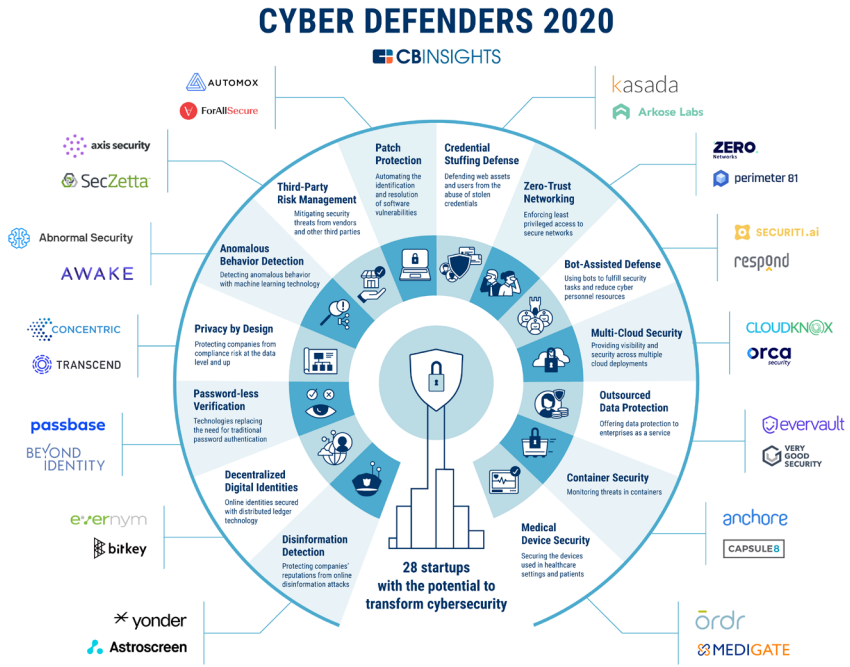
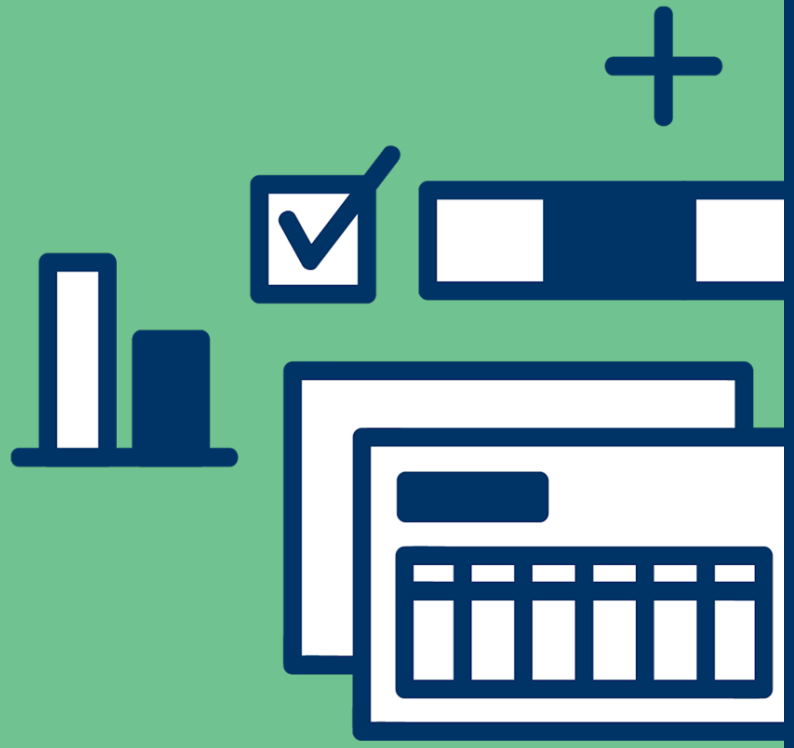
2020 Cyber Defenders

This year's trends, opportunities, and high-momentum startups with the potential to shape **the future of cybersecurity**

CBINSIGHTS



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.

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

12 Cybersecurity funding trends

20 Cyber Defender categories

21 2020 Cyber Defenders

95 Appendix & Methodology

CYBERSECURITY IS TOP OF MIND

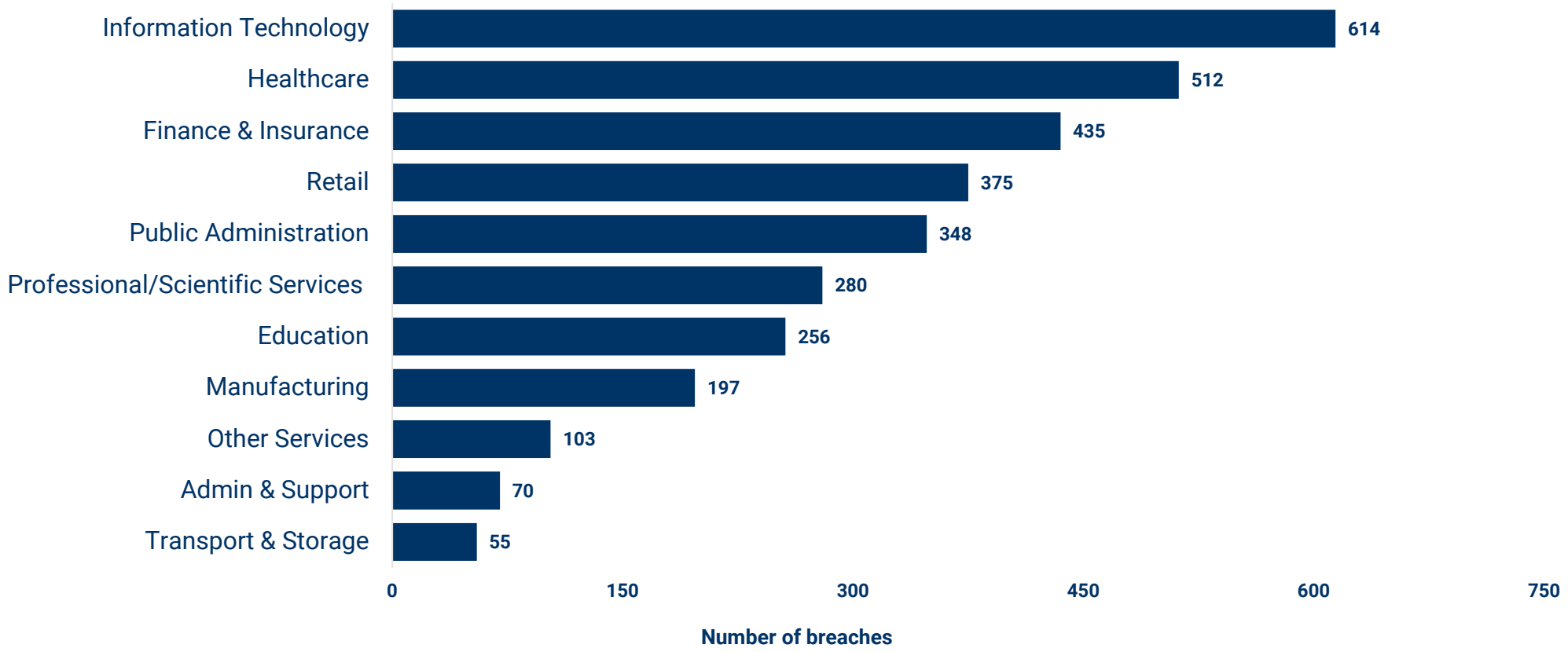
Over 7,000 **data breaches** were reported in 2019.

Protecting customer data weighs on corporations, which are facing increasingly sophisticated cyber attacks.

Source: Risk Based Security

CYBER INSECURITY IS FELT ACROSS INDUSTRIES

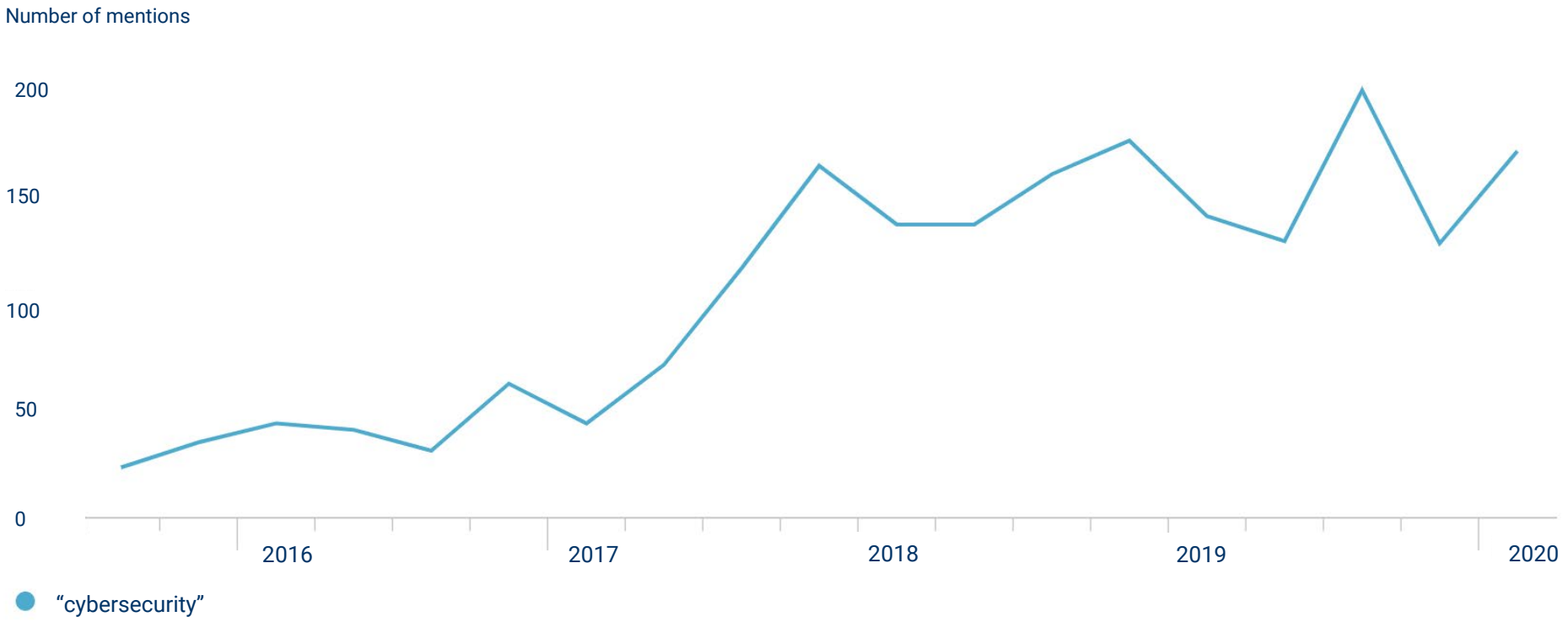
NUMBER OF DATA BREACHES BY ECONOMIC SECTOR IN 2019



Source: Risk Based Security

CONSISTENT TALK OF CYBERSECURITY AMONG THE C-SUITE

NUMBER OF EARNINGS CALLS MENTIONS OF "CYBERSECURITY" Q3'15 – Q1'20



Source: CB Insights

"So, you never know, the bad guys are continuing to invest as much as the good guys. And we got to stay out ahead of it. We got to remain vigilant."

- Alfred Kelly, CEO Visa, Q3'19 earnings call

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?

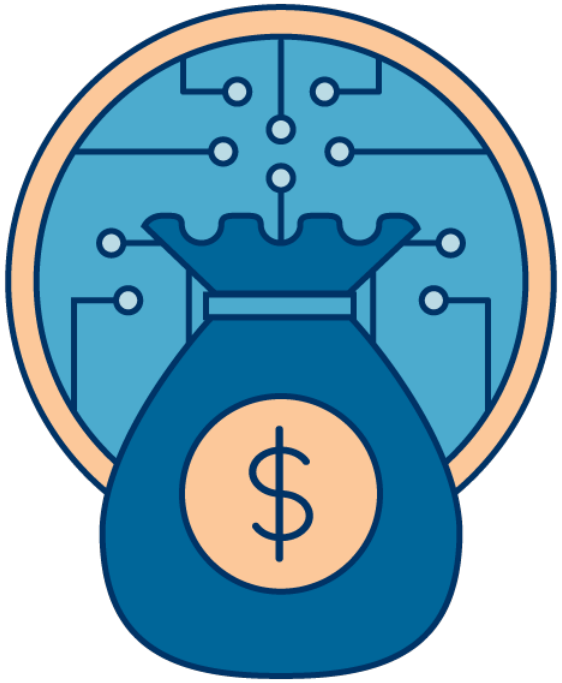
Our selected startups are early- to mid-stage, high-momentum companies pioneering technology with the potential to transform cybersecurity.

Unicorns valued at $1B+, companies that have raised funding past the Series C stage, and companies that have not raised funding since 2018 are excluded.

But first, some funding trends…

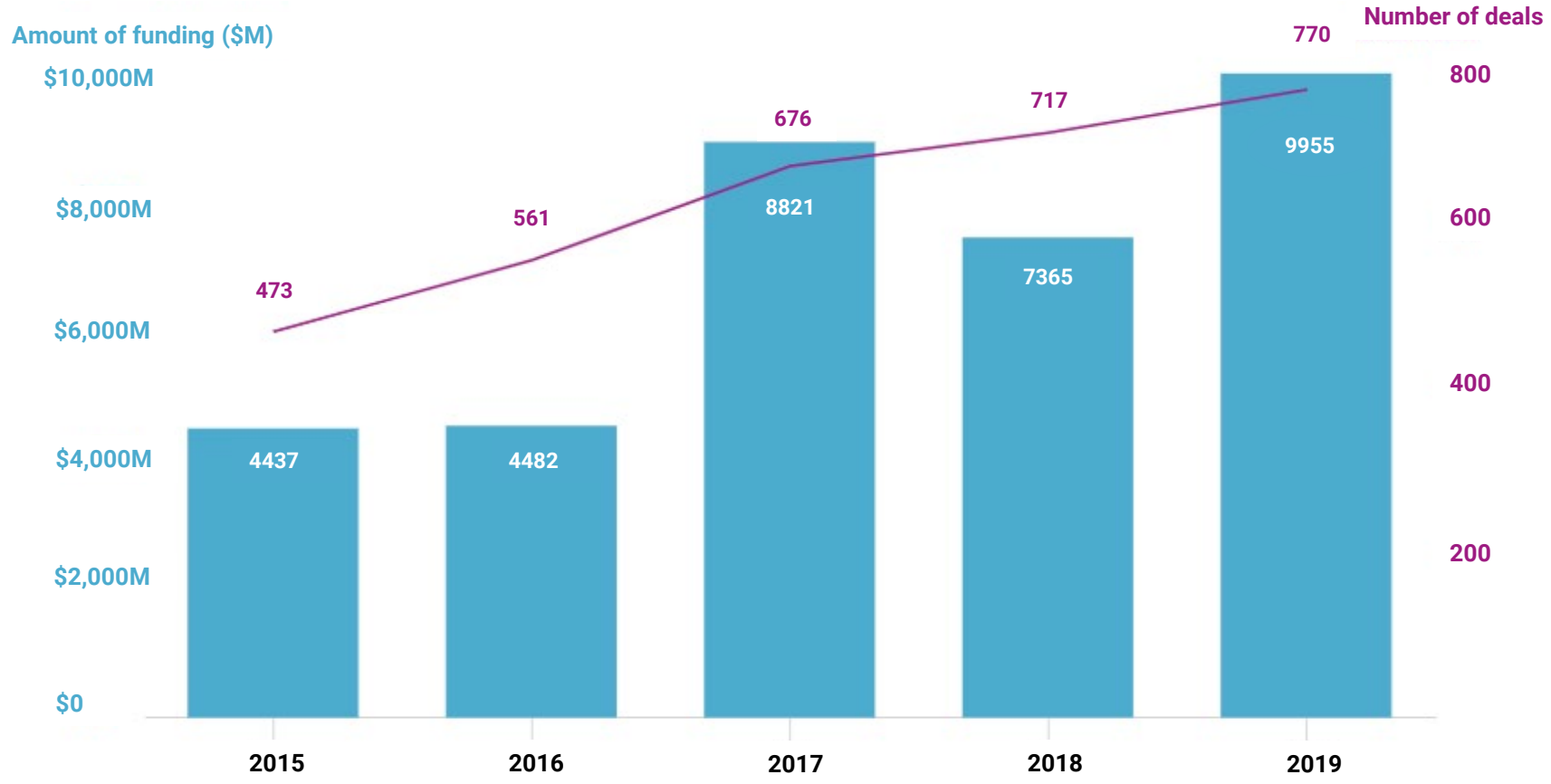
CYBERSECURITY

Global equity funding trends



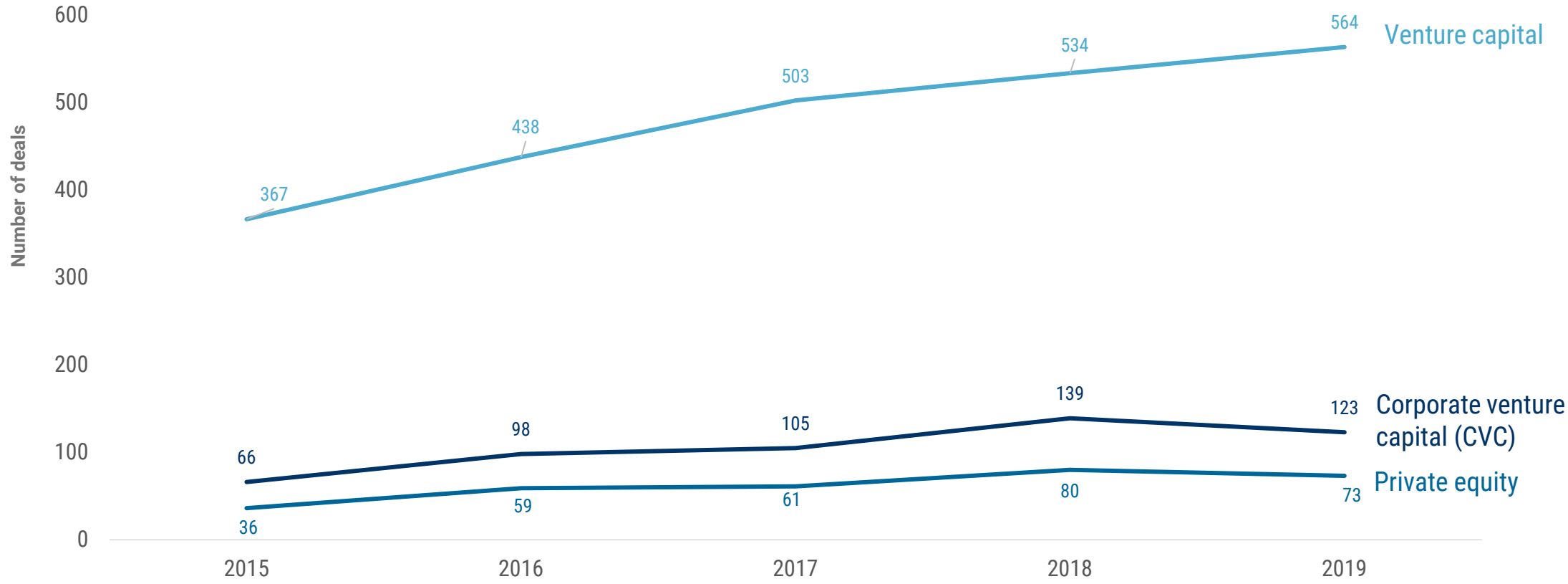
Cybersecurity funding and deals hit record highs

