WINDSOR DRAKE

WINDSOR DRAKE RESEARCH · 2026

The Cybersecurity Consolidation Report

Windsor Drake is a sell-side M&A advisory firm focused on software, financial technology, artificial intelligence, cybersecurity, and other technology-enabled businesses in the lower middle market. The firm publishes research on transaction activity, deal structure, and valuation for founders, boards, and investors.

This report is provided for general information only. It does not constitute investment, legal, tax, or accounting advice, and it is not a recommendation to pursue or refrain from any transaction. Deal figures and valuation data are drawn from public sources, company disclosures, and Windsor Drake analysis as of June 2026, and remain subject to revision. Announced transactions referenced here may remain subject to closing conditions and regulatory review. Multiples vary widely within every category discussed; the central tendencies reported describe the sample, not any individual company. Estimates and frameworks attributed to Windsor Drake are analytical judgments, not guarantees.

About this report

This report examines the consolidation of the cybersecurity industry through 2025 and into 2026: the scale of the deal wave, the strategy driving it, who is buying, what they are paying, and what it means for founders deciding whether and when to sell. It introduces the category clock, a Windsor Drake framework for timing a cybersecurity exit against the consolidation cycle. It is intended to be read alongside the firm's cybersecurity valuation research.

CONTENTS

Contents

OVERVIEW

The year cybersecurity stopped being a market of tools

In 2025, the cybersecurity industry was reorganized by acquisition. Roughly $96 billion of mergers and acquisitions changed the shape of the sector in a single year, the average deal grew by more than 80 percent to about $2.5 billion, and the largest cybersecurity transaction in history, Google's $32 billion purchase of Wiz, was agreed and cleared.[1,2] The story of the year is not that more deals happened. It is what the deals were for: a small number of platforms buying their way to completeness, and a long tail of independent vendors discovering that their category had a closing window.

This report calls that dynamic platformization, after the term the industry itself adopted, and it traces the consequences for the companies on the other side of it.[3] The thesis is straightforward. Large security platforms are no longer assembling a portfolio of products; they are building a single architecture and acquiring whatever capability they lack to complete it. For a founder, that produces a binary outcome. A company whose capability fills a gap in a platform's architecture can command an extraordinary multiple, often two to three times the public market, while there is still a gap to fill. A company whose category the platforms have already absorbed, or built themselves, faces a collapsing standalone multiple and a shrinking buyer list.[2]

The implication is that, in cybersecurity more than in any adjacent market, the exit is a question of timing as much as of quality. A strong company taken to market while its category is contested by multiple platform buyers will clear a price that the same company cannot reach once the category is settled. The central contribution of this report is a way to read that timing, the category clock, which places each major security category in one of four phases and identifies where the exit window is open and where it has closed.

In cybersecurity, the question is no longer only whether a company is good. It is whether its category still has a gap left for a platform to buy.

The report proceeds as follows. It opens with the scale of the wave and a ledger of the defining transactions. It then examines the logic of platformization and why it produces the buy-or-be-bundled pressure that defines the moment. It identifies who is buying, separating the strategic platforms from the private equity consolidators, and what each pays. It introduces the category clock and places today's categories on it. It closes with the practical implications for founders and a near-term outlook. Throughout, the argument is the same: consolidation has changed what a cybersecurity company is worth and, more importantly, when it is worth the most.

THE MARKET IN BRIEF

Cybersecurity in numbers

$96B Cybersecurity M&A value in 2025, a record year for the sector.[1]	**+82%** Increase in average deal size, to roughly $2.47 billion.[1]	**$32B** Google's acquisition of Wiz, the largest cybersecurity deal ever.[2]
~$25B Palo Alto Networks' acquisition of CyberArk, anchoring identity as a platform pillar.[2]	**~19x** Average disclosed M&A EV/ revenue, against roughly 8x in public markets.[4]	**$100B+** Scale of the consolidation cycle now anticipated as it extends into 2026.[5]

Windsor Drake view: the headline that matters is not the $96 billion. It is the roughly two-and-a-half times premium that strategic acquirers paid over public valuations to close gaps in their platforms. That premium is the prize, and it is available only while the gap is open.

01 · THE WAVE

The consolidation wave

The 2025 deal wave was not a cyclical uptick. It was the visible surface of a structural shift in how enterprises buy security and, therefore, in how security companies are built and sold.

For most of the past decade, enterprise security was a market of point solutions. A large organization might run dozens of separate tools, each addressing a specific threat, each from a different vendor, each with its own console and contract. That fragmentation was the business model: a new threat created a new category, a new category created a wave of startups, and the best of them grew into public companies. The result was a sprawling, well-funded ecosystem of independent vendors, and a customer base quietly drowning in complexity.[3]

The 2025 wave is the market correcting that fragmentation. Enterprises, facing rising AI-enabled threats and unmanageable tool sprawl, began consolidating spend onto a small number of integrated platforms.[1,3] The platforms, in turn, raced to become comprehensive enough to win that consolidated budget, and the fastest way to fill a gap in coverage is to buy the company that leads the missing category. The deal wave is the mechanical consequence: $96 billion of acquisitions, an average deal size up more than 80 percent, and the largest transaction the sector has ever seen.[1,2]

Three forces behind the surge

The first is the threat environment. The rise of AI-enabled attacks has expanded what a complete security posture must cover, and has done so faster than any single vendor can build, which makes acquisition the only way to keep pace.[1] The second is enterprise fatigue with complexity. Buyers are actively reducing their vendor count, and a platform that can replace ten tools with one integrated architecture wins budget that a standalone product cannot.[3] The third is capital. A favorable financing environment and large balance sheets at the leading platforms made it possible to fund deals of unprecedented size, and the prospect of further activity has drawn both strategic and private equity capital into the sector.[5]

The threat environment is the accelerant

Of the three forces, the threat environment is the one that makes the cycle urgent rather than merely logical. The arrival of AI-enabled attacks has done two things at once. It has widened the attack surface, adding the security of AI systems themselves, model inputs, training data, agent behavior, to the list of things an enterprise must defend, and it has accelerated the pace at which attackers operate, compressing the time defenders have to respond.[1] Neither problem can be solved by a single vendor improving a single tool. They require coverage across the whole estate, updated continuously, which is precisely what an integrated platform is built to provide and what a collection of point solutions is not. The threat environment, in other words, is not just driving more security spend; it is driving spend toward platforms specifically, and that is what turns a gradual trend into a consolidation wave.

