

WINDSOR DRAKE

Cybersecurity M&A Activity: Q2 2026

MAY 2026

Windsor Drake · Market Intelligence

A Record Value Cycle

Deal value has stepped to a level the sector has never seen.

- Disclosed value of pure-play cybersecurity deals reached **\$84B in 2025**, roughly triple the 2024 figure.
- Q1 2026 recorded about **\$47B** of cybersecurity deal value in a single quarter.
- Median transaction value climbed above **\$300M** in Q1 2026.
- Buyers are paying up for platforms, not browsing for point tools.

Volume Holds, Value Concentrates

Deal count is steady while value collects at the top.

- About **426 cybersecurity deals** were announced in 2025, up roughly 22% on 2024.
- Q1 2026 logged **108 transactions**, the second-highest quarterly count on record.
- Most deals remain small tuck-ins; financial terms are disclosed on a minority.
- A barbell has formed: many small deals, a thin band of very large ones.

The Megadeal Era

Two of the largest software deals on record are cybersecurity deals.

- **Google / Wiz** (\$32B) closed in March 2026, the largest cybersecurity acquisition ever.
- **Palo Alto Networks / CyberArk** (\$25B) closed in February 2026.
- Eleven 2025 cybersecurity deals exceeded \$1B, carrying roughly \$75B of value.
- Scale has become the organising principle of the sector.

Platformisation Drives Demand

Enterprises are consolidating onto integrated security platforms.

- Buyers acquire to close platform gaps in cloud, identity and security operations.
- AI-native capability is the single most contested asset class.
- Strategic platform vendors and hyperscalers lead the buyer field.
- Private equity is active in parallel through take-privates and roll-ups.

Identity as the Control Layer

Identity has become the security architecture of the AI era.

- Palo Alto Networks bought CyberArk to make identity a core platform pillar.
- Agentic AI and machine-to-machine traffic multiply the identities to secure.
- Machine and non-human identity is now a primary acquisition theme.
- Identity assets command the clearest scarcity premium in the sector.

Cloud Security Consolidation

The hyperscalers are buying their way to full-stack cloud security.

- Google's \$32B purchase of Wiz anchors cloud-native security inside Google Cloud.
- IBM acquired HashiCorp (\$6.4B) to secure and automate hybrid cloud.
- Cloud posture, data security and runtime protection are converging in one buy.
- The build cycle is too slow; incumbents are acquiring the category leaders.

Private Capital Pressure

Record dry powder is pushing sponsors deep into cybersecurity.

- About **\$3.7T** of global private equity dry powder is seeking deployment.
- Specialist sponsors hold multi-billion-dollar cybersecurity portfolios.
- Take-privates of mature security software are accelerating.
- Aging 2020 to 2022 vintages are also pushing sponsors toward exits.

A Reopening M&A Market

The broad deal backdrop is the most constructive since 2021.

- Goldman Sachs forecasts about **\$3.8T** of global M&A in 2026.
- EY-Parthenon finds 62% of US CEOs plan to pursue M&A, up 27 points.
- Rate stabilisation and reopened capital markets are lifting confidence.
- Cybersecurity is one of the few tech segments holding premium valuations.

1. The Strategic Sale Is the Default

Platform vendors, hyperscalers and sponsors are all competing for cybersecurity assets, making a strategic sale the central exit path well ahead of the IPO.

- Map your capability against the declared platform gaps of named acquirers.
- Engineer the asset to be acquirable, not only fundable.

2. Quantify Synergies Early

Headline multiples now rest on identifiable cross-sell and consolidation synergies; vague strategic fit no longer moves valuation.

- Model revenue and cost synergies before the LOI stage.
- Present the synergy case in the management presentation.

3. The Window Has Lead Time

A full process runs 12 to 18 months, so capturing the current constructive market requires preparation to begin in the present planning cycle.

- Begin diligence readiness well ahead of market engagement.
- Hold 12 to 18 months of runway to negotiate from strength.

4. Platform Fit Beats Standalone Scale

Acquirers pay premiums for capability that slots cleanly into an integrated security platform, especially in cloud, identity and AI security.

- Frame the asset around a concrete platform capability deficit.
- Evidence clean integration paths and production-grade AI.

5. Expect Structured Consideration

All-cash deals have returned for certainty, but earn-outs remain standard for bridging valuation gaps on AI-native and early-traction assets.

- Prepare for performance-linked payments over 12 to 24 months.
- Negotiate clear, measurable earn-out milestones up front.

6. Point Solutions Must Choose

In a platformising market, single-feature vendors face a clear strategic decision as enterprises consolidate spend onto fewer suites.

- Extend toward a platform, or position decisively to be acquired.
- Delay narrows options as buyers complete their platform maps.

Founder FAQs: Process, Timing & Deal Terms

WINDSOR DRAKE

The questions founders ask most, answered against the Q2 2026 cybersecurity M&A market.

Q1 How long does a sale process take?

Plan for a **12 to 18 month** total timeline: six to nine months of preparation, three to six months of market engagement and negotiation, and three or more months for regulatory clearance and closing conditions.

Q3 Is M&A a better route than an IPO?

For most cybersecurity companies, yes. The IPO window has reopened but favours scaled, profitable platforms. A strategic sale to a consolidating acquirer often delivers a superior risk-adjusted outcome through control and scarcity premiums.

Q5 When is the right time to run a process?

After **4 to 6 quarters** of predictable performance, while still holding 12 to 18 months of runway. Negotiating from strength, rather than necessity, is what captures a scarcity premium.

Q7 What kills cybersecurity deals in diligence?

Weak net revenue retention, customer concentration, unproven AI claims, security or compliance gaps in the target's own stack, and integration risk. Most are addressable with disciplined preparation before engagement.

Q2 Who are the most active buyers right now?

Security platform vendors closing capability gaps, **hyperscalers** building full-stack cloud security, and **private equity** executing take-privates and roll-ups. Strategic buyers drive the large majority of cybersecurity exits.

Q4 What gets a deal the highest price?

A capability an acquirer cannot quickly build, a clean fit into the buyer's platform, durable recurring revenue, and a credible AI story. Competitive tension among two or more platform buyers does the rest.

Q6 Should we expect earn-outs?

Often. All-cash consideration has returned for certainty, but **earn-outs** remain standard for bridging valuation gaps, particularly for AI-native or early-traction assets, typically paid over 12 to 24 months.

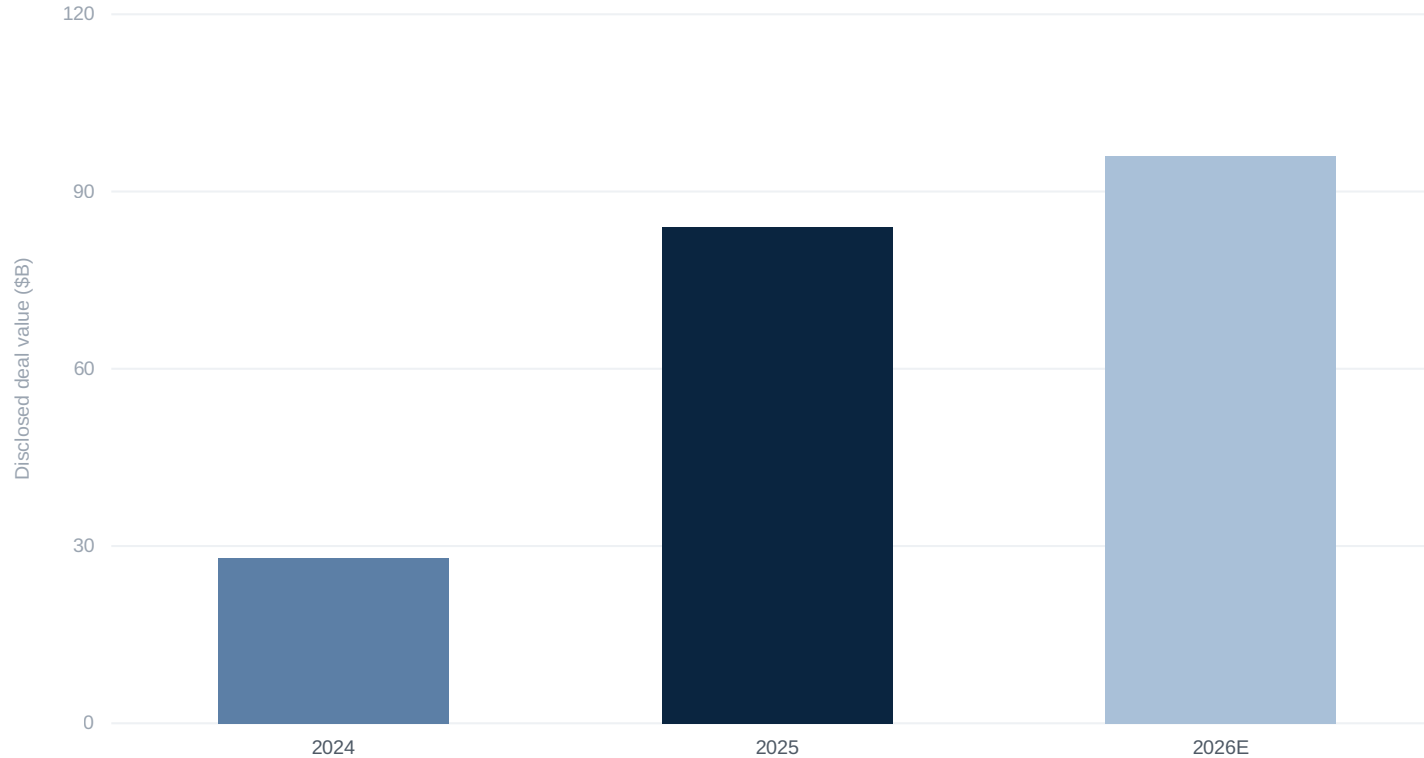
Q8 What are the main cross-border risks?