Annual global cybersecurity deals and financing 2015 – 2019



VC interest in cybersecurity persists

Annual number of investments in cybersecurity by investor type, 2015 – 2019



Ten Eleven, Lightspeed, and Accel top rankings

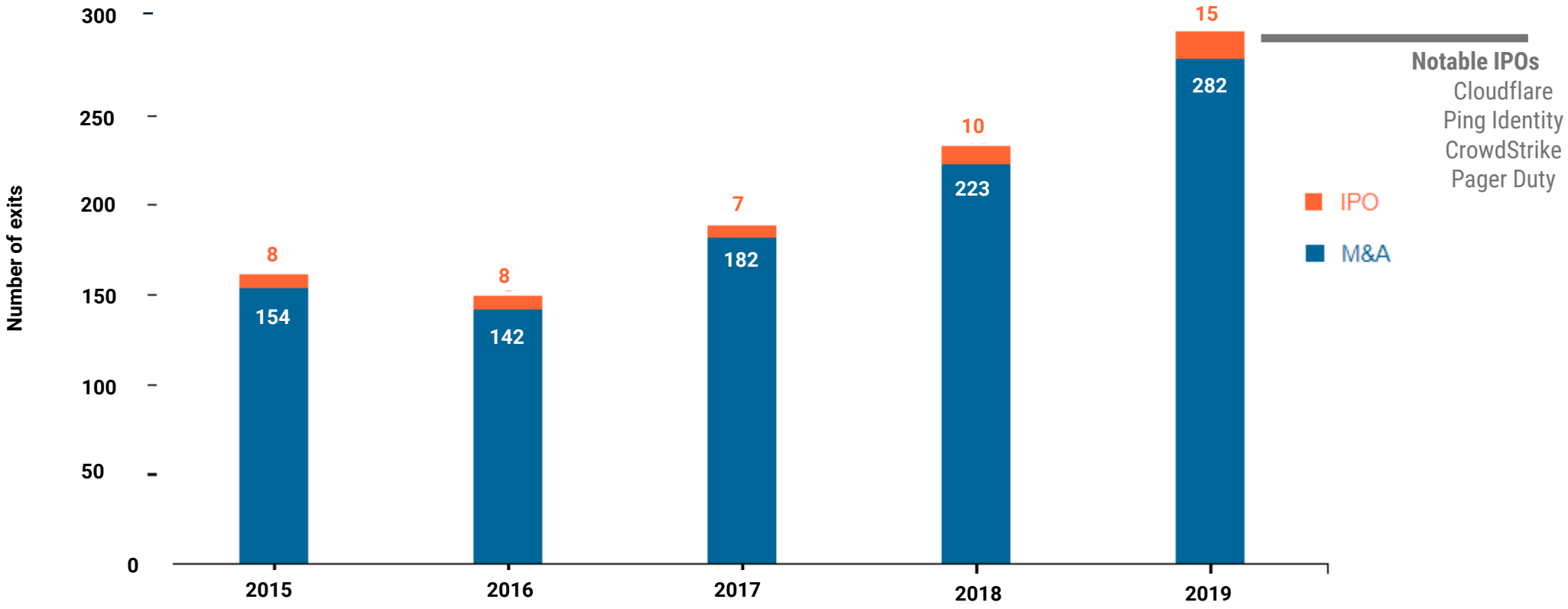
Most active investors in cybersecurity startups by type for 2019

*Ten Eleven, Lightspeed, and Accel each made **10 investments**.

EXITS REACH AN ALL-TIME HIGH

IPOs and acquisitions up from 2018

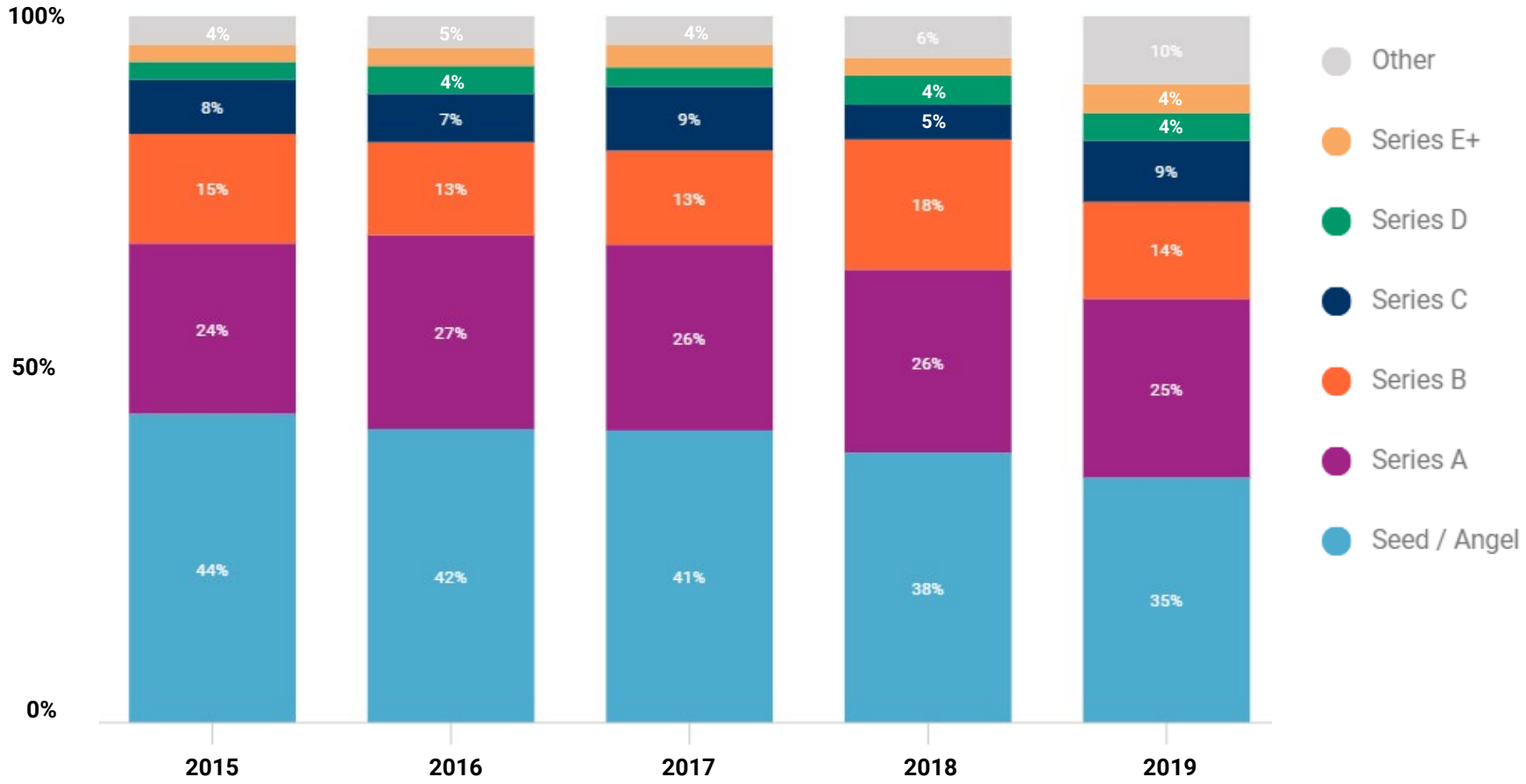
Annual number of cybersecurity company exits through either M&A or IPO, 2015 – 2019



LATE-STAGE DEALS REACH FIVE YEAR HIGH IN 2019

Late-stage investments increase

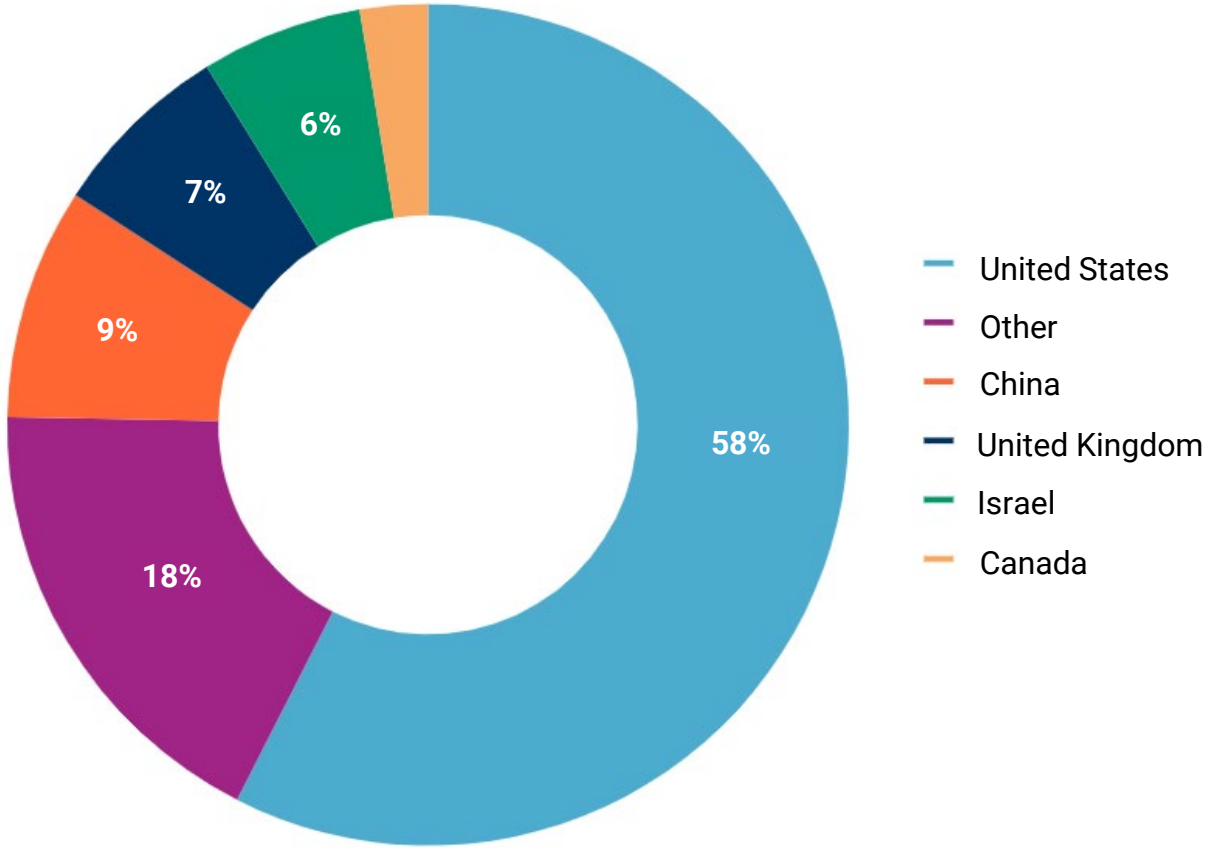
Annual deal share by stage of investments in private cybersecurity companies, 2015 – 2019



CBINSIGHTS Note: Early-stage deals include Seed/Angel and Series A rounds; mid-stage deals include Series B and Series C rounds; late-stage deals are Series D+ rounds.

China surpasses Israel and the UK in deal share

Cybersecurity global deal share by country, 2015 – 2019



Number of cybersecurity unicorns doubles to 16

Private cybersecurity companies valued at $1B+ as of 6/01/2020:

Note: There were 8 cybersecurity unicorns as of 3/21/2019.

This year's Cyber Defender categories

Disinformation detection
Protecting companies' reputations from online disinformation attacks

Decentralized digital identities
Online identities secured with distributed ledger technology

Password-less verification
Technologies replacing the need for traditional password authentication

Privacy by design
Protecting companies from compliance risk at the data level and up

Anomalous behavior detection
Detecting anomalous behavior with machine learning technology

Third-party risk management
Mitigating security threats from vendors and other third parties

Patch protection
Automating the identification and resolution of software vulnerabilities

Credential stuffing defense
Defending web assets and users from the abuse of stolen credentials

Zero-trust networking
Enforcing least privileged access to secure networks

Bot-assisted defense
Using bots to fulfill security tasks and reduce cyber personnel resources

Multi-cloud security
Providing visibility and security across multiple cloud deployments

Outsourced data protection
Offering data protection to enterprises as a service

Container security
Monitoring threats in containers

Medical device security
Securing the devices used in healthcare settings and patients

