YL VENTURES

10th Edition

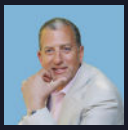
The State of the Cyber Nation 2025

By **Or Salom**
Analyst at YL Ventures

$5.1B Across a Record 136 Rounds

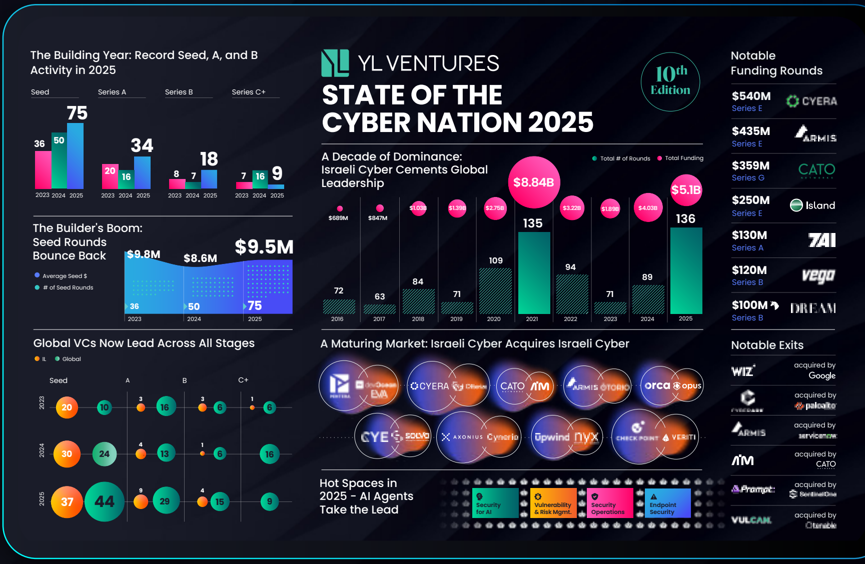
The Benchmark of a Decade of Dominance

> “Israeli cybersecurity now operates with executional consistency shaped by a decade of real company-building and reinforced by sustained global market validation. From our position working alongside founders from inception through scale, we see a market in which global investors are no longer arriving late to proven outcomes, but engaging earlier and more deliberately in company formation. That shift reflects a deeper recognition that Israeli cybersecurity has become a reliable source of category-defining companies.”

