

Cybersecurity's Consolidation Wave

M&A, Market Structure, and Strategic Implications Across the Sector, 2025–2026

Prepared August 2026

Category-wide analysis, not a single subject company

Cover Note

This report is offered as a **sample of sector-level research and analysis capability**. It treats the Computer & Network Security industry as a whole: its M&A and consolidation activity, its market structure, and the strategic questions this activity should raise for companies operating in it, rather than profiling or promoting any single vendor. No subject company is referenced as the basis of the analysis; every finding below is checked against the category broadly, across at least three independent sub-segments and multiple named transactions.

All figures are drawn from public sources current as of **August 2026**: deal trackers, company and regulatory disclosures, analyst forecasts, and industry surveys. These are cited in the Sources section. Cybersecurity M&A tracking is a genuinely contested exercise: reputable trackers use different deal universes, disclosure thresholds, and taxonomies, and routinely arrive at meaningfully different totals for the same year. **Where sources disagree, this report says so and shows both figures** rather than quietly picking the more convenient one. Amounts described as market-size or spending *estimates* are exactly that: commercial forecasts that vary by provider, and are labeled accordingly. Amounts tied to a specific announced or completed transaction are treated as the closest thing to fact this market offers, sourced to company disclosures or primary deal trackers wherever possible.

This document is a work sample. It is not investment, legal, or M&A advice, and nothing in it should be read as a recommendation about any specific security.

Executive Summary

Cybersecurity M&A had a real, multi-tracker-confirmed rebound in 2025, and it has continued, on different terms, into 2026. Beyond that one-sentence version, the data gets more interesting, and more useful, the closer you look.

What the data supports

- **2025 set a record on both major trackers' own terms, exceeding the prior 2021 peak on the one series that runs back that far. They do not agree on the size of it.** On the nearest thing to a like-for-like comparison, the two most-cited trackers land close together on totals: 426 deals and \$92.5 billion of disclosed value (SecurityWeek, all deals) against 400 and \$96.0 billion (Momentum Cyber). Narrow SecurityWeek to pure-play cybersecurity and the counts diverge further rather than converging, 334 against 400. Reported year-over-year growth diverges most of all, from roughly 82% to 270% on value, because the two are working from different 2024 baselines. All of that is detailed and reconciled in Section 2.
- **The rebound is concentrated, not broad.** A small number of platform megadeals, Google/Wiz (\$32B) and Palo Alto Networks/CyberArk (\$25B) chief among them, account for a large share of 2025's disclosed value. Strategic acquirers (as opposed to private equity) deployed roughly 92% of all disclosed M&A capital in 2025 on Momentum Cyber's count, and cloud-native, SaaS-delivered targets absorbed 97% of all disclosed capital despite being only 59% of deal volume. Those two figures describe the same concentration rather than confirming it twice: Wiz and CyberArk alone are roughly \$57 billion of Momentum Cyber's \$96.0 billion total, and both were strategic acquisitions of SaaS-delivered targets. The target-profile skew is real, but it is largely the two headline deals seen from a second angle.
- **Consolidation is not the same story in every sub-segment.** Cloud security posted the highest disclosed deal value of any category (essentially one company's transaction), on one of the lowest deal counts of any tracked category. Identity saw both a megadeal and genuine depth (40-plus transactions). SOC and detection tooling consolidated quietly, mostly on undisclosed terms, around telemetry and observability data rather than classic SIEM products. Governance, risk and compliance (GRC) had the highest deal count of any of the four product categories analyzed, at the smallest average size. These are different shapes of consolidation, not one trend wearing four names. See Section 2.
- **Browser security is real but not (yet) a headline category.** Genuine, named 2025-2026 deals exist (CrowdStrike/Seraphic, Akamai/LayerX, Zscaler/SquareX), but combined disclosed value is more than an order of magnitude below cloud security or identity, and no major tracker gives it its own taxonomy line. We report it proportionately rather than force it into the top tier.
- **2026 complicates the simple growth narrative.** Deal count in the first half of 2026 was flat to record-high depending on the tracker, but disclosed deal value fell sharply: no transaction cleared \$1 billion until June's \$4.175 billion Accenture/Dragos deal. Breadth of dealmaking looks durable; 2025's record dollar total looks, so far, more like a high-water mark than a new baseline. Section 2 covers this in detail.
- **The underlying demand signal is real and independently corroborated.** Security budgets are rising by double digits (Gartner), a majority of CISOs report actively pursuing vendor consolidation, and a workforce gap last measured at 4.8 million people (ISC2, 2024) is pushing buyers toward platforms and managed services rather than more point tools. Section 4 has the detail and the honest caveats on each estimate.

How this report is organized

Section 2 lays out the consolidation data itself: headline 2025 numbers with the multi-tracker discrepancies flagged explicitly, a sub-segment breakdown across four distinct categories, an explicit note on why browser security is not treated as a fifth, and a 2026 year-to-date update. Section 3 illustrates the pattern with three named, real transactions, each checked against multiple sources. Section 4 places the M&A activity in the context of broader market sizing, growth-rate, and survey data, again flagging estimate vs. fact throughout. Section 5 turns the data into a general framework: the questions this pattern should raise for a Founder or Product Marketing leader trying to work out whether their company looks, on the evidence, like a likely acquirer, a likely target, or neither.

Market Overview & Consolidation Data

2.1. Five-year context

Cybersecurity M&A activity is well tracked but not uniformly tracked, which matters for everything that follows. On **Momentum Cyber's** own decade-long series, disclosed M&A value ran \$31.9B (2019) → \$20.6B (2020) → \$82.6B (2021, the prior peak) → \$51.5B (2022) → \$48.0B (2023) → \$25.9B (2024, the trough) → **\$96.0B (2025)**. Deal *count* peaked separately, at 455 in 2022, per **SecurityWeek's** tracker, before declining for two straight years. The two are measuring different things here, and it is worth being clear which. The value series above is Momentum Cyber's alone; SecurityWeek is cited only for count. On Momentum Cyber's numbers the shape is a 2021 value peak driven by zero-interest-rate-era exuberance, a 2023-2024 correction that cut disclosed value by roughly two-thirds from that high, and a sharp 2025 rebound to a new record. On SecurityWeek's count series the peak falls in 2022 instead, as the market kept transacting even as prices softened, followed by two years of decline and a 2025 rebound. Both call 2025 a record year on their own terms, and they disagree, sometimes sharply, on how large it was. We have not found a SecurityWeek disclosed-value series running back to 2019, so the seven-year value line in Figure 1 should be read as one tracker's view rather than a consensus.

