AXA VENTURE PARTNERS

White Paper
by Camille Périssère
Associate

2024 cybersecurity market trends

New York - London - Paris

www.axavp.com

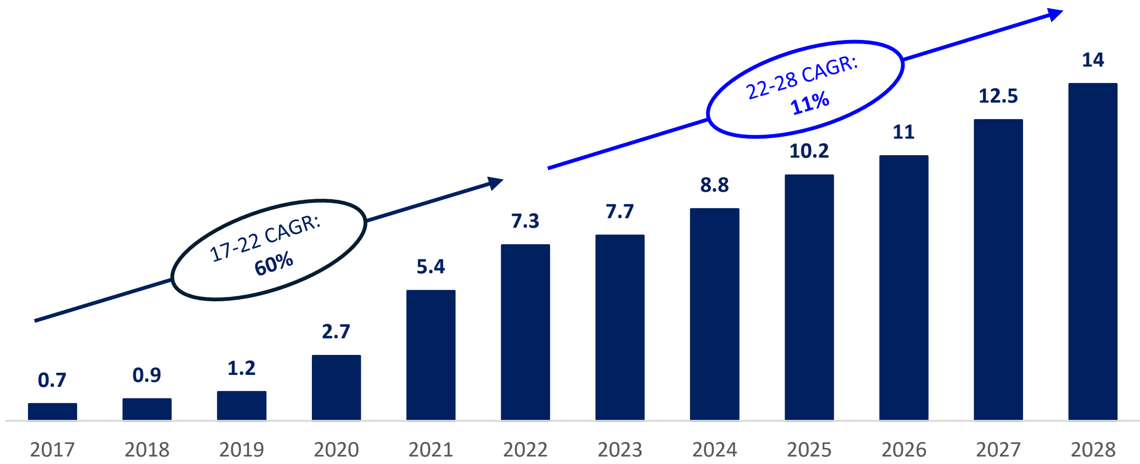
Cybersecurity is not a new topic.

We all can picture the Trojan attack in the 1990s or the ILOVEYOU worm in the 2000s, or if you were not born yet, you might at least have in mind the typical hacking scene in Hollywood movies with the several pop-up messages on the computer screen (ALERT SYSTEM BREACHED!) – the one that would make every cybersecurity professional cringe. These (stereotypical) images are now deeply rooted in the collective imagination and demonstrate how much cybersecurity has become a central topic for governments, businesses, IT leaders but also in our personal lives. And for good reasons.

In a world escaping from the pandemic and entering global conflicts, the past couple of years have created a renewed sense of urgency when it comes to security. First, cybersecurity remains on the front page (e.g. recent attack in January 2024 on Microsoft's systems by the Russian hacking group Midnight Blizzard), but these tentacular attacks also affect everyone. In 2022, 9 businesses out of 10 experienced at least one cyber attack in the last 12 months[i]. Recent cyberattacks on core government infrastructures such as the shutdown of the US Colonial Pipeline had huge financial and political consequences for the governmental defense. The recent SolarWinds scandal – also conducted by Midnight Blizzard and considered as the biggest cybersecurity breaches of the 21st century – affected 20,000 organizations around the world including main US government agencies or tech giants such as Microsoft, Intel, Deloitte which used the SolarWinds' system management tool for their network and infrastructure monitoring[ii]. In this case, the dwell time (i.e., the time between the moment an attack is started and the moment it is discovered) amounted to 14 months, illustrating the level of sophistication of the code written by hackers that were presumably able to collect so many data that delimiting the real impact of the attack is almost impossible today.

The advent of remote working since Covid crisis has intensified the trends already initiated in recent years with the continuous shift from monolithic to distributed systems, from on-premises to cloud infrastructure, contributing to more and more connected and interlinked systems. As a result, the number of attacks and data breaches exploded since 2020 while the complexity and the associated costs of those attacks have exploded as well - from $2.7 trillion in 2020 to more than $7 trillion in 2023[iii], measured as a country, it would be the world's third largest economy after the US and China.