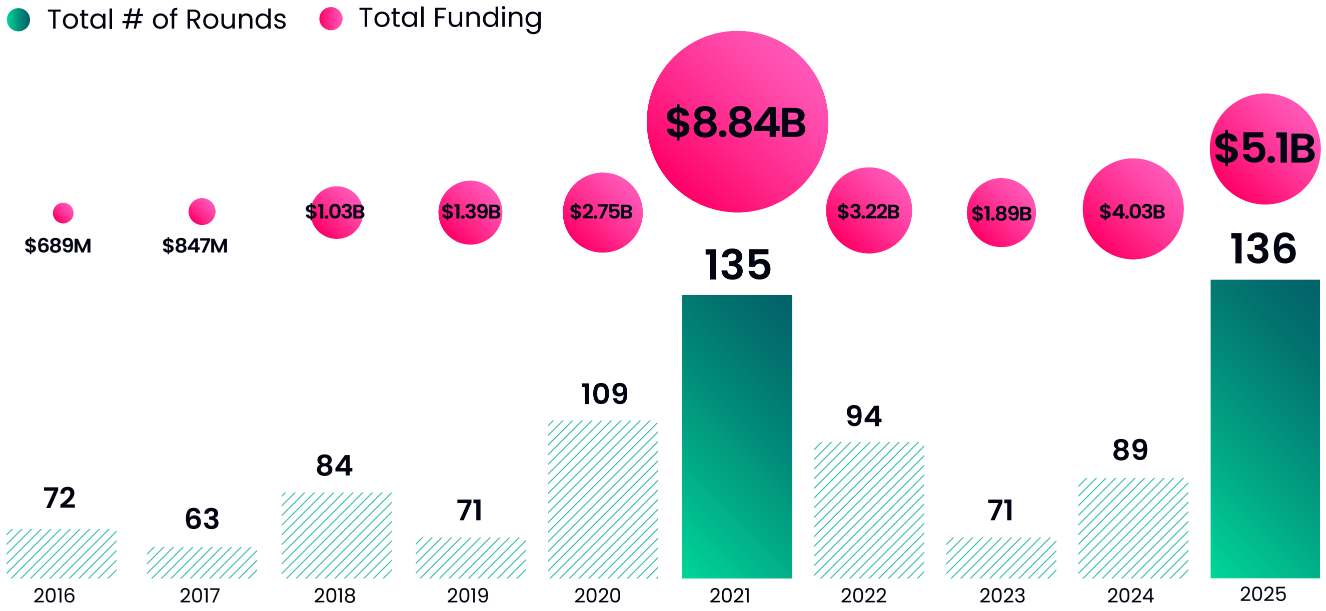


Yoav Leitersdorf
Managing Partner at
YL Ventures

A decade of data confirms that the Israeli cybersecurity ecosystem has transitioned from a source of technical innovation to a primary engine of global market leadership. At YL Ventures, we have spent the last ten years tracking the industry’s most consequential activity while investing in many of its defining companies. Continuous data collection has produced a comprehensive record of every funding round, M&A activity, and trend in Israeli cybersecurity from 2015 through 2025.



Israeli Cyber Cements Global Leadership



To understand the true performance of the Israeli cybersecurity ecosystem in 2025, it is necessary to view this year in the context of the past three years, which together reflect the full cycle from market correction to recovery and renewed growth.

In 2023, Israeli cybersecurity absorbed the full impact of the post - 2021 market reset, as funding declined to 1.89$B across 71 rounds and follow-on capital became significantly harder to secure. Many companies that raised aggressively during the 2021 peak struggled to progress to their next stages, forcing down-rounds, delayed growth plans, or a turn toward acquisition discussions. The year marked a clear inflection point, resetting expectations across the ecosystem and bringing greater discipline to how capital was deployed and companies were built.

In 2024, the industry began a decisive recovery. Total funding more than doubled to 4.03$B across 89 rounds, reflecting a strong return of capital and renewed investor confidence despite ongoing geopolitical instability. While funding rebounded sharply, activity increased more moderately, indicating that the recovery was driven primarily by larger, more selective rounds rather than a broad reopening of the funding pipeline.

In 2025, the signal shifted from recovery to breadth. Total funding reached $5.1B across 136 rounds, surpassing the 135 rounds recorded in 2021 and marking the highest level of deal activity in the ecosystem's history.

Unlike that earlier peak, which was driven largely by late-stage capital, 2025 reflected a structurally broader market, indicative of stronger pipeline health and a maturing ecosystem increasingly capable of translating technical excellence into scalable, fundable businesses.

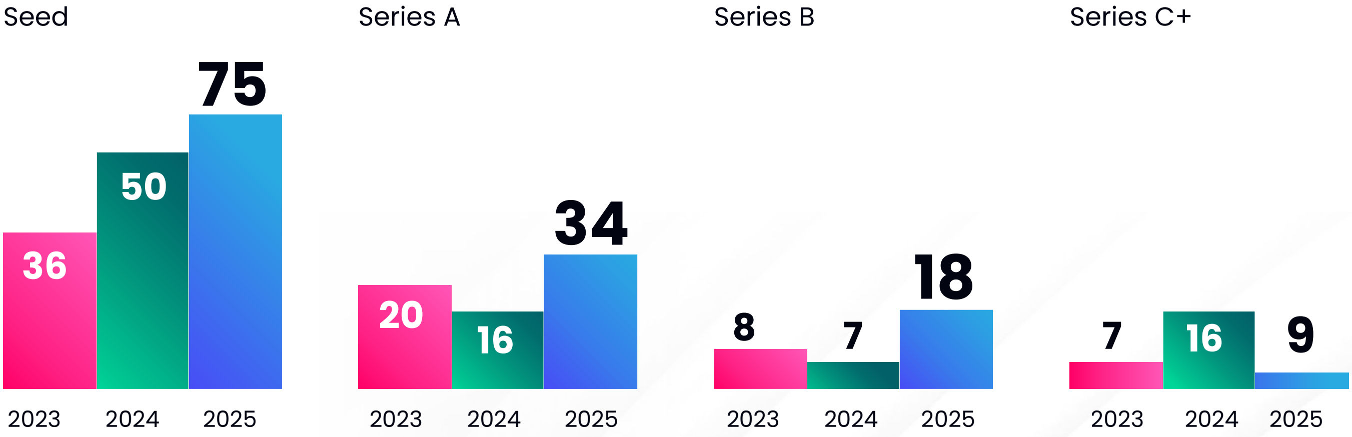
The Building Year: Record Seed, A, and B Activity in 2025

The shift that began to take shape in 2024 became unmistakable in 2025. After several years in which follow-on capital represented a structural bottleneck, the Israeli cybersecurity ecosystem entered a clear building phase, marked by record activity at Seed, Series A, and Series B stages.

