Cybersecurity

Industry Report 2025

Now, for tomorrow

bakertilly

Contents

Feed summary

Cybersecurity Industry Report 2025

- This study covers **27,000** companies worldwide related with the **Cybersecurity** industry. All the data about companies, acquisitions and founding rounds was extracted on **10 December 2024**. Deals, rounds and companies founded after this date have not been included.

- In this Market Analysis you will be able to solve your doubts regarding what **type of investors** are investing in the sector, what **type of companies** are acquiring market share companies, how much **investment** has been made and is expected to be made...

Overview

27K
Active

3,8K
Funded

153
IPOs

$165bn
Funding

10K
Rounds

21K
Investments
made

2,711
Acquisitions
by Sector's
Companies

1,886
Sector's
Companies
acquired

WordCloud


program
telecommunications
content
marketing
disaster
Research
provides
professional
hardware
help
detection
computing
penetration
intelligence
protect
VoIP
remote
hosting
real
mobile
advisory
products
threats
application
defense
Group
organizations
recovery
networking
providing
website
custom
transformation
Information
Advanced
Networks
cyber
ERP
customers
consultancy
Center
compliance
Global
AI
engineering
COMMUNICATIONS
training
develops
technology
big
Systems
consulting
innovative
fraud
outsourcing
development
Support
business
Cybersecurity
analysis
IoT
enterprise
software
Data
digital
provider
control
specializing
email
artificial
project
leading
secure
design
specializes
Internet
Protection
clients
assessment
threat
Analytics
ICT
solution
managed
Services
audit
product
private
tech
Management
surveillance
applications
based
SaaS
network
cloud
app
Technologies
computer
process
Blockchain
backup
businesses
solutions
access
end
industry
quality
forensics
automation
infrastructure
monitoring
against
focusing
testing
technical
through
offers
privacy
firm
risk
security
Inc
small
powered
one
Companies
focused
Financial
operations
service
company
offering
identity
platform
system
including
integration
driven
web
helps
government
agency
attacks
communication
assurance
strategy
enterprises
online
maintenance

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, devices, and data from cyber threats, such as unauthorized access, theft, damage, or disruption. It involves implementing technologies, processes, and policies to safeguard digital information and ensure the confidentiality, integrity, and availability of data and services.

Some of the **benefits** of Cybersecurity include the following:

- **Data protection**: Prevents data breaches and loss of sensitive information.
- **Operational Continuity**: Ensures that businesses and services remain functional despite cyber threats.
- **Trust**: Builds confidence among users, customers, and stakeholders.
- **Compliance**: Meets legal and regulatory requirements, such as GDPR, HIPAA or PCI DSS.
- **Financial Security**: Reduces the risk of costly cyber attacks like ransomware or fraud.

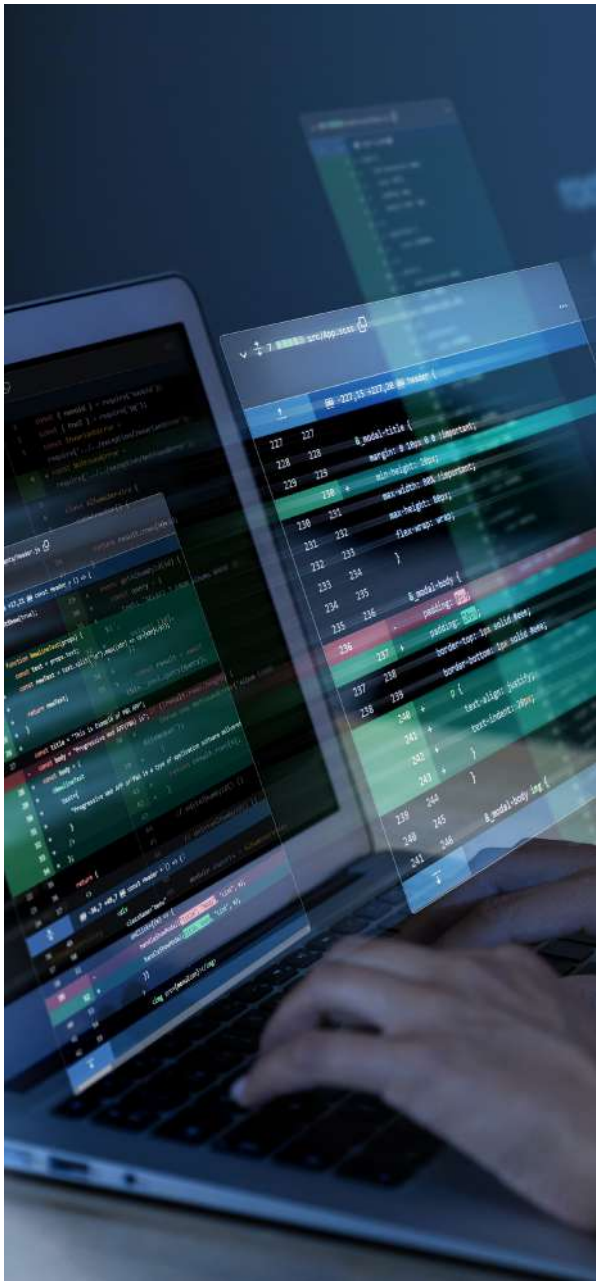
The cybersecurity process can be summarized in different steps as we are going to see in the value chain:

- **R&D**: A company develops an AI-powered intrusion detection system (IDS).
- **Design and Production**: The IDS is integrated into a cloud-based SIEM solution for easy deployment.
- **Distribution**: The solution is marketed to enterprises via direct sales and cybersecurity integrators.
- **Implementation**: The SIEM solution is deployed and configured in client environments.
- **Monitoring**: A managed SOC service monitors the solution, detecting anomalies in real-time.
- **Incident Response**: If a breach occurs, the SOC team provides containment, forensic analysis, and recommendations.

Data Privacy vs Cybersecurity

- Cybersecurity and data privacy are closely related, but they are not exactly the same. While cybersecurity focuses on protecting data from attacks and unauthorized access, data privacy is more oriented towards controlling and managing personal information and ensuring its ethical and appropriate use.

- Both concepts work together, as a good cybersecurity strategy is essential for protecting privacy, and privacy relies on having robust cybersecurity measures in place.



Cybersecurity Types

Network Security

Protects and organizations network infrastructure from unauthorized access, misuse, or attacks.