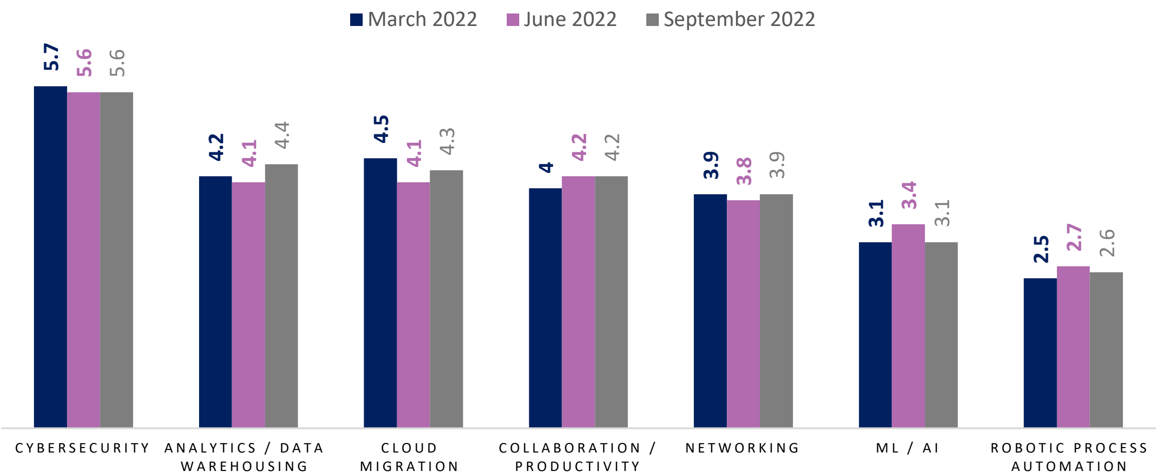
Estimate cost of cybercrime, worldwide ($tr)



Source: Cybersecurity Ventures

Logically enough, and most especially during economic slowdown considering the potential costs at stake, cybersecurity remains the highest priority budget spend areas for IT leaders, ahead of cloud migration initiatives or analytics and data warehousing, or even ML / AI efforts. In fact, 66% of CTOs interviewed by Gartner as part of a survey with over 2,000 CIOs planned to increase their investments in cybersecurity[iv].

Main technology areas aiming to be addressed by IT leaders in the year (av. ranking)

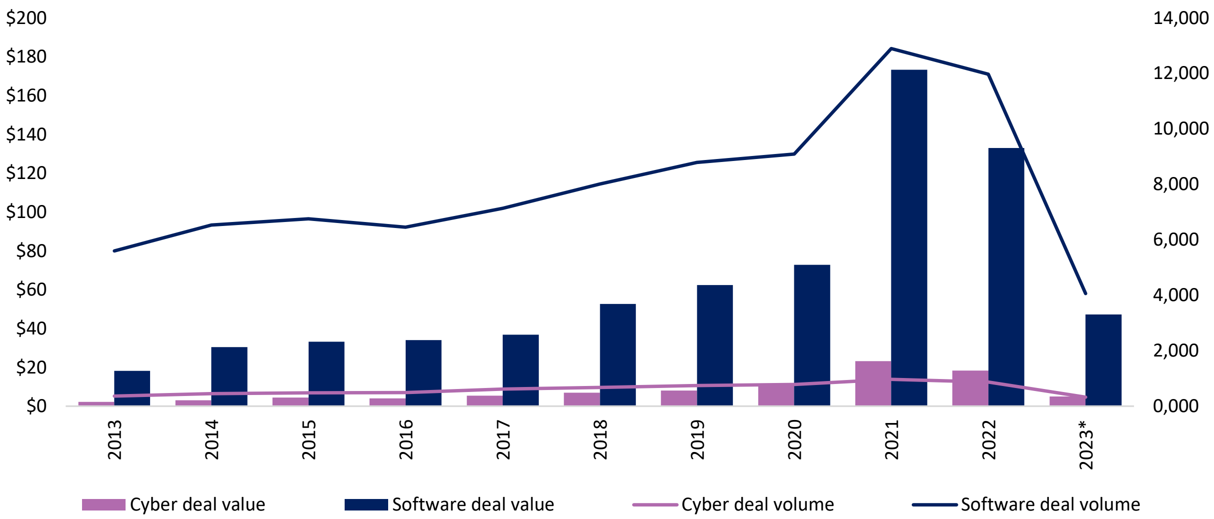


Source: CNBC and ETR Survey

Not surprisingly, cybersecurity has been a hot topic for VC investors for years.

Given what is at stake, VC investors have been continuously and closely tracking innovation in this field. In 2021, cybersecurity deals accounted for 13% of the total software deal value and 8% of the volume. Today, market leaders such as Palo Alto Networks, ZScaler, Fortinet, and CrowdStrike have been continuously outperforming the rest of the software industry and enjoyed strong last quarters.