In 2024, while seed rounds rebounded, advancing beyond the initial round remained difficult. Series A and B rounds were comparatively scarce, reflecting heightened scrutiny and a market still cautious about underwriting growth. In 2025, those constraints eased materially. Seed rounds climbed to 75, while Series A rounds increased to 34 and Series B rounds rose to 18, more than doubling year over year. This expansion indicates that a larger cohort of companies was not only being formed, but successfully advancing into sustained execution mode.

Investor expectations evolved alongside this change. Rather than requiring fully realized commercial metrics at the Series A stage, investors increasingly backed teams that demonstrated a strong strategic thesis, a clear understanding of the problem space, and early indications of market pull. This has enabled the strongest companies to progress more quickly through early stages, reinforcing a build-first mindset centered on long-term positioning.

Global venture capital participation has reinforced this momentum. For many companies, partnering with global investors at Seed or Series A has become a strategic choice rather than a purely financial one. Early involvement by established global funds strengthens confidence around follow-on financing and reflects a broader reassessment of Israeli cybersecurity as a source of category leaders worth backing from inception.



One visible expression of this shift is the shortening path from Seed to Series A. Many founders now choose to emerge from stealth only after securing their Series A, reflecting a deliberate response to a more competitive and capital-disciplined environment. Remaining in stealth longer allows teams to refine product direction and positioning without the pressure of early exposure.

Seed rounds climbed to 75, while Series A rounds increased to 34 and Series B rounds rose to 18, more than doubling year over year.

“

As a second-time founder, you don’t chase validation - you build conviction. You focus on executing correctly from day one, with sharper decisions and laser focus. But what truly sustains a company over time is the team. Great people turn execution into momentum - and momentum into endurance"

Eran Barak
CEO and Co-founder
of MIND Security

The evolution of Israeli founding teams has further accelerated this dynamic. In emerging categories across the global security landscape, Israeli startups now account for a meaningful share of the most competitive companies. These teams are executing faster, committing earlier to go-to-market, and raising larger rounds sooner in the company lifecycle. Customers and investors increasingly evaluate them as primary competitors rather than future acquisition targets, signaling a shift in ambition toward category leadership.

A meaningful driver of this shift is the growing presence of experienced cybersecurity entrepreneurs. In 2025, a notable share of new companies were founded by teams with prior startup and exit experience. These founders enter with a clear understanding of how global security companies are built and scaled, which reduces early execution risk and increases investor confidence at formation. As a result, they progress more quickly through early stages and attract larger capital commitments earlier in the company lifecycle.

Against this backdrop, the decline in Series C+ rounds in 2025 to 9, down from 16 in 2024, reflects concentration and timing rather than contraction. In 2024, several large growth rounds were raised to support inorganic expansion, enabling companies such as Silverfort and Cyera to acquire smaller startups and accelerate platform consolidation. In 2025, that build mode continued. A number of companies raised substantial growth capital and then deployed it toward acquisitions of Israeli peers, reinforcing their leadership positions. With larger Series A and B rounds providing longer operational runways, many companies faced less urgency to pursue a C+ round immediately.

Growth-stage capital therefore flowed to a smaller set of companies, but at greater scale. Some companies that exited in 2024 would otherwise have been candidates for growth rounds in 2025, while others raised growth capital specifically to support expansion through acquisition rather than organic growth alone. Overall, 2025 marked a shift from recovery to execution. The ecosystem demonstrated its capacity to form companies at scale, move them through critical early stages, and support more ambitious growth paths without relying on late-stage excess.

Against this backdrop, the decline in Series C+ rounds in 2025 to 9, down from 16 in 2024, reflects concentration and timing rather than contraction. In 2024, several large growth rounds were raised to support inorganic expansion, enabling companies such as Silverfort and Cyera to acquire smaller startups and accelerate platform consolidation.