Cybersecurity is treated as critical infrastructure, so national-security screening (CFIUS and equivalents) and data-sovereignty rules are the primary friction. Cross-border clearance typically runs 30 to 50% longer than a domestic deal.

Cybersecurity M&A Deal Volume & Value

Deal count is steady while deal value steps to a record: the market is paying far more for platform-defining assets.

Disclosed Cybersecurity M&A Deal Value, Pure-Play Targets (\$B)



A record value cycle: disclosed value of pure-play cybersecurity acquisitions rose from about \$28B in 2024 to roughly \$84B in 2025, driven by a small set of platform megadeals. The 2026 estimate is Windsor Drake analysis of the cited outlooks and Q1 run rate.

2025 DISCLOSED VALUE

~\$84B

Pure-play cybersecurity deals, up from about \$28B in 2024 (S&P Global; CB Insights).

Q1 2026 DEAL VALUE

~\$47B

A single quarter, lifted by the close of two platform megadeals.

2025 DEAL COUNT

~426

Announced cybersecurity deals, up roughly 22% on 2024.

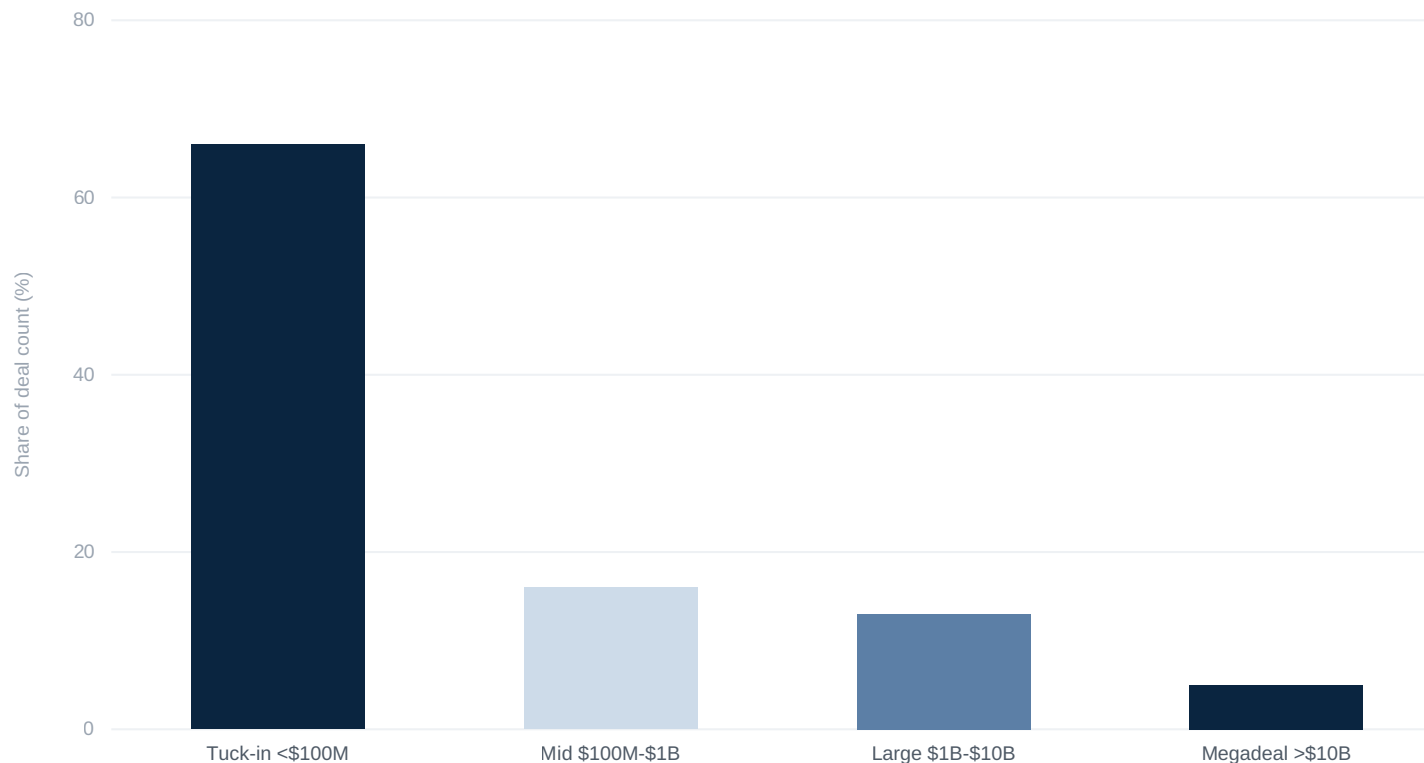
Key Driver

Value is concentrating in a thin band of platform-defining acquisitions while the cadence of small deals continues.

The Barbell Market: Deal-Size Distribution

Activity concentrates in high-volume tuck-ins and a thin band of platform megadeals, hollowing the middle.

Indicative Share of Cybersecurity M&A Deal Count by Size Band (%)



TUCK-IN DOMINANCE

Count

Small capability and acqui-hire deals are the bulk of activity by number.

MEGADEAL CONCENTRATION

Value

Eleven 2025 deals above \$1B carried roughly \$75B of total value.

THE SQUEEZED MIDDLE

\$100M-\$1B

Mid-sized point solutions face the thinnest buyer pool and the longest path to exit.

Strategic Implication

Mid-market founders face a binary choice: extend toward a platform, or position decisively for a strategic sale.

A hollowing middle: capability tuck-ins dominate by count while a handful of deals above \$10B dominate by value. The distribution shown is Windsor Drake analysis; the directional pattern is corroborated by S&P Global and McKinsey.

Notable Transactions of the Cycle

WINDSOR DRAKE

Four transactions that define the strategic logic of the current cybersecurity M&A market.

Google / Wiz

Valued at **\$32B**, closed March 2026.

- The largest cybersecurity acquisition ever completed.
- Anchors cloud-native security inside Google Cloud.
- All-cash consideration after a full year of regulatory review.
- Rationale: cloud security platform.

Palo Alto Networks / CyberArk

Valued at about **\$25B**, closed February 2026.

- The largest transaction in the security industry at announcement.
- Makes identity a core pillar of the Palo Alto platform.
- Cash and stock consideration, cleared in four jurisdictions.
- Rationale: identity as the control layer.

HPE / Juniper Networks

Valued at about **\$14B**, closed July 2025.

- Combines networking with AI-driven network security.
- Cleared a contested antitrust review in the United States.
- Positions secure, AI-native networking as one stack.
- Rationale: network and infrastructure security.