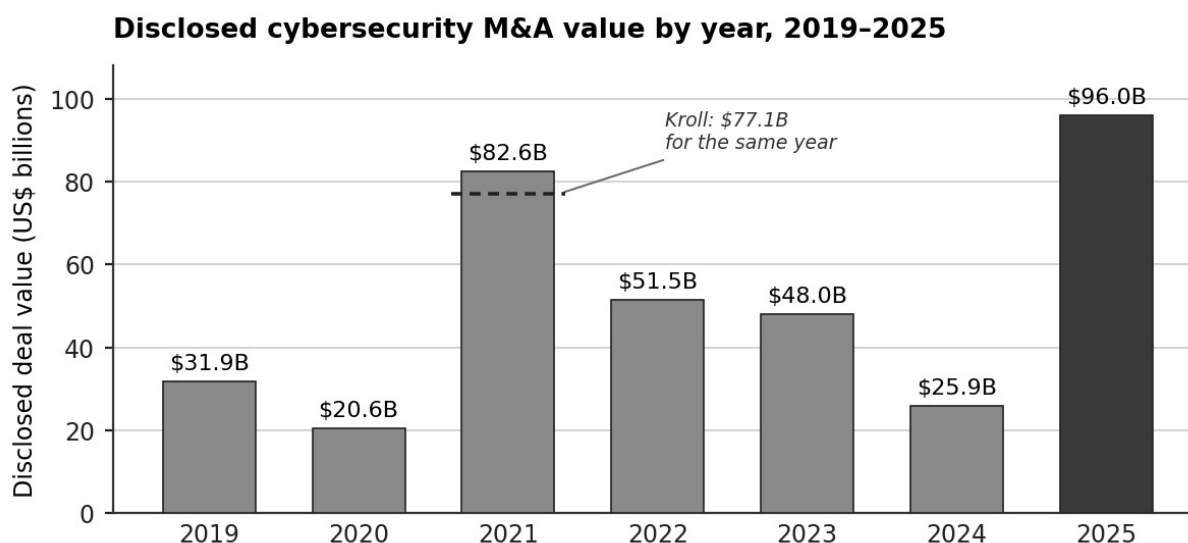


Figure 1. Disclosed cybersecurity M&A value by year, 2019-2025. Source: Momentum Cyber, *Cybersecurity Almanac: 2025 Cybersecurity M&A and Capital Markets Report*, January 2026 (Momentum Cyber's own decade-long disclosed-value series). The dashed marker on the 2021 column is Kroll's competing figure of \$77.1B for the same year: Kroll, *Cybersecurity Sector M&A Industry Insights: Fall 2025*. Deal count is tracked separately and is not shown here; on SecurityWeek's tracker, count peaked in 2022, not 2021.

2.2. 2025 headline figures: how the trackers compare

Three independent, reputable sources tracked 2025 cybersecurity M&A activity in detail. They tell the same broad story and disagree meaningfully on the specifics. That disagreement is itself the most important methodological fact in this report.

Tracker	2025 deal count	2025 disclosed value	YoY value growth	YoY volume growth
SecurityWeek	426 total (334 "pure-play")	\$92.5B across 74 deals with terms disclosed; \$84.0B among 63 pure-play deals	~82%	~5%
Momentum Cyber	400	\$96.0B	~270%	~22%
Kroll (partial year, through Q3 only)	234 (YTD Q3)	\$63.3B (YTD Q3)	n/a (partial year)	n/a (partial year)

Sources: SecurityWeek, "SecurityWeek Report: 426 Cybersecurity M&A Deals Announced in 2025," Feb. 25, 2026; Momentum Cyber, *Cybersecurity Almanac: 2025 Cybersecurity M&A and Capital Markets Report*, Jan. 2026; Kroll, *Cybersecurity Sector M&A Industry Insights: Fall 2025*.

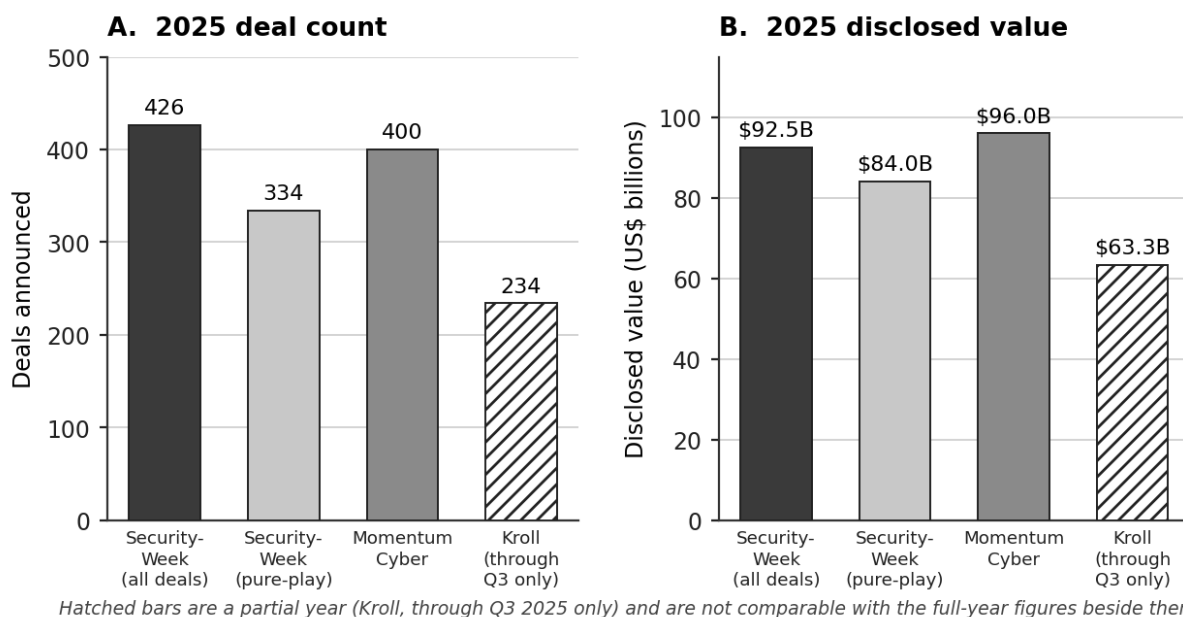


Figure 2. 2025 cybersecurity M&A: deal count and disclosed value, by tracker. Sources: SecurityWeek, “SecurityWeek Report: 426 Cybersecurity M&A Deals Announced in 2025,” Feb. 25, 2026 (both the all-deals and pure-play figures); Momentum Cyber, Cybersecurity Almanac: 2025 Cybersecurity M&A and Capital Markets Report, Jan. 2026; Kroll, Cybersecurity Sector M&A Industry Insights: Fall 2025, which covers year-to-date Q3 2025 only and is therefore not comparable with the full-year figures beside it.

Where sources disagree:

SecurityWeek and Momentum Cyber both call 2025 a record year, both flag Google/Wiz and Palo Alto/CyberArk as the two largest deals, and both put total disclosed value in a broadly similar range. But their **reported year-over-year growth rates differ by roughly 3x** (approximately 82% vs. approximately 270% on value; approximately 5% vs. approximately 22% on volume), because the two trackers use different deal universes and different 2024 baselines. SecurityWeek’s methodology counts *any deal with a cybersecurity component*, including distributors, consultancies, and diversified acquirers, and states plainly that its data “could also include some deals that may have not been completed after they were announced.” Momentum Cyber applies its own CYBERScape taxonomy of “pure” cybersecurity companies, which produces a smaller universe. Neither is wrong; they are measuring overlapping but distinct populations. Treat any single-source figure in cybersecurity M&A as an estimate bounded by a range, not a precise count, and note that even the 2021 prior-record figure is disputed: Kroll cites \$77.1B, Momentum Cyber’s own historical series shows \$82.6B for the same year.