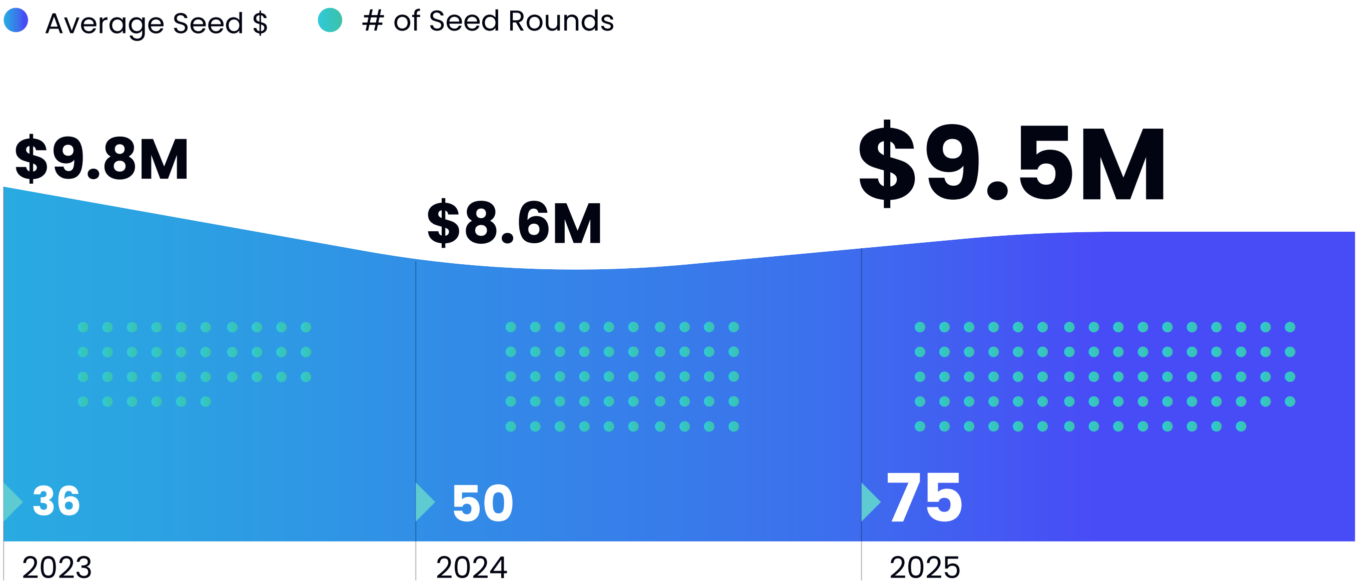
The Builder's Boom: Record Seeds Fuel Israeli Cyber

Seed-stage activity in 2025 did not simply increase in volume. It matured in character. With 75 seed rounds completed and an average round size of 9.5$M, the market demonstrated an uncommon combination of scale and selectivity. Capital was deployed broadly, but not thinly.

This combination is significant. In 2023, average seed rounds reached 9.8$M, but across a much smaller cohort of companies. In 2025, a comparable level of capital was deployed across more than double the number of startups, indicating that a broader set of teams met the bar for substantial early investment. Rather than reflecting looser standards, the data suggests a market in which more strong teams are being formed and funded with sufficient capital to build competitively from the outset.

The size of seed rounds further reinforces this point. Average checks remained materially higher than historical norms, reflecting the reality that cybersecurity startups now face competitive environments from day one. Building defensible products, hiring senior talent, and establishing early customer validation require meaningful upfront investment. The 2025 data shows that investors were willing to fund these requirements early, rather than forcing teams to operate undercapitalized through their most formative stages.

In 2023, average seed rounds reached $9.8M, but across a much smaller cohort of companies. In 2025, a comparable level of capital was deployed across more than double the number of startups, indicating that a broader set of teams met the bar for substantial early investment.



> “The acceleration we’re seeing in early-stage funding is a direct response to the widening gap between machine-speed attacks and human-scale defense. By operating with deliberate focus in stealth, we were able to validate our proprietary AI models against real-world exploitation challenges before seeking the public eye..."

Another defining feature of the 2025 seed market is intentional restraint around visibility. A large portion of newly funded companies are operating quietly in the market, limiting external exposure while they build product maturity and sharpen their category narrative. This reflects a sober assessment of today’s cybersecurity landscape, where early exposure without differentiation can be punitive. Founders are optimizing for strength at launch, not speed to announcement. Launching later allows companies to present themselves with greater maturity, clearer category definition, and stronger signals of momentum, particularly in crowded or fast-moving spaces.

The seed data from 2025 points to a builder’s market in the truest sense. Formation is active, capital is deployed with intent, and both founders and investors are aligned around durability rather than immediacy. This environment rewards preparation, clarity, and ambition, and it establishes a stronger foundation for the companies that will define the next generation of Israeli cybersecurity leaders.