Application Security

Focuses on securing applications from vulnerabilities during development and throughout their lifecycle.

Cloud Security

Safeguards data, applications, and services hosted in cloud environments.

Data Security

Protects sensitive data from breaches or unauthorized access.

Endpoint Security

Secures devices such as laptops, smartphones, and IoT devices connected to a network.

Identity and Access Management (IAM)

Ensures that only authorized users can access specific systems or data.

Cybersecurity Types

Operational Security (OpSec)

Focuses on protecting the processes and decisions involved in handling sensitive information.

Critical Infrastructure Security

Protects essential systems such as power grids, water supplies, and transportation networks.

Disaster Recovery

Concentrates specifically on restoring IT systems, data, and technology infrastructure **after** a disruptive event, such as a cyberattack, hardware failure, or natural disaster.

Business Continuity

Focuses on maintaining essential business operations **during and after** a disruption. It ensures that critical functions and services can continue with minimal impact, even if systems, facilities, or resources are compromised.

IoT Security (Internet of Things)

Protects interconnected devices and sensors from vulnerabilities.

Artificial Intelligence and Machine Learning Security

Addresses threats to AI-based systems or uses AI to enhance cybersecurity defenses.

Segmentation

CYBERSECURITY

By Service

Professional Services:
- Design, Consulting and Implementation
- Risk & Threat Assessment
- Training & Education
- Support & Maintenance

Managed Services

By Security Type

- Network Security
- Cloud Security
- Application Security
- Endpoint & IoT Security
- & more

By Vertical / Industry

- Aerospace & Defense
- Government
- Telecommunications
- Media & Entertainment
- IT & ITeS
- Manufacturing
- Others

By Component

Solutions
- Standalone Hardware
- Software Solutions

Services

By Solution Type

- IAM
- Antivirus / Antimalware
- Long Management & SIEM
- Encription & Tokenization
- Compliance & Policy Management
- Patch Management
- Other solution type

By Deployment Mode

Cloud

On-premises
- Hybrid

By Enterprise Size

Large Enterprises

SMEs
- Medium Enterprises
- Small Enterprises

Niches by #Funding (2023)

We highlight three groups or business models classified according to the **description** of the companies:

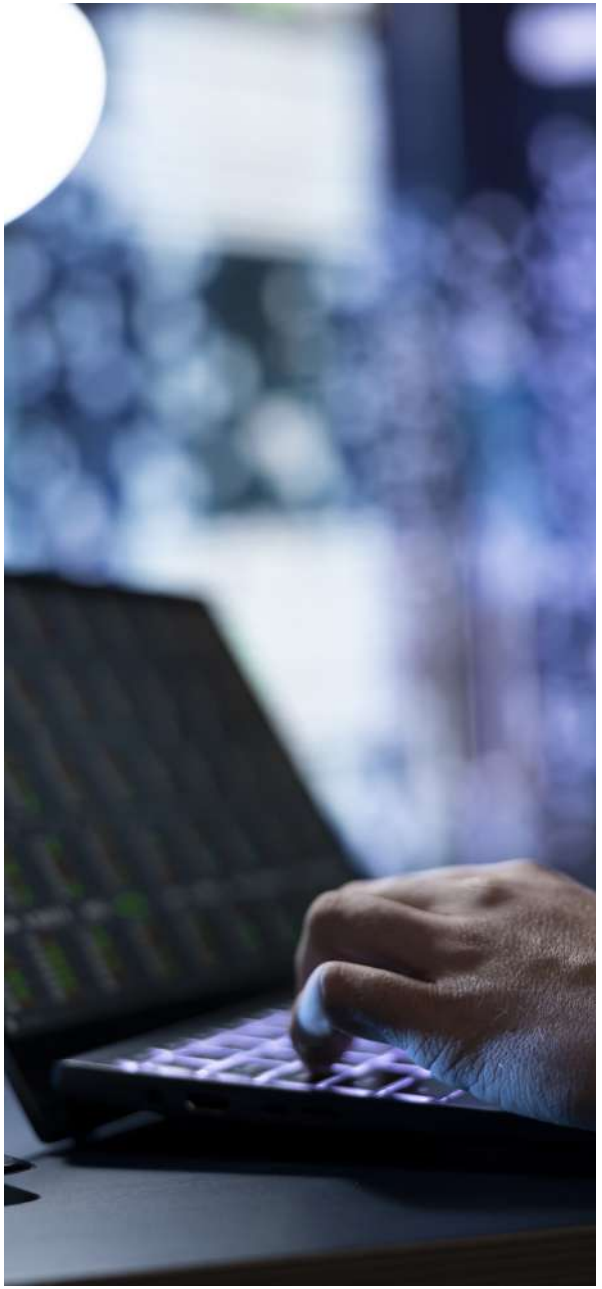
- Companies dedicated to providing **cloud security**
- **Threat Intelligence, threat detection**
- SaaS Security

These fairly well-defined and specific groups are the ones that received the highest number of funding rounds in 2023 or experienced the greatest growth in funding rounds during that year.

On one hand, the **Cloud Security** group recorded 106 funding rounds, with a total of 351 companies. The average funding amount for these rounds was **$3.00 million**.

On the other hand, the **Threat Intelligence** group saw 110 funding rounds, with a total of 400 companies and an average funding amount of **$1.58 million** per round.

Finally, the **SaaS Security** group experienced the highest growth in funding rounds between 2022 and 2023. While there was a decline between 2021 and 2022, the last year saw a **70% increase**. The total number of companies in this group is **101**.



Niches by #Acquisitions (2023)

In terms of acquisitions, the groups achieved through company descriptions vary. We highlight two and repeat one:

- Machine Learning, AI software system
- Identity access management
- Threat intelligence

In terms of acquisitions, these are more **"traditional"** or generic niches, such as Business Intelligence. This had an increase of **28%** in 2022 and are companies such as **EDB** (bought by Bain Capital [Private Equity]) or **Warung Pintar** (bought by SIRCLO [e-commerce]).

Being a very **small and young niche**, climate change analytics companies in 2022 have seen an increase in acquisitions. Few companies are categorised in this area, but it is worth nothing this positive trend in this currently in-demand sector. Companies such as **The Climate Service** (bought by S&P Global) or **Urgentem** (bought by Intercontinental Exchange) stand out.

