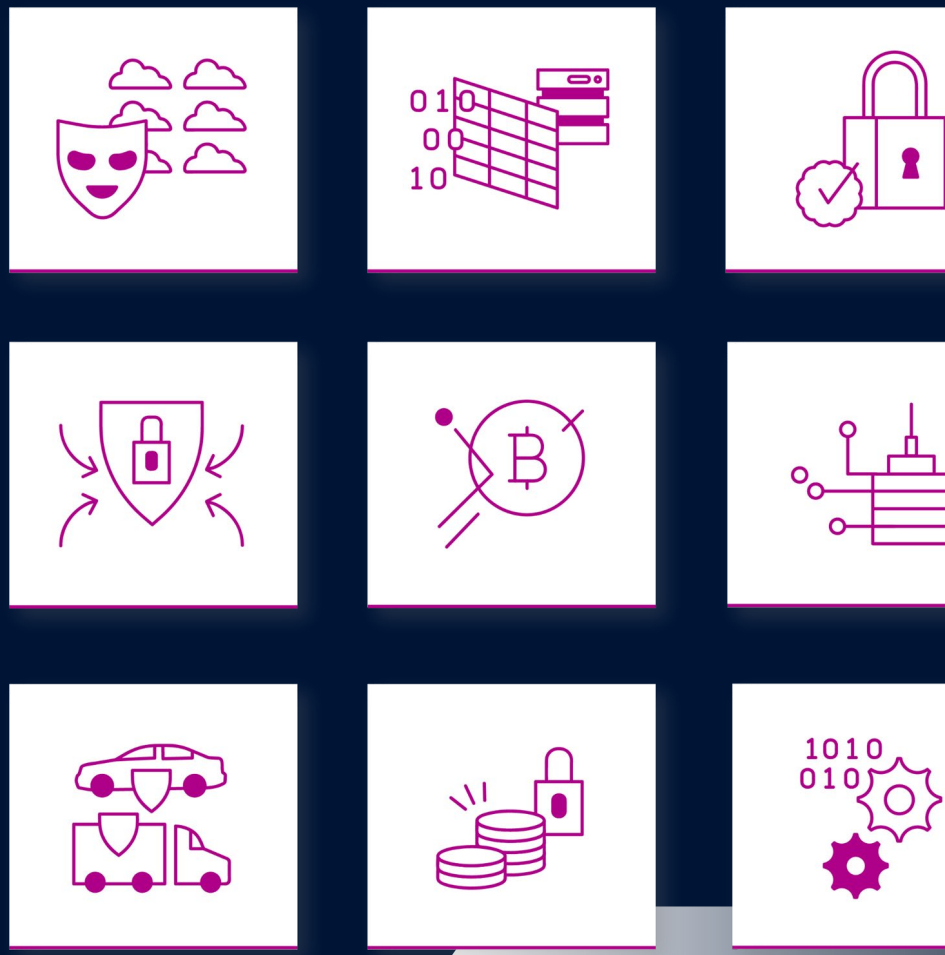
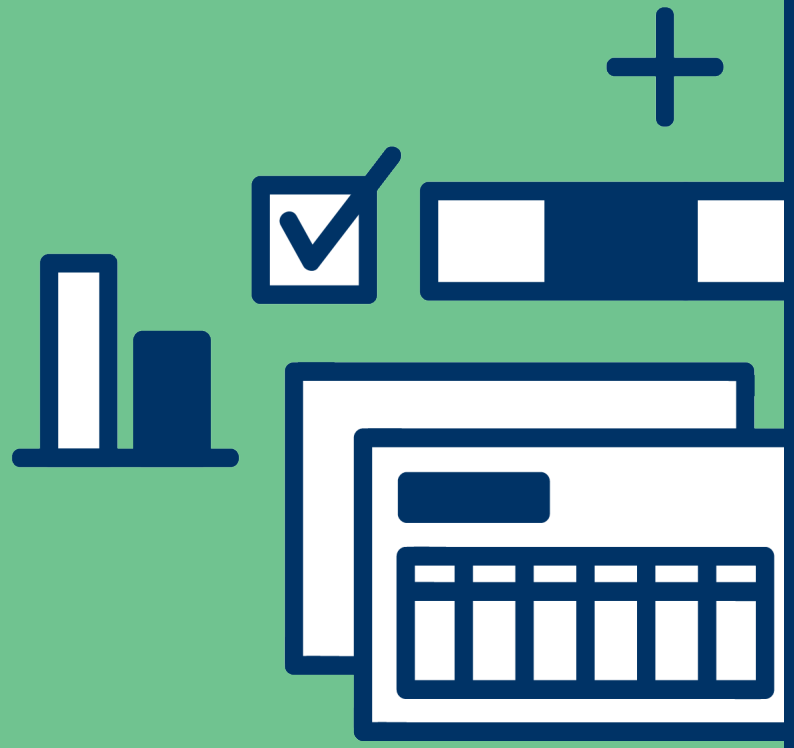
Cyber Defenders 2021

The 28 companies defending businesses from next-gen cyber attacks



CBINSIGHTS



WHAT IS CB INSIGHTS?

CB Insights helps the world's leading companies make smarter technology decisions with data, not opinion.

Our Technology Insights Platform provides companies with comprehensive data, expert insights and work management tools to drive growth and improve operations with technology.

CLICK HERE TO SIGN UP FOR A FREE TRIAL

CB Insights helps us compress our time-to-decision when gathering and analyzing data and getting an external view on what's happening in the market so we can quickly take action.

Meraj Mohammad
Vice President, Ventures Group, ADP

ADP | CBINSIGHTS

Contents

Cybersecurity Market Drivers

"…the scale of this [cyber criminal attacks] is something that I don't think this country has ever really seen anything quite like it and it's going to get much worse."

- Christopher Wray, FBI director, June 2021

CYBER ATTACKS MAKE HEADLINES, PROMPT GOVERNMENT RESPONSES

Ransomware Attack Affecting Likely Thousands of Targets Drags On

July 2021 | THE WALL STREET JOURNAL.

EU wants emergency team for 'nightmare' cyber-attacks

June 2021 | BBC

SolarWinds Hack Grabs Senate Spotlight With CEO in the Hot Seat

February 2021 | Bloomberg

Executive order aims to protect software supply chains

June 2021 | REUTERS®

More than 20,000 U.S. organizations compromised through Microsoft flaw

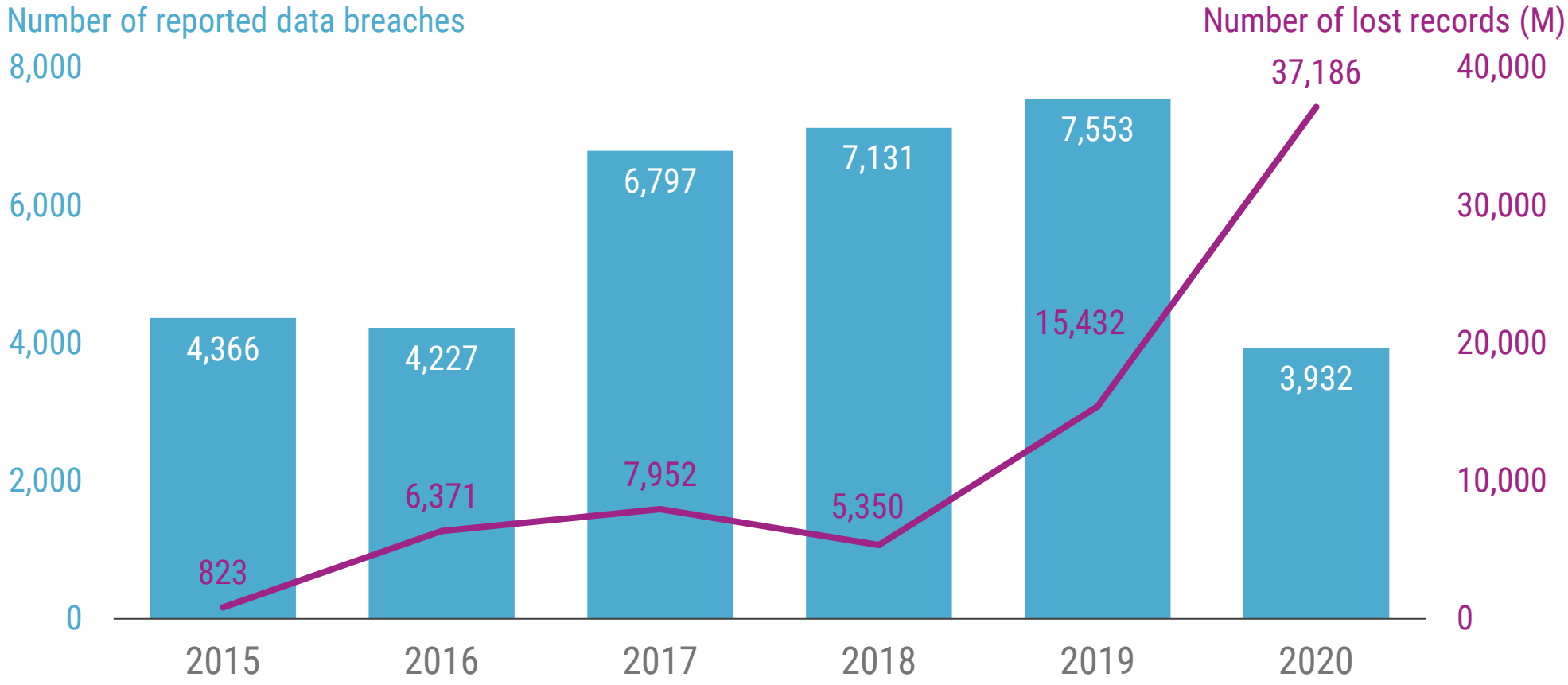
March 2021 | REUTERS®

U.S. Pipeline Cyberattack Forces Closure

May 2021 | THE WALL STREET JOURNAL.

DATA BREACHES LEAVE BILLIONS OF RECORDS EXPOSED

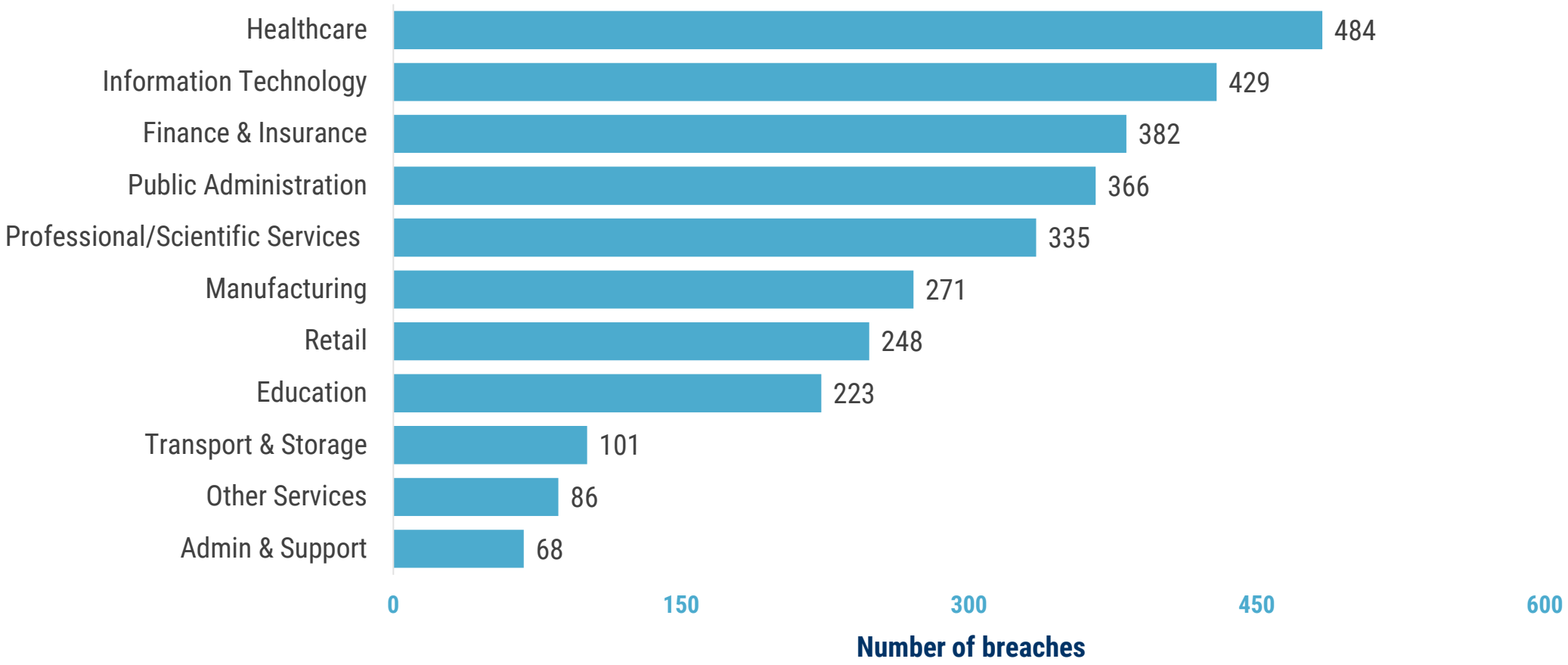
NUMBER OF DATA BREACHES AND LOST RECORDS, 2015 – 2020



Source: Risk Based Security

CYBER INSECURITY IS FELT ACROSS INDUSTRIES

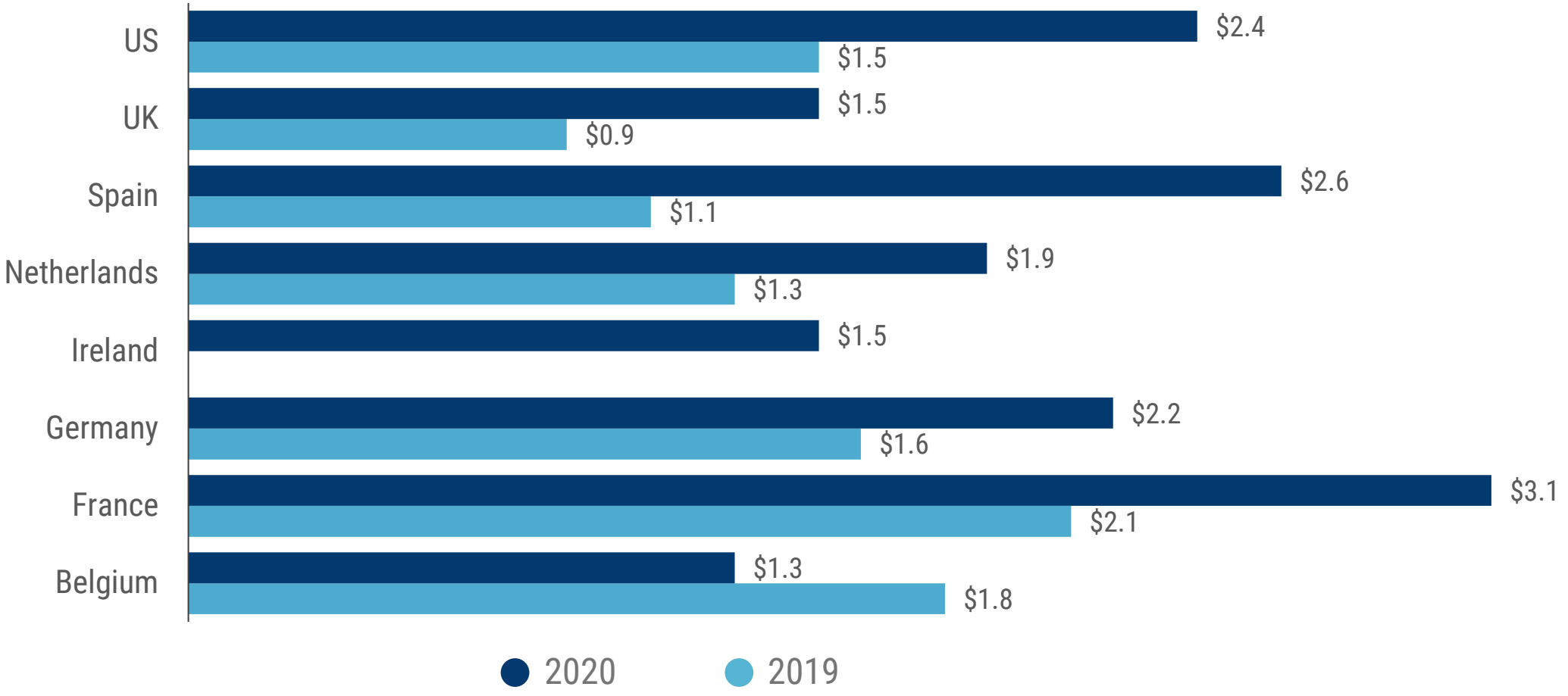
NUMBER OF DATA BREACHES BY ECONOMIC SECTOR IN 2020