> “...This allowed us to enter the market with more than just a thesis, bringing proven customer traction and a Series A secured within four months of inception. In this environment, the most ambitious founders are no longer waiting for market permission to scale. We are building the engine first, ensuring that when we finally emerge, the momentum is already undeniable and our position as a category leader is firmly established.”

Ido Geffen

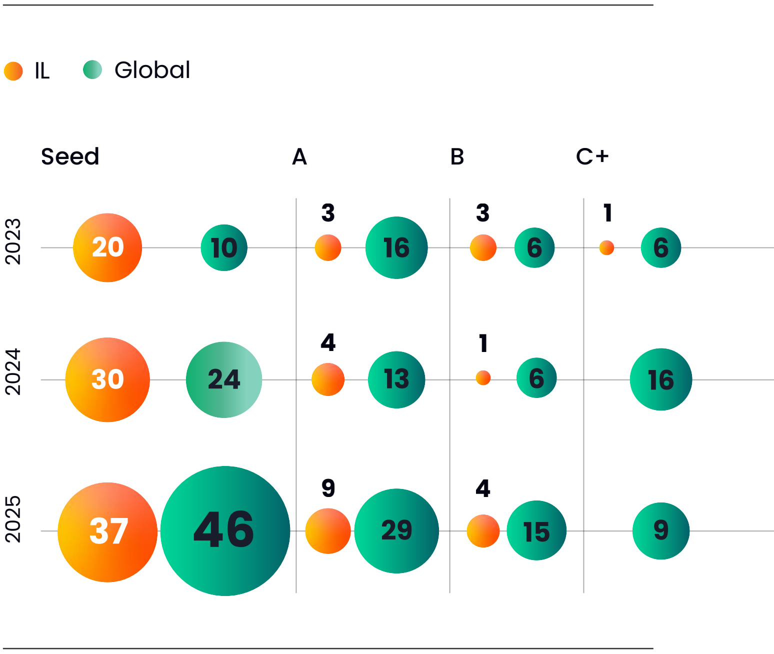
CEO and Co-founder of Novee Security
(an in-stealth YL Ventures portfolio company)

Global Investors Move Earlier: US VCs Now Lead Across All Stages

Global venture capital has long played a central role in Israeli cybersecurity, but historically that involvement began at the growth stages. For years, global funds concentrated their activity in Series A and beyond, where larger check sizes, clearer market signals, and limited local competition made Israeli cyber an attractive destination for late-stage capital. Early-stage rounds, by contrast, remained largely the domain of Israeli cybersecurity-focused funds.

In 2025, that boundary shifted decisively.

Global investors participated in 46 seed rounds in 2025, surpassing Israeli VCs' 37 seed investments and marking the first time foreign capital led seed-stage participation in Israeli cybersecurity. This represents a structural change. While global funds had steadily increased their presence at Series A and B in recent years, Seed remained the final frontier. In 2025, that hesitation gave way to conviction.



> “The transition from a bootstrapped, profitable business to a $65M funding round is a testament to the renewed maturity of the Israeli ecosystem. In today's market, the 'growth at all costs' mentality has been replaced by a focus on fundamental resilience. Global investors are no longer just looking for technical ingenuity, they are betting on the Israeli entrepreneurial spirit's ability to build sustainable, large-scale pillars. For founders, this creates a powerful synergy: we provide the battle-tested conviction of having built from the ground up, and they provide the fuel to turn that proven foundation into a global category leader.”

Tal Kollender
CEO and Co-founder
of Remedio

> “Israel consistently produces founding teams that have already executed together under real pressure. That shared experience, combined with an unmatched founder intensity, means companies move from zero to shipping at extraordinary speed - and do so with a clear sense of what ‘great’ looks like. We're excited to continue to invest at the earliest stages in these extremely high performance teams with grand ambitions for global scale."

Erica Brescia
Managing Director at
Redpoint Ventures

This move upstream reflects a recalibration in how global investors assess risk and opportunity in Israeli cybersecurity. Global VCs are no longer treating seed as a speculative entry point, but as the earliest moment to secure exposure to teams they expect to build category leaders at global scale. Global investors continued to dominate Series A (29 rounds) and Series B (15 rounds) activity in 2025, extending a pattern established in prior years. What changed is not their appetite for growth, but their willingness to engage before outcomes are proven. Seed has moved from a local specialty to a globally contested entry point.