This is also why AI security has become the most active new front in the deal record. The same technology that is expanding the threat surface is creating the categories that defend against it, and the platforms are moving early to own them, as the Protect AI, Lakera, and Observo AI transactions show.[2] A founder watching where the threat is heading is also watching where the next contested categories, and the next premiums, will appear.

Together these forces produced a market in which the dominant transaction is no longer a financial sponsor buying a mature asset for cash flow, nor a startup selling to its nearest competitor. It is a platform buying a capability it needs to complete an architecture, and paying a strategic premium to do so before a rival closes the same gap.[2] Understanding that motive is the key to everything that follows, because it explains both the size of the premiums and the reason they do not last.

> *The wave is not more buyers wanting more companies. It is a few platforms racing to become complete, and paying up to fill the gaps before a rival does.*

The rest of this report unpacks that dynamic. The deal ledger in the next section records what the wave actually bought. The sections after it explain the strategy, identify the buyers, quantify the premiums, and set out the framework a founder needs to act on any of it.

02 · THE RECORD

The deal ledger

The transactions below define the cycle. Read together, they show platforms buying across every major category, identity, cloud, observability, threat intelligence, and the new frontier of AI security, in a coordinated push toward completeness.

EXHIBIT 1

Defining cybersecurity transactions, 2024–2026

TARGET	ACQUIRER	DATE	VALUE	CATEGORY
Wiz	Google	2025	$32B	Cloud security
Splunk	Cisco	2024	$28B	SIEM / observability
CyberArk	Palo Alto Networks	2025	~$25B	Identity security
Darktrace	Thoma Bravo	2024	$5.3B	AI network security (take-private)
Chronosphere	Palo Alto Networks	2025	$3.35B	Observability
Recorded Future	Mastercard	2024	$2.65B	Threat intelligence
Protect AI	Palo Alto Networks	2025	$700M	AI / model security
Talon	Palo Alto Networks	2023	$625M	Enterprise browser
Lakera	Check Point	2025	$300M	AI security
Observo AI	SentinelOne	2025	$225M	AI data pipeline security

Source: Momentum Cyber, company disclosures, and contemporaneous press reporting, 2024–2026.[1,2,6] Values are announced or reported figures.

Two patterns stand out. The first is the dominance of a handful of acquirers, with Palo Alto Networks alone accounting for four of the transactions above as it assembled identity, observability, AI security, and browser capabilities into a single platform.[2] The second is the arrival of AI security as a category. Protect AI, Lakera, and Observo AI are small relative to the megadeals, but they mark the platforms moving early to own the security of AI systems themselves, a category that barely existed two years ago.[2,6] Where the platforms are spending tells you which gaps they consider urgent, and the spread of these deals across categories is the clearest signal that the goal is completeness.

The ledger also understates one thing in proportion to its importance: the large number of smaller, undisclosed transactions beneath these headlines. A record set by Momentum Cyber and others counts hundreds of deals a year, most of them modest, as platforms and sponsors absorb point solutions across every subsector.[1,6] The megadeals define the narrative, but the bulk of the consolidation, and most of the exits available to lower-middle-market founders, happens in the long tail beneath them. That is the part of the market this report is ultimately written for.

The cadence is worth noting as well. Activity has not come in a single burst but as a steady stream, with trackers recording dozens of cybersecurity transactions in a typical month through 2025 and into 2026, spanning every subsector and every deal size.[1,6] That steadiness is itself a signal. It tells a founder that the consolidation is not a one-time event tied to a particular quarter or financing window, but a sustained reorganization of the industry that will continue to create, and close, exit windows across categories for some

time. The question for any individual company is therefore not whether consolidation will reach its category, but when, and whether the company will be ready to act when it does.

CASE STUDIES

Three deals that defined the cycle

Three transactions, more than any others, show the strategy at work: a cloud-security purchase, an identity purchase, and an analytics purchase, each a platform buying its way to completeness in a category it could not afford to lack.

Google and Wiz: buying the cloud-security category

Google's $32 billion acquisition of Wiz is the largest cybersecurity transaction ever recorded, and it is the clearest statement of how much a platform will pay to own a contested category outright.[2] Wiz had become the leader in cloud-native application protection, the layer that secures workloads across the major clouds, and that position made it strategically valuable to every hyperscaler at once. For Google, acquiring Wiz both completed a critical gap in its cloud security offering and denied the asset to its cloud competitors, the double effect that justifies a strategic premium. The price, and the fact that it followed an earlier, lower approach that did not close, illustrates how competition among platforms sets the number: Wiz was worth more because more than one buyer needed it.[2]

Palo Alto Networks and CyberArk: anchoring a pillar

Palo Alto's roughly $25 billion acquisition of CyberArk brought the leader in privileged access and identity security into the platform, and Palo Alto framed identity explicitly as a core pillar of its platformization strategy.[2,3] The logic is the gap-filling logic in its purest form. Identity had become indispensable to a complete security architecture, Palo Alto did not lead the category, and CyberArk was the asset that would establish it there in a single move. The deal also moved identity security from a contested category toward a settled one, which is why, on the category clock, identity now reads as absorbing rather than open. The premium Palo Alto paid was available because the category was contested at the moment it acted; the next buyer into identity will not find the same opportunity.