Source: Risk Based Security

COMPANIES ARE INVESTING IN PROTECTION

AVERAGE CORPORATE CYBERSECURITY SPEND ($M) BY COUNTRY



Source: Hiscox

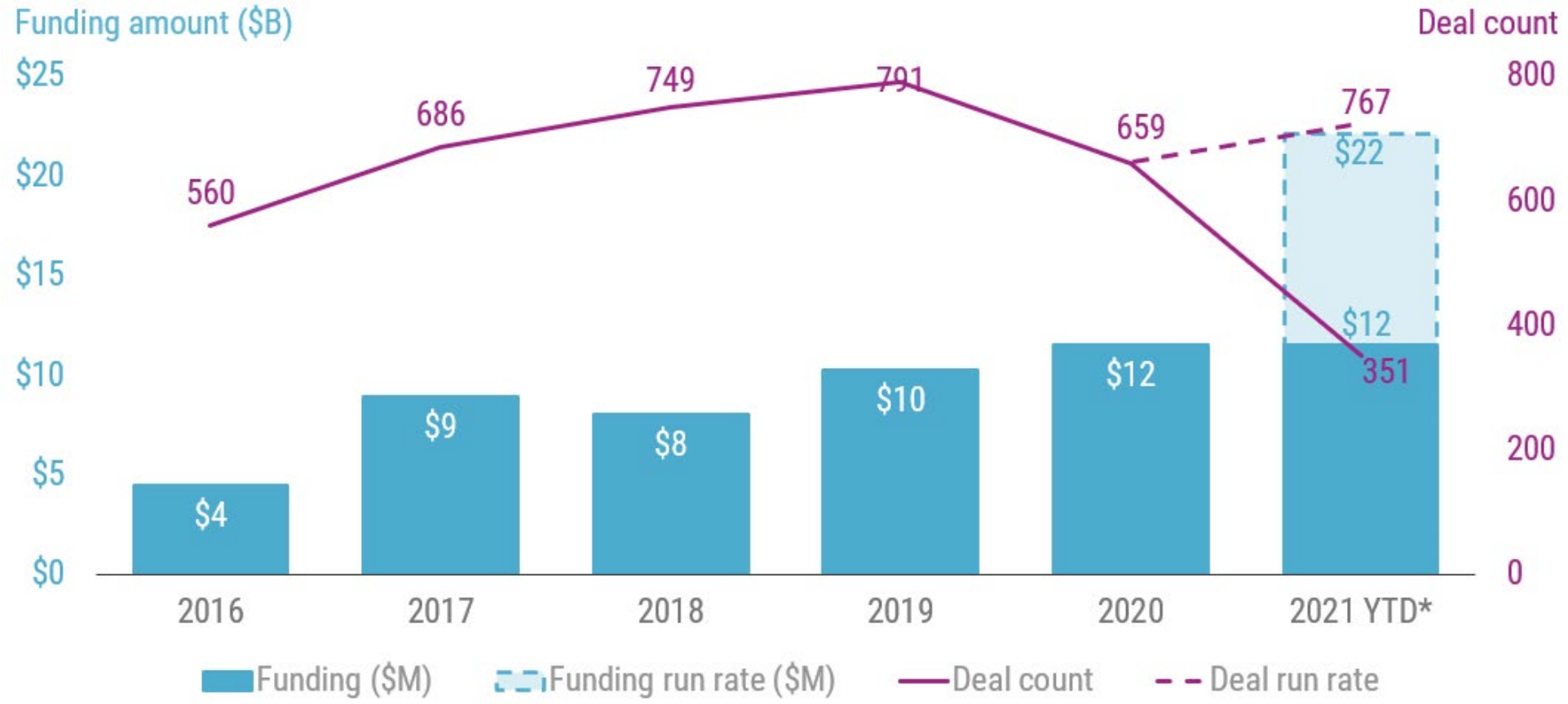
TALK OF CYBERSECURITY AMONG THE C-SUITE INCREASES

NUMBER OF EARNINGS CALLS MENTIONS OF "CYBERSECURITY," Q2'16 – Q1'21

Cybersecurity Funding Trends

Cybersecurity funding up in 2021 despite fewer deals

Annual global cybersecurity deals and equity funding ($B), 2016 – 2021 YTD (06/15/21)

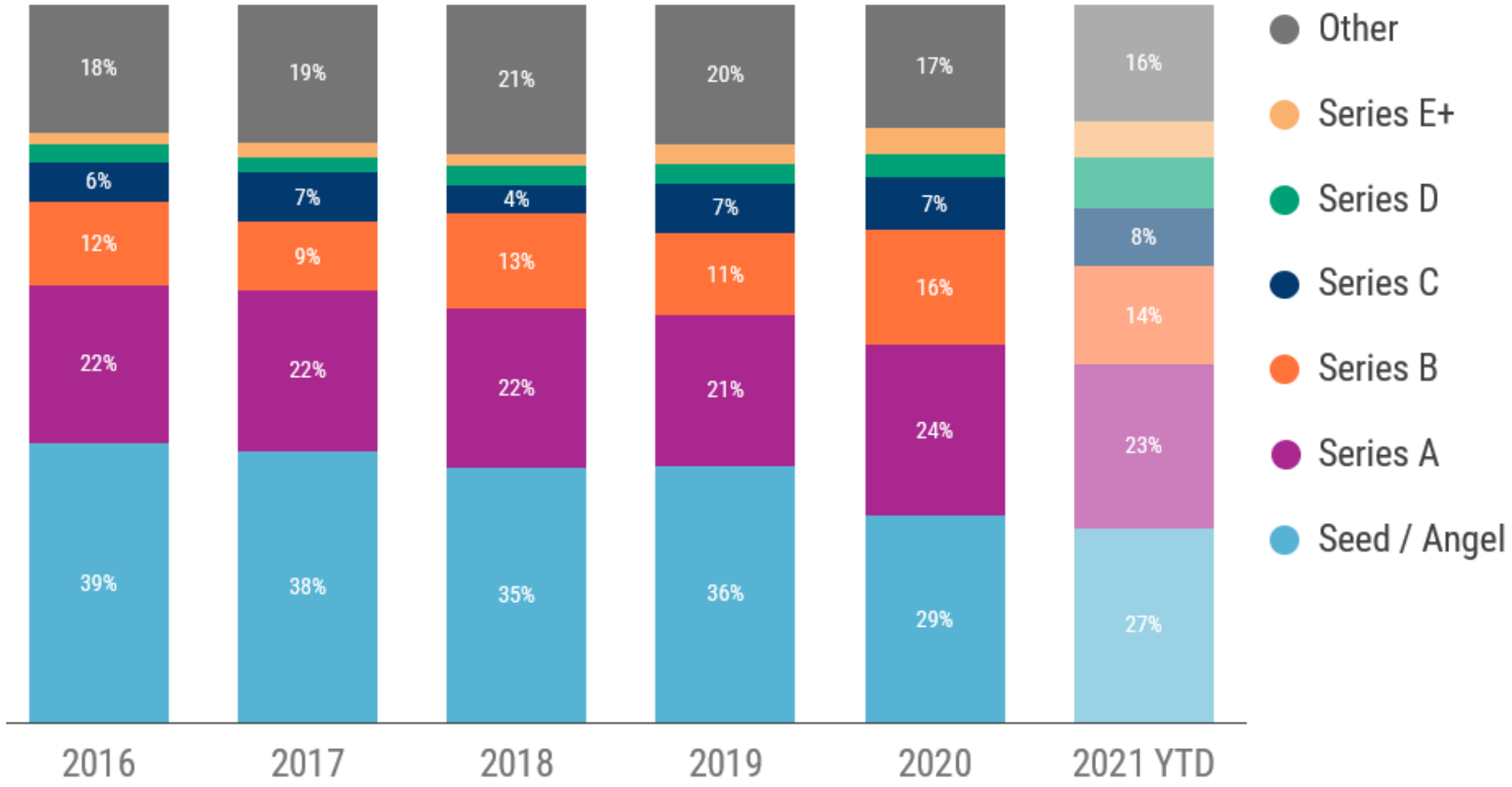


*2021 full-year data is based on a run rate as of 06/15/21.

SEED-STAGE DEALS REACHED FIVE-YEAR LOW IN 2020

Series A & B deal shares jumped YoY in 2020

Annual deal share by stage, 2016 – 2021 YTD (06/15/2021)



MOST ACTIVE INVESTORS

Insight, Lightspeed, and Salesforce top rankings

Most active investors in cybersecurity startups by investor type, 2020

Venture capital

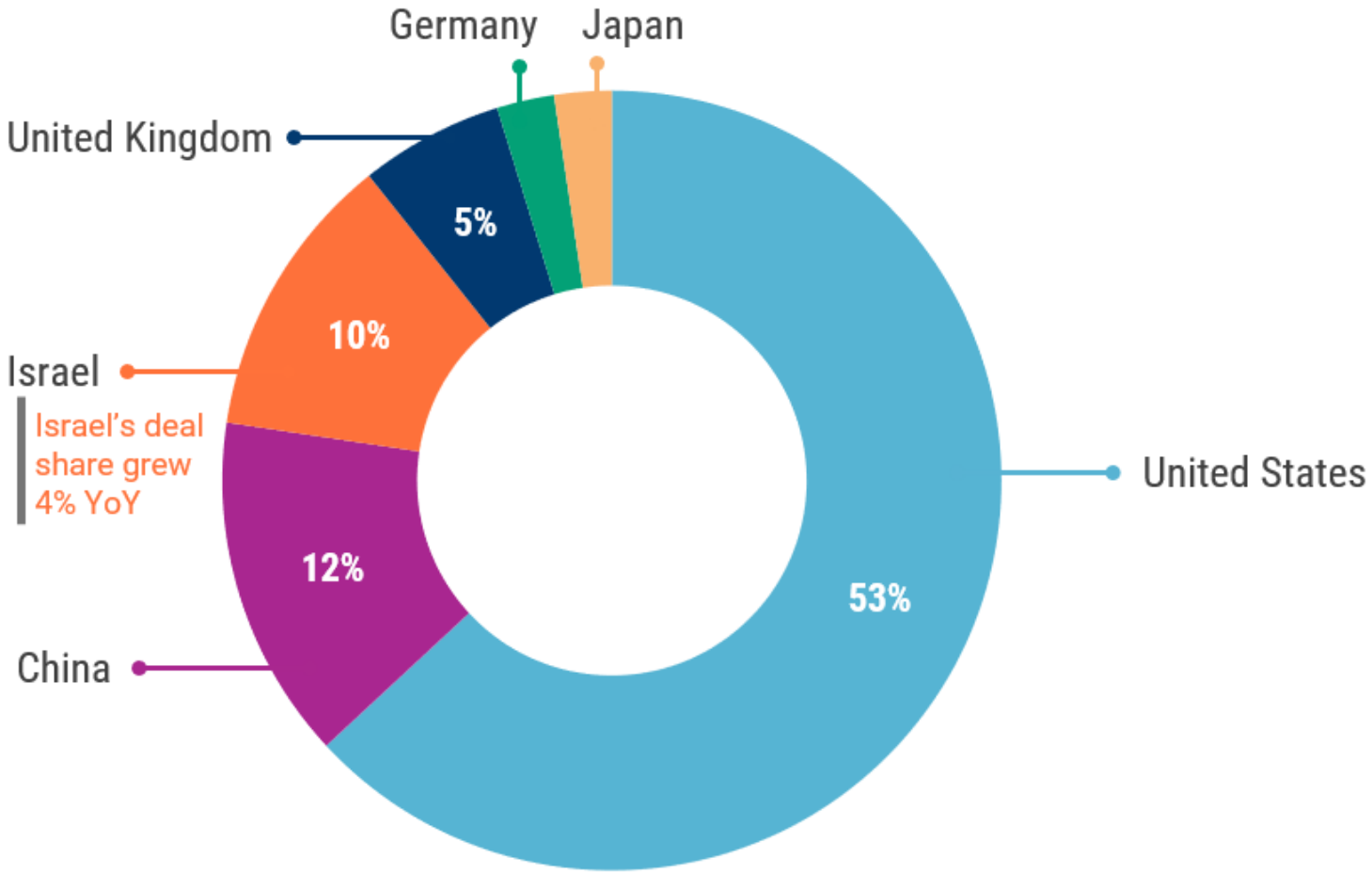
Corporate venture

*Lightspeed and Accel each made 12 investments.

ISRAEL'S DEAL SHARE GREW IN 2020

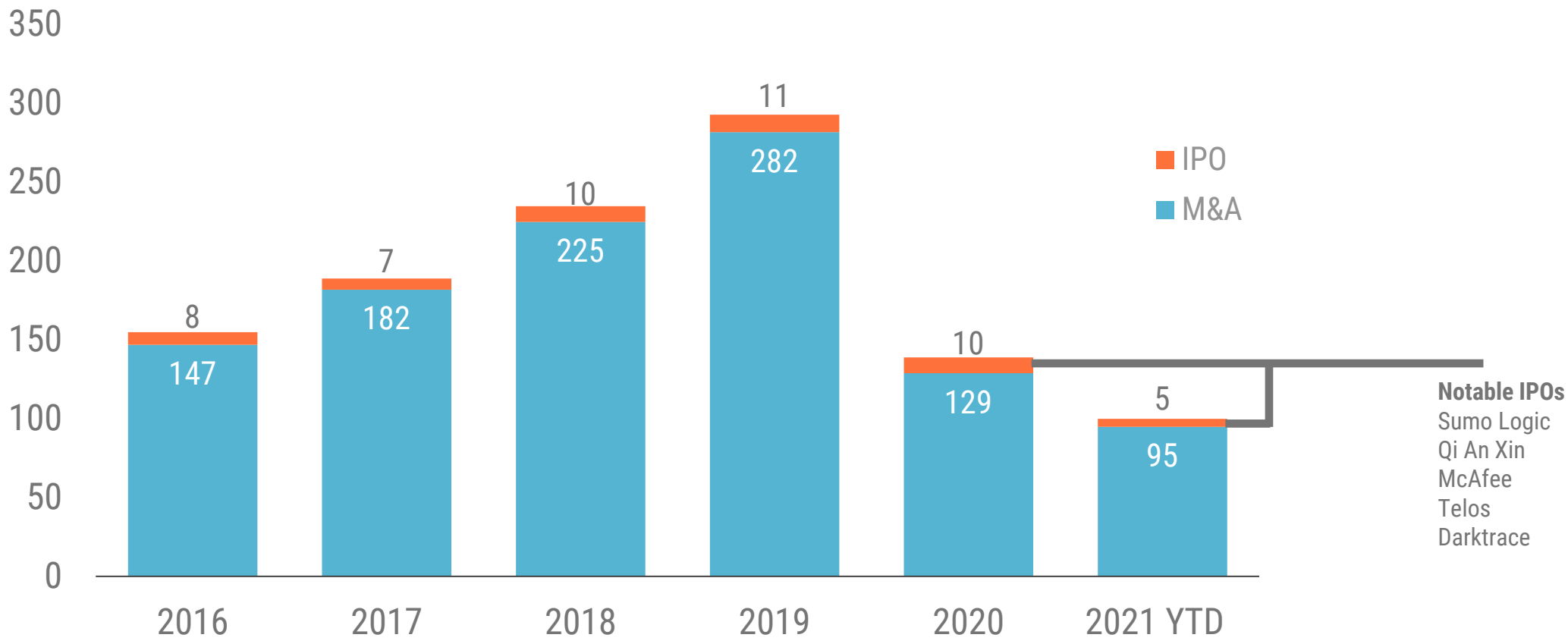
Israel takes a greater role in the cyber space

Cybersecurity global deal share by country, 2020



IPOs and acquisitions fell in 2020

Annual number of cybersecurity exits through M&A or IPO, 2016 – 2021 YTD (06/15/21)



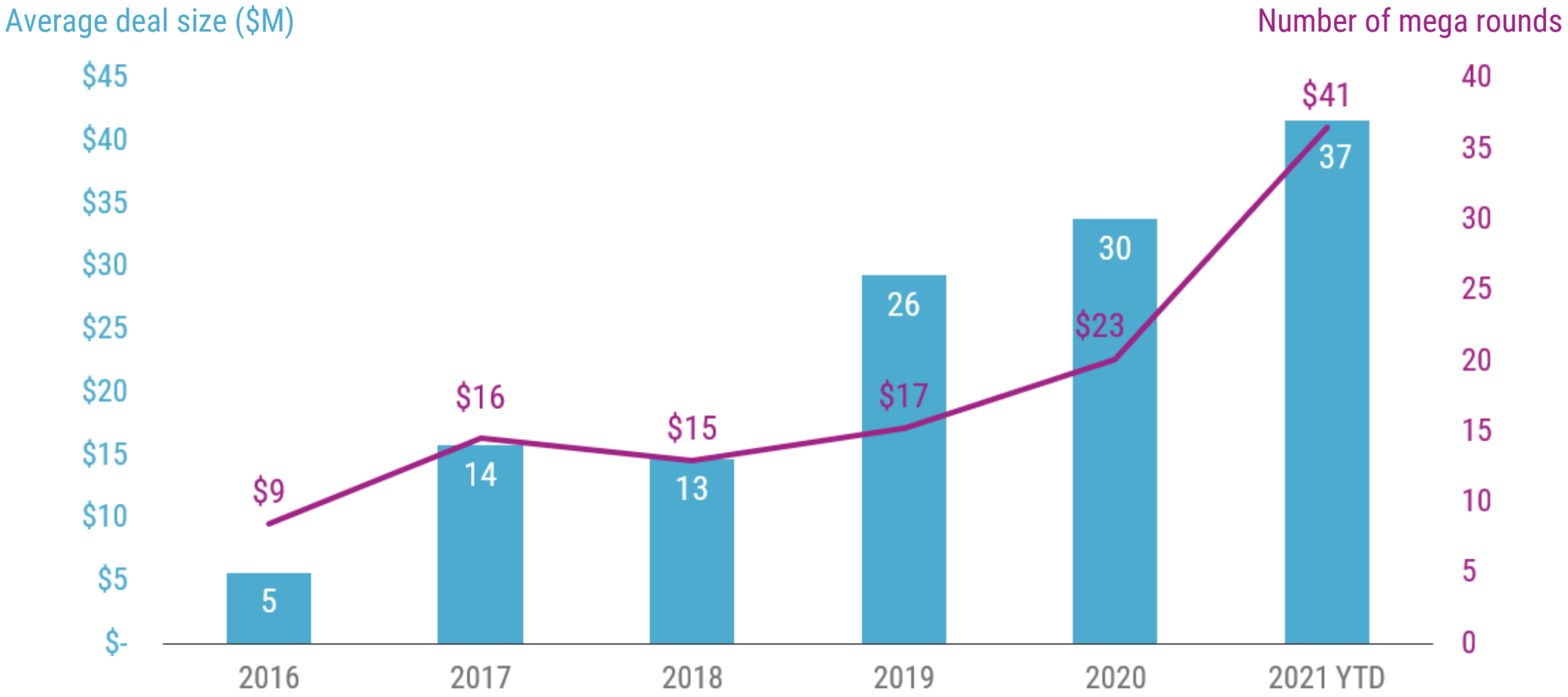
Notable cybersecurity acquisitions

Select cybersecurity acquisitions, 2020 – 2021 YTD (06/15/21)

Date	Acquirer	Company	Amount	What they're saying
Mar 2021	okta	Auth0	$6.5B	*"Together, we will shape the future of identity on the internet, empowering developers to build with identity at the foundation."*
Nov 2020	paloalto NETWORKS	EXPANSE	$800M	*"Integrating Expanse's capabilities into Cortex will enable us to offer the first holistic solution for attack surface management, threat detection, and response."*
Aug 2020	fastly	Signal Sciences	$775M	*"This new solution will integrate with our Compute@Edge platform, accelerating the adoption of edge computing, while simultaneously solving for modern security challenges."*
May 2021	CISCO	KENNA Security	Undisclosed	*"Combined with SecureX, Kenna Security will weave threat management and risk-based vulnerability management together to further extend our lead in providing the broadest XDR capabilities…"*
Jan 2021	Red Hat	StackRox	Undisclosed	*"StackRox helps to simplify DevSecOps, and by integrating this technology into Red Hat OpenShift, we hope to enable users enhance cloud-native application security across every IT footprint."*

Increase in mega-rounds drives up deal size

Average cybersecurity deal size ($M) and number of mega-rounds*, 2016 – 2021 YTD (6/15/21)



CBINSIGHTS *Deals worth $100M+.

