

Introduction to the cloud security market

We invest in great entrepreneurs
We support outstanding companies

June 2023



2-1. Introduction to the cybersecurity market trends

Cybercrime is not new, but the past two years have seen increasing risk from cyberattacks, creating a renewed sense of urgency not only for big enterprises but now more and more for SMEs

'Trojan' threatens 10,000 computers

FEARS ARE growing that more than one mailing list was used to distribute the "Aids Information" computer diskette which is dam.

By Tom Wilkie
Science Editor

AIDS_Trojan

The first malicious cyber attack was created.
Joseph Popp created a Malware called the AIDS Trojan, which was distributed through his postal mailing lists using a floppy disk

1990

2000

2010

2020s

From monolithic to distributed systems / From on-premise to cloud

ANALYSIS

Stuxnet explained: The first known cyberweapon

Stuxnet

Major milestone in malicious computer malware attacks. The program was co-developed by the US and Israeli intelligence services to sabotage Iran's nuclear weapons

ICS/OT Security | @5 min read @news

2 Years After Colonial Pipeline, US Critical Infrastructure Still Not Ready for Ransomware

Sweeping changes implemented since the May 2021 cyberattack are helping — but more work remains to be done, security experts say.



Jai Vijayan
Contributing Writer: Dark Reading

May 05, 2023

Log4j: Why Organizations Are Failing to Remediate This Risk

Log4j vulnerability is a serious issue for many companies, making it difficult to identify services and issues affected by the problem.

Dec 14th, 2022 12:04pm by Eric Goebelbecker

ILOVEYOU worm

In the early 2000s, with the rise of personal computers in the wake of Microsoft Windows 98, there was the ILOVEYOU worm that affected millions of computers within just a few hours of release

How the ILOVEYOU worm exposed human beings as the Achilles Heel of cybersecurity

Colonial Pipeline, Log4j, SolarWinds, ...

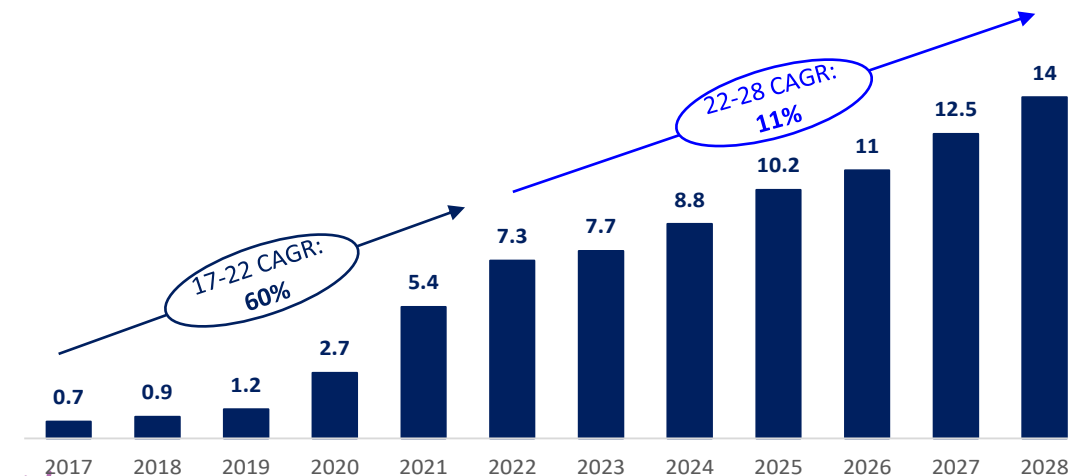
Attacks on core US infrastructures such as the shutdown of the Colonial pipeline, SolarWinds, and Log4j discovery have created a renewed sense of urgency

- Cyberattacks against small businesses have been on the rise in recent years
 - +60% of SMEs were the target of a cyberattack in 2021
 - +80% of ransomware attacks in 2021 were against companies fewer than 1,000 employees
- Despite the attitude among many small business owners that hackers only go after behemoths, smaller companies make increasingly attractive prey

As the number of cyber attacks has tripled over the last decade, Cyber Security remains the highest priority budget spend areas for CTOs, over ML and AI

As cybercrime costs continue to explode worldwide...

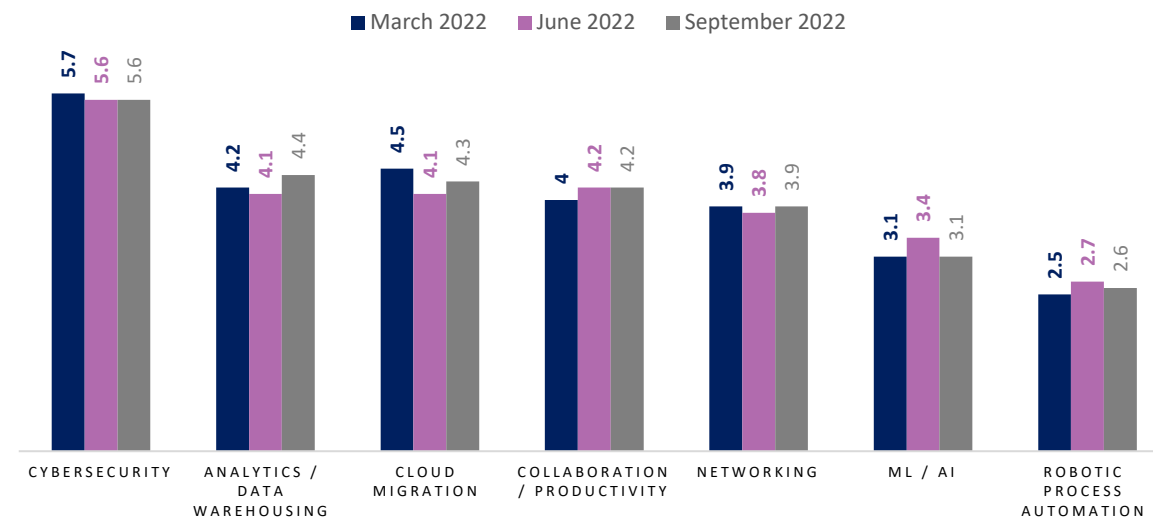
Estimate cost of cybercrime, worldwide in trillion \$