And finally, the medical industry, which, as with the rounds, stands out in the field of acquisitions. Companies such as **Hospital IQ** (bought by LeanTaaS) or **OKRA Technologies** (bought by Encision Pharma Group) have already been acquired in 2023. It is worth noting that this year they already account for almost **40%** of the acquisitions in 2022 in the healthcare analytics sector.

Value Chain

Primary activities

Research and Development (R&D)

Development of new technologies, algorithms, and tools to address emerging threats. Innovation in areas like AI-based threat detection, cryptography, or zero-trust frameworks.

Product and Service Design

Creating cybersecurity software (antivirus, firewalls, SIEM tools) or hardware (UTM appliances). Designing managed security services such as SOC (Security Operations Centers).

Production and Distribution

For products: Manufacturing hardware devices or developing software solutions. For services: Establishing cloud-based delivery platforms, SaaS models, or consultancy offerings.

Implementation

Installing and configuring cybersecurity solutions at customers sites or via remote management. Offering tailored solutions for enterprises based on specific risk profiles.

Monitoring and Incident Response

Real-time network monitoring to detect and mitigate threats. Incident response services, including forensic analysis and threat containment.

Post-Incident Recovery

Helping organizations recover from breaches through data restoration, infrastructure repair, and implementing lessons learned to strengthen defenses.

Value Chain

Support activities

Infrastructure Management

Maintaining the tools, platforms, and cloud services used for cybersecurity operations.

Talent and Training

Recruiting and training cybersecurity professionals such as ethical hackers, analysts, and engineers. Continuous upskilling to keep pace with evolving threats and technologies.

Marketing and Awareness

Educating potential clients on the importance of cybersecurity through campaigns, reports, and threat intelligence updates. Promoting products and services to targeted industries.

Regulatory and Compliance Management

Ensuring solutions meet legal and industry-specific regulations (e.g., GDPR, HIPAA, PCI, DSS). Advising clients on compliance to avoid penalties or operational risks.

Ecosystem Partnerships

Collaborating with technology vendors, cloud providers, and others stakeholders to enhance solutions. Partnering with law enforcement and government agencies for threat intelligence sharing.

SWOT

Strengths

- **High Demand:** Growing reliance on digital technologies creates a strong, constant demand for cybersecurity solutions. Increasing frequency and sophistication of cyber threats drive investments.
- **Innovation-Driven:** Cutting-edge advancements in AI, machine learning, and threat detection enhance industry capabilities. Development of scalable solutions (e.g., SaaS, cloud security) broadens market research.
- **Regulatory Push:** Stringent regulations (e.g., GDPR, CCPA, HIPAA) ensure cybersecurity remains a priority for businesses accross industries.
- **Broad Applicability:** Solutions span multiple sectors (IT, BFSI, healthcare, manufacturing, etc.), ensuring diversified revenue streams.
- **Global Collaboration:** Growing networks for threat intelligence sharing and partnerships strengthen collective defenses.

Weaknesses

- **Talent Shortages:** Significant gap in skilled cubersecurity professionals, leading to operational challenges.
- **High Costs:** Advanced cybersecurity solutions can be expensive, limiting adoption among SMEs. Continuous R&D investments strain profitability for smaller firms.
- **Complexity of Solutions:** Difficulty in integrating security tools into existing IT environments. Overlap in offerings leads to inefficiencies and confusion for end-users.
- **Reactive Approach:** Industry focus often remains on reacting to threats rather than proactive risk management.

Opportunities

- **Expansion into Emerging Markets:** Rapid digitalization in regions like Asia-Pacific, Latin America, and Africa opens new revenue streams.
- **Cloud Security Growth:** Increased cloud adoption offers vast opportunities for securing cloud-based infrastructures and services.
- **IoT and 5G Security Needs:** Proliferation of IoT devices and 5G networks introduces new vulnerabilities, requiring tailored solutions.
- **AI and Automation:** Using AI to predict and respond to threats in real-time can enhance market leadership.
- **Regulatory Evolution:** Stricter data protection laws globally increase demand for compliance-focused cybersecurity services.
- **SME Market:** Rising awareness among small and medium enterprises presents opportunities for affordable, scalable solutions.

Threats

- **Evolving Cyber Threats:** Increasingly sphisticated attacks (e.g., ransomware, zero-day exploits) challenge current defenses.
- **Intense Competition:** Market saturation with numerous vendors, including large tech companies, drives down margins.
- **Economic Uncertainty:** Budget constraints in businesses during economic downturns may delay investments in security solutions.
- **Global Political Instability:** Geopolitical tensions and cyber warfare risks create unpredictable market dynamics.
- **Regulatory Penalties:** Non-compliance with evolving data protection regulations could lead to legal risks for service providers.

Market Value

The global cybersecurity market size was valued at USD 172.24 billion in 2023. The market is projected to grow from USD 193.73 billion in 2024 to USD 562.72 billion by 2032, exhibiting a CAGR of 14.3% during the forecast period.

Cybersecurity Market Trends

1. Zero Trust Architecture adoption

The **Zero Trust** model restricts network access exclusively to those who truly need it. Bases on context awareness, access is granted only to authorized users through patterns that take into account identity time, and the device being used. This model eliminates default access, requiring every access request to go through security protocols, including access controls and user identity verification.

Micro-Segmentation

Micro-segmentation divides the network into smaller, more secure segments, ensuring that **even if an attacker gains access to one segment, they cannot easily move laterally to other critical parts**. This practice minimizes the potential damage from a breach by limiting the attacker's ability to reach valuable data or systems.

Identity and Access Management (IAM)

Strong IAM policies enforce least-privilege access, **ensuring users and devices only have access to the resources necessary for their role**. By controlling access based on user identity and context, organizations can reduce the risk of unauthorized access and mitigate insider threats.

Continuous Monitoring and Authentication

Zero Trust emphasizes continuous monitoring of user activities and authentication. By constantly validating users and devices, **it ensures that any anomalous behavior is detected early**. This proactive approach reduces the window of opportunity for attackers and enhances the overall security posture.

1. Zero Trust Architecture adoption

CrowdStrike's Acquisition of Preempt Security

In September 2020, CrowdStrike, a leader in cybersecurity, acquired Preempt Security for $96 million. Preempt specialized in Zero Trust and conditional access technologies, focusing on identity and access management to prevent security breaches. This acquisitions enabled CrowdStrike to integrate Preempt's Zero Trust capabilities into its Falcon platform, enhancing its ability to enforce strict access controls and continuous verification of user identities. By adopting Zero Trust principles, CrowdStrike strengthened its defense against sophisticated cyber threats, aligning with the industry's shift towards more robust security frameworks.