The rise of the split-seed model has played a critical role in enabling this transition. In these rounds, a U.S. global VC and an Israeli cybersecurity-focused firm commit equal capital at seed, aligning early around company formation. For global investors, this structure provides domain depth, local execution support, and confidence in early-stage decision-making. For founders, it combines specialized cybersecurity expertise with global reach and follow-on capacity. As a result, split-seed rounds increased from 12 in 2024 to 14 in 2025, reinforcing early alignment between local and global capital.

Global VCs are no longer approaching Israeli cybersecurity as a market to enter once risk has been resolved. They are competing to establish positions at formation, shaping companies from their earliest decisions, and aligning themselves with teams they believe can define categories at global scale. The shift to seed marks the most meaningful evolution in global participation in Israeli cybersecurity to date.

> “At Mayfield, we're people-first investors, and Israeli cybersecurity stands out for its founders. They bring deep technical grounding paired with the vision to build enduring companies. Investing alongside YL Ventures in companies like Minimus and Opti showed us what's possible when domain expertise, strong execution, and founder ambition come together early. That's why we’re excited to lean in and partner with exceptional teams from day one through their full growth journey.”

Navin Chaddha
Managing Partner
at Mayfield

Hot Spaces in 2025

Security for AI

Vulnerability & Risk Mgmt.

Security Operations

Endpoint Security

The dominant cybersecurity themes of 2025 reflect a market that has moved past incremental improvement and is now responding to structural shifts driven by AI in how software is built, operated, and attacked. Across categories, the common thread is autonomy: AI-powered systems that act independently, generate decisions at machine speed, and operate beyond traditional human control models. The most active areas of innovation are those addressing the security implications of this transition toward autonomous, agent-driven computing.

Security for AI: Governing Autonomous Agents

Security for AI remains the most strategically important domain in 2025, but its focus has evolved materially. The first generation of AI security companies emerged to address risks associated with large language models, including prompt injection, data leakage, and misuse. Many of these early players, such as Aim Security (acquired by Cato Networks) and Prompt Security (acquired by SentinelOne), were built for an era in which AI systems responded to human input.

That paradigm has shifted. In 2025, enterprises are deploying AI agents across core business functions, including engineering, finance, HR, marketing, and operations. These agents execute tasks autonomously, interact directly with sensitive systems and data, and operate continuously across heterogeneous environments such as cloud platforms, SaaS applications, and internal tooling. As a result, the primary security challenge is no longer protecting models, but governing agent behavior.

This transition has exposed a new class of risk. Autonomous agents operate with delegated authority, make decisions without human intervention, and can initiate actions that propagate across systems at machine speed. Traditional security controls, designed for human-driven workflows and deterministic software, struggle to enforce accountability, intent, and policy in this environment. As AI agents become embedded deeper into enterprise operations, the need for security frameworks that can monitor, constrain, and audit autonomous behavior has become urgent.

The second wave of Security for AI innovation is therefore focused on control, oversight, and governance, rather than surface-level protection. These approaches aim to ensure that AI agents act within defined boundaries, respect privilege models, and remain observable as they interact with critical systems. Security for AI has moved decisively from guarding interfaces to enforcing trust and control across AI-driven decision-making itself.

The second wave of Security for AI innovation is therefore focused on control, oversight, and governance, rather than surface-level protection. These approaches aim to ensure that AI agents act within defined boundaries, respect privilege models, and remain observable as they interact with critical systems. Security for AI has moved decisively from guarding interfaces to enforcing trust and control across AI-driven decision-making itself.

Security Operations and Endpoint Security

As AI agents assume greater autonomy, their impact does not remain confined to dedicated AI systems. It propagates directly into the operational core of security. The center of gravity shifts toward Security Operations and Endpoint Security, where agent-driven activity becomes visible, measurable, and increasingly difficult to manage with legacy approaches.

This shift collides with two long-standing pressures that security teams already face: an overwhelming volume of alerts and a persistent shortage of skilled practitioners. In Security Operations, AI is no longer an optional efficiency layer. The scale and speed of modern threats, amplified by automated attackers and AI-assisted exploitation, have made purely human-driven SOC models unsustainable. As a result, AI agents are being introduced not just to automate tasks, but to augment analysts directly, absorbing repetitive investigation work and enabling teams to operate at machine speed, creating operational leverage in an environment where headcount cannot scale with threat volume.