50% of cyberattacks are committed against SMEs and 60% of them go out of business within 6 months

...it remains the prioritized budget spend area within IT spend, over ML/AI

Main technology areas aiming to be addressed by IT leaders in the year (av. ranking)⁽¹⁾



- Cybercrime is expected to cost the world \$10.2 trillion annually by 2025. As a result, Cyber security remains the highest spending intent for IT leaders, over other important enterprise initiatives such as AI/ML tools. 98% of IT and security leaders say they dealt with a cyberattack over the last year (47 attacks on average/year). Spending in **information security and risk management** products and services is forecast to reach **+\$188.3 billion in 2023**, with **cloud security** being the category with the **fastest growth**
- Besides, the financial losses, there are often even more significant losses including reputational damage, loss of consumer trust, and low employee morale that can cripple an organization
- SMEs are not left out. In fact, more than 50% of cyberattacks are committed against SMEs and 60% of them go out of business within 6 months of falling victim to a data breach or hack. Most of them lack the financial resources and skill set to combat the emerging cyber threat (phishing attacks, malware spying, ransomware, password cracking, identity theft, major breaches and hackers)

Focus on cybersecurity in SMEs - SMEs are much more vulnerable in a post-COVID digital world

SMEs are intrinsically more vulnerable to cyberattacks...

- **Rapid and growing digitalization has increased the number of entry points and attack surface areas**

- In order to survive the Covid-19 pandemic and to continue in business, many SMEs had to take urgent business continuity measures such as adopting cloud services, upgrading their internet services, improving their websites, and 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*

- **Lack of awareness and expertise to assess the digital risk exposure and to implement appropriate prevention and remediation measures (commonly used among large enterprises)**

- *In Europe, only **19%** of SMEs have provided their employees with training or awareness raising about the risks of cybercrime in 2022*

- **Lack of reporting of cybercrime incidents**

- ***50%** of SMEs do not report incidents to the police and deal with it internally*

...with limited room for improvement for the moment

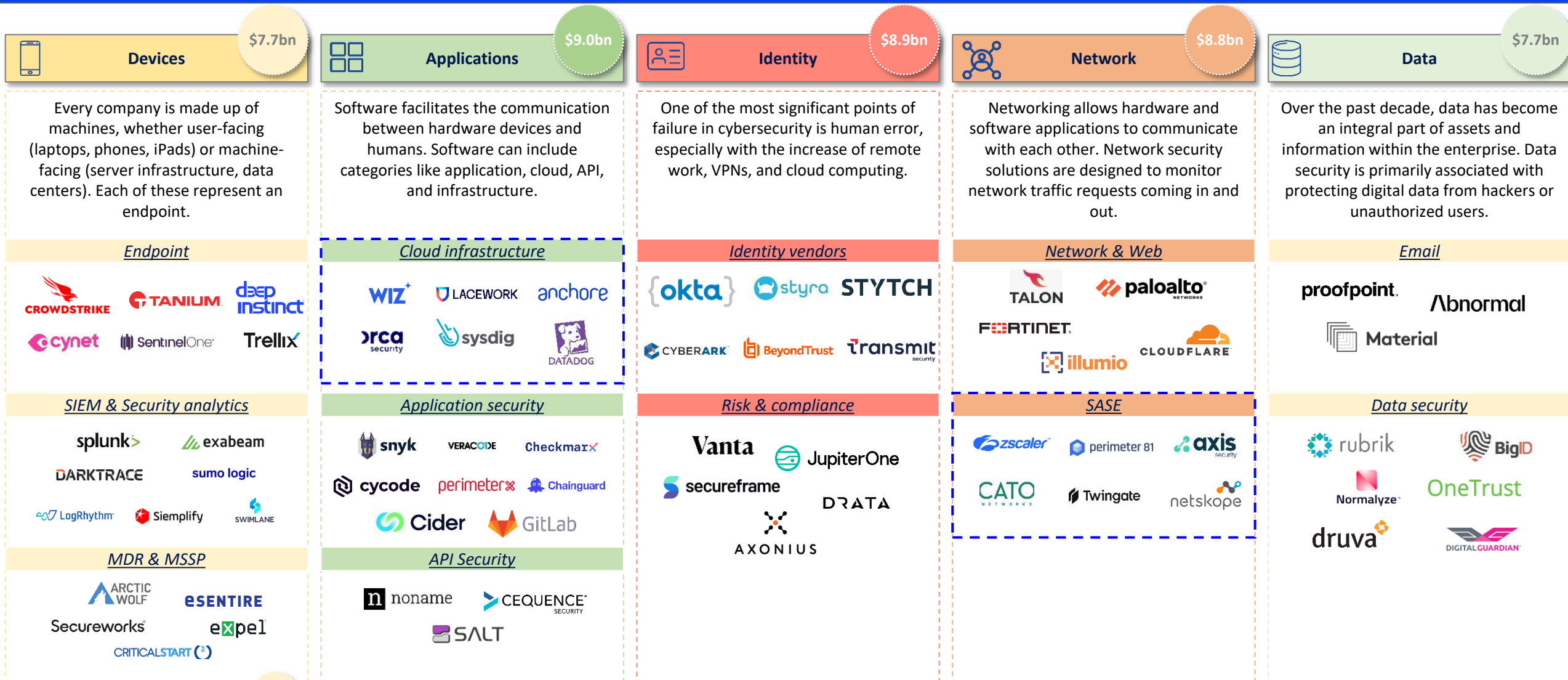
- **Providing trainings for employees** are a necessary condition to protect against cyber-attacks (human error being one of main cause of incidents), they remain insufficient when it comes to sophisticated attacks