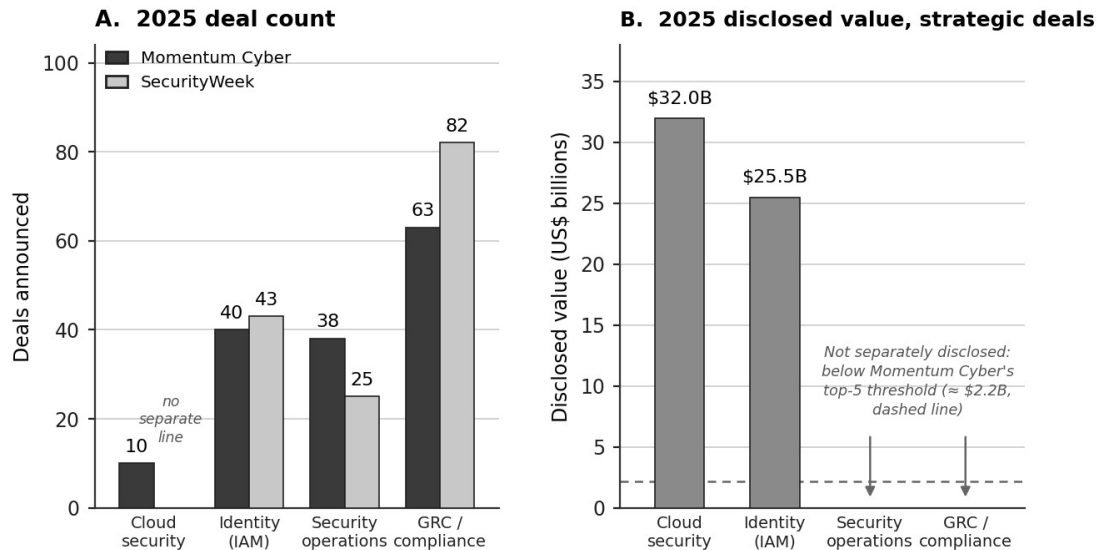
2.3. Sub-segment breakdown

Both trackers publish sub-segment detail, using different taxonomies that map only approximately onto one another, another point where forcing false precision would do readers a disservice. What both taxonomies agree on, independently, is that **consolidation is not one uniform trend**: it takes at least four distinct shapes across the sector. We focus on four categories where the 2025-2026 data is genuinely substantial: cloud security, identity, SOC & security operations / detection tooling, and governance, risk & compliance (GRC). A fifth category, security services / MSSPs, is in fact the single largest by deal count in both trackers (125-126

deals) but reflects IT-services and managed-security roll-ups more than product-technology consolidation, so we treat it as important context rather than a core focus.

Sub-category	2025 deal count	2025 disclosed value (strategic deals)	What the shape tells you
Cloud security	10 deals (Momentum Cyber), among the lowest counts of any tracked category	~\$32.0B (Momentum Cyber, strategic acquirers)	Extreme concentration: one transaction (Wiz) is effectively the entire category's disclosed value.
Identity (IAM)	40 (Momentum Cyber) / 43 (SecurityWeek), a top-3 category by count	~\$25.5B (Momentum Cyber, strategic acquirers)	Concentrated AND broad, but in different units: one megadeal (CyberArk) is roughly 98% of the disclosed value, so on dollars this is as concentrated as cloud security. The breadth is in count, 30-plus further transactions, most on undisclosed terms.
SOC & security operations / detection tooling	38 (Momentum Cyber "Security Operations"); SecurityWeek's overlapping "Incident Response" bucket shows 25, down from 38 in 2024	Not among Momentum Cyber's top five by disclosed value, which places the category below roughly \$2.2B, until the \$3.35B Chronosphere announcement in November 2025, which on its own clears that threshold	High count, quiet consolidation: most deals are undisclosed tuck-ins of data-pipeline/observability capability rather than classic SIEM products.
GRC / Risk & Compliance	82 (SecurityWeek, a 5-year peak) / 63 (Momentum Cyber, narrower definition)	Not in the top 5 by disclosed value in either tracker	Highest volume, smallest average ticket: many small compliance and posture tools being absorbed into larger platforms.

Sources: Momentum Cyber CYBERScape 4.0 sector data (2025 M&A Activity by Sector; Strategic M&A Activity by Sector); SecurityWeek 2025 M&A sub-sector data. Category definitions differ by source. See 2.4.



Panel A shows both trackers where both publish a comparable line. SecurityWeek's "Security operations" bar is its "Incident Response" bucket, which is not defined the same way as Momentum Cyber's "Security Operations"; the two counts are not strictly comparable.

Figure 3. Four sub-segments: 2025 deal count and disclosed strategic-deal value. Sources: Momentum Cyber CYBERScape 4.0 sector data (2025 M&A Activity by Sector; Strategic M&A Activity by Sector); SecurityWeek 2025 M&A sub-sector data. SecurityWeek publishes no standalone cloud-security line. Disclosed value for security operations and for GRC is not separately published by either tracker; both fall below Momentum Cyber's top-five disclosure threshold of approximately \$2.2B, so no value is plotted for them. Category definitions differ by source. See Section 2.4.

A taxonomy caveat worth taking seriously:

SecurityWeek's published sub-sector breakdown has no standalone "cloud security" line at all: cloud-security deals are distributed across its Network Security and "Other" buckets. Momentum Cyber's "Security Operations" (38 deals) and SecurityWeek's "Incident Response" (SOAR/SIEM/SOC/forensics, 25 deals, down from a 2024 peak of 38) plainly are not counting the same thing, since one shows an active, growing category and the other shows a declining one over the same period. This is not a flaw in either report. It reflects real definitional judgment calls about where CNAPP, XDR, and observability products belong, but it means a claim like "SOC tooling M&A grew X% in 2025" cannot be made cleanly from public data without naming whose taxonomy is being used. We name it throughout.

2.4. Why browser security is not treated as a headline category here

Vendor narratives in 2025-2026 gave browser security outsized attention, and it is worth checking that against the deal data rather than assuming it. The category **does** show real, named M&A activity: CrowdStrike acquired browser-runtime security vendor Seraphic Security for roughly \$420 million in January 2026 (alongside its separate \$740 million purchase of identity vendor SGNL the same month); Akamai acquired LayerX, an AI-and-browser-security platform, for roughly \$205 million in May 2026; Zscaler acquired SquareX in February 2026 on undisclosed terms. Palo Alto Networks' 2023 purchase of Talon (reportedly \$458.6 million), which became Prisma Access Browser, was the category's opening move.