The 2020 Cyber Defenders

Disinformation detection

yonder

Astroscreen

Decentralized digital identities

evernym

bitkey

Password-less verification

passbase

BEYOND IDENTITY

Privacy by design

CONCENTRIC

TRANSCEND

Anomalous behavior detection

ABNORMAL SECURITY

AWAKE

Third-party risk management

axis security

SecZetta

Patch protection

AUTOMOX

ForAllSecure

Credential stuffing defense

Arkose Labs

kasada

Zero-trust networking

perimeter 81

ZERO Networks

Bot-assisted defense

SECURITI.ai

respond

Multi-cloud security

CLOUDKNOX

orca security

Outsourced data protection

evervault

VERY GOOD SECURITY

Container security

anchore

CAPSULE8

Medical device security

ordr

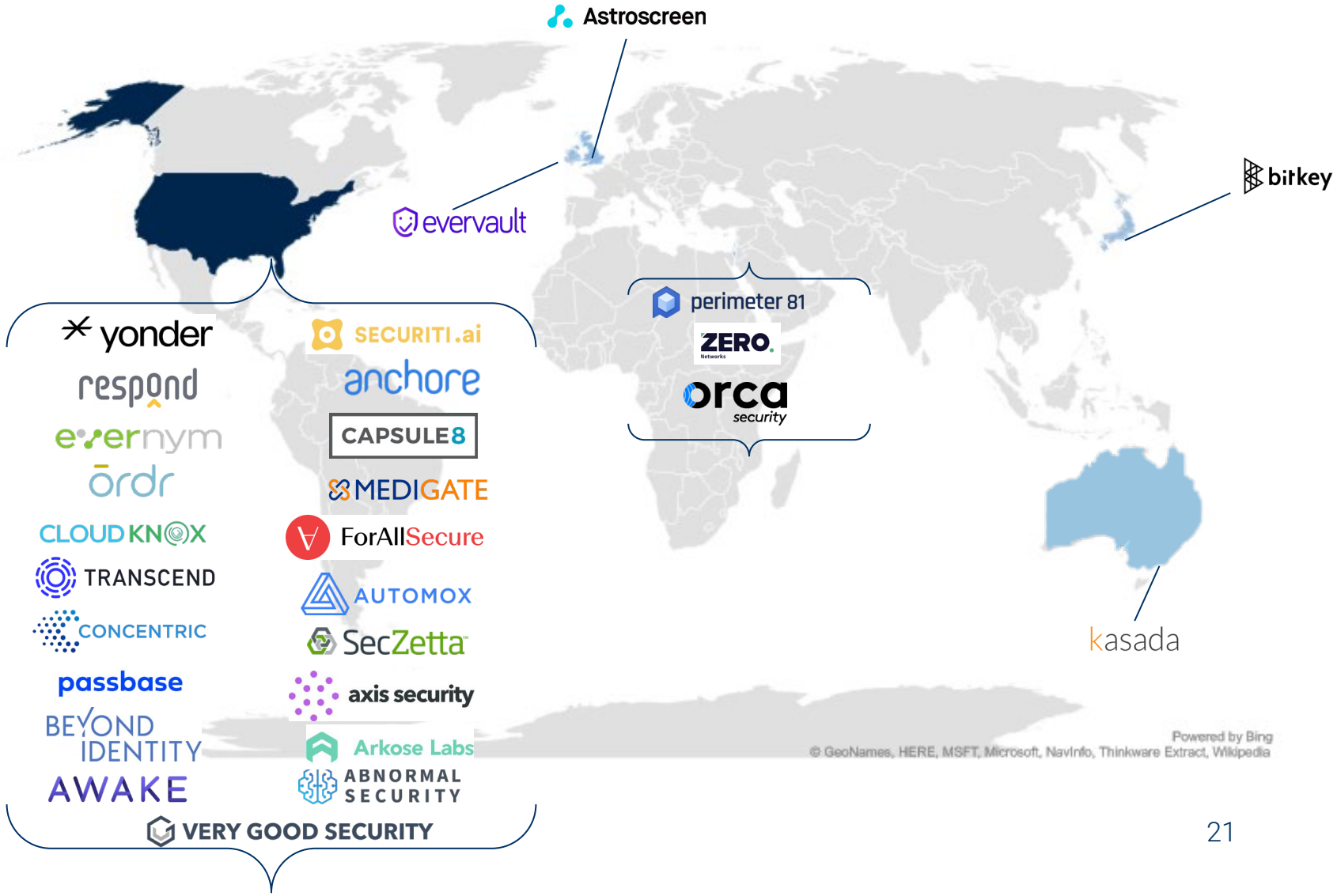
MEDIGATE

The US has the most Cyber Defenders

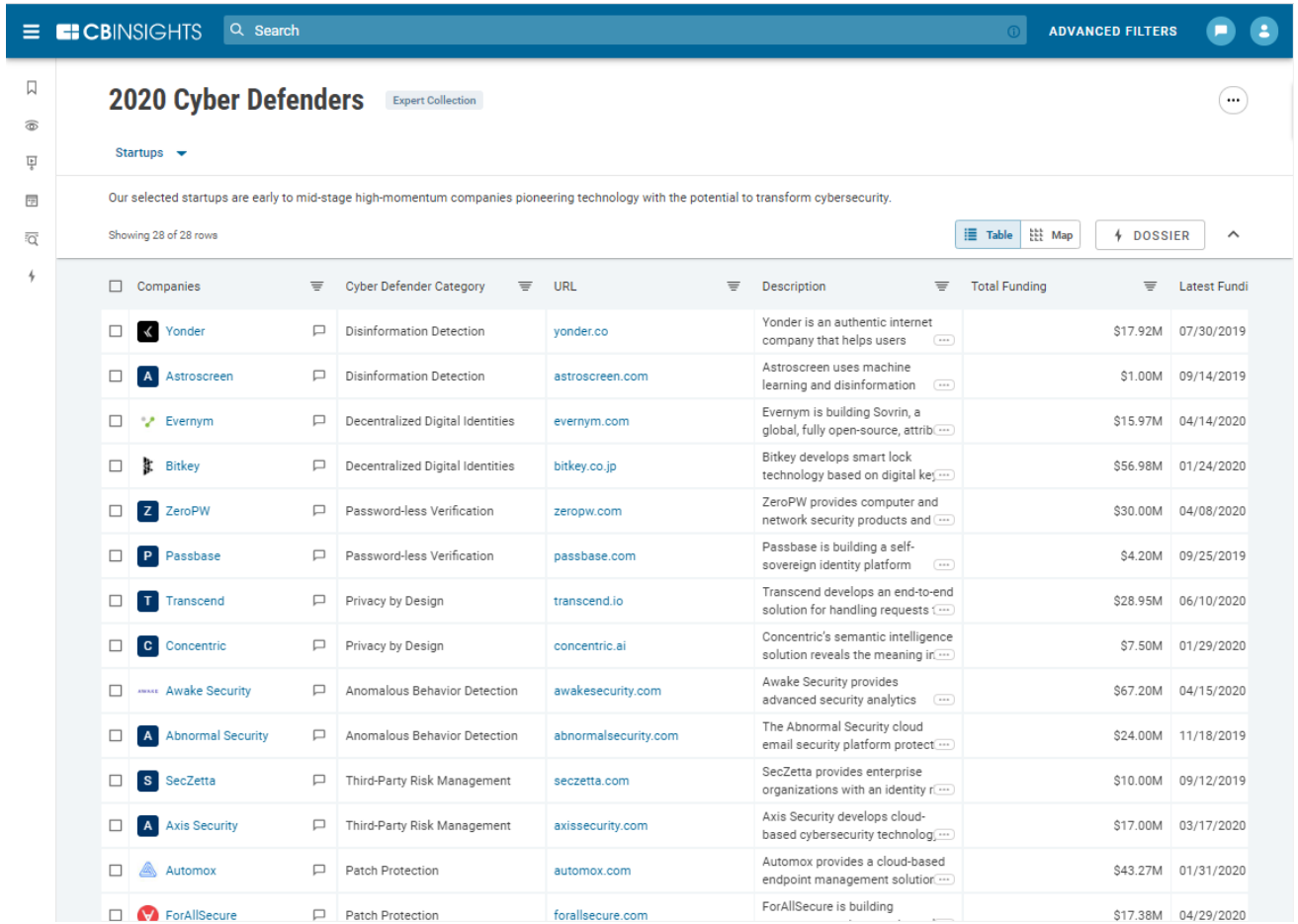
75% of the 2020 Cyber Defenders are headquartered in the US — mostly in California.

The next highest concentration of Cyber Defenders is in Israel.

The United Kingdom, Japan, Ireland, and Australia each have one Cyber Defender.



2020 Cyber Defenders Expert Collection on CBI



Companies	Cyber Defender Category	URL	Description	Total Funding	Latest Fundi
Yonder	Disinformation Detection	yonder.co	Yonder is an authentic internet company that helps users	$17.92M	07/30/2019
Astroscreen	Disinformation Detection	astroscreen.com	Astroscreen uses machine learning and disinformation	$1.00M	09/14/2019
Evernym	Decentralized Digital Identities	evernym.com	Evernym is building Sovrin, a global, fully open-source, attrib	$15.97M	04/14/2020
Bitkey	Decentralized Digital Identities	bitkey.co.jp	Bitkey develops smart lock technology based on digital ke	$56.98M	01/24/2020
ZeroPW	Password-less Verification	zeropw.com	ZeroPW provides computer and network security products and	$30.00M	04/08/2020
Passbase	Password-less Verification	passbase.com	Passbase is building a self-sovereign identity platform	$4.20M	09/25/2019
Transcend	Privacy by Design	transcend.io	Transcend develops an end-to-end solution for handling requests	$28.95M	06/10/2020
Concentric	Privacy by Design	concentric.ai	Concentric's semantic intelligence solution reveals the meaning in	$7.50M	01/29/2020
Awake Security	Anomalous Behavior Detection	awakesecurity.com	Awake Security provides advanced security analytics	$67.20M	04/15/2020
Abnormal Security	Anomalous Behavior Detection	abnormalsecurity.com	The Abnormal Security cloud email security platform protect	$24.00M	11/18/2019
SecZetta	Third-Party Risk Management	seczetta.com	SecZetta provides enterprise organizations with an identity r	$10.00M	09/12/2019
Axis Security	Third-Party Risk Management	axissecurity.com	Axis Security develops cloud-based cybersecurity technolog	$17.00M	03/17/2020
Automox	Patch Protection	automox.com	Automox provides a cloud-based endpoint management solution	$43.27M	01/31/2020
ForAllSecure	Patch Protection	forallsecure.com	ForAllSecure is building	$17.38M	04/29/2020

Visit the Cyber Defenders 2020 collection on the CB Insights platform

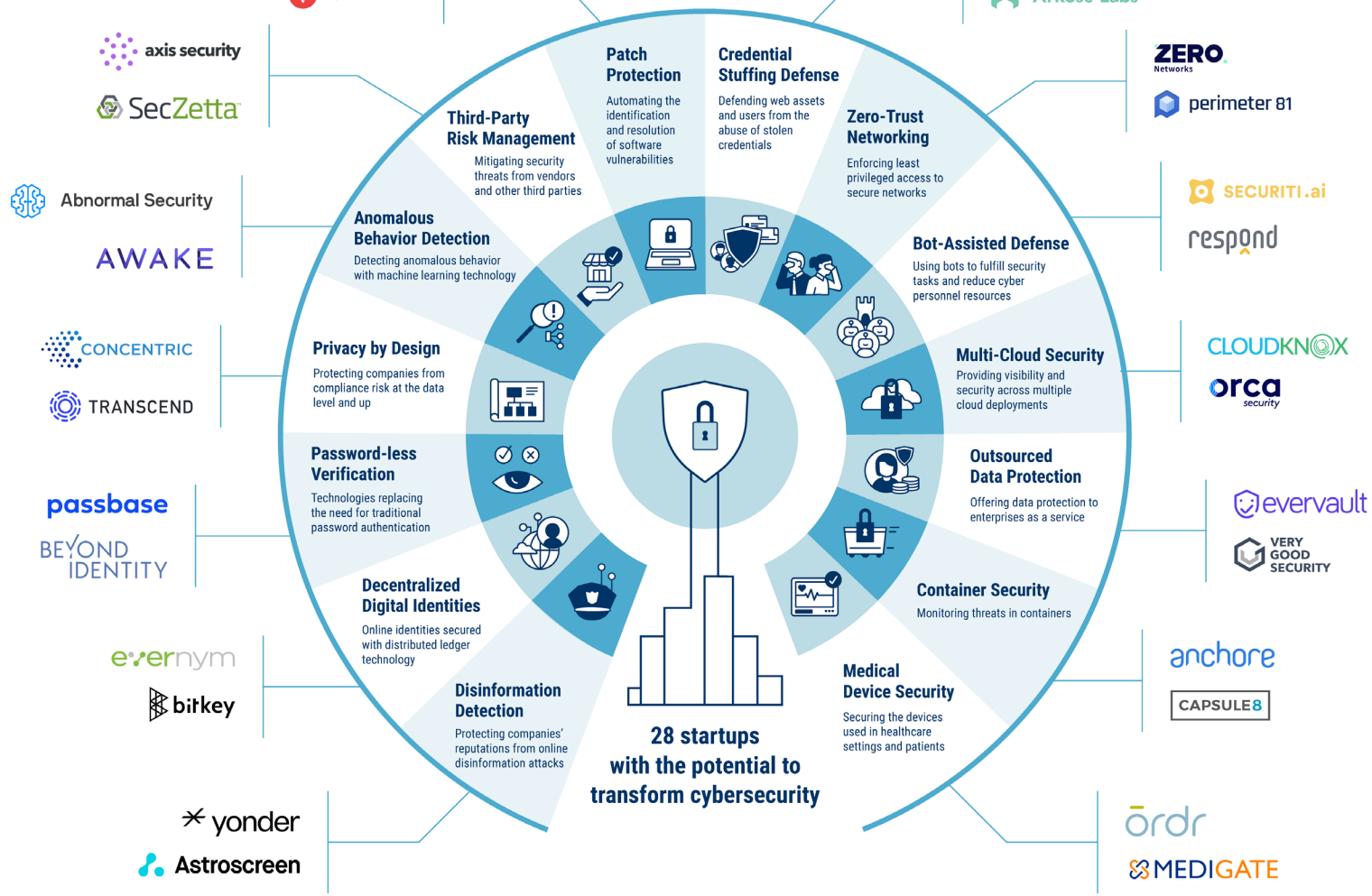
CBI Cyber Defenders 2020

Track all of the startups in this presentation and many more on our platform using CB Insights' Collections.

Create dynamic market landscapes, collaborate within and beyond your organization, seamlessly manage what new areas the team needs to have on their radar when making growth decisions.

CYBER DEFENDERS 2020

CBINSIGHTS

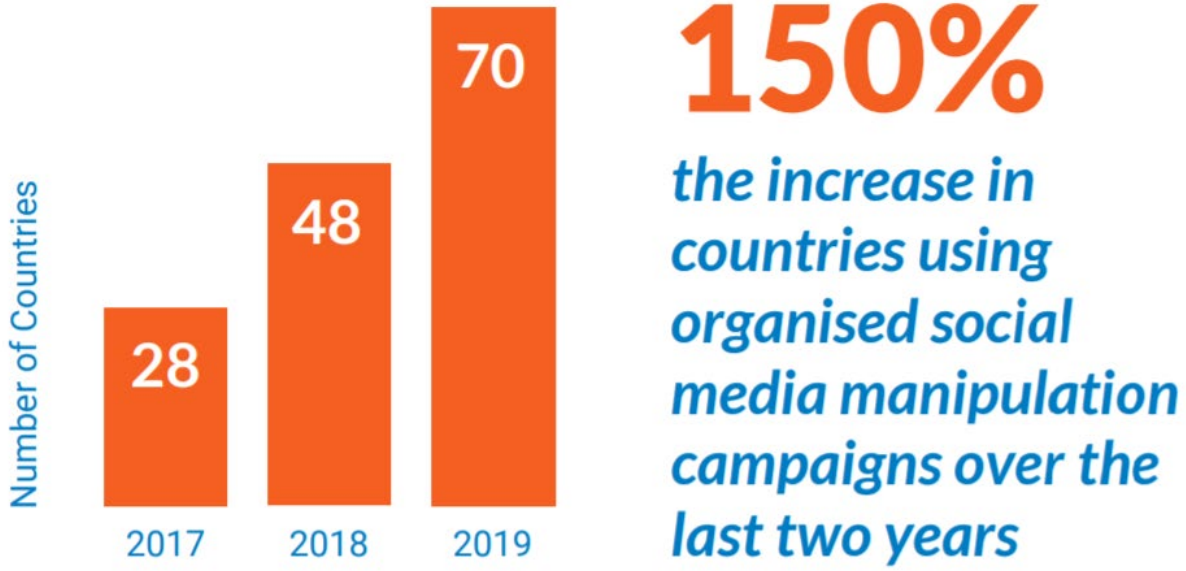


Disinformation detection

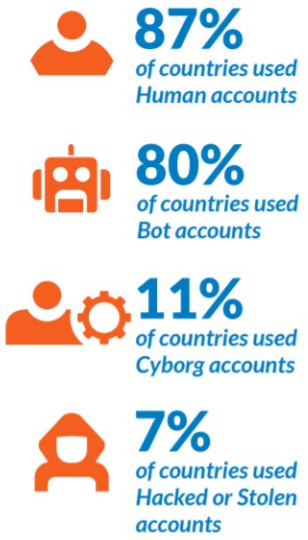
Disinformation campaigns are on the rise

Bot technology and ease of access to social media and other online platforms enable **quick, inexpensive creation of disinformation campaigns**.

Number of countries where a disinformation campaign originated, 2017-2019



Mode of distribution by country



Source: The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation

"Anonymous bad actors frequently spread false or misleading claims about a targeted stock via blogs, forums, social media, bot networks, or spam. These campaigns seek to either artificially increase the stock's price…or lower it…for quick profit."

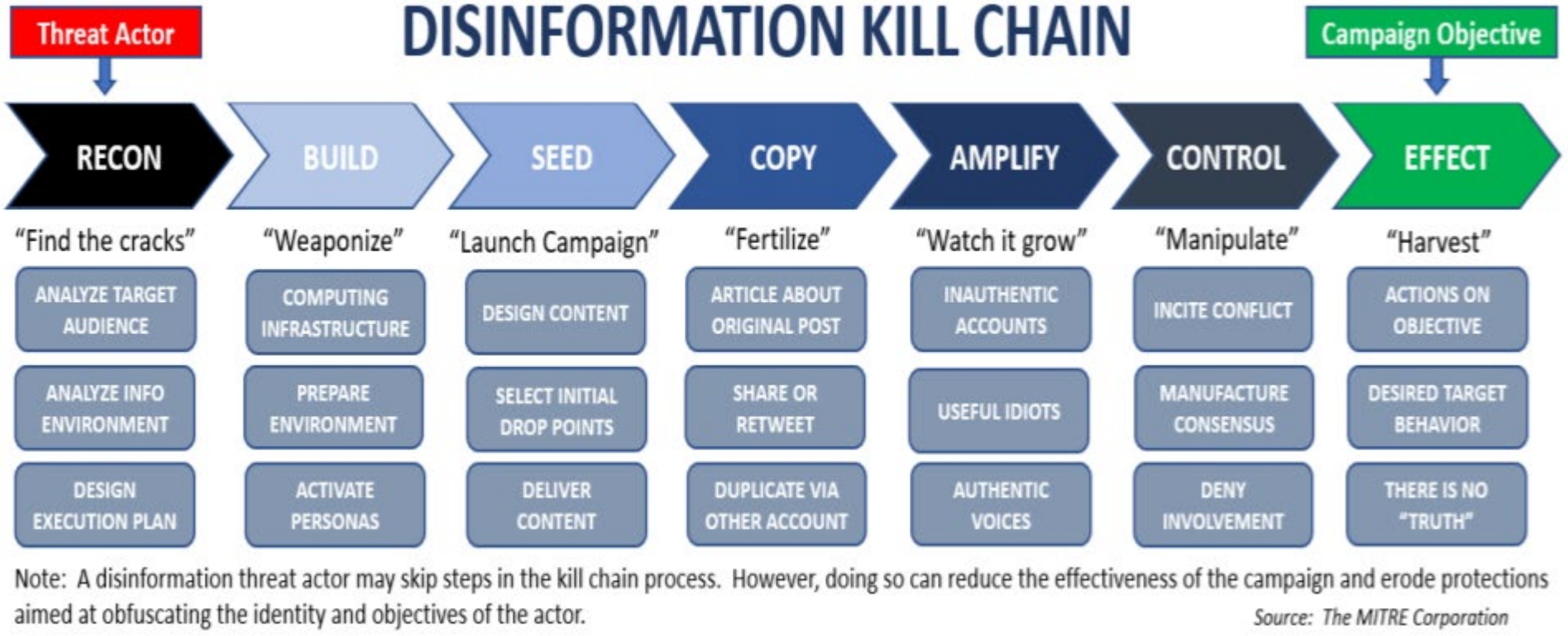
CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

- Jon Bateman, Cyber Policy Fellow at the Carnegie Endowment for International Peace, 2020

Source: Carnegie Endowment for International Peace

Identify disinformation early to disrupt the chain

Startups monitoring brands across online platforms help companies **thwart or respond to disinformation** before it has the chance to spread.



Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation

Source: Department of Homeland Security

Disinformation detection

Astroscreen

Astroscreen uses machine learning to detect disinformation.

The company monitors social media to identify bots, coordinated disinformation campaigns, and anomalous behavior or content.

Astroscreen was founded in 2018 by media entrepreneur Ali Tehrani and researcher Juan Echeverria, who discovered a 350,000 automated account botnet on Twitter in 2017.

Investors include Cyber London Accelerator, AI Seed, and Speedinvest, among others.

Most recent financing: Seed (9/14/2019)

Total disclosed funding: $1M

Location: London, United Kingdom

yonder

Yonder tracks internet factions responsible for creating disinformation.

Monitoring conversations across the internet from Twitter to message boards to the dark web, Yonder's platform identifies disinformation threats to a company's brand.

The company launched in 2017 to help governments identify foreign, malicious factions. It now helps companies monitor online risk, counting Walmart, Viacom, and others among its customers.

Investors include Lux Capital, GGV Capital, and BuildGroup Management, among others.

Most recent financing: $3M Series A (7/30/2019)

Total disclosed funding: $17.9M

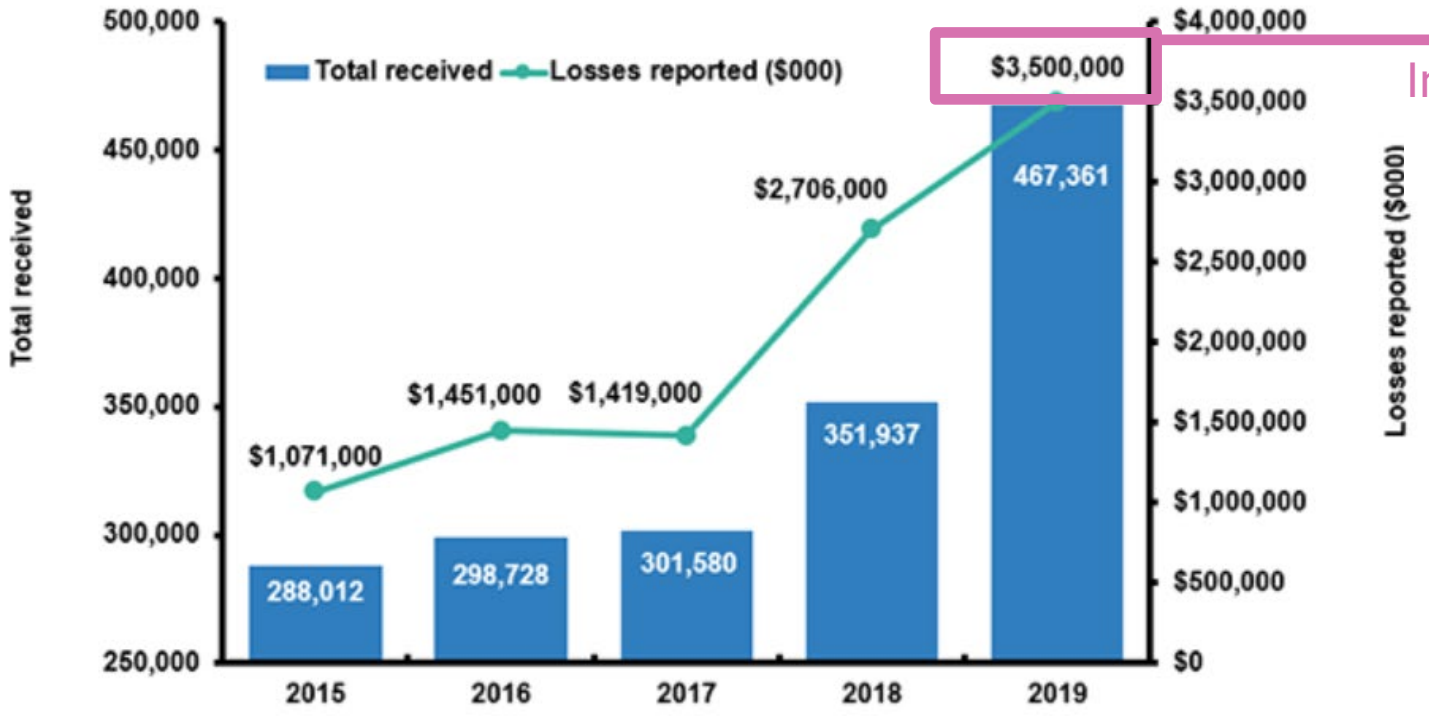
Location: Austin, TX

Decentralized digital identities

Digital transactions can be costly

From conversations to shopping to banking, people's lives are moving online and leaving behind a digital footprint. Without a seamless and secure process for authenticating these disparate transactions, there's a risk for cybercrime.

Number of cybercrimes in the United States 2015 – 2019



Includes **$280M** in identity theft and personal data breach losses

Source: Insurance Information Institute; Internet Crime Complaint Center

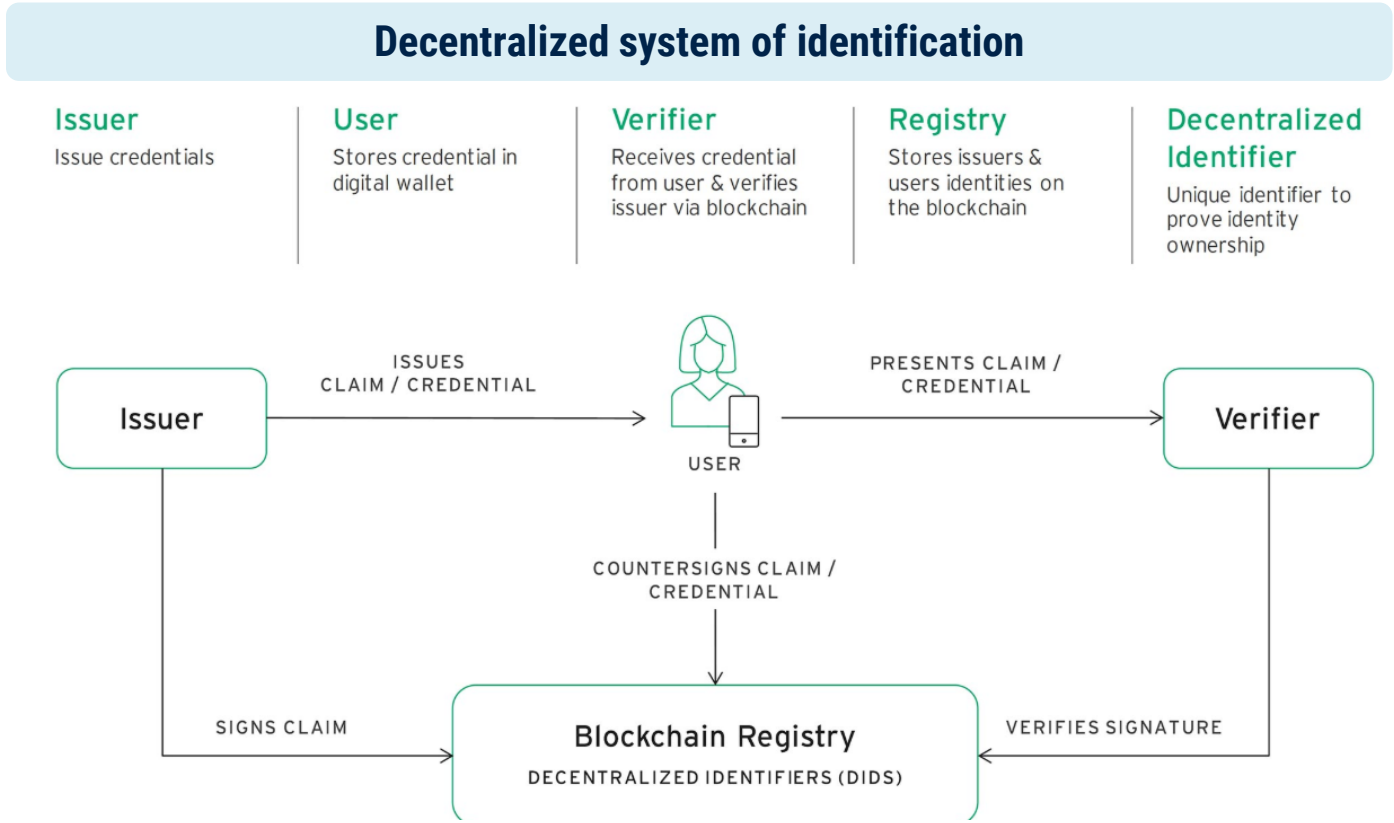
"Identity is a hard problem, but it's by no means an impossible problem. Plus, how imperfect is the current system? It's entirely broken."

- Emin Gün Sirer, Co-Director, Initiative for Cryptocurrencies and Smart Contracts, Cornell University, 2019

Source: Wired

Digital ledger tech adds security and privacy

Digital ledger technology creates a system of authentication keys with the aim of letting an individual retain control over their identity and to reduce the risk of identity theft.



Source: Citi Ventures

Decentralized digital identities

Bitkey provides distributed key technology.

The company is developing a digital key platform to manage individual online authentication.

Founded in August 2018, Bitkey offers its distributed ledger technology to users as a subscription. It currently supports applications such as smart lock technology, where a digital key is used to unlock the door to a hotel room or home.

Investors include Goldman Sachs, Global Brain Corporation, and 31VENTURES, among others.

Most recent financing: $11.3M Series A (1/24/2020)

Total disclosed funding: $57M

Location: Tokyo, Japan

Evernym is an open-source provider of decentralized identity software.

The company offers 3 main products that support the issuance, verification, and storage of digital credentials.

Evernym created the Sovrin Foundation in 2016 to serve as the public ledger infrastructure and to support the adoption of decentralized identity solutions. The company also created an open-source codebase called Hyperledger Indy, as well as identifier standards in collaboration with the W3C Credentials Community Group.

Investors include Barclays Ventures, Medici Ventures, and Alumni Ventures Group, among others.

Most recent financing: $6M Seed (9/26/2019)

Total disclosed funding: $15.3M

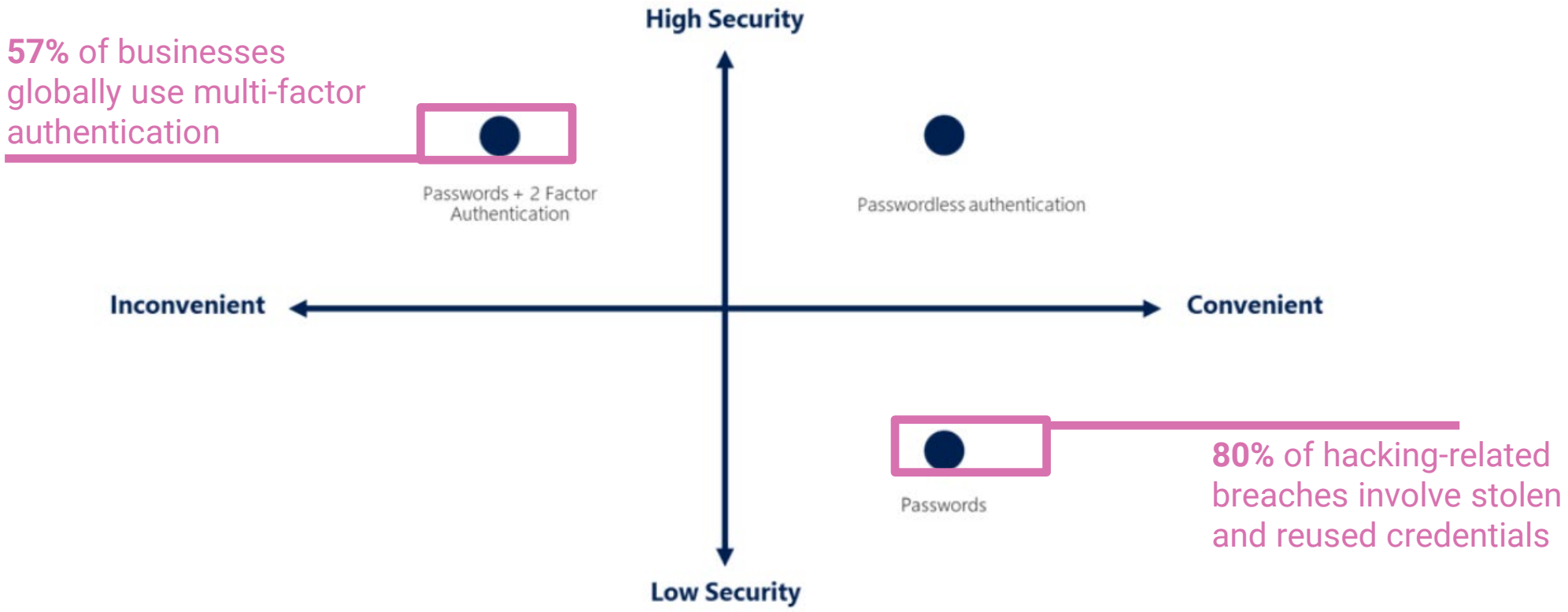
Location: Draper, UT

Password-less verification

Passwords are burdensome and insecure

Passwords and secondary authentication measures burden customers and employees while simultaneously representing a security risk for companies.

Password security vs. convenience



CBINSIGHTS Source: Microsoft, Lastpass

"Over time, market forces will make the password less and less interesting, **less viable, and less effective.**"

- Brett McDowell, Executive Director, The FIDO Alliance, 2019

Source: The Verge

Passwords can be replaced

Startups are looking to deliver secure alternatives to passwords that improve the user experience.

A password-less verification process

End user/device

The properties of the device or user (e.g., certificates, biometrics) can serve as means of identification.

Authentication/verification

AI-enabled technologies, such as facial or voice recognition, improve the efficacy of verification.

Access

Password alternatives create a more secure and seamless process for accessing accounts and resources.

Password-less verification

BEYOND IDENTITY

Beyond Identity aims to eliminate the need for passwords with personal certificates.

The company extends the chain of trust, or transit layer security, from the web to end users and devices with personal certificates.

Founded by serial entrepreneur Jim Clark and technology veteran Tom Jermoluk, Beyond Identity's self-signed X.509 certificates verify device security with the aim of removing the need for a password.

Investors include New Enterprise Associates and Koch Disruptive Technologies.

Most recent financing: $30M Series A (4/8/2020)

Total disclosed funding: $30M

Location: New York, NY

passbase

Passbase provides identification verification software, including tools for embedding document and biometric verification capabilities into corporate applications.

The company offers its solution as an API with scaled verification methods like SMS, biometric login, and liveliness detection to meet risk requirements.

Investors include Cowboy Ventures, Kleiner Perkins Caufield & Byers, and Alphabet, among others.

Most recent financing: $3.6M Seed (9/25/2019)

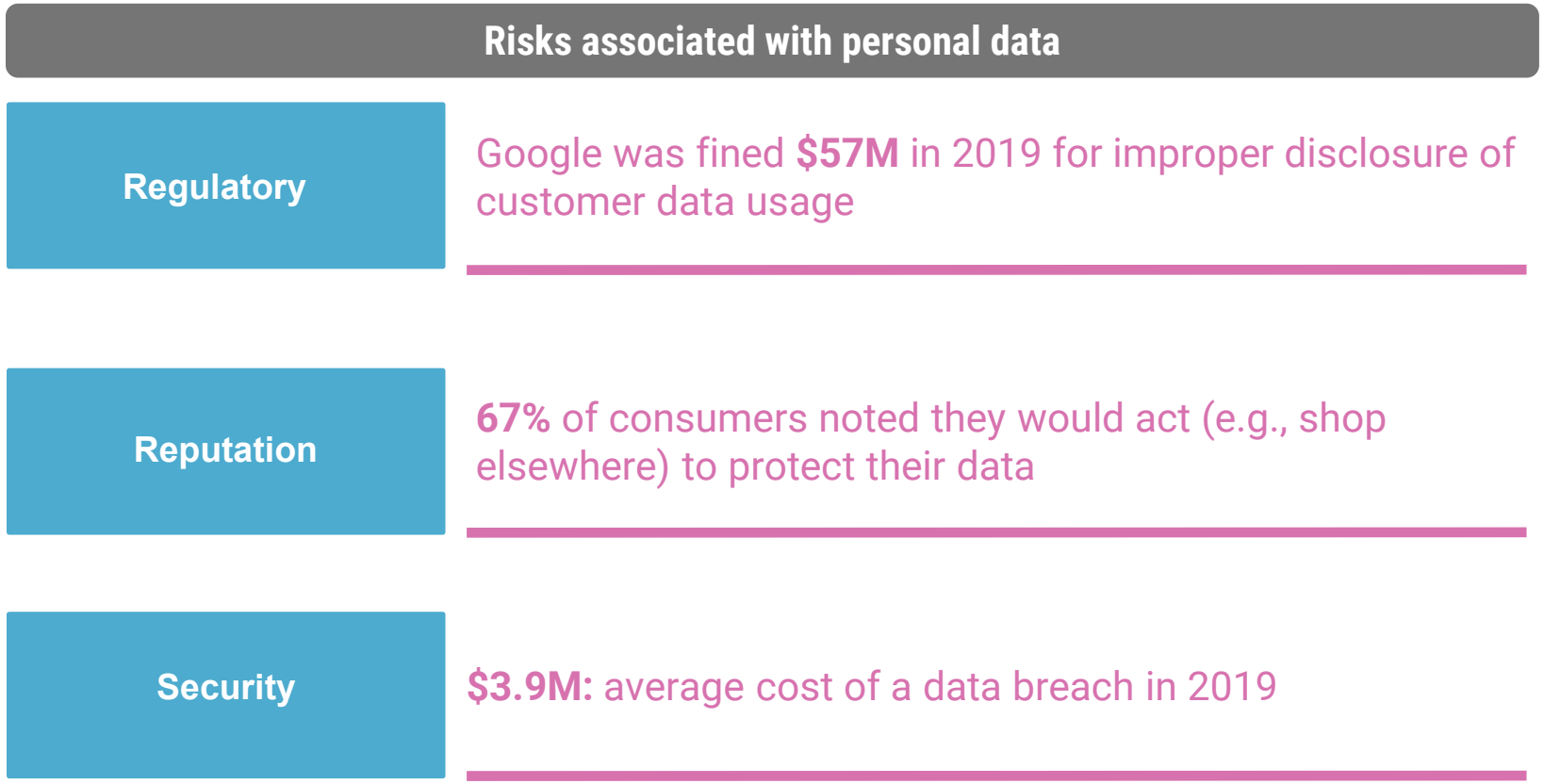
Total disclosed funding: $4.2M

Location: San Francisco, CA

Privacy by design

Storing and using personal data is risky for companies

Collecting, storing, and using personally identifiable data has regulatory risk (e.g., GDPR and the California Consumer Privacy Act), security risk, and reputation risk, with consumers skeptical of how companies use the data.