- **Hiring a dedicated security person/team** but low security budget among SMEs, combined with skill & talent shortage

- **Shifting to the cloud.**

- **"Shared Responsibility Model"**: cloud services providers (e.g. (AWS, Microsoft Azure, Google) provide high levels of security on physical assets, so their clients can focus on the rest and prioritize most urgent expenses
- Cloud services might be safer than traditional systems but at a greater ecosystem level if all small firms are dependent on the same provider there is a risk of **catastrophic disruption** if the cloud platform is compromised

The modern IT enterprise stack is fragmented and complex and has given rise to a wide range of solutions tracking specific niches within the enterprise



Cloud security companies
Sources: Contrary Research, Pitchbook

\$Xbn

Total raised



2-2. Focus on Cloud Security

Cloud security is one of the most rapidly evolving categories in cybersecurity

Cloud Computing

- Cloud computing is the delivery of on-demand computing services over the internet on a **pay-as-you-go** basis, allowing one to save them over the internet rather than managing them on a local storage device
- It exists multiple advantages in choosing cloud computing over on-premise (payment based on usage, no server space required, disaster recovery, high flexibility, automatic software updates, easy collaboration between teams from widespread locations, rapid implementation, etc.)
- Two types of models:

Deployment model

Public Cloud

Accessible to everyone



Private Cloud

Exclusively operated by a single organization



Hybrid Cloud

Typically used by federal agencies



Service model

Infrastructure-as-a-Service (IaaS)

Cloud service that provides basic computing infrastructure



Platform-as-a-Service (PaaS)

Cloud platforms and runtime to develop, test, manage apps



Software-as-a-Service (SaaS)

Licensing of an app to customers

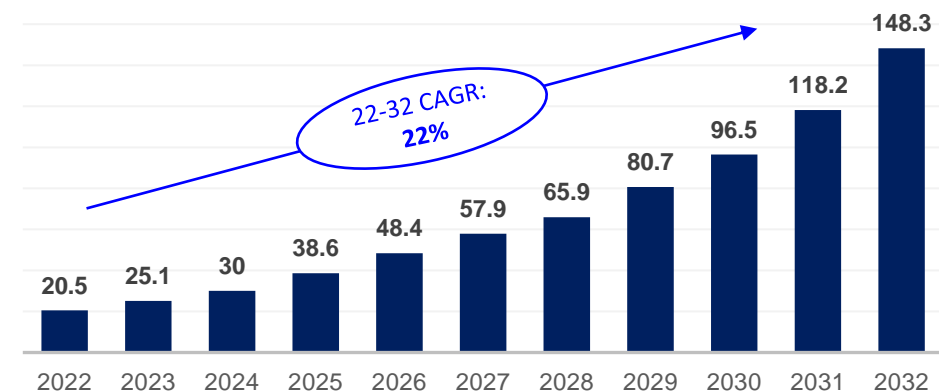


In the past 3 years, notably due to the pandemic, there has been a **massive adoption** of the cloud that creates a meaningful opportunity for bad actors, given the diversity of available attack vectors

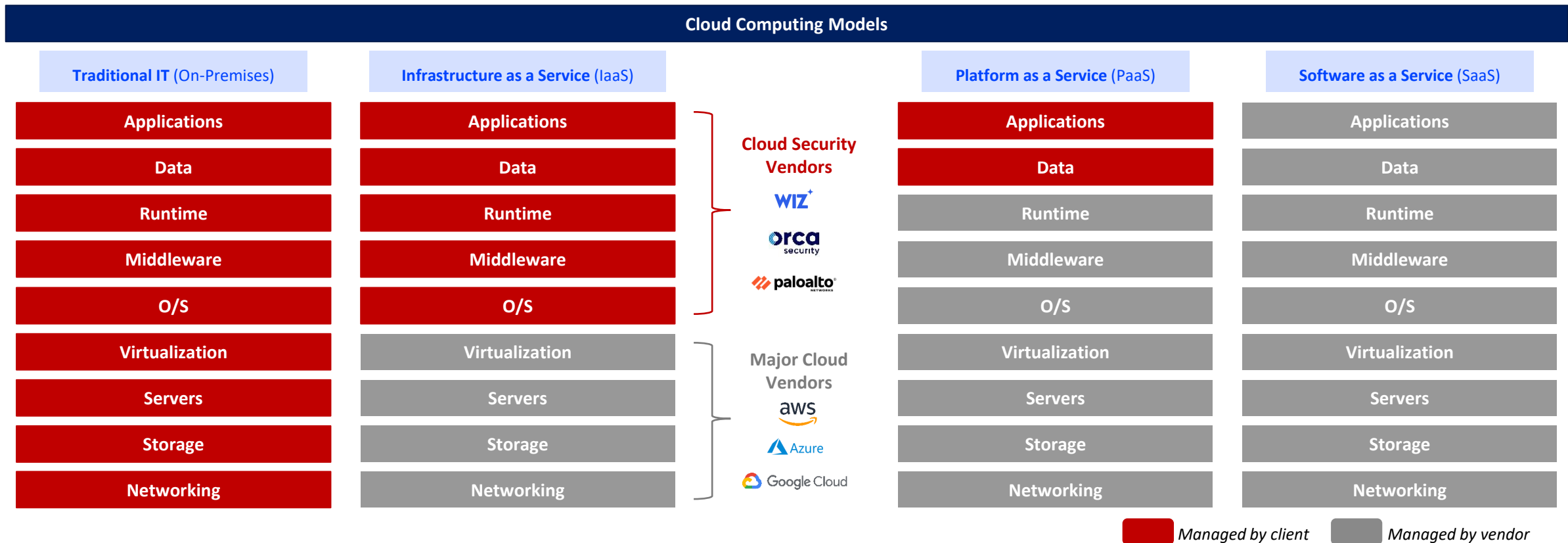
- By 2025, **95%** of digital workloads will be hosted in the cloud, a major increase from the 30% recorded in 2021
- From 2018 to 2021, public cloud revenue grew from \$32 billion to over **\$400 billion**
- +38%** in global cyberattacks in 2022 vs. 2021, notably driven by a **48%** increase in the number of **cloud-based network cyberattacks**