PRIVATE MARKET LEADERS

Number of cybersecurity unicorns soars past 30

Private cybersecurity companies valued at $1B+, as of 6/15/2021

2021 Cyber Defenders

CHALLENGES = OPPORTUNITIES

The **next generation of cybersecurity startups** is rising to meet the threats and challenges of today's cybersecurity landscape.

WHAT MAKES A CYBER DEFENDER?

Our selected startups are early- to mid-stage, high-momentum companies pioneering technology with the potential to transform cybersecurity.

Unicorns valued at $1B+, companies that have raised funding past the Series C stage, and companies that have not raised funding since 2019 are excluded.

CYBER DEFENDERS 2021

14 tech categories
shaping the future of cybersecurity

CBINSIGHTS

Identity orchestration
Managing access to multi-cloud environments and enforcing a least-privileged framework

Data firewalls
Classifying, monitoring, and controlling access to an enterprise's most valuable asset: data

Security creds
Meeting compliance standards and completing security audits

Outsourced security
Turning cybersecurity over to the professionals

SaaS security
Securing the sprawling ecosystem of enterprise SaaS apps

Crypto defense
Protecting the integrity of blockchain transactions

Security-infused networks
Adding protections to corporate networks

Cyber automation
Developing cybersecurity processes and automating workflows

API protection
Providing visibility into APIs to thwart malicious activity

Cyber insurance
Measuring cyber risk and providing a financial hedge for cyber costs

Shift left security
Reducing vulnerabilities at the app development stage

Secure data sharing
Protecting the privacy of data shared with third parties or used in analysis

Auto security
Defending connected vehicles from wireless and proximity attacks

Post-quantum cryptography
Offering protections against quantum computer attacks

The 2021 Cyber Defenders

Identity orchestration	Data firewalls	Security creds	Outsourced security	SaaS security	Crypto defense	Security-infused networks
ermetic	Cyral	Vanta	ActZero	AppOmni	valid.network	Twingate
STRATA	OPEN RAVEN	DRATA	confluera	grip	CERTIK	ananda networks

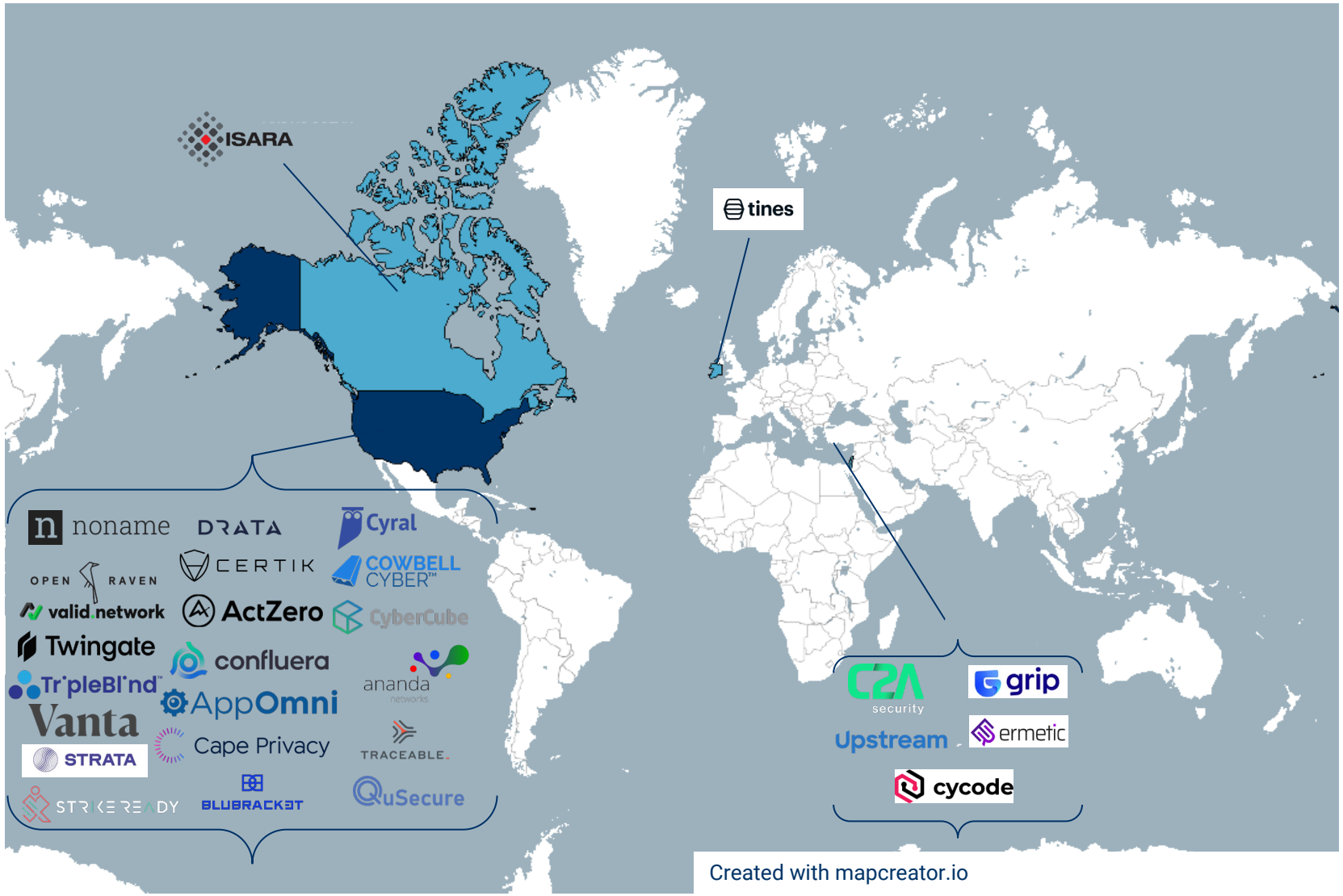
Cyber automation	API protection	Cyber insurance	Shift left security	Secure data sharing	Auto security	Post-quantum cryptography
tines	noname	COWBELL CYBER™	cycode	Cape Privacy	Upstream	ISARA
STRIKE READY	TRACEABLE.	CyberCube	BLUBRACKET	TripleBlind	C2A security	QuSecure

The US has the most 2021 Cyber Defenders

75% of the 2021 Cyber Defenders are headquartered in the US — mostly in California.

The next highest concentration of Cyber Defenders is in Israel, at roughly 20%.

Canada and Ireland each have one Cyber Defender.



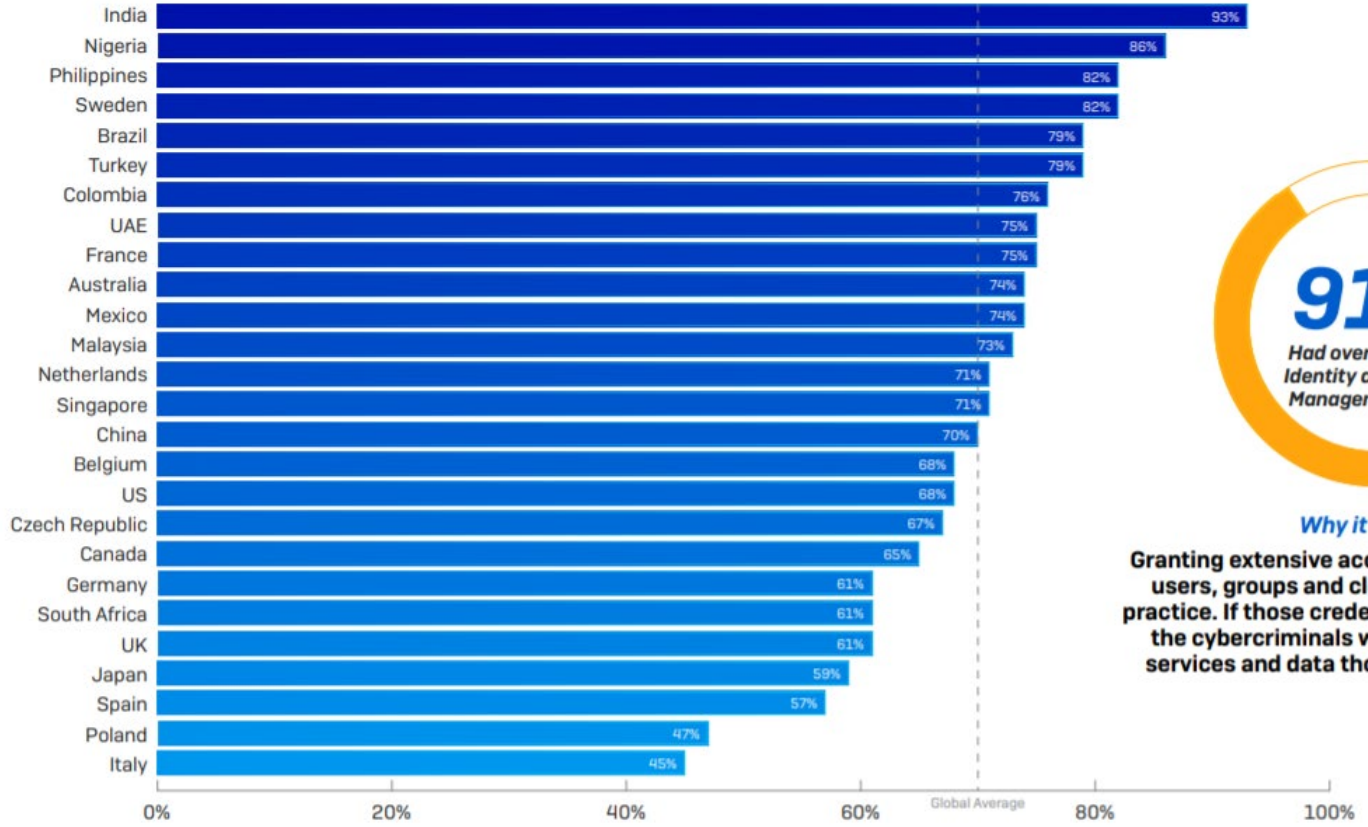
CBINSIGHTS

Identity orchestration

Identity presents a challenge for cloud security

Companies operating across on-premise systems and multiple clouds lack a single, unified solution for managing identity and limiting access to data and systems.

% of organizations suffering a public cloud security incident last year by country



Why it Matters

Granting extensive access permissions to IAM users, groups and cloud services is a risky practice. If those credentials are compromised, the cybercriminals will have access to any services and data those permissions grant.

Why it Matters

All user accounts should have MFA enabled to ensure protection against password compromises. MFA adds an extra layer of protection on top of a username and password.

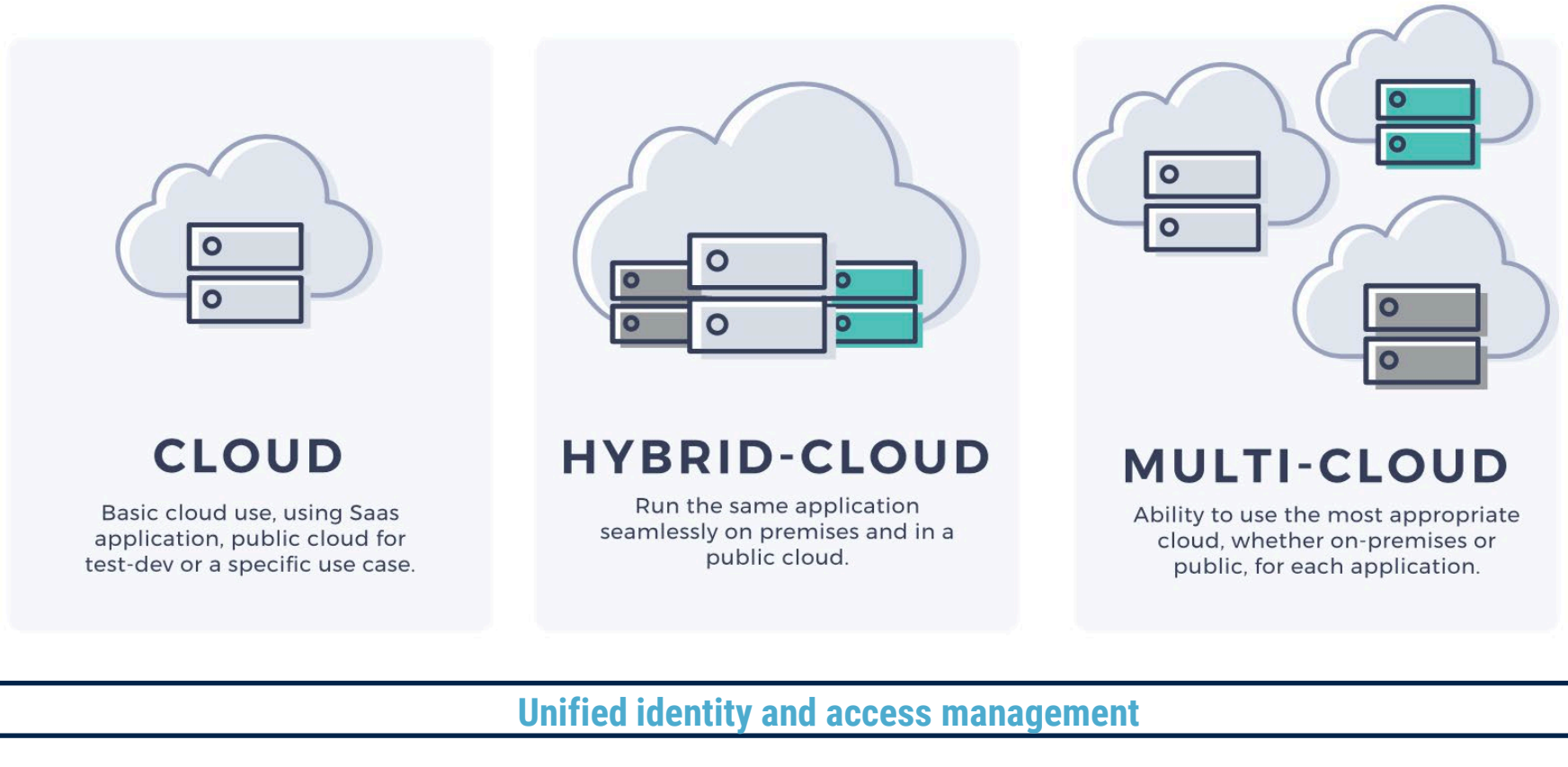
CBINSIGHTS Source: 2020 Sophos State of Cloud Security Report

"It was a Whack-A-Mole game, from a security perspective. Each one of those separate IAM solutions was an opportunity to get the configuration wrong."

- Pat O'Neil, cybersecurity fellow at FedEx, 2020

Unifying identity management across systems

Managing identity and access for each cloud and on-premise application is asking for trouble. Startups are rising to the challenge to unify identity across IT infrastructure.



Source: Xorlogics

Identity orchestration

Ermetic inventories identities and assets across multiple clouds.

Identifying risky permissions and behavior across cloud platforms and applying uniform policies can mitigate the impact of cyber attacks.

The company's co-founder and CEO, Shai Morag, has previously led 2 cybersecurity companies – Secdo and Integrity-Project – to successful exits.

Investors include Accel, Northwest Venture Partners, and Sierra Ventures, among others.

Most recent financing: $17.3M Series A (7/29/2020)

Total disclosed funding: $27.3M

Location: Tel Aviv, Israel

Founded: 2019

Strata provides an abstraction layer to consolidate disparate identity management systems.

By providing a single identity solution for on-premise apps and multi-cloud deployments, Strata helps mitigate security risks.

The company was founded by identity veterans Eric Olden (who founded and exited Securant and Symplified), Topher Marie, and Eric Leach.

Investors include Menlo Ventures, ForgePoint Capital, and New York Life Ventures, among others.

