ICON CORPORATE FINANCE

Cybersecurity Sector Update

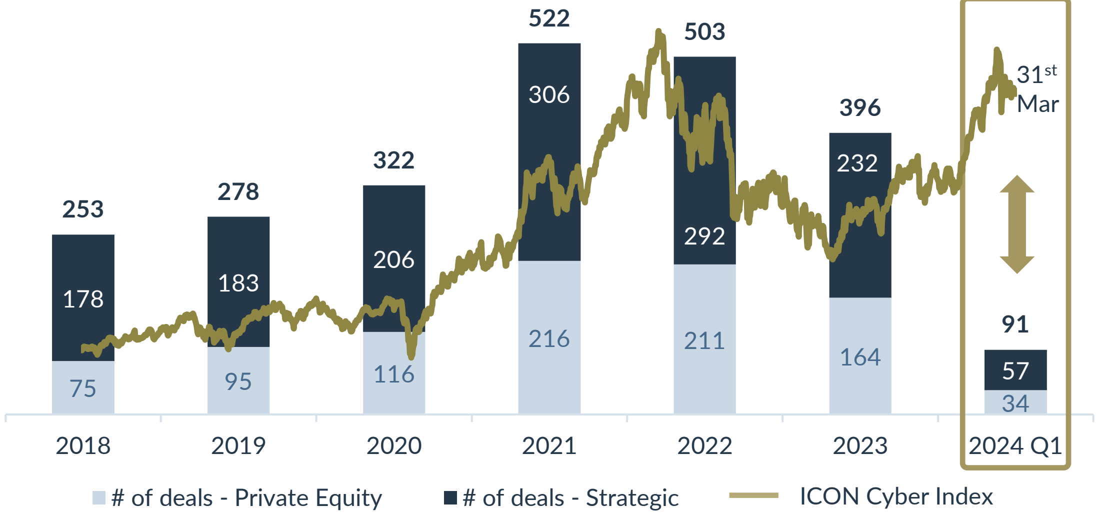
May 2024

Strictly private and confidential

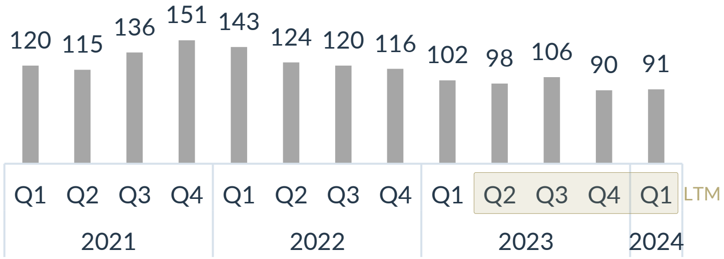
Cybersecurity sector fast facts

Market momentum rebounds: Stock markets have turned a corner, boosting M&A activity – funding still stalling

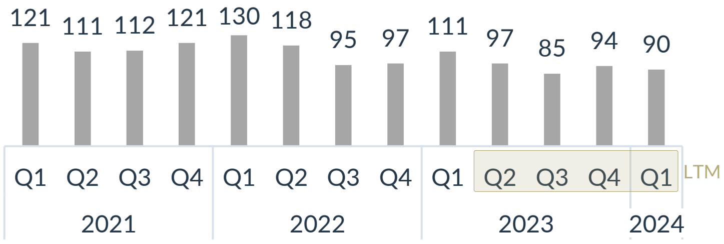
Global M&A activity vs ICON Cybersecurity Index performance: Public markets rebound expected to exercise pull effect on M&A activity



Number Cybersecurity M&A deals



Number Cybersecurity funding rounds



$91.8bn

Total disclosed M&A deal value across 385 deals LTM

-17%	+12%
Deal Volume *LTM vs LTM -1*	**Deal Value** *LTM vs LTM -1*

$6.8bn

Raised across 366 private funding rounds LTM

-13%	-39%
Deal Volume *LTM vs LTM -1*	**Deal Value** *LTM vs LTM -1*

Volatile public equity markets have stabilised, and high-growth stocks regained significant lost ground

+116.5%

5-year cybersecurity index performance vs +96% of the NASDAQ

8.4x 2024F rev

Top Quartile Cybersecurity peer group valuation

15.4%

Top Quartile avg. growth 23-25F

4.5x 2024F rev

Cybersecurity peer group median valuation

9.1%

Peer group avg. growth 23-25F

2.2x 2024F rev

Bottom Quartile Cybersecurity peer group valuation

3.0%

Bottom Quartile growth 23-25F

ICON CORPORATE FINANCE

Cybersecurity sector snapshot

May 2024

1 Public markets are rebounding, M&A deal activity back in line with pre-Covid levels, but fundraising still lagging

- Whilst M&A activity has followed the public market recovery, later stage fundraising remains behind recent highs
- Valuations have stabilised at a new re-based level. Publicly listed cybersecurity companies continue to trade at a significant premium to broader tech market peers
- 2023 recorded 396 M&A deals, surpassing pre-Covid levels. Vendor platform consolidation, largely backed by Private Equity, is a major driver behind the sustained deal activity. Q1 2024, with 91 noted deals, provides a promising outlook for the full year
- $6.8bn of VC money was invested in the sector globally across 366 deals during the last twelve months. Fundraising transaction volume was down -13% vs the first period and but total investment value was also down by -39%

2 Market fundamentals remain as strong as ever… but how future-proof are current cybersecurity tech stacks?

- Cybercrime activity continues to thrive on a perfect storm of significant geopolitical and economic uncertainty, rapidly advancing technology sophistication, a fragmented regulatory landscape, and persistent skills shortages
    - Splunk's October 2023 CISO research poll revealed that 90% of organisations suffered at least one major cyber-attack in the last year and 93% of all CISOs are expecting their companies' cybersecurity budget to increase over the next year
    - According to ISC2, the gap between the number of cybersecurity professionals needed and the number available is now 3.4m (compared to a total workforce of 4.7m globally). This is despite the news of job cuts at large cybersecurity companies (see SecureWorks, Rapid 7, Sophos, etc.) – resulting mainly from corporate efficiency drives as opposed to perceived skill oversupply
- Companies continue to invest vast amounts in their cyber defences but with the arrival of AI and Quantum Computing, existing software-based solutions can be outsmarted and can no longer guarantee safe protection from adverse threats (see highlights section🔒)
- Cybersecurity companies are themselves becoming the victims of hacking activity, raising the stakes for the protection of critical national infrastructure and large legacy IT estates:
    - Owning to its large share in cloud infrastructure, data and apps, Microsoft continues to successfully exercise its weight on the cyber industry, pushing its Sentinel and Defender solutions. However, on 11th July 2023, Microsoft revealed that a Chinese threat actor had obtained an MSA consumer signing key, allowing the creation of access tokens for Exchange Online and Outlook.com
    - On 23rd October 2023, Okta disclosed a breach that a hacking group had accessed client files through the support system, wiping more than $2bn of its market cap

3 Rebound in public equity markets and robust sector fundamentals continue to drive M&A deal activity

- Whilst market conditions remained choppy during 2023, we expect the recovery in public markets to bolster M&A activity in 2024
- Strategic interest to consolidate a fragmented market landscape and move from point product to solution offerings remains a key driver, whilst direct PE activity continues to be challenged by the high-interest environments and lack of suitable debt options

ICON
CORPORATE FINANCE

AI disruption is upping the stakes in the cybersecurity arms race

AI is a polarising top priority and the battle between defence and offence has reached a new dimension with the surge of GenAI

Consequently, the global market for AI-based cybersecurity products is expected to swell from $24.3bn in 2023 to $133.8bn 2030 (+26.7% CAGR)

Increase in AI-powered attack sophistication…

Equipped with a strengthened arsenal of AI-powered cyber weapons, adverse threat actors can cause potent damage. Examples of the new capabilities include:

