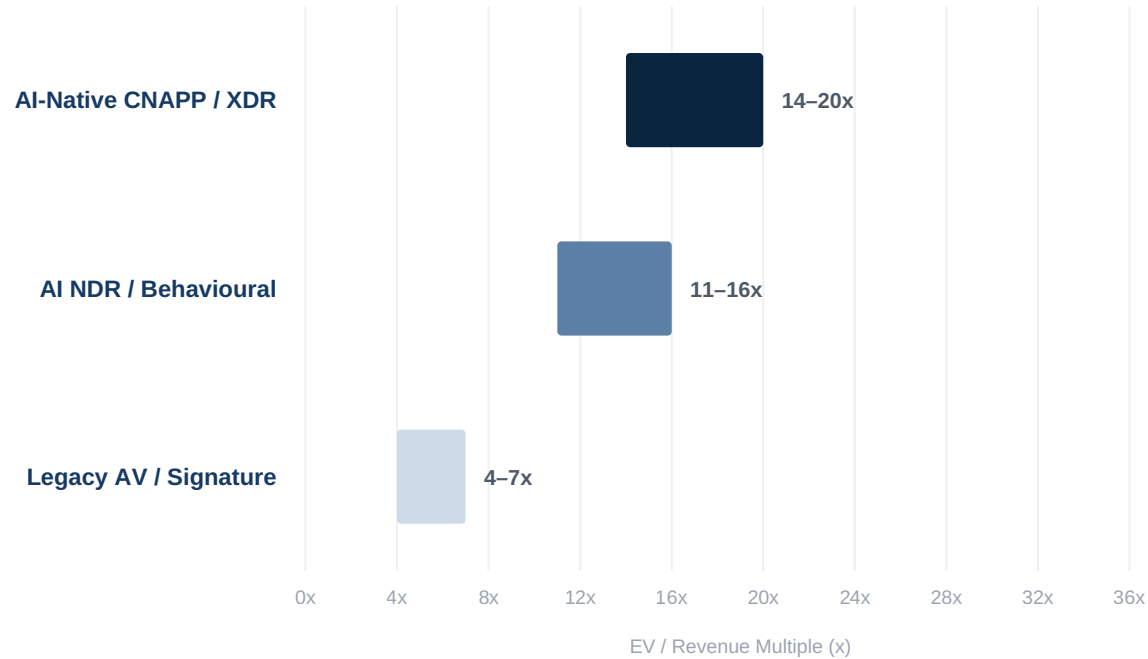
#### VALUATION DRIVER

Model security is priced as critical AI infrastructure, not an experiment; scarcity of genuine capability sustains 20x to 35x revenue multiples in private rounds.

# AI-Native Threat Detection & Response

AI-native cloud, network and endpoint detection re-rated the category, with cloud-native, agentless platforms at premium multiples.

EV / Revenue Multiple Range (x)



## Valuation Drivers

### Architecture Premium

Cloud-native, agentless and identity-aware detection displaces legacy agents at lower cost. Wiz's \$32B exit confirmed the ceiling for category-defining AI-native cloud detection.

### Data-Lake Economics

Detection platforms are increasingly valued as security data lakes that train proprietary models and anchor adjacent SIEM, identity and SOC-automation workloads, expanding wallet per customer.

### Buyer Priorities

Hyperscalers and platform incumbents pay up for AI-native detection that bolts directly onto an existing customer footprint and compounds a telemetry advantage.