2. Rise of Artificial Intelligence

AI has become a cornerstone of modern business operations, enabling companies to streamline processes, make data-driven decisions, and enhance customer experiences. Defined as the simulation of human intelligence by machines, AI spans machine learning, natural language processing, and computer vision, among others. Its benefits are transformative: from automating repetitive tasks to uncovering insights form complex datasets, AI empowers businesses to innovate faster, operate efficiently, and stay ahead of the competition.

Threat Intelligence and Predictive Analytics

AI leverages historical data and threat intelligence to predict future attacks. This **allows security teams to anticipate and prepare for potential breaches before they happen**, ensuring proactive defense mechanisms are in place and minimizing reactive measures.

AI-driven Threat Detection

AI algorithms analyze large volumes of data to identify suspicious patterns and behaviors that may indicate a cyberattack. **Machine learning models can detect subtle anomalies that may go unnoticed by human analysts**, thus speeding up the identification of threats and minimizing the potential impact of attacks.

Automated Incident Response

AI can automate certain security processes, such as blocking malicious IP addresses or isolating affected systems, **to contain and mitigate incidents quickly.** By reducing the need for manual intervention, AI helps improve response times and ensures that security protocols are consistently enforced across the organization.

2. Rise of Aritificial Intelligence

Thoma Bravo's Acquisition of Darktrace

Darktrace is known for its AI-powered self-learning systems that detect and respond to cybersecurity threats in real-time. Using machine learning algorithms, Darktrace's technology analyzes network activity to identify anomalies and potential threats without human intervention. This acquisition highlights the increasing importance of integrating AI into cybersecurity frameworks to proactively detect threats and enhance an organization's overall security posture.

The acquisition of AI-driven cybersecurity companies like Darktrace demonstrates the growing reliance on advanced AI technologies to predict, detect, and mitigate increasingly sophisticated cyber threats, underscoring the market trend of AI's rise in the cybersecurity sector.

3. Endpoint security for remote work

The shift to remote work has dramatically transformed how organizations approach cybersecurity, with endpoint security emerging as a cornerstone of defense strategies. Endpoint security refers to the measures taken to protect devices like laptops, smartphones, and tablets that connect to an organization's network remotely. As remote work expands the attack surface, endpoint security ensures data protection, mitigates risks from unsecure networks, and maintains compliance with regulations.

Endpoint Detection and Response (EDR)

EDR solutions provide continuous monitoring of endpoints, looking for signs malicious activities such as unusual file access or unauthorized network connections. By detecting these threats early, **EDR systems help prevent breaches and reduce the need for costly incident investigations**.

Mobile Device Management (MDM)

MDM solutions **enable organizations to enforce security policies on mobile devices**, including remote wipe capabilities in case of theft or loss. By securing mobile devices, companies ensure that sensiitve data remains protected even when employees access corporate resources on the go.

Data Loss Prevention (DLP)

DLP solutions help prevent the unauthorized transfer of sensitive data from endpoints to external locations. By monitoring and controlling data movement across devices, DLP **ensures that confidential information does not leave the organization**, even if an endpoint is compromised.

3. Endpoint security for remote work

SentinelOne's Acquisition of Attivo Networks

SentinelOne's acquisition of Attivo Networks in March 2022 represents a critical move to strengthen its position in the growing endpoint security market, especially in the context of remote work. Attivo Networks is a leader in identity detection and response (IDR) technologies, which address vulnerabilities associated with identity-based cyberattacks - one of the most significant threats in remote environments.

The $616.5 million deal enables SentinelOne to integrate Attivo's advanced identity protection capabilities with its AI-driven endpoint detection and response (EDR) platform. This combination is highly strategic, as it offers organizations a more comprehensive security solution, combining endpoint protection with identity threat detection. In the era of remote work, where distributed workforces and diverse access points are the norm, this integration ensures stronger defenses against lateral movement, credential theft, and Active Directory attacks.

4. Managed security services (MSS)

Managed Security Services (MSS) are reshaping the cybersecurity landscape by offering outsourced solutions to monitor, detect, and respond to cyber threats in real-time. These services provide companies with 24/7 security expertise, access to advanced tools, and cost-efficient protection against evolving cyber risks. By partnering with Managed Security Service Providers (MSSPs), organizations can enhance their threat detection capabilities, maintain compliance with regulatory standards, and focus on core business objectives while leaving cybersecurity to trusted experts.

Increasing Adoption of AI-Driven Managed Security Services

Artificial intelligence (AI) is revolutionizing MSS by enabling faster and more accurate threat detection. MSSPs are leveraging AI and machine learning algorithms to analyze vast volumes of data, identify anomalies, and predict potential vulnerabilities. **These technologies empower MSSPs to respond to threats in real-time, reducing incident response times** and minimizing damage. As the volume of cyberattacks grows, AI-driven MSS is becoming a critical asset for organizations seeking scalable and efficient security solutions.

Growth of Industry-Specific MSS Solutions

MSSPs are increasingly tailoring their services to meet the unique needs of specific industries, such as healthcare, finance, and retail. **These specialized solutions address industry-specific threats and regulatory requirements**, such as HIPAA compliance in healthcare or PCI DSS standards in retail. By offering sector-focused services, MSSPs enable organizations to address their most pressing security challenges while ensuring compliance with complex legal and regulatory frameworks.

Expansion of Cloud-Based Managed Security Services

With the rapid adoption of cloud technologies, **MSSPs are developing cloud-native solutions to protect hybrid and multi-cloud environments**. Cloud-based MSS provides centralized monitoring, automated updates, and seamless integration with existing IT infrastructures. These services allow organizations to secure their cloud workloads without compromising scalability or flexibility.

4. Managed security services (MSS)

IBM's Acquisition of Randori

A recent example of M&A in the MSS market is IBM's acquisition of Randori in 2022. Randori specializes in attack surface management and continuous automated red-teaming solutions, allowing organizations to identify and mitigate vulnerabilities before attackers exploit them. By integrating Randori's technology, IBM enhanced its MSS offerings, enabling clients to proactively manage their security postures. This acquisition highlights how companies are using M&A strategies to expand their capabilities, innovate, and address the evolving cybersecurity needs of their customers.