As a result, cloud security market has been growing accordingly

Global Cloud security market, \$bn



Cloud Computing Models operate under a “Shared Responsibility Model” when it comes to cybersecurity



Shared responsibility model

- The adoption of the cloud ushered a **shared responsibility model** in which cloud vendors take on aspects of a customer's security requirements, while customers work directly with cloud security vendors for additional security needs they may have
 - Companies will work with **cloud security providers** in securing applications, workloads, and data.
 - **Cloud providers** are responsible for managing the security and compliance of the platform in terms of the network, container, runtime, and isolation

Three different categories of players are trying to take a leadership position in the cloud security market with the aim to provide a complete product suite, now also to the SME market

1

Cloud Security Startups

Former cloud security startups have recently exploded onto the scene showing spectacular growth

2















Cybersecurity leaders

Traditional cybersecurity leaders are trying to of end-to-end solution

3

Major cloud providers

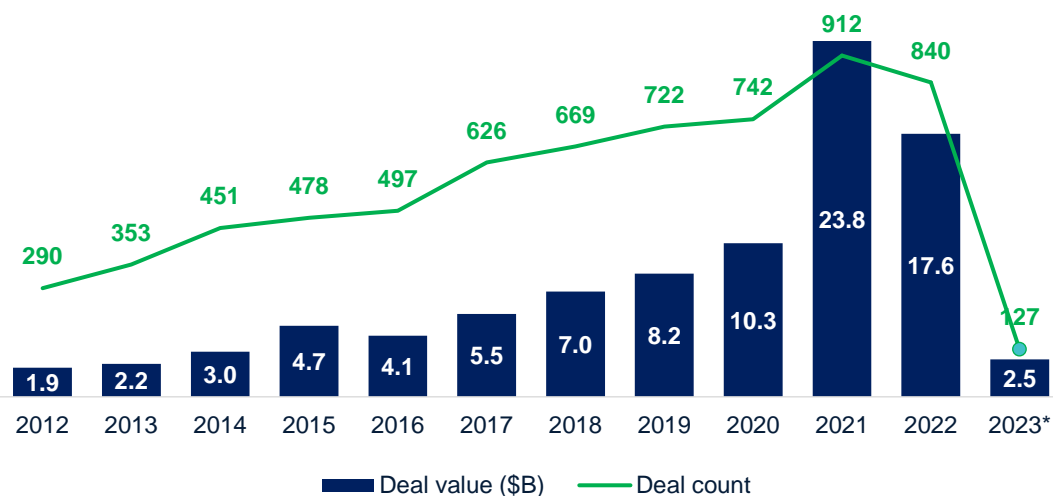
Cloud providers are taking a more active role in security

Selected companies	Founded	Location	Size in FTEs	Amount Raised	Description	Market activity
	2020	 	785	\$900m	Wiz, Inc. is a developer of a cloud security platform designed to help businesses secure cloud infrastructure at scale.	Founded in 2020, Wiz was able to surpass \$100 million in ARR within 18 months
	2019	 	450	\$780m	Orca is a developer of a cloud-based security platform designed to deliver comprehensive full-stack visibility into cloud infrastructure.	In Oct 2021 , Orca Security Extended Series C Round to \$550M , Boosting Valuation to \$1.8 Billion , showing an impressive YoY growth of 800%
	2005		15 000	\$330m	Palo Alto Networks has one of the most comprehensive cloud security products	Palo Alto Networks has evolved from being a network security tool to becoming a broader platform, coming from 16 acquisitions over the last 5 years
	2011		7 150	\$481m	One of the major platform companies in cybersecurity, expanding from endpoint security to cloud workload protection and Falcon Container Security	CrowdStrike's has expanded into cloud-native products and has seen ~\$100 million ARR in cloud security and 100%+ growth in cloud-based workloads.
	2006		122 000	n.a	AWS offers website hosting, backup, digital marketing, analytics, application integration, blockchain, networking, and other related services	In Dec 2022 , Amazon announced security products or services across product categories like cloud native application protection (CNAPP) or identity and access management (IAM)
	1975		221 000	n.a	Azure is Microsoft's public cloud platform. Azure offers a wide range of services, including PaaS (platform as a service), IaaS (infrastructure as a service) and managed database services.	In Jan 2023 , Microsoft announced that their security business had surpassed \$20 billion in revenue

