Cybersecurity M&A Activity: Q2 2026

Q2 2026 finds cybersecurity M&A in the richest value cycle the sector has ever recorded. The headline is not a surge in deal count but a concentration of capital: buyers are paying platform-defining sums for a thin band of category-leading assets, and the average check has stepped sharply higher even as the cadence of small deals continues. Windsor Drake characterises the current environment as a barbell market, with a high volume of capability tuck-ins at one end and a small set of transformational megadeals at the other.

The figures frame the shift. Disclosed value of pure-play cybersecurity acquisitions rose from about **$28B in 2024** to roughly **$84B in 2025**, close to a tripling, while announced deal count rose more modestly to about **426 deals**, up roughly 22% on 2024. Q1 2026 then recorded about **$47B** of cybersecurity deal value in a single quarter and **108 transactions**, the second-highest quarterly deal count on record, with the median transaction value climbing above **$300M**.

Two of the largest software transactions ever completed are cybersecurity deals. Google's **$32B** all-cash acquisition of Wiz closed in March 2026, the largest cybersecurity acquisition in history, and Palo Alto Networks' roughly **$25B** acquisition of CyberArk closed in February 2026. Eleven cybersecurity deals exceeded $1B in 2025, together carrying roughly $75B of value. The demand behind these deals is platformisation: enterprises are consolidating security spend onto fewer integrated suites, and the leading vendors and hyperscalers are acquiring to complete those platforms rather than build over years.

For founders, the central conclusion is that the strategic sale has become the default cybersecurity exit. Platform vendors, hyperscalers and private equity are all competing for assets at once, and that competition, not the IPO, is the central exit route for venture-backed cybersecurity companies. This report sets out who is buying, what is driving them, and how transactions are being structured in a market that rewards prepared, integrable assets.

What is the state of cybersecurity M&A this quarter?

The defining feature of the Q2 2026 market is the divergence between deal count and deal value. Volume is steady at a high level, yet disclosed value has stepped to a record, because capital is concentrating in a small number of platform-defining transactions. The market is paying far more for category leaders, and the distribution of activity has stretched toward its two extremes.

This is what Windsor Drake terms the barbell market. High-volume capability tuck-ins anchor one end of the distribution by count, while a thin band of platform megadeals anchors the other by value. The middle, mid-sized point solutions in the $100M to $1B range, faces the thinnest buyer pool and the longest path to exit as enterprises consolidate spend onto fewer suites.

Table 1. Cybersecurity M&A Deal Volume and Value, 2024 to 2026E

Metric	2024	2025	2026E
Disclosed value, pure-play targets	~$28B	~$84B	~$96B
Announced deal count	~405	~426	Steady
Value growth (YoY)	Baseline	Close to 3x	+14% (base case)
Median transaction value	Baseline	Rising	Above $300M (Q1 2026)

Source: S&P Global Market Intelligence; CB Insights; PitchBook; Windsor Drake analysis.

A barbell distribution

By deal count, small capability and acqui-hire transactions are the bulk of activity, and financial terms are disclosed on only a minority of deals. By value, a handful of transactions above $10B carry a disproportionate share: the eleven 2025 cybersecurity deals above $1B together accounted for roughly $75B. The squeezed middle is the strategic problem of the quarter, as mid-sized point solutions face both the thinnest buyer pool and the most acute pressure to extend toward a platform or be acquired.

Table 2. Indicative Cybersecurity M&A Deal-Count Distribution by Size Band, Q2 2026

Size Band	Share of Deal Count	Character
Tuck-in, below $100M	~66%	Capability and acqui-hire deals; the bulk of activity
Mid-market, $100M to $1B	~16%	The squeezed middle; thinnest buyer pool
Large, $1B to $10B	~13%	Platform and scale transactions
Megadeal, above $10B	~5%	Platform-defining deals; disproportionate share of value

Source: Windsor Drake analysis; directional pattern corroborated by S&P Global Market Intelligence and McKinsey & Company.

Megadeals defining the cycle

Four transactions illustrate the strategic logic of the current market. Google and Wiz is cloud security platform consolidation; Palo Alto Networks and CyberArk establishes identity as the control layer; HPE and Juniper Networks merges networking with AI-driven network security; ServiceNow and Armis adds exposure management and security operations. Together they map the rationales now driving the largest cybersecurity transactions.

Table 3. Notable Cybersecurity Transactions of the Cycle, 2025 to 2026

Transaction	Value	Timing	Strategic Rationale
Google / Wiz	$32B	Closed Mar 2026	Cloud security platform
Palo Alto Networks / CyberArk	~$25B	Closed Feb 2026	Identity as the control layer
HPE / Juniper Networks	~$14B	Closed Jul 2025	Network and infrastructure security
ServiceNow / Armis	~$7.75B	Completed 2026	Exposure and security operations

Source: Company and SEC filings; CB Insights; PitchBook.

Who is buying cybersecurity companies in 2026?