At the same time, the data foundations of the SOC are being re-examined. Traditional SIEM architectures, burdened by high costs and rigid ingestion models, struggle in a world where anything not collected and analyzed effectively does not exist from a security perspective. The rise of AI-driven security data platforms reflects a recognition that visibility, cost efficiency, and continuous analysis are prerequisites for defending AI-powered environments. Security Operations is being rebuilt around data architectures that can sustain AI-driven detection and response at scale.

This same logic extends to the endpoint, which has undergone a fundamental transformation. Endpoints are no longer static containers for binaries operated exclusively by humans. They now host a growing array of non-traditional execution artifacts, including AI models, containers, automation frameworks, and agent runtimes, many of which operate dynamically and fall outside classic binary-based security controls. More importantly, they are increasingly operated by non-human actors, such as coding agents, browser assistants, and local AI systems, all of which execute with privileges historically reserved for users.

> “Security operations has become the pressure point where everything converges, and we're watching a rare moment where enterprise adoption and investor conviction are moving in lockstep. AI agents aren't theoretical..."

Because traditional endpoint protection platforms were designed for human behavior, they are largely blind to this new reality. The result is an expanding security gap at the point where autonomous agents execute. Closing that gap requires endpoint security models capable of understanding behavior, intent, and context in environments where machines, not people, are the primary operators.

Together, these shifts underscore a broader truth of 2025: as autonomy moves deeper into enterprise systems, security must evolve from monitoring human activity to governing machine behavior. Security Operations and Endpoint Security are no longer adjacent domains. They are the operational front lines of an AI-driven ecosystem.

> "...Fortune 500 CISOs are deploying them in production today because they've concluded the traditional approach can’t scale. Investors see it too, placing the largest bets in cybersecurity history on companies transforming how security actually operates. The question isn't whether AI agents will run in the SOC. It's how quickly they can be leveraged and how security leaders can finally let their teams do human work.”

Lior Div

CEO and Co-founder
of 7AI

Steady Exits, Stronger Building: Israeli Acquirers Lead 2025

Prior to 2025, the Israeli cybersecurity ecosystem had rarely produced $1B+ exits within a single calendar year; 2025 shattered this ceiling with three multi-billion dollar transactions occurring in rapid succession.

Precedent-Setting Scale in 2025

Exit activity in 2025 was defined by two parallel dynamics operating at very different scales. At the upper end of the market, a small number of landmark acquisitions - including Wiz by Google for 32$B, CyberArk by Palo Alto Networks for 25$B, and Armis by ServiceNow for 7.75$B - underscored that Israeli cybersecurity companies can be built to generational scale and strategic importance for the world's largest technology platforms. In parallel, a growing number of Israeli cybersecurity companies acted as acquirers themselves, using M&A deliberately to expand platforms, deepen technical capabilities, and consolidate leadership across core security domains.

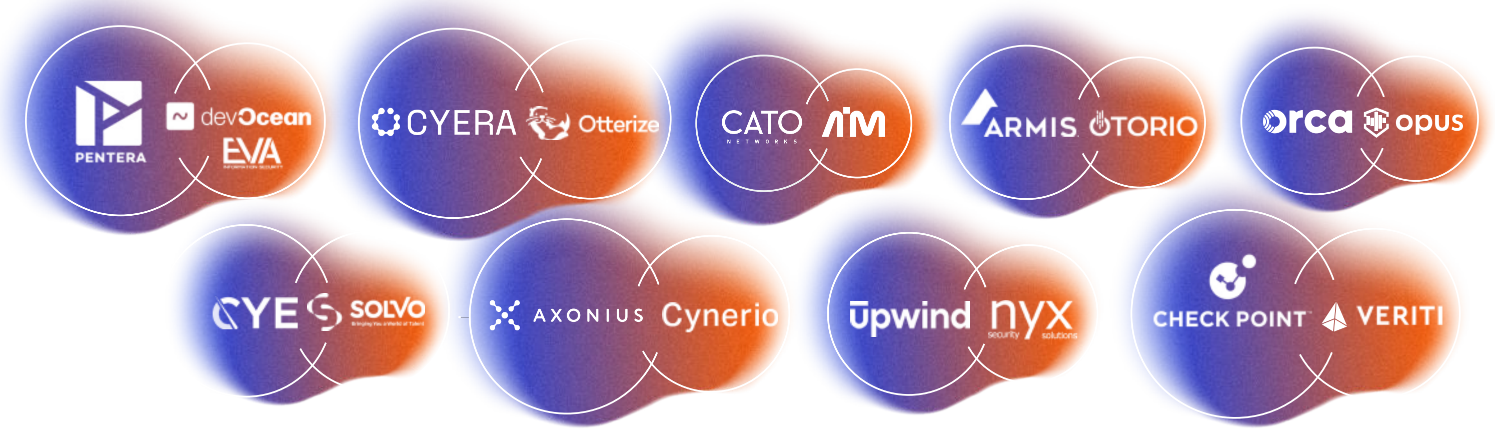
The scale of these transactions represents a fundamental structural break from historical norms. Prior to 2025, the Israeli cybersecurity ecosystem had rarely produced 1$B+ exits within a single calendar year; 2025 shattered this ceiling with three multi-billion dollar transactions occurring in rapid succession. This concentrated surge of ten-figure exits signals that the ecosystem has moved beyond the era of tactical acquisitions. For global technology giants and strategic acquirers, Israeli companies are no longer viewed merely as sources of specialized technical components, but as foundational pillars capable of anchoring entire global security stacks.