Combined disclosed value across the 2025-2026 window is roughly \$625 million on the deals named above, or about \$1.1 billion if Palo Alto's Talon purchase is counted, which strictly it should not be in a 2025-2026 window since that deal closed in 2023. On either basis it is real money, and on either basis it is more than **an order of magnitude below** cloud security or identity, concentrated entirely in bolt-on acquisitions by larger platforms

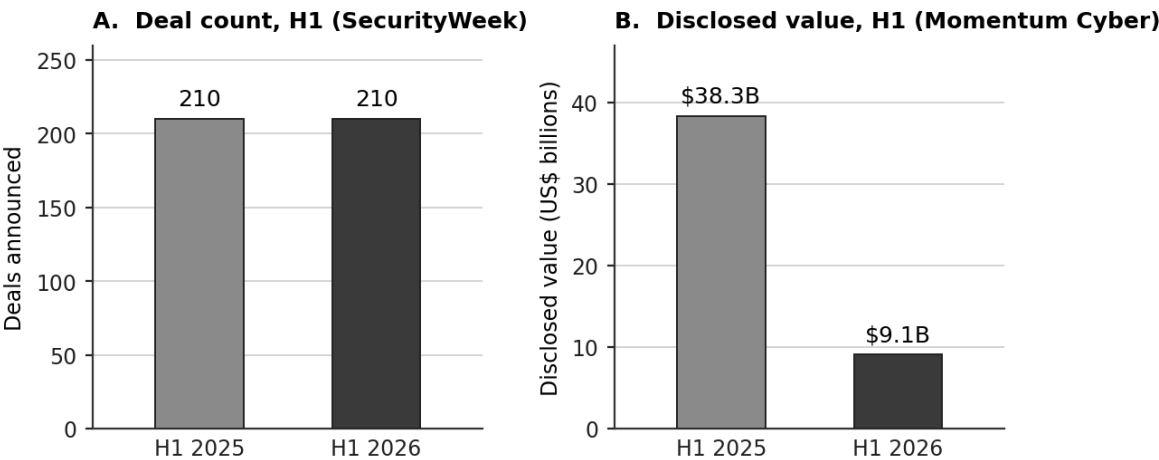
(CrowdStrike's Falcon, Zscaler's Zero Trust suite, Akamai's Zero Trust portfolio) rather than in a standalone wave of its own. Neither SecurityWeek nor Momentum Cyber gives browser security its own taxonomy line. We report this as what the evidence supports: a genuine, emerging area of feature-level consolidation, not (yet) a fifth pillar of the 2025-2026 wave.

2.5. 2026 year-to-date: a more complicated picture

With more than half of 2026 behind it as of this writing, the year does not simply extend 2025's trajectory. It complicates it in an informative way.

Tracker	H1 2026 deal count	H1 2026 disclosed value	vs. H1 2025 (same tracker)
Momentum Cyber	219, described by the firm as a record for any half-year period	\$9.1B	Value down sharply from ~\$38.3B in H1 2025 (Momentum Cyber's own Q1+Q2 2025 figures); no \$1B+ deal until June
SecurityWeek (monthly roundups, Jan–Jun 2026 summed)	210	Not separately aggregated	Exactly flat vs. SecurityWeek's own H1 2025 count of 210
Kroll (Q1 2026 only)	75	\$2.2B	Zero transactions exceeded \$1B in the quarter

Sources: Momentum Cyber, "H1 2026 Cybersecurity Capital Markets Review," July 1, 2026; SecurityWeek monthly M&A roundups, January–July 2026; Kroll, Cybersecurity Sector M&A Industry Insights: Spring 2026.



The two panels use different trackers because neither publishes a comparable half-year figure for both count and value.

Figure 4. First-half 2026 against first-half 2025: deal count and disclosed value. Sources: Panel A, SecurityWeek monthly M&A roundups, January–July 2026 (monthly totals of 34, 42, 38, 33, 26 and 37 summing to 210) against the same tracker's H1 2025 total of 210. Panel B, Momentum Cyber, "H1 2026 Cybersecurity Capital Markets Review," July 1, 2026, against Momentum Cyber's own Q1 and Q2 2025 figures. Momentum Cyber's H1 2026 count of 219 is not plotted, as that tracker publishes no comparable H1 2025 count.

Where sources disagree, and why it matters more than usual here:

Momentum Cyber frames H1 2026 as a “*record-breaking*” half-year on deal count. SecurityWeek's independently tracked monthly totals (34, 42, 38, 33, 26, 37 for January through June) sum to exactly 210, precisely flat against the same tracker's own H1 2025 total. Both statements can be true simultaneously, because each tracker is only internally consistent with itself, not with the other. The more reliable, cross-source finding is the **divergence between count and value**: Axios's Pro Rata newsletter independently headlined its July 2026 coverage “Cybersecurity M&A deal count is up, value drops for first half of 2026,” and Kroll's Q1 2026 report, from a third, independent methodology, corroborates the value-side finding directly, noting “no transactions exceeding \$1 billion” in Q1 and a moderation in disclosed value to \$2.2 billion. Three independent sources agree on the *direction* of the 2026 story even where they disagree on its magnitude.

The first \$1 billion-plus deal of 2026 did not arrive until **June**, when Accenture agreed to acquire a majority stake in OT-security firm Dragos and all of runZero and NetRise for a combined enterprise value of approximately \$4.175 billion, the largest industrial-cybersecurity deal on record (see Section 3 for related context). Nine-figure deals did happen earlier in the year, several of them named in 2.4 above; what was absent until June was any transaction at the scale that produced 2025's total. Other notable 2026 activity spans exactly the categories this report highlights: Cyera agreed to acquire non-human-identity governance firm Oasis Security for roughly \$1 billion in July; Cisco made three security-related acquisitions in H1 2026 (Astrix Security, Galileo, and WideField Security) aimed at what it calls an “Agentic SOC” for its Splunk platform; Databricks, not a traditional security vendor, acquired cloud-native SIEM company Panther Labs, continuing a pattern of adjacent enterprise-software players (ServiceNow, HPE, Databricks, Accenture) buying rather than building their way into security.

Read together, the honest interpretation is this: 2025's record *dollar total* was substantially a function of two or three unusually large platform deals landing in the same twelve months. The underlying **breadth** of dealmaking, the number of companies changing hands, looks durable and, on at least one major tracker's count, still at record levels. Whether 2025's dollar total was the start of a new normal or a cyclical high-water mark is a genuinely open question the 2026 data does not yet resolve; the more defensible claim is that consolidation itself, as a strategic behavior, is continuing, even where megadeal-driven value is not.

Deal Spotlights

Three transactions, each real, named, and independently verifiable, illustrate how the broader pattern in Section 2 played out in specific instances, one per sub-category theme. Two of the three have Palo Alto Networks as the acquirer, and that concentration in the selection is worth naming rather than glossing: Momentum Cyber lists Palo Alto Networks among the sector's most active strategic acquirers of 2025, and it is the only company to appear among the year's largest deals in two different sub-categories (identity and SOC/observability), which is a pattern in its own right. It also means a reader is getting one acquirer's strategy twice, and should discount accordingly.

Google / Wiz: Cloud Security (\$32 billion)

Google's acquisition of cloud-security platform Wiz is, on every tracker's count, the largest cybersecurity transaction ever announced. The deal has an unusually well-documented arc: Google and Wiz held earlier talks that collapsed around a reported \$23 billion offer in July 2024; talks revived, and Google announced a definitive \$32 billion all-cash agreement on March 18, 2025, an extraordinary price even by the standards of this cycle and a useful marker of what "category leadership" is worth in a hot sub-segment.