The buyer field has consolidated around the strategic acquirer. Platform vendors and hyperscalers, not financial buyers, drive the large majority of cybersecurity exits, and the strategic sale has displaced the IPO as the central exit route for venture-backed cybersecurity companies. For a well-prepared seller, the presence of three distinct buyer pools at once is the single most reliable lever on final price.

Table 4. The Cybersecurity Buyer Landscape, Q2 2026

Buyer Group	Primary Mandate	Characteristic Deal
Security platform vendors	Close suite gaps and consolidate enterprise spend	Platform megadeals and capability tuck-ins
Hyperscalers & tech platforms	Embed full-stack security into core infrastructure	Acquisition of scaled cloud and exposure leaders
Private equity	Deploy record dry powder into mature software	Take-privates and buy-and-build roll-ups
Defence & sovereign buyers	Secure domestic and sovereign cyber capability	Defence primes acquiring national security firms

Source: PitchBook; CB Insights; McKinsey & Company.

Strategic acquirer activity by subsector

The three principal buyer groups pursue different assets. Security platform vendors seek capability that fills a declared suite gap; hyperscalers seek cloud depth and exposure intelligence; private equity targets cash flow and consolidation. Cloud security and identity draw the highest activity, while endpoint and email security is the natural home of the sponsor take-private.

Table 5. Strategic Acquirer Activity by Subsector, Q2 2026

Subsector	Platform Vendors	Hyperscalers	Private Equity
Cloud Security	High	High	Moderate
Identity & Access	High	Moderate	High
Security Operations	High	High	Moderate
Network Security	High	Moderate	High
Endpoint & Email	Moderate	Low	High
Data Security & GRC	High	Moderate	High

Source: Windsor Drake analysis of McKinsey, CB Insights and PitchBook research.

Why platform vendors are buying

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. Vendors pursue both platform-defining megadeals, such as Palo Alto Networks and CyberArk, and a steady cadence of capability tuck-ins that close precise gaps. Identity, cloud security and the emerging field of securing AI itself are the priority targets.

Why private equity is active

With roughly $3.7T of global dry powder to deploy, sponsors face acute pressure to transact, and cybersecurity is a favoured destination: recurring revenue, mission-critical demand and resilient growth make it well suited to leverage. Specialist sponsors now hold multi-billion-dollar cybersecurity portfolios assembled through take-privates and add-on acquisitions. Mature security software trading below intrinsic value is the prime target, and aging 2020 to 2022 vintages are pushing sponsors toward exits in parallel.

What is driving cybersecurity dealmaking?

Four forces explain the concentration of capital in the current market. The first two sit on the demand side and shape what buyers want; the second two are macro conditions that determine how much they can spend.

Platformisation and identity

Enterprises are consolidating security spend onto integrated platforms, and identity has emerged as the architecture of that consolidation. Palo Alto Networks acquired CyberArk to make identity a core platform pillar, and agentic AI is multiplying the machine and non-human identities that must be secured. Identity assets command the clearest scarcity premium in the sector because the scaled assets are few and the strategic logic is universal.

Cloud security consolidation

Hyperscalers are buying their way to full-stack cloud security. Google's $32B purchase of Wiz anchors cloud-native security inside Google Cloud, and IBM's $6.4B acquisition of HashiCorp adds infrastructure security and automation for hybrid cloud. Cloud posture, data security and runtime protection are converging into single platforms, and the build cycle is too slow, so incumbents are acquiring the category leaders outright.

A reopening market

The broad M&A backdrop is the most constructive since 2021. Goldman Sachs forecasts about $3.8T of global M&A in 2026, and EY-Parthenon finds 62% of US CEOs plan to pursue M&A, up 27 points. Rate stabilisation and reopened capital markets are lifting confidence, and cybersecurity is one of the few technology segments holding premium valuations through the cycle. Record private equity dry powder, roughly $3.7T globally, adds a second, parallel source of demand.

Table 6. Cybersecurity M&A Demand Drivers, Q2 2026

Driver	Mechanism	Evidence
Platformisation & identity	Buy capability to complete an integrated suite	Palo Alto Networks / CyberArk; identity as control layer
Cloud security consolidation	Hyperscalers embed native full-stack security	Google / Wiz; IBM / HashiCorp
Private capital pressure	Record dry powder seeking deployment	~$3.7T global PE dry powder; sponsor take-privates
A reopening market	Rate stability and converged expectations	~$3.8T forecast global M&A; 62% of CEOs plan M&A

Source: McKinsey & Company; Goldman Sachs; EY-Parthenon; PwC; S&P Global Market Intelligence.

Geographic distribution

North America anchors cybersecurity M&A, featuring in roughly two thirds of deals on the strength of the deepest pool of platform acquirers and the largest share of targets. Europe is the second deepest pool at roughly a quarter of deal count, with sovereign-security transactions a rising theme. Israel punches far above its size as a source of acquired innovation: the cycle's two defining assets, Wiz and CyberArk, are both Israeli-founded companies.