Source: Cisco; Reuters; IBM

"Instead of thinking like 'data owners,' companies **must act as 'data custodians'** who protect personal information and use it only with a customer's best interests in mind"

GUSTO

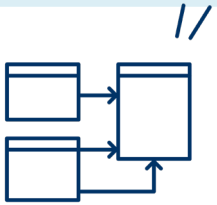
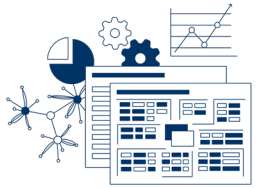
- Fredrick "Flee" Lee, chief information security officer at Gusto, 2020

Source: HBR

Privacy-first solutions are emerging

Privacy-focused solutions have entered the market to support companies hit by a wave of personal data, breaches, and regulation. From data ingestion to user data requests, new solutions are supporting a privacy-by-design approach.

Privacy-first data solutions

Data ingestion	Data management	Data usage	Regulatory compliance
			
Consent management	**Personal data mapping and protection**	**Data anonymization/ de-identification**	**Automated data subject request fulfillment**
Tools for collecting and managing user consent of data collection and usage	Tools for identifying and mapping personal data across channels and ensuring adequate protection	Tools that enable the use or analysis of data without exposing user identity	Tools that help companies comply with regulations that require users have access to their data

Privacy by design

TRANSCEND

Transcend is a data privacy company that aims to help users control their data.

It offers companies tools to comply with privacy regulations and build trust with customers.

Founded in 2017, Transcend's privacy center offering supports data subject requests (DSR) and consent management to support customers control how their personal data is used. The company counts Robinhood and Patreon among its customers.

Investors include Index Ventures and Accel.

Most recent financing: $25M Series A (6/10/2020)

Total disclosed funding: $29M

Location: San Francisco, CA

CONCENTRIC

Concentric provides a data discovery, monitoring, and mapping solution that classifies unstructured data.

Concentric finds personally identifiable information to help fulfill regulatory requirements and avoid reputation-damaging data breaches or disclosures.

Investors include Homebrew, Clear Ventures, and Engineering Capital, among others.

Most recent financing: $7.5M Series A (1/29/2020)

Total disclosed funding: $7.5M

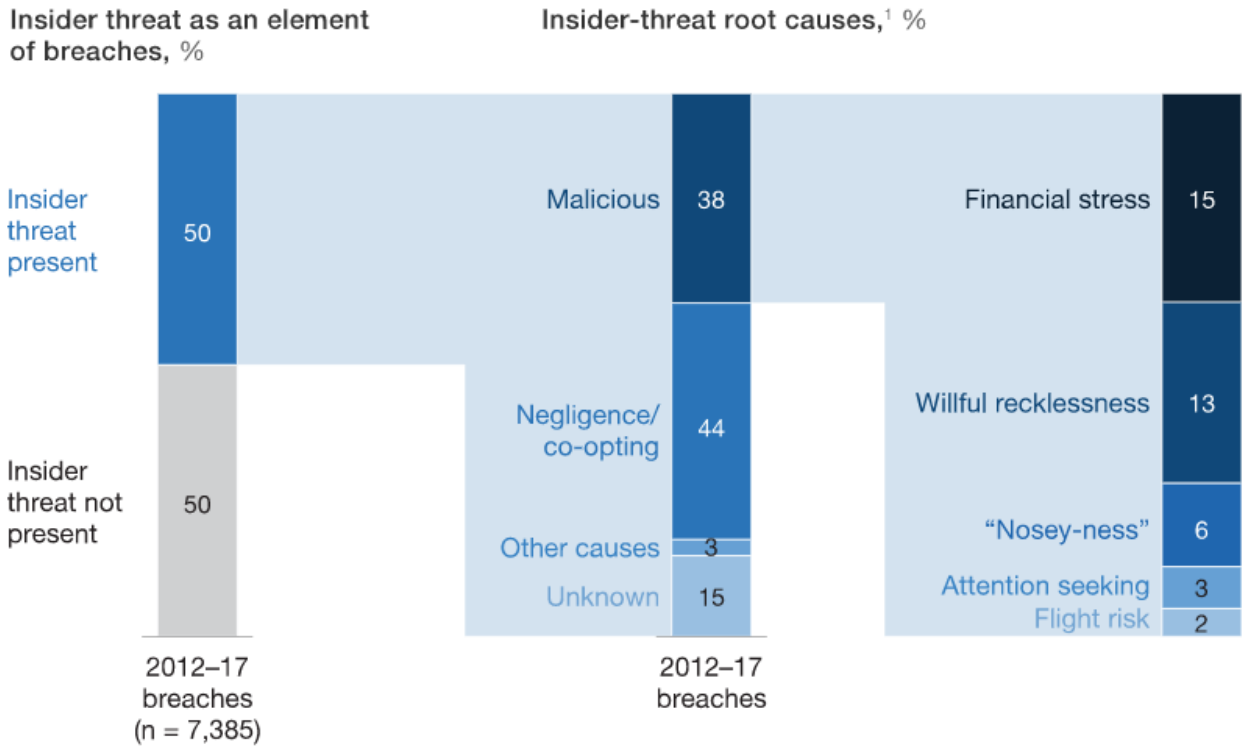
Location: San Jose, CA

Anomalous behavior detection

Humans are the ultimate security threat

Cybersecurity protects computer systems and networks from harm. However, human behavior is an unknown variable in cybersecurity. Employees who maliciously or inadvertently share sensitive information or enable access to company systems pose an inside threat.

Insider threat is a factor in 50% of breaches



[1]Figures are approximate and may not sum, because of rounding.

Source: McKinsey

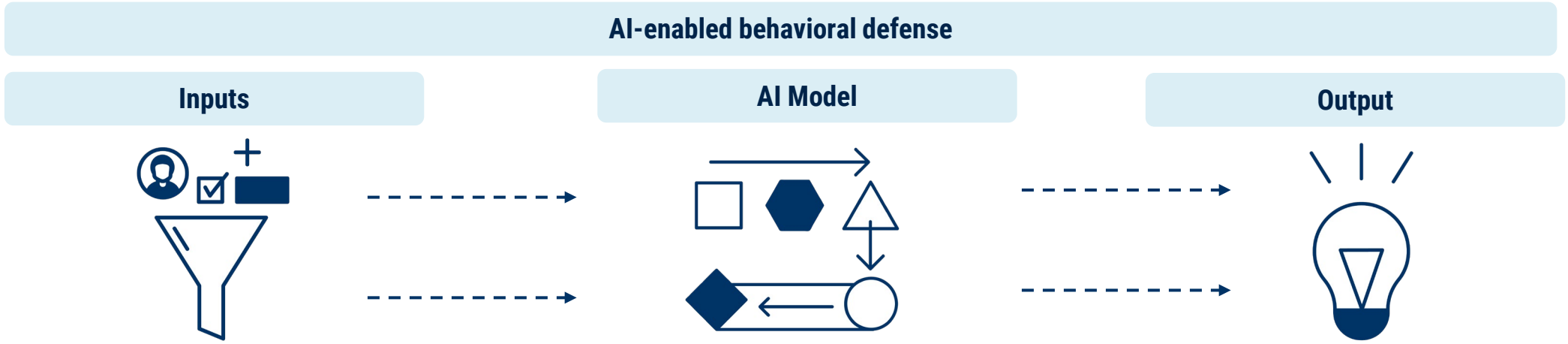
"…it's almost always **human error** that enables attackers to access encrypted channels and sensitive information. Staff can make a variety of mistakes that **put their company's data or systems at risk**."

- Oz Alashe, CEO of CybSafe, 2020

Source: Infosecurity Magazine

Analyzing human behavior offers a defense

Advances in machine learning and access to massive datasets provide insight into normal and abnormal human behavior. Identifying abnormal behavior — inside or outside the company— allows companies to direct their resources to correcting behaviors or mitigating threats.



Anomalous behavior detection

Abnormal Security is an email security provider.

The company uses machine learning technology to analyze email content and context to help prevent email attacks, such as phishing.

Abnormal Security was founded in 2018 by two former Twitter employees. In 2019, the company appointed a chief product officer and chief revenue officer from Amazon and Proofpoint, respectively.

Investors include Greylock Partners.

Most recent financing: $24M Series A (11/18/2019)

Total disclosed funding: $24M

Location: San Francisco, CA

AWAKE

Awake is a network traffic security company.

It monitors users, devices, and applications across a network to understand their behavior and detect and respond to threats.

The company was launched in 2014 by three cybersecurity veterans coming from McAfee, HP, and Cylance. Since its founding, the company has filed several patents for detecting malicious activity.

Investors include Greylock Partners, Bain Capital, and Liberty Global Ventures, among others.

Most recent financing: $36M Series C (4/15/2020)

Total disclosed funding: $67.2M

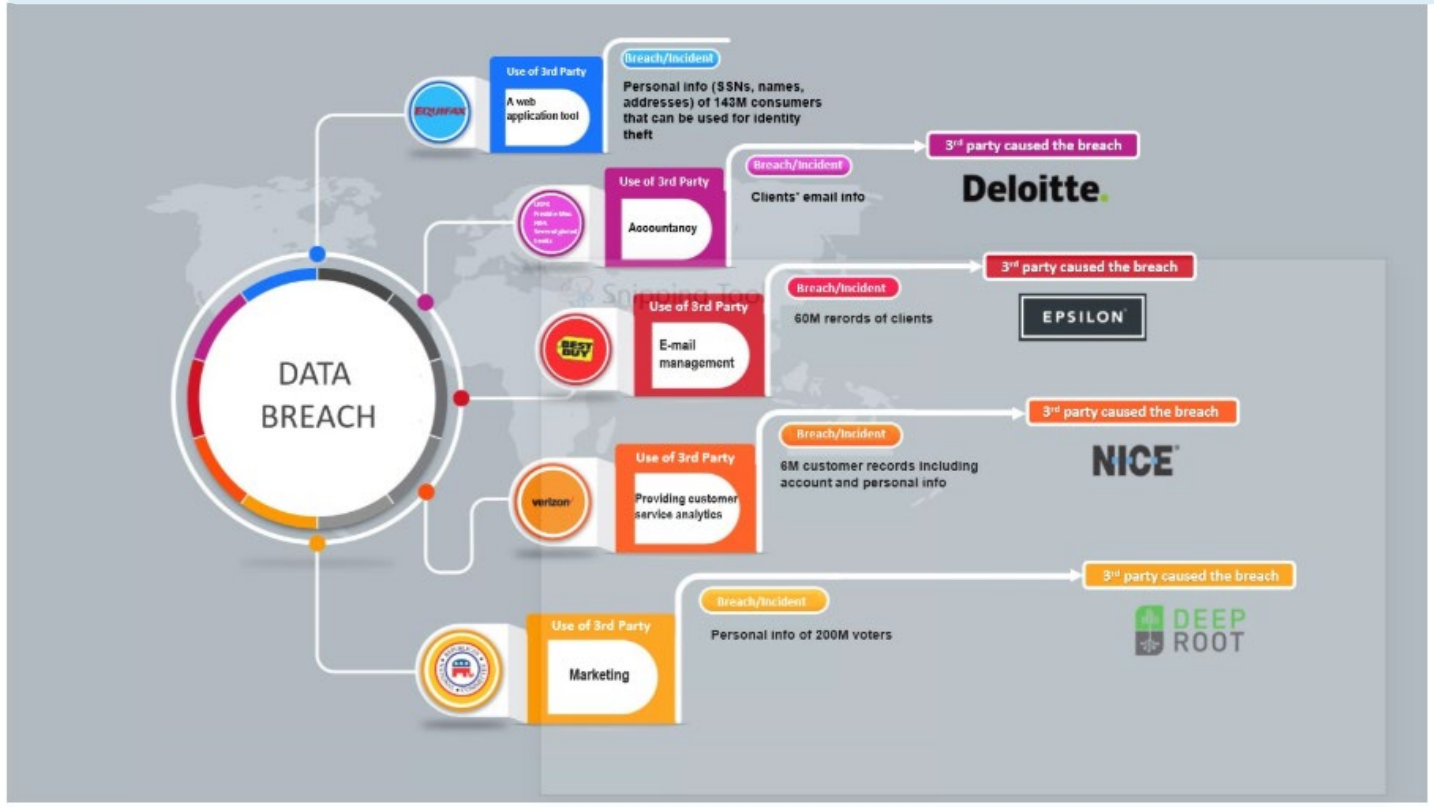
Location: Santa Clara, CA

Third-party risk management

Threats extend down the supply chain

Many companies rely on third parties — like contractors, vendors, and consultants — to deliver final products to customers. Exchanging information or providing network access to third parties with inferior security practices represents a vulnerability.

Notable data breaches caused by a third party



44% of data breaches are caused by a third party

Only 15% of these vendors informed impacted parties of the breach

Source: Normshield; Becker's Health IT

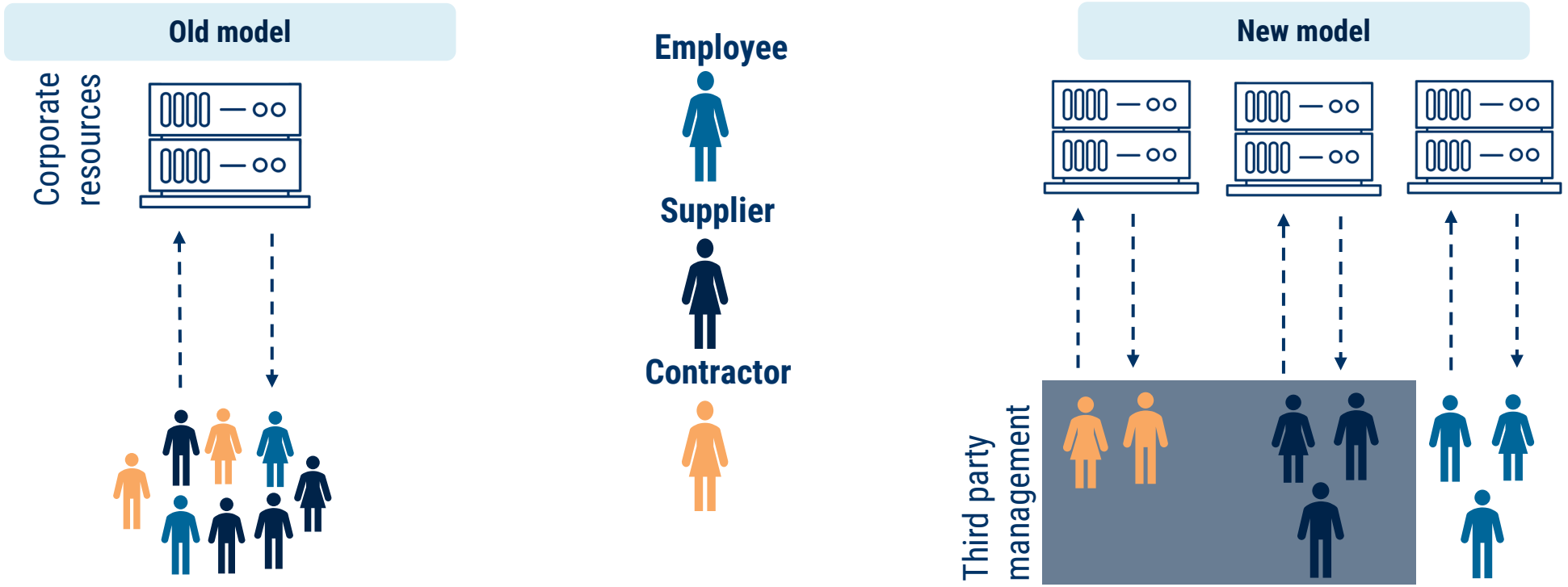
“The implications [of third-party breaches] are stark and the potential impacts very real.”