In our State of the Cyber Nation 2024 report, we identified the early signals of homegrown consolidation, as a small but meaningful group of Israeli cybersecurity companies began acquiring younger local startups as a strategic growth lever. At the time, these transactions pointed to an ecosystem entering a more mature phase, where leading companies were no longer optimizing solely for standalone growth, but for platform expansion and category control.

Notable Exits

WIZ	acquired by Google
CYBERARK	acquired by paloalto NETWORKS
ARMIS	acquired by servicenow
AIM	acquired by CATO NETWORKS
Prompt:	acquired by SentinelOne
VULCAN.	acquired by tenable

What distinguishes this wave of activity is intent. The majority of these transactions were not driven by opportunistic exits or financial distress. Many of the acquired companies were young, often founded within the past three to five years, and had raised relatively modest capital prior to acquisition.



In 2025, that signal became a defining feature of the market. A growing group of Israeli cybersecurity companies acted as acquirers, using M&A deliberately to accelerate platform expansion, deepen technical capabilities, and reinforce category leadership. These acquisitions spanned Security Operations, Vulnerability and Risk Management, Cloud Security, Identity, IoT, and Security for AI, reflecting both the breadth of innovation in the ecosystem and the maturity of its leading companies.

What distinguishes this wave of activity is intent. The majority of these transactions were not driven by opportunistic exits or financial distress. Many of the acquired companies were young, often founded within the past three to five years, and had raised relatively modest capital prior to acquisition. For acquirers, these deals represented a faster path to roadmap expansion and market differentiation in increasingly competitive categories.

This consolidation trend is tightly linked to how leading Israeli cybersecurity companies approached capital in the preceding period. Many of the large growth rounds raised in 2024 were explicitly intended to support inorganic growth. Raising ahead of acquisition has become a clear strategic signal: companies are capitalizing early in order to move decisively, using M&A to compress development timelines and assemble broader platforms faster than organic execution alone would allow.

Several Israeli companies executed this strategy directly in 2025. Cato Networks raised growth capital and subsequently acquired Aim Security to deepen its platform in Security for AI. Cyera expanded its roadmap through the acquisition of Otterize, while Pentera used acquisitions such as DevOcean to strengthen its Security Operations offering. Similar inorganic growth strategies were pursued by Axonius, Armis, Orca Security, and Upwind, each acquiring Israeli startups to expand platform breadth and reinforce category position. In this context, growth capital is being used not just to scale faster, but to scale broader, enabling Israeli cybersecurity companies to consolidate innovation locally and compound value within the ecosystem itself.

Looking Ahead to 2026

2026 opens with the Israeli cybersecurity ecosystem operating as a formative force in the global security market. Company creation is intentional, capital is committed early with conviction, and an expanding group of Israeli companies now determines its own path through scale, acquisition, and platform expansion. Global investors are no longer positioning around outcomes after they appear; they are embedding at formation and staying through growth.

AI is accelerating everything. Products are built faster, attackers iterate faster, and new companies enter the market earlier with fewer constraints. Development cycles are shorter, go-to-market windows close quickly, and early mistakes are harder to recover from. In this environment, advantage belongs to teams that can execute decisively from the start and sustain momentum as markets evolve.

As AI reshapes how software is built and how risk propagates, Israel's advantage lies in the repeated conversion of deep technical capability into companies that define their categories and reshape markets. After ten years of sustained execution, Israeli cybersecurity has become a structural force in the global security industry.

The State of the
Cyber Nation 2025

YL VENTURES