5. Cloud Security Expansion

Cloud security has become a critical focus as businesses increasingly migrate their operations and data to cloud environments. Defined as the practices and technologies designed to protect cloud infrastructure, applications, and data, cloud security ensures confidentiality, integrity, and availability. The benefits are compelling: enhanced scalability, cost efficiency, and protection against data breaches.

Cloud Acces Security Brokers (CASBs)

CASBs act as **intermediaries between users and cloud services**, offering visibility into cloud activity and ensuring compliance with security policies. By monitoring cloud traffic, CASBs help prevent data breaches and unauthorized access to sensitive information stored in the cloud.

Cloud Encryption

Encypting dtaa both at rest and in transit within cloud environments **ensures that sensitive information remains protected from unauthorized access**. Even if a hacker gains access to the cloud infrastructure, encrypted data remains unreadable, minimizing the risk of data theft.

Identity and Access Management (IAM) in the Cloud

IAM solutions for the cloud control user access to cloud applications and resources, **ensuring that only authorized personnel can access critical systems**. These solutions implement features like single sign-on and multi-factor authentication to prevent unauthorized access, especially in large and complex cloud environments.

5. Cloud Security Expansion

Palo Alto Network's Acquisitions of Dig Security

In December 2023, Palo Alto Networks announced its acquisition of Dig Security, a data security posture management (DSPM) company, for $400 million. This strategic move aims to enhance Palo Alto Network's cloud security capabilities by integrating Dig Security's advanced data protection solutions into its existing platform. The acquisition reflects Palo Alto Networks' commitment to providing comprehensive security across multi-cloud environments, addressing the growing need for robust data security as organizations increasingly adopt cloud technologies. By incorporating Dig Security's expertise, Palo Alto Networks positions itself to offer more holistic and effective cloud security solutions to its clients.

6. Regulatory compliance

Regulatory compliance has become a pivotal aspect of cybersecurity strategies as businesses face an evolving landscape of legal and industry requirements. Defined as adherence to laws and regulations governing data security, privacy, and operations, regulatory compliance protects organizations from legal penalties and reputational damage. Beyond risk mitigation, it fosters customer trust, ensures data integrity, and enhances resilience against cyber threats, amking it indispensable for sustainable business growth.

Rise of Privacy-Centric Regulations

The adoption of privacy regulations like GDPR in Europe and CCPA in California has set a global standard for data protection. Businesses are increasingly implementing frameworks to ensure compliance with these regulations, such as establishing data governance policies and enabling user control over personal information. **This trend has amplified the demand for tools that automate compliance processes**, such as data mapping and breach notification systems, helping organizations stay aligned with dynamic privacy laws.

Integration of Compliance with Cybersecurity Frameworks

Companies are moving towards integrating compliance requirements directly into their cybersecurity frameworks. Standards like NIST and ISO 27001 serve as blueprints for **aligning regulatory obligations with robust cybersecurity practices**. This approach ensures that security measures not only prevent breaches but also address compliance mandates proactively. Automated compliance reporting tools and regular audits are becoming essential to bridge the gap between regulatory adherence and cyber defense.

Expansion of Sector-Specific Compliance Solutions

Different industries face unique regulatory challenges, prompting a rise in sector-specific compliance solutions. For instance, financial institutions must comply with PCI DSS, while healthcare providers adhere to HIPAA. Companies are adopting tailored tools and services that address these niche requirements, such as solutions for securing payment data or safeguarding patient records. **This specialization ensures that compliance efforts are both effective and industry-relevant.**

6. Regulatory compliance

Cisco's Acquisition of Splunk

In September 2023, Cisco announced its intent to acquire Splunk, a leader in data analytics and security information and event management (SIEM), for $28 billion. This strategic move aims to bolster Cisco's cybersecurity portfolio, particularly in regulatory compliance. Splunk's capabilities in monitoring and analyzing machiine-generated data enable organizations to meet compliance requirements effectively. By integrating Splunk's advanced analytics with its existing security solutions, Cisco plans to offer comprehensive tools that assist businesses in adhering to complex regulatory standards, thereby overall security posture.

7. Focus on ransomware prevention

Ransomware attacks have become one of the most damaging cyber threats, crippling businesses by encrypting critical data and demanding payment for its release. Ransomware prevention focuses on proactive measures such as advanced threat detection, endpoint protection, and employee training to mitigate these risks. The benefits are significant: safeguarding data integrity, ensuring business continuity, and avoiding costly downtime. Companies adopting robust ransomware prevention strategies are better positioned to resist this growing menace.

Regular Data Backups and Recovery Plans

Regularly backing up data and establishing a disaster recovery plan is essential for recovering from a ransomware attack without paying the ransom. Secure backups, both on-site and off-site, help **ensure that organizations can restore their systems quickly and resume normal operations**.

Employee Awareness and Training

Educating employees on recognizing phishing emails, malicious attachments, and unsafe links is one of the most effective ways to prevent ransomware infections. By training staff to follow best security practices, **organizations can significantly reduce the likelihood of a successful attack**.

Incident Response Playbooks and Automation

Organizations are increasingly developing detailed **incident response playbooks** that outline step-by-step actions to take in the event of a ransomeware attack. These playbooks include predefined protocols for isolating infected systems, identifying the attack vector, and restoring systems from secure backups. To streamline this process, many companies are integrating **automation** tools that can execute specific recovery actions without human intervention, such as triggering backup restorations or blocking malicious network traffic.