Cisco and Splunk: consolidating the data layer

Cisco's $28 billion acquisition of Splunk, which closed in early 2024 and helped set the tone for the cycle that followed, brought security analytics and observability under one owner.[6] Splunk's position in machine data and security information and event management made it the backbone of how many enterprises detect and investigate threats, and owning that data layer gave Cisco a central role in the security stack rather than a peripheral one. The deal is a reminder that platformization is not only about adding features; it is about

owning the layers through which a platform sees and controls everything else, and the data layer is among the most valuable of those.

> *Each deal bought a layer a platform could not afford to lack, at a price set by how many rivals needed the same thing. That is the cycle in three transactions.*

Read together, the three deals trace the same arc the rest of this report describes. A category becomes essential, the platforms compete to own it, the leader is acquired at a strategic premium, and the category moves toward settled. The founders on the other side of these transactions captured the premium because their companies were the clear leaders of categories the platforms were actively contesting. The lesson for the next founder is not to envy the size of these numbers but to understand the conditions that produced them, and to recognize those conditions forming in their own category before the window closes.

03 · THE STRATEGY

The logic of platformization

Every large transaction in the ledger serves one strategy. To understand the premiums, and to predict where they will appear next, a founder has to understand what the platforms are actually building and why it forces a choice on everyone else.

Platformization is the consolidation of many security functions into a single, integrated architecture, sold and operated as one system rather than assembled by the customer from separate products.[3] The distinction matters. A portfolio is a collection of tools a vendor happens to own; a platform is an architecture in which those tools share a data model, a control plane, and a single point of management. The leading vendors have made platformization their explicit strategy, and the acquisitions are the means of executing it.[2,3]

Why the platform wins the budget

Platformization works because it aligns with what enterprises now want to buy. Three advantages compound. The first is economic: a customer consolidating ten tools onto one platform reduces cost, vendor management, and integration overhead, and the platform captures budget that was spread across many vendors. The second is data: security improves when signal from every function flows into one model, so a platform that sees endpoint, identity, cloud, and network together detects what siloed tools miss. The third is lock-in: once a customer runs its security on one architecture, switching costs rise sharply, and the platform's revenue becomes durable in exactly the way the valuation discussion in the firm's companion research rewards.[3,4]

Why the platform must buy rather than build

If platforms could build every capability themselves, there would be no deal wave. They cannot, for two reasons. Speed is the first: the threat surface expands faster than any single engineering organization can cover, and a category leader has a multi-year head start that is cheaper to buy than to replicate.[1] Competition is the second: when several platforms are racing to complete the same architecture, the one that acquires the leading asset in a missing category denies it to its rivals as much as it adds it to itself. That competitive dynamic is what turns a fair price into a strategic premium, and it is why the same asset can command far more in a contested process than its standalone economics would justify.[2]

> *A platform that buys the leader in a missing category does two things at once: it completes itself, and it denies the category to a rival. That is what the premium pays for.*

Platformization in practice

The clearest way to see the strategy is to watch one platform assemble itself. Across the transactions in the ledger, Palo Alto Networks added identity security through CyberArk, observability through Chronosphere, model security through Protect AI, and secure browsing through Talon, each acquisition closing a specific gap in a single architecture rather than adding a standalone product line.[2] Read individually, these are four deals. Read together, they are one strategy: become the platform an enterprise can standardize on, by owning the leading capability in each function the enterprise needs. Every acquirer in the strategic field is running a version of the same play, which is why the deals cluster across categories rather than within one.

The consequence for a founder is that the relevant question about any acquirer is not what products it sells but what gaps its architecture still has. A platform with a hole in its coverage is a motivated, premium-paying buyer for the company that fills it, and a platform that has already filled that hole is not a buyer at all. Mapping the gaps of the likely acquirers is therefore the starting point for understanding who might pay the most for a given company, and when.

The customer is driving this

It would be a mistake to read platformization as a strategy imposed on the market by vendors. It is, more fundamentally, a response to what buyers are demanding. Chief information security officers spent the previous decade accumulating tools, and many now run dozens of them, each with its own console, contract, and integration burden, producing alert fatigue, coverage gaps between products, and a management overhead that does not scale.[3] The current priority for many security organizations is the opposite of acquisition: it is consolidation, reducing the number of vendors and tools to a manageable, integrated core. Platformization is the vendor side of that customer demand, and it is durable precisely because it serves the buyer's interest, not only the seller's.

This matters to a founder because it tells you the consolidation wave is not a passing financial cycle that will reverse when conditions change. It is anchored in a structural shift in how enterprises want to buy security, and that shift will continue to favor platforms over point solutions regardless of the interest-rate environment or the M&A calendar. The pressure on independents is therefore unlikely to ease, which raises the stakes on reading the timing correctly rather than waiting for the cycle to turn.

The pressure this puts on everyone else

For an independent vendor, platformization creates a stark choice that the market has come to call buy or be bundled. As platforms become comprehensive, a standalone point solution faces a customer that would rather buy the function as part of a platform it already runs than add another vendor. The independent can sell into a platform, becoming the capability that fills its gap, or it can watch the platforms build or buy an adequate substitute and bundle it for free, at which point the standalone product's growth and multiple both compress.[3,5] There is a window in which selling is highly rewarded, and a period after it in which the option closes. The category clock in Section 06 is the tool for seeing which one a company is in.

This is the core mechanism of the entire report. Platformization makes a small number of buyers willing to pay extraordinary premiums for the specific capabilities they lack, for as long as they lack them. The strategy explains the size of the deals, the concentration of the buyers, and, most importantly for a founder, why the value of an independent cybersecurity company is so sensitive to timing.

04 · THE BUYERS

Who is buying

Two very different kinds of buyer drive the cycle, and they value a company differently. Knowing which one a business is built for shapes how, and to whom, it should be sold.