ServiceNow / Armis

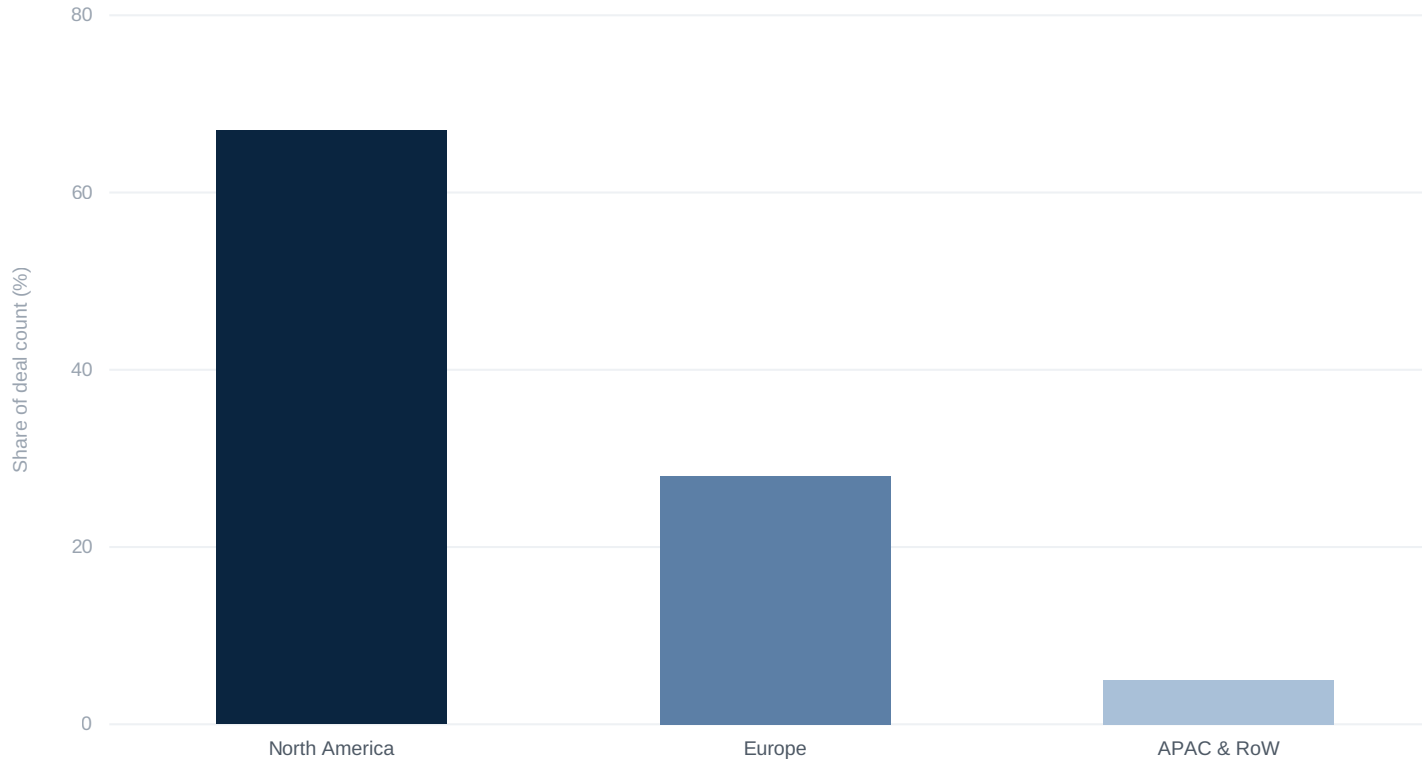
Valued at about **\$7.75B**, completed in 2026.

- Adds asset visibility and cyber exposure management.
- Extends coverage across IT, OT and connected devices.
- Cash consideration funded with cash and debt.
- Rationale: exposure and security operations.

Geographic Deal Distribution

North America anchors cybersecurity M&A; Europe and Israel are dense sources of acquisition targets.

Indicative Share of Cybersecurity M&A Deal Count by Region (%)



NORTH AMERICA

~67%

The deepest pool of platform acquirers and the largest share of targets.

EUROPE

~28%

A steady source of targets, with sovereign-security deals a rising theme.

ISRAEL

Outsized

The origin of the cycle's two defining assets, Wiz and CyberArk.

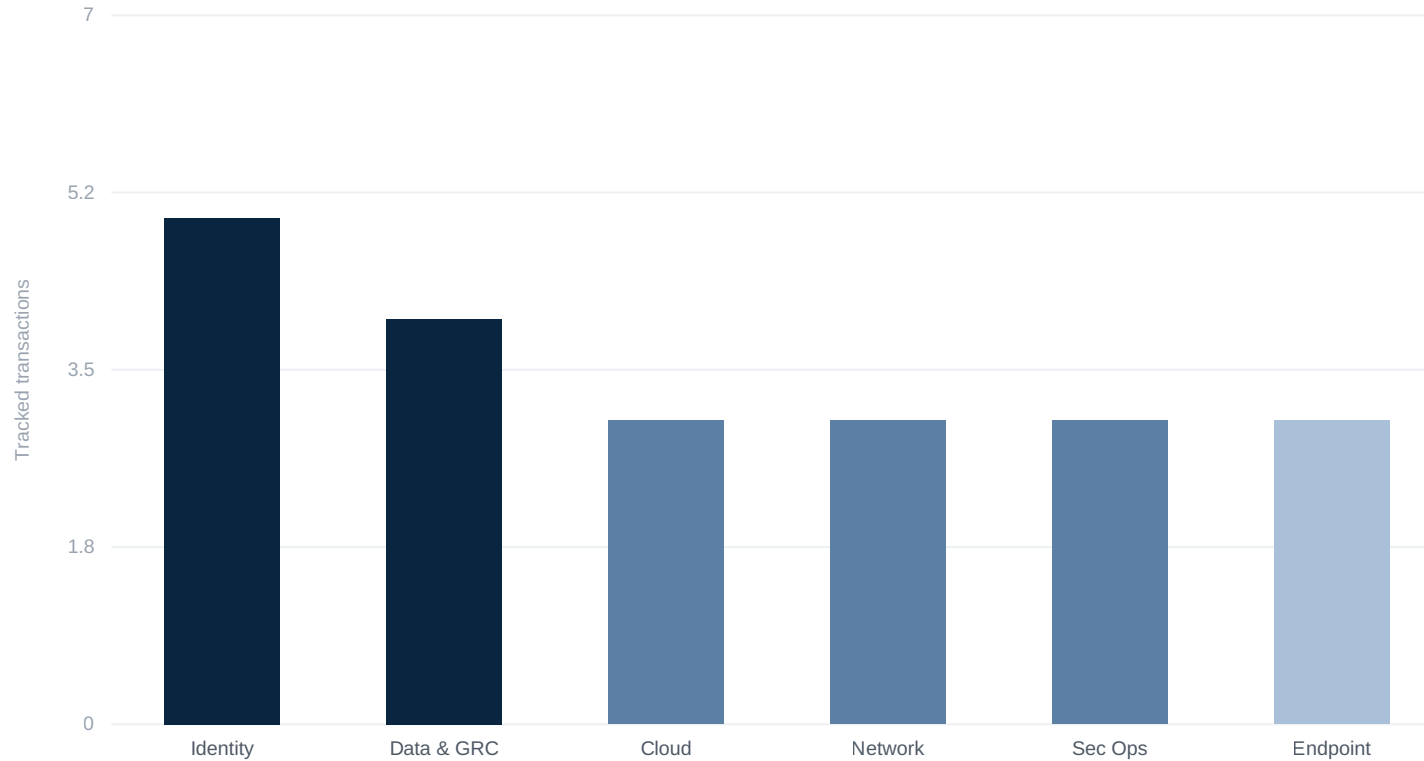
A US-anchored market: North American companies featured in the clear majority of cybersecurity deals, with Europe the second deepest pool. Israel punches far above its size as a source of acquired innovation, including Wiz and CyberArk.

The Windsor Drake Cybersecurity Transaction Index

WINDSOR DRAKE

A proprietary index of verified and reported cybersecurity transactions calibrates the firm's deal benchmarking.

Tracked Transactions by Subsector (count, 2019-2026)



COVERAGE

2019-2026

Verified and reported cybersecurity deals across six capability subsectors.

RECURRING BUYERS

FIs too

Financial-services strategics also acquire cyber capability: RiskRecon, Ekata and Recorded Future sit in the index.

REFRESH CADENCE

Quarterly

The index is updated each quarter as new transactions are verified.

Calibrated to real deals: the index spans verified and reported cybersecurity transactions from 2019 to 2026, from sub-\$200M capability tuck-ins to deals above \$30B, and underpins the comparable-set analysis used throughout this report.

The Buyer Landscape

Three buyer groups are competing for cybersecurity assets, each with a distinct mandate.

A Strategic-Led Market

Platform vendors and hyperscalers, not financial buyers, drive the large majority of cybersecurity exits. The strategic sale has displaced the IPO as the central exit route for venture-backed cybersecurity companies.