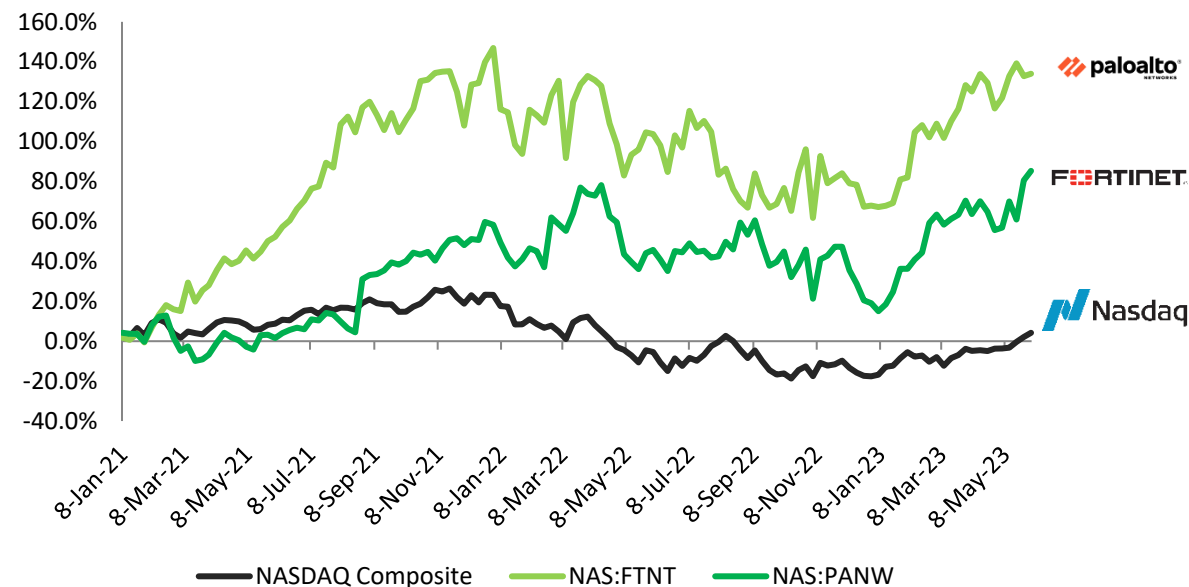
2-3. VC ecosystem market mapping

Even if volatile economic conditions, cybersecurity remains the most resilient category of enterprise software...

EU & NA deal value & number of deal counts – Cybersecurity, as of Q1 23 (in \$bn)



Public companies' performances vs. market (as of 06/06/2023)

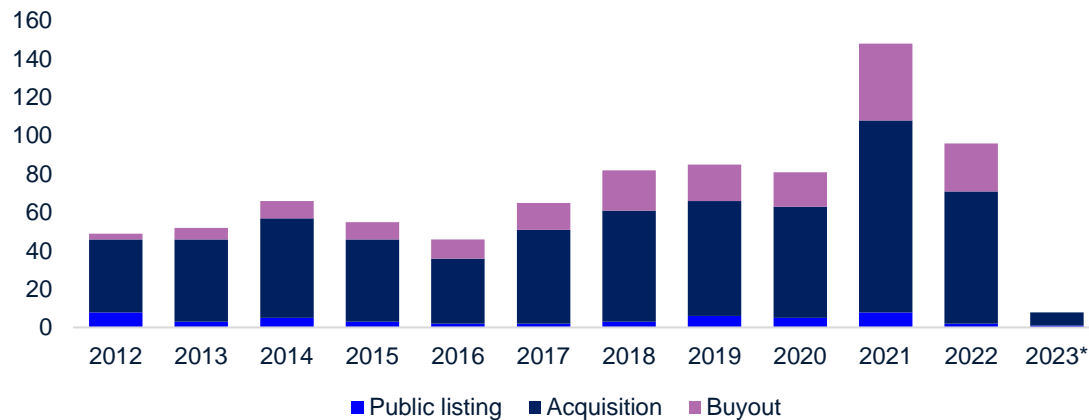


- Deal value in 2022 were down by 26% vs. last year (after having doubled in 2021 to reach \$24bn of deal value) while number of deals decreased by only 8% (vs. c. 20% in the overall market) also due to the larger size of deals
- Market leaders are outperforming the rest of software. Public companies including Palo Alto Networks, ZScaler, Fortinet, and SentinelOne enjoyed strong quarters
- Overall, the market will continue to be supported by strong growth drivers:
 - Cyber security remains the number one priority** for 31% of corporations, while over 92% expect their security budgets to increase between 2022 and 2023
 - Governments are also taking significant steps to invest in their own cybersecurity infrastructure** (e.g. President Joe Biden signing an executive order to galvanize public and private efforts to respond to persistent malicious cyber campaigns)
 - Regulatory constraints regarding data privacy protection** (e.g. GDPR, one of the world's most stringent privacy and security laws with significant consequences for anyone not compliant)