- More persuasive phishing emails: spell-proof, multi-lingual, distributed at large scale, taking advantage of enhanced social engineering
- Increased pace and scale of attacks to maximise zero-day exploitations
- Better design of visual or audio deep-fakes that can bypass biometric authentications
- Faster and more accurate password guessing
- Data poisoning: Hackers can infiltrate the training data used for AI algorithms and manipulate ultimate decision-making software
- AI has become a welcome workforce multiplier for cyber criminals: create new ransomware at unprecedented scale
- Hacking gets democratised: GenAI provides now access to sophisticated technology for lower-skilled people (e.g. "WormGPT")

…drives growing reliance on AI to harden and adapt defences

According to IBM, organisations employing AI and automation extensively in their security operations were able to shorten the average data breach lifecycle by 108 days

Applying the NIST framework, there are several ways how AI can significantly enhance an organisation's security posture

1. **Identify**: Improved vulnerability identification across the IT asset base by leveraging automated AI red teaming platforms
2. **Protect**: Utilise AI-powered Dev Sec Ops to minimise coding errors; implement superior anti-spam and anti-phishing protection
3. **Detect**: Enhanced data analytics to spot anomalies in user behaviour, data movements, network traffic, endpoint devices, etc., in real-time
4. **Respond**: Automate mitigating actions and minimise response time through AI co-piloting (e,g. CrowdStrike's Charlotte AI)
5. **Recover**: Embed AI-guided recovery processes across the organisation

Cybersecurity industry takeaways

> "*What we talked about in the earnings call is the ability to create more adversaries with lower skill levels, but operating at a much higher skill level, leveraging generative AI.*
>
> *Of course, on the security side, we leverage generative AI to help protect our customers, so* ***it's going to be the battle of AI in the future.*** "
>
> George Kurtz, CrowdStrike CEO, 6 March 2024

> "*We have to protect our customers from anything that bad actors use these AI platforms for and that's going to be a big deal.*"
>
> Nikesh Arora, Palo Alto Networks CEO, 21 March 2024

Related companies

EU & UK

DARKTRACE
deep instinct
SEON
TESSIAN proofpoint
raito
GATEWATCHER

Global

VECTRA
Armorblox
CROWDSTRIKE
ACALVIO AI-POWERED DECEPTION
cisco
cybereason
LogRhythm
Dropzone AI
QUANTUM ARTIFICIAL INTELLIGENCE
CALYPSOAI

Source(s): Technopedia, Morgan Stanley, IBM, CNBC, FT

The Quantum Computing revolution: how to avoid all data becoming hackable?

Quantum Computing is going to have a profound impact on cybersecurity: the rapid advancements in quantum computing bring extraordinary new potential, but also new and yet unknown security threats to our data security

The raising quantum threat to cryptography

- Much of the encryption that underpins today's internet and its secure electronic data transfer uses complex integer factorisation-based cryptography, employed for example in the RSA public key infrastructure (PKI)
- These encryption systems prevent unauthorised access of sensitive data used in financial transactions, trade secrets, health information, critical infrastructure, classified communication, etc. Using conventional computing, they cannot be hacked
- Quantum technology provides a revolutionary step change in processing power: leveraging qubits (which can simultaneously take on all possible combinations of the binary 1 and 0 bits used in classical computing), quantum computers can perform highly complex algorithms at a massive scale, which brings enormous advantages. One of them is the ability to decode complex systems
- The point at which large quantum computers will be able to crack encryption code using Shore's algorithms to factor a 2048-bit key is called **Q-Day.** It will have drastic consequences for data security

Harvest now, decrypt later (HNDL)

- The question is not if but when Q-day will come. In 2023, Chinese researchers claimed to have developed a quantum computer that can break RSA encryption, which would be widely ahead of expectations that this is still 5-20 years out
- If proven to be scalable, all conventional cryptographic algorithms (RSA, DSS, Diffie-Hellman, TLS/SSL, etc.) would become obsolete, all systems vulnerable and sensitive data eventually readable
- This is yet to be verified, but a massive exercise by criminal gangs and nation-state actors is already underway, focused on stealing data from organisations now and then decrypting it when quantum computing has reached maturity (HDNL attacks). People will look different at spy balloons in this light
- Not only do these data compromises carry huge regulatory penalties, but the scale of damage from highly sensitive information ending up in the wrong hands is barely fathomable
- Organisations need to wake up to the significant risks of quantum computing and take steps to protect against them now

Emerging quantum-safe cybersecurity tech

- Organisations need to migrate their network architecture to quantum-resistant cryptography and methods: In Sep 2023, the NSA announced that it would implement new quantum-proof algorithms on all national security systems by 2035
- Taking stock: One of the first measures for every organisation is to discover what cryptography is being used in software applications across IT, OT, and the IT supply chain, i.e. creating an inventory of all cryptography, allowing to assess the potential exposure and evaluate appropriate mitigating actions
- Quantum-safe or post-quantum cryptography algorithms are currently being developed and standardised by NIST
- Quantum Key Distribution (QKD): Allows detection if a third-party quantum system is trying to gain knowledge of the key by using photon transmission, which can monitor the key exchange between two communicating users and assess possible photon perturbation by quantum machine interference

Related companies

EU & UK

KETS, SANDBOXAQ™, CRYPTO QUANTIQUE, ARQIT, PQSHIELD, IDQ, ssh, QuBalt, CRYPTONEXT SECURITY Post-Quantum, VeriQloud, Crypta Labs

Global

MagiQ, QuSecure, ISARA, QUANTINUUM, Quintessence Labs, QUANTUMXCHANGE™, Qrypt, QuantLR

Source(s): IBM, Deloitte, EY, Michael McLaughlin

Hardsec revival: Fixing a broken cybersecurity market

Quantum-safe hardware-based ('hardsec') solutions will become an essential part of organisations' cybersecurity armour, in particular for critical national infrastructure

Insufficient response to a systemic threat

- Relentless and determined cybercrime activity is one of the most systemically important issues facing the world today, costing the global economy over 10 trillion dollars annually
  - Phishing is the second most common cause of a cyber breach; only stealing or compromising credentials ranks higher
  - 70% of attacks originate at the endpoint but 42% of all endpoints remain unprotected at any given time; in addition, organisations are struggling to control and monitor their large shadow IT estates
  - Massive legacy tech stacks across IT and OT environments that provide critical infrastructure functions continue to run unpatched despite being increasingly vulnerable to rapidly advancing cyber threat vectors
- In response, a gigantic, multi-billion-dollar cybersecurity industry has emerged, comprising a plethora of vendors, all addressing the same problems, predominately with software, and limited to no tangible differentiation in their approach

Software alone cannot solve the problem

- Cybersecurity software is inherently vulnerable and subject to bugs and attacks. With the arrival of powerful quantum computing all current conventional encryption may eventually become obsolete. The most recent hacks of Okta (Oct 2023) or the SolarWinds (Dec 2020) attack are sobering example cases
- Current cybersecurity solutions are costly and re-active rather than pro-active, i.e. cannot anticipate tomorrow's attack vectors
- In fact, having acquired a software solution can create a false perception of having bought an insurance policy. Consequently, cyber fatigue, or apathy to proactively defending against cyberattacks, affects as much as 42 % of companies
- Even patching or updating software to safe standards invites SCM attackers to gain access through the backdoor (see SolarWinds)
- Additionally, information asymmetries between buyers and sellers of cybersecurity products can lead to suboptimal outcomes where the efficacy of a solution is not sufficiently evaluated