The strategic platforms

The strategic acquirers are the platform builders, and they pay for capability and architecture fit. Palo Alto Networks has been the most aggressive, assembling identity, observability, AI security, and browser capabilities through acquisition as it executes platformization.[2,3] The hyperscalers have entered decisively, with Google's $32 billion purchase of Wiz the defining move, and Microsoft and Amazon building security into their cloud platforms.[2] Cisco's $28 billion acquisition of Splunk brought observability and security analytics under one roof.[6] CrowdStrike, Zscaler, Check Point, Fortinet, and SentinelOne round out the strategic field, each acquiring to extend its own platform, and system integrators such as Accenture acquire to build security services at scale.[1,2] For these buyers, the question is not the target's standalone cash flow but what it adds to the architecture and what it denies to a competitor.

The private equity consolidators

The second buyer is the financial sponsor running a buy-and-build strategy, and it values a company on cash flow, durability, and the potential to anchor or extend a platform of its own. Thoma Bravo is the archetype, having taken private a series of major security businesses and assembled them into operating platforms; its $5.3 billion take-private of Darktrace sits in the ledger above, and it has a long record across identity, email security, and beyond.[2,6] Vista, Advent, TA Associates, and Vitruvian are also active.[1] Sponsors provide a different kind of exit: they will buy profitable, durable assets that may not fit any strategic platform's immediate gap, and they often become the path to liquidity for companies the strategics are not racing to acquire.

The buy-and-build playbook

The private equity approach deserves a closer look, because it has quietly reshaped the sector in parallel with the strategic megadeals. The model is to take a strong but undervalued security business private, improve its operations and margins, acquire complementary capabilities to broaden it, and exit it later at scale, either to a strategic acquirer or back to the public market. Thoma Bravo built the template across a series of identity, email, and network security businesses, and its $5.3 billion take-private of Darktrace continues it.[2,6] The pattern matters to founders for two reasons. It creates a second, parallel buyer for assets the strategics are not racing to own, and it manufactures new strategic sellers, because a sponsor that has built a platform will eventually bring it to market, adding to the consolidation rather than resolving it.

For a lower-middle-market founder, the sponsor route is often the more realistic one. A profitable, durable niche leader that does not fit any platform's immediate gap can still be an attractive bolt-on for a sponsor assembling a portfolio, or an anchor for a new one. The valuation will be set on fundamentals rather than on a strategic premium, but the certainty and the access to a disciplined, repeat buyer are real advantages, particularly in categories where the strategic window has closed. A founder should understand both buyer types and, where possible, run a process that puts them in competition with each other.

EXHIBIT 2

Two buyer archetypes, two valuation logics

BUYER	EXAMPLES	WHAT THEY PAY FOR	IMPLICATION FOR SELLERS
Strategic platform	Palo Alto, Google, Cisco, CrowdStrike, Zscaler, Check Point	Capability, architecture fit, competitive denial	Highest multiples, but only while the gap is open
Private equity	Thoma Bravo, Vista, Advent, TA, Vitruvian	Cash flow, durability, buy-and-build potential	A path to liquidity regardless of strategic fit; priced on fundamentals

Source: Windsor Drake, from the transaction record, 2024–2026.[1,2]

The two logics produce very different outcomes for the same company. A category leader in a contested space will be worth far more to a strategic racing to fill the gap than to a sponsor underwriting cash flow, and the right process is one that brings the strategics into competition. A solid, profitable business in a category the

platforms have already settled may find its best outcome with a sponsor, priced on its fundamentals rather than on a strategic premium that is no longer available. Matching the company to the right buyer is the first decision in any cybersecurity sale, and getting it wrong leaves either money or certainty on the table.

05 · THE PRICE

What gets bought, and for how much

Cybersecurity carries the widest gap between public and acquisition multiples of any software market. Understanding where that gap comes from, and which assets capture it, is the difference between a good exit and a great one.

Public cybersecurity companies trade around eight times revenue at the median, with a wide range underneath: cloud and AI-native security in the high teens to low twenties, application security in the low-to-mid teens, data security and governance in a middle band, and legacy hardware and services at four to six times.[4] Acquisitions price far higher. Disclosed deals have averaged close to nineteen times revenue, and competitive strategic processes have cleared well above that.[4] That gap, more than two times the public multiple on average, is the platform-gap premium, and it is the single most important number in a cybersecurity sale.

EXHIBIT 3

Cybersecurity multiples: public versus acquisition

SEGMENT	PUBLIC EV/REVENUE	NOTE
Cloud / AI-native security	~18–22x	The "haves"
Application security	~13–15x	High growth
Data security / GRC	~6–8x	Middle band
Legacy hardware / services	~4–6x	The "have-nots"
Public median	~7.8x	Average ~9.2x
Disclosed M&A (average)	~18.8x	Strategic deals higher still

Source: Finro cybersecurity valuation data, Multiples.vc, and Windsor Drake cyber valuation research, Q4 2025–Q2 2026.[4]

What makes an asset capture the premium

Not every company earns the platform-gap premium. Four traits separate the assets that command it from those that do not. Category leadership is first: platforms buy the leader, not the third-place product, because the point is to own the category, not to add a redundant tool. Architecture is second: an asset built to integrate

cleanly, with a modern data model and clear interfaces, is worth more because it can be absorbed into a platform quickly, while a tangle of legacy code carries integration risk that discounts the price. Mission-criticality is third: capabilities a customer cannot operate without are stickier and more valuable than convenient add-ons. Growth is fourth: a category still growing fast signals an open, contested space, which is precisely where the premium lives.[2,4]

EXHIBIT 4

The four traits that capture the platform-gap premium

TRAIT	WHY IT MATTERS TO A PLATFORM	HOW A FOUNDER BUILDS IT
Category leadership	Platforms buy the leader to own the category, not a redundant tool	Win a well-defined niche outright rather than chase feature parity
Clean architecture	Faster, lower-risk integration means less discount and quicker value	Modern data model, clear interfaces, minimal legacy debt
Mission-criticality	Capabilities a customer cannot remove are stickier and more valuable	Embed into core workflows and the customer's security posture
Growth	A fast-growing category signals an open, contested space	Demonstrate durable expansion and strong retention

Source: Windsor Drake analysis of strategic acquisition criteria in cybersecurity, 2024–2026.[2,4]

The premium is not paid for revenue. It is paid for being the leader of a category a platform must own, built so it can be absorbed before a rival moves.