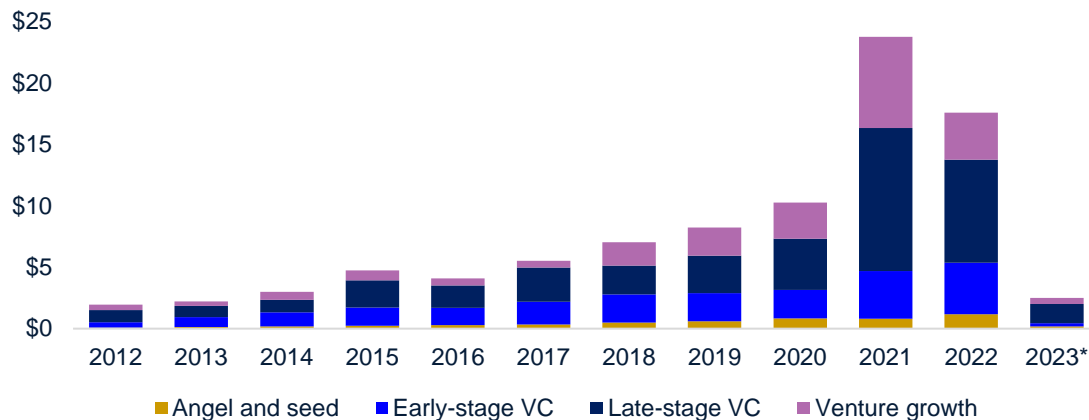
... but recent macroeconomic environment undoubtedly favors larger deals, lower valuation and consolidations, thus benefiting biggest players...

Like for the all the VC ecosystem, the market has slowed down considerably for cybersecurity start-ups...

Cybersecurity VC exit count by type



Cybersecurity VC volume by stage



Source: Pitchbook

...while significant acquisitions continued and benefit to larger incumbents

Top strategic acquirers of cybersecurity companies since 2019

Investor	Deal count	Known deals examples
FORTRA	13	Tripwire, Feb-22, (\$350m)
CISCO GLOBAL	11	Creatrix, Jun-22 (\$3.6m) CyberViking, Jul-22 (\$1.8m)
accenture	11	Fiftyfive5, Dec-22 (\$132m)
paloalto NETWORKS	11	Cider, Dec-22, (\$300m) Bridgecrew, Mar-21, (\$152m)
Deloitte	10	Makros, Dec-22 Hacktive, Oct-22

- Late-stage VC deal count exceeded both angel and seed and early-stage deal count yet again. Yet only five VC megadeals closed, indicating that unicorns remain constrained in funding outside of venture debt
- Leading specialist VC investors remained active in leading early-stage deals yet focused on seed and Series B investments, suggesting a preference for lower valuations
- Exit value continued to dry up

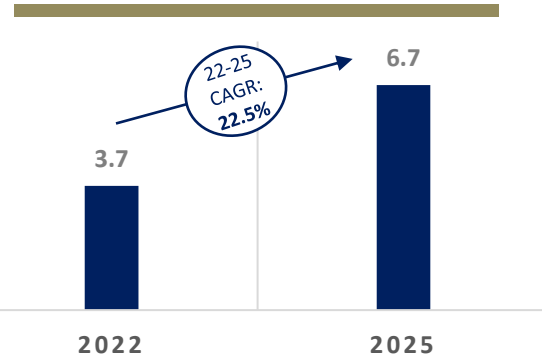
...leading to a main question: is there still room for growth for new entrants in this market?

- The recent consolidation in **network security** and **endpoint security** however leaves **application security** and **data security** as outstanding segments for startups to address
- More specially, there are two emerging opportunities we are observing over the last few months:
 - Cloud workload protection**: Startups are driving open-source detection for Kubernetes monitoring via the eBPF project
 - Data security posture management**: Startup vendors are disrupting the dormant segment of data security to offer consolidated platforms across cloud data discovery and threat detection

Cloud workload protection (CWP)

- CWP refers to cybersecurity controls for cloud-based applications and containers that increasingly house cloud-native applications
- In contrast to DevOps security platforms that seek to enforce secure coding policies from the earliest stage of the application lifecycle, CWP focuses on the deployment of application
- Market value in 2022 was estimated at **\$3.7bn** and is expected to grow at a CAGR of **22.5%** to reach **\$6.7bn** in 2025
- Growing market with two trends (1) **large players** willing to extend their **CSPs**, like **Wiz** by offering cloud-scanning solutions, and (2) **startups** driving open-source detection or Kubernetes monitoring via the extended Berkeley Packet Filter (eBPF) like Isovalent

CWP Market Size



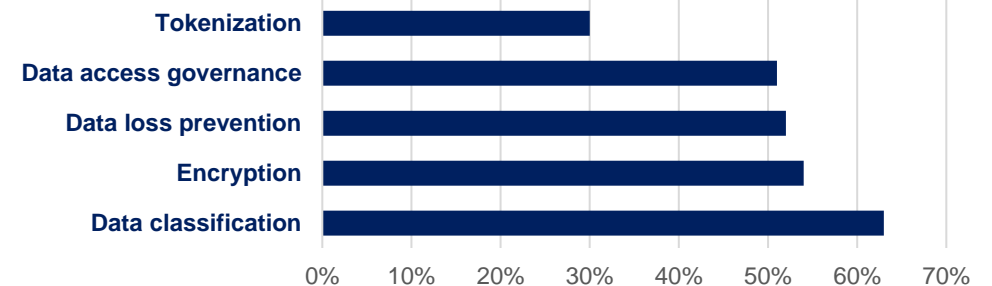
Recent CWP Security VC Deals

Company	Close Date	Deal size	Post-money valuation (\$m)
Wiz	Feb-23	\$300m	\$10.3Bn
Accuknox	Mar-23	\$5.8m	\$18.8m
Isovalent	Sep-22	\$40m	\$225m

Data security posture management (DSPM)