- Steve Durbin, managing director of the Information Security Forum, 2019

Source: WSJ

A new way to manage third-party access

To help reduce third-party risk, startups are developing solutions for managing access to corporate systems and data as well as on-boarding and off-boarding. These new solutions will augment or replace the traditional approach to risk management.



Indiscriminate access to shared corporate resources once approved

Segmentation by role and controlled access to corporate resources

Third-party risk management

axis security

Axis Security uses technology to give third-party users secure access to private, company applications without risk of compromising the network.

Founders Dor Knafo and Gil Azrielant started Axis Security in 2018, having both come from Israel's military cybersecurity unit.

In April 2020, the company announced a partner program and its first partner, value-added reseller BlackLake Security.

Investors include Ten Eleven Ventures and CyberStarts, among others.

Most recent financing: $14M Series A (3/17/2020)

Total disclosed funding: $17M

Location: San Mateo, CA

SecZetta

SecZetta provides third-party identity management.

The company offers a system of record for third parties that can manage user privileges and vendor certification.

SecZetta announced several partnerships in the past year with service providers such as SystemDomain and technology providers like OneLogin.

Its client list includes a diverse range of companies from Mayo Clinic to Cargill.

Investors include Rally Ventures and ClearSky.

Most recent financing: $10M Series A (9/12/2019)

Total disclosed funding: $10M

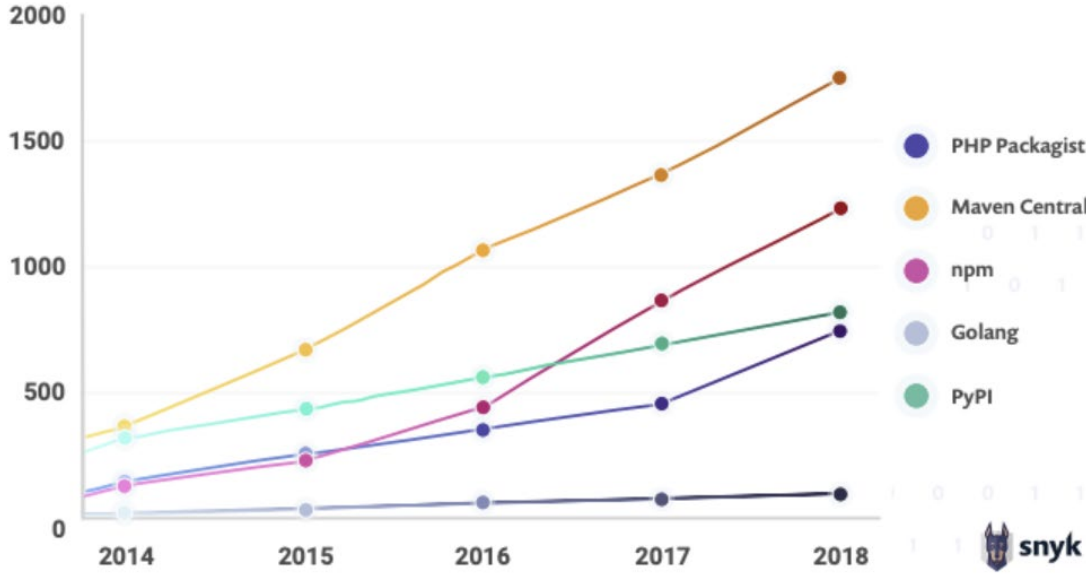
Location: Newport, RI

Patch protection

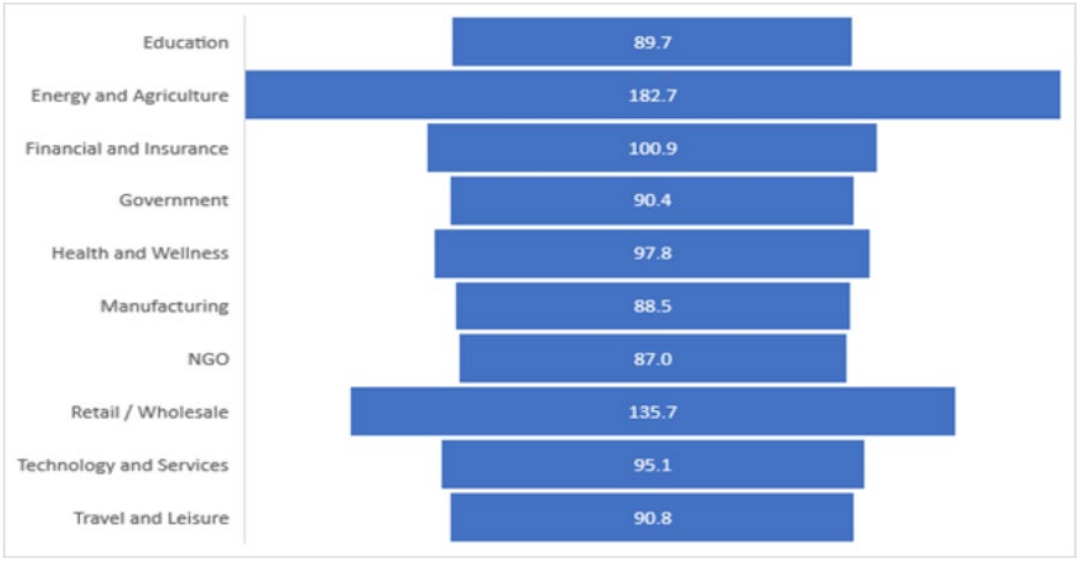
Software vulnerabilities are overwhelming

The number of vulnerabilities in open-source software code has risen consistently over the last several years. In June 2020, Microsoft disclosed **129 vulnerabilities** — a record high — during its monthly "Path Tuesday" update.

New vulnerabilities each year by open-source ecosystem



Avg. number of days to patch vulnerability by industry



Source: ZDNet; Syxsense; Snyk; Outpost24

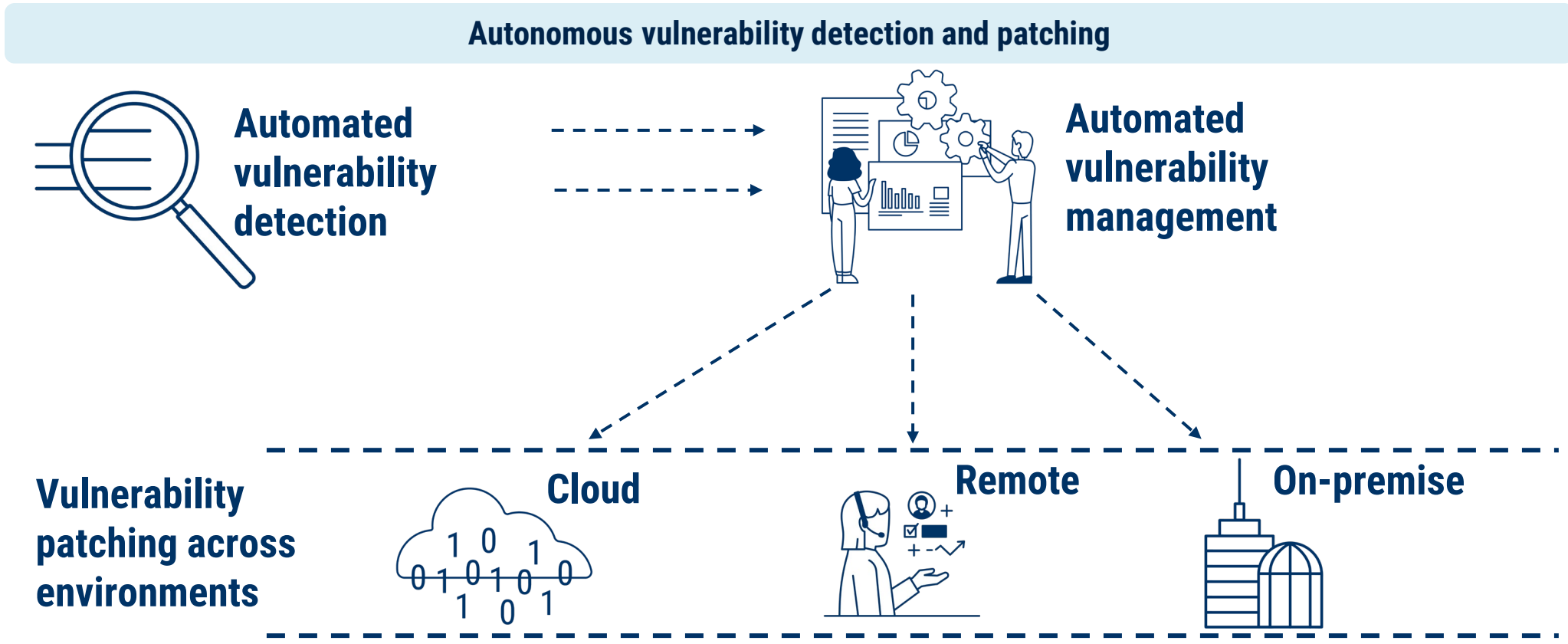
"Managing updates on so many different pieces of software, on so many systems, can be overwhelming and effective **updates may slip through the cracks**."

- Peter Romness, Cisco Cybersecurity Solutions Lead - US Public Sector, 2019

Source: GovTech

Autonomous patching could help

Startups are creating **tech for autonomously identifying and patching software vulnerabilities**. Companies with limited cybersecurity resources often look for software patching solutions that reduce the associated administrative burden.



Patch protection

Automox offers tools for automating endpoint patching.

The product manages and applies operating system and software patches through the cloud.

Automox was founded in 2015 and counts Greyhound, Yale University, NASA, and Xerox among its customers.

The company announced a partnership with endpoint security provider CrowdStrike in April 2020.

Investors include CRV, Koch Disruptive Technologies, and Blue Note Ventures, among others.

Most recent financing: $30M Series B (1/31/2020)

Total disclosed funding: $43.3M

Location: Boulder, CO

ForAllSecure offers an autonomous tool for finding and resolving software vulnerabilities.

The company uses a technique called “advanced fuzzing” to test and detect software vulnerabilities in code.

ForAllSecure first demonstrated its technology in 2016 when it won DARPA’s Cyber Grand Challenge. In May 2020, the company announced it was awarded a contract up to $45M by the US Department of Defense to secure its systems.

Investors include DARPA and New Enterprise Associates.

Most recent financing: $14.7M Unattributed VC (3/27/2019)

Total disclosed funding: $16.7M

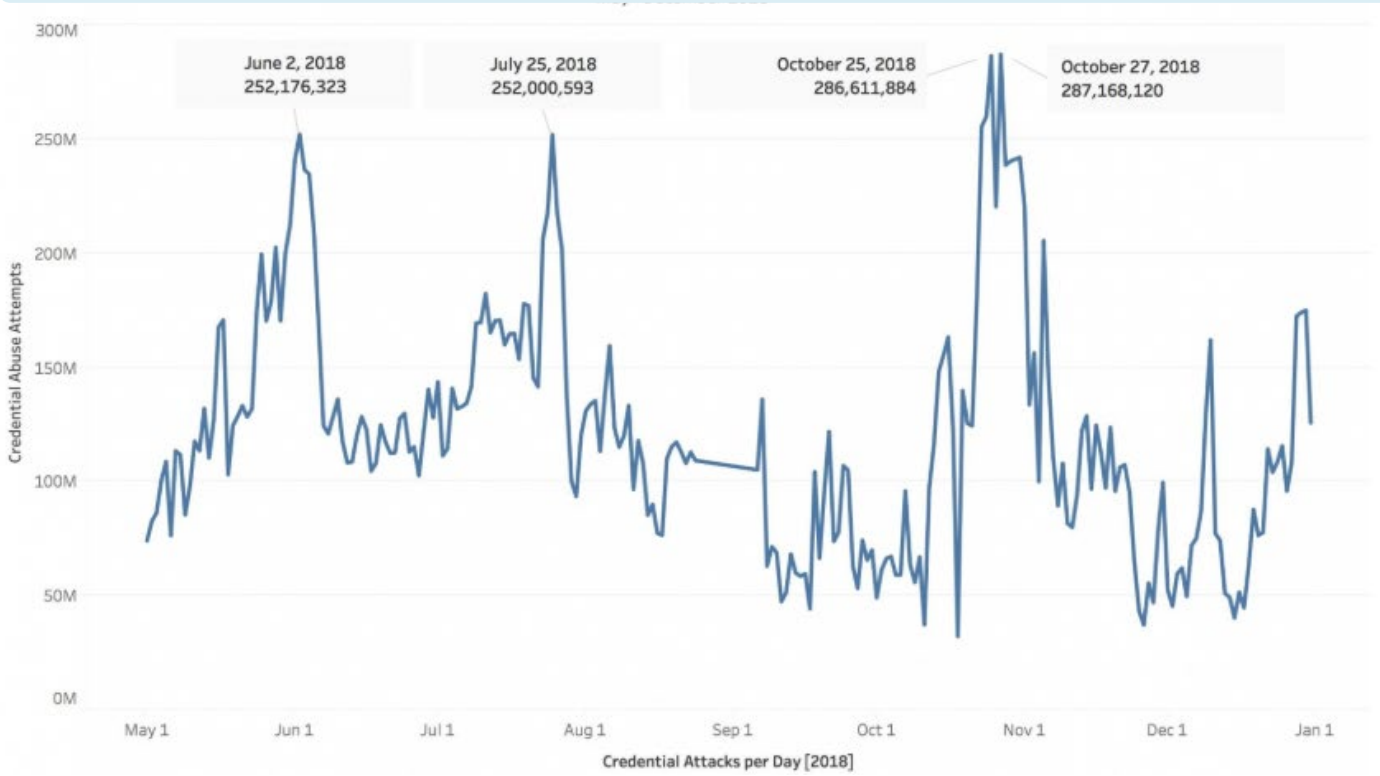
Location: Pittsburgh, PA

Credential stuffing defense

Online fraud is automated and well-sourced

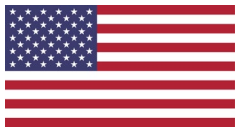
Companies and consumers face a mounting challenge of online fraud, or “credential stuffing.” This type of attack occurs when a hacker purchases inexpensive user credentials from past data breaches and automates the log-in process across hundreds of platforms.

Daily credential abuse from May to December 2018



Source: Bleeping Computer

"Economic gain through **theft, fraud, and deception**. One study estimates that cybercrime revenues hit **$1.5T** in 2018. This is an entire shadow economy **larger than many legitimate nation-states**."



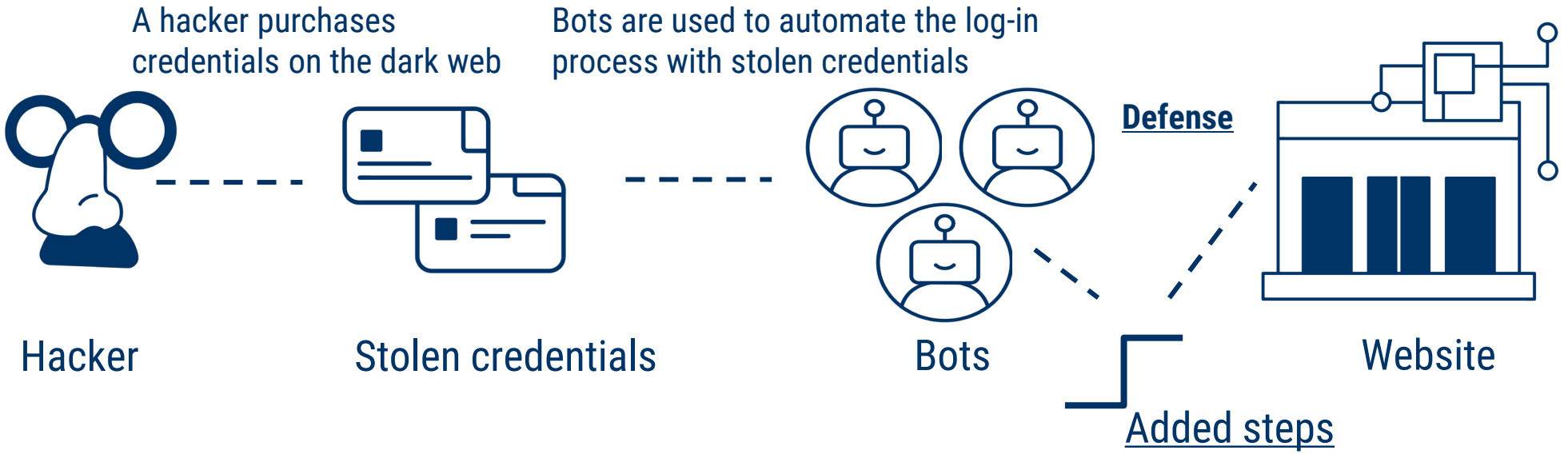
- Sumit Agarwal, former US deputy assistant secretary of defense, 2019

Source: TechRepublic

Startups are reducing economic incentives

By developing solutions to identify bots and create burdensome authentication processes for them, startups are making credential stuffing more difficult and deterring hackers.

Breaking down a credential stuffing attack



Startups identify malicious activity and add layers of complexity to the authentication process, increasing the resources required for the attack and diminishing the economic incentive.

Credential stuffing defense

Arkose Labs

Arkose Labs fights online fraud by detecting and thwarting malicious web traffic.

The company uses risk-based profiling to uncover fraud and creates an authentication process intended to eliminate the economic incentives of credential stuffing.

Founded in 2016, the company counts several large companies among its customers, including Electronic Arts and Microsoft. In 2019, it reported a 400% year-over-year increase in sales.

Investors include US Venture Partners, M12, and PayPal Ventures, among others.