The corollary is that a company can raise its own exit multiple by building toward these traits well before a process begins: by pursuing category leadership rather than feature parity, by keeping the architecture clean and integrable, and by deepening into the parts of a customer's operations that cannot be removed. These are product and strategy decisions made years ahead of a sale, and they matter more to the eventual price than any negotiation tactic. The premium is earned in how the company is built, and captured in when it is sold.

What buyers diligence in cybersecurity

The traits that command the premium are also what a buyer's diligence is built to test, and a founder should know what will be examined before it is. Three areas receive the most scrutiny. Revenue durability comes first: net retention, gross retention, and the share of revenue under multi-year contract, because a platform is buying a stream it intends to keep, and churn undercuts the entire thesis for a strategic price. Technical integrability is second: the cleanliness of the codebase, the modernity of the data model, and the clarity of the interfaces, because the faster the asset can be absorbed into the platform, the sooner the acquirer realizes the

value it paid for, and the less it discounts for integration risk. Security and trust posture is third, and is specific to this sector: a security company is held to its own standard, and any weakness in its own controls, compliance, or track record is both a diligence finding and a reputational risk to the acquirer.

A founder who prepares these areas in advance, clean retention metrics, a defensible architecture, an unimpeachable internal security posture, both raises the price and shortens the process, because diligence that finds what it expected proceeds quickly while diligence that finds surprises stalls or re-prices. In a market where speed and certainty are part of what the buyer is paying for, being easy to diligence is itself a source of value.

06 · THE FRAMEWORK

The category clock

If platformization makes timing the central question, a founder needs a way to read the clock. The framework below places any cybersecurity category in one of four phases, each with a characteristic level of M&A premium and a clear answer to whether the exit window is open.

The logic is that every security category moves through a predictable cycle as the platforms react to it. A new threat creates a category; the category attracts startups and then platform attention; the platforms acquire or build the capability; and finally the capability becomes a standard feature that no one pays a premium for. The strategic premium, the two-and-a-half times uplift over public multiples documented in Section 05, is not available throughout that cycle. It appears in one phase and disappears in the next.

EXHIBIT 5

The category clock: four phases of a security category

1 · EMERGING	2 · CONTESTED	3 · ABSORBED	4 · COMMODITIZED
The category forms	**The platforms compete**	**The gap closes**	**It becomes table stakes**
A new threat creates a new category. Startups proliferate, no platform owns it, and the first acquisitions begin. Premiums are rising but uncertain.	Multiple platforms need the capability at once and bid against each other for the leaders. This is the peak premium and the open exit window.	The leaders are acquired or the platforms build their own. The category becomes a pillar inside platforms, and the standalone premium compresses.	The capability is bundled for free and expected by default. Multiples fall to legacy levels; remaining deals are for cash flow, not strategy.

Source: Windsor Drake framework. The exit window for a strategic premium is open primarily in the Contested phase and begins to close in the Absorbed phase.

Where today's categories sit

Applying the clock to the current market locates the opportunities and the closed doors. The most valuable observation is that the megadeals of 2025 did not open windows; they closed them. Google's purchase of Wiz

and Palo Alto's of CyberArk moved cloud security and identity from contested toward absorbed, which means the richest premiums in those categories have likely already been paid. The open windows are elsewhere.

EXHIBIT 6

Major cybersecurity categories on the clock, mid-2026

CATEGORY	PHASE	SIGNAL
AI / model security	Emerging → Contested	Early platform moves (Protect AI, Lakera, Observo); window opening
Cloud security (CNAPP)	Contested → Absorbed	Wiz to Google; richest premiums likely paid
Identity security	Absorbing	CyberArk to Palo Alto; SailPoint, Ping already with sponsors
Threat intelligence	Absorbing	Recorded Future to Mastercard
SIEM / observability	Absorbed	Splunk to Cisco; Chronosphere to Palo Alto
Endpoint (EDR)	Mature / Absorbed	Dominated by a few scaled platforms
Legacy network / firewall	Commoditized	Discounted multiples; cash-flow deals

Source: Windsor Drake analysis applying the category clock to the 2024–2026 transaction record. Phase assignments are judgments, not precise measurements.

The pattern in the table is the whole point of the framework. The categories where the megadeals just closed are the ones where a founder has likely missed the peak, while the category drawing the smallest deals today, AI security, is the one with the most open window, precisely because the platforms are early in filling that gap. A founder reading only the headlines would chase the categories that just printed huge numbers; a founder reading the clock would recognize that those numbers mark a window closing, not opening, and would look instead to where the platforms are about to compete.

Reading the clock, category by category

AI and model security, the open window. This is the category to watch, because it is early in its cycle and the platforms have only begun to move. The acquisitions so far, Protect AI, Lakera, Observo AI, are small relative to the megadeals, which is exactly the signature of an emerging category moving toward contested rather than one that has settled.[2,6] As enterprises deploy AI systems and demand security for them, the leading companies in model security, AI data protection, and agent oversight are likely to become contested, and the founders who lead those categories sit closest to the next round of premiums. The risk specific to this phase is froth: enthusiasm can price assets ahead of demonstrated demand, and not every early entrant will become the category leader a platform must own.

Cloud and identity, the windows that just closed. Cloud security and identity were the contested categories of 2025, and the Wiz and CyberArk transactions are what moved them toward settled.[2] A founder in either category today faces a thinner field of strategic buyers, because the largest gaps have been filled, and should

calibrate expectations accordingly. There remains room for smaller, complementary acquisitions as platforms round out these areas, but the category-defining premiums have likely been paid, and the realistic path for most remaining companies is a complementary sale or a sponsor exit rather than a contested strategic process.