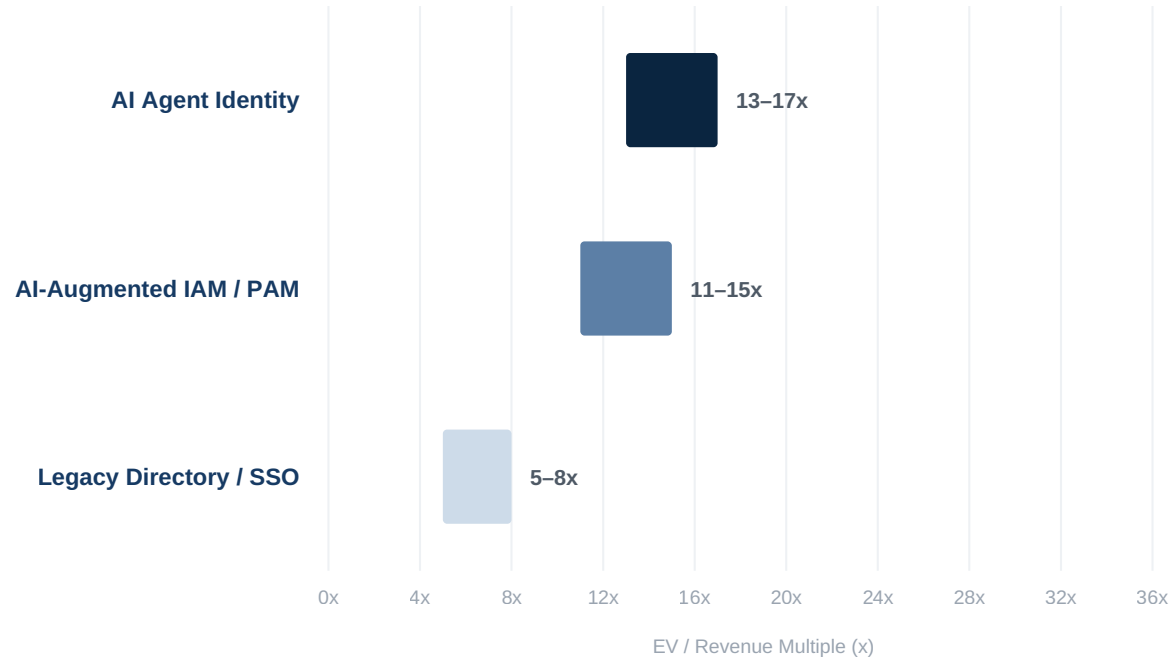
## KEY OBSERVATION

Cloud security is the **fastest-growing cyber subsegment at 28.8% in 2026 (Gartner)**, and the AI-native detection multiple structure reflects that durable growth.

# AI for Identity & Agent Security

Identity has become the control plane for AI agents, and Palo Alto Networks' \$25B CyberArk deal underwrites the strategic premium.

EV / Revenue Multiple Range (x)



## Valuation Drivers

### Platform Pull

Identity is the connective tissue between SaaS, cloud and AI agents. Strategic acquirers pay for identity to anchor a broader platform thesis, not for standalone tools.

### Non-Human Identity

Governing non-human and AI-agent identity is the fastest-growing identity subcategory, with venture and strategic capital actively building category leaders for an agentic enterprise.

### Buyer Priorities

Platform incumbents bolt identity onto existing stacks to govern agent access; the CyberArk transaction sets the template and the pricing anchor.

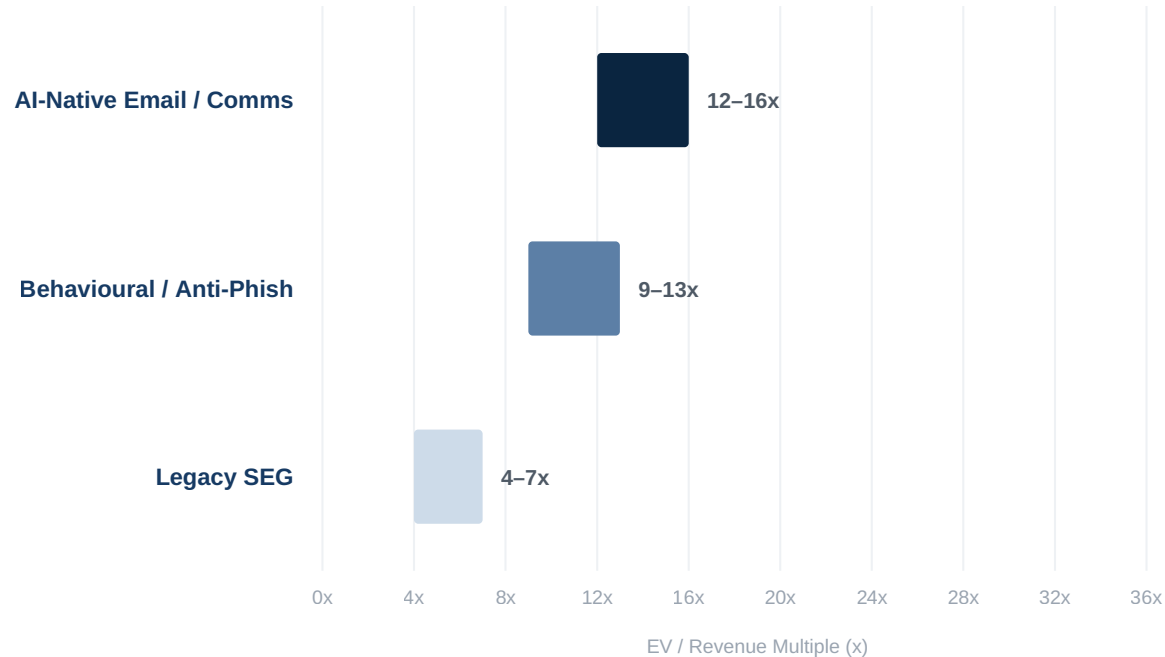
## KEY OBSERVATION

The **Palo Alto Networks / CyberArk** transaction at \$25B confirmed identity as the control plane for the AI-agent era, repricing comparable identity assets upward.

