clairfield

Clairfield sector report

Cybersecurity

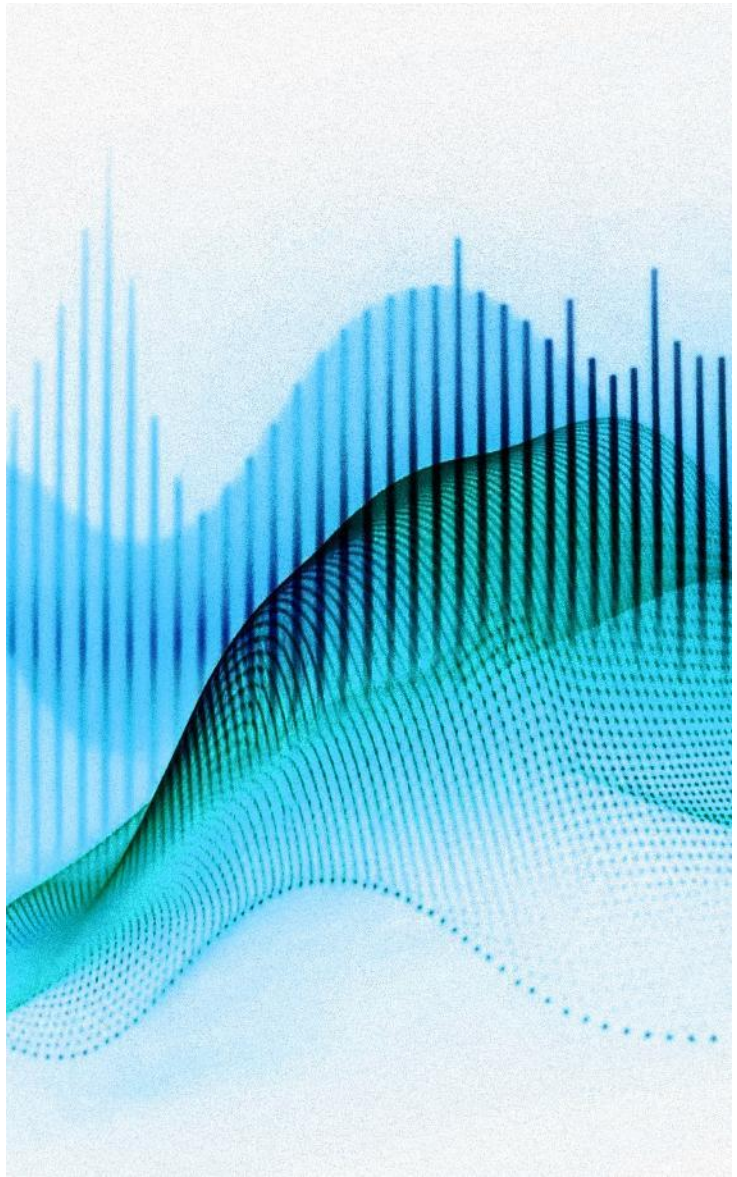
Inside: Overview · Valuations · Trends in cybersecurity in 2025 · Selected transactions · Case study · About Clairfield

March 2026

Cyber world overview 2025 - 2026

clairfield

Cyber outlook 2025–2026: rising threats in a geopolitical world



The global cyber environment in 2025–2026 is defined by rapid escalation in AI-driven attacks, ransomware, deepfake fraud, and supply-chain compromises. Cybercrime has matured into a highly organised industry capable of causing large-scale financial and operational disruption in both public and private sectors.

Cyber activity is now closely tied to geopolitics. State-aligned groups linked to China, Russia, Iran, and North Korea are actively targeting critical infrastructure, energy systems, telecommunications, defense contractors, financial institutions, and election processes. Cyber operations are now embedded into conflicts and tensions involving Ukraine, Taiwan, the Middle East, and the South China Sea.

Governments worldwide are strengthening regulation and enforcement. The US, EU, China, and the Middle East have expanded cyber reporting, resilience testing, and data sovereignty rules, raising financial and legal consequences for cyber incidents.

Cybersecurity M&A and market update — 2025

In 2025 the cybersecurity sector recorded 400 M&A deals[2], of which 165 companies were acquired by PE. There was a value surge of 270% year over year driven by several mega deals - reflecting continued consolidation momentum.