How are cybersecurity deals being structured?

Deal structure in 2026 reflects a market where buyers are well capitalised and want certainty, but valuation gaps on AI-native and early-traction assets still need bridging. The result is a return of all-cash consideration

alongside the continued use of earn-outs, with control premiums reserved for synergy that can be concretely underwritten.

Consideration and earn-outs

All-cash consideration has returned as well-capitalised buyers prize certainty and remove financing and share-price risk; the $32B Google and Wiz transaction was all-cash. Stock still features where buyer and seller want aligned upside, as in the cash-and-stock structure of Palo Alto Networks and CyberArk. Earn-outs remain standard for AI-native and early-traction assets, with performance-linked tranches typically paid over 12 to 24 months to bridge gaps where forward growth is genuinely unproven.

Control premiums and synergy

Strategic control premiums typically run 20 to 30% over standalone value, but the premium is paid only where synergies can be concretely underwritten, and scarce platform pillars such as identity can command more. Vague strategic fit no longer commands a premium on its own. Headline values rest on identifiable cross-sell and consolidation synergies, and the synergy case belongs in the management presentation, quantified before the LOI stage rather than after it.

Table 7. Cybersecurity Deal Structure and Terms, Q2 2026

Element	Current Market Practice	Founder Consideration
Consideration mix	All-cash resurgence; stock where upside is shared	Weigh certainty against future participation
Earn-outs	Standard for AI-native and early-traction assets, 12 to 24 months	Negotiate clear, measurable, controllable milestones
Control premium	Typically 20% to 30% over standalone value	Quantify the synergy case before the LOI
Regulatory remedies	Antitrust and security screening designed in from the outset	Model screening timelines into runway and structure

Source: McKinsey & Company; EY-Parthenon; company filings.

Cross-border considerations

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 regulatory clearance runs 30 to 50% longer than a domestic transaction: the Google and Wiz review took roughly a year. The same scrutiny creates opportunity. Governments and defence primes are acquiring domestic cybersecurity capability, a fast-rising sovereign-security theme, and milestone-tied earn-outs can release consideration on specific clearances or licence transfers.

The 2026 outlook

With 2025 disclosed value at about $84B, the 2026 trajectory turns on rates, the IPO window and the pace of platform consolidation. Windsor Drake's base case sees disclosed value surpassing 2025 as platform and capability deals lead activity. A full sale process runs 12 to 18 months end to end, so a founder who intends to meet this market while the current alignment of platform demand, capital availability and reopened deal flow still holds is, in practice, preparing in the present cycle.

Table 8. 2026 Cybersecurity M&A Outlook Scenarios

Scenario	2026 Disclosed Value	Key Conditions	Implication
Bull case	~$116B	Aggressive rate cuts, open IPO window, a further megadeal	A seller's market
Base case	~$96B	Steady rate normalisation, platform and capability deals lead	A constructive market
Bear case	~$70B	Inflation resurgence or rate-cut pause, tighter security screening	A buyer's market

Source: Windsor Drake analysis; Goldman Sachs and EY-Parthenon outlooks; S&P Global Market Intelligence.

Key takeaways for founders

Translating the M&A picture into strategy means concentrating on six areas that consistently determine outcomes in the current market.

1. Treat the strategic sale as the default

Platform vendors, hyperscalers and sponsors are all competing for cybersecurity assets, which makes a strategic sale the central exit path well ahead of the IPO. Map your capability against the declared platform gaps of named acquirers, and engineer the asset to be acquirable, not only fundable.

2. Lead with platform fit, not 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, and evidence clean integration paths and governed, production-grade AI rather than pilots.

3. 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 and present the synergy case in the management presentation, doing the buyer's math for them.

4. 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 and negotiate clear, measurable earn-out milestones up front.

5. If you are a point solution, choose deliberately

In a platformising market, single-feature vendors face a clear 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 and the squeezed middle widens.

6. Respect the lead time

A full process runs 12 to 18 months end to end, with six to nine months of preparation alone. Capturing the current constructive market, while platform demand, capital availability and reopened deal flow remain aligned, requires diligence readiness to begin in the present planning cycle and 12 to 18 months of runway so the process can be run from strength.

Sources

- S&P Global Market Intelligence, global M&A and cybersecurity deal analyses
- CB Insights, State of Cybersecurity and State of Venture research
- PitchBook, information security M&A and venture data
- McKinsey & Company, 2026 M&A Trends and Global Private Markets Report 2026
- PwC, Global M&A Industry Trends and Technology Deals 2026 Outlook
- Goldman Sachs, 2026 Global M&A Outlook
- EY-Parthenon, M&A Outlook 2026 and CEO Outlook Survey
- Bloomberg, deal coverage of Google / Wiz and Palo Alto Networks / CyberArk
- Federal Reserve, FOMC statement and Summary of Economic Projections
- Company and SEC filings on Wiz, CyberArk, Armis, HashiCorp and Juniper Networks