Competition Favours the Seller

With three distinct buyer pools active at once, a well-prepared asset can manufacture genuine competitive tension, the single most reliable lever on final price.

3

ACTIVE BUYER POOLS

11

2025 DEALS ABOVE \$1B

Security Platform Vendors

Palo Alto Networks, CrowdStrike, Cisco and Microsoft acquiring to close platform gaps and consolidate enterprise security spend onto their suites.

Hyperscalers & Tech Platforms

Google, IBM and ServiceNow buying full-stack cloud, data and exposure security to embed protection into their core infrastructure.

Private Equity

Specialist sponsors deploying record dry powder into take-privates of mature security software and buy-and-build consolidation.

Defence & Sovereign Buyers

Aerospace and defence primes acquiring sovereign cybersecurity capability, a fast-rising European acquisition theme.

Strategic Acquirer Mapping by Subsector

WINDSOR DRAKE

Platform vendors seek capability fit; hyperscalers seek cloud depth; private equity targets cash flow.

Subsector	Platform Vendors	Hyperscalers	Private Equity
Cloud Security	HIGH Closing cloud posture and runtime gaps in the suite.	HIGH Embedding native security into the cloud platform.	MODERATE Selective buy-and-build of cloud security software.
Identity & Access	HIGH Identity as a core platform control layer.	MODERATE Securing machine and workload identity in cloud.	HIGH Mature, recurring-revenue identity platforms.
Security Operations	HIGH Consolidating detection and response into the platform.	HIGH Exposure and asset intelligence for connected estates.	MODERATE Analytics and SIEM assets with durable economics.
Network Security	HIGH Secure access and AI-driven network defence.	MODERATE Networking and security convergence plays.	HIGH Cash-generative network security take-privates.
Endpoint & Email	MODERATE Selective tuck-ins to round out the suite.	LOW Rarely core to a cloud platform thesis.	HIGH Prime take-private and consolidation target.
Data Security & GRC	HIGH Data security posture is a fast-growing gap to fill.	MODERATE Governing data risk across cloud workloads.	HIGH Recurring-revenue GRC and compliance software.

■ High Activity / Priority Target

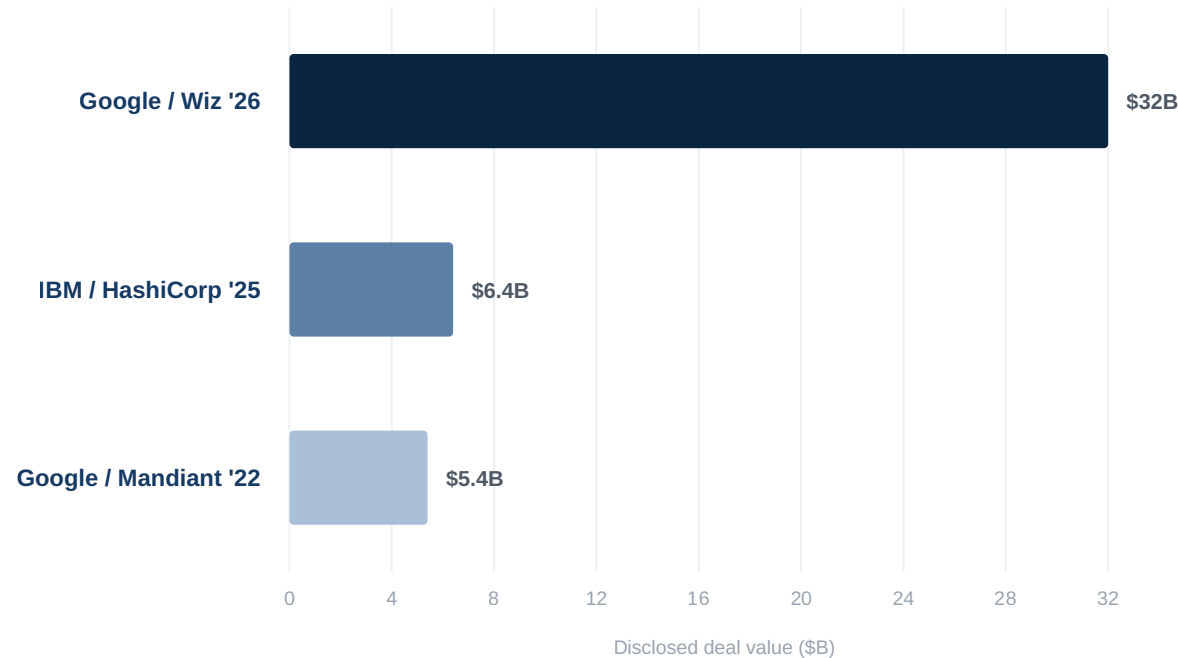
■ Moderate / Opportunistic

■ Low Activity / Niche Only

Cloud Security M&A: The Hyperscaler Land Grab

Cloud security is the highest-value cybersecurity subsector, led by hyperscalers buying category leaders outright.

Representative Transactions, Disclosed Deal Value



Deal Drivers

Hyperscaler Demand

Cloud providers are acquiring the leading cloud-native security platforms to embed protection directly into their infrastructure rather than build it.

Posture and Runtime Converge

Cloud posture management, data security and runtime protection are consolidating into single platforms, and buyers pay for the converged asset.

Scarcity of Scaled Assets

Few cloud security companies have reached genuine scale, so the proven category leaders command outsized, scarcity-driven valuations.

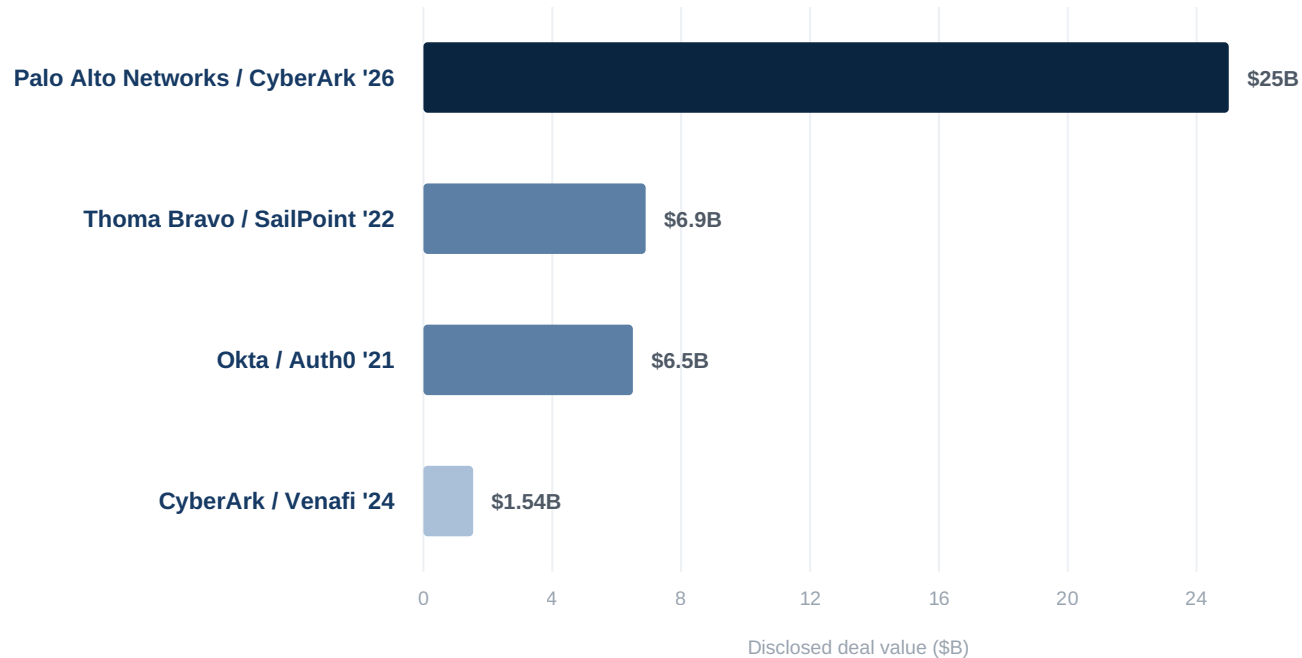
KEY OBSERVATION

Cloud security megadeals carry a disproportionate share of total cybersecurity M&A value, anchored by the \$32B Google and Wiz transaction.

Identity & Access Management M&A

Identity has become the control layer of the AI era, and the most contested platform pillar in cybersecurity M&A.