SIEM, endpoint, and the commoditized edge. The data and analytics layer consolidated with Cisco's acquisition of Splunk, endpoint protection is dominated by a few scaled platforms, and legacy network and hardware categories have drifted into commoditization where multiples reflect cash flow rather than strategic value.[4,6] Founders in these categories should not expect a strategic premium and should plan around fundamentals, durability, and the private equity buyer, or around repositioning toward an adjacent category where a window is still open. The clock does not run backward; a settled category does not become contested again without a genuinely new threat reopening it.

FOCUS

The lower middle market view

The megadeals make the headlines, but most cybersecurity founders will never be Wiz or CyberArk. The consolidation cycle reaches them differently, and the rules for capturing it are not the same as the ones the billion-dollar deals follow.

Beneath the handful of megadeals sits the part of the market where most transactions actually happen: companies with revenue in the single-digit to low-tens of millions, sold to strategic acquirers extending a platform, to larger security vendors filling a narrower gap, or to private equity consolidators building a portfolio.[1,6] These are the companies Windsor Drake advises, and the consolidation wave shapes their outcomes as much as it shapes the giants', though the mechanics differ in three ways that matter.

The buyer is rarely the obvious one

A lower-middle-market cybersecurity company is seldom bought by Google or Palo Alto directly. It is more often acquired by a mid-sized platform extending its coverage, by a private equity-backed consolidator assembling a portfolio, or by a larger vendor that needs the specific capability and does not want to build it. The practical implication is that the buyer universe for a smaller company is both wider and less obvious than the megadeal headlines suggest, and identifying it requires mapping the gaps of dozens of mid-tier acquirers rather than watching the five names that dominate the news.

The premium is smaller but the principle holds

A smaller company will not command a $32 billion strategic premium, but the same gap-filling logic applies at its scale. A capability that a mid-sized platform needs, in a category that platform's competitors are also

eyeing, still draws a competitive premium relative to a financial-only valuation. The category clock works at every size; the absolute numbers shrink, but the difference between selling into a contested category and a settled one is just as decisive for a $30 million company as for a $3 billion one.

Architecture and focus matter more, not less

At the lower end, the traits that make a company acquirable carry even more weight, because a smaller company has less margin for the integration risk and strategic ambiguity that a buyer will discount. A clean, integrable product that clearly leads a well-defined niche is far more valuable to an acquirer than a broader but messier offering, because it can be absorbed quickly and slotted into the platform without friction. For lower-middle-market founders, the lesson is to be unambiguously the best at one thing a platform will need, rather than adequate at several.

> *The category clock works at every size. For a $30 million company, the difference between a contested category and a settled one is just as decisive as it is for a $3 billion one.*

The encouraging conclusion for smaller founders is that the consolidation wave is an opportunity, not a threat, provided it is read correctly. A market consolidating onto platforms is a market in which well-built, focused, category-leading companies are in demand, because every platform needs exactly those companies to complete itself. The risk is not being too small to matter; it is being unfocused, hard to integrate, or late to a category the platforms have already closed. The remainder of the report's guidance applies to companies of every size, with the absolute figures scaled to match.

07 · APPLICATION

What it means for founders

The framework is only useful if it changes a decision. The guidance below is organized by where a company sits on the clock, because that position should drive the strategy more than anything happening inside the company.

If your category is Emerging

The decision is whether to build toward becoming the leader a platform must buy, or to sell early to the first platform moving into the space. Building toward leadership aims at the peak premium of the Contested phase, at the cost of time and the risk that the window develops differently than expected. Selling early trades a

lower price for certainty and avoids the risk of being passed over later. Neither is wrong; the choice depends on the company's ability to win the category and the founder's appetite for the risk of waiting. What a founder should not do is treat an emerging position as a reason to delay all planning, because emerging categories can move to contested quickly.

If your category is Contested

This is the moment the report is written for. With multiple platforms needing the capability at once, the right move is a competitive process that brings those buyers into direct contention, because the premium is a function of competition, not of fundamentals alone. The window is open but not permanent, and a founder in a contested category who delays risks watching the first megadeal close the category before reaching the market. The single most valuable action available to a cybersecurity founder is to run a well-advised, competitive process while the category is genuinely contested.

If your category is Absorbing

The window is closing, and speed matters more than optimization. With the leading assets already acquired, the remaining strategic buyers are fewer and the premium is compressing, so a founder should move quickly to the buyers that still have a gap, and should prepare a private equity alternative in parallel, because the sponsor path does not depend on a strategic gap remaining open. Waiting for a better strategic offer in an absorbing category is usually waiting for an offer that will not come.

If your category is Commoditized

The strategic premium is gone, and the company should be run and sold on its fundamentals. The realistic buyer is a financial sponsor or a consolidator pricing cash flow, and the work is to present a durable, profitable business rather than to chase a strategic narrative the market will not pay for. The alternative is to reposition the company toward an adjacent emerging category, which is a genuine product strategy rather than a sale strategy and has to be undertaken well in advance.

Read the clock before you read the offers. Where your category sits decides whether to run a competitive process now, prepare a sponsor exit, or rebuild toward the next open window.

WORKSHEET

Reading your own position

QUESTION	WHAT THE ANSWER TELLS YOU
Have the major platforms already acquired the leaders in your category?	If yes, you are in the Absorbing or Absorbed phase; the strategic window is closing. If no, it may still be open.
How many platforms still lack your capability?	The count is your competitive tension. Several means a contested process is possible; one or none means the premium has largely gone.
Is your category growing fast and drawing new entrants?	Growth and new entrants signal an Emerging or Contested category, where the premium lives.
Could a platform build an adequate substitute cheaply?	If yes, you are closer to commoditization and should not count on a strategic premium.
Is your product clean and quick to integrate?	Integration ease raises the price in every phase and widens the buyer pool.