The total disclosed value for cybersecurity M&A deals in 2025 exceeded **US$84 billion**[3]. The year was marked by "mega-mergers" and a significant return of strategic buyers.

Strategic acquirors are focusing primarily on:

- Infrastructure security
- Risk management
- Data protection & identity
- Artificial intelligence (AI) — increasingly viewed as a core enabler for scalable, automated security operations.

North America continues to lead in deal volume, followed by Europe, while Israel is seen as a significant hub for innovation. Indeed, 40% of all M&A transactions were crossborder and pure-play cybersecurity firms remain the primary acquisition targets.

[1] Security Brief Australia (August 20, 2025)
[2] Meridian Capital Q4 2025 Cybersecurity M&A Market Update
[3] Security Week; 8 cybersecurity acquisitions surpassed US$1 billion mark in 2025

Valuations in the cybersecurity market 2025

clairfield

Privately held cybersecurity product companies sell at revenue multiples of around 8.5X, while their public counterparts trade at a commanding 14.2X multiples. That's a 6.5X valuation gap depending on whether the company is private or public[1]. The cybersecurity segments that command the highest valuation multiples for M&A include cloud security, identity access management, and data security[2].

A December 2025 study by the Phenom Institute found that just 18% of organisations have fully adopted and integrated AI cybersecurity tools. 65% of security teams report challenges of integrating AI security solutions with legacy systems. These aren't simple market-fit problems. These are implementation problems that require human expertise to solve[1].

Ongoing trends include strategic acquisitions of specialised Managed Security Services Providers (MSSPs) to enhance offerings. These transactions enable consolidators to obtain clients in new verticals and build end-to-end security operations. In August 2025, LevelBlue completed the acquisition of Trustwave, creating the world's largest pure-play (MSSP). Two months later, LevelBlue completed the acquisition of CybeReason. The two transactions enhance LevelBlue's proactive threat intelligence and defence[1] with Managed Detection and Response (MDR), Extended Detection Response (XDR) and digital forensic and incident response capabilities[3]. It also provided the acquiror with Cybereason's AI-driven endpoint security. This transaction highlights consolidation of related managed services in cybersecurity, driven by enterprise demand for outsourced security amid talent shortages, cloud complexity, and rising threats.

Organisations are responding by shifting to Zero Trust security models, phishing-resistant multi-factor authentication, passkeys, and AI-driven detection and response. Security operations are increasingly automated to keep pace with faster and more sophisticated attacks.

Funding

VC investment into cybersecurity businesses continues to accelerate, especially for technologies enabling agentic AI, autonomous threat detection, and governance & compliance augmentation. Capital deployment is particularly strong in early- and growth-stage companies with differentiated AI capabilities. Dedicated cybersecurity investors driving this trend include Dragon, YL Ventures, CyberStarts, and the US venture fund Striker, all of which focus on backing emerging cyber technologies and high-potential AI-enabled security solutions.

Outlook

Market sentiment remains positive heading into 2026, with:

- Strong appetite for innovation in AI-native security.
- Continued premium valuations for high-growth, cloud-delivered, and identity-centric solutions.
- Rising deal competition among both strategics and private equity buyers.
- Cybersecurity remains one of the most resilient technology investment categories globally as threat complexity and regulatory pressures continue to rise.