Representative Transactions, Disclosed Deal Value



Deal Drivers

Identity as Architecture

Platform vendors now treat identity as the core control layer, not a feature, and are paying platform-defining sums to own it.

Machine Identity Surge

Agentic AI and machine-to-machine traffic multiply non-human identities, making machine-identity and secrets management a priority acquisition theme.

Sponsor Appetite

Private equity competes hard for identity assets, drawn by high recurring revenue, strong retention and durable switching costs.

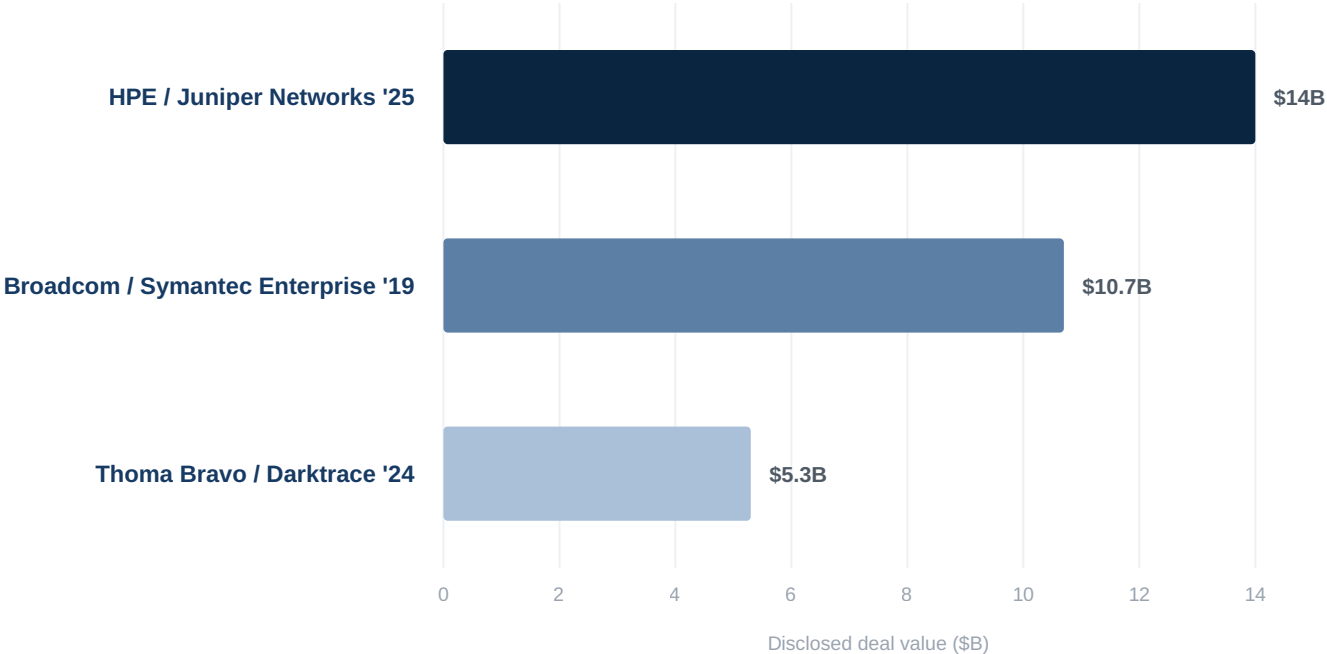
KEY OBSERVATION

Identity is the clearest scarcity premium in cybersecurity: the assets are few, the strategic logic is universal, and the buyer pool is deep.

Network Security M&A: Convergence and Scale

Network security M&A pairs networking scale with AI-driven defence, with private equity an active third bidder.

Representative Transactions, Disclosed Deal Value



Deal Drivers

Networking Meets Security

Infrastructure vendors are combining networking with security so that secure connectivity is delivered as a single, AI-native stack.

AI-Native Defence

Buyers pay for autonomous detection and response built into the network, the capability that distinguishes a modern network security platform.

Take-Private Pressure

Mature network security vendors trading below intrinsic value are prime private equity take-private targets, as the Darktrace deal showed.

KEY OBSERVATION

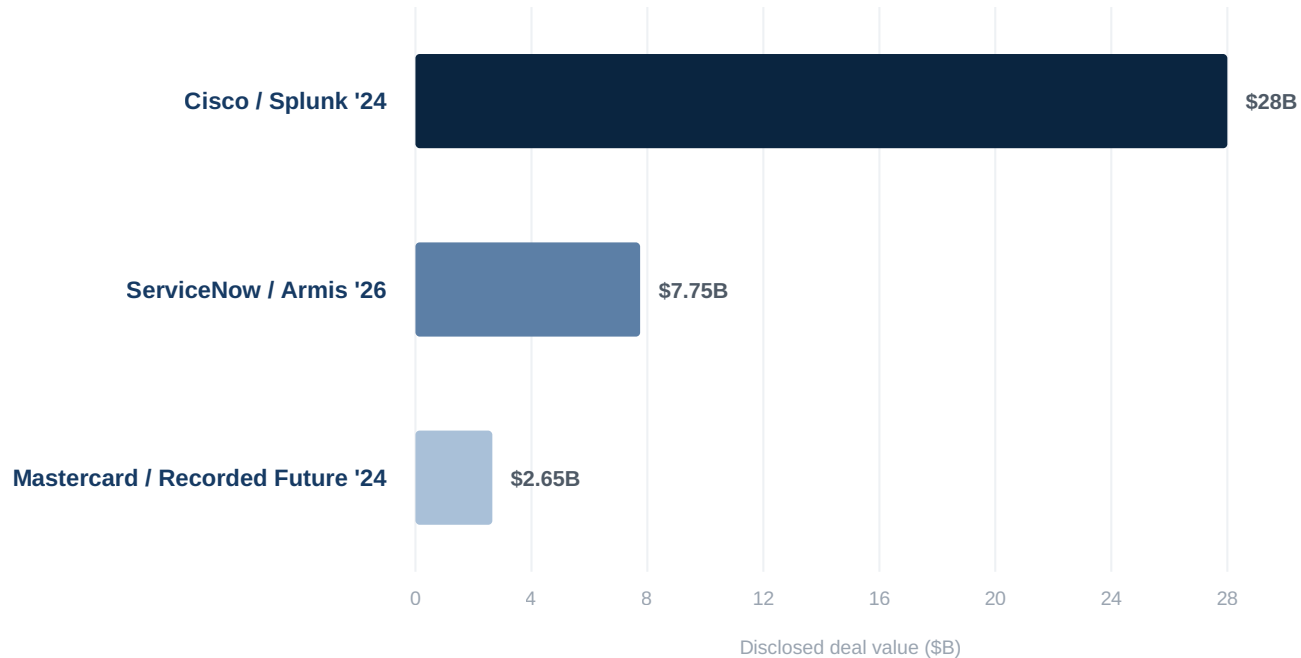
Network security M&A is a scale story: large infrastructure combinations on one side, sponsor-led take-privates of mature platforms on the other.

Sources: company and SEC filings; CB Insights; PitchBook. See appendix.

Security Operations & Threat Detection M&A

Security operations M&A consolidates detection, exposure and threat intelligence into unified, AI-driven platforms.

Representative Transactions, Disclosed Deal Value



Deal Drivers

Platform Consolidation

Buyers are merging detection, response, exposure management and threat intelligence into single platforms to reduce enterprise tool sprawl.

Exposure Management Rises

Asset visibility and cyber exposure management have become priority acquisitions as connected IT, OT and device estates expand.

Intelligence as Infrastructure

Threat intelligence is increasingly bought by adjacent strategics, including financial-services groups extending fraud and risk defence.