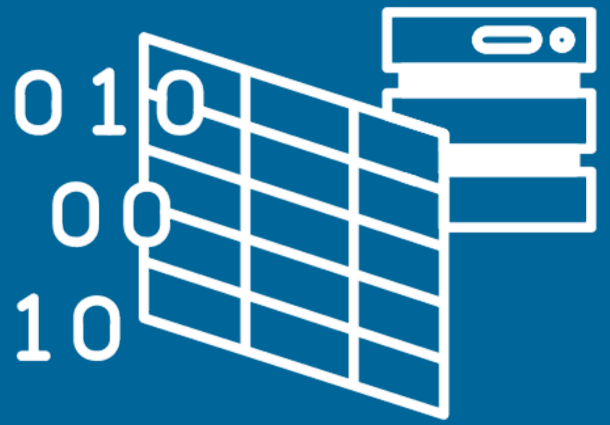
Most recent financing: $11M Series A (2/26/2021)

Total disclosed funding: $14.3M

Location: Boulder, CO

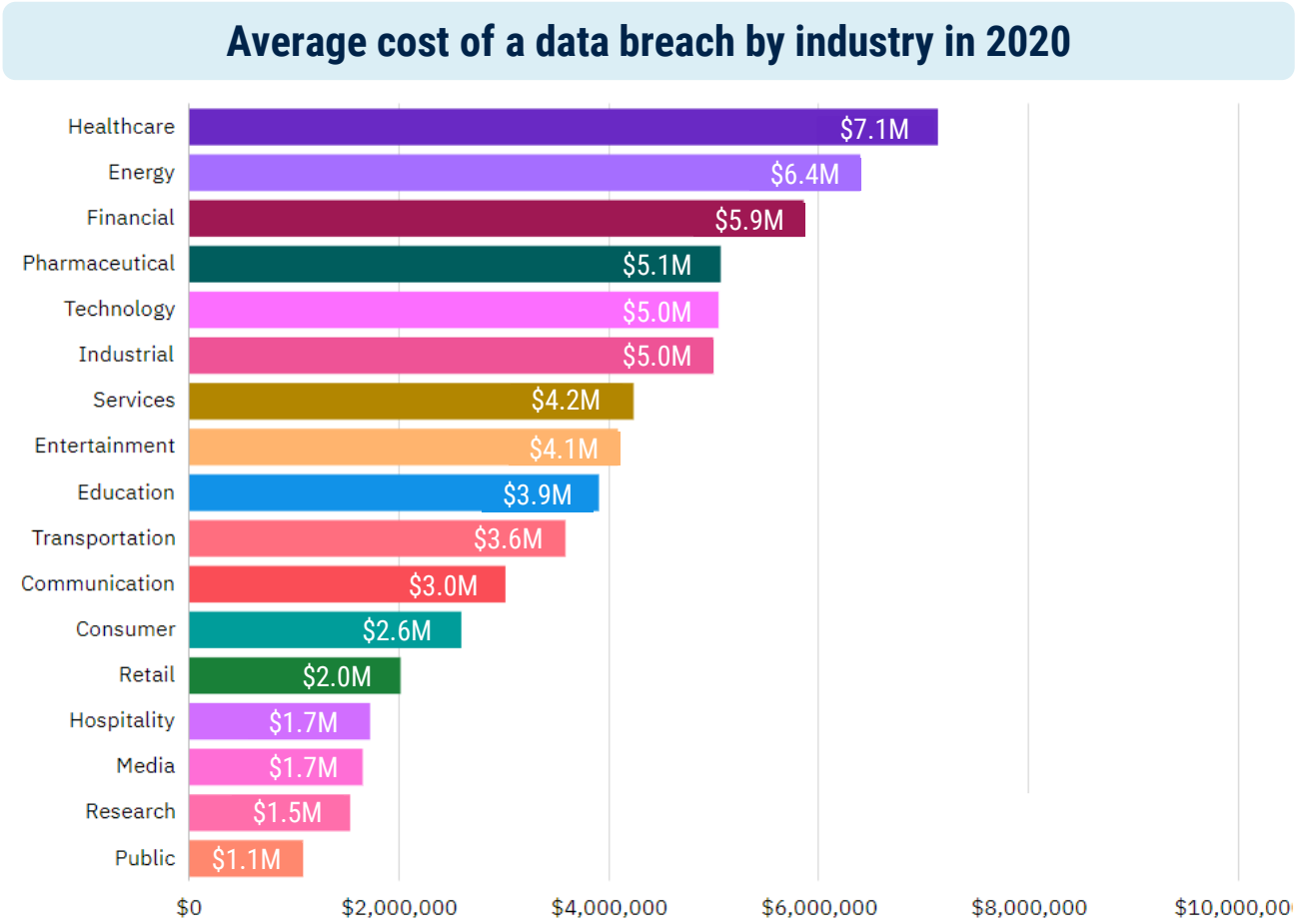
Founded: 2019

Data firewalls



Data breaches come at a cost to all industries

Businesses face financial and reputation costs when their data is stolen by hackers or leaked to the public.



80% of data breaches involve personally identifiable customer information

32% of data breaches involve intellectually property

CBINSIGHTS Source: IBM 2020 Cost of a Data Breach Report

"The cybersecurity apparatus is still geared around a traditional definition of systems — you know, full-stack, storage, compute, processing — all in one device. I think that we don't talk enough about data: data integrity, data security."

- Matt Conner, IC CISO at the Office of the Director of National Intelligence, 2021

Data security as the last defense

Attempts to build defenses around an organization's crown jewel — data — have proven insufficient, so organizations must enact solutions that discover, classify, and add protection measures to the data itself.

Adding protections to enterprise data

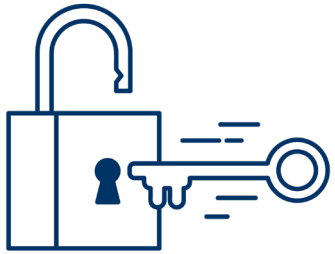
Identify & classify

Locating and classifying data is a necessary first step in adding protections.

Monitor

Monitoring high-value or sensitive data usage for suspicious activity can prevent abuse.

Access



Limiting access to the most sensitive data is essential in a zero-trust security framework.

Data firewalls

Cyral

Cyral allows companies to control access to their data.

The product operates at the data layer to identify malicious activity and manage access by identity.

Cyral integrates with 60+ solutions, from PagerDuty to Looker, and has 20 patents pending for its “single sidecar” (i.e., stateless) technology.

Investors include Redpoint Ventures, Silicon Valley CISO Investments, and Firebolt Ventures, among others.

Most recent financing: $21M Series A (5/13/2021)

Total disclosed funding: $41.1M

Location: Redwood City, CA

Founded: 2018

OPEN RAVEN

Open Raven maps a company’s data to ensure its protection.

Classifying and mapping data enables companies to monitor data use and apply appropriate safeguards (e.g., encryption, access controls).

Open Raven’s leadership team includes the former chief product officer at CrowdStrike, Dave Cole, and SourceClear founder Mark Curphey.

Investors include Kleiner Perkins Caufield & Byers, Upfront Ventures, and Signal Sciences, among others.

Most recent financing: $15M Series A (6/16/2021)

Total disclosed funding: $19.1M

Location: Los Angeles, CA

Founded: 2019

Security creds

Proof of security is required for business

Past breaches have highlighted that a company is only as strong as its weakest partner. Adjusting to this new threat landscape, companies are seeking to differentiate themselves from the competition and win business by exhibiting their security credentials.

VW says data breach at vendor impacted 3.3 million people in North America

June 2021 | REUTERS®

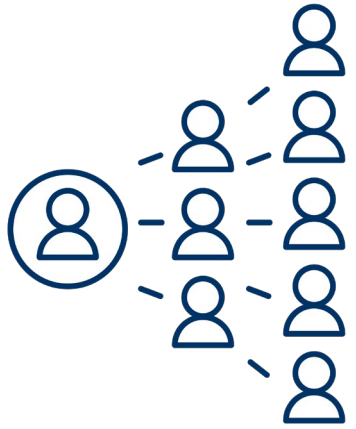
Hack of Federal Agencies Shows Cyber Dangers to Supply Chains

December 2020 | THE WALL STREET JOURNAL.

Supply Chain Hit Spurs Companies to Rethink Vendor Relationships

February 2021 | Bloomberg

51% of data breaches within the past 12 months were caused by a third party



CBINSIGHTS Source: Infosecurity-magazine

"…areas like e-commerce or financial services…are dependent on having qualifications like SOC 2 or PCI or security offerings such as web application firewall. As we add more and enhance our solutions, we're able to win those [opportunities] faster and ultimately ramp those faster."

- Adriel Lares, CFO at Fastly, 2019

Security credentials become a bigger business

To verify their cybersecurity posture and win business, companies are undergoing audits to receive security certifications (e.g., SOC 2, ISO 27001). New vendors have entered the space, seeking to streamline an often tedious credentialing process and provide continuous monitoring.

Components of an SOC 2 audit

Source: Imperva

Security creds

Vanta

Vanta helps companies achieve SOC 2, HIPAA, or ISO 27001 compliance.

By offering a continuous monitoring solution that connects to corporate infrastructure and tools, Vanta helps companies meet compliance standards and pass audits.

The company has supported more than 1,000 customers with SOC 2 prep and surpassed $10M in annual recurring revenue.

Investors include Sequoia Capital and Y Combinator.

Most recent financing: $50M Series A (5/4/2021)

Total disclosed funding: $53M

Location: San Francisco, CA

Founded: 2017

DRATA

Drata provides security monitoring to ensure continuous SOC 2 & ISO 27001 compliance.

The product integrates with numerous IT systems to implement security controls and monitor compliance.

Since coming out of stealth in early 2021, Drata has passed the 100-customer mark. Its founders previously led the startup Portfolium to a successful exit.

Investors include Cowboy Ventures, Okta Ventures, and Silicon Valley CISO Investments, among others.

Most recent financing: $25M Series A (6/23/2021)

Total disclosed funding: $28.2M

Location: San Diego, CA

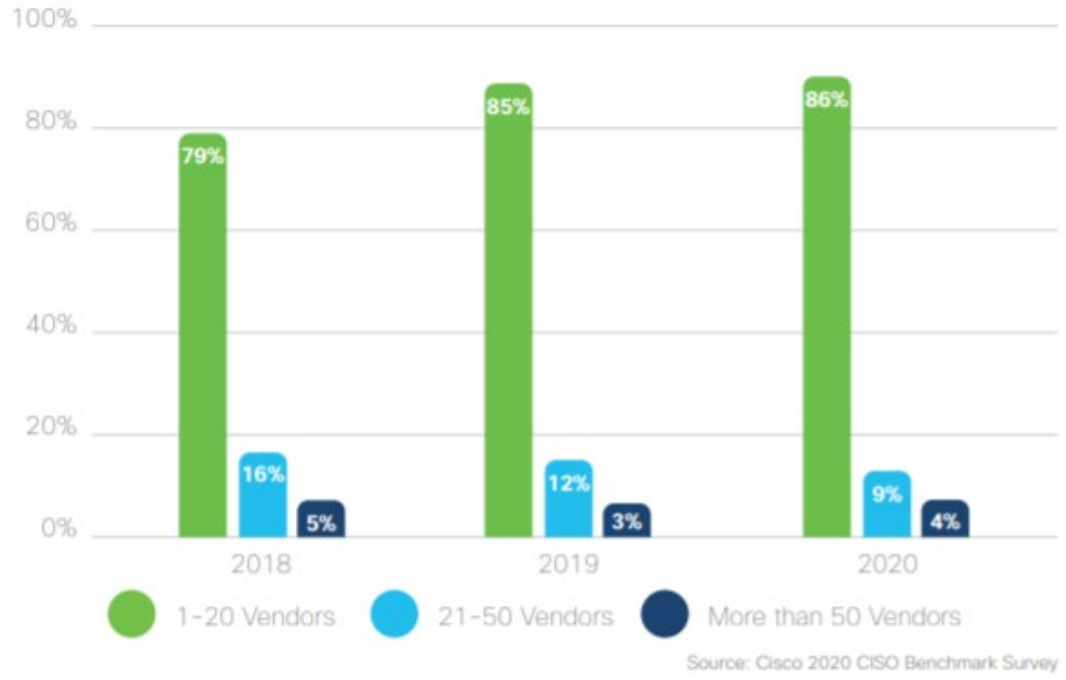
Founded: 2020

Outsourced security

A DIY approach to cybersecurity is challenging

Managing multiple vendors, staying up to date on the latest technology and threats, and hiring qualified talent can strain corporate security teams.

Number of cybersecurity vendors used



Number of daily security alerts

Source: Cisco 2020 Benchmark Survey

"Building out a security operations center would have required 12-15 additional full-time staff members but with [a managed security solution] we can accomplish an equivalent or better coverage for far less expense."

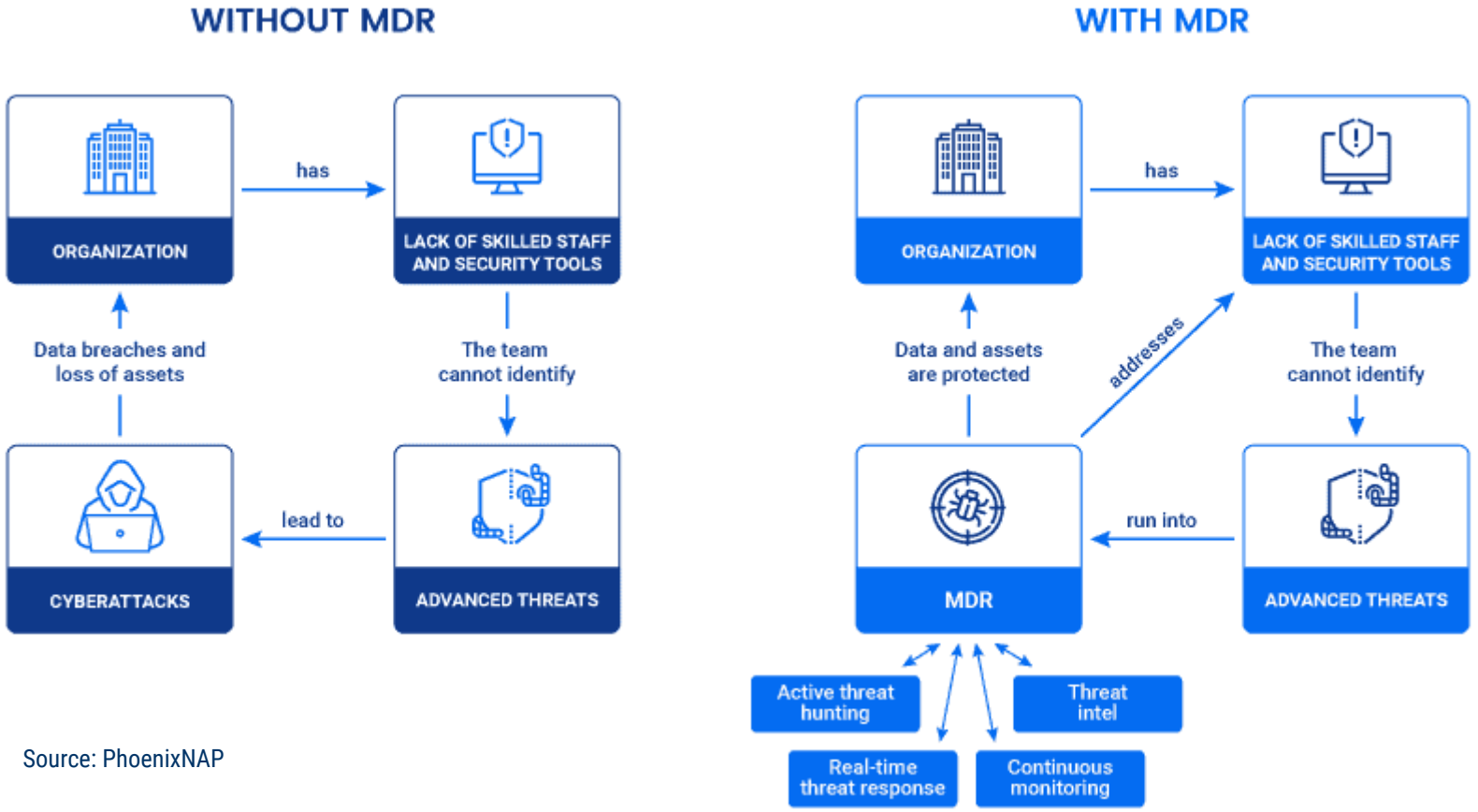
- Matthew Snyder, chief information security officer (CISO) at Penn State Health, Hershey Medical Center, 2020

PennState Health
Milton S. Hershey
Medical Center

Managed security provides relief and protection

Managed detection and response providers often leverage artificial intelligence to help companies identify and respond to threats. Their view across customers can provide a greater understanding of the threat landscape.

A comparison: managed detection and response (MDR) vs. internal security team only



Source: PhoenixNAP

Outsourced security

ActZero

ActZero offers a managed detection and response (MDR) solution for small- and medium-sized businesses (SMBs).

To train its artificial intelligence cyber threat models, ActZero acquired MDR company IntelliGo Networks in January 2020.

The company's founders include Sameer Bhalotra, who co-founded cybersecurity company StackRox and served as senior director for cybersecurity on the US National Security Council.

Investors include Point72 Ventures.

Most recent financing: $40M seed (3/9/2021)

Total disclosed funding: $40M

Location: Seattle, WA

Founded: 2019

confluera

Confluera provides a managed detection and response (MDR) solution for workloads running in the cloud and on premise.

The company uses machine learning techniques to identify attacks in real time and has accrued 6 patents of its technology since 2019.

Its founders have extensive cybersecurity experience, with co-founder and chairman Bipul Sinha having founded data protection and storage company Rubrik.

Investors include Lightspeed Venture Partners and Icon Ventures, among others.

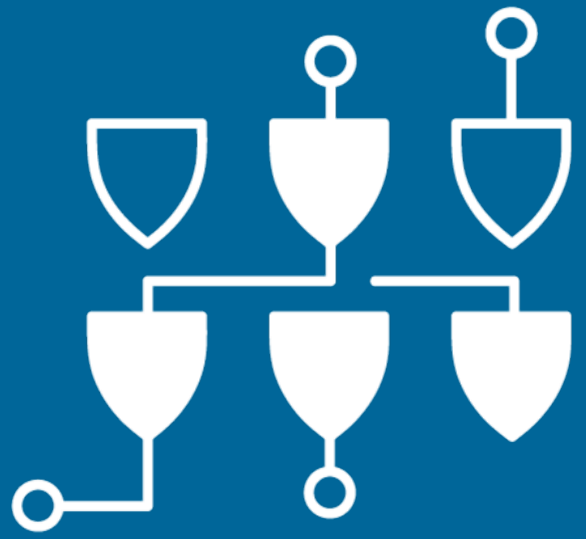
Most recent financing: $20M Series B (5/19/2020)

Total disclosed funding: $29M

Location: Palo Alto, CA

Founded: 2019

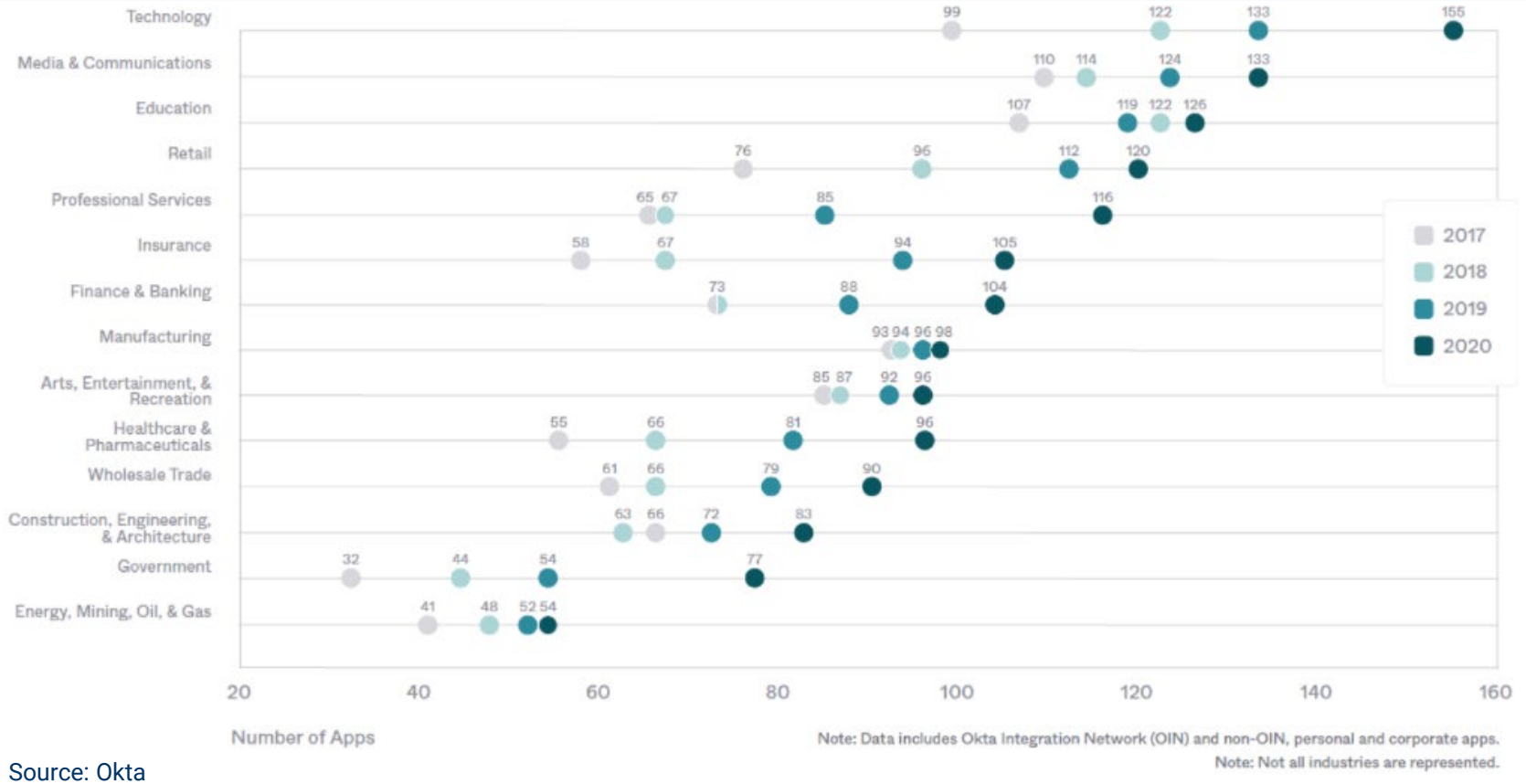
SaaS security



Corporations are relying on SaaS apps

Companies across industries have increased their use of SaaS applications — or third-party software running in the cloud — in recent years. Managing and monitoring a sprawling network of applications provides a unique set of challenges.