- DSPM platforms **identify cloud data repositories** and discover sensitive data, enabling remediation to breaches, along with privacy compliance
- Data classification** remains the most valuable data security tools of data privacy professionals (classify data, including unknown database, according to data types and level of sensitive to compliance regulations, without false positives)
- DSPM remains an **immature market**, yet has **large addressable budgets**, and could well become a **\$1bn market** over the next 3 years
- Startups** are **disrupting** this field by offering **consolidated platforms** across cloud data discovery and threat detection, with 6 startups raising rounds of **+\$20m** in 2022, **more than previous 6 years**

Top data security tools according to data privacy professionals



Conclusion related to the opportunity on the SMEs market

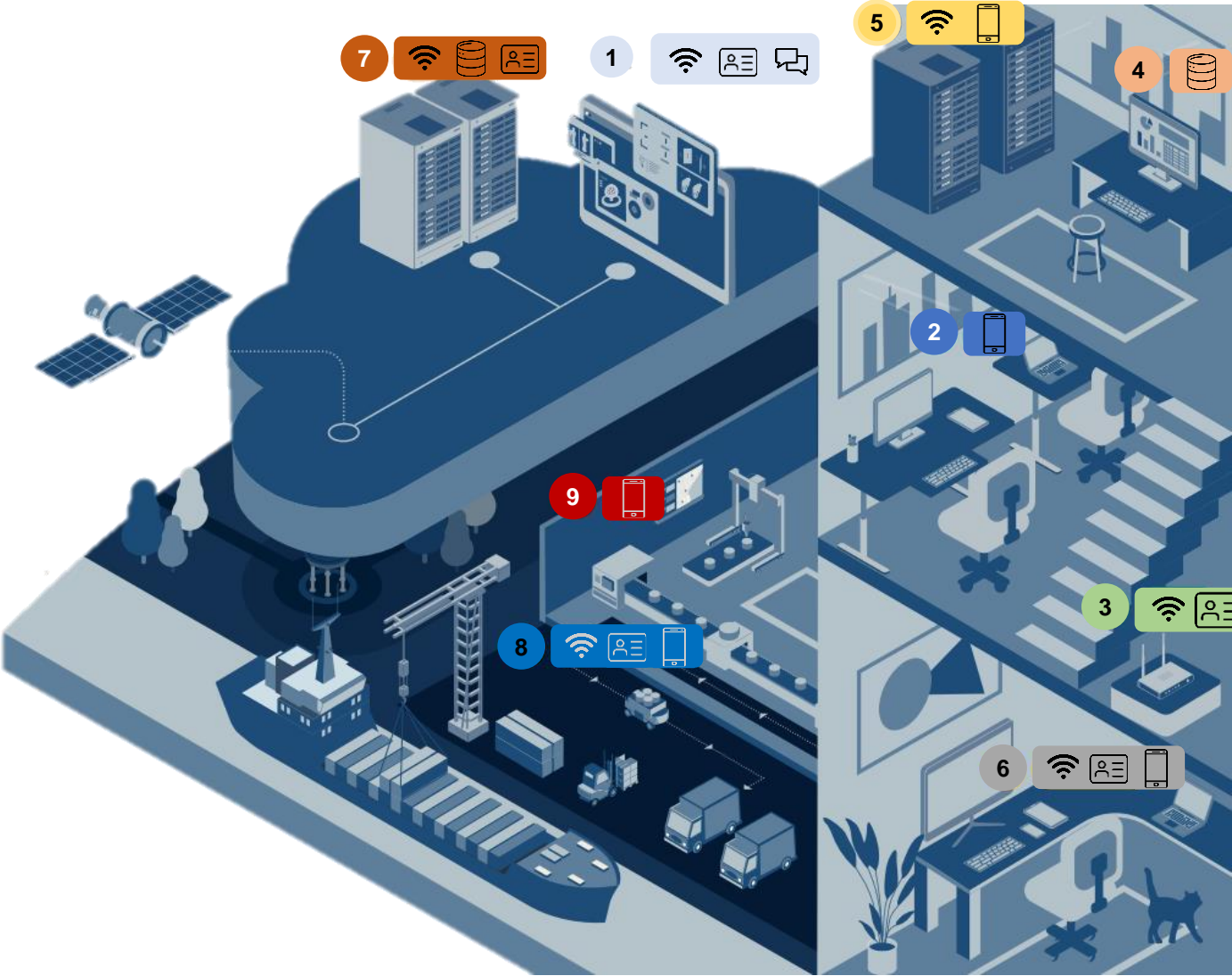
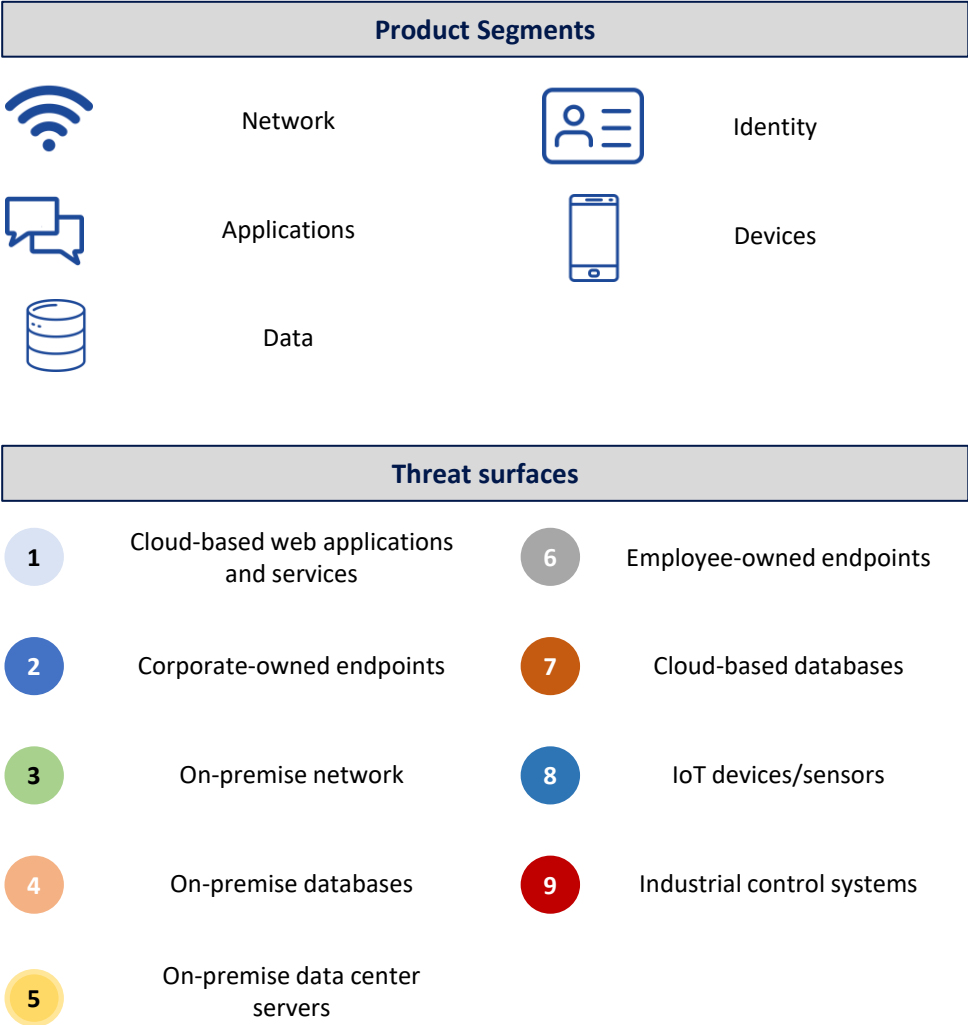
- The cybersecurity market lacks solutions specifically designed for SMEs
- Most established market leaders have a **complex product offering** that aim to solve specific components of the IT stack and designed for big enterprises with **high Security budget** and **experienced IT and Security teams**
- **Still room for new entrants in the SMEs segment**, considering the limited competition and **market specificities** (limited budget and undeniable lack of knowledge/awareness of interlocutors that need to be educated on the cybersecurity topic, etc.)
 - *Very few actors claim to play a role in the SME market such as Trend Micro, Forcepoint, Sonicwall, Cygilant (acquired by Silversky) Bastion Technologies, etc.*
- **How to unlock the SME opportunity?**
 - *Maxime Cartan, CEO of citalid*