Sources disagree on the revenue multiple this implies:

Momentum Cyber's own deal-tracking table lists Wiz's trailing revenue at signing as **\$500 million, implying a 64.0x multiple**. Forbes, however, reported Wiz's ARR at **over \$700 million by the time the \$32 billion deal was signed** in March 2025, and independent deal analyses (Everest Group, Acquirify, Value Add VC) corroborate a figure in that range, implying a multiple closer to **45x-46x**. Forbes itself frames the deal's multiple as spanning **45x to 65x**, a range wide enough to bracket both figures. Two things are in play here, and we can name them without pretending to resolve them. First, these are not the same metric: Momentum Cyber's \$500 million is described as trailing revenue, while the \$700 million Forbes reports is ARR. Second, there is a vintage question, since \$500 million was Wiz's widely reported ARR around *July 2024*, when the earlier \$23 billion offer was on the table and walked away from. Whether the gap is a metric difference, a vintage difference, or both is not something the public record settles, and we are not in a position to assert that any tracker carried a stale figure forward. We report both the \$500M/64x and \$700M/45x figures rather than pick one, and treat the multiple as a range rather than a number.

The deal then spent a full year in regulatory review, an unusually long process reflecting both its size and Google's simultaneous antitrust exposure elsewhere. U.S. clearance came in November 2025; the European Commission granted unconditional approval in February 2026; the transaction closed on March 11, 2026, 358 days after the March 18, 2025 announcement and just under a full year later, folding Wiz into Google Cloud while preserving its multicloud support for AWS and Azure customers. Wiz's roughly 1,800 employees held equity valued at approximately \$3 billion at closing, with Google committing a further \$1.5 billion in retention incentives, a reminder that megadeal economics extend well beyond the headline purchase price. On every major tracker, cloud security is 2025's highest-value M&A sub-segment by a wide margin, and this single transaction is the reason why.

Palo Alto Networks / CyberArk: Identity (\$25 billion, disputed)

Sources disagree on the price of this specific deal:

Palo Alto Networks' own announcement and the great majority of press coverage value the transaction

at **approximately \$25 billion**. Kroll's Fall 2025 M&A report, by contrast, cites the deal at **\$24.1 billion** in its year-to-date tally. Both figures likely trace to the same underlying mechanism and simply differ in when they were measured: the deal's consideration was structured as \$45.00 in cash plus 2.2005 Palo Alto Networks shares per CyberArk share, so its dollar value moves with Palo Alto's own stock price between the announcement date and whatever date a given tracker struck its estimate. We report both figures rather than pick one.

Announced July 30, 2025, the acquisition of privileged-access-management leader CyberArk represented a 26% premium to CyberArk's unaffected 10-day volume-weighted average price. CyberArk's board had rebuffed an approach from Palo Alto CEO Nikesh Arora as early as May 2023; talks restarted in June 2025 and moved quickly, with a non-binding letter of interest on July 1, a counter-proposal, and a signed agreement by July 30. It was a compressed, competitive process. CyberArk's trailing revenue at signing was approximately \$1.2 billion, implying roughly a 20.8x revenue multiple, and the deal was partly funded by approximately \$15 billion in new debt. U.S. antitrust clearance came in September 2025 without a further review requirement; CyberArk shareholders approved the deal in November 2025; the transaction closed in February 2026.

Strategically, the deal is squarely about machine and “agentic AI” identity, not just human single sign-on. Arora has framed it explicitly around securing “human, machine, and agentic” identities as AI agents proliferate inside enterprises. Identity is the one sub-category in this report that shows both concentration (one megadeal drives most of the disclosed value) *and* genuine depth: more than 40 separate identity transactions were tracked in 2025 alone, and 2026 has already added CrowdStrike/SGNL (\$740M, January), Cyera/Oasis Security (~\$1B, July), and Okta/Permiso Security (~\$200M, July), among others, all organized around the same non-human/machine-identity theme.

Palo Alto Networks / Chronosphere: SOC & Detection Tooling (\$3.35 billion announced; \$2.951 billion booked)

Where the first two spotlights show mega-deal-driven categories, this one shows the quieter, more typical shape of 2025-2026 SOC/detection consolidation: still consequential, but built around infrastructure rather than headline products. Palo Alto Networks agreed to acquire Chronosphere, a cloud-native observability platform and a named Leader in Gartner's 2025 Magic Quadrant for Observability Platforms, for a total consideration announced at \$3.35 billion on November 19, 2025; the deal closed on January 29, 2026.

A caveat on the price:

The \$3.35 billion figure is what appeared in the deal announcement and in virtually all contemporaneous coverage, and is what we use elsewhere in this report for consistency with other 2025-2026 deals. But Palo Alto's own 10-Q, filed with the SEC after closing, books **total purchase consideration for Chronosphere at \$2.951 billion**, made up of cash of \$2,842 million plus \$109 million of replacement equity awards, roughly **12% below** the announced figure. This is an accounting gap, not a tracker disagreement, and Palo Alto's filing explains it: the company issued \$525 million in total replacement equity awards to Chronosphere employees, but under standard acquisition accounting only the portion attributable to service already performed before close, which is the \$109 million included above, counts as purchase consideration. The remaining roughly \$416 million is treated as compensation for *future* service and will be expensed as stock-based compensation over the following two to three years rather than booked as part of what Palo Alto paid for the company. Announced deal values and SEC-booked purchase consideration will not always match for this reason, and this is a useful, verifiable example of exactly how much they can diverge.

The strategic logic is worth stating precisely because it is not a conventional “SIEM buys SIEM” deal: Chronosphere's telemetry pipeline sits in front of Palo Alto's Cortex XSIAM security-operations platform, filtering and routing security and observability data before it is ingested. The company claims a 30%-plus reduction in data volume and up to 20x less required infrastructure versus legacy approaches. The explicit goal, in Palo Alto's own language, is to let customers “scale their security posture, not their spending” as security operations move toward autonomous, AI-driven detection. This follows Palo Alto's September 2024 acquisition of IBM's QRadar SaaS assets, the same platform-building logic applied a year earlier to a more traditional SIEM base, and it is not an isolated strategy: CrowdStrike acquired data-pipeline vendor Onum in August 2025 for the same stated purpose (feeding its own next-generation SIEM), and Databricks, a data-and-AI platform and not a security company, acquired cloud-native SIEM vendor Panther Labs in June 2026. The pattern across at least three different acquirers points to a genuine, if under-the-radar, sub-trend: security-operations platforms consolidating around who controls and pre-processes telemetry data, rather than around detection content itself.

Market Benchmarks

This section separates confirmed transaction facts (Sections 2-3) from forward-looking market sizing and survey data, which are, by nature, estimates. Commercial market-sizing research is notoriously inconsistent across providers. We show that inconsistency directly rather than picking a single number and presenting it as settled.