# AI Email & Social-Engineering Defence

Generative AI has industrialised phishing and deepfakes, re-rating behavioural, AI-native email and communications defence.

EV / Revenue Multiple Range (x)



## Valuation Drivers

### Threat-Driven Demand

AI-generated phishing, business-email-compromise and voice and video deepfakes have outrun signature-based gateways, forcing buy-side modernisation toward behavioural, AI-native defence.

### Behavioural Moats

Platforms that model normal human and account behaviour across email and connected apps build proprietary data moats that compound as the install base and event history grow.

### Buyer Priorities

Platform incumbents and email providers acquire behavioural AI to defend the inbox as the most-attacked surface and to feed adjacent identity and SOC workloads.

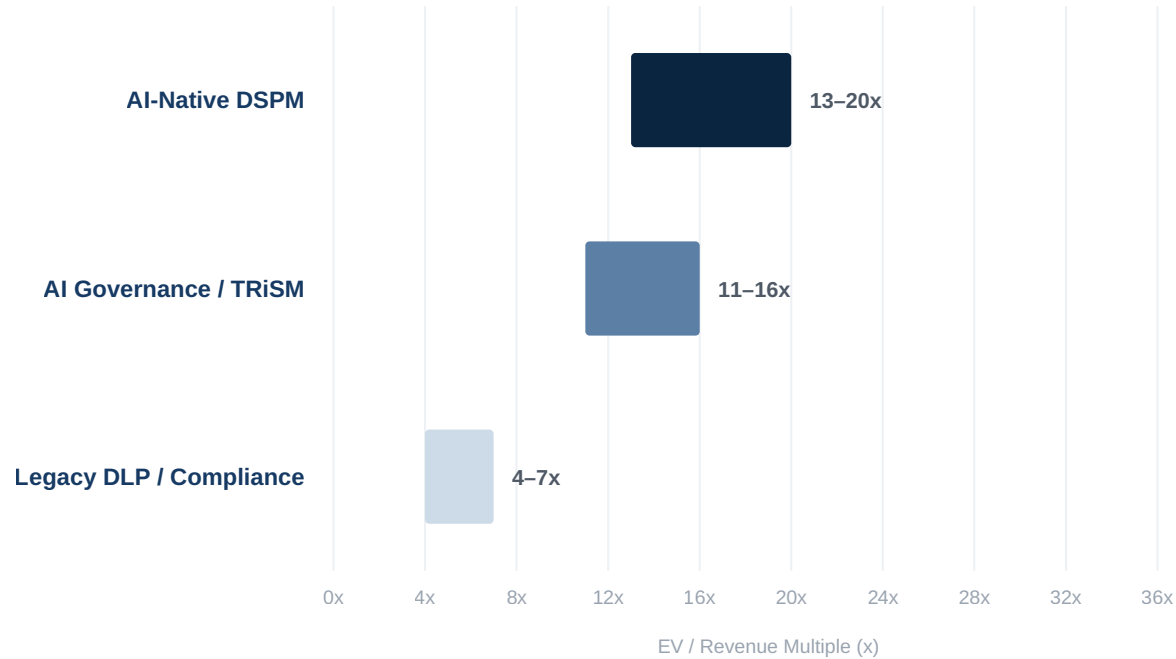
#### KEY OBSERVATION

**Abnormal Security** reached a **\$5.1B** valuation on AI behavioural email defence, the clearest private mark for the category.

# AI Data Security & Governance (DSPM for AI)

Data security posture and AI governance are re-rating on the need to make enterprise AI safe, narrowing the gap to model security.

EV / Revenue Multiple Range (x)



## Valuation Drivers

### AI Governance Surface

Enterprises adopting LLMs need data classification, lineage and access governance to deploy AI safely, expanding the DSPM TAM. Strategic buyers price DSPM as an AI-readiness adjacency.