Emerging hardsec tech

- Incorporating hardware can future-proof cybersecurity defence: hardware cannot be hacked or easily modified; it can effectively prevent malicious code form entering the systems and cause any damage
- Mandatory use of hardware-enforced solutions is also an essential part of the new National Cybersecurity Strategy by the White House, as it is due to tighten defences for critical national infrastructure
- FPGA chips can provide a significant HW defence: Unlike the highly-flexible CPUs, FPGA chips can only perform a precise range of functions. They don't run any software and can only be programmed using specific physical pins, essentially making them too dumb to hack
- Creating gateways using these chips means data packages can be checked, enabling safe communications and ensuring malicious threats cannot spread across a network. This can be performed at lighting fast speeds without reducing performance or slowing down the system. The technology is considered quantum-safe

Related companies

EU & UK

GARRISON utimaco® XIPHERA
DEEP SECURE | by Forcepoint securosys
NEXOR® SECURE-IC

Global

OWL CYBER DEFENSE Q-Net Security
FUTUREX

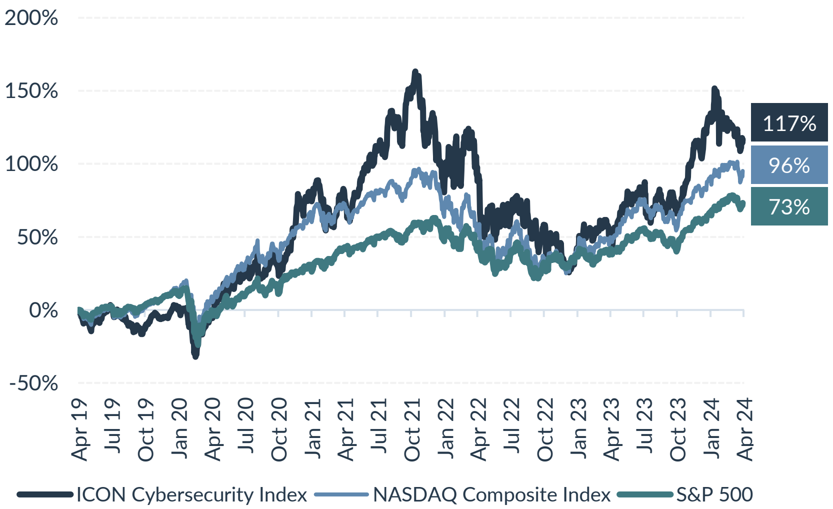
Source(s): IBM's 2022 Cost of Data Breach Report, Varonis

Public market valuation overview

Public markets have stabilised and returned to performance, albeit in a re-based valuation environment

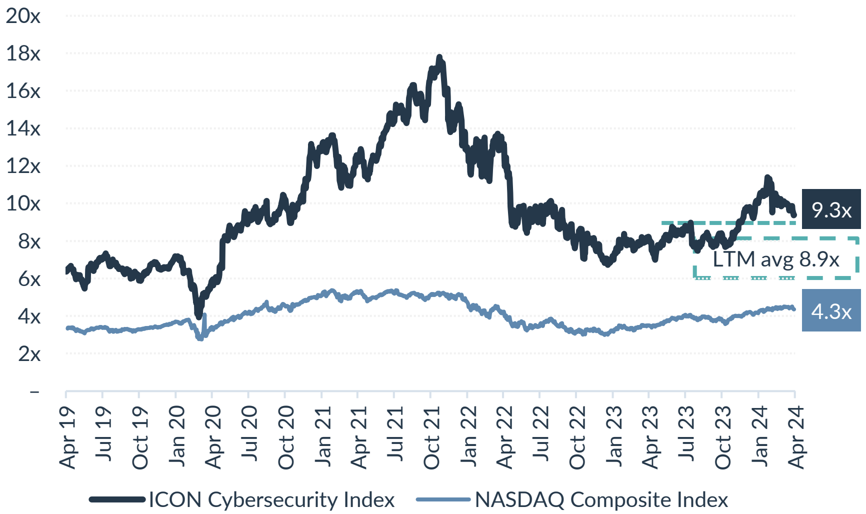
+117% 5-year (+21% 3-year) cybersecurity index performance vs
+96% (+13% 3-year) of the NASDAQ

5 years cybersecurity price performance index



- Following the broader tech market sell-off, publicly listed cybersecurity stocks have experienced a significant rebound
- With markets peaking in Nov 2021, macro-economic volatility forced investors to sharpen their focus on profit metrics and return on capital
- In 2023 cybersecurity stocks experienced a healthy albeit volatile rebound, led by companies with well-balanced Rule of 40 metrics (e.g. Crowdstrike)
- Given the solid market fundamentals and benefitting from a public market recovery driven by a softening interest rate environment, we expect this trend to continue and the sector valuations to stabilise again. This in turn will lead to an ongoing recovery in M&A and eventually fundraising activities

5 years EV/LTM revenue multiples performance



- Following the decline in 2022, valuations have now stabilised at a new base level and continue to outperform the broader tech market significantly
- The recent compression in valuations led to an increase in take-private transactions as private equity is taking advantage of the price levels. In 2023, we saw four large-cap cybersecurity companies being taken off the market by private equity: Absolute Software, ForgeRock, Splunk, Sumo Logic. In Feb 2024, Zerofox and in April 2024, Darktrace followed this take-private trend
- The first IPO in a while by Rubrik on April 25th 2024 on NYSE provides an encouraging sign of a thawing public market for cybersecurity companies
- The last twelve months' average EV/LTM revenue multiple is now at 8.9x, which is more than double the NASDAQ average and still a premium to pre-Covid times

Source(s): ICON, Cap IQ

Select large cap cybersecurity stock performance

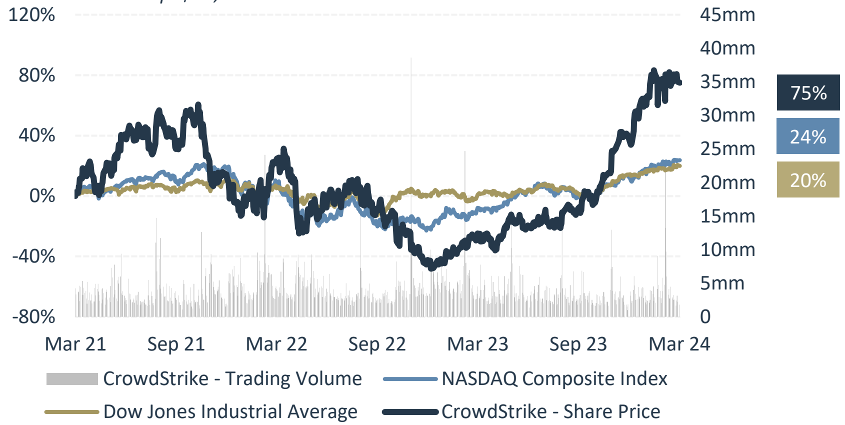
Large cap cybersecurity companies have shown resilience to recent macroeconomic uncertainty and are significantly outperforming from the overall markets

(*Exceptions include Palo Alto's share price dropping by 19% as it lowered its full-year guidance for 2024 due to a change in its product pricing strategy. Similarly, Fortinet's stock dropped 23% despite topline growth of 26% as investors' predictions for the upcoming quarter were less bullish than anticipated by the investor community)

3-year large cap stock trading performance

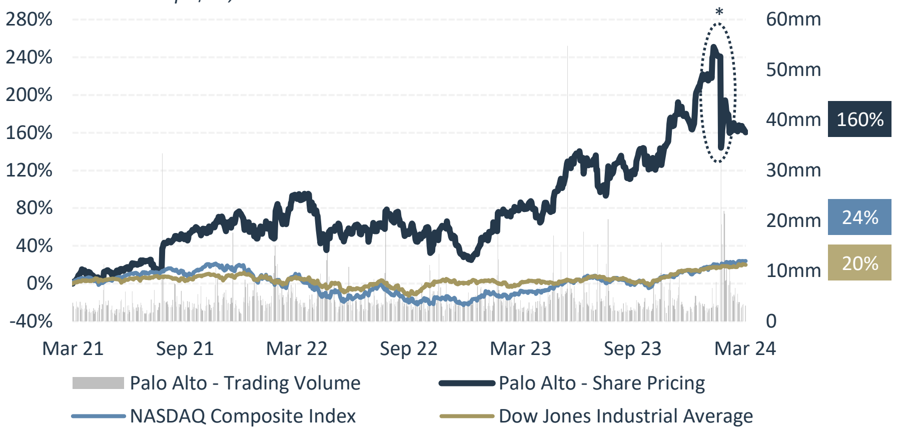
CROWDSTRIKE

Market cap: $73,545bn[(1)]