4.1. Overall security spending: confirmed forecasts, not confirmed facts

Gartner's most-cited figure, **\$213 billion in worldwide end-user information-security spending for 2025, rising 12.5% to \$240 billion in 2026**, comes from the firm's July 2025 forecast. That 2026 figure has been **revised upward in every subsequent quarterly update we can confirm**: to **\$244.2 billion** (up 13.3%) in Gartner's December 2025 (4Q25) update; to **\$246.2 billion** in its March 2026 (1Q26) update; and to **\$248.9 billion** (up 12.7% year-over-year against a similarly revised 2025 base) in its June 25, 2026 (2Q26) update, the most current figure we can locate as of this report. Those four vintages are not all sourced at the same standard, and we would rather say so than let the series look tidier than it is: the 3Q25 and 4Q25 numbers come from Gartner documents citable by document number, while the 1Q26 and 2Q26 figures reach us secondhand, through analyst commentary and trade coverage rather than a Gartner release we have read directly. We report them because their direction is consistent with the first two, not because we can vouch for them equally. Four vintages of the same forecast, each higher than the last, is itself the point: even a single analyst firm's own headline number moves materially as the year progresses and should always be dated, not treated as fixed. Forrester's competing estimate puts 2026 spending at “\$200 billion or more.” Cybersecurity Ventures, using a substantially broader definition of the market, has separately projected **\$522 billion for 2026**, more than double Gartner's figure. These are not really measuring the same thing: Gartner and Forrester scope to information-security spending narrowly defined, while Cybersecurity Ventures' broader “cybersecurity market” definition captures a wider set of adjacent spending. All are legitimate; none should be quoted without its source, scope, and vintage attached.

4.2. Sub-segment sizing: the estimates vary more than the deal data does

Commercial market-research estimates for the same sub-segment, in the same year, routinely differ by 20-50% depending on provider, as the table below shows, and by considerably more than that once the underlying

definition of the market changes (see Gartner against Cybersecurity Ventures in 4.1). This is normal for the industry and worth showing plainly rather than smoothing over.

Sub-segment	2025 size: range across providers	CAGR: range across providers	Illustrative sources
Identity & Access Management (IAM)	~\$22B–\$27B	~10%–16%	Grand View Research, Fortune Business Insights, Precedence Research, MarketsandMarkets
Cloud security	~\$39B–\$51B (2026 estimates spread wider, not tighter: ~\$34B–\$60B, with a floor below the 2025 floor)	~12%–18%	Grand View Research, Precedence Research, Fortune Business Insights, MarketsandMarkets
SIEM / security analytics	~\$8.4B–\$10.7B	~10%–12%	Mordor Intelligence, MarketsandMarkets, MarkWide Research
CNAPP (cloud-native app protection, a cloud-security sub-segment)	~\$10.9B (2025)	~21% to 2030	Mordor Intelligence, via Gartner Market Guide framing

Ranges reflect independently published 2025-2026 market-sizing reports; see Sources. Widely divergent estimates for the same category and year are a known feature of commercial market-sizing research, not an error in any single report.

Two figures are worth separating from the cross-provider ranges above, because they come from a single, consistently updated analyst series rather than an average of competing ones, subject to the caveat in 4.1 about how its most recent vintages reach us: Gartner's own subsegment breakdown shows **cloud security (CSPM, CASB, and CWPP combined) as its fastest-growing subsegment, at roughly 28.8% growth in 2026**. Nothing else in Gartner's eleven tracked subsegments comes close, and Cloud Security Posture Management specifically is Gartner's single fastest-growing line item, projected to grow from \$4.7 billion (2025) to \$16.2 billion (2030). That finding comes from spending data rather than deal data, and it is worth being exact about what it can carry. It does not corroborate the M&A finding in Section 2.3. Cloud security's disclosed M&A value is one transaction, and a single deal cannot be confirmed by a growth forecast. On deal count the two series point in opposite directions: the category Gartner shows growing fastest is also the one with one of the lowest transaction counts of any we track. What the spending data does support is narrower and separate: buyer demand in cloud security is growing faster than anywhere else in Gartner's series, which is a plausible reason a category leader in it commanded the price Wiz did. That is a hypothesis the deal data is consistent with, not a second methodology confirming a first.

4.3. Demand-side signals: surveys and workforce data

- **Vendor consolidation intent:** Gartner's frequently cited finding that **75% of organizations were pursuing security vendor consolidation** originates from a 2022 Gartner survey and continues to be the most recent equivalent headline figure in wide circulation as of 2025-2026, worth knowing when it is being cited as if it were new. A more recent, independent data point: the 2025 Fortra State of Cybersecurity Survey found 40% of organizations had already begun consolidating tools and vendors, with a further 21% planning to. It comes from a different survey and a different year, but points in the same direction.

- **Vendor fragmentation:** Industry vendor-tracking databases (e.g., IT-Harvest-style datasets cited across CyberDB and Momentum Cyber's own research partnership) put the number of active cybersecurity vendors at **5,000-plus**, useful context for why buyers report tool sprawl and why M&A functions, in part, as a thinning mechanism for an oversupplied market.
- **Workforce shortage:** ISC2's 2024 Cybersecurity Workforce Study documented a global workforce gap of **4.8 million professionals** (up 19% year-over-year), with 90% of organizations reporting skills shortages. Gartner separately reports managed-security-services spending as the fastest-growing services line in 2026, at 11.1% growth, which is still marginally below Gartner's own 12.7% for information-security spending overall. That makes it a demand signal within services rather than evidence that services are pulling the market. It is consistent with a link between the labor shortage and the fact that "Security Services" is the single largest M&A category by deal count in both trackers in Section 2.3, but it does not establish one.
- **AI security: a financing story more than an M&A story, so far.** Momentum Cyber and research partner IT-Harvest count 330-plus dedicated AI-security vendors as of early 2026, up from a handful in 2024, and AI security was 2025's single most-financed venture category (144 rounds). Yet it ranked only 10th of 12 categories by M&A deal count (10 deals, the same count Momentum Cyber gives cloud security in 2.3) and did not crack the top five by disclosed M&A value. Gartner separately estimates AI-amplified security spending growing from \$49 billion (2025) to \$160 billion (2029), and that more than 75% of enterprises will use AI-amplified security products by 2028, up from under 25% in 2025. Read together, this is a category where capital formation is running well ahead of consolidation, worth watching for 2026-2027 M&A activity rather than citing as already having happened.

4.4. Public markets, briefly

2025 was a positive year for publicly traded cybersecurity companies but not a market-beating one, and the dispersion inside the sector was wider than the headline: per Momentum Cyber/Pitchbook data (as of December 31, 2025), high-growth cybersecurity stocks rose roughly 10% for the year, materially behind the S&P 500 (+17%) and Nasdaq 100 (+20%), while lower-growth cybersecurity names fell roughly 7%. That is worth holding onto, because it cuts against the M&A story rather than supporting it: the sector underperformed the broad indices in the same twelve months its deal market set a disclosed-value record. Strategic appetite and public-market enthusiasm were not moving together in 2025. Individual results varied widely: Cloudflare (+83%), CrowdStrike (+37%), and Zscaler (+25%) were among the year's strongest performers. High-growth names traded at a median 12.0x EV/2025 revenue versus 4.0x for low-growth names, a valuation gap that mirrors the M&A market's own bifurcation between category leaders and everyone else (see Section 5). Two companies went public in 2025 after prior take-privates: SailPoint (re-listed at a \$12.8 billion valuation after being taken private by Thoma Bravo in 2022) and Netskope (\$7.3 billion valuation). Momentum Cyber's pre-IPO tracking separately lists more than 30 additional PE- and VC-backed candidates as a potential 2026-2027 pipeline, though which of them actually list, and when, is inherently a forecast rather than a fact.