7. Focus on ransomware prevention

Sophos Acquires Secureworks

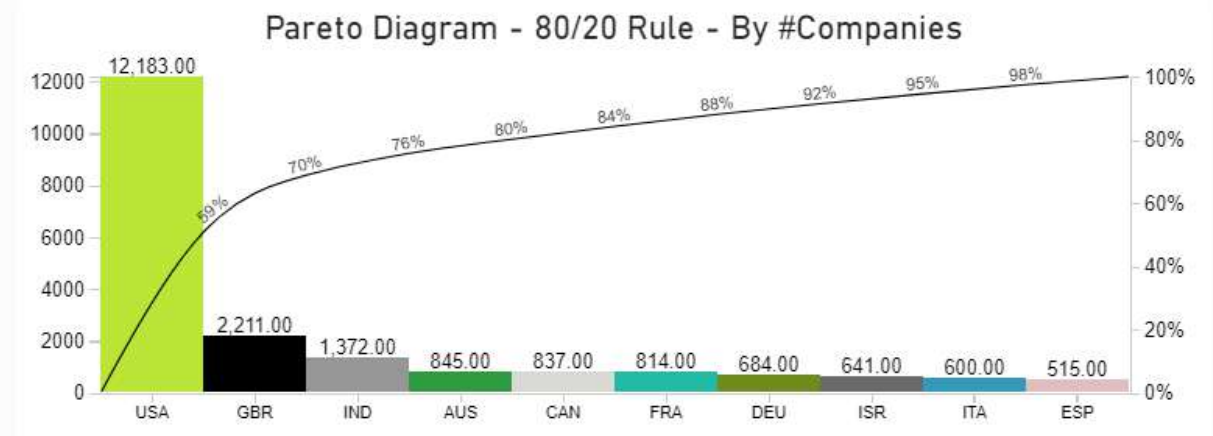
In October 2024, Sophos, a cybersecurity firm backed by Thoma Bravo, announced its acquisition of Secureworks from Dell Technologies for $859 million in cash. Secureworks' flagship platform, Taegis, specialized in detecting advanced threats, thereby enhancing Sophos' capabilities in ransomware prevention. This strategic move aims to bolster Sophos' product lineup for enterprise customers, providing more robust defenses against ransomware attacks. The transaction is expected to close in early 2025.

Cybersecurity Market Funding

Global Funding

SOURCE | **Crunchbase**

Global Funding by Geography



Top Countries by funding

Country	#Rounds
United States	5754
United Kingdom	817
Israel	646
Canada	302
France	275
China	207
India	160
Germany	154
Switzerland	148
Australia	144
Singapore	134
Spain	101
The Netherlands	96
Ireland	75
Italy	70
South Korea	68
Estonia	67
Japan	60
Sweden	59

SOURCE | **Crunchbase**

Global Funding by Sectors

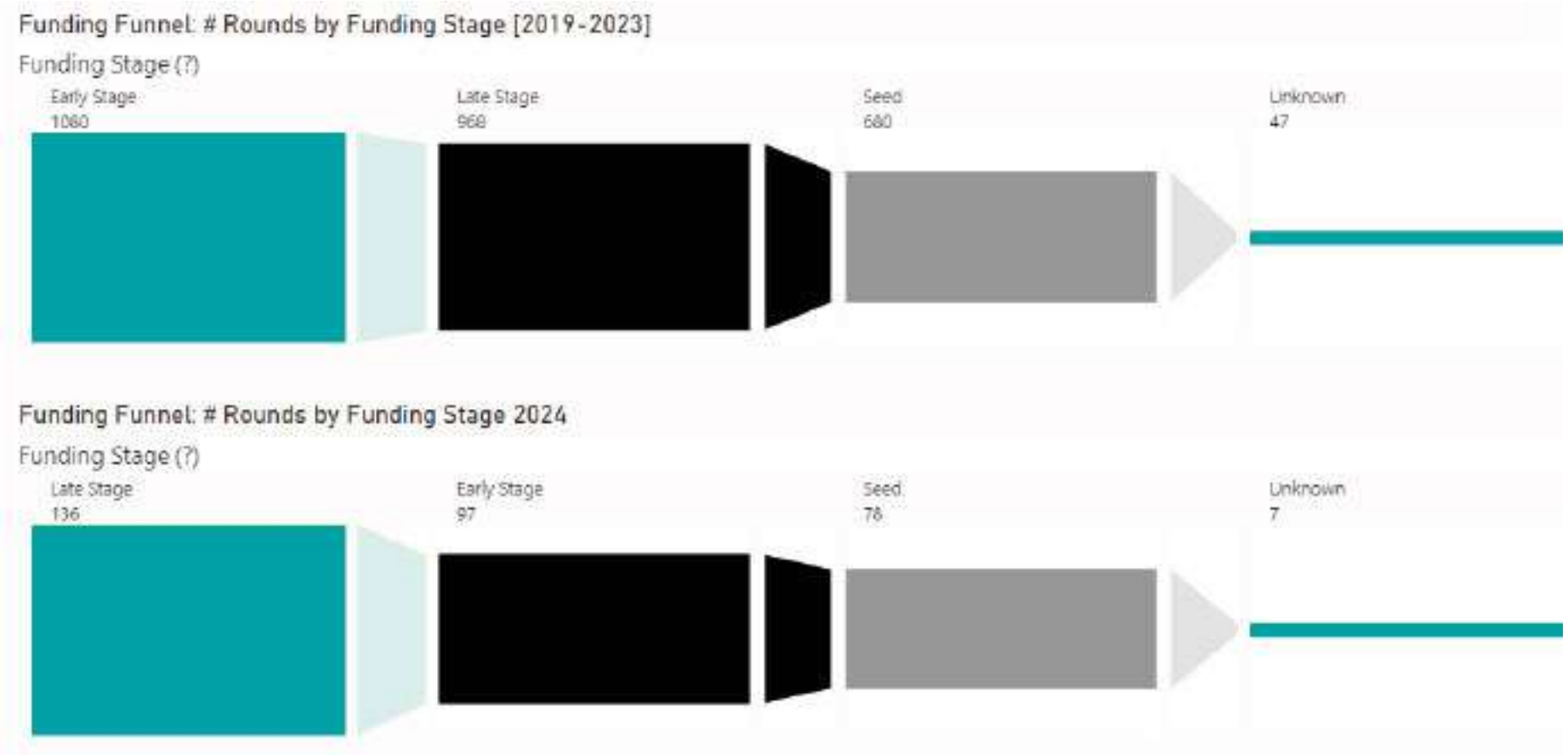
Category Name	Companies	Funding Rounds	Total Funding ($)
Cyber Security	27755	9107	$165,39 mil M
Information Technology	15017	3208	$62,66 mil M
Software	7059	3853	$62,41 mil M
Security	4469	3074	$62,34 mil M
Network Security	3993	2273	$48,16 mil M
Consulting	5835	229	$12,68 mil M
Cloud Security	1490	1323	$26,44 mil M
Computer	833	451	$10,76 mil M
Enterprise Software	535	925	$16,02 mil M
Information Services	918	314	$4,06 mil M
SaaS	903	1281	$16,98 mil M
Analytics	843	584	$10,70 mil M
Cloud Computing	2248	314	$4,82 mil M
Internet	1153	535	$9,42 mil M
Artificial Intelligence (AI)	1401	1165	$20,41 mil M
Risk Management	1141	579	$6,54 mil M
IT Management	1491	129	$1,25 mil M
Telecommunications	891	157	$7,19 mil M

NOTE

The table shows the distribution of **Cybersecurity** companies segmented by different sectors or categories. It should be noted that a company, in addition to being categorized as Cybersecurity, may also be in one or more other categories.