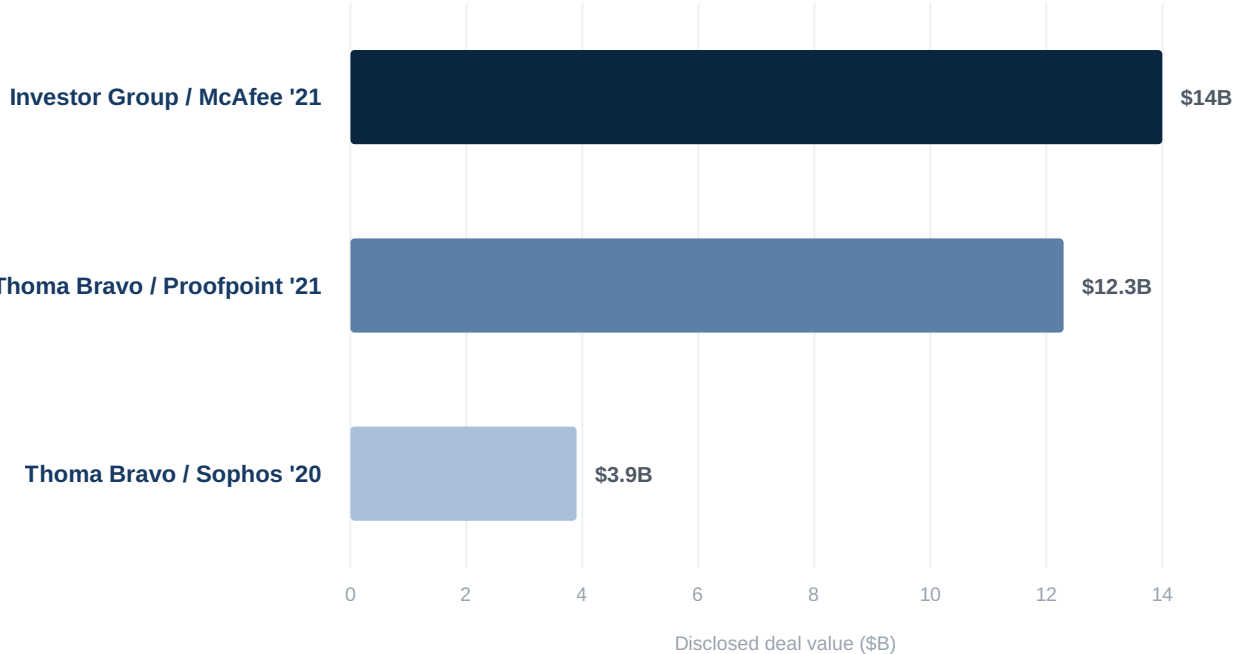
KEY OBSERVATION

Security operations M&A is driven by consolidation: enterprises want fewer, smarter platforms, and buyers are assembling them through acquisition.

Endpoint & Email Security M&A: Sponsor Territory

Endpoint and email security is mature, cash-generative and the natural home of private equity take-privates.

Representative Transactions, Disclosed Deal Value



Deal Drivers

Mature, Cash-Generative

Endpoint and email security platforms generate strong recurring cash flow, the profile that supports leverage and a take-private thesis.

Private Equity Leadership

Specialist sponsors have repeatedly taken endpoint and email vendors private, then driven value through pricing and buy-and-build.

AI Refresh Cycle

AI-driven phishing and deepfake threats are reviving demand for modern email and endpoint defence, supporting renewed buyer interest.

KEY OBSERVATION

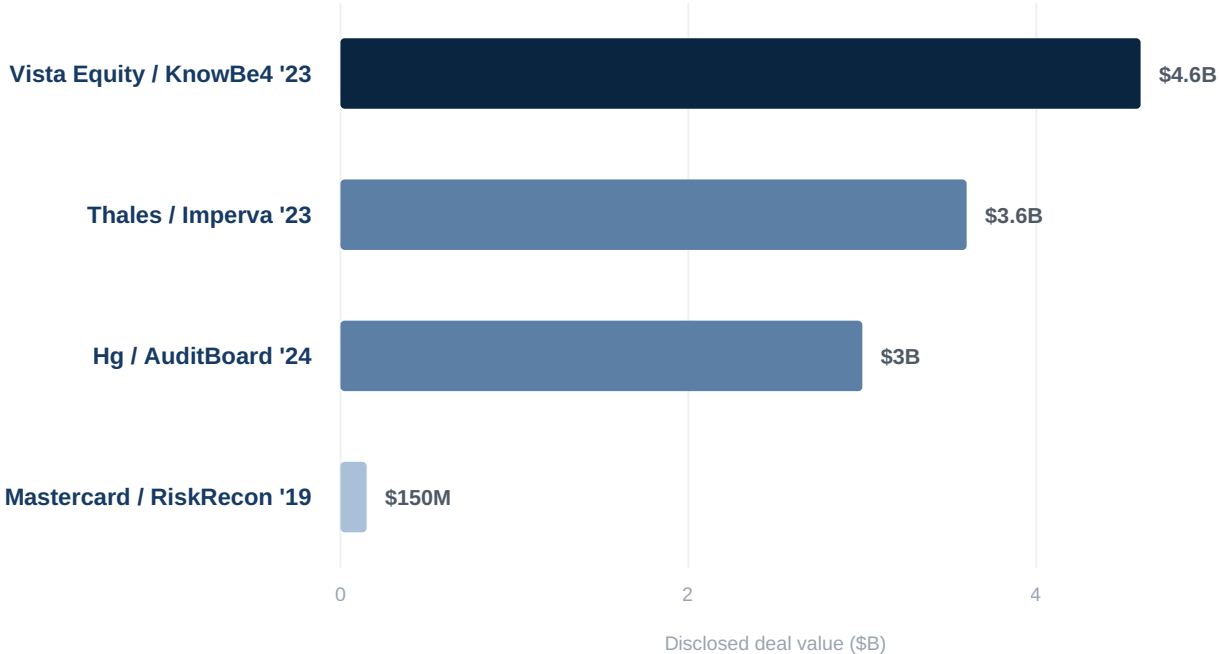
Endpoint and email security M&A is led by private equity, which prizes the segment's recurring revenue and resilient cash generation.

Sources: company and SEC filings; CB Insights; PitchBook. See appendix.

Data Security & GRC M&A

Data security and governance M&A is high in deal count, with values clustered well below the platform megadeals.

Representative Transactions, Disclosed Deal Value



Deal Drivers

Data Security Posture

Securing data across sprawling cloud estates is a fast-growing gap, and posture and classification assets attract strong strategic interest.

GRC Consolidation

Governance, risk and compliance software saw heavy deal activity in 2025, with private equity consolidating fragmented point solutions.

High Count, Lower Values

Data security and GRC generate many transactions, but disclosed values cluster well below the cloud and identity megadeals.

KEY OBSERVATION

Data security and GRC are volume subsectors: the deal count is high, the strategic logic is clear, but values sit below the platform megadeals.

Sources: company and SEC filings; CB Insights; PitchBook. See appendix.

Comparable Transaction Analysis Framework

WINDSOR DRAKE

A rigorous quality-of-revenue filter rather than broad industry codes.

1. Select Peer Set

Identify genuinely comparable transactions by fundamental business characteristics: model, revenue quality, growth profile and buyer type, never by broad sector labels alone.

2. Normalise the Deal

Adjust for deal structure: consideration mix, earn-out weighting and assumed liabilities, to recover the true economic value behind a headline figure.

3. Calibrate the Premium

Apply a control-premium layer, typically 20 to 30%, where cost and revenue synergies can be concretely underwritten by a strategic buyer.

Proprietary Transaction Index

Calibration draws on the firm's proprietary index of **verified and reported cybersecurity transactions (2019-2026)**, refreshed each quarter.

Quality-of-Revenue Filter

Peer selection prioritises net revenue retention, gross-margin profile and customer-concentration risk over headline scale.

Strategic-Fit Weighting

Comparable sets weight transactions by strategic rationale, since platform-gap buys and scale deals price on different logic.

Confidence Grading

Every tracked deal is graded Verified, Reported or Estimated, so calibration leans on the best-evidenced transactions.

6

SUBSECTORS TRACKED

2019-26

INDEX COVERAGE

Security Platform Vendors as Buyers

WINDSOR DRAKE

Platform vendors are acquiring to close suite gaps and consolidate enterprise security spend.

Strategic Motives: Buy vs. Build

Enterprises are consolidating onto fewer security platforms, so the leading vendors must offer a complete suite. The internal build cycle is too slow to match that demand, which makes acquisition the default route to platform completeness.

Acquisition Patterns

Vendors pursue both platform-defining megadeals, such as Palo Alto Networks and CyberArk, and a steady cadence of capability tuck-ins that round out specific gaps in the suite.

Platform

THE PRIMARY MOTIVE

Suite gap

WHAT BUYERS TARGET

Priority: Identity

Identity is the most contested pillar; platform vendors are paying platform-defining sums to own the control layer of the AI era.

Priority: Cloud Security

Cloud posture, data and runtime protection are essential suite components, and the scaled assets are scarce and richly valued.

Priority: AI Security

Securing AI models, agents and pipelines is an emerging gap that vendors are racing to fill through early, often smaller, acquisitions.