### Regulatory Tailwinds

The EU AI Act, SEC cyber-disclosure rules, NIS2 and DORA have widened the AI-governance buying centre and raised the value of automated, audit-ready compliance evidence.

### Buyer Priorities

Platform incumbents and hyperscalers acquire DSPM and AI-governance capability to make existing security stacks 'AI ready' for enterprise buyers.

#### VALUATION DRIVER

Cyera raised at a **\$6B** valuation in 2025, rising toward **\$9B** since, the benchmark private mark for AI-native data security and governance.

# Comparable Transaction Analysis Framework

WINDSOR DRAKE

A rigorous quality-of-revenue and quality-of-AI filter rather than broad cyber sector labels.

## 1. Select Peer Set

Identify genuinely comparable assets by AI posture (AI-native vs AI-augmented vs AI-washed), buyer (SOC vs identity vs platform team), revenue model (consumption vs subscription) and architecture, not by broad cyber labels.

## 2. Normalise Metrics

Adjust KPIs to a pro-forma basis: normalise ARR for M&A, standardise NRR and GRR definitions, separate platform from 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.

236

WD INDEX TRANSACTIONS

2020–26

INDEX COVERAGE

## Proprietary Transaction Index

Calibration draws on Windsor Drake's proprietary index of **236 verified and reported transactions (2020 to 2026)**, refreshed each quarter and supplemented by current-quarter AI-security research for niche-specific comps.

## Quality-of-AI Filter

Peer selection prioritises demonstrated AI outcomes (autonomy, false-positive reduction, analyst leverage) over AI marketing, and weights proprietary training data and model defensibility heavily.

## 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 without a path to leverage.

## Control Premium Calibration

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

# Strategic Acquirer Mapping by Segment

WINDSOR DRAKE

Hyperscalers chase AI-native rails; platform incumbents pursue capability roll-ups; PE concentrates on services and mid-market software.

Segment	Hyperscalers / Strategics	Platform Incumbents	Private Equity
<b>AI SOC / Copilots</b>	<b>MODERATE</b> Hyperscalers build copilots in-house; selective autonomy M&A only.	<b>HIGH</b> XDR and platform leaders acquire autonomy to lift NRR and analyst leverage.	<b>MODERATE</b> PE consolidates mid-market SOC automation into managed-service platforms.
<b>Model &amp; LLM Sec</b>	<b>HIGH</b> Hyperscalers buy security-for-AI to make their AI platforms safe by default.	<b>HIGH</b> Platforms acquire model security to anchor AI-readiness; Protect AI is the template.	<b>LOW</b> Early-stage and venture-funded; PE largely waits for scale.
<b>AI Cloud &amp; Detection</b>	<b>HIGH</b> Hyperscalers backfill AI-native cloud detection; Google / Wiz is the template.	<b>HIGH</b> Platforms acquire cloud-native detection to defend share against AI-native entrants.	<b>MODERATE</b> PE plays come via take-privates of mid-market detection assets.
<b>AI Identity &amp; Agent</b>	<b>HIGH</b> Identity is the control plane for AI agents; a priority hyperscaler target.	<b>HIGH</b> Platform incumbents bolt identity onto stacks; PANW / CyberArk template.	<b>MODERATE</b> PE pursues workforce IAM and verticalised identity assets.
<b>AI Email Defence</b>	<b>MODERATE</b> Email providers add behavioural AI selectively to defend the inbox.	<b>HIGH</b> Platforms acquire behavioural AI to feed identity and SOC workloads.	<b>MODERATE</b> PE consolidates anti-phishing and SEG point tools.
<b>AI Data Sec / DSPM</b>	<b>HIGH</b> Hyperscalers acquire DSPM and AI governance to ready cloud platforms.	<b>HIGH</b> Cyber platforms add DSPM and TRiSM adjacencies to platform stacks.	<b>MODERATE</b> PE buys compliance and governance SaaS for buy-and-build theses.

# Hyperscalers & Platform Incumbents as Buyers

WINDSOR DRAKE

Hyperscalers and platform incumbents are using M&A to convert AI security into a defensive moat for cloud, identity and SOC revenue.

## Strategic Motives: Buy vs. Build

The internal build cycle for AI-native, autonomous defence is too slow to counter category-defining startups. That gap is compelling hyperscalers and incumbents to acquire modern stacks outright, treating M&A as defensive modernisation rather than expansion.

## Acquisition Patterns

Mega-deals (Google / Wiz \$32B, PANW / CyberArk \$25B) sit at the top; capability bolt-ons under \$1B (Protect AI, Robust Intelligence, Lakera) dominate by volume, often preceded by partnership or technology-integration de-risking.