Source: Windsor Drake. Use with the category clock in Section 06 to locate the company and choose a strategy.

What holds in every phase

Two things matter regardless of position. The first is to build the company to be acquirable: a clean, integrable architecture and clear category leadership raise the price in any phase and are decided years before a sale. The second is to cultivate the buyer pool early. The set of strategic acquirers in cybersecurity is small and concentrated, and relationships, partnerships, and technical integrations built well ahead of a process are what put a company on the shortlist when a platform decides to fill its gap. The exit is won in the years before it, by being the obvious company to buy in a category the platforms are about to contest.

08 · OUTLOOK

Outlook

The consolidation that defined 2025 is not finished. The questions for the year ahead are which categories contest next, whether the buyers stay this concentrated, and whether anything slows the cycle.

The cycle continues, led by AI security

Windsor Drake expects the consolidation to extend through 2026, with the sector's deal activity continuing at or above the scale of 2025 as platforms keep completing their architectures.[5] The clearest open front is AI security, where the platforms have made early, small acquisitions and where the next round of contested deals is

most likely to appear as enterprises demand security for the AI systems they are deploying.[2] Founders building in that category sit closest to an opening window; founders in the categories that just consolidated sit behind a closing one.

The regulatory signal is permissive

The clearance of Google's $32 billion acquisition of Wiz is a meaningful signal that the largest cybersecurity transactions can proceed, which removes a brake that might otherwise have slowed the megadeals.[2] That permissiveness supports continued large-scale strategic activity, though it remains subject to the broader and shifting posture toward technology concentration, and a change in that posture is among the risks to the outlook.

Private equity re-engages

As financing conditions ease, private equity is expected to return to the sector in force, both taking public companies private and rolling up the long tail of point solutions.[5] For founders, this widens the set of available exits, particularly in categories where the strategic window has closed, because a sponsor will buy a durable, profitable asset that no platform is racing to acquire.

The cross-border dimension

Cybersecurity is an unusually international market on the supply side, and consolidation is pulling the leading companies toward a small number of mostly United States buyers. Two of the defining assets of the cycle illustrate the pattern: Wiz was built by an Israeli founding team, and Darktrace was a United Kingdom public company, and both were absorbed by larger, US-centered acquirers.[2,6] Israel and the United Kingdom in particular have produced a disproportionate share of category leaders, and the consolidation cycle is, in effect, routing that innovation into the major platforms regardless of where it originated. For a founder outside the United States, this means the most likely premium buyer is often a US platform or a US-based sponsor, which has implications for how a company is positioned, where it builds its commercial presence, and how a cross-border process is run. Cross-border transactions also carry longer timelines and additional regulatory review, which a seller should build into both the schedule and the certainty calculus.

The risks

Three risks bear watching. Buyer concentration is the first: a cycle driven by a handful of platforms is vulnerable if any of them steps back, which would thin the buyer pool quickly in the categories that depend on them. Valuation froth is the second, most acute in AI security, where early enthusiasm could price assets ahead of demonstrated demand and set up a correction. A regulatory shift is the third, since a harder line on technology concentration would directly target the megadeals at the center of the cycle. None of these is a base case, but each is a reason for a founder to treat an open window as a thing to act on rather than to assume will stay open.

EXHIBIT 7

Three scenarios for cybersecurity M&A, 2026–2027

SCENARIO	WHAT HAPPENS	IMPLICATION FOR FOUNDERS
Base case: cycle continues	Consolidation extends at or above 2025 scale; AI security contests next; PE re-engages	Act while your category's window is open; build the sponsor alternative in parallel
Upside: super-cycle accelerates	Permissive regulation and easy financing drive more megadeals and a deeper long tail	Strong assets clear exceptional premiums; competitive processes pay off most
Downside: the brakes come on	A regulatory shift or financing tightening thins the buyer pool, especially the strategics	Windows close faster; certainty and a credible sponsor path become more valuable

Source: Windsor Drake analysis. Scenarios are illustrative, not forecasts; the base case is the firm's working assumption.

The window moves category by category. The founders who do best are the ones who act while theirs is open, rather than waiting for a market that consolidates on its own schedule, not theirs.

The throughline of this report is that cybersecurity has become a market defined by consolidation, and that consolidation has made timing the decisive variable in a sale. The category clock is the tool for reading that timing. A founder who understands where their category sits, builds the company to be acquirable, cultivates the small buyer pool early, and runs a competitive process while the window is open will capture the platform-gap premium that defines this cycle. One who waits will watch it close.

THE EARLY READ

Into 2026: platformization accelerates

Cybersecurity entered 2026 as the most consolidated corner of technology, and the new year pressed the accelerator. A record 2025 gave way to a first quarter in which the largest deal in the sector's history closed, strategic buyers took near-total command of the spend, and a new front, AI security, opened in earnest.

The numbers describe a sector reorganizing by acquisition. Cybersecurity M&A reached roughly $102 billion in 2025, almost a 300 percent jump in value over the prior year across more than 400 deals, and the pace carried into 2026 with dozens of transactions a month and median deal values climbing above $300 million in the first quarter. Alphabet finalized its $32 billion purchase of Wiz in early 2026, the largest cybersecurity

deal ever, while ServiceNow committed close to $9 billion to Armis and Veza and Palo Alto Networks digested its roughly $25 billion acquisition of CyberArk.

A record 2025 became a faster 2026: the largest cyber deal in history closed, strategics took over ninety percent of the spend, and AI security opened as the new contested front.

Strategics own the board

The most striking 2026 statistic is who is buying. Strategic corporate acquirers accounted for more than ninety percent of cybersecurity deal value by mid-spring, as platform vendors raced to complete integrated architectures before rivals could. This is platformization in its late, decisive phase: the category leaders in identity, cloud, data, and now AI security are being absorbed into a handful of platforms, and the window to sell as an independent leader narrows with each large deal.