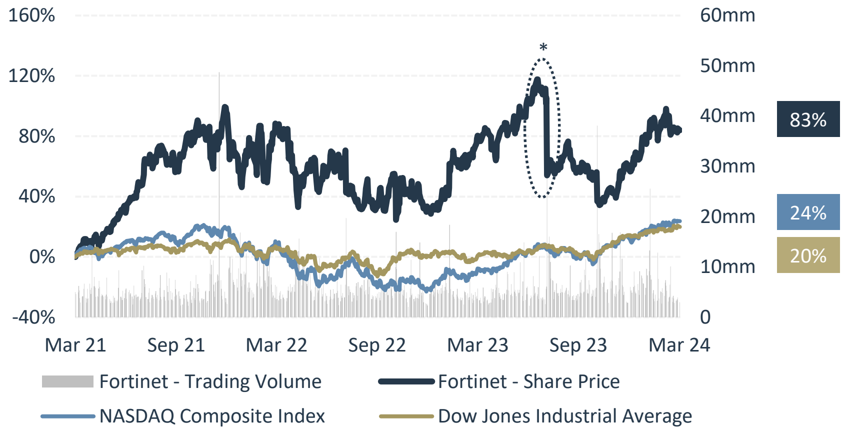
paloalto NETWORKS

Market cap: $94,041bn[(1)]



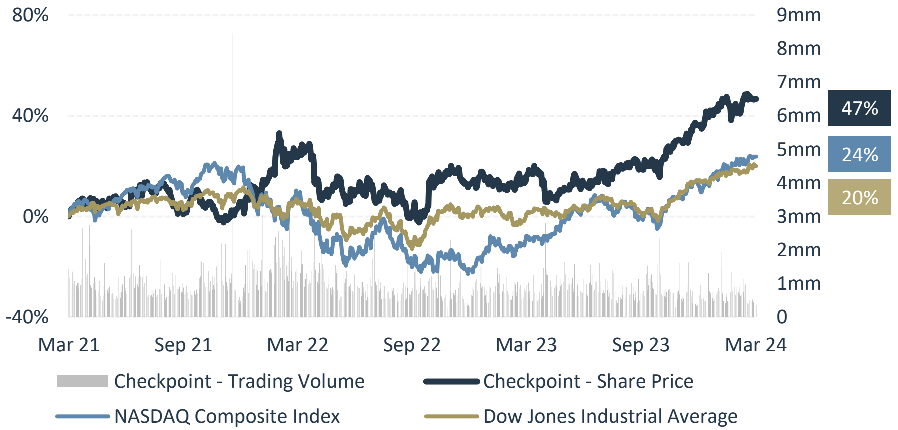
FORTINET

Market cap: $49,360bn[(1)]



CHECK POINT™

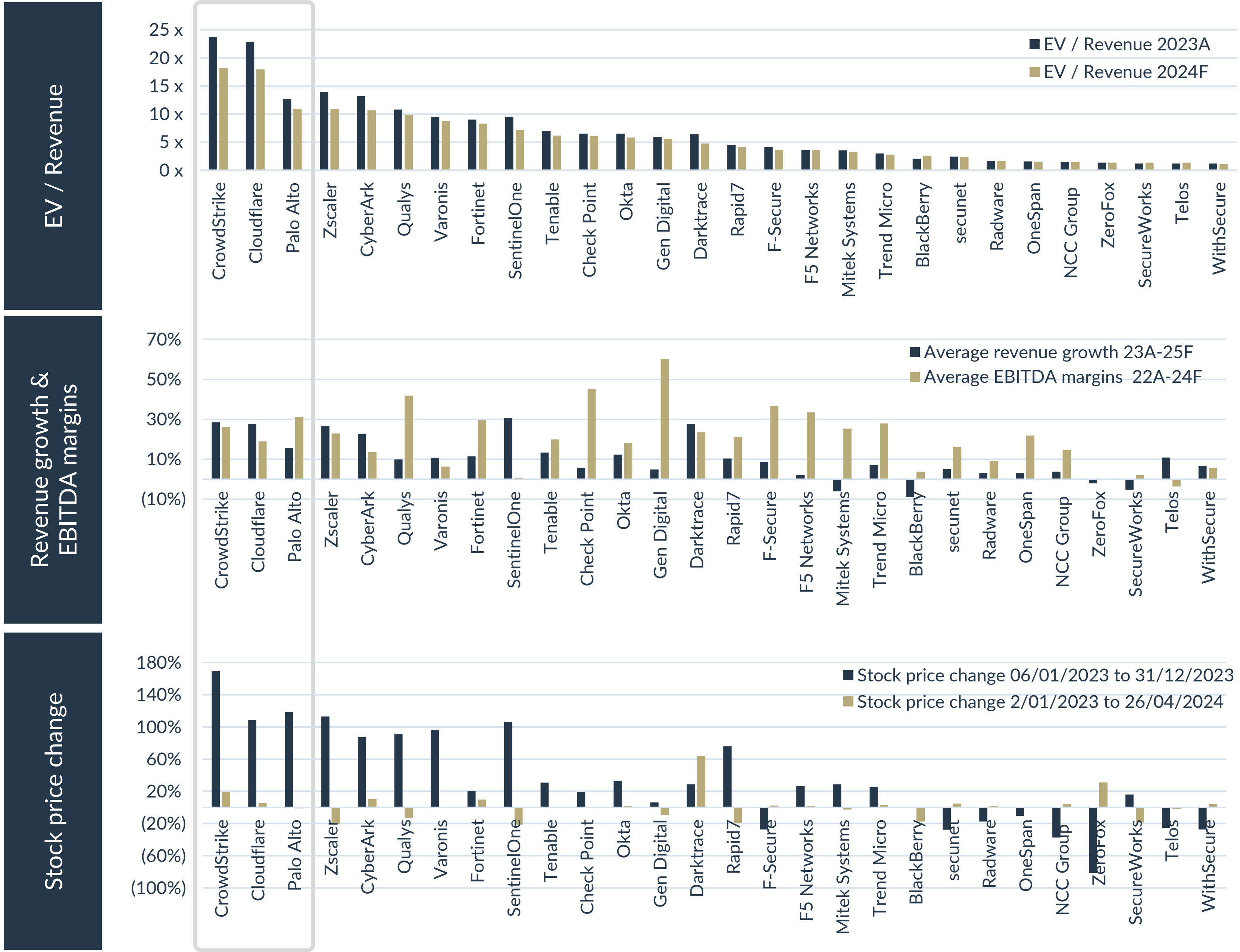
Market cap: $17,315bn[(1)]



Source(s): ICON, Cap IQ
Notes (1): As of 26 April 2024

Key valuation metrics

The fast-growing cohort with strong Rule of 40 metrics was able to recover significant ground and stock prices more than doubled during 2023 (Crowdstrike, Cloudflare, Palo Alto)



Source(s): Capital IQ as of 26 April 2024

Valuation is a result of striking the right balance between growth and profitability…but growth and size matter!