**\$32B**

GOOGLE / WIZ, CLOSED MAR 2026

**\$25B**

PANW / CYBERARK, CLOSED FEB 2026

## Semi-Autonomous Integration

A federated model preserves the target's product cadence and retains scarce AI talent, while platform-grade compliance and identity controls are overlaid at the backend.

## Priority: Security for AI

Top focus is securing the enterprise's own AI: model security, AI posture and governance that make a platform safe to adopt at scale.

## Priority: Identity & AI Agents

Identity is the control plane for AI agents; assets like CyberArk are priced as platform pillars, not point tools.

## Priority: Autonomous SOC

Autonomous detection and response is acquired to lift net revenue retention and to compound a proprietary telemetry and policy advantage.

# Private Equity Acquisition Patterns

WINDSOR DRAKE

Record dry powder is creating intense deployment pressure even as sponsors stay disciplined on AI-security pricing.

## Deployment Pressure

With roughly **\$1.3T** of global dry powder to deploy (Bain), sponsors face acute pressure to transact. Bain notes tech deal value fell about **70%** from Q4 2025 to Q1 2026 on valuation uncertainty, so capital concentrates in fewer, higher-conviction assets.

## New Deal Math

Bain captures the new environment with the shorthand that '12 is the new 5': today's entry multiples require far larger EBITDA gains to clear target returns, pushing sponsors toward efficient, AI-leveraged operating models.

~\$1.3T

GLOBAL PE DRY POWDER

-70%

TECH DEAL VALUE, Q4 25 TO Q1 26

## 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 a higher-rate environment.

## Value-Creation Playbook

Pricing optimisation, deploying AI to decouple delivery cost from revenue, and buy-and-build consolidation of mid-market AI-security software and managed detection.

## Public-to-Private Thesis

Mid-cap cyber names trading below AI-native peers remain prime take-private targets, with an AI-modernisation thesis underwriting the value-creation plan.

## Deal Structure Trends

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

# Competitive Moats Driving Premium Valuations

WINDSOR DRAKE

AI-security valuations above 16x revenue are reserved for companies that can demonstrate structural defensibility.

## Proprietary Training Data

ASSET VALUE: HIGHEST

### First-party telemetry training detection models

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

## Demonstrated Autonomy

SCALE VALUE: HIGHEST

### Outcomes decoupled from analyst headcount

- Quantified investigations handled, false positives cut and faster response.
- Shows non-linear margin expansion as the customer base scales.
- Directly lifts the Rule of 40 score that gates premium multiples.
- **Action:** instrument and publish autonomy and ROI metrics buyers can diligence.

## 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.
- Increasingly central to government and critical-infrastructure AI theses.
- **Action:** invest early in certifications that gate the most defensible verticals.