[1] The Valuation Trap, March 16, 2026

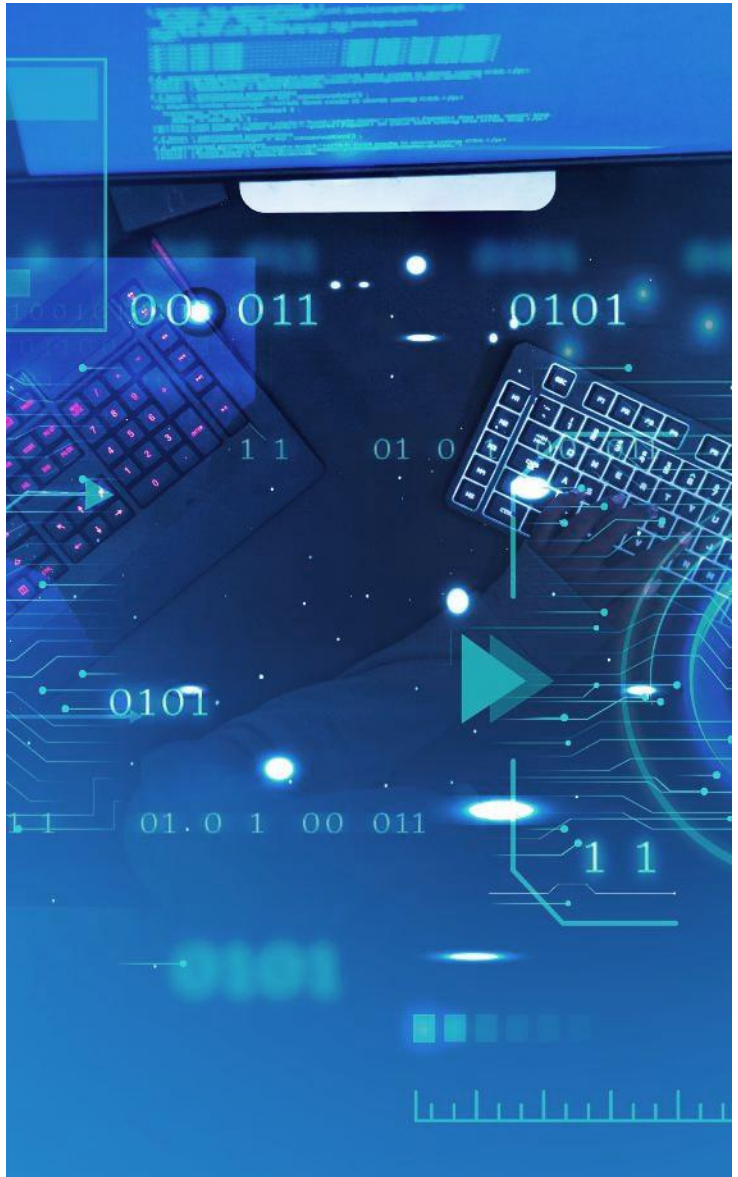
[2] Finro Fiancial Consulting, "Cyber Security Valuation Multiples" June 2025

[3] Globes, (October 15, 2025)

Middle East conflict and Israel's cyber exits

clairfield

Middle East instability and impact on M&A



Despite ongoing instability in the Middle East, Israeli cybersecurity companies continue to lead globally in relevance and investor interest.

In 2025 the cybersecurity total exit value of reached a record US$72.6 billion (including transactions signed, but yet to close). This is an increase of more than 1,500% compared to 2024. Capital raising also hit an all-time high, climbing to US$8.27 billion, an increase of nearly 110% compared to the previous year when funding amounted to US$3.96 billion, and surpassing the previous record set in 2021 of US$7.5 billion.[1]

This extraordinary spike is driven by several historic mega-deals.

Google acquired WIZ

- Wiz was acquired for US$32 billion, marking the largest cybersecurity acquisition ever globally and the biggest exit in Israeli cyber history.

paloalto NETWORKS acquired CYBERARK

- A few months later, CyberArk was acquired by Palo Alto Networks for US$25 billion, becoming the second-largest Israeli cyber exit to date.

servicenow acquired ARMIS

- In parallel, ServiceNow's acquisition of Armis for US$7.75 billion further underscored global strategic demand for Israeli cybersecurity platforms, particularly in asset visibility and operational security. Together, these transactions account for nearly all the exit value realised in 2025, underscoring the magnitude of this year's valuation "re-set."

Meanwhile, the broader ecosystem remains strong. Israel continues to host around 500–550 active cybersecurity companies. Excluding Wiz, there are 22 cybersecurity unicorns (companies valued over US$1 billion), collectively estimated at about US$58 billion. Notably, two new firms — Dream Security and Pentera — reportedly joined the unicorn cohort in 2025.

As for exit timing and investor dynamics, 2025's wave of large acquisitions suggests that the exit horizon may be shortening for promising startups, particularly those with niche, high-demand technologies such as cloud security, identity, operational visibility, and AI-driven security solutions. The surge in mega-deals has redefined what success looks like in Israeli cyber, creating both opportunity and pressure for remaining unicorns and emerging companies alike.