SOURCE | **Crunchbase**

Global Funding Funnel

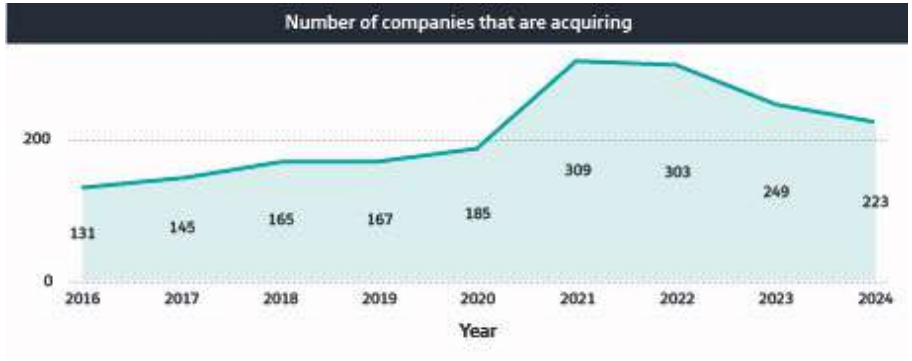


SOURCE | **Crunchbase**

Cybersecurity M&A

Global Acquisitions

Number of companies in the **Cybersecurity** sector that have been acquired by other companies (in the sector or not) in the last years.



Number of companies in the **Cybersecurity** sector that have bought from other companies (in the sector or not) in the last years.

SOURCE | **Crunchbase**

Global Acquisitions by Geography

Number of companies in the **Cybersecurity** sector that have been acquired by other companies (in the sector or not) in the last years by continent.

Number of companies in the **Cybersecurity** sector that have bought from other companies (in the sector or not) in the last years by continent.

SOURCE | **Crunchbase**

Global Acquisitions by Sectors

Category Name	Companies	Acquisitions
Cyber Security	27755	1886
Information Technology	15017	878
Software	7059	651
Security	4469	648
Network Security	3993	392
Consulting	5835	208
Cloud Security	1490	165
Computer	833	136
Enterprise Software	535	113
Information Services	918	111
SaaS	903	111
Analytics	843	100
Cloud Computing	2248	90
Internet	1153	89
Artificial Intelligence (AI)	1401	86
Risk Management	1141	85
IT Management	1491	64
Telecommunications	891	60

NOTE

The table shows the distribution of **Cybersecurity** companies segmented by different sectors or categories. It should be noted that a company, in addition to being categorized as Cybersecurity, may also be in one or more other categories. #Acquisitions show the number of companies bought during the whole time.

SOURCE | **Crunchbase**

Latest Acquisitions

Date	Logo	Acquiree	Acquiree Description	Founded on	Acquiree Location	Logo	Acquirer	Acquirer Description	Acquirer Founded Date
2024-12-02	KYRUS	Kyrus Tech	Cybersecurity R&D, Services	2009-04-01	United States		SIXGEN	SIXGEN provides cybersecurity services and products protecting critical assets and infrastructure from global adversaries.	2014-01-01
2024-11-27	Blowfish	Blowfish	Blowfish detects and prevents fraud before any fraud occurs.	2022-01-01	Spain		Phantom	The friendly crypto wallet built for DeFi & NFTs.	2021-03-01
2024-11-25		IDX	IDX is a consumer privacy platform that enables consumers to take control of their privacy and identity.	2003-01-01	United States		Kingswood Capital Management	Kingswood Capital Management is a private investment firm.	2013-01-01
2024-11-25	tmc	Tmc3	Tmc3 provides cloud and cyber security services.	2021-01-01	United Kingdom	Qodea	Qodea	Qodea provides security and infrastructure, data activation and AI, and modernisation and innovation.	2009-01-01
2024-11-22	OTRS	OTRS	Open Source Help Desk solutions and ITSM	2003-01-01	Germany	easyVISTA	EasyVista	ITSM and Self Help Software That Makes it Easy to Deliver Services to Employees and Customers	1988-01-01
2024-11-22	JGROUP	J Group Consulting	J Group Consulting is an IT consulting firm that provides access management strategy, cloud integrations, and cyber security solutions.	2022-01-01	Australia	EY	EY	EY Japan is a professional services firm that specialises in consulting, assurance, tax, strategy, and transaction services.	1989-01-01
2024-11-21	appviewx	AppViewX	AppViewX is a certificate lifecycle management and network automation company.	2015-01-01	United States		Haveli Investments	Haveli Investments is a technology-focused private equity firm.	2021-01-01
2024-11-20	KC	Karthik Consulting	Karthik Consulting provides services in cybersecurity, software development, operations management & project management.	2008-01-01	United States		CoreStack Inc	CoreStack delivers continuous and autonomous cloud governance for enterprises.	2016-11-04

SOURCE | **Crunchbase**

Cybersecurity IPOs

Latest IPOs

Logo	Went Public on	Amount Raised ($)	Company	Description	Founded Date	# Acquisitions	Country	Listed Stock Symbol	Valuation ($)
	2024-09-15	150,00 mill.	ReverseMails	ReverseMails is an email verification application made to assist users in locating and handling dubious or unreliable email addresses.	2023-01-15		United States	nasdaq	$0,00 mil M
	2024-04-12	946,90 mill.	UL Solutions	UL Solutions is a safety science company that promotes safety science through research and investigation.	1894-01-01	23	United States	nyse	
	2024-04-05	3,60 mill.	TAC Security	TAC Security is a vulnerability management that protects Fortune 500 companies, large enterprises & governments globally.	2013-02-27	1	United States	nse	$0,03 mil M
	2024-01-24	5,00 mill.	SU Group Holdings	SU Group Holdings specializes in the development, installation, and maintenance of cyber-security systems and related infrastructure.	1998-01-01		Hong Kong	nasdaq	
	2023-10-10	1,25 mill.	Integrated Cyber	Integrated Cyber is a managed cyber security service that manages both the human firewall and cyber software to keep the company safe.	2017-01-01		United States	cse	
	2023-09-21	30,78 mill.	Yubico	Yubico protects logins with hardware devices like YubiKey, which offer secure and user-friendly two-factor and passwordless authentication.	2007-01-01	1	United States	sto	$0,66 mil M
	2023-03-01		HUB Security	HUB Security is redefining cyber security with quantum-driven confidential computing.	2017-11-01	3	Israel	nasdaq	
	2022-12-31	0,02 mill.	Cyberwebnic Watch	Cyberwebnic Watch is a well-established and respected Internet Security company specializing in Anti-Phishing solutions.	2022-01-01		United States	amex	$0,00 mil M