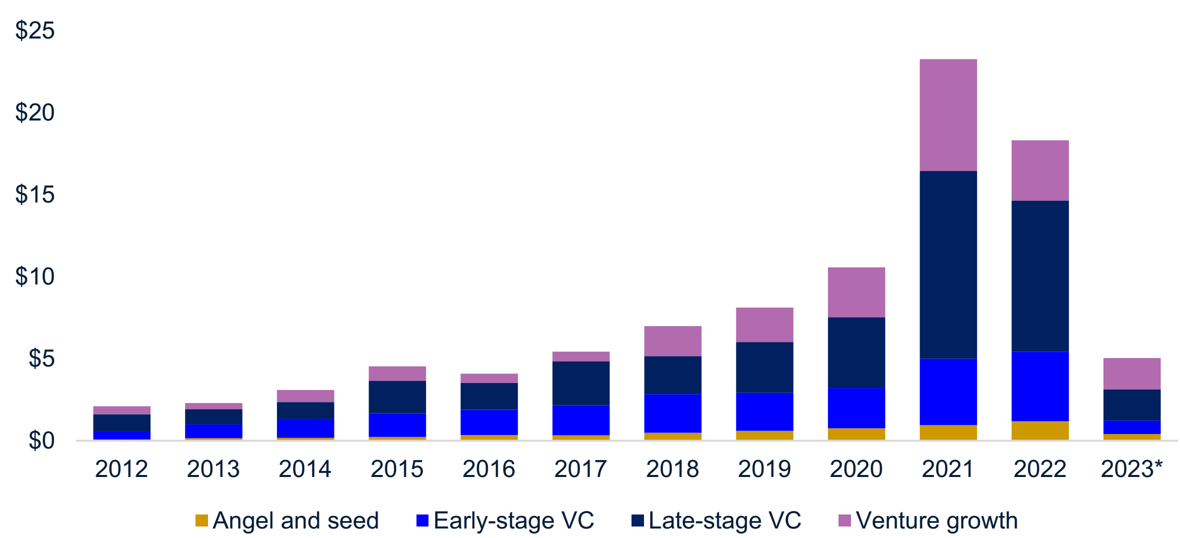
Deal activity in the software market vs. cybersecurity, North America & Europe ($bn)



Source: Pitchbook

However, in this context of volatile economic conditions, cybersecurity is not spared by the general VC market collapse. The total cybersecurity deal volume surprisingly showed not so much resilience by dropping by 44% in H1'23 YoY (vs. 32% for the overall software industry), and the deal value severely felt by 60% YoY while the recorded decrease was 40% for the software industry, demonstrating a significant correction in the cybersecurity startups value.

Cybersecurity VC volume by stage, North America & Europe in H1'23 ($bn)