## Platform Attach

GROWTH VALUE: HIGH

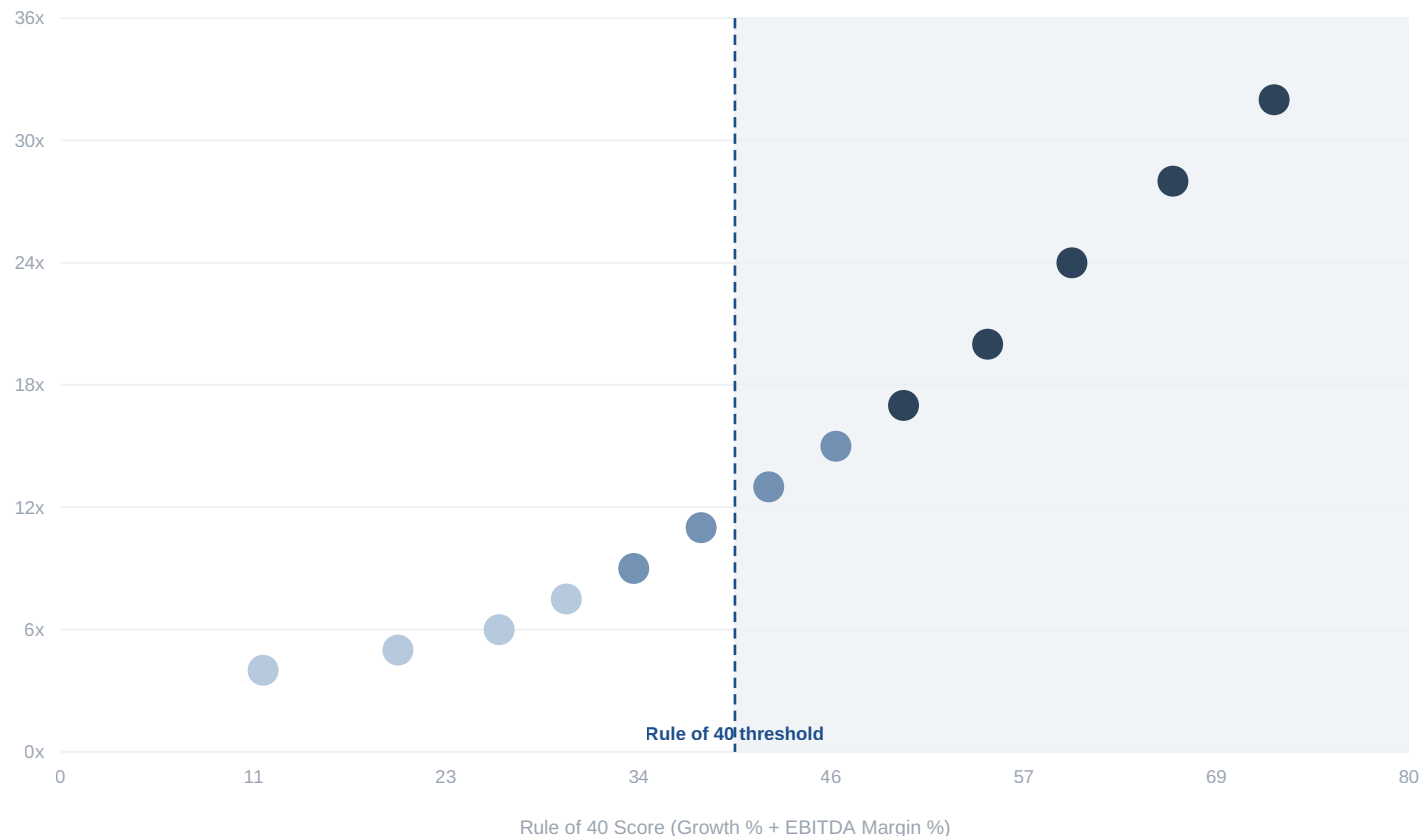
### Multi-product attach and identity-aware policy

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

# Rule of 40 Performance Distribution

Clearing the Rule of 40 still roughly doubles the multiple; AI infrastructure cost is pressuring the rule across the cohort.

EV / Revenue Multiple vs Rule of 40 Score



TOP QUARTILE ( SCORE >50 )

## 17x to 35x

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

RULE OF 40 MET ( 40 TO 50 )

## 12x to 17x

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

BELOW THRESHOLD ( <40 )

## 4x to 9x

Transition and value-trap zones; vulnerable to consolidation.

**Bain finds Rule-of-40 outperformers carry roughly double the EV/Revenue of companies below the line**, and AI-security leaders that clear the bar trade far higher. AI infrastructure cost is pressuring the rule, leading Bain to discuss a 'Rule of 30' for AI-native players reinvesting to compete.

# Cross-Border M&A Considerations

WINDSOR DRAKE

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

## Regulatory Regimes

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

## Currency & WACC Impact

US acquirers are leveraging a strong dollar and premium domestic multiples to buy discounted European and Israeli AI-security 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 AI-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 AI 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.

# Exit Valuation Optimisation Strategies

WINDSOR DRAKE

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

## 1. Prove AI Outcomes

6 TO 12 MONTHS PRE-EXIT

Make the AI case diligence-ready

- Instrument autonomy, false-positive reduction and analyst-leverage metrics.
- Document model performance, drift monitoring and data-rights provenance.
- Quantify customer cost-to-defend reduction with hard ROI cases.
- Evidence that AI investment is converting into operating leverage.

## 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 AI 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 delivery cost 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 AI infrastructure

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

# Positioning for Strategic Acquisition

WINDSOR DRAKE

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

---

## Capability Fit

Demonstrate unique IP and proprietary training data, model or autonomy 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, model interfaces 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 base, and model the cost synergies from shared infrastructure and AI tooling, 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 AI-security deficits.

---

## Proof-of-Integration

Develop technical materials that demonstrate speed-to-value within the acquirer's ecosystem, pre-empting the technical and model 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, data-rights, customer-concentration and certification risk before the first buyer engagement.