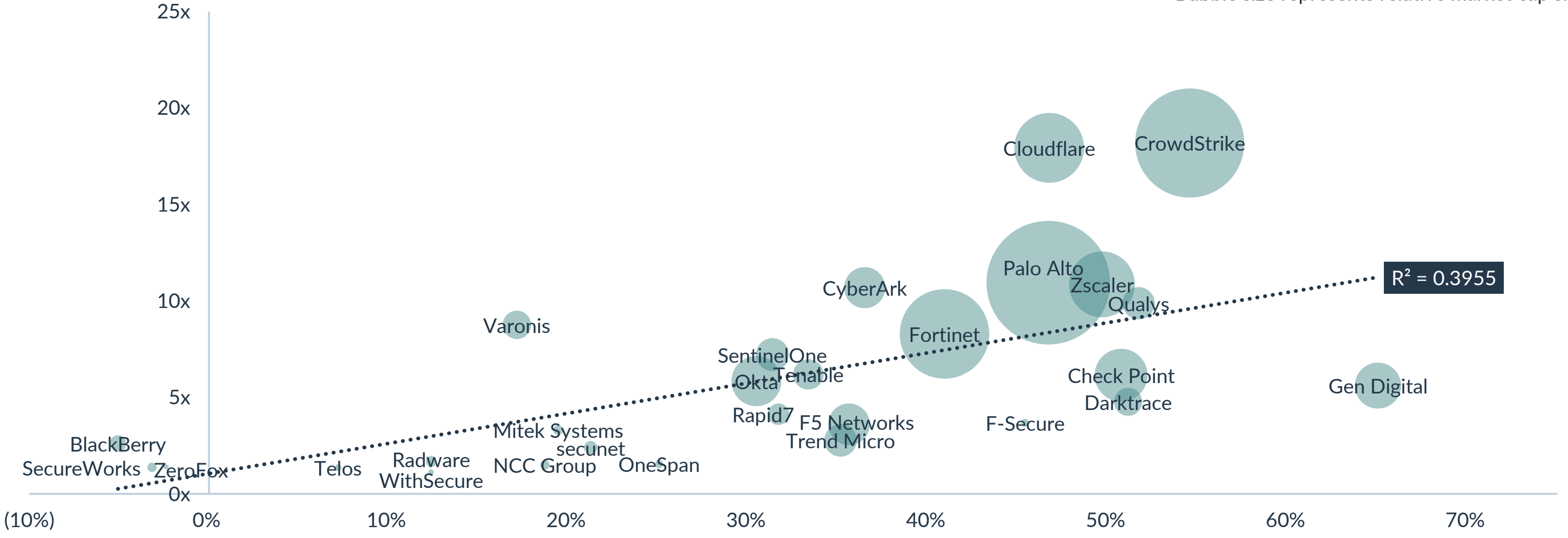
Investors’ focus on profitable growth is the key driver for valuation and has overtaken the “growth at all cost” mantra

As pointed out in Ross Haleliuk’s excellent blog Venture in Security, size and the ability to leverage economies of scale from vast data access are key drivers of cybersecurity industry success (concept of “data gravity”). Other than for the high-flying, fast-growing sector darlings (Cloudflare, Crowdstrike, Zscaler), peer group valuation is strongly correlated to revenue growth & scale

ICON CORPORATE FINANCE

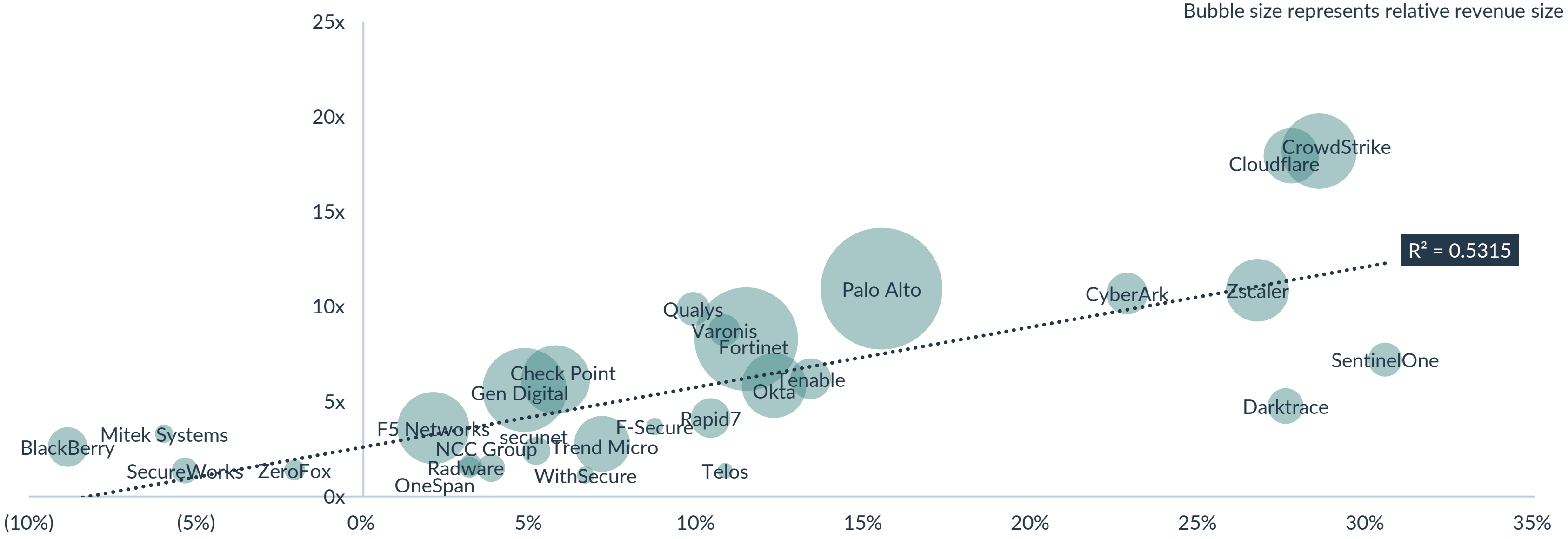
EV/Revenue 2024F vs (avg. Revenue Growth (2023-2025) + avg. EBITDA margins (2023-2025))

Bubble size represents relative market cap size



EV/Revenue 2023E vs avg. Revenue Growth (2023-2025)