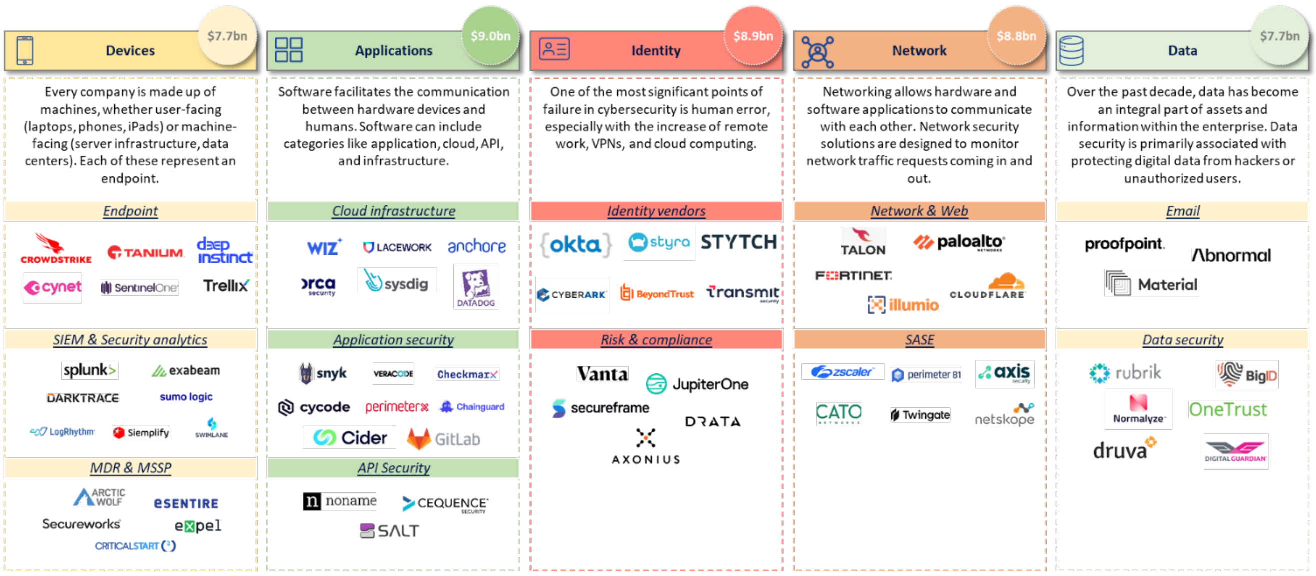
Source: Pitchbook

If we look at the VC volume by stage, the volume of seed & early stage deals drastically dropped by more than half in H1'23 YoY, later stage deals accounting for 75% of total volume of H1'23 deals, questioning investor's stable level of confidence in cybersecurity startups' ability to innovate. Even though that needs to be qualified and should be read in conjunction with the general valuation collapse pushing most startups to postpone their fundraising (see below), the observation is still quite counterintuitive. As mentioned above, cybersecurity is anticipated to remain the main budget priority for CTOs, over AI, which, however, attracted more investments from VCs in H1'23 for a total deal value of $39.5bn (vs. $5bn in cybersecurity).

As a result, we can legitimately wonder what could be the barriers to cybersecurity investments? Here, in our view, are some possible explanations:

1/ Generally speaking, the modern IT enterprise stack is fragmented and complex. There has been a proliferation of cybersecurity solutions aiming to solve one specific pain point by protecting one isolated component of the technology stack. Consequently, distinguishing different product offerings available in the market can be challenging from a buyer standpoint, but also from an investor perspective. Plenty of market studies out there have tried to segment the cybersecurity landscape and we think that classifying solutions by main attack surface areas they are trying to protect can be the best way to approach the problem. Again, the complexity of the industry means that no segmentation is perfect. Indeed, more and more companies are trying to play in multiple buckets to offer an end-to-end solution as CTOs are now looking for consolidating spending.

Mapping of the cybersecurity landscape by entry points



Source: Contrary research, Pitchbook

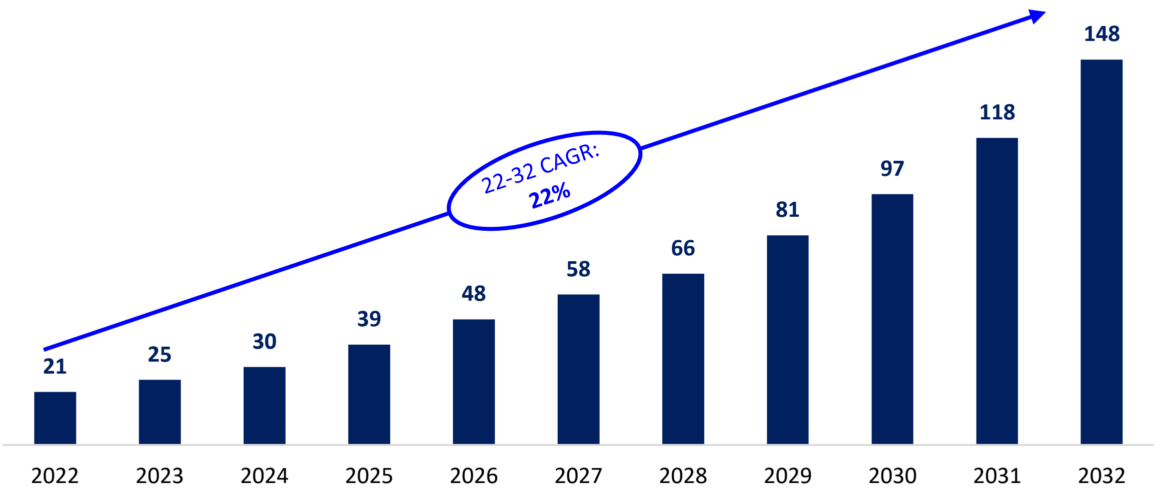
Indeed, as budgets are globally being restricted even in large enterprises, CTOs are looking at cybersecurity vendors that can integrate across their heterogeneous environment from endpoint to cloud. As a result, we have been observing over the last few years a vendor consolidation in the market with the biggest incumbents trying to extend their product offering, mostly through M&A.