Average number of SaaS apps used by industry and year



Note: Data includes Okta Integration Network (OIN) and non-OIN, personal and corporate apps.
Note: Not all industries are represented.

Source: Okta

"Many companies are not even aware of the kind of sensitive data that is being inadvertently stored in SaaS solutions, or who has access to it."

- Robert Walden, CIO at Epsilon, 2020

SaaS customers have a security obligation

Organizations must establish a plan for managing and securing their burgeoning app ecosystems, specifically for the users accessing them. Emerging cybersecurity providers are tackling this challenge by mapping a company's SaaS apps and implementing security measures.

SaaS security responsibilities		SaaS security protections
SaaS customer	User access	 Visibility into SaaS application ecosystem
	User identity	
	Data/application integration	 Management of SaaS application permissions
SaaS provider	Application	
	Operating system	
	Virtualization	
	Network	 Monitoring SaaS application activity
	Infrastructure	
	Physical	

CBINSIGHTS Source: Forbes

SaaS security

AppOmni provides tools for managing and securing a company's SaaS application ecosystem.

The company's solution monitors SaaS applications for suspicious activity and helps manage permissions to limit access to data and app functions.

Since its founding, AppOmni has maintained a 100% customer renewal rate. The company has grown its revenue 900% in the past year.

Investors include Scale Venture Partners, ClearSky, and Salesforce Ventures, among others.

Most recent financing: $40M Series B (4/21/2021)

Total disclosed funding: $53M

Location: San Francisco, CA

Founded: 2018

Grip helps companies understand and protect their SaaS applications.

By mapping SaaS applications and monitoring their usage, Grip helps companies identify abuse and set permissions that reduce risk.

Grip counts several cybersecurity heavyweights among its early backers, including CrowdStrike's CEO and co-founder George Kurtz and Zscaler's former CISO Michael Sutton.

Investors include YL Ventures, among others.

Most recent financing: $6M seed (4/20/2021)

Total disclosed funding: $6M

Location: Tel Aviv, Israel

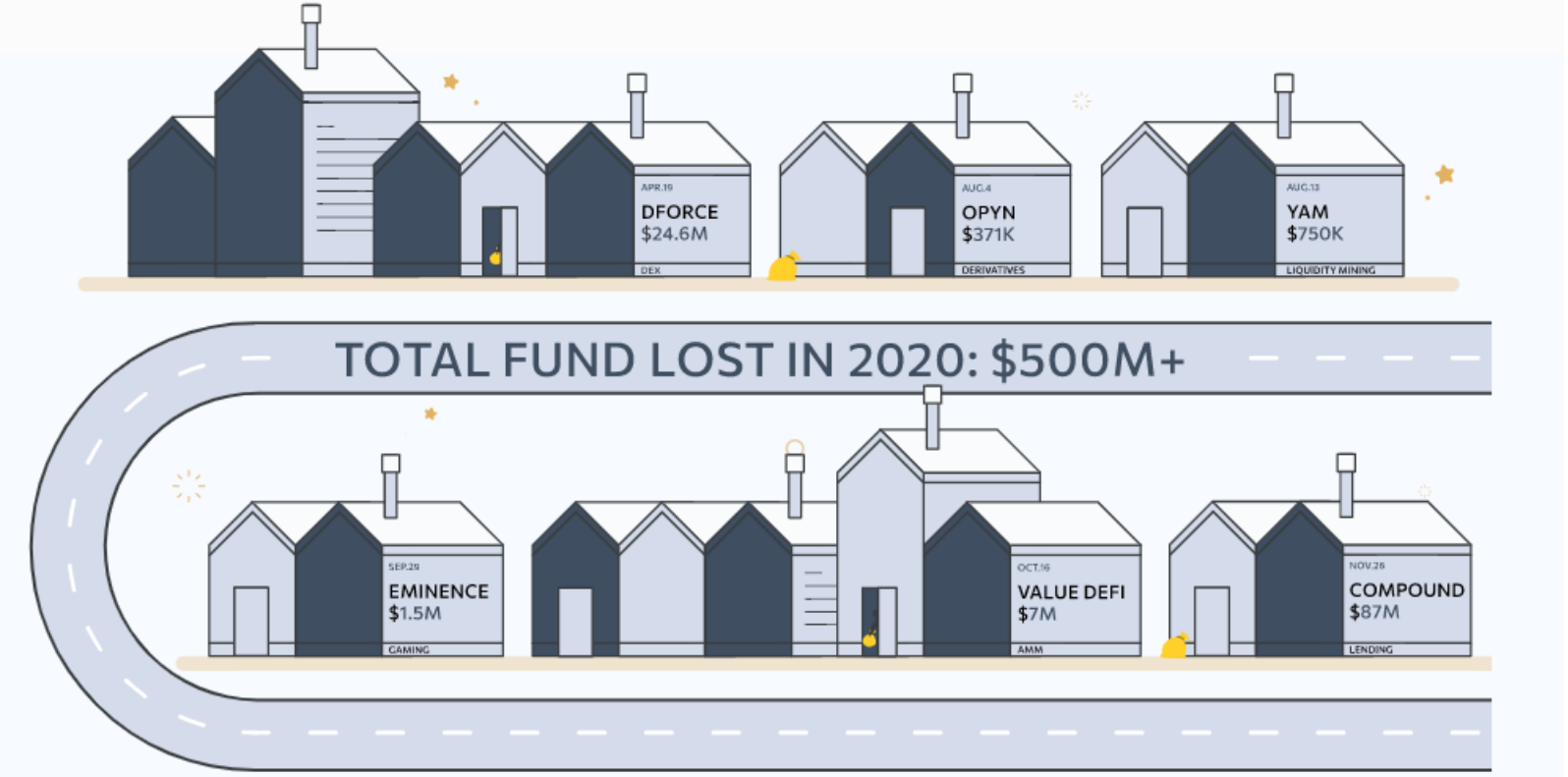
Founded: 2021

Crypto defense

Blockchain is not inherently secure

While blockchain has properties that support security and privacy (i.e., an immutable ledger), it is not immune to cybersecurity attacks. In fact, more than $500M was lost or stolen from decentralized finance (DeFi) projects in 2020.

Money lost or stolen from DeFi projects in 2020



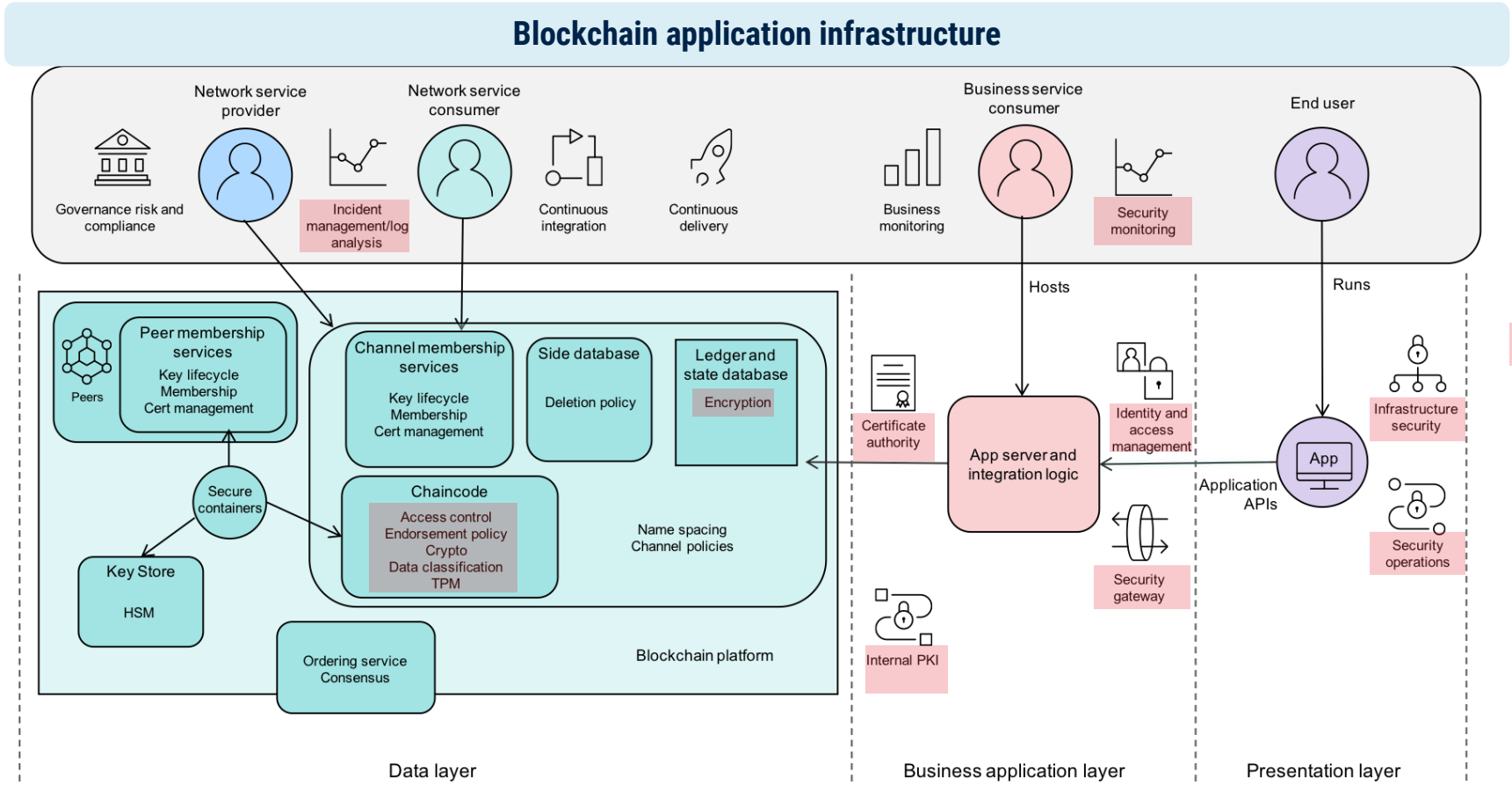
Source: Certik

"At the end of the day, the software is only as good as the coding that was done, and sometimes, there are unknown errors in the code that governs these protocols."

- Meltem Demirors, chief strategy officer at CoinShares, 2021

Adding security to the blockchain

Startups are emerging to identify vulnerabilities and prevent abuse as the code underlying blockchain applications and infrastructure becomes more complex.



Cybersecurity function embedded in blockchain application

Source: IBM

Crypto defense

valid.network

Valid Network provides visibility into decentralized applications.

The company offers tools to highlight vulnerabilities in decentralized app code and monitor and control transactions in real time.

Valid Network was founded by cybersecurity veterans and is a member of the Ethereum Enterprise Alliance and the Hyperledger Alliance.

Investors include Ten Eleven Ventures and Jerusalem Venture Partners.

Most recent financing: $8M seed (7/14/2020)

Total disclosed funding: $10M

Location: San Francisco, CA

Founded: 2018

CERTIK

Certik audits smart contracts and blockchains to identify risks.

Since its inception, the company has conducted more than 220 audits — including for crypto exchanges Huobi, OKEx, and Binance — and secured $10B+ in digital assets.

Certik uses a formal verification method developed by researchers at Yale University to mathematically prove “program correctness and hacker resistance.”

Investors include IDG Capital, Spark Digital Capital, and AU21, among others.

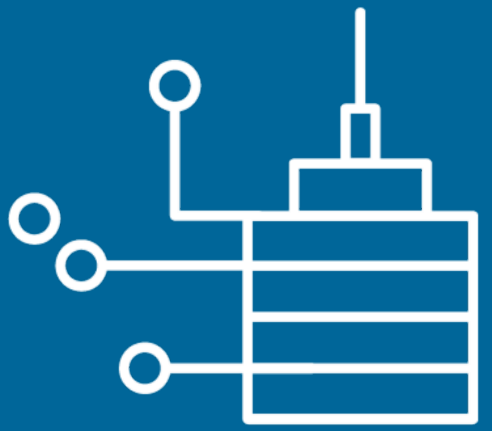
Most recent financing: $7.6M Series A (6/18/2020)

Total disclosed funding: $7.9M

Location: New York, NY

Founded: 2018

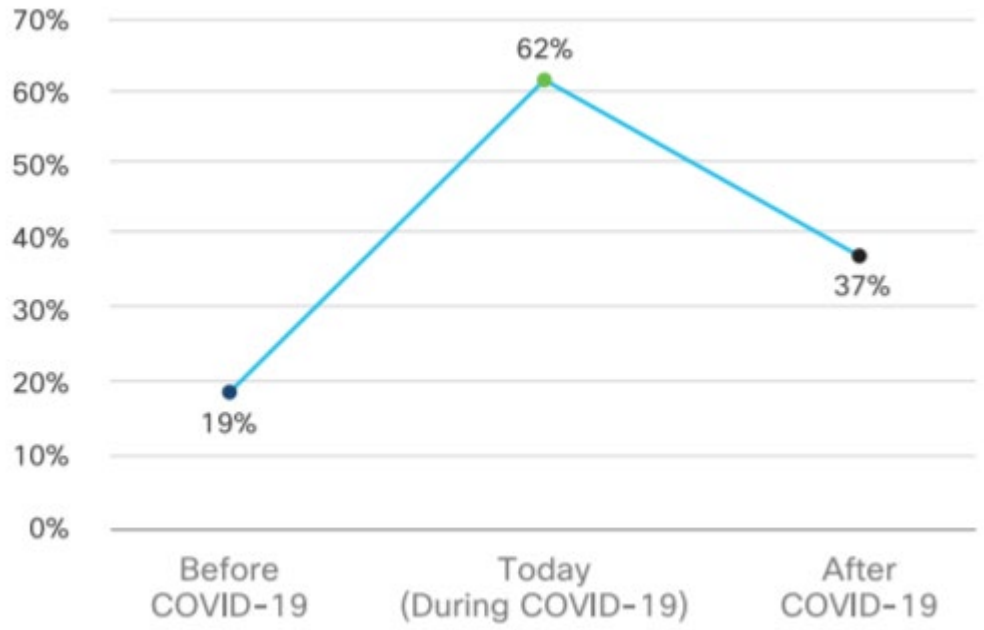
Security-infused networks



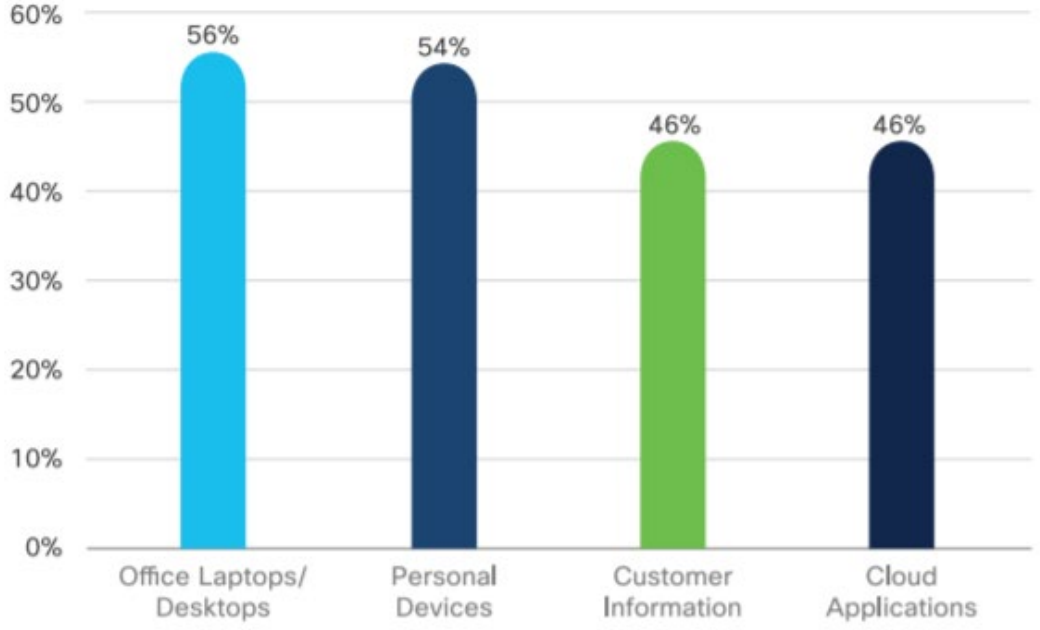
Companies must secure a distributed workforce

Companies depend on reliable networks to enable an effective remote workforce. Historically, these networks have been protected with numerous point solutions (e.g., VPNs, firewalls, cloud access security brokers), which can frustrate IT teams and employees.