Bubble size represents relative revenue size



Source(s): Capital IQ as of 26 April 2024

Publicly listed comparables

Trading metrics summary

USD millions							Enterprise Value Multiples						Operating Statistics					
		Price	% of 52	Market	Net	Enterprise	Revenue			EBITDA			Revenue Growth		EBITDA Margin		
Company	Vertical	(26-Apr-24)	Week High	Cap	Debt	Value	FY 2023A	FY 2024F	FY 2025F	FY 2023A	FY 2024F	FY 2025F	2023-24F	2024-25F	FY 2023A	FY 2024F	FY 2025F
ICON Cybersecurity Comps																	
CrowdStrike	XDR	304.07	83.3%	73,545	(2,649)	70,896	23.7 x	18.2 x	14.4 x	n.m.	n.m.	n.m.	30.4%	26.7%	2.9%	24.3%	27.6%
Cloudflare	Network Security	88.01	75.9%	29,903	(239)	29,665	22.9 x	17.9 x	14.0 x	n.m.	n.m.	n.m.	27.5%	28.0%	(5.5%)	18.5%	19.5%
Palo Alto	Diversified	291.42	76.5%	94,041	(1,187)	92,855	12.6 x	10.9 x	9.5 x	n.m.	36.5 x	29.2 x	15.3%	15.6%	18.3%	30.0%	32.4%
Zscaler	Cloud Security	177.05	68.2%	26,733	(1,221)	25,512	14.0 x	10.9 x	8.7 x	n.m.	48.8 x	36.8 x	28.4%	25.0%	4.3%	22.3%	23.6%
CyberArk	IAM	242.60	85.7%	10,305	(391)	9,914	13.2 x	10.7 x	8.7 x	n.m.	n.m.	n.m.	23.3%	22.3%	(13.3%)	10.7%	16.6%
Qualys	Vulnerability Analytics	170.36	82.6%	6,400	(397)	6,003	10.8 x	9.9 x	9.0 x	31.59 x	23.6 x	21.5 x	9.6%	10.1%	34.3%	42.0%	41.7%
Varonis	Data Security	45.33	85.7%	4,972	(223)	4,750	9.5 x	8.8 x	7.8 x	n.m.	n.m.	n.m.	8.6%	13.0%	(21.1%)	4.9%	7.8%
Fortinet	Network Security	64.18	79.0%	49,360	(1,369)	47,991	9.0 x	8.3 x	7.3 x	35.6 x	28.5 x	24.4 x	9.0%	13.9%	25.4%	29.1%	29.8%
SentinelOne	XDR	21.56	70.1%	6,684	(903)	5,781	9.6 x	7.2 x	5.6 x	n.m.	n.m.	n.m.	32.5%	28.6%	(56.7%)	(5.0%)	6.6%
Tenable	Vulnerability Analytics	45.99	86.0%	5,650	(58)	5,592	7.0 x	6.2 x	5.4 x	n.m.	32.7 x	26.0 x	12.9%	13.8%	(1.4%)	19.0%	21.0%
Check Point	Network Security	151.20	89.6%	17,315	(1,568)	15,747	6.5 x	6.2 x	5.8 x	16.9 x	13.7 x	12.9 x	6.0%	5.5%	38.6%	44.8%	45.1%
Okta	IAM	92.29	80.6%	15,449	(905)	14,544	6.5 x	5.8 x	5.2 x	n.m.	35.3 x	26.2 x	11.6%	13.0%	(18.0%)	16.6%	19.8%
Gen Digital	Consumer and SMB	20.63	84.7%	13,139	8,810	21,949	5.9 x	5.6 x	5.4 x	10.5 x	9.4 x	8.9 x	5.9%	3.8%	56.4%	59.9%	60.5%
Darktrace	XDR	7.50	96.2%	4,829	(324)	4,504	6.4 x	4.8 x	4.0 x	34.4 x	20.4 x	16.8 x	34.9%	20.2%	18.7%	23.4%	23.7%
Rapid7	Vulnerability Analytics	45.93	74.2%	2,884	641	3,526	4.5 x	4.1 x	3.7 x	n.m.	19.6 x	17.3 x	9.7%	11.1%	2.4%	21.1%	21.5%
F-Secure	Endpoint Security	2.22	69.2%	388	196	584	4.2 x	3.7 x	3.6 x	15.9 x	10.2 x	9.5 x	13.7%	3.8%	26.4%	36.1%	37.3%
F5 Networks	Network Security	181.94	91.2%	10,715	(550)	10,165	3.6 x	3.6 x	3.5 x	13.6 x	9.5 x	11.9 x	0.4%	3.8%	26.7%	37.9%	29.1%
Mitek Systems	IAM	12.70	78.2%	598	20	618	3.5 x	3.3 x	4.1 x	15.5 x	13.8 x	15.2 x	6.8%	(18.7%)	22.8%	24.0%	26.7%
Trend Micro	Cloud Security	49.39	86.5%	6,623	(1,899)	4,724	3.0 x	2.8 x	2.6 x	12.2 x	10.2 x	9.0 x	7.6%	6.6%	24.5%	27.2%	28.8%
BlackBerry	Endpoint Security	2.83	49.5%	1,666	15	1,681	2.0 x	2.6 x	2.5 x	n.m.	n.m.	39.3 x	(21.6%)	3.9%	0.2%	1.2%	6.4%
secunet	Cybersecurity services	163.13	59.7%	1,055	(24)	1,032	2.5 x	2.4 x	2.2 x	19.3 x	15.2 x	13.6 x	2.2%	8.2%	12.7%	15.8%	16.3%
Radware	Network	17.03	81.3%	712	(271)	441	1.7 x	1.7 x	1.6 x	n.m.	21.1 x	15.3 x	0.7%	5.8%	(9.4%)	7.9%	10.4%
OneSpan	IAM	10.79	62.7%	408	(34)	374	1.6 x	1.5 x	1.5 x	n.m.	7.7 x	6.4 x	2.8%	3.5%	(2.2%)	20.2%	23.5%
NCC Group	Cybersecurity services	1.67	97.7%	528	104	632	1.5 x	1.5 x	1.4 x	13.2 x	10.7 x	9.1 x	2.0%	5.7%	11.6%	14.1%	15.6%
ZeroFox	Threat mgmt	1.14	91.2%	142	168	311	1.4 x	1.4 x	1.4 x	n.m.	n.m.	n.a.	(0.6%)	(3.5%)	(8.4%)	(0.7%)	0.0%
SecureWorks	Cybersecurity services	6.00	63.2%	522	(61)	461	1.2 x	1.4 x	1.4 x	n.m.	n.m.	29.5 x	(12.1%)	1.4%	(17.9%)	(0.3%)	4.6%
Telos	Network Security	3.57	71.4%	262	(88)	175	1.2 x	1.4 x	1.0 x	n.m.	n.m.	36.5 x	(12.2%)	33.8%	(24.0%)	(10.1%)	2.8%
WithSecure	Endpoint Security	1.15	70.5%	203	(21)	182	1.2 x	1.1 x	1.1 x	n.m.	27.4 x	14.4 x	6.1%	7.2%	(18.4%)	4.1%	7.3%
Median							**5.2 x**	**4.5 x**	**4.0 x**	**15.9 x**	**19.6 x**	**16.0 x**	**8.1%**	**9.1%**	**2.7%**	**19.6%**	**21.2%**
Mean							**6.8 x**	**5.9 x**	**5.1 x**	**19.9 x**	**20.7 x**	**19.5 x**	**9.3%**	**11.1%**	**4.6%**	**19.3%**	**21.6%**
Top quartile							**9.5 x**	**8.4 x**	**7.4 x**	**25.4 x**	**28.0 x**	**26.1 x**	**14.1%**	**16.8%**	**23.2%**	**27.7%**	**28.9%**
Bottom quartile							**2.0 x**	**2.2 x**	**2.1 x**	**13.4 x**	**10.4 x**	**12.2 x**	**2.1%**	**3.9%**	**(10.4%)**	**7.2%**	**9.7%**

Source(s): Capital IQ as of 26 April 2024

Cybersecurity M&A activity USA & EUROPE

Bracing the economic uncertainty and a challenging public equity market environment, cybersecurity M&A activity remained stable. This increase was largely due to highly active private equity investors who accounted for 47% of the LTM M&A volume

USA Cybersecurity M&A– Key Stats

LTM Q2 2023 to Q1 2024

84 (-30% YoY)

Strategic deals

77 (-25% YoY)

PE deals

$69bn

Largest Strategic Deal[1]

$2.5bn

Largest PE Deal[2]

Europe Cybersecurity M&A– Key Stats

LTM Q2 2023 to Q1 2024

82 (-7% YoY)

Strategic deals

64 (-16% YoY)