Take, for instance, Palo Alto Networks, which started as a network security tool but has transformed into a comprehensive platform by incorporating offerings from 16 acquisitions in the past 5 years. Like Crowdstrike, which has evolved from providing single endpoint security into multiple product categories in security. This consolidation movement has been drastically facilitating the process for CTOs to purchase one product that tackles a wide array of challenges.

2/ Market consolidation should create some exit opportunities for established startups but raise barriers to scale for early-stage companies.

Let's take the eloquent example of the cloud security market which is undoubtedly one of the most rapidly evolving categories in cybersecurity. In the past 3 years, notably due to the pandemic, there has been a massive adoption of the cloud that creates a meaningful opportunity for criminals, given the diversity of available attack vectors. Indeed by 2025, 95% of digital workloads are expected to be hosted in the cloud, a major increase from the 30% recorded in 2021[v]. Public cloud revenue already grew from $32bn in 2018 to over $400bn in 2021. Cloud security market is expected to boom accordingly.

Global cloud security market ($bn)



Source: Globe NewsWire

Although relatively nascent, the cloud security market is already being consolidated by three categories of players with colossal financial capabilities to be injected in innovation. Indeed, besides the security incumbents already mentioned before, some "cloud-native" security (former) startups but also tech giants are currently competing to take a leadership position in the cloud security market.

On one hand, some emerging challengers with only 2-3 years of existence have positioned themselves as a key player in the cloud security segment. Take Wiz for instance, which has developed a cloud security platform designed to help businesses secure their cloud infrastructure at scale. Wiz provides a comprehensive cloud-native platform that gives customers actionable insights within minutes, showing them their areas of vulnerabilities, the risks they face and how to resolve them. Founded in 2020, the former startup surpassed $100 million in ARR in only 18 months, with blue chip clients including BMW, Morgan Stanley, Salesforce, Slack, etc., and is now value at around $10bn after its last $300m Series D round in February 2023. Same hyper-growth trajectory for Orca Security, another US-based cloud native security platform. As of today, the two startups combine a total financing of $1.5bn, both to be injected in product development and most promising technologies such as DSPM (Data Security Posture Management, see below).

On the other hand, major cloud providers (Amazon, Google, Microsoft) are also taking a more active role in security. In theory, they operate under a shared responsibility model with their clients, meaning that they are responsible for managing the security and compliance of the platform in terms of network, container, runtime, and isolation but their clients will manage the security of their applications, workloads and data by working with third-parties cloud security vendors. Having said that, major cloud providers undoubtedly want to take a more active role in security by leveraging a facilitated go to market strategy selling their security products to existing cloud clients. For instance, in January 2023, Microsoft announced that their security business had surpasses $10bn in revenue.

3/ Finally, the exit question is also a key concern for early-stage investors considering lower valuations and, sometimes, sovereignty concerns that can be a barrier to internationalization and cross-border M&A, especially in Europe.

As we mentioned before, the volume of cyber early-stage deals dropped drastically in 2023. The first seven months of this year saw only 26 cybersecurity startups being acquired in North America and Europe – putting the dealmaking at its slowest pace since 2017. The drop can be partly explained by the general cut in valuations that pushes startups (and their shareholders) to postpone the sale or fundraising rounds. However, this goes without saying, runway may be coming to an end and experts expect that Q4-23 will see dealmaking really pick up in a more buyers' market. Startups and their historic investors would be obliged to accept down rounds, and this is already the case. We've seen little evidence of changed behaviour regarding low price tolerance. Unicorns are not closing acquisition deals, as evidenced by Cybereason's valuation cut after failing to find a buyer. Data management vendor Informatica acquired data security scale-up, Privitar, for an undisclosed valuation, suggesting the company's last private valuation of $435m was not reached.

This trend is relatively common to all the tech and ecosystem but may be more important in cybersecurity as valuation reached astronomic levels in 2021 up to 14-15x EV/revenue in Q1 '22 vs. an average of 9-10x for software companies at the same period, according to SEG SaaS Index[vi]. Today, valuation multiples have been drastically cut, now down to below pre-pandemic levels and decreased by 50% or more to reach 7-8x for cybersecurity companies vs. 5-6x for SaaS[vii] – leaving investors clearly worried about not reaching their return expectations.