# 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 and elevated AI-capability premia 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 AI data-rights audit**



## Strategic Positioning

Q4 2026

- Launch dual-track process preparation
- Build the strategic buyer-targeting list
- Draft the CIM and management presentation
- Lock key AI-talent 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

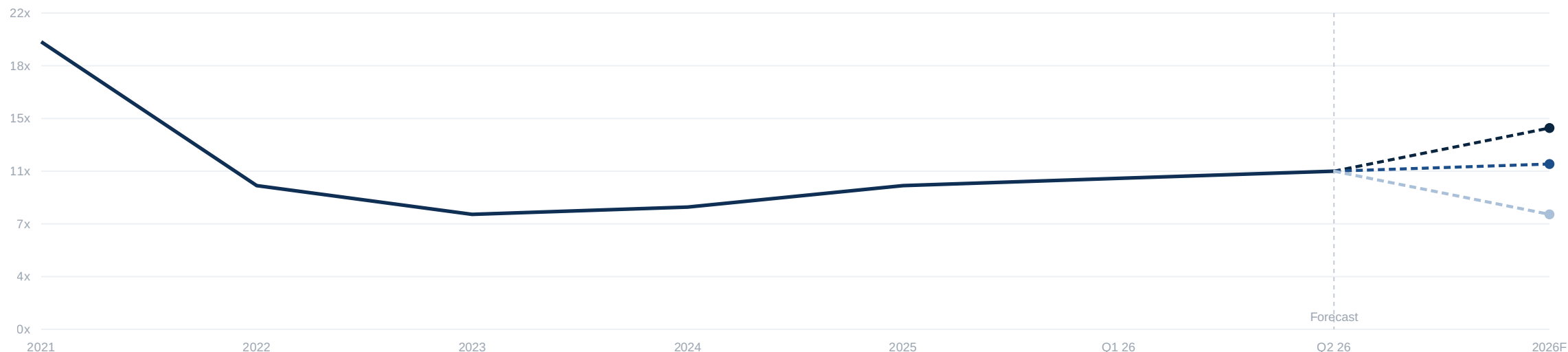
KEY MILESTONE

**No-MAC event verification**

# 2026 Valuation Forecast Scenarios

WINDSOR DRAKE

With the niche benchmark near 11x, forward trajectories diverge sharply on rates, AI pricing dynamics and the durability of platform consolidation.



## BULL CASE

**14.0x**

### Key Drivers

- Fed pivots to cuts late in 2026
- AI defence supercycle lifts multiples
- Model-security and SOC IPO pipeline opens

STRATEGY: ACCELERATE GROWTH

## BASE CASE

**11.5x**

### Key Drivers

- Rates held higher for longer
- Strategic-buyer consolidation continues
- Selective IPOs from scaled AI-native cohort

STRATEGY: BALANCE GROWTH & PROFIT

## BEAR CASE

**8.0x**

### Key Drivers

- Inflation resurgence, rate hikes return
- AI infrastructure cost compresses Rule of 40
- An AI-hype correction reprices private rounds

STRATEGY: CASH PRESERVATION

# Emerging Opportunities & Buyer Trends

WINDSOR DRAKE

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

---

## Security for AI Agents

Identity, policy and runtime security for autonomous AI agents is the fastest-emerging category, with venture and strategic capital both actively building category leaders for an agentic enterprise.

## Model & LLM Security

Securing models, pipelines and AI applications is repricing fast; Palo Alto Networks' Protect AI deal, Cisco's Robust Intelligence and Check Point's Lakera all underline strategic appetite.

## Autonomous SOC Automation

Fully autonomous investigation and response is moving from pilot to production, with public leaders and venture-backed entrants competing to set the category's economics.

## Hyperscaler Capability Acquisitions

Hyperscalers prioritise AI-native, identity and model-security capability over distribution, buying technology to make their platforms safe to adopt for enterprise AI.

---

## PE Platform Roll-Ups

Sponsors are consolidating fragmented managed detection and mid-market AI-security software to build scale and drive multiple expansion.

---

## Regional Champions Go Global

European and Israeli AI-security leaders are acquiring North American assets to capture premium valuations and access deeper capital markets.

---

## Market Intelligence

Top-tier forecasts point to durable, AI-led cyber demand through 2026. Record dry powder and capability-driven buyer demand are chasing a supply of genuine AI-native assets that has not kept pace.

# M&A Case Study: Palo Alto Networks Builds the AI Security Platform

WINDSOR DRAKE

The defining AI-security platform play of the cycle, and the playbook it sets for founders.