SOURCE | **Crunchbase**

Cybersecurity Investments

Most Active Investors last 3 Years

Venture Capital

VC	Description	Investments	Lead Investments	Sector Companies	Total Invested	Acquisitions of Invested	Funding Rounds	Investors
Techstars	Techstars is a global platform that provides investment and innovation.	5425	2783	66	$103,54 M	5	190	182
Bossanova Investimentos	Bossa nova investimientos is a brazilian Micro-VC focused on pre-seed stage technology companies.	1686	27	44	$993,25 M	35	232	228
Tiger Global Management	Tiger Global Management is an investment firm that deploys capital globally in both public and private markets.	1141	684	40	$6.975,83 M	35	225	319
Plug and Play	Plug and Play is an innovation platform bringing together startups and large corporations.	1523	72	31	$294,94 M	6	126	155
Accel	Accel is an early and growth-stage venture capital firm that helps a global community of entrepreneurs.	1889	734	29	$3.124,83 M	12	131	252
Gaingels	Gaingels represents the LGBT+ community and allies investing in VC-backed companies with diverse and inclusive leadership teams.	611	6	28	$2.285,23 M	18	157	362

Private Equity

PE	Description	Investments	Lead Investments	Sector Companies	Total Invested	Acquisitions of Invested	Funding Rounds	Investors
Insight Partners	Insight Partners is a private equity firm that invests in growth-stage technology and software companies.	980	657	45	$6.155,35 M	22	228	309
Tiger Global Management	Tiger Global Management is an investment firm that deploys capital globally in both public and private markets.	1141	684	40	$6.975,83 M	35	225	319
Coatue	Coatue invests in public and private equity markets focusing on the technology, media, and telecommunications industries.	389	192	19	$5.314,42 M	15	97	201
SoftBank Vision Fund	SoftBank Vision Fund specializes in growth capital and social impact investments.	412	313	14	$3.901,00 M	21	90	109
BlackRock	BlackRock is an investment company that offers its services to institutions, intermediaries, foundations, and individual investors.	284	99	12	$5.521,00 M	28	84	137
Valor Equity Partners	Valor Equity Partners is an operational growth investment firm focused on high growth.	175	58	11	$843,65 M	7	64	84

SOURCE | **Crunchbase**

Latest Investments

Funded	Funded Description	Founded Date	Funded Location	Investor	Investor Description	# Investments	Date	Money Raised	Investment Type
Wiz	Wiz is a cybersecurity company that allows companies to find security issues in public cloud infrastructure.	2020-01-01	United States	SoftBank Vision Fund	SoftBank Vision Fund specializes in growth capital and social impact investments.	438	2024-11-18		debt_financing
Ripjar	Ripjar is a data intelligence company that transforms global institutions ability to manage strategic risks.	2012-01-01	United Kingdom	Dow Jones	Dow Jones is a news and business information provider that delivers content to consumers and organizations via newspapers and more.	4	2024-11-08		private_equity
Performive	The first hyperconverged, VMware multicloud provider specifically built to serve the Mid-Market.	2005-01-15	United States	Renovus Capital Partners	Renovus Capital Partners provides equity capital and strategic assistance to small and mid-sized education companies.	8	2024-11-04		private_equity
Armis Security	Armis is a developer of an asset intelligence platform to analyze endpoint behavior to identify risks and attacks.	2015-01-01	United States	Alkeon Capital	Alkeon Capital Management is a service that assists investors with their financial endeavors.	62	2024-10-28	$200,00 mill.	series_d
Armis Security	Armis is a developer of an asset intelligence platform to analyze endpoint behavior to identify risks and attacks.	2015-01-01	United States	General Catalyst	General Catalyst is a venture capital firm that provides early-stage and growth equity investments.	1297	2024-10-28	$200,00 mill.	series_d
Human	HUMAN is a cybersecurity company that protects the internet and enterprises from fraud and sophisticated bot attacks.	2012-06-20	United States	WestCap	WestCap is a strategic operating and investing firm that focuses on tech-enabled, asset-light marketplaces.	54	2024-10-09	$50,00 mill.	series_unknown
Roke Manor Research	Roke is a leading innovator in science and engineering, trusted by clients across National Security, Defence and Commercial sectors.	1956-01-01	United Kingdom	Defence and Security Accelerator	Defence and Security Accelerator is a Defense & Space organisation.	6	2024-09-26		grant
Siemens	Siemens is a technology company that offers cybersecurity, digital consulting, and business services.	1847-01-01	Germany	US Department of Energy	US Department of Energy is a government administration that regulates energy policy, research, and development.	1038	2024-09-17	$1,50 mill.	grant
DAZZ	Dazz delivers unified security remediation across code, clouds, infrastructure, and applications for security and development teams.	2021-01-01	United States	Cyberstarts	Cyberstarts is an early-stage cybersecurity-focused venture capital firm.	41	2024-07-24	$50,00 mill.	series_unknown
DAZZ	Dazz delivers unified security remediation across code, clouds, infrastructure, and applications for security and development teams.	2021-01-01	United States	Greylock	Greylock Partners invests in entrepreneurs that focus on consumer and enterprise software companies.	873	2024-07-24	$50,00 mill.	series_unknown

SOURCE | **Crunchbase**

About Baker Tilly

Baker Tilly is a leading advisory, tax and assurance firm dedicated to building long-lasting relationships and helping you win now and anticipate tomorrow. We have only one agenda: Yours.

"We describe change as progress because that is exactly what is happening at Baker Tilly. Our fundamental purpose is to enhance and protect our clients' value"

Francesca Lagerberg - CEO

"Relationships are the foundation of our firm. They are the way we earn the trust of our clients and our teammates".

Bill Chapman - Partner

Contact us

advisory@bakertilly.es

+34 946 42 41 42

www.techma.bakertilly.es

bakertilly