[1] Jerusalem Post. January 2026

HACK ETF of cybersecurity

Over the past year, the HACK ETF — which tracks leading cybersecurity companies — has underperformed the S&P 500 by approximately 10%.

This performance gap suggests that while cybersecurity remains a strategically important and rapidly evolving sector, near-term investor returns have lagged broader market gains. Several key market dynamics help explain this relative underperformance:

1. Valuation reset after strong prior years

Cybersecurity stocks delivered strong gains in prior years, leading to elevated valuations. As the broader market continued upward, some investors rotated out of high-growth and premium valuation names into sectors with stronger near-term earnings momentum, contributing to HACK's relative underperformance.

2. Profit-taking and sector rotation

After significant appreciation in defence and security technology shares, investors may have taken profits or refocused on value-oriented areas, especially amid evolving economic conditions and interest-rate expectations.

3. Macroeconomic sensitivities

Despite ongoing demand for cyber solutions, broader macro pressures — such as tightening monetary policy or slowing corporate IT budgets — may have temporarily dampened spending or investor confidence in tech-intensive sectors.

4. Competitive and execution challenges

Intense competition and rapid technological change can compress margins or delay monetisation for some cybersecurity firms. Companies within the HACK ETF may have faced headwinds related to execution timing or market share shifts.

Despite relative underperformance, continued sector growth supports steady capital inflows, selective exits, and a healthy, more disciplined pipeline of cybersecurity deals heading into 2026.

The 25 companies in the HACK ETF currently have a mean price-to-sales (P/S) ratio of **8.93** and a median of **5.38**, reflecting a modest decline in valuations compared with the prior year. The fact that the median sits well below the mean indicates that a small number of high-multiple companies continue to skew the average upward, though overall valuations have clearly moderated. This moderation, alongside continued absolute growth in the ETF, suggests that while investor enthusiasm has cooled slightly, confidence in the long-term prospects of the cybersecurity sector remains intact. Notably, the index includes several defence and telecommunications hardware companies that carry lower valuation multiples but above-average weightings, which dampen reported multiples; excluding these firms implies a P/S ratio closer to **10x**.

Source: Clairfield Analysis

Overview of 2025 activity

clairfield

HACK ETF of cybersecurity

***VOO** is the **Vanguard S&P 500 ETF**, a popular exchange-traded fund that aims to track the performance of the S&P 500 Index - a benchmark made up of roughly the 500 largest publicly traded US companies by market capitalisation.

Source: Yahoo Finance

Trends in cybersecurity in 2026

clairfield

Cloud security

As enterprises continue to migrate critical workloads to the cloud, securing cloud infrastructure, applications, and data has become paramount. Cloud security now encompasses workload protection, misconfiguration detection, and continuous monitoring across multi-cloud environments. High-profile breaches and regulatory scrutiny are driving adoption, making cloud security one of the fastest-growing segments in cybersecurity investment and M&A activity.

Ransomware defence & incident response

Ransomware remains one of the most disruptive cyber threats, prompting enterprises to strengthen prevention, detection, and rapid response capabilities. Managed Detection & Response (MDR) services and ransomware recovery solutions are in high demand, allowing organisations to minimise downtime, protect critical data, and recover more quickly from attacks. The rising prevalence of ransomware has also increased investor interest in this segment.

Identity & access management (IAM))

Zero Trust adoption is fueling demand for robust identity and access management solutions. Multi-factor authentication, privileged access management, and passwordless technologies are increasingly standard, protecting both user and machine identities. Companies are focusing on reducing the attack surface by controlling access at a granular level, which makes IAM a critical foundation for modern cybersecurity strategies.

Network & endpoint security

Securing endpoints and networks remains a foundational priority as hybrid workplaces and IoT/OT devices expand the attack surface. Endpoint Detection & Response (EDR) and advanced network security platforms are evolving to meet modern threats, integrating AI analytics and real-time monitoring. Consolidation and strategic acquisitions continue to reshape this space, highlighting its enduring relevance in enterprise defence.