## The Platform Playbook

Palo Alto Networks' acquisition of **CyberArk**, valued at **\$25B** and closed in **February 2026**, paired with its roughly **\$700M** purchase of **Protect AI**, is the defining AI-security platform play of the cycle. Identity becomes the control plane for AI agents while Protect AI anchors the new Prisma AIRS platform for securing models and LLMs end to end.

## Strategic Rationale

- **Identity for the AI-agent era:** CyberArk makes Palo Alto Networks the governor of human and non-human identity.
- **Security for AI:** Protect AI adds model discovery, posture and runtime defence as Prisma AIRS.
- **Platform compounding:** identity, model security and SOC data combine into a defensible AI-security stack.

## Implications for Founders

### Pure-Play AI Security Commands a Bid

Incumbents are paying up for **category-defining AI-security capability**: CyberArk anchored identity pricing, and Protect AI showed that even an early-revenue security-for-AI asset can command a strategic premium. The window for follow-on category-definers in model security, agent identity and autonomous SOC is open, but narrowing as platforms consolidate.

### Quantify Platform Pull Pre-LOI

Headline multiples on AI-security assets rest on **identifiable, underwritable platform synergies**. Vague AI positioning no longer moves valuation; rigorous synergy math and proven outcomes, presented before the LOI, do.

### Platform vs. Point Solution

Assets framed as broad **AI-security platforms** capable of absorbing bolt-ons trade at clear premiums to narrow point solutions. Integration readiness, clean APIs and model interfaces are themselves a valuation lever.

# Valuation Methodology: Choosing the Right Metric

WINDSOR DRAKE

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

## EV / Revenue

12–35X

### High-growth AI-native

- Applied where profitability is suppressed by deliberate growth reinvestment.
- Software revenue (above 80% margin) is valued far above services revenue.
- The Rule of 40 score and proven AI outcomes dictate placement in the range.
- Best suited to model security, AI SOC, AI detection and identity platforms.

## EV / EBITDA

12–22X

### Mature & cash-generative

- Essential for mature, slower-growth or services-heavy cyber 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 segments.

## ARR & NRR Lens

RECURRING FOCUS

### SaaS-delivered AI security

- 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 AI SOC, detection and governance assets.

## Strategic Premium

+25–30%

### Platform & capability fit

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

# Appendix: Sources & Methodology (Part 1)

WINDSOR DRAKE

Institution	Report / Source	Date
Gartner	<i>Forecast: Information Security and Risk Management, Worldwide (4Q25); AI-amplified security</i>	Mar 2026
Gartner	<i>Worldwide AI Spending Forecast 2026; Top Cybersecurity Trends 2026</i>	Jan-Feb 2026
McKinsey & Company	<i>Global Private Markets Report 2026; software value-creation research</i>	2026
Bain & Company	<i>Hacking Software's Rule of 40; AI Brings Headwinds and Tailwinds to the Rule of 40</i>	2025
Bain & Company	<i>Global Private Equity Report 2026 (dry powder; new deal math)</i>	Mar 2026
PwC	<i>Global M&amp;A Industry Trends: 2026 Outlook (TMT)</i>	Jan 2026
EY	<i>M&amp;A Activity Insights and 2026 Outlook</i>	Apr 2026
S&P Global Market Intelligence	<i>Global M&amp;A by the Numbers: Q1 2026</i>	Apr 2026
PitchBook	<i>Q1 2026 Global M&amp;A Report; AI and Cybersecurity coverage</i>	2026
Goldman Sachs	<i>US rates outlook (2026 policy path)</i>	2026

# Appendix: Sources & Methodology (Part 2)

WINDSOR DRAKE

Institution	Report / Source	Date
CB Insights	<i>State of AI and Cybersecurity Venture Funding</i>	2026
KPMG	<i>Venture Pulse Q4 2025</i>	Jan 2026
Federal Reserve	<i>FOMC Statement (Apr 2026); Summary of Economic Projections</i>	2026
Alphabet Inc.	<i>SEC filings, Wiz acquisition close</i>	Mar 2026
Palo Alto Networks	<i>SEC filings and press, CyberArk close and Protect AI / Prisma AIRS</i>	2025-2026
Netskope Inc. / SailPoint	<i>SEC Form S-1 / 424B; IPO pricing</i>	2025
World Economic Forum	<i>Global Cybersecurity Outlook 2026</i>	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 AI posture (AI-native vs AI-augmented), buyer (SOC, identity, platform), 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 11x niche median benchmark and the segment multiple ranges, are the firm's own synthesis of the cited institutional data, presented as a house view rather than third-party consensus.