Capability Tuck-Ins

Alongside the megadeals, vendors run a steady cadence of smaller deals to close precise feature gaps before competitors do.

Private Equity Acquisition Patterns

WINDSOR DRAKE

Record dry powder is pushing sponsors deep into cybersecurity through take-privates and roll-ups.

Deployment Pressure

With roughly \$3.7T of global dry powder to deploy, sponsors face acute pressure to transact. Cybersecurity is a favoured destination: recurring revenue, mission-critical demand and resilient growth make it well suited to leverage.

The Take-Private Thesis

Mature security software trading below intrinsic value is a prime target. Specialist sponsors now hold multi-billion-dollar cybersecurity portfolios assembled through take-privates and add-on acquisitions.

~\$3.7T

GLOBAL DRY POWDER

Recurring

WHAT SPONSORS PRIZE

Ideal Target Profile

Sponsors prioritise high recurring-revenue mix, strong net retention and efficient growth, the profile that supports leverage capacity.

Value-Creation Playbook

Pricing optimisation, a mix-shift toward high-margin software revenue, and buy-and-build consolidation of fragmented subsectors.

Aging-Portfolio Catalyst

Many cybersecurity holdings now exceed a five-year hold, signalling a parallel wave of sponsor exits and secondary deals.

Deal Structure

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

Capability M&A: AI Security, Identity & Exposure

WINDSOR DRAKE

The fastest-growing strand of cybersecurity M&A is the acquisition of specific technical capability.

AI-Native Detection

HIGHEST DEMAND

Buying production-grade automation

- Acquirers are buying governed, production AI, not pilots or research teams.
- Autonomous detection and response is the defining modern capability.
- The build cycle for agentic security workflows is too slow to match demand.
- **Signal:** evidence measurable analyst efficiency from deployed AI.

Securing AI Itself

EMERGING GAP

Protecting models, agents and pipelines

- AI security, model defence and AI gateways are a fast-rising target class.
- Platform vendors are acquiring early to own the emerging category.
- Agentic AI widens the attack surface that buyers must now cover.
- **Signal:** prove coverage of real model and agent attack paths.

Identity & Machine Identity

CORE PILLAR

The control layer of the AI era

- Identity is the most contested pillar in cybersecurity M&A.
- Machine and non-human identity is multiplying with agentic AI.
- Secrets management and workload identity are persistently acquired.
- **Signal:** demonstrate scale, retention and clean platform fit.

Exposure & Posture

CONSOLIDATION LEVER

Seeing and reducing the attack surface

- Asset visibility and exposure management reduce enterprise tool sprawl.
- Data security posture is a fast-growing gap across cloud estates.
- Buyers value capability that unifies what enterprises must defend.
- **Signal:** quantify the risk reduction and tool consolidation delivered.

Deal Structure & Terms

WINDSOR DRAKE

How cybersecurity transactions are being structured in the current market.

Consideration Mix

ALL-CASH RESURGENCE

Certainty is back in favour

- All-cash consideration has returned as well-capitalised buyers prize certainty.
- Google and Wiz was an all-cash transaction; cash removes financing risk.
- Stock still features where buyer and seller want aligned upside.
- **Founder note:** weigh certainty against participation in future value.

Earn-Outs

STANDARD BRIDGE

Bridging the valuation gap

- Earn-outs remain standard for AI-native and early-traction assets.
- Performance-linked tranches typically run over 12 to 24 months.
- They bridge gaps where forward growth is genuinely unproven.
- **Founder note:** negotiate clear, measurable, controllable milestones.

Control Premiums

20-30% LAYER

Paid for underwritable synergy

- Strategic control premiums typically run 20 to 30% over standalone value.
- The premium is paid only where synergies can be concretely underwritten.
- Scarce platform pillars, such as identity, can command more.
- **Founder note:** quantify the synergy case before the LOI stage.

Regulatory Remedies

DESIGNED IN

Screening planned from day one

- Cybersecurity is critical infrastructure, so screening risk is designed in.
- Large deals plan for antitrust and national-security review from the outset.
- Cross-border clearance runs 30 to 50% longer than a domestic deal.
- **Founder note:** model regulatory timelines into runway and structure.

Cross-Border M&A Considerations

Cybersecurity is treated as critical infrastructure, making screening the primary execution risk.

National-Security Screening

Because cybersecurity assets touch critical infrastructure and sensitive data, cross-border deals draw heightened national-security review. CFIUS and its equivalents are the principal source of friction and timeline risk.

The Sovereign Opportunity

The same scrutiny creates opportunity: governments and defence primes are acquiring domestic cybersecurity capability, a fast-rising sovereign-security acquisition theme in Europe.

12-18mo

CROSS-BORDER CYCLE

+30-50%

LONGER CLEARANCE

Extended Timelines

Regulatory clearance for cross-border cybersecurity deals runs 30 to 50% longer than domestic transactions; the Google and Wiz review took roughly a year.

Data Sovereignty

Data-residency rules and divergent national AI frameworks complicate integration and can shape where capability must be domiciled.

Sovereign Buyers Rising

Defence and aerospace acquirers are buying sovereign cyber capability, as Airbus did in acquiring a French security specialist in Q2 2026.

Milestone-Tied Earn-Outs

Regulatory earn-outs can unlock tranches of consideration on specific clearances or licence transfers, sharing timeline risk.

Competitive Moats That Attract Acquirers

WINDSOR DRAKE

Acquirers pay premiums for structural defensibility that they cannot quickly build.

Platform Fit

ASSET VALUE: HIGHEST

Clean integration into a suite

- Capability that slots into a buyer's platform is faster to buy than to build.
- Clean APIs and architecture make the buy-versus-build choice self-evident.
- Platform completeness is the dominant strategic logic of the cycle.
- **For the buyer:** an asset that closes a precise, declared gap.

AI-Native Operations

SCALE VALUE: HIGH

Detection that scales without headcount

- AI-driven detection and response cut the marginal cost to defend.
- Production AI is among the most-sought capabilities in 2026 M&A.
- Demonstrates operating leverage as the customer base scales.
- **For the buyer:** deployable automation across the install base.

Proprietary Threat Data

DATA VALUE: HIGH

Telemetry that compounds over time

- Unique telemetry and threat data train models rivals cannot replicate.
- Creates a virtuous cycle of detection quality and product improvement.
- Compounds in value as the install base and data history grow.
- **For the buyer:** a data advantage that is slow to recreate.

Mission-Critical Stickiness

RETENTION VALUE: HIGH

Embedded, hard to displace

- Security tooling embedded in operations carries very high switching costs.
- Strong net revenue retention signals durable, defensible demand.
- Regulated and critical-infrastructure customers rarely churn.
- **For the buyer:** a predictable, resilient revenue base.

Positioning for Strategic Acquisition

WINDSOR DRAKE

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

Platform Fit

Demonstrate a capability that fills a specific, declared gap in a named buyer's platform, 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 thoroughly, and present clean, audited financials.

Synergy Density

Quantify the revenue lift from cross-selling into the acquirer's installed base, and model cost synergies from a consolidated platform, to support a higher offer.

Strategic Buyer Mapping

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

Proof-of-Integration

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

Synergy Quantification

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

Comprehensive VDR Readiness

Build a defensive data room addressing the company's own security posture, IP and customer-concentration 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 platform demand, capital availability and reopened deal flow still holds.