Strategic Framework: Acquirer, Target, or Neither?

This section is a general framework, grounded in the patterns documented above. It is not advice to, or commentary on, any specific company. The honest starting point is that the 2025-2026 data supports a **three-way** outcome, not two. Alongside "we get acquired" and "we acquire others," the data shows a growing third category: companies that are *neither*: too undifferentiated to be bought at a good price and too thinly

capitalized to keep raising or growing independently. Momentum Cyber's own 2025 data is explicit about this: "elevated valuations and intense bidding for top-tier companies lengthened processes, while the number of failed sales increased for businesses that would have traded easily in prior years." That is a barbell market, not a rising tide, and it means the comfortable assumption that "someone eventually buys everyone" is not what the data actually shows.

5.1. Signals consistent with being a likely acquirer

- Genuine platform scale and an existing strategic narrative that a target's capability would deepen: not just "we have the cash," but a specific gap the market can already see. Palo Alto Networks had been building toward a telemetry-and-data-control layer for over a year, buying IBM's QRadar SaaS assets in September 2024, before Chronosphere filled the same gap at greater scale. The public evidence here is the prior acquisition, not a pre-announcement statement of need; we have not found the latter and do not claim it.
- Balance-sheet and financing capacity sufficient to both pay a platform premium and fund the integration that follows. The CyberArk acquisition alone carried a disclosed ~\$15 billion debt component, and the roughly \$416 million of Chronosphere retention equity that Palo Alto will expense after close rather than book as purchase price (Section 3) is a documented reminder that the cost does not stop at the headline number. Underestimating post-close cost is a common failure mode for first-time platform acquirers.
- A track record, or a credible plan, for integrating rather than merely owning acquired technology. The most active acquirers of this cycle bought sequentially and thematically rather than opportunistically: Palo Alto's QRadar (September 2024) then Chronosphere; Cisco's three 2026 identity/SOC deals in service of one "Agentic SOC" thesis. Whether that approach actually outperforms one-off buying is not something this report can show, since no public data used here measures integration outcomes. It is the pattern the largest buyers have chosen, which is a weaker claim and the one the evidence supports.
- Being a non-traditional entrant is not disqualifying: ServiceNow, HPE, Databricks, and Accenture all made large, credible 2025-2026 cybersecurity acquisitions despite not being pure-play security vendors. The acquirer pool in this cycle is broader than the five or six largest security companies.

5.2. Signals consistent with being a likely target (on attractive terms)

- Clear #1 or #2 position in a specific, analyst-recognized sub-category, rather than a feature set inside a category someone else already owns. The premium deals in Section 3 were paid for category leadership: Wiz in cloud security, CyberArk in privileged access management, not for technology alone.
- Real, defensible scale, though the public data supports this more loosely than it first appears. Momentum Cyber publishes a median disclosed enterprise value of \$675 million for companies with 50-plus employees at the time of sale, and \$163 million for companies in the \$10-50 million revenue band. Those are worth quoting separately rather than as a contrast: one is an employee band and the other a revenue band, they are not two halves of a single split, and the populations almost certainly overlap, so the gap between them is not a like-for-like premium and should not be read as one. What both figures are consistent with is the unsurprising direction that disclosed exit values rise with scale. Separately, companies that grew headcount an average of 99% in the 18 months before a transaction (its "momentum gainers") look nothing like the average 58% headcount decline seen among its "underperformers" over the same window before their (typically smaller, and sometimes non-existent) exits. Those two labels are assigned partly by outcome, so they describe what good exits looked like in hindsight rather than predicting which companies will have one.

- Cloud-native, SaaS-delivered architecture: 97% of 2025's disclosed M&A capital went to SaaS-native targets on Momentum Cyber's count, even though such targets were only 59% of deal volume. Being cloud-native is close to table stakes for a premium outcome in this cycle, not a differentiator on its own.

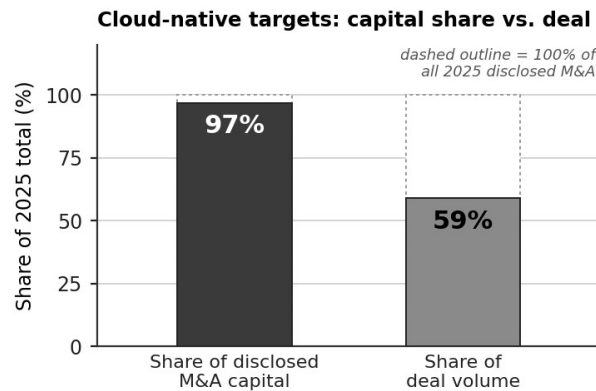


Figure 5. Cloud-native, SaaS-delivered targets: share of 2025 disclosed M&A capital against share of deal volume. Source: Momentum Cyber, *Cybersecurity Almanac: 2025 Cybersecurity M&A and Capital Markets Report*, January 2026. Both shares are percentages of Momentum Cyber's 2025 totals; they measure two different denominators (capital and deals) and do not sum.

- A capability an acquirer would find measurably harder to build than to buy within its own product cycle: not “we could build this in a year” but “this would cost us three years and we would still be behind on the dataset.” Chronosphere's pre-built, de-risked telemetry pipeline is the clearest 2025-2026 example of this logic stated explicitly by the acquirer.

5.3. Signals consistent with being neither, at least for now

This is the category most worth being honest about, because it is the one most companies are least likely to volunteer that they are in. The 2025-2026 data points to a specific, recognizable profile:

- A real but narrow point solution, without a #1/#2 position in a named category, competing on “better,” not on “only.”
- Sub-scale relative to what 2025-2026 acquirers actually targeted: the data above suggests the credible “premium exit” zone starts well above the smallest tier of company, and the same data shows failed sale processes rising specifically for smaller, less differentiated assets. That is not a hypothetical risk; it is something Momentum Cyber's own 2025 report flags directly.
- A feature that a platform incumbent is now shipping natively or absorbing by acquisition anyway (browser add-ons, posture-management dashboards, point compliance checklists): precisely the categories showing the highest deal count and the lowest average disclosed value in Section 2.3.
- Being a forced seller on a compressed timeline, which the data associates with worse terms, not better ones: “lengthened processes” and “intense bidding” in 2025 applied to top-tier assets specifically; nothing in the data suggests the same dynamic protected weaker ones.

The correct response to landing in this bucket is not comfort (“we'll get bought eventually”). The data does not support that as a base rate. It is urgency: narrowing toward defensible category leadership, building the scale and cloud-native architecture the data shows acquirers actually paying for, or deliberately building toward strategic partnership rather than acquisition as the realistic outcome.