There is another concern among investors when it comes to examining exit opportunities from early-stage startups. In Europe and more specifically in recent years, cybersecurity has been considered the cornerstone of European digital sovereignty. Each European countries has seen the emergence of local cybersecurity leaders, but the European landscape remains very fragmented, as opposed to the US. Indeed, in the first 7 months of 2023, c. 60% of M&A cybersecurity deals were in between US companies, demonstrating the consolidation trend in the North American cybersecurity market highlighted by massive acquisitions such as the recent acquisition of Splunk by Cisco for $28bn[viii]. However, data shows little to no cross-border deals between the US and Europe: only 3 deals were US acquirers of European companies, and 2 European companies acquired US players. A few potential reasons for this: the dominance of American (and Chinese) technological advancements in terms of cybersecurity, but also a European wish to achieve technological independence from foreign suppliers (and investors?), and the ability to assert control over data and digital assets.

There is no denying that some cybersecurity subsectors (such as network security, endpoint security) seem overcrowded today and prime for consolidation. Plus, as part of the entire tech ecosystem, exit opportunities seem more challenging as they used to be a few months ago. However, beyond these legitimate concerns, we are convinced at AVP that some areas in cybersecurity are still untapped and poised for booming growth.

We could mention the use of AI applied to cybersecurity (security protection AI modelling, using LLMs for static code analysis, etc.) but we wanted to focus here on (1) the SMEs-specific segment that we consider as underserved, and (2) the Data Security segment, which is currently disrupted by promising emerging opportunities.

1/ SMEs

Contrary to popular belief, hackers do not go only after behemoths. Over 50% of cyber incidents target SMEs, and a staggering 60% of them go bankrupt within six months following a cyber-attack[ix].

Indeed, SMEs are intrinsically more vulnerable to cyberattacks, for many reasons. The rapid and growing digitalization has multiplied attack surface areas by forcing many SMEs to take urgent business continuity measures such as adopting cloud services, enabling staff to work remotely. In 2022, 48% of European SMEs report that their employees use personally owned devices to carry out business-related activity. In parallel, no appropriate preventive nor reactive measures are commonly adopted, mainly due to low security budget among SMEs, combined with a general skills and talents shortage. Only 19% of European SMEs in 2022 provided their employees with training or awareness raising about the risks of cybercrime, whereas human errors remain one of the main causes of incidents. Finally, when victim of a breach, more than 50% of SMEs do not report cybercrime incidents to the police and deal with them internally, which often exacerbates the problem.

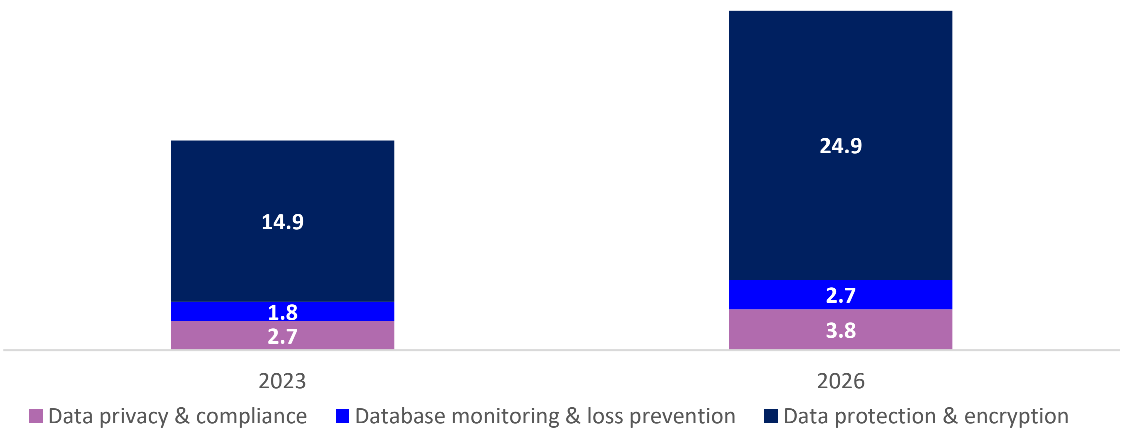
However, although they are the main victims of cybercrime, there is still a lack of solutions specifically designed for SMEs, which require from security vendors a specific go-to-market strategy - with more evangelization effort, customer success services, flexible pricing. Most established market leaders, with a complex product offering that aim to solve specific components of the IT stack, are not really set up for SMEs. They are more designed for big enterprises with high security budget and experienced security teams that can spend loads of time evaluating the scattering tooling out there (both licenses products and open-source) and managing them once set up i.e. dealing with massive amounts of alerts, notifications, false-positives, etc. To maintain high levels of margins and minimize customer success costs, most major cybersecurity providers are not incentivized to focus on the SMEs market.