Most recent financing: $22M Series B (3/24/2020)

Total disclosed funding: $29.7M

Location: San Francisco, CA

kasada

Kasada helps protect against credential stuffing by identifying automated web traffic or bots.

The company uses algorithms to detect signs of automation in web traffic and assigns asymmetric cryptographic challenges to the traffic deemed malicious.

Kasada was founded in 2015 and received In-Q-Tel's first investment in Australia. With new funding from Ten Eleven Ventures, the company plans to expand into the US.

Investors include Ten Eleven Ventures, In-Q-Tel, and Reinventure, among others.

Most recent disclosed financing: $10M Series B (6/16/2020)

Total disclosed funding: $16.7M

Location: New South Wales, Australia

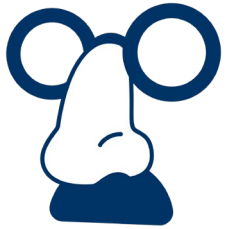
Zero-trust networking

Networks cannot be trusted

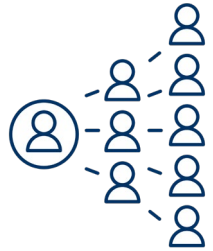
Company networks that look to account for remote workers, connected devices, and cloud technologies are vulnerable to attack. The users and assets using the network, therefore, cannot be automatically trusted.

Networks are too complex to ensure security

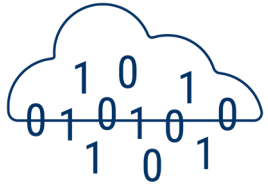
Remote work



Sophisticated attackers

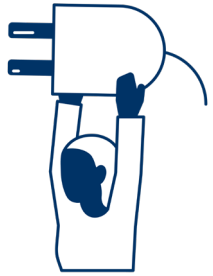


More users



Cloud computing

More devices



Limited cybersecurity resources

"So the fact that you built an environment where you're **trusting all of your insiders** is really **not going to help you** and not going to allow you the capabilities that you need."

- Grant Schneider, Senior Director for Cybersecurity Policy at National Security Council, 2020

Source: FedTech

A zero-trust approach reduces the risk of breach

Startups are developing cloud-based solutions for monitoring and authenticating traffic on company networks. Access to data and resources is not assumed for users on the network — instead, it must be validated.

Zero-Trust Architecture Framework: Devices on the network must prove themselves trustworthy

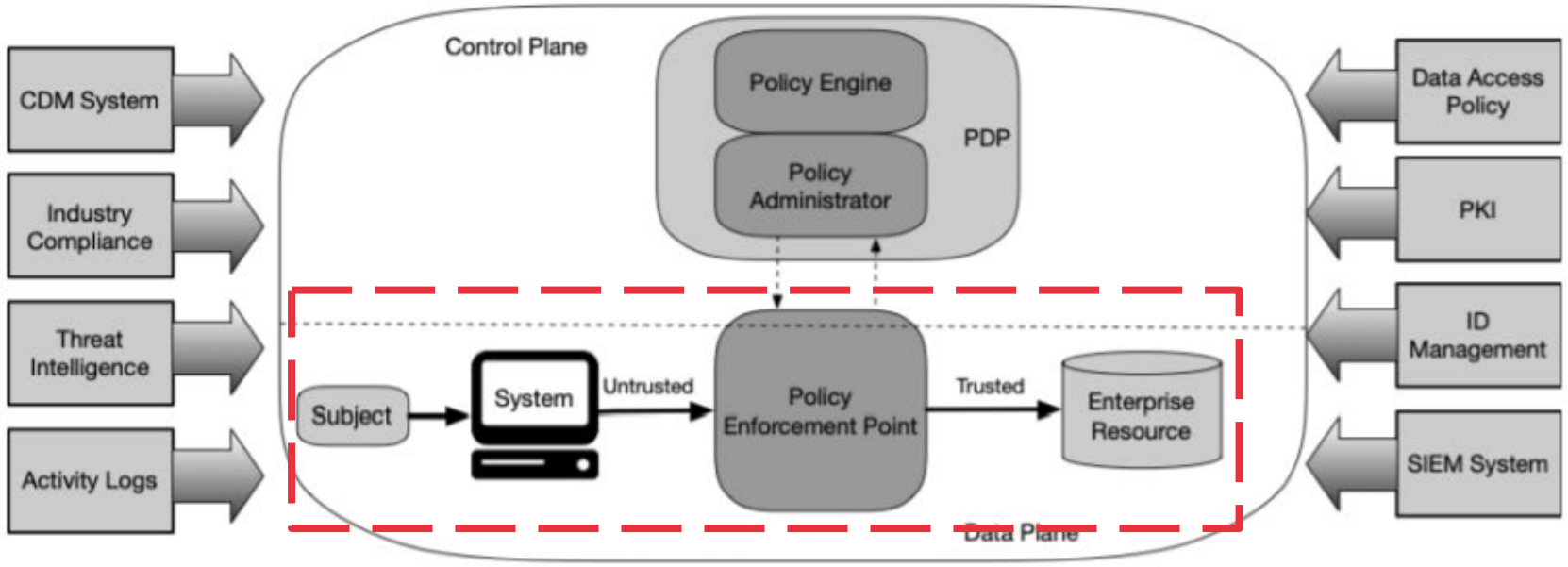


Figure 2: Core Zero Trust Logical Components

Source: NIST

Zero trust networking

perimeter 81

Perimeter 81 delivers network security services like policy-based segmentation and monitoring in the cloud.

Perimeter 81 was founded in 2018 by the creators of SaferVPN, which was sold to J2 Global in 2019. In 2019, Perimeter 81 reportedly grew 450% and was included in Deloitte's Technology Fast 500™ for EMEA list.

Investors include Toba Capital, SonicWall, and Spring Ventures.

Most recent financing: $4.5M Series A (3/11/2020)

Total disclosed funding: $19.5M

Location: Tel Aviv, Israel

ZERO. Networks

Zero Networks defines, enforces, and adapts network access policies to create a zero-trust model.

The company was founded in 2019, and its network access orchestrator became available in Q1'20.

Zero Networks was among 3 companies selected to present at the 2020 RSA conference's Launch Pad event.

Investors include PICO Partners and F2 Capital, among others.

Most recent disclosed financing: $4.7M Series A (2/20/2020)

Total disclosed funding: $4.7M

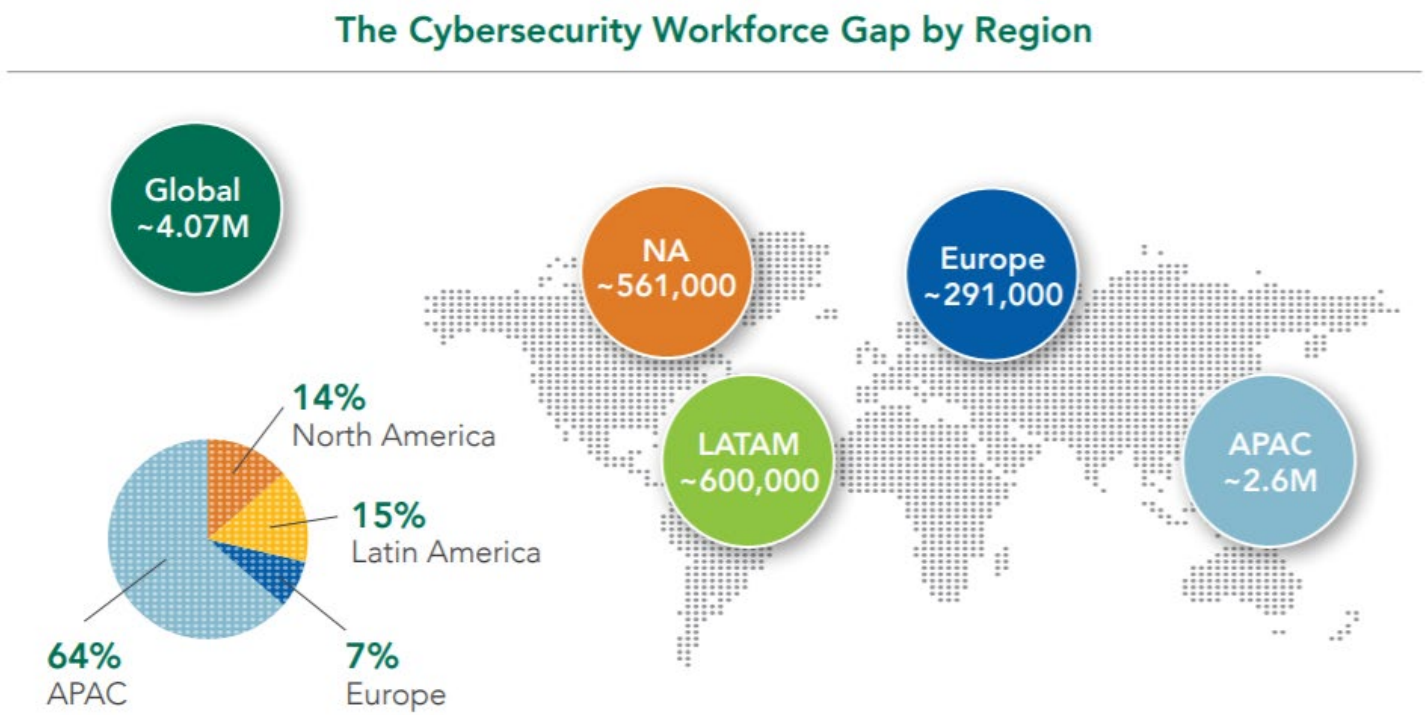
Location: Tel Aviv, Israel

Bot-assisted defense

Cybersecurity needs more qualified people

There is a global shortage of qualified personnel available for employment in the cybersecurity industry — estimates say **the world is short roughly 4M cybersecurity professionals**.

Number of additional cybersecurity personnel needed around the world, 2019



Source: (ISC)² Cybersecurity Workforce Study, 2019

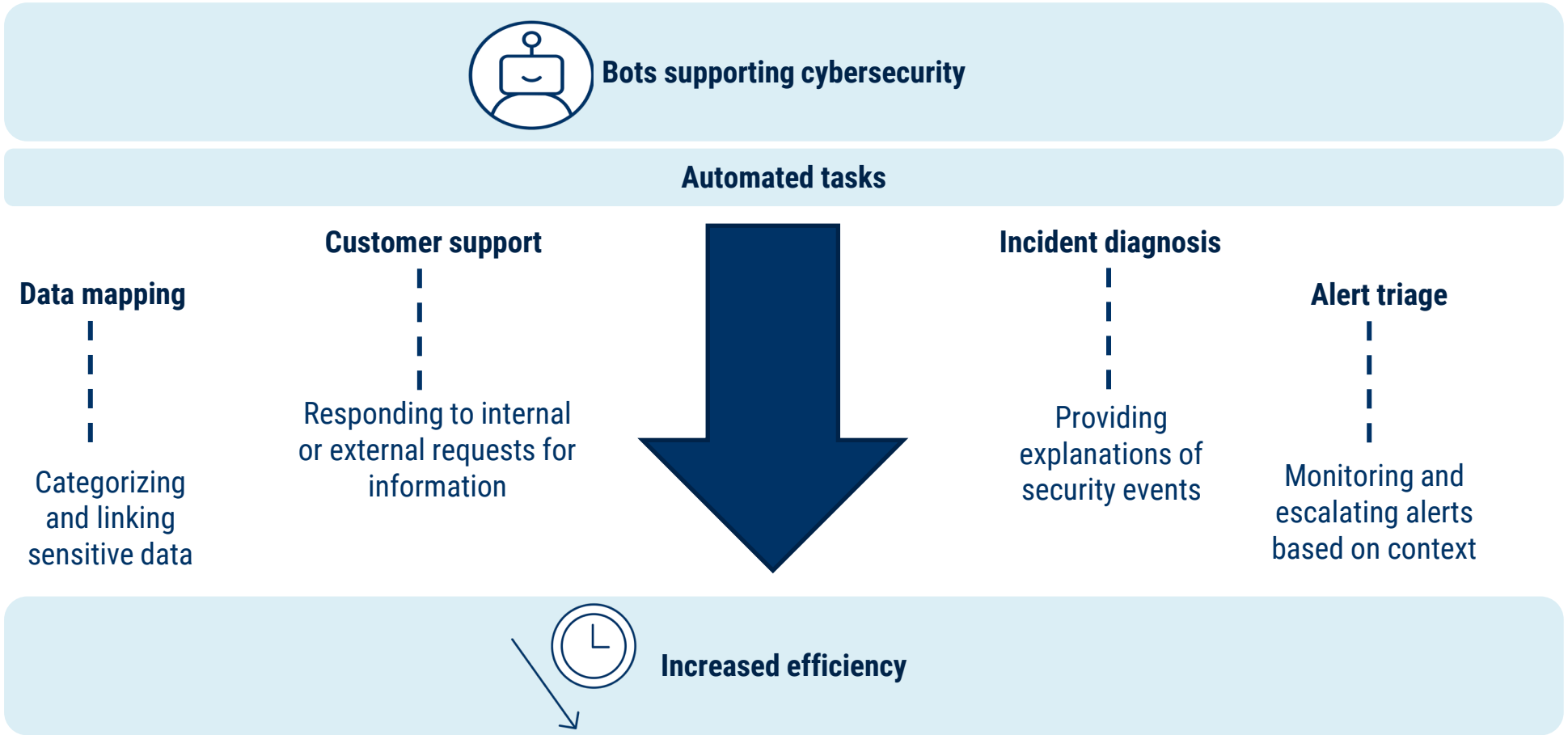
"Although automation and machine learning will **improve efficiency**, human expertise, logical thinking, and creativity will be **further valued to deploy and effectively use new technology**, as well as deter against emerging threats."

- Caroline Wong, Chief Strategy Officer at Cobalt.io, 2020

Source: CIO

Bots empower cybersecurity professionals

Startups are offering bots to reduce the administrative burden placed on over stretched cybersecurity professionals.



Bot-assisted defense

SECURITI.ai

Securiti.ai provides automated data privacy software.

The company offers an intelligent bot (Auti) to scan, identify, link, and respond to question about personal data.

The company was launched in 2019 by cybersecurity veteran Rehan Jalil, who previously led Symantec's cloud security business.

Securiti.ai was named most innovative startup at the 2020 RSA conference.

Investors include Mayfield Fund and General Catalyst.

Most recent financing: $50M Series B (1/28/2020)

Total disclosed funding: $81M

Location: San Jose, CA

respond

Respond leverages robotic decision automation technology to provide companies with a bot that monitors and triages security events.

Launched out of stealth in 2017, Respond was founded by Mike Armistead, who previously created and sold cybersecurity company Fortify to HP in 2010.

In 2020, the company announced a partnership with Agio. As part of the deal, Agio will include Respond's solution as part of its product offering.

Investors include Foundation Capital, CRV, and ClearSky.

Most recent financing: $20M Series B (5/13/2019)

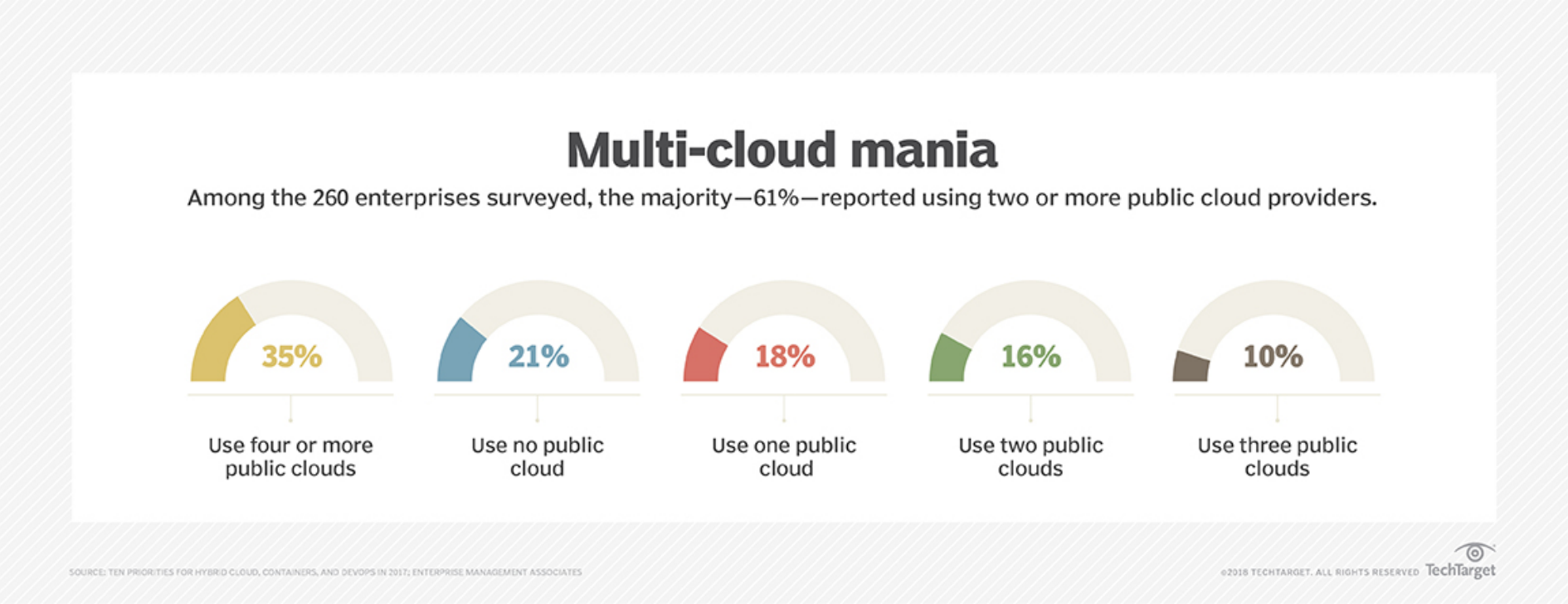
Total disclosed funding: $32M

Location: Mountain View, CA

Multi-cloud security

Companies embrace a multi-cloud environment

Companies moving to the cloud are often choosing to use multiple public cloud providers. Some are also deciding to keep certain assets on a private cloud. These multi-cloud set ups create administrative and security challenges.