AI security is the open front

The newest contest is AI security itself. Early 2026 marked an inflection, with dedicated AI-security acquisitions clustering and even AI model labs entering the security buying field. For a founder, the message is the one this report has pressed throughout, sharpened by the new data: in a sector consolidating this fast, category leadership is the asset that commands the premium, and the buy-or-be-bundled pressure on point solutions intensifies as the platforms complete their maps. The clock on an independent cybersecurity exit is running faster in 2026 than it was in 2025.

Sources for this section: SecurityWeek cybersecurity M&A roundups (Feb–Apr 2026); Momentum Cyber Q1 2026 review; FinancialContent and CyberDB (platformization, AI-native integration, strategic share >90%); company disclosures (Alphabet/Wiz, ServiceNow/Armis & Veza, Palo Alto/CyberArk).

Methodology and sources

This report draws on public records of cybersecurity mergers and acquisitions from 2024 through mid-2026, company disclosures, public market valuation data, and Windsor Drake analysis. Aggregate market figures, including total deal value and average deal size, are drawn from published year-end M&A reviews and reflect the methodology and sample of their sources; different trackers count deals differently, and the figures should be read as directional measures of a clear trend rather than as precise totals. Individual deal values are announced or reported figures and, for transactions still subject to closing or regulatory review, remain provisional.

Valuation multiples are EV/revenue unless otherwise stated and describe central tendencies across wide ranges; any individual company can sit far from the figures shown. The category clock and the phase assignments in Exhibits 4 and 5 are a Windsor Drake analytical framework and represent the firm's judgment about where categories sit in the consolidation cycle, not a precise or exhaustive measurement. They are intended to guide timing decisions, not to predict the outcome of any specific transaction. Nothing in this report is investment, legal, tax, or accounting advice.

Endnotes and sources

1. 2025 market totals ($96B in cybersecurity M&A; average deal size up ~82% to ~$2.47B; deal counts; key acquirers): Momentum Cyber, "Cybersecurity M&A Update Report 2025."
2. Defining deals and platformization (Google / Wiz $32B and DOJ clearance; Palo Alto Networks / CyberArk ~$25B, Chronosphere $3.35B, Protect AI $700M, Talon $625M; identity as a platform pillar): Infosecurity Magazine, "The Biggest Cybersecurity Mergers and Acquisitions of 2025"; Palo Alto Networks 8-K filings; contemporaneous press reporting.
3. Platformization strategy and enterprise consolidation of spend: Palo Alto Networks investor materials and CEO commentary; industry analysis of platform versus point-solution dynamics.
4. Cybersecurity valuation multiples (public median ~7.8x; disclosed M&A ~18.8x; subsector ranges): Finro cybersecurity valuation data; Multiples.vc; Windsor Drake, "Cybersecurity Valuation Report."
5. Cycle scale and 2026 outlook ($100B+ consolidation; private equity re-engagement; financing conditions): "The Great Consolidation: Falling Rates Ignite a $100 Billion Cybersecurity M&A Super-Cycle," market commentary, January 2026.
6. Additional transactions (Cisco / Splunk $28B; Thoma Bravo / Darktrace $5.3B; Mastercard / Recorded Future $2.65B; Check Point / Lakera; SentinelOne / Observo AI) and the long tail of deal activity: Momentum Cyber; company announcements; contemporaneous press reporting, 2024–2026.

REFERENCE

The categories, defined

The consolidation cycle moves category by category, so the categories themselves are worth defining plainly. The terms below are the ones that recur throughout this report.

Cloud security (CNAPP)	Cloud-native application protection: securing workloads, configurations, and identities across public cloud environments. The category Wiz came to lead.
Identity security (IAM / PAM)	Identity and access management, including privileged access management: controlling who and what can access systems and data. The category CyberArk anchors.
SIEM	Security information and event management: collecting and analyzing security data across an enterprise to detect and investigate threats. Splunk's core.
Endpoint (EDR / XDR)	Endpoint and extended detection and response: protecting and monitoring devices and, in XDR, correlating signals across the estate.
Application security	Securing software through its development and runtime, including code scanning, dependency analysis, and runtime protection.
Data security / DSPM	Protecting data wherever it resides, including data security posture management: discovering, classifying, and governing sensitive data.
GRC	Governance, risk, and compliance: managing security policy, risk, and regulatory obligations as a program.
Threat intelligence	Collecting and analyzing data on adversaries and emerging threats. The category Recorded Future leads.
AI / model security	Securing AI systems themselves: model inputs and outputs, training data, agent behavior, and the new attack surface AI creates. The emerging frontier.
Platformization	Consolidating multiple security functions into a single integrated architecture sold and operated as one system, the strategy driving the cycle.

Source: Windsor Drake. Definitions are intended for general orientation, not as technical specifications.

ABOUT

About Windsor Drake Research

Windsor Drake is a sell-side M&A advisory firm for founders and boards of software, financial technology, artificial intelligence, and cybersecurity companies in the lower middle market.

The firm advises technology founders through the full arc of a sale, from positioning the company and building the buyer universe to running a competitive process and negotiating terms. Its research program exists to make the dynamics that decide outcomes legible to the people on the selling side, who face these transactions once or twice in a career against buyers who do them constantly. Each report is built from public sources and the firm's transaction experience, and is written to be useful before a process begins, when the decisions that determine price are still open.

This report is part of the Windsor Drake Research series, a set of independent studies on valuation, deal structure, and consolidation across the firm's sectors. Other titles examine the talent-led acquisition of AI companies, the cross-sector valuation premium captured by the Rule of 40, and sector-specific valuation benchmarks. The series is intended to be read by founders, boards, investors, and the journalists and analysts who cover these markets.

Contact

Windsor Drake maintains offices in Toronto and New York. Founders considering a transaction, and members of the press citing this research, can reach the firm through windsordrake.com.

Windsor Drake Research · Toronto · New York · windsordrake.com