% of organizations with more than half of workforce remote



% reporting as a challenge to protect in remote environments



CBINSIGHTS Source: Cisco

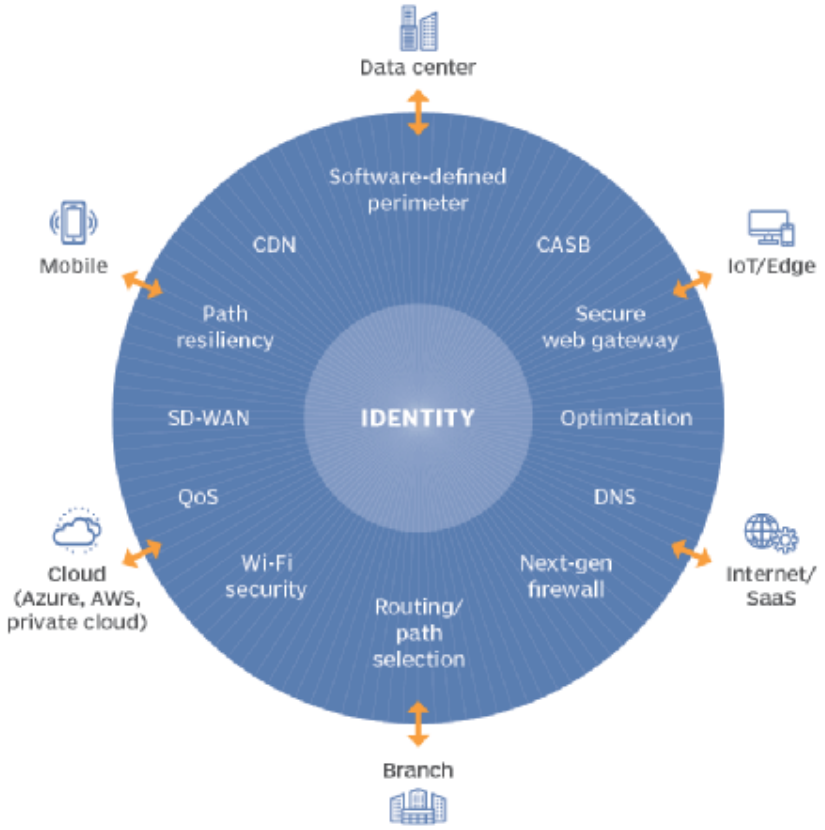
“Any time you disperse the workforce, you’re going to get increased risk.”

- Michael Daniel, president and CEO of the Cyber Threat Alliance, 2020

A modern approach to network security

Startups and tech incumbents are building cybersecurity into software-defined networking solutions (e.g., SD-WAN). The unified security model, which is delivered as a service, reduces complexity and helps companies keep their cybersecurity protocols up to date.

Secure Access Service Edge (SASE) architecture



CBINSIGHTS Source: TechTarget

Security-infused networks

Twingate

Twingate provides users with secure access to corporate applications.

The company secures networks by offering built-in access controls and keeping them invisible to the internet.

Twingate was founded by veterans of Dropbox and has filed 2 patents for its technology.

Investors include SignalFire, 8VC, and Green Bay Ventures.

Most recent financing: $17M Series A (10/29/2020)

Total disclosed funding: $17M

Location: Redwood City, CA

Founded: 2019

ananda networks

Ananda Networks offers a cloud-managed, secure global local area network (LAN).

The company allows companies to create their own private networks with security features like encryption, micro-segmentation, and granular access controls.

Ananda Networks was founded by 2 serial entrepreneurs – Adi Ruppin and Elad Rave – who have founded a combined total of 6 companies.

Investors include Citrix Systems, GreatPoint Ventures, and J Ventures.

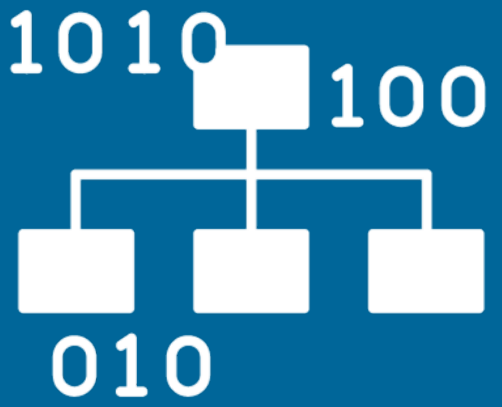
Most recent financing: $6M seed (8/19/2020)

Total disclosed funding: $6M

Location: Los Altos, CA

Founded: 2019

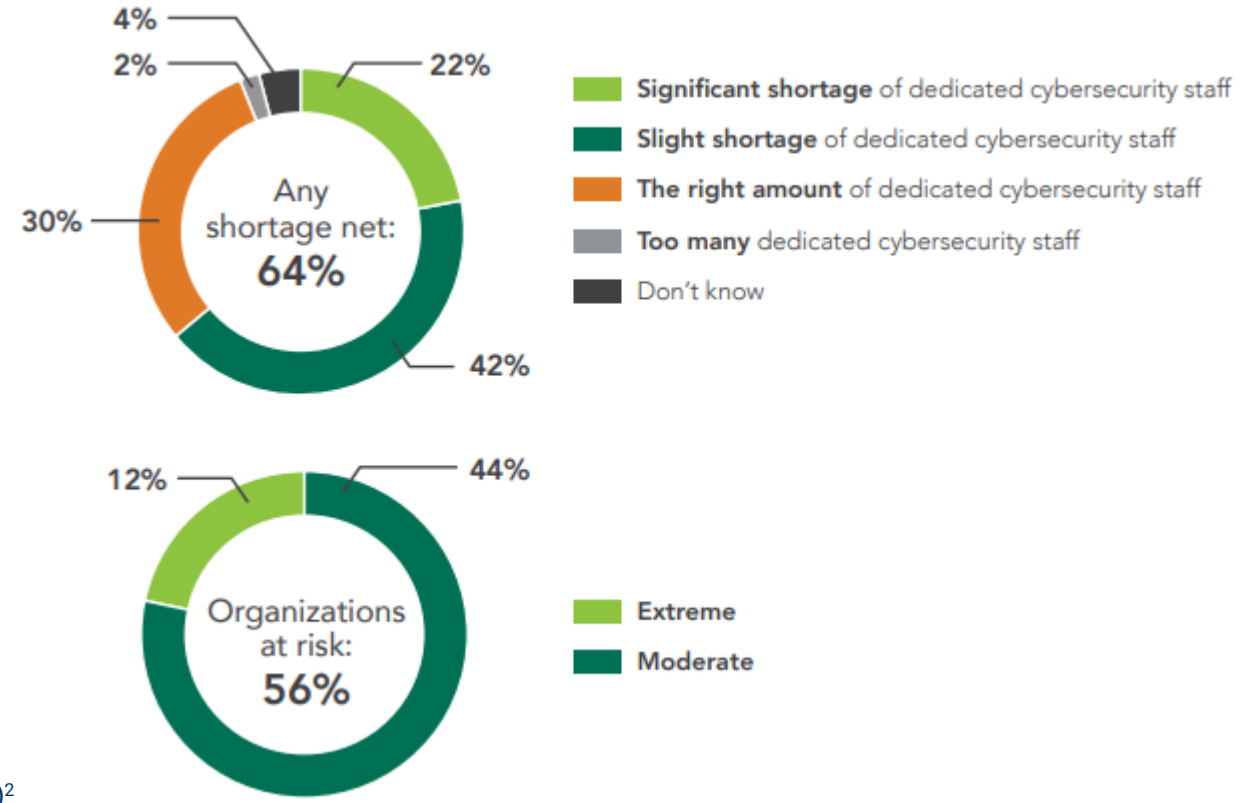
Cyber automation



Cybersecurity has an efficiency problem

Cyber attacks, alerts, and vulnerabilities continue to rise while the supply of qualified cybersecurity professionals remains constrained. This imbalance challenges companies seeking to protect their systems and data.

Cybersecurity professionals with staff shortages cite associated security risks



CBINSIGHTS Source: (ISC)²

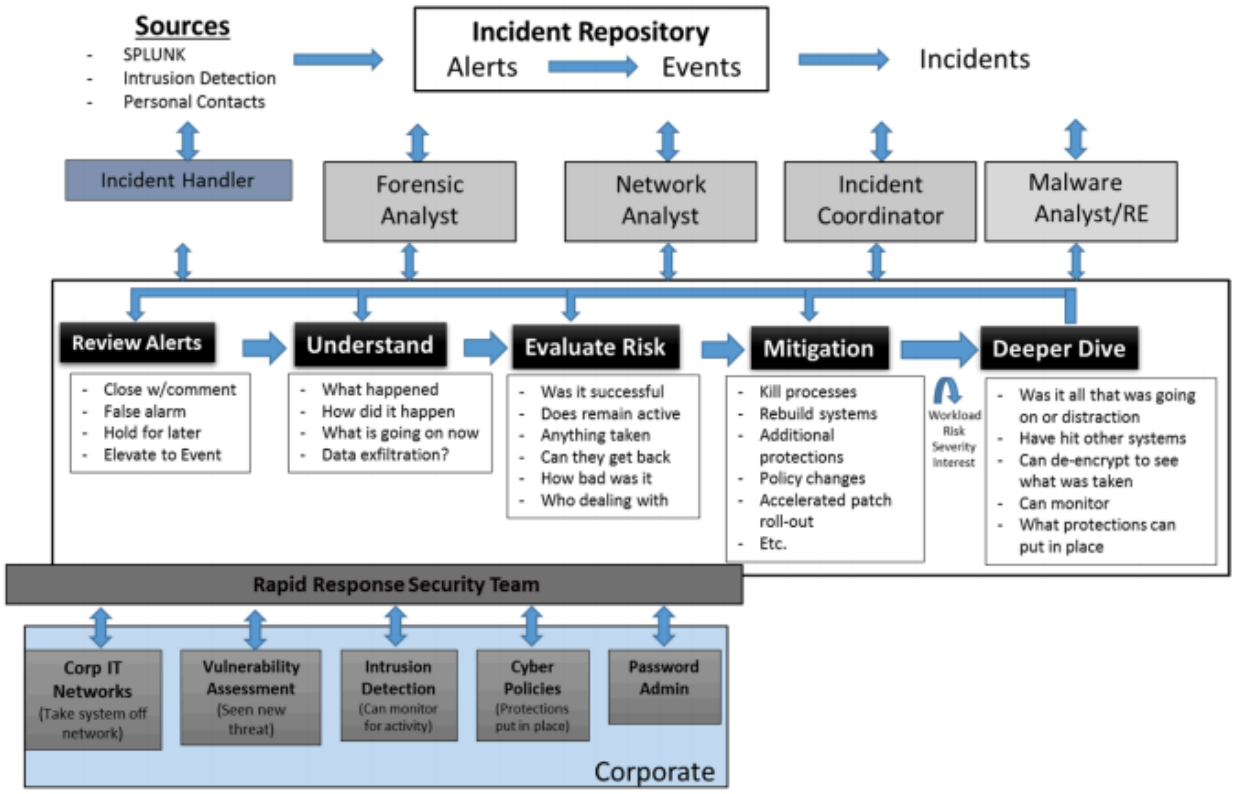
"We have a lot of repetitive tasks — we can build the right framework so those controls happen automatically to a point where we need a human looking at it. So, I can repurpose my smart people who I want making the decisions that I'm not comfortable AI making. If I can get that designed well enough to pull some workload off of them, we'll start moving the needle faster."

- Ken Foster, head of global cyber risk governance at Fiserv, 2020

Automation empowers the cyber workforce

Companies taking advantage of a defined cybersecurity workflow and threat data have automated cyber processes and integrated with supportive systems like Slack, Atlassian, and SIEM (security information and event management) solutions.

Cybersecurity incident response workflow



Source: Sandia National Laboratories

Cyber automation

tines

Tines offers a no-code platform for automating cybersecurity workflows.

Integrating with numerous enterprise tech tools (e.g., Okta, Slack), Tines can automate tasks such as phishing response, security ticket enrichment, and alert ingestion.

The company was founded by 2 former DocuSign security professionals and counts Sophos, Box, and OpenTable among its early customers.

Investors include Accel and Addition, among others.

Most recent financing: $26M Series B (4/08/2021)

Total disclosed funding: $41.1M

Location: Dublin, Ireland

Founded: 2018

STRIKE READY

Strike Ready develops a digital cyber awareness and response analyst to analyze and resolve security incidents.

Strike Ready can help security teams be more efficient and effective by autonomously prioritizing alerts, performing vulnerability testing, and responding to attacks.

The company's founders and much of the team come from threat intelligence cybersecurity company FireEye. Strike Ready counts Aflac and some US government agencies as early adopters.

Investors include Outlier Ventures and 11.2 Capital, among others.

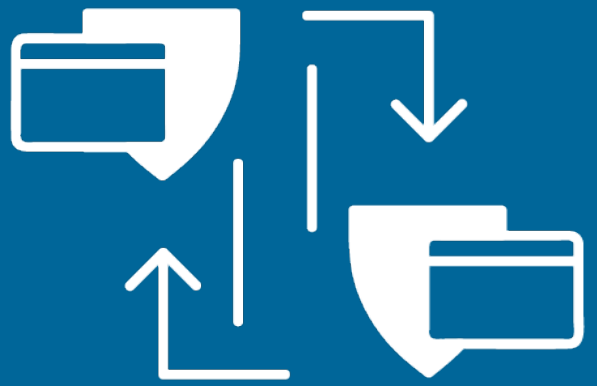
Most recent disclosed financing: $3.6M seed (4/28/2021)

Total disclosed funding: $3.6M

Location: Fremont, CA

Founded: 2019

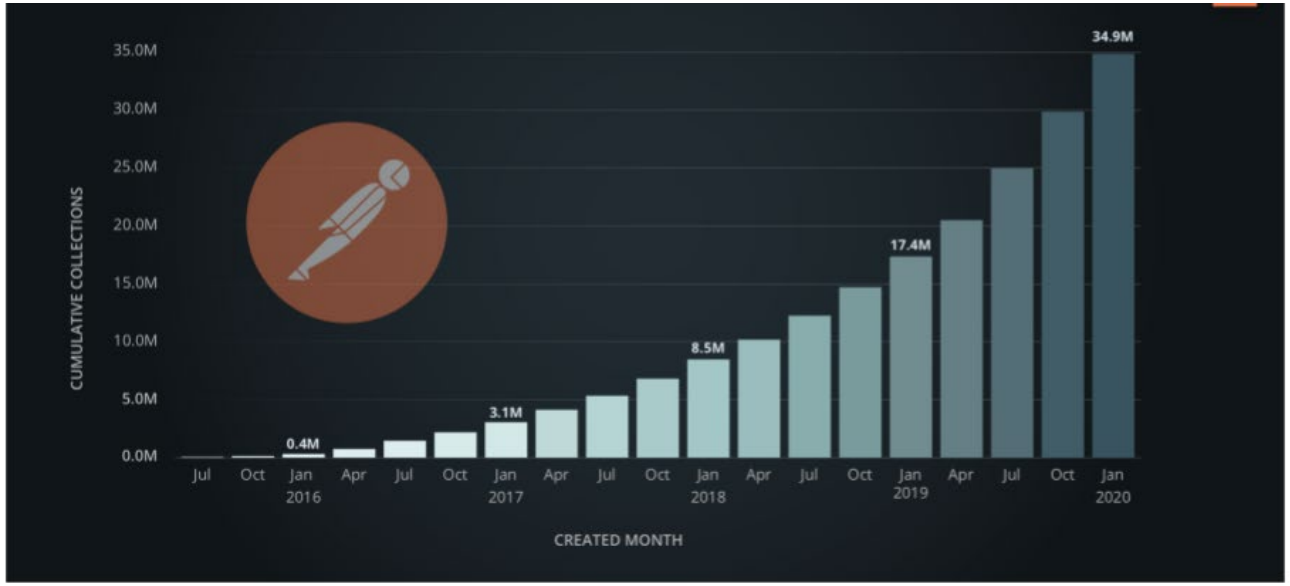
API protection



Security risks accompany the rise in API use

Application programming interface (API) usage has skyrocketed across all industries over the past few years. This brings security risks that require new protections.