5.4. A working checklist

Grounded in the evidence above, six questions a Founder or Product Marketing leader can ask honestly, without outside help, using only information already inside the company:

- **1. Category or feature?** Would an analyst, a competitor, or a customer name us as the #1 or #2 company in a specific, named sub-category, or would they describe what we do as a feature of someone else's platform?
- **2. Public gap or silent substitute?** If we vanished tomorrow, would a public company have to say so on an earnings call, the way the identity and telemetry-control gaps in Palo Alto's platform were visible to the market before it bought CyberArk and Chronosphere, or would our five closest competitors quietly absorb our customers within a quarter?
- **3. Is our growth still compounding, and would it survive diligence?** SaaS-native, cloud-delivered, and still-growing is close to a precondition for a premium outcome in this cycle, not a nice-to-have.
- **4. Are we a forced seller or a patient one?** Do we have 12-24 months of runway to wait for the right acquirer and the right multiple, something the data shows materially affects outcome quality, or are market or investor pressure likely to compress our timeline?
- **5. For an acquirer: do we have the integration muscle, not just the capital?** Multi-billion-dollar 2025-2026 deals carried integration costs and timelines that were a substantial fraction of the deal itself. A credible acquisition strategy prices that in before signing, not after.
- **6. For Product Marketing specifically:** does our external positioning describe a category buyers search for by name, or does it read, even to a sympathetic reader, as "a nice capability inside a bigger platform"? 2025-2026 acquirers shopped for named, specific gaps: machine identity, telemetry cost control, exposure management. A company's own public narrative about which named gap it fills is itself a strategic asset or a liability, independent of the underlying technology.

A Note on Scope

This report deliberately stays at the sector level. Every finding above is built to be checked against public sources: SecurityWeek's monthly roundups, Momentum Cyber's Almanac, Gartner's dated forecasts, Palo Alto Networks' own SEC filings, precisely *because* no single company's position ever has to be called right or wrong for the analysis to hold up.

That is also its limit. What this report demonstrates is synthesis: gathering scattered, sometimes contradictory public data, reconciling it honestly, and turning it into a framework a reader can apply for themselves. It does not attempt the harder, riskier work of making a specific, falsifiable call about one real company: whether a named company is undervalued or overpriced, well-positioned or exposed, a likely acquirer or a likely target on the specific evidence. That is what a report built for one company does differently, using the same sourcing standard shown here.

Sources

All sources were accessed in August 2026. Where a figure is disputed between sources, both are cited in the relevant section above.

M&A trackers and deal-volume data

- SecurityWeek, “SecurityWeek Report: 426 Cybersecurity M&A Deals Announced in 2025,” Feb. 25, 2026.
- SecurityWeek, “8 Cybersecurity Acquisitions Surpassed \$1 Billion Mark in 2025,” Dec. 31, 2025.
- SecurityWeek, monthly “Cybersecurity M&A Roundup” series, January–July 2026 editions.
- Momentum Cyber, Cybersecurity Almanac: 2025 Cybersecurity M&A and Capital Markets Report, January 2026.
- Momentum Cyber, “H1 2026 Cybersecurity Capital Markets Review” (press release via GlobeNewswire), July 1, 2026.
- Kroll, Cybersecurity Sector M&A Industry Insights: Fall 2025 (through Q3 2025) and Spring 2026 (Q1 2026) editions.
- Solganick, Cybersecurity M&A Market Update, Q4 2025.
- Windsor Drake, Cybersecurity M&A Report Q4 2025 (citing PitchBook, Houlihan Lokey, EY data).
- Herbert Smith Freehills Kramer, “Cybersecurity: Consolidation and Competition,” Global M&A Report 2026.
- Axios Pro Rata, “Cybersecurity M&A deal count is up, value drops for first half of 2026,” July 14, 2026.
- PRISM MarketView, “Cybersecurity M&A Surges in 2025 as Mega-Deals Redefine the Industry,” Dec. 30, 2025.

Deal-specific primary sources

- Palo Alto Networks, press release, “Palo Alto Networks Announces Agreement to Acquire CyberArk,” July 30, 2025.
- Palo Alto Networks, press release, “Palo Alto Networks Completes Chronosphere Acquisition,” Jan. 29, 2026.
- Google Cloud / Alphabet, press release, “Google Completes Acquisition of Wiz,” March 11, 2026.
- Cleary Gottlieb, “Google Completes \$32 Billion Acquisition of Wiz,” March 2026.
- Sophos, press release, “Sophos Completes Secureworks Acquisition,” Feb. 3, 2025.
- Accenture, press release, “Accenture to Strengthen Critical Infrastructure Defense...,” June 18, 2026; Dragos, “Dragos and Accenture: A New Chapter for OT Security.”
- CNBC, BankInfoSecurity, Forbes, Forrester (blog), GovConWire, DelMorgan & Co., and M&A Watch coverage of the Palo Alto Networks/CyberArk transaction, July 2025–February 2026.
- TechCrunch, Cybersecurity Dive, and SecurityWeek coverage of the Google/Wiz transaction, March 2025 and March 2026; Forbes, “Google’s \$32 Billion Wiz Purchase: Strategic Buy Or Overpriced Gamble?” Mar.

24, 2026, and “The Biggest Winners From Google's \$32 Billion Wiz Takeover,” Mar. 11, 2026 (ARR-at-signing figures).

- Cybersecurity Magazine and BankInfoSecurity coverage of the Palo Alto Networks/Chronosphere transaction, January–February 2026; Palo Alto Networks, Form 10-Q for the quarterly period ended April 30, 2026, Note 7 (“Acquisitions”), filed with the U.S. Securities and Exchange Commission (SEC EDGAR), source for the \$2.951 billion booked purchase-consideration figure.
- SecurityWeek, “Accenture to Acquire Majority Stake in Dragos, All of runZero, NetRise in \$4.1 Billion OT Cybersecurity Push,” June 2026; Help Net Security and Industrial Cyber, same transaction.

Market sizing, spending forecasts, and analyst research

- Gartner, “Gartner Forecasts Worldwide End-User Spending on Information Security to Total \$213 Billion in 2025,” July 29, 2025; Gartner, Forecast: Information Security, Worldwide, 2023-2029 (3Q25 and 4Q25 updates, Gartner document nos. 6998666 and 7291530). Subsequent 1Q26 (\$246.2B) and 2Q26 (\$248.9B, document no. G00855892, June 25, 2026) revisions as reported by Louis Columbus / softwarestrategiesblog.com and Axis Intelligence, “Cybersecurity Spending Statistics 2026,” July 2026.
- Forrester, Security Planning 2026 Budget Guide (as cited in Elisity, “Cybersecurity Budget 2026”).
- Cybersecurity Ventures, Cybersecurity Market Report 2025-2026.
- Grand View Research, Fortune Business Insights, Precedence Research, and MarketsandMarkets, respective Identity & Access Management market size reports, 2025-2026 editions.
- Grand View Research, Precedence Research, Fortune Business Insights, and MarketsandMarkets, respective Cloud Security market size reports, 2025-2026 editions.
- Mordor Intelligence, MarketsandMarkets, and MarkWide Research, respective SIEM / Security Analytics market size reports, 2025-2026 editions.
- SNS Insider, Machine Identity Security Market Size report, 2026.

Survey and workforce data

- ISC2, 2024 Cybersecurity Workforce Study, October 2024.
- Fortra, 2025 State of Cybersecurity Survey Results (as cited in TechTarget, “CISO's guide to security vendor consolidation”).
- Gartner 2022 security vendor consolidation survey (75% figure), as cited in multiple 2026 secondary sources including Digital Chiefs, “Vendor Consolidation 2026.”
- Gartner C-level Communities, 2026 CISO Leadership Perspective Survey (as reported by Evanta).