We think, given the limited competition, that the SMEs cybersecurity market is massively underserved and, from a VC perspective, could generate very promising investment opportunities.

2/ Data Security

No need to remind the importance of data security in modern organization – the technology world revolves around data. There is unimaginable power in data but also incredible risk if they fall into the wrong hands – and that's why it's crucial to focus security efforts on the data itself rather than only on infrastructure perimeters. With the widespread adoption of data analytics in businesses and the rise of data-centric regulations, the demand for data security platforms that can oversee database access and provide data backup and protection services is increasing. The data security market, today estimated at $17.6bn, is expected to grow at a CAGR of 19.1% up to 2026 to reach $29.6bn, mainly driven by data protection and encryption. The latter, expected to grow by more than $10bn in the next three years, encompasses companies safeguarding databases from breaches and developing innovative encryption algorithms and applications for data (at rest, in transit or in use), notably supported by technologies such as confidential computing, tokenization, distributed ledgers, and post-quantum cryptography.

Data security market size estimate ($bn)



Source: Pitchbook

As investors, there is one fast-growing subsegment that particularly attracts our attention which is the Data Security Posture Management (DSPM). DSPM startups are disrupting the dormant segment of data security with platforms able to identify cloud data repositories and discover sensitive data, enabling remediation to breaches, along with privacy compliance.

Along with the shift towards cloud infrastructures, organizations might feel they have less visibility and control over their data in a cloud environment. Data discovery and then classification stands out as the most valuable security tool of data privacy professionals[x].

The traditional data security tools have been gradually experiencing buyers' fatigue because of too many false positives or missing unknown databases. Buyers want the ability to automatically detect the presence of various classes of sensitive and high-risk data while creating their own categories, to meet data privacy compliance.

On one hand, cloud-native players like Orca Security and Wiz are taking the lead, launching DSPM modules within their cloud-native protection platforms, but there are still nascent products. On the other hand, (not so) early-stage startups like Dig Security, Laminar, Open Raven and Symmetry Systems stand out for their technical innovations and raised outsized rounds in a challenged market environment. Both Dig and Open Raven achieved both $120m valuations in Q3 2022, offering real-time data attack detection and response, compared with periodic scans from cloud security tools.

Lastly, quantum computing's rise challenges traditional encryption methods, urging adoption of novel encryption algorithms, known as Post-Quantum Cryptography (PQC). While large-scale quantum computers may be years away, banks, institutions, and governments with sensitive long-term data face immediate threats, such as 'Store now, Decrypt later' attacks. In this type of attack, hackers can store data now to decrypt it once quantum computing techniques are made available. This threat has led the US to pass the Quantum Computing Cybersecurity Act in December 2022[xi]. Today, most cyber and data security companies are looking at building PQC solutions to prepare for this emerging menace. A fascinating topic that we are looking at very closely, as demonstrated by our recent investment at AVP in CryptoNext, a company specialized in providing post quantum cryptography solutions.

Special thanks to Roeland Delrue (CEO of Aikido), Sipan Vardanyan (CEO of Hexens.io) who shared with us their valuable views on the market.

---

[i] https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm#scroll=off&pdf-overlay=//www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/global-data-protection-index-key-findings.pdf
[ii] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T
[iii] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
[iv] https://www.gartner.com/en/newsroom/press-releases/2022-10-18-gartner-survey-of-over-2000-cios-reveals-the-need-to-accelerate-time-to-value-from-digital-investments
[v] https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences
[vi] https://aventis-advisors.com/software-valuation-multiples/
[vii] https://finerva.com/report/cybersecurity-2023-valuation-multiples/
[viii] https://www.securityweek.com/securityweek-analysis-over-210-cybersecurity-ma-deals-announced-in-first-half-of-2023/
[ix] https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/
[x] https://www.idc.com/getdoc.jsp?containerId=US50221523
[xi] https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/?sh=16661d7e368a

We invest in great entrepreneurs.

We support outstanding companies.

AXA VENTURE PARTNERS

New York - London - Paris

www.axavp.com