Growth in Postman API collections



API security risks

- **Data injection**
- **Flawed authentication process**
- **Excessive data exposure**
- **Lack of usage limits**

CBINSIGHTS Source: Postman

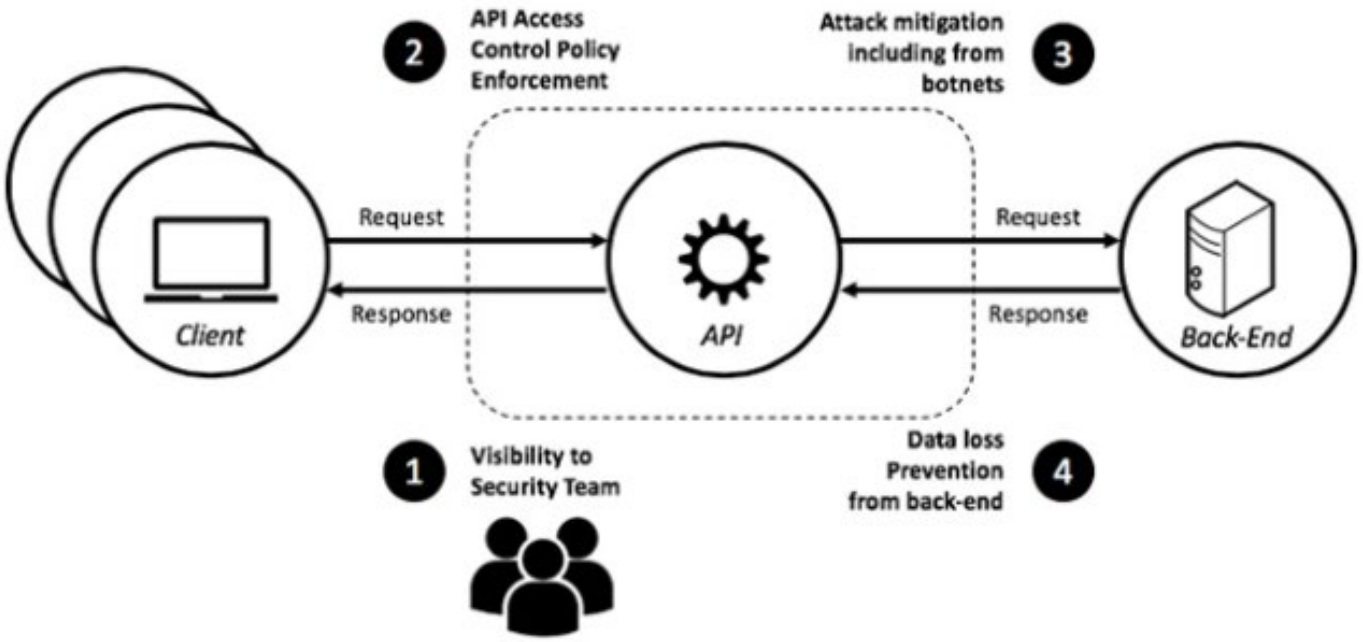
"These same CISOs are saying, APIs are mission-critical to the company. All of our most sensitive data, apps and services are connected to them. We understand that we have to protect them."

- Andre Durand, founder & CEO of Ping Identity, 2020

API-specific security solutions emerge

Startups are developing solutions for securely developing APIs, including testing for vulnerabilities and ensuring proper configuration. Others are monitoring and responding to API abuse, such as code injection and unauthorized access.

API security methods



CBINSIGHTS Source: Help Net Security

API security

noname

Noname offers a suite of API security tools.

The API security platform can locate a company's APIs, identify suspicious activity, and block attacks in real time. It also can test the integrity of APIs prior to production.

Noname emerged from stealth in December 2020 with $25M in funding. Its 2 co-founders got their start in the Israeli Intelligence Corps, Unit 8200.

Investors include Insight Partners, Lightspeed Venture Partners, and next47, among others.

Most recent financing: $60M Series B (6/30/2021)

Total disclosed funding: $85M

Location: Palo Alto, CA

Founded: 2020

TRACEABLE

Traceable discovers, secures, and monitors APIs.

Its product protects against known threats (e.g., SQL injection, Cross-Site Scripting) while also providing visibility into API activity to identify, investigate, and resolve threats.

The company was co-founded by Jyoti Bansal, who previously founded and led the application performance company AppDynamics, which was sold to Cisco for $3.7B.

Investors include Silicon Valley CISO Investments and Unusual Ventures, among others.

Most recent disclosed financing: $250K angel (2/11/2021)

Total disclosed funding: $20.3M

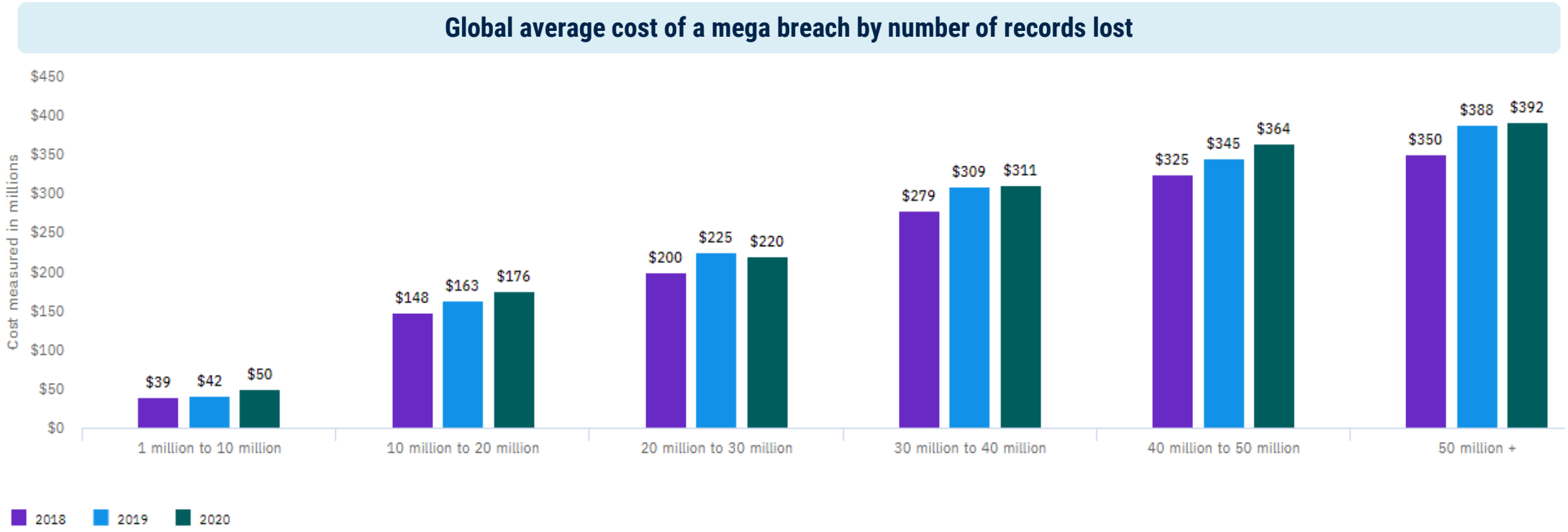
Location: San Francisco, CA

Founded: 2018

Cyber insurance

Cyber attacks inflict a high financial toll

Data breaches of all sizes have become more costly over the past 3 years. For example, a breach of more than 10M records is now expected to cost a company $100M+.



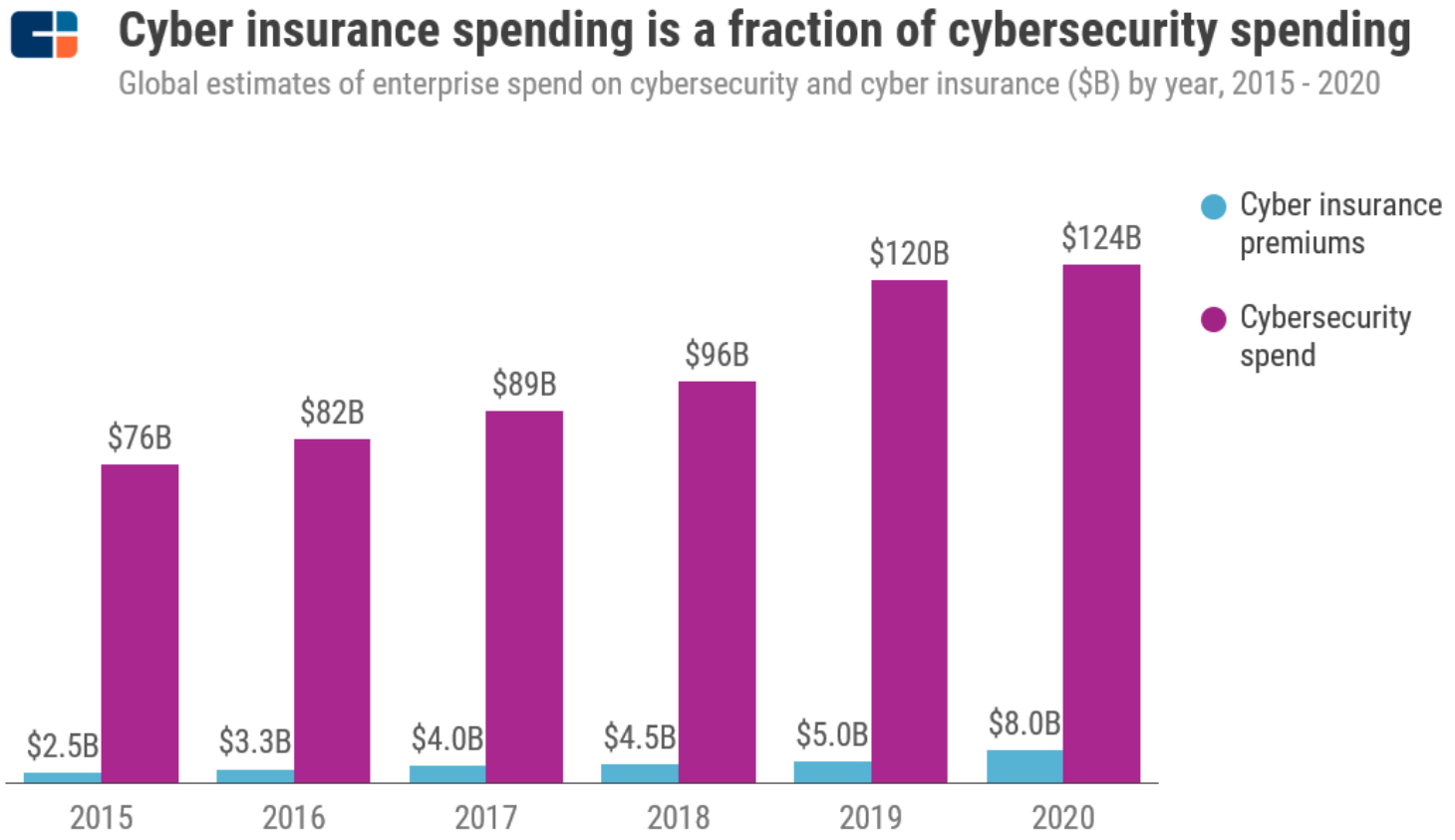
Source: IBM 2020 Cost of a Data Breach Report

"Thirty years of history have shown us that cyber risk is difficult to understand, problematic to hedge, only likely to grow, and characterized by a continually changing threat environment."

- Tom Johansmeyer, head of PCS, 2021

Cyber insurance provides some relief

Startups offering risk analysis tools to enterprises and insurance providers seek to address the main challenges hindering the market's growth: a lack of historical data to inform risk models and the potential for substantial losses.



Source: Munich Re, Gartner

Cyber insurance

Cowbell Cyber leverages data science and cybersecurity monitoring to offer cyber insurance.

The company looks at factors such as cybersecurity posture and dark web intelligence to inform insurance coverage. It also offers services like cyber awareness training to reduce a company's cyber risk.

Cowbell Cyber's founding team comes from senior roles in insurance (Markel) and cybersecurity (ZIMPERIUM, Lacework).

Investors include Markel, Avanta Ventures, and Pivot Investment Partners.

Most recent financing: $20.3M Series A (3/01/2021)

Total disclosed funding: $24M

Location: Pleasanton, CA

Founded: 2019

CyberCube provides insurance companies with cybersecurity analytics and data to inform coverage risk.

By compiling cybersecurity datasets and developing risk models, CyberCube delivers insights into the creation of cyber insurance products.

The company was incubated within Symantec and spun out as a separate business in 2018. It counts Chubb, Aon, and Munich RE among its customers.

Investors include MTech Capital and ForgePoint Capital, among others.

Most recent financing: $5M Series B (3/09/2020)

Total disclosed funding: $41.5M

Location: San Francisco, CA

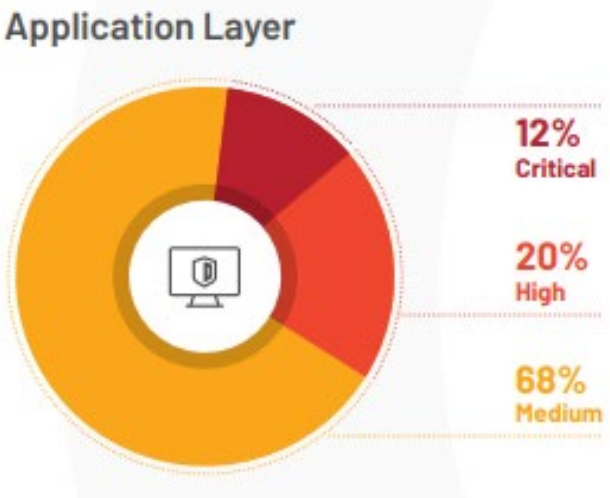
Founded: 2018

Shift left security

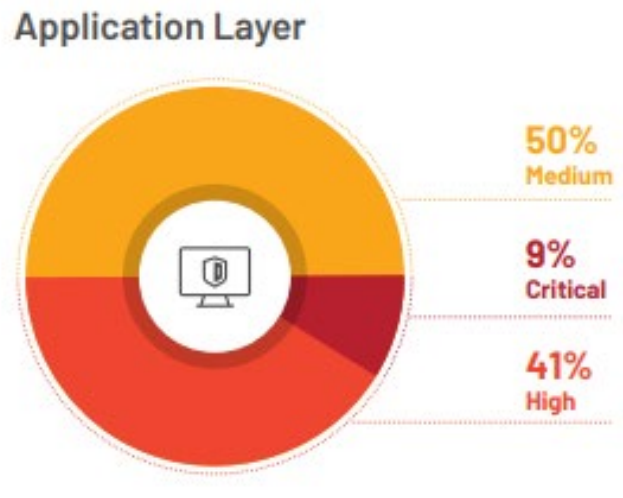
Security is too often an afterthought

When it comes to software development, security considerations are often the last step before launch. Building software without security in mind can, at best, result in delays and inefficiencies and, at worst, create serious vulnerabilities.

Vulnerability severity in external-facing apps



Vulnerability severity in internal-facing apps



Average time to remediate web application vulnerabilities:

50.3 days

Source: Edgescan

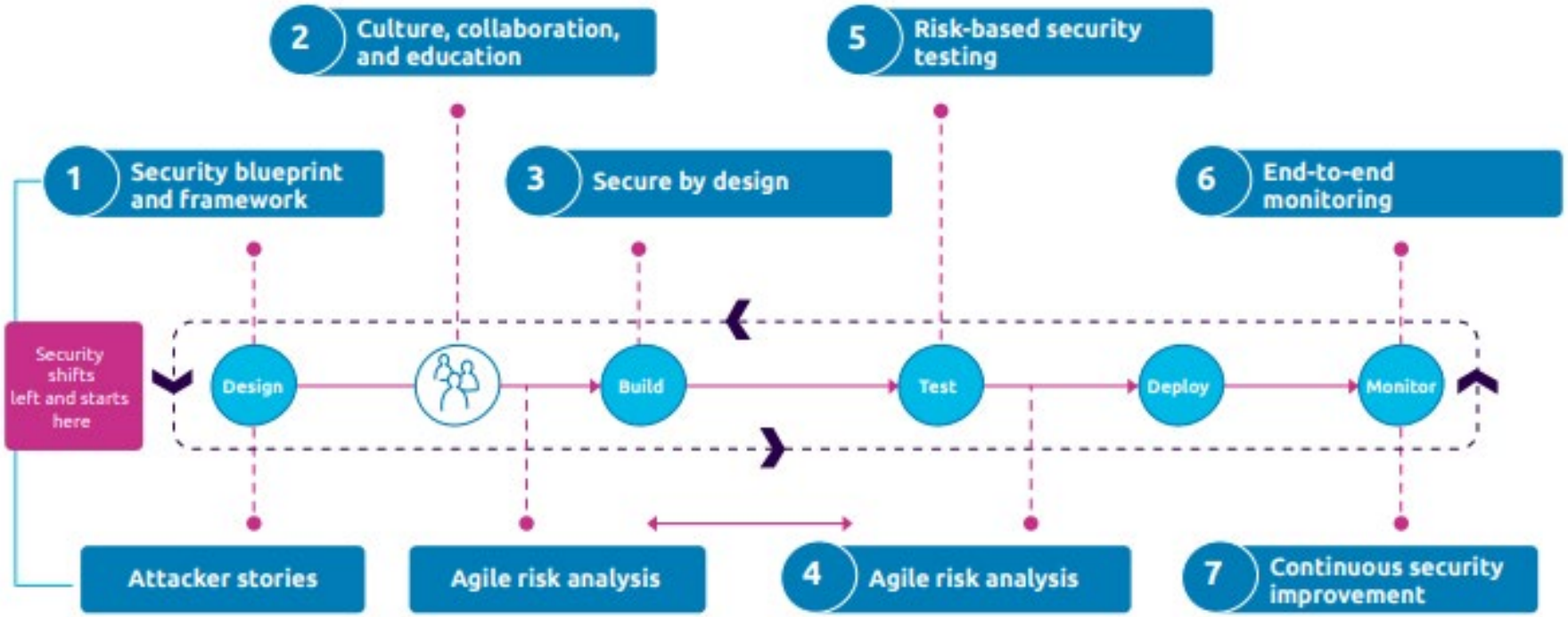
“I'd estimate that the current industry ratio sits around 1.5 security experts per 100 software engineers. This model simply does not scale when companies are confronting modern decentralized development.”

- Richard Seiersen, CISO and co-founder of Soluble, 2021

Adding security throughout the devops process

Multiple points exist within the software development lifecycle to add security measures, which could reduce the likelihood of vulnerabilities and the time to deploy safer apps. Startups are approaching these software development points with risk-mitigation solutions.

Places to add security within the software development lifecycle



CBINSIGHTS Source: Capgemini

Shift left security

cycode

Cycode secures the software development process from source code to cloud configurations.

The company provides tools such as code fingerprinting, misconfiguration scanning, and security policy enforcement to reduce security risks in the software development lifecycle.

Cycode's founders got their start in cybersecurity within the Israeli Defense Forces, and the company's early customers include Grubhub, Databricks, and Flexport.

Investors include Insight Partners and YL Ventures, among others.

Most recent financing: $20M Series A (5/11/2021)

Total disclosed funding: $24.6M

Location: Tel Aviv, Israel

Founded: 2019

BLUBRACKET

BluBracket protects software code by assessing its risk and tracking its usage.

By tracking sensitive code, highlighting misconfigurations, and scanning code repositories for risks such as hardcoded secrets and multiple owners, BluBracket brings security to the software development process.

The company was founded by serial entrepreneurs Ajay Arora and Prakash Linga, who previously founded cybersecurity companies Vera and RAPsphere.

Investors include Point72 Ventures, Unusual Ventures, and SignalFire, among others.