AI & threat intelligence

AI-powered platforms are transforming how organisations detect, predict, and respond to threats. Leveraging machine learning and real-time threat intelligence, security teams can automate monitoring, prioritise alerts, and anticipate attacks. As attackers increasingly use AI themselves, investing in AI-native cybersecurity tools has become essential for maintaining resilience and operational efficiency.

Governance, risk & compliance (GRC)

With tightening regulations like NIS2, CCPA/CPRA, and national cybersecurity laws, governance, risk, and compliance frameworks are increasingly essential. GRC solutions help organisations manage risk, ensure regulatory compliance, and align security policies with operational objectives. Integrating GRC into security operations allows enterprises to respond quickly to threats while maintaining accountability and audit readiness.

Selected cybersecurity M&A and financing transactions 2025

clairfield

Acquiror	Google	paloalto NETWORKS	HPE	paloalto NETWORKS	FP FRANCISCO PARTNERS	VEEAM
Deal size	acquired for $32B	acquired for $25B	acquired for $14B	acquired for $3.35B	acquired for $2.2B	acquired for $1.75B
Target	WIZ	CYBERARK	JUNIPER NETWORKS	chronosphere	jamf	securiti

Top financing rounds

ReliaQuest — US$500 million PE Growth Investment
SandboxAQ — US$450 million Series E
Nerdio — US$500 million PE Growth Financing
Cato Networks — US$359 million Series G
Armis — US$435 million Financing
Exein — US$108 million Series C

Notable transaction

servicenow

acquired for US$7.75 billion

ARMIS

ServiceNow's Blockbuster Armis Deal

ServiceNow agreed to acquire cybersecurity firm Armis for US$7.75 billion in an all-cash transaction, marking the largest acquisition in the company's history. The deal values Armis at about 23 times its annual recurring revenue (ARR), highlighting both Armis's rapid growth and ServiceNow's strategic bet on cybersecurity.

Armis brings real-time asset discovery and exposure management across IT, IoT, OT, and medical devices, which ServiceNow will integrate into its AI-driven workflow and remediation platform. This move expands ServiceNow's security and risk capabilities and signals strong momentum in enterprise cybersecurity M&A.

Source:

Clairfield's cybersecurity successes

clairfield

Fintech

GBG

acquired

IDOLOGY

IT services

REPLY

acquired the German operation of

CSPi

Internet services

CLOUDALLY
Secured Cloud Backup

was sold to

zix®

IT services

BCT Solutions

was sold to

accenture

IT services

GRAYSHIFT

received strategic growth investment from

THOMABRAVO

IT services

QUADRUM CAPITAL

acquired

DataExpert

Professional advisory

XKG

Vrai
Trusted. Authentic. Expertise.