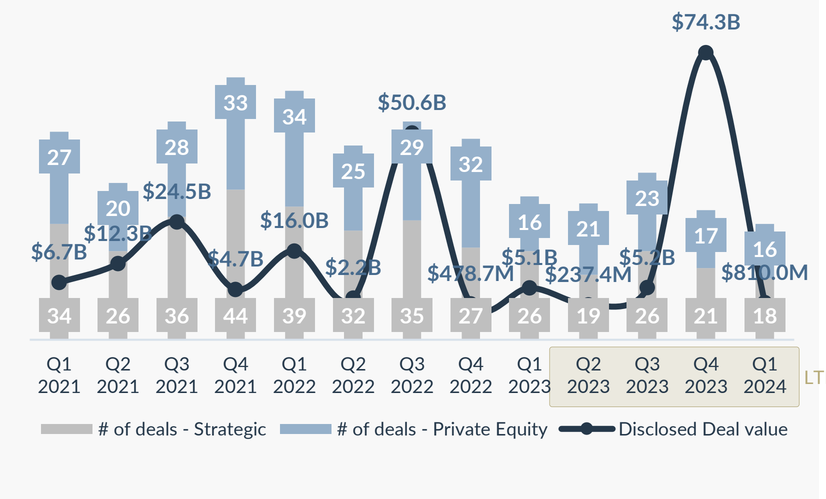
PE deals

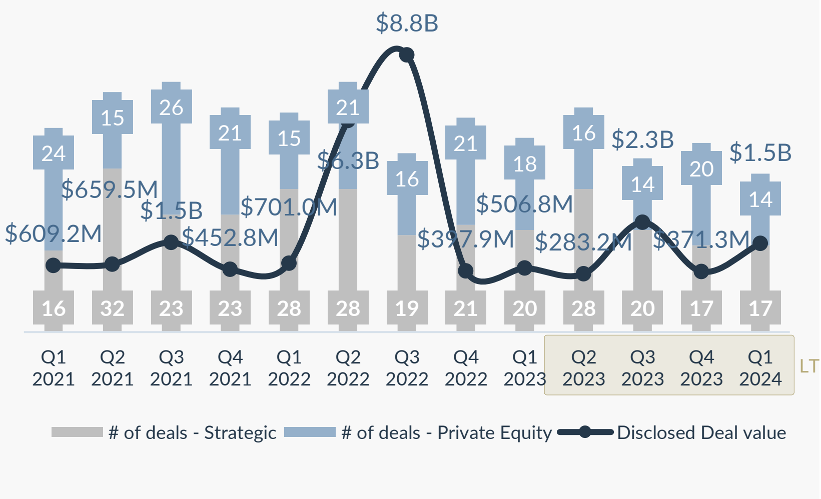
$1.5bn

Largest Strategic Deal[3]

$1bn

Largest PE Deal[4]





Source(s): ICON, Pitchbook

Note(s): (1) 22nd Nov 2023: Broadcom's acquisition of VM Ware for $69bn (2) 29th Sept 2023: Everfox acquired by TPG for $2.5bn (3) 28th Mar 2024: $1.5bn Spirent's acquisition by KeySight (4) 15th July 2023: Wendel Group acquired of Scalian for $1bn

Recent European M&A highlights

THOMABRAVO

acquired

DARKTRACE

AI-powered threat management

- **Date:** 26/04/20224
- **Target Description:** AI-enabled security platform that delivers a proactive approach to cyber resilience, providing pre-emptive visibility into security posture, real-time detection of and autonomous response to known and unknown threats

KnowBe4

acquired

egress

Email security

- **Date:** 24/04/2024
- **Target Description:** AI-powered email security platform, using adaptive learning capabilities to help prevent, protect and defend organisations against advanced email cybersecurity threats

HORNETSECURITY

acquired

vade

Email security

- **Date:** 05/03/2024
- **Target Description:** Email security platform, fed by data from huge mailboxes, to detect threats such as spam, malware, and phishing links and block them in real time, enabling enterprises to filter threat emails

proofpoint.

acquired

TESSIAN

Email security

- **Date:** 30/10/2023
- **Target Description:** Email security software platform that helps enterprises counteract human error and significantly reduce the risk of data loss

Notable global cybersecurity M&A activity

Date	Acquirer	Target	Target company description	EV ($m)	EV / Rev
Apr-24	THOMABRAVO	DARKTRACE	AI-powered cyber-threat defence technology solutions	5,212.5	8.5x
Mar-24	zscaler	Avalor	Data security platform that acts as a source of truth for cybersecurity assets	350.0	n.a.
Mar-24	CROWDSTRIKE	FLOW.	Data security platform offering features, such as automating data discovery and classification, detecting risk and managing data posture	115.0	n.a.
Feb-24	HAVELI	ZEROFOX	Advanced AI analytics, digital risk, full-spectrum threat intelligence, and incident and takedown response	322.4	1.4x
Nov-23	paloalto	TALON Cyber Security	Cybersecurity software for the distributed workforce.	458.6	n.a.
Oct-23	paloalto	Dig Security	Develops data detection and response solution. it provides real-time visibility, control, and protection of user's data assets	251.1	n.a.
Oct-23	Blackstone	RTX	Cybersecurity, Intelligence and Services Business within Raytheon Segment of RTX Corporation	1,300.0	n.a.
Oct-23	The Chertoff Group	Trustwave	Security operations platform offering managed detection and response, PS, pen-testing, database security, email security and management.	205.0	n.a.
Sep-23	CISCO	splunk>	Unified security and observability platform that helps allowing search, monitor, and analyze machine-generated data.	28,549.9	7.4x
Aug-23	CHECK POINT	perimeter 81	Designs and develops an online platform designed to simplify local networks, cloud infrastructures, and business applications	490.0	n.a.
Aug-23	rubrik	Laminar	Data security posture management (DSPM) platform that protects data in cloud-native applications	225.0	n.a.
Jul-23	THALES	imperva	Application data security and compliance platform that provides data governance and protection solutions	3,600.0	7.2x
Jul-23	SpireCapital	COBWEBS TECHNOLOGIES	Threat Intelligence solutions for enforcement bodies, national security agencies, and financial services worldwide	200.0	n.a.
Jun-23	THALES	tesserent	Provides cyber security consulting, cloud, and managed services	147.7	1.7x
May-23	IBM	POLAR	Data Security Posture Management platform to discover and calssify managed, unmanaged, and shadowed data	60.0	n.a.
May-23	CROSSPOINT CAPITAL	ABSOLUTE	Provides solutions that support the management, visibility, control and self-healing capabilities to endpoints, applications, and network connections	867.6	3.9x
Apr-23	F-Secure	LookoutLife	Mobile security platform that provides device security, privacy, online safety, identity, and financial protection to consumers	223.5	5.6x
Mar-23	RAPID7	MINERVA CYBER TECHNOLOGIES	Provider of anti-evasion and ransomware prevention technology	37.9	n.a.
Mar-23	hp	axis security	Security Services Edge (SSE) platform that enables access to corporate and public-cloud resources and secure enterprise applications	412.0	n.a.
Feb-23	FP FRANCISCO PARTNERS	sumo logic	SIEM analytics and observability platform	1,397.4	4.6x

Source(s): ICON, Cap IQ, Pitchbook

Cybersecurity fundraising activity

Fundraising activity is still lagging behind historic trends. The US continues to lead the way in global cybersecurity fundraising, accounting for almost twice as many funding rounds in the last twelve months compared to Europe. However, European cybersecurity fundraising has gained significant traction over recent years and activity remained more resilient to recent economic uncertainty

USA Cybersecurity funding rounds – Key Stats

LTM Q2 2023 to Q1 2024

167

Funding rounds LTM

387

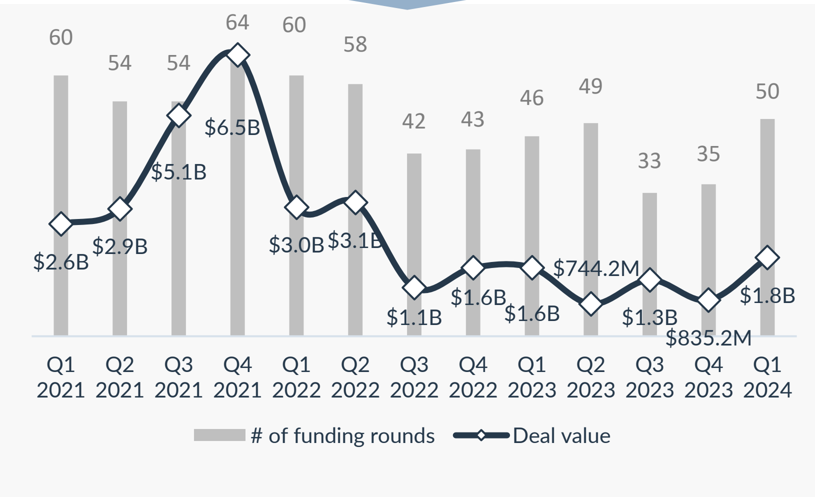
Investors

$400m

LTM Largest deal[1]