Most recent financing: $12M Series A (5/13/2021)

Total disclosed funding: $18.5M

Location: Palo Alto, CA

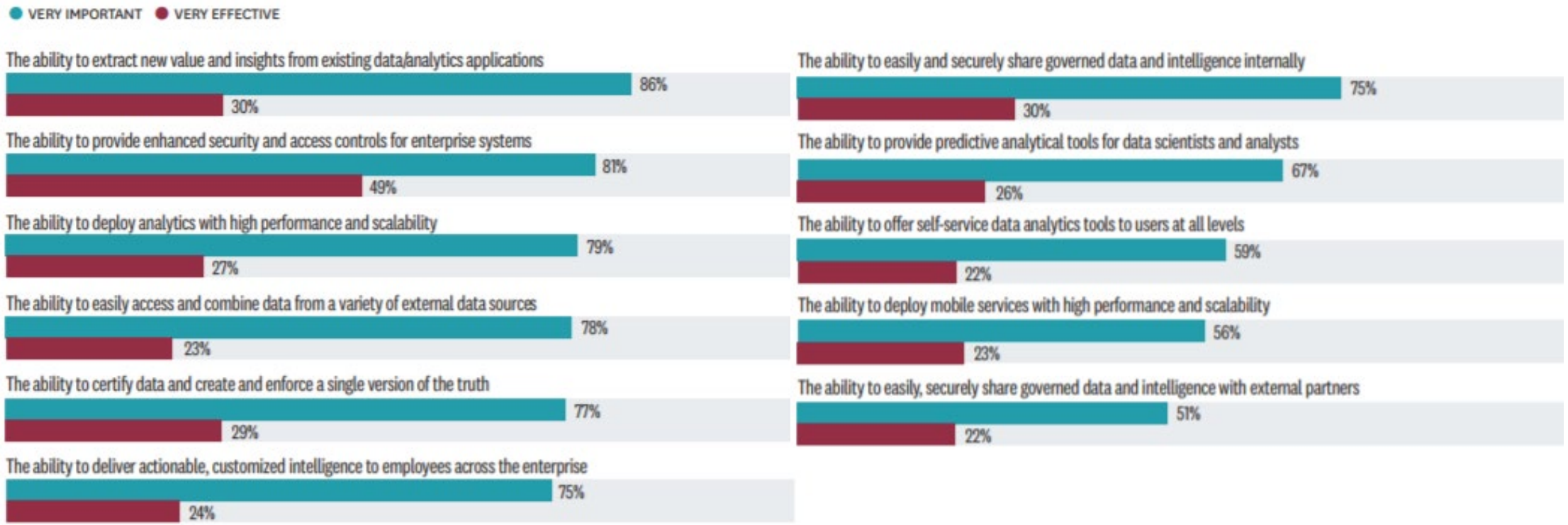
Founded: 2019

Secure data sharing

Getting value from sensitive data is difficult

To make use of their data (e.g., identify new treatments in medicine, develop customer personas in retail, etc.), companies may seek to share, combine, and analyze sensitive information. Protecting this shared data while meeting regulatory standards presents a challenge.

Reported importance and effectiveness of data operations



CBINSIGHTS Source: Harvard Business Review

“Data is considered the new oil of the economy, but privacy concerns limit their use, leading to a widespread sense that data analytics and privacy are contradictory. ”

- Jaap Wieringa, marketing professor at University of Groningen, the Netherlands, 2021

New encrypted data use cases emerge

Encrypted data's protective elements historically came at the cost of analysis and collaboration. However, startups have developed new techniques to make data more usable while keeping it secure.

Privacy preserving computation (PPC) techniques

Trusted Execution Environment (Secure Enclave):
An environment with special hardware modules that allow for data processing within hardware-provided, encrypted private memory areas directly on the microprocessor chip only accessible to the running process (page 22).

Homomorphic Encryption:
A technology that enables computation on encrypted data without the need to decrypt it first (or at all). In this way, the sensitive data are encrypted and protected at all stages of transport and processing (page 31).

Differential Privacy:
A data obfuscation mechanism—often used with other traditional anonymization or de-identification techniques—that allows broad statistical information to be gathered and inferred from data without the actual specifics of individual items being exposed (page 26).

Secure Multi Party Computation (MPC):
A technology that provides a mechanism that allows a group of parties to share the benefits of combining their data to create useful outputs while keeping their actual source data private from each other (page 36).

Source: Accenture

Secure data sharing

Cape Privacy

Cape Privacy enables data scientists to share and work with encrypted data.

Its product allows organizations to train AI models on encrypted data so that it can be shared without compromising privacy or security.

The company was founded by Gavin Uhma, who previously founded GoInstant. Cape Privacy has found early traction for its product in the financial services industry.

Investors include Evolution Equity Partners, Tiger Global Management, and Haystack Fund, among others.

Most recent disclosed financing: $20M Series A (4/20/2021)

Total disclosed funding: $25.1M

Location: New York, NY

Founded: 2018

TripleBlind

TripleBlind provides a solution for sharing and analyzing encrypted data.

Its platform allows companies to encrypt their data and algorithms to support protected data analysis and sharing.

The company's patented technology is currently being tested by the Mayo Clinic.

Investors include Mayo Clinic, Accenture Ventures, and Anorak Ventures, among others.

Most recent financing: $8.2M seed (4/27/2021)

Total disclosed funding: $8.2M

Location: Kansas City, MO

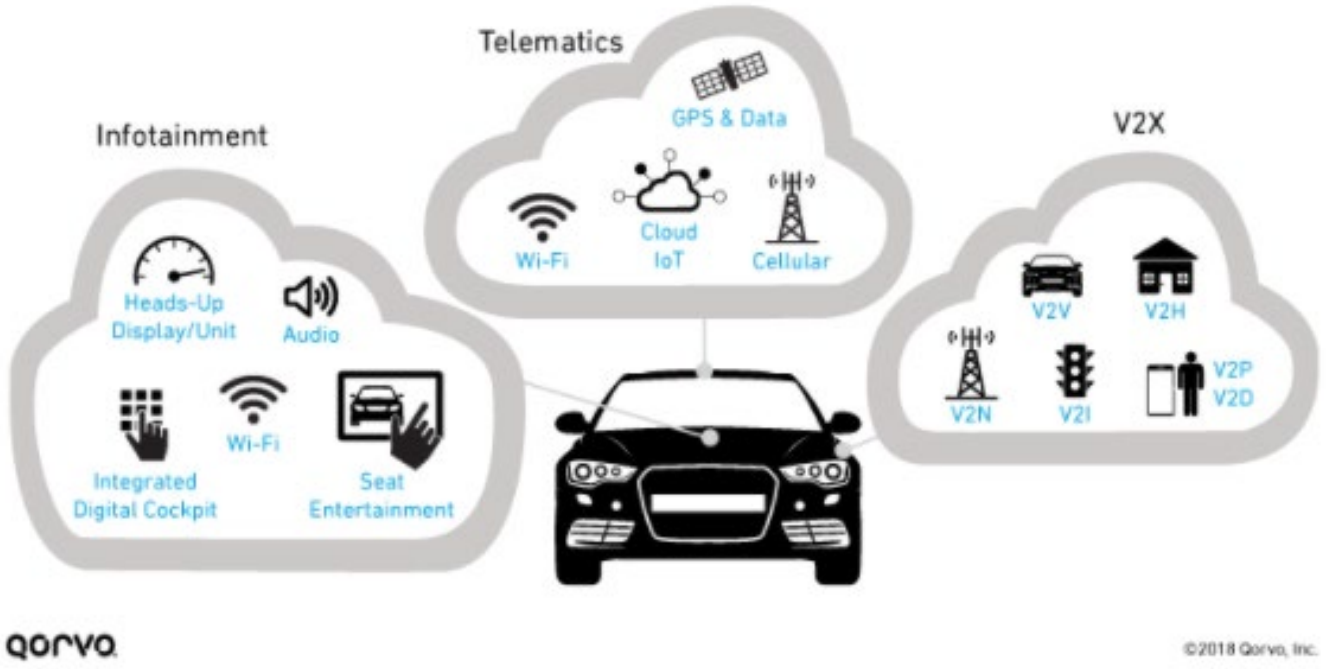
Founded: 2019

Auto security

Connected cars heighten cyber risks

As vehicles adopt new technologies and effectively become data centers on wheels, they create new opportunities for hackers.

The car's expanded attack surface



Source: Qorvo

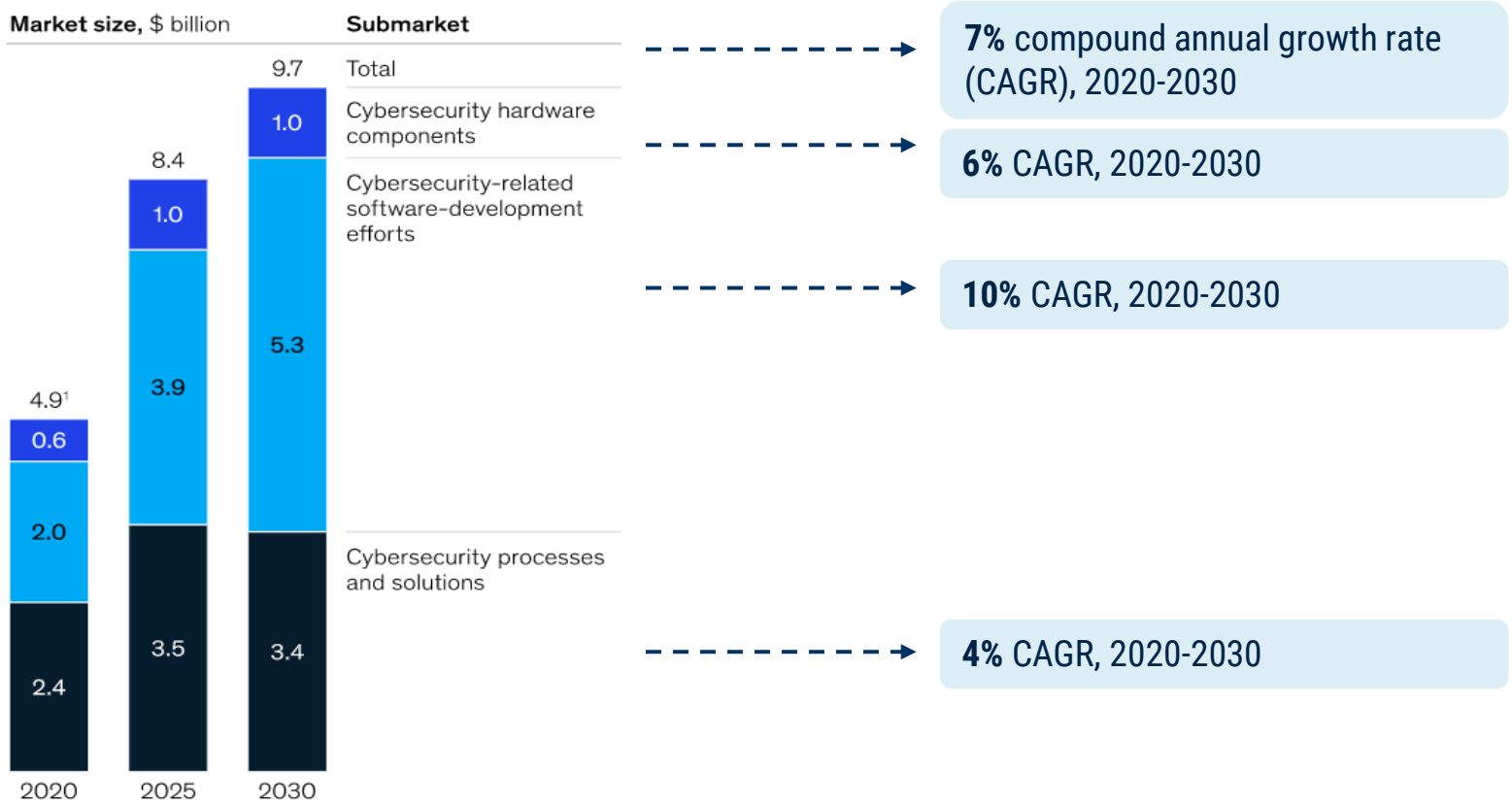
“As we connect more things to the internet, we're connecting a lot more devices that haven't been designed with cyber-security in mind. And if the trend continues, bad guys will go after it.”

- Robert Potter, cybersecurity researcher, 2021

Automotive-first cyber companies emerge

A new breed of startups looks to capitalize on the opportunity that comes with tackling automotive security's unique challenges.

Cybersecurity market size



CBINSIGHTS Source: McKinsey

Auto security

Upstream

Upstream monitors vehicles to identify and respond to cyber attacks and misuse.

The company's platform analyzes automotive data feeds to detect and respond to cyber threats. Further, its threat intelligence product monitors automotive-specific risks and malicious actors.

Founded by cybersecurity veterans, Upstream has filed more than 5 patents for its technology since 2018 and counts several automotive companies among its financial backers.

Investors include CRV, Hyundai Motor Company, and Volvo Group Venture Capital, among others.

Most recent financing: $36M Series C (5/20/2021)

Total disclosed funding: $77M

Location: Herzliya, Israel

Founded: 2017

C2A security

C2A Security provides a tool for monitoring a vehicle's internal systems.

The company aims to support Tier 1 automotive suppliers and manufacturers by offering security capabilities that identify attacks on a vehicle's systems (e.g., powertrain, ADAS system).

C2A was founded by Michael Dick, who previously co-founded content security company NDS. The company has filed 2 patents for its embedded security technology.

Investors include MoreVC, Maniv Mobility, and Labs/02.

Most recent financing: $6.5M Series A (2/11/2019)

Total disclosed funding: $6.5M

Location: Derech Hebron, Israel

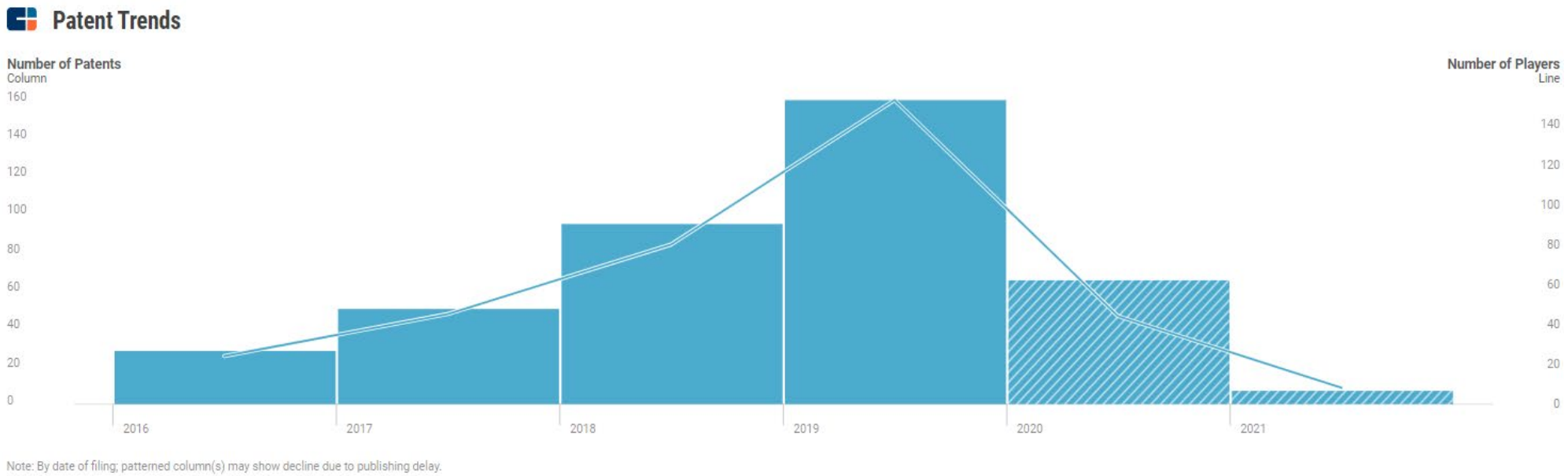
Founded: 2016

Post-quantum cryptography

Quantum computers threaten today's encryption

As quantum computing develops, it will eventually be able to crack today's public-key encryption methods. For example, it's estimated that a 20M qubit computer could break the commonly used 2,048-bit RSA encryption system in just 8 hours.

Quantum computing progress as measured by number of patents



“If you have secrets which need to remain secret 10 to 30 years from now, you should begin this migration sooner than later.”

- Vadim Lyubashevsky, cryptography researcher at IBM Research, 2021

Start considering quantum-safe protections

The National Institute of Standards and Technology (NIST) is currently developing standards for post-quantum cryptography, or methods for securing data and communications in a world with quantum computers. Wasting no time, several startups have jumped in front of technology to create early post-quantum solutions.

Examples of quantum-secure algorithms

Lattice-based cryptography	Code-based cryptography	Multivariate-based cryptography
Based on abstract structures of mathematics. It currently looks like the most promising method.	Uses error-correcting-codes that allows read or data being transmitted to be checked for errors and corrected in real time.	Based on solving multi variable equations. These equations are hard to solve using brute force.

CBINSIGHTS Source: TechTarget

Post-quantum cryptography

Isara offers tools to protect against future quantum computing attacks.

Specifically, Isara allows companies to view and manage their cryptographic assets or infrastructure through a single tool, which can support the move to quantum-safe algorithms.

The company was founded by senior BlackBerry security executives and counts Thales, DigiCert, and others as partners.

Investors include Quantum Valley Investments, Shasta Ventures, and Science and Economic Development Canada.

Most recent disclosed financing: $5.4M grant (4/18/2019)

Total disclosed funding: $26.9M

Location: Ontario, Canada

Founded: 2015

QuSecure provides solutions for evading quantum computing attacks.

Leveraging quantum-safe algorithms, QuSecure provides key management and data-at-rest security solutions.

The company has partnered with Amazon and Google, and its founders include serial entrepreneurs with a track record of successful exits.

Investors include Techstars Starburst Space Accelerator.

Most recent financing: $120K seed (6/07/2021)

Total disclosed funding: $120K

Location: Menlo Park, CA

Founded: 2019

Appendix

METHODOLOGY

How the categories were selected: We used CB Insights data — including startup funding, media mentions, earnings call transcripts, patents, and more — to identify our Cyber Defenders technology categories.

How the companies were selected: We used CB Insights' machine learning-powered Mosaic Score to select our Cyber Defenders, which uses data to track private company health based on metrics like recency of financing, total funding raised, and investor quality. The CB Insights Mosaic page walks through the factors considered in the algorithm.