were sold to

Infrastructure Advisory Group

Software & apps

IMPACT partners

sold

SECURIVIEW
NEXT GENERATION SOC

to

LINKBYNET
WATCHMAKERS OF THE DIGITAL WORLD

backed by KEENSIGHT CAPITAL

Software & apps

Aurora

owner of rcs
BEHIND A SAFER WORLD

was sold to

CY4GATE
ELETTRONICA GROUP

Software & apps

OGL

was sold to

wavenet

Software & apps

BOSS INDUSTRIES

sold

elektron

to

CHAPSVISION
DATA MAKE SENSE

Software & apps

GRAYSHIFT

completed a minority growth recapitalisation with an investor group led by

PEAKEQUITY PARTNERS

Clairfield's cybersecurity successes

clairfield

Software & apps

B4Finance

was sold to

RISK CONCILE

backed by

MAIN CAPITAL PARTNERS

IT services

WCC

backed by AVEDON CAPITAL PARTNERS

was sold to

Software Combined

backed by NAVIS CAPITAL PARTNERS

IT services

Hermes, a subsidiary of

WCC

backed by AVEDON CAPITAL PARTNERS

was sold to

vision-box

a subsidiary of

AMADEUS

IT services

/LIBRAESVA

was sold to

PSG

IT services

OneEquity

acquired

Digital Value

IT services

NEXTIOS

sold contract assets to

BRLink

An INGRAM MICRO Company

Software & apps

icomedias®

was sold to

ALTAMOUNT

Software & apps

DATAFUSION SYSTEMS

was sold to

LUMINE

IT services

embeddeers

ENGINEERING EXPERTS

was sold to

spyrosoft

IT services

sold its **Vision** business to

SPX CAPITAL

IT services

SOLUTEC

INGENIERIE INFORMATIQUE

was sold to

qubay

ahead of innovation

Software & apps

weezevent

minority backed by

naxicap PARTNERS

BFC CROISSANCE CAPITAL INVESTISSEMENT

acquired

Kaboodle

Case study

ISH sells private client cybersecurity business to SPX Capital

ISH Tecnologia is a Brazilian cybersecurity services and software provider that delivers monitoring, detection and response services, as well as infrastructure solutions, to many of the largest corporate clients in Brazil. The company has built a strong national footprint and established a prominent position in the country's fast-growing cybersecurity market.

Vision Cybersecurity was created through the spin-off of ISH's private sector activities and begins operations with more than 400 clients. Its platform combines in-house technology with global partnerships.

SPX Capital is one of Brazil's largest independent asset managers, with approximately US$10 billion in assets under management. The investment was made through its private equity arm, which is backed by The Carlyle Group and focuses on partnering with high-growth companies.

The spin-off was designed to give the private client business greater commercial agility and strategic focus by separating it from ISH's public and defence activities.

SPX's investment is largely primary capital and will support Vision's innovation agenda, including expanded use of artificial intelligence for predictive threat detection and automated response. The funds will also underpin an active acquisition strategy aimed at consolidating Brazil's fragmented cybersecurity market.

The transaction took place against a backdrop of strong sector growth. Brazil is one of the countries most targeted by cyberattacks globally, yet penetration of advanced cybersecurity services remains relatively low with significant expansion potential.

The transaction required a full operational and legal carve-out. ISH did not previously operate separate legal entities by client type, which meant that the private client business had to be constructed as a standalone company during the transaction process.

Client contracts were migrated to the newly created entity, while agreements with software vendors and internal systems providers were duplicated to ensure continuity. Teams and employees were formally separated and reallocated between the two organisations, and selected intellectual property was transferred as part of the establishment of the new Vision Cybersecurity brand.

In parallel, multiple related-party agreements were negotiated between the two companies, including a Transitional Services Agreement, a distribution agreement for proprietary software, and a data centre licence agreement.

All financial information and valuation metrics were prepared on a pro forma basis, as Vision did not yet exist as an independent entity. With careful structuring of these workstreams, Clairfield ensured that ISH could present a robust standalone platform to investors and execute a technically demanding separation without disrupting ongoing operations.

clairfield

A leading independent M&A advisor for midmarket deals

500+
TEAM MEMBERS

80%
OF OUR MANDATES ARE INTERNATIONAL

6
SECTOR TEAMS OF SPECIALISED EXPERTISE BACKED BY **70**
INDUSTRY ADVISORS

34
COUNTRIES

30%
DEALS CLOSED WITH INTERNATIONAL BUYERS

Founded in 2004, Clairfield International provides advisory services on midmarket transactions to a diverse clientele, including large companies, private investors, private equity, public sector entities, and family businesses.

We connect clients with regional and international strategic parties, investors, and decision-makers, while providing expert knowledge of local markets, regulations, and cultures.

Clairfield ranks as one of the top independent M&A advisors in worldwide league tables.

Top 10
IN EUROPEAN MIDMARKET RANKINGS

Top 20
IN WORLDWIDE MIDMARKET RANKINGS

1,000
DEALS CLOSED IN THE LAST 5 YEARS

EUR 56 billion
CUMULATIVE DEAL VALUE IN THE LAST 5 YEARS

We look forward to speaking with you soon.

clairfield

TECH, SOFTWARE & DIGITAL TEAM

Joseph Sabet
Head of cybersecurity practice
jsabet@clairfield.com
T: +972 3 607-4100

Bertrand Hermez
Head of tech, software & digital sector group
bhermez@clairfield.com
T: +33 1 40 20 12 34

CLAIRFIELD INTERNATIONAL SA

11 Rue du Conseil-Général
1205 Geneva
Switzerland

Tel: +41 22 518 0242
info@clairfield.com