$32.1bn

Cumulative deal value



Europe Cybersecurity funding rounds – Key Stats

LTM Q2 2023 to Q1 2024

80

Funding rounds LTM

126

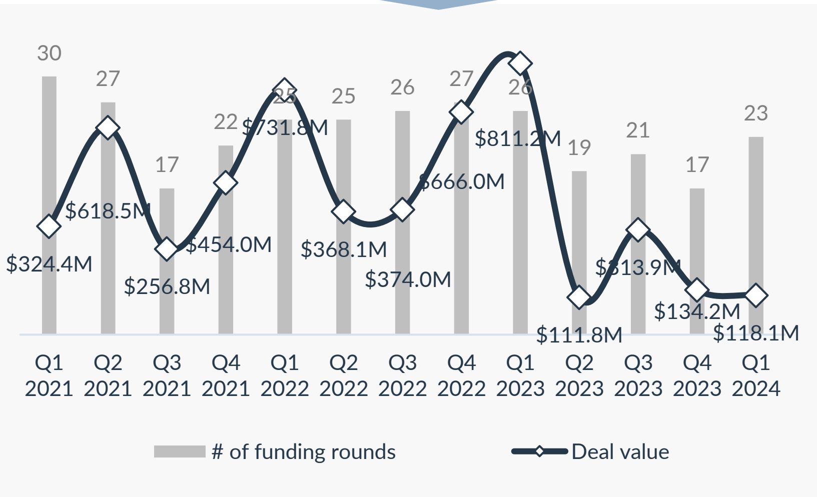
Investors

$100M

LTM Largest deal[2]

$5.3bn

Cumulative deal value



Source(s): ICON, Pitchbook

Note(s): (1) 01 Mar 2024: Accel's $400m equity investment into Axonius (2) 18th Jul 2023: Spectrum's $100m equity investment into Netcraft

Recent European fundraising highlights

NORD SECURITY

Raised $100m from

WARBURG PINCUS

NOVATOR

BurdaPrincipal Investments

Digital security & privacy platform

- **Date**: 28/09/2023
- **Deal type: PE growth**
- **Raised to date**: $200m
- **Post money valuation**: $2.9bn
- **Target description**: Developer of digital security and privacy solutions intended for businesses and consumers

FILIGRAN

Raised $16m from

Accel

Motier ventures

MOONFIRE

Threat management software

- **Date**: 29/02/2024
- **Deal type: Series A**
- **Raised to date**: $21.6m
- **Post money valuation**: N/a
- **Target description**: Developer of cyber threat intelligence platform designed to offer cybersecurity and crisis management services

LYNX SOFTWARE TECHNOLOGIES

Raised $18m from

FORGEPOINT CAPITAL

Santander

Fraud prevention software

- **Date**: 18/07/2023
- **Deal type: Series A**
- **Raised to date**: $18m
- **Post money valuation**: N/a
- **Target description**: Developer of artificial intelligence-based anti-fraud and anti-money laundering products designed to predict, detect, and prevent fraud across all channels

HarfangLab Deep Integrity | Paramount Security

Raised $33m from

Crédit Mutuel Innovation

elaia

MassMutual Ventures

Endpoint Detection and Response

- **Date**: 9/10/2023
- **Deal type: Series A**
- **Raised to date**: $33m
- **Post money valuation**: $120m
- **Target description**: Developer of a cloud-based threat detection and response software designed to offer real-time threat identification, threat elimination, and attack prevention

Overview of specialised cybersecurity funds

Firm	Location	HQ	AUM	Selected Cybersecurity Portfolio Companies					
ALLEGISCYBER	🇺🇸	Palo Alto	n.a.	vicarius Jan-24	DRAGOS Sep-23	cyberGRX Jun-23	source defense Apr-22	varmour Sep-20	
BALLISTIC VENTURES	🇺🇸	San Francisco	n.a.	ALETHEA Apr-24	Reach Mar-24	ArmorCode Oct-23	AUTHMIND Jul-23	SPECTEROPS Jul-23	oligo Feb-23
ClearSky	🇺🇸	North Palm Beach	$840m	Guardz. Dec-23	cyberGRX Jun-23	MITIGA Mar-23	revelstoke Mar-23	AppOmni May-22	Phylum May-22
evolution EQUITY PARTNERS	🇺🇸 🇨🇭	New York, Zurich	$1.5b	Protect AI Jul-23	Metomic Feb-23	BEYOND IDENTITY Feb-22	PENTERA Dec-21	panaseer May-21	ONAPSIS Apr-18
FORGEPOINT CAPITAL	🇺🇸	San Mateo	$770m	LUMU Sep-23	SYMMETRY SYSTEMS Aug-23	converge Aug-23	whistic Jun-22	SUREFIRE Jan-22	Constella INTELLIGENCE Mar-20
PALADIN CAPITAL GROUP	🇺🇸	Washington	$1b	hushmesh Aug-23	SECURE CODE WARRIOR Aug-23	RADICL Nation State Threat Defense Jun-23	GREYNOISE Jun-22	semperis May-22	NISOS May-22
33N VENTURES	🇵🇹	Porto	$165m	Panorays Mar-23	hackuity Oct-22	cybersixgill Mar-22	SafeBreach May-22	IriusRisk Jul-18	
Strategic Cyber Ventures	🇺🇸	Washington	n.a.	evo Mar-23	HackNotice Jun-22	Impervious Apr-22	SNAPATTACK Nov-21	iddataweb Feb-17	
SYN VENTURES	🇺🇸	Boston	$500m	Phosphorus Dec-23	Adlumin Oct-23	Upfort Oct-23	METABASE Q Aug-23	revelstoke Mar-23	
TENELEVEN	🇺🇸	West Palm Beach	$1b	DEVICE AUTHORITY Feb-24	VULCAN. Nov-23	cyberGRX Jun-23	CYWARE Jun-23	IMMUTA Jun-22	
YL VENTURES	🇺🇸 🇮🇱	Mill Valley, CA	$800m	VULCAN. Nov-23	Spera Mar-23	opus Sep-22	Hunters. Jan-22	eureka Jan-22	
TIN CAPITAL	🇳🇱	Utrecht, Netherlands	$65m	eye cyber security Mar-24	EGERIE Jan-23	Probely July-22	emproof embedded security July-22	awen COLLECTIVE May-22	breachlock Mar-22

Source(s): ICON, Pitchbook. Cap IQ
Notes: Dates indicate last funding rounds

ICON at a glance

Specialist independent M&A and fundraising adviser to fast-growing technology businesses

Leader in technology deals

250+	190+	7/10	15
Deals	Combined years of deal making	7 of last 10 deals were cross border	Investment Bankers

Independent

Independently owned and 100% committed. Fully aligned with clients with results-based fees

Trusted

Consistent track record over 20 years. Built significant intellectual capital. Partner led teams

Global

Local advice but extensive global reach. Superb record of cross-border deals

Tech Focus

Deep understanding of disruptive Tech business models and the entrepreneurial journey

Strong sub-sector expertise

- Enterprise Software
- Cybersecurity
- IT Services
- Cloud Solutions

ICON CORPORATE FINANCE

ICON CORPORATE FINANCE

London | Bristol | San Francisco

www.iconcorpfin.com

Florian Depner
Director
Florian@iconcorpfin.com