Readiness & Hygiene

Q3 2026

- Audit completion to PCAOB standard
- AI governance and data-rights review
- Net retention and synergy mapping
- Clean up the cap table and option pool

KEY MILESTONE

Clean IP and security posture review



Strategic Positioning

Q4 2026

- Build the strategic buyer-targeting list
- Draft the CIM and management presentation
- Quantify the synergy case per acquirer
- Lock key-employee retention packages

KEY MILESTONE

Retention packages locked



Market Engagement

Q1 2027

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

KEY MILESTONE

Competitive bid tension



Execution & Closing

Q2 2027

- Definitive agreement negotiation
- Regulatory filings and security screening
- Confirmatory diligence support
- Closing and integration kickoff

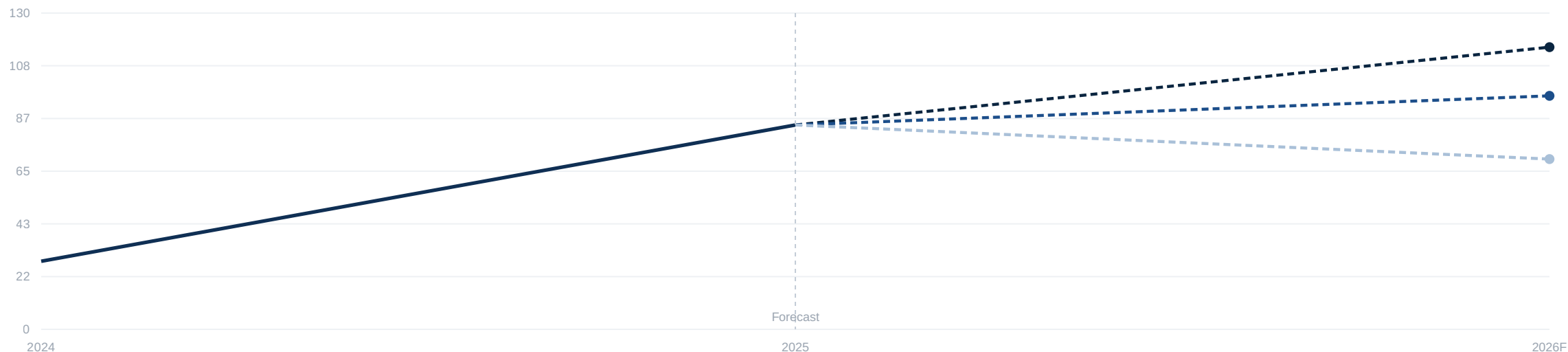
KEY MILESTONE

No-MAC event verification

2026 Cybersecurity M&A Outlook Scenarios

WINDSOR DRAKE

With 2025 disclosed value at about \$84B, the 2026 trajectory turns on rates, the IPO window and the pace of platform consolidation.



BULL CASE

~\$116B

Key Drivers

- Aggressive rate cuts and a fully open IPO window
- Platform consolidation accelerates across subsectors
- A further cloud or identity megadeal lands

IMPLICATION: A SELLER'S MARKET

BASE CASE

~\$96B

Key Drivers

- Steady rate normalisation, one further cut
- Disclosed value surpasses 2025 on steady deal count
- Platform and capability deals lead activity

IMPLICATION: A CONSTRUCTIVE MARKET

BEAR CASE

~\$70B

Key Drivers

- Inflation resurgence or a rate-cut pause
- Tighter security screening cools cross-border deals
- Buyers retreat to the smallest tuck-ins

IMPLICATION: A BUYER'S MARKET

Emerging Deal Themes

WINDSOR DRAKE

Where the next wave of cybersecurity M&A is concentrating, and what it means for sellers.

Securing Agentic AI

As autonomous agents enter enterprise workflows, buyers are acquiring AI security, model defence and AI-gateway capability, a theme moving quickly from experiment to core priority.

Machine Identity at Scale

Non-human and machine identity is multiplying faster than human identity, and secrets management and workload identity are rising acquisition targets.

Sovereign Cyber Capability

Governments and defence primes are acquiring domestic cybersecurity capability, widening the buyer pool well beyond traditional technology acquirers.

Platform Consolidation Continues

Enterprises keep consolidating spend onto fewer suites, so platform vendors will keep buying to complete the stack and defend their share.

PE Roll-Ups Intensify

Sponsors are consolidating fragmented data security and GRC software, with record dry powder still seeking deployment.

Exposure Management Scales

Asset visibility and exposure management are becoming standard platform components, sustaining a steady cadence of acquisitions.

A Demand-Led Market

Platform-completion demand and record dry powder are chasing a supply of scaled, high-quality cybersecurity assets that has not kept pace.

M&A Case Study: Google & Wiz

WINDSOR DRAKE

The defining cybersecurity transaction of the cycle, and the playbook it sets for founders.

The Platform Playbook

Google's acquisition of **Wiz**, valued at **\$32B** and closed in **March 2026**, is the largest cybersecurity acquisition ever completed. It confirms that owning a category-leading cloud security platform is now strategic infrastructure for a hyperscaler, not an optional add-on.

Strategic Rationale

- **Cloud-native fit:** embedding a leading cloud security platform directly into Google Cloud.
- **Category leadership:** acquiring the scaled leader rather than building over years.
- **All-cash certainty:** a clean, all-cash structure that absorbed a year-long regulatory review.

Implications for Founders

Scarcity Commands a Premium

Wiz was the scaled leader of its category, and scarce, category-defining assets command the cycle's largest premiums. Reaching genuine scale before a sale is what unlocks that pricing.

Platform Fit Is the Thesis

The deal was underwritten on **clean fit** into the acquirer's platform. Assets engineered to integrate, with clear architecture and a defined gap to fill, attract the strongest buyers.

Plan for the Regulatory Clock

The review ran roughly a year. In cybersecurity, **screening timelines** are now part of the deal; sellers who model them into runway negotiate from strength rather than pressure.

The M&A Readiness Mandate

WINDSOR DRAKE

Four workstreams that convert a strong company into a prepared, acquirable asset.

1. Financial Hygiene

FOUNDATION

Make the numbers diligence-ready

- Complete an audit to institutional standard well ahead of a process.
- Reconcile metrics so reported net retention survives buyer scrutiny.
- Clean the cap table, option pool and any related-party items.
- Resolve revenue-recognition and contract questions early.

2. Platform Narrative

POSITIONING

Frame the asset for a specific buyer

- Identify the precise platform gap the asset fills for each acquirer.
- Evidence governed, production-grade AI rather than pilots.
- Position as an integrable platform component, not a silo.
- Map the story to the declared strategy of the top five buyers.

3. Synergy Case

VALUE

Do the buyer's math for them

- Model revenue synergies from cross-sell into the acquirer's base.
- Quantify cost synergies from a consolidated platform.
- Present the case in the management presentation, not after.
- Anchor the price conversation on underwritable numbers.

4. Risk & Data Room

EXECUTION

De-risk before first contact

- Build a defensive VDR covering posture, IP and concentration risk.
- Pre-empt technical diligence with integration-readiness materials.
- Lock key-employee retention before the process begins.
- Model regulatory and security-screening timelines into the plan.

Appendix: Sources & Methodology (Part 1)

WINDSOR DRAKE

Institution	Report / Source	Date
S&P Global Market Intelligence	<i>Global M&A by the Numbers: Q4 2025 and Q1 2026</i>	2026
CB Insights	<i>State of Cybersecurity 2025; State of Venture Q1 2026</i>	2026
PitchBook	<i>Q1 2026 Information Security Report; Emerging Tech: Cyber</i>	Apr 2026
McKinsey & Company	<i>2026 M&A Trends: Navigating a Rebounding Market</i>	Feb 2026
McKinsey & Company	<i>Global Private Markets Report 2026</i>	Mar 2026
PwC	<i>Global M&A Industry Trends: 2026 Outlook; Technology Deals Outlook</i>	2026
Goldman Sachs	<i>2026 Global M&A Outlook</i>	Jan 2026
EY-Parthenon	<i>M&A Outlook 2026 (Deal Barometer); CEO Outlook Survey</i>	2025-26
Bloomberg	<i>Deal coverage: Google / Wiz; Palo Alto Networks / CyberArk</i>	2026
Federal Reserve	<i>FOMC Statement (Apr 2026); Summary of Economic Projections (Mar 2026)</i>	2026

Appendix: Sources & Methodology (Part 2)

WINDSOR DRAKE

Institution	Report / Source	Date
Alphabet Inc.	<i>Press release and filings, Wiz acquisition close</i>	Mar 2026
Palo Alto Networks Inc.	<i>SEC filings and investor releases, CyberArk acquisition</i>	2025-26
ServiceNow Inc.	<i>SEC Form 8-K and investor releases, Armis acquisition</i>	2025-26
Hewlett Packard Enterprise	<i>Investor releases, Juniper Networks acquisition close</i>	Jul 2025
Company filings & financial press	<i>Event reporting on Wiz, CyberArk, Armis, HashiCorp and Quarkslab (Reuters, Bloomberg, CNBC)</i>	2025-26

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

Comparable transactions are normalised for consideration mix, earn-out weighting and assumed liabilities to recover the economic value behind a headline figure.

Deal Data & the Transaction Index

Transaction analysis draws on a proprietary index of verified and reported cybersecurity deals (2019-2026), each graded for evidence quality, alongside the top-tier sources above. Deal-count and disclosed-value tallies reflect public M&A announcement tracking.

Synthesis & Attribution

Figures labelled as firm analysis or estimate, including the 2026 deal-value scenarios and size-band distribution, are the firm's own synthesis of the cited institutional data, presented as a house view rather than third-party consensus.