Appendix

Glossary

- **Cloud computing:** A means to offer computing services to the public or for internal use through remote services.
- **Cloud workload protection (CWP):** cybersecurity controls for cloud-based applications and containers that increasingly house cloud-native applications
- **Cryptography:** The application of mathematical processes on data-at-rest and data-in-transit to provide the security benefits of confidentiality, authentication, integrity and non-repudiation.
- **Data breach:** The occurrence of disclosure of confidential information, access to confidential information, destruction of data assets or abusive use of a private IT environment.
- **Data integrity:** A security benefit that verifies data is unmodified and therefore original, complete and intact.
- **Data security posture management (DSPM):** platforms identify cloud data repositories and discover sensitive data, enabling remediation to breaches, along with privacy compliance
- **Encryption key:** The secret number value used by a symmetric encryption algorithm to control the encryption and decryption process.
- **Firewall:** A security tool, which may be a hardware or software solution that is used to filter network traffic.
- **IaaS (Infrastructure-as-a-Service):** A type of cloud computing service where the provider offers the customer the ability to craft virtual networks within their computing environment. An IaaS solution enables a customer to select which operating systems to install into virtual machines/nodes as well as the structure of the network including use of virtual switches, routers and firewalls.
- **PaaS (Platform-as-a-Service):** A type of cloud computing service where the provider offers the customer the ability to operate custom code or applications. A PaaS operator determines which operating systems or execution environments are offered.
- **SaaS (Software-as-a-Service):** A type of cloud computing service where the provider offers the customer the ability to use a provided application. Examples of a SaaS include online e-mail services or online document editing systems.
- **SIEM (Security Information and Event Management):** A formal process by which the security of an organization is monitored and evaluated on a constant basis. SIEM helps to automatically identify systems that are out of compliance with the security policy as well as to notify the IRT (Incident Response Team) of any security violating events.
- **Firewall:** A security tool, which may be a hardware or software solution that is used to filter network traffic
- **MDR (Managed Detection & Response):** A cybersecurity service that combines advanced technology and human expertise to perform threat hunting, monitoring and incident response
- **MSSP (Managed Security Services Provider):** An IT service provider that offers cybersecurity solutions and services. MSSPs typically provide broad monitoring of the network for events and send validated alerts to other tools or to the organization's security team.
- **Phishing:** A social engineering attack that attempts to collect information from victims.
- **Trojan Horse :** A form of malware where a malicious payload is imbedded inside of a benign host file.

Overview of the Cybersecurity Landscape: Attack surface areas & entry points



2-4. Citalid Presentation





AXA VENTURE PARTNERS

www.axavp.com