Source: TechTarget

"Security remains one of the biggest concerns among multi-cloud users. **The larger the cloud environment, the greater the potential for vulnerability.**"

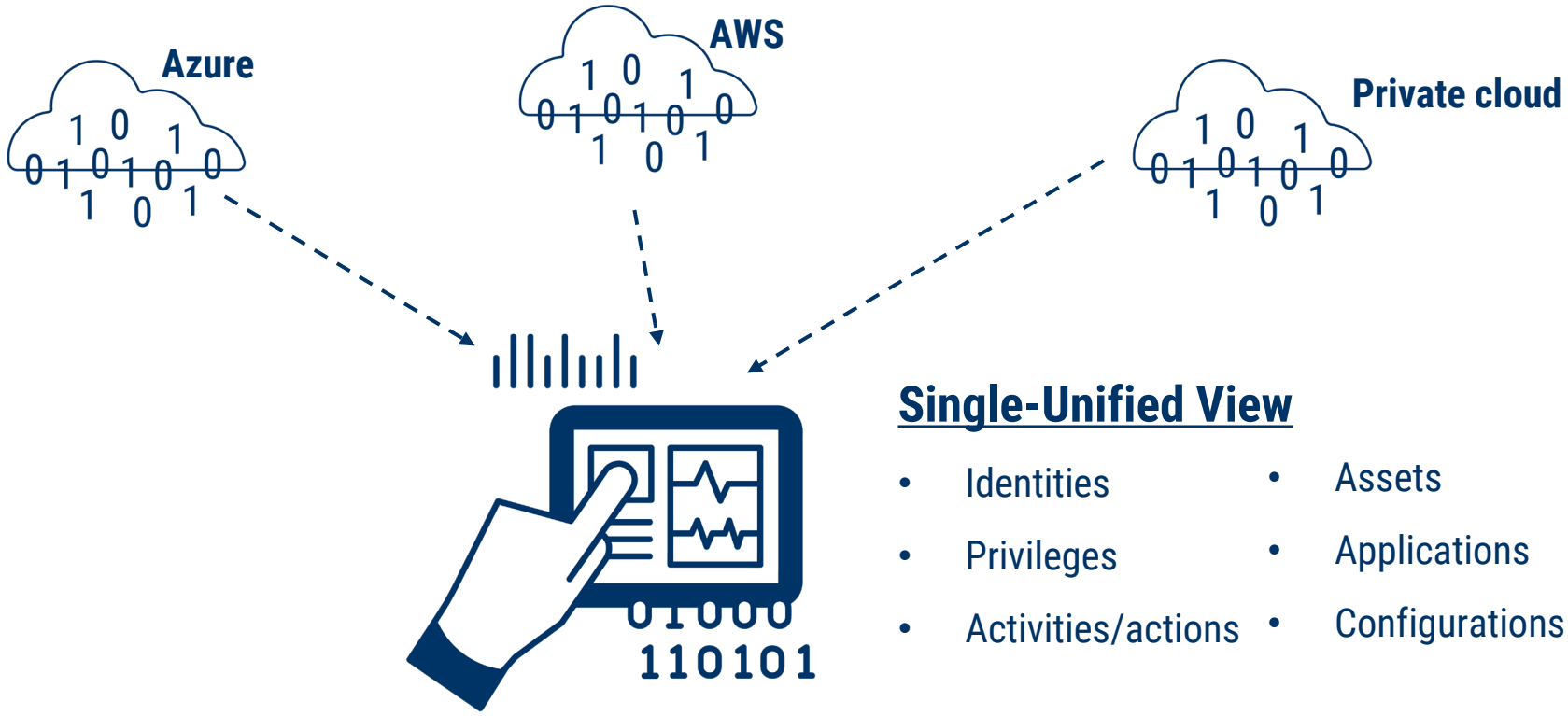
- Charles Phillips, Chairman of Infor's Board of Directors, 2020

Source: Personal Blog

Startups are unifying security across clouds

Startups are rising to help enterprises protect their various cloud environments. By providing visibility into the infrastructure across clouds, companies can identify security vulnerabilities and maintain a unified security posture.

Multi-cloud security via visibility and control



Single-Unified View

- Identities
- Privileges
- Activities/actions
- Assets
- Applications
- Configurations

Multi-cloud security

CLOUDKNOX

CloudKnox monitors activity across multi-cloud environments.

It provides a single view across public and hybrid clouds to help identify and resolve security violations.

CloudKnox takes an identity-based approach to cloud security, ensuring only appropriate users gain access to cloud resources.

In 2019, the company was granted 2 patents for its access control and threat identification technology.

Investors include ClearSky, Foundation Capital, and Dell Technologies Capital, among others.

Most recent financing: $12M Series B (1/23/2020)

Total disclosed funding: $22.8M

Location: Sunnyvale, CA

orca security

Orca Security offers a tool for scanning multi-cloud environments.

The company provides visibility into cloud environments — including AWS, Google Cloud, and Azure — at the workload level to identify misconfigurations, malware, and other risks.

Founded in 2019 by former executives of Checkpoint Software, the company reportedly plans to use its funding to double its headcount by the end of 2020.

Investors include YL Ventures, GGV Capital, and Silicon Valley CISO Investments.

Most recent financing: $20.5M Series A (5/5/2020)

Total disclosed funding: $27M

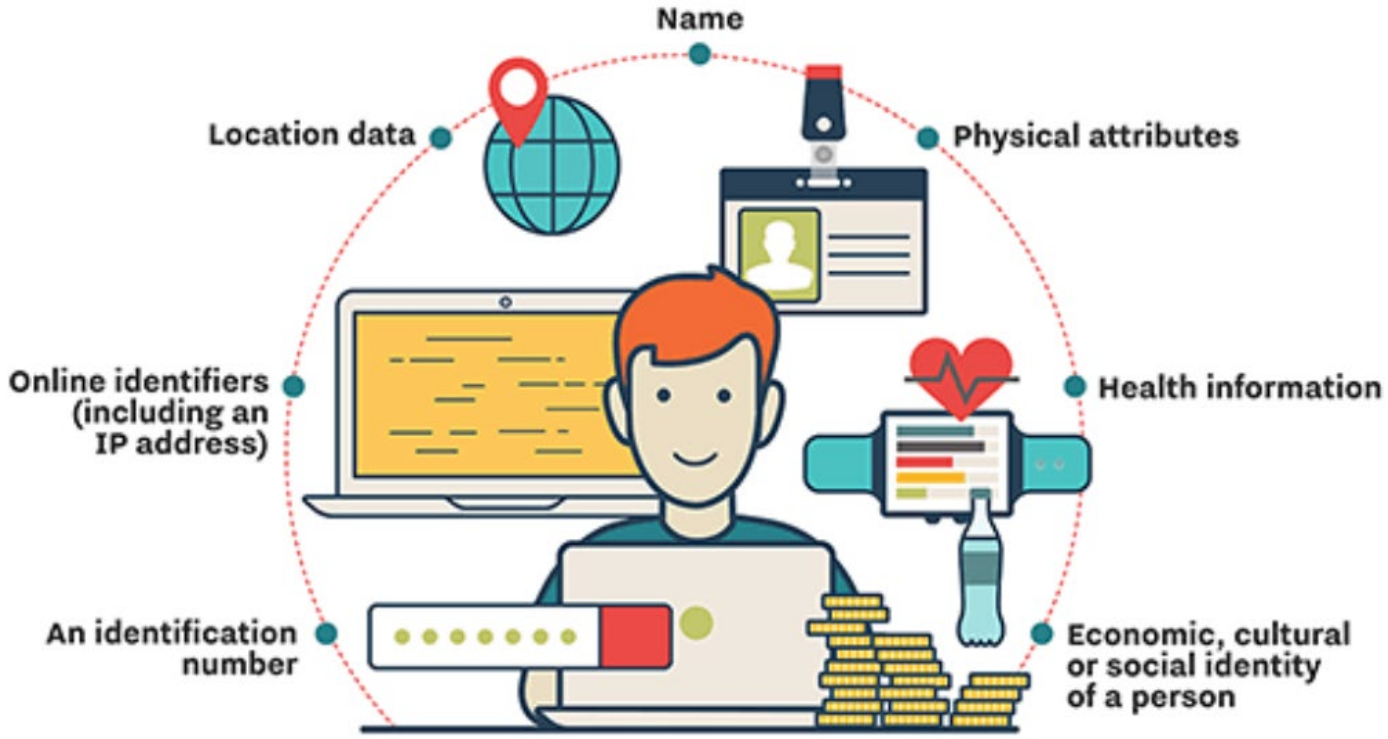
Location: Tel Aviv, Israel

Outsourced data protection

Personal data is abundant

Though valuable, data can represent a liability for companies. As data becomes increasingly abundant, companies could become overwhelmed and attract the attention of hackers.

Types of regulated personal data



1,900

The number of pieces of personal information on the Web per individual

Source: TechTarget; Vox

"Unshared data cannot be bought, sold, shared, or hacked, but **any data shared is a liability** for its owner and the provider holding it."

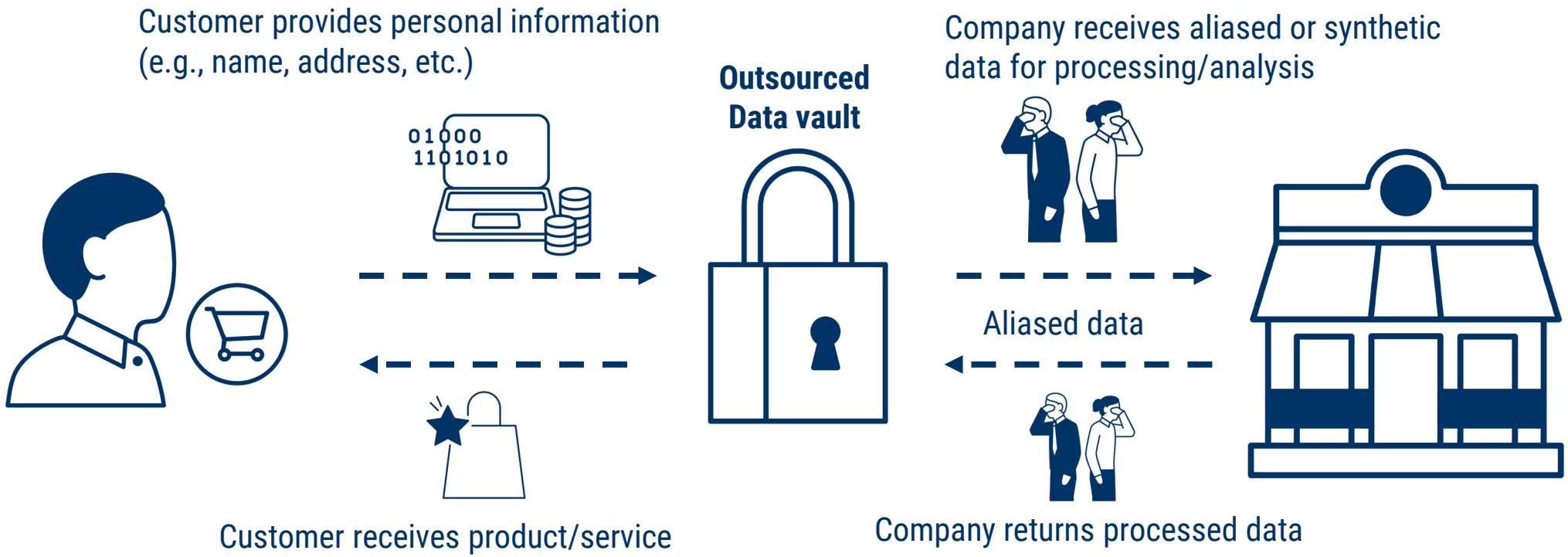
- Paul Mee and Rico Brandenburg, partners in Oliver Wyman's cybersecurity practice, 2020

Source: MIT Sloan Management Review

Outsourced data protection reduces liability

Startups are offering solutions for enterprises to off-load the risk of sensitive data. These tools enable companies to interact with the data without having to store or manage it.

Outsourced data protection



Outsourced data protection

VERY GOOD SECURITY

Very Good Security holds sensitive data for companies and provides access to the data without liability.

Founded in 2015, the company has entered partnerships with Visa, Plaid, Amazon, and others to make its offering more accessible.

Investors include Andreesen Horowitz, Goldman Sachs, and Visa Ventures, among others.

Most recent disclosed financing: $35M Series B (10/24/2020)

Total disclosed funding: $44.9M

Location: San Francisco, CA

evervault

Evervault is developing a data protection solution for developers.

The company's API-based solution is intended to allow companies to process personal data without seeing, storing, or handling it.

Despite not having a customer-ready product, Evervault has raised funding from several prominent backers.

The company was founded in 2018 by the now 20-year old winner of the BT Young Scientist Award, Shane Curran.

Investors include Sequoia Capital, Kleiner Perkins Caufield & Byers, and Index Ventures, among others.

Most recent financing: $16M Series A (5/18/2020)

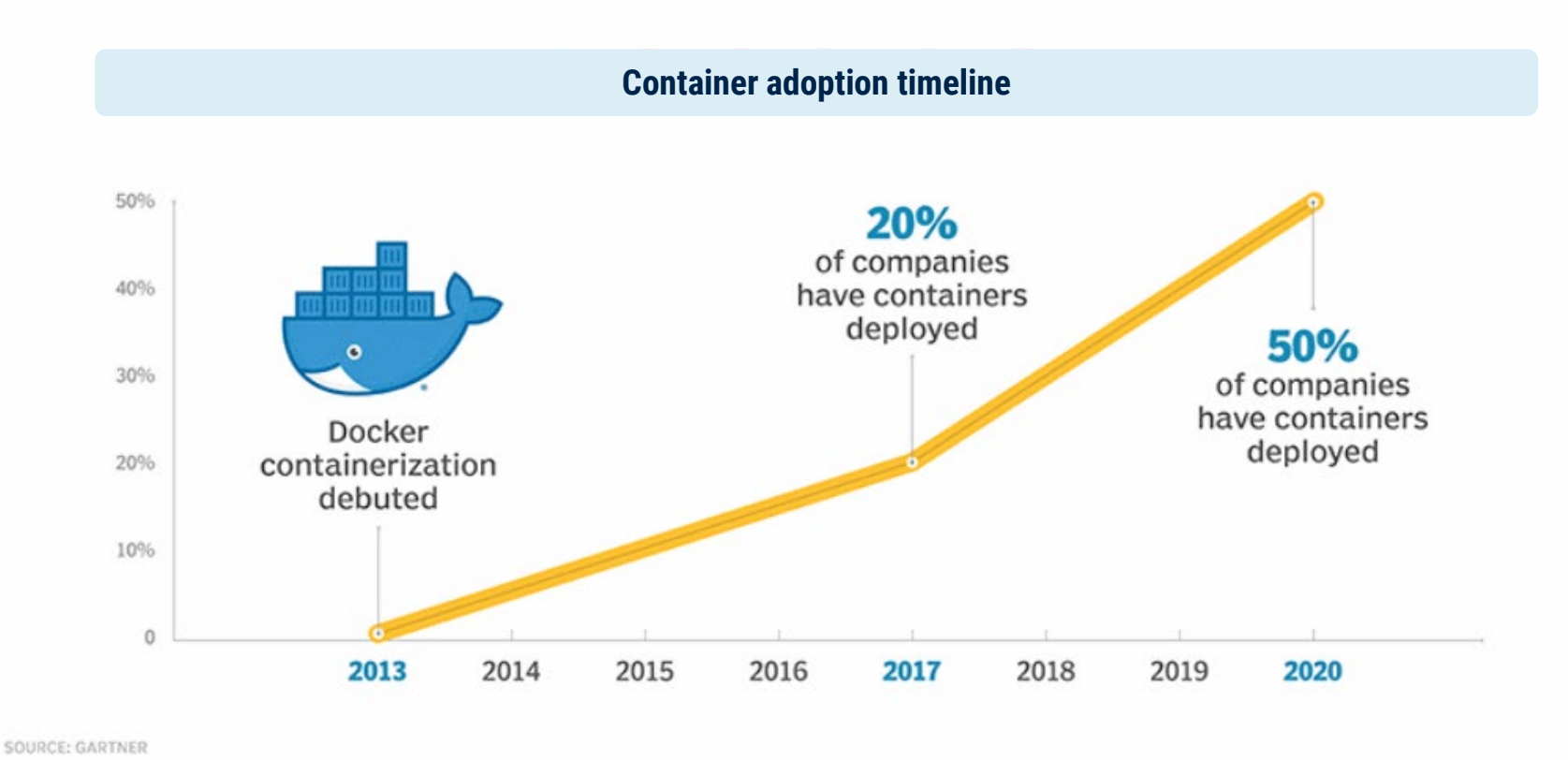
Total disclosed funding: $19.2M

Location: Dublin, Ireland

Container security

Companies are embracing containers

Containers are a tool for deploying software applications easily across computing environments (e.g., on-premise to the cloud). While improving productivity, this approach does introduce security concerns.



CBINSIGHTS Source: Dzone

"The difference now is that containers, and the microservices they provide, have **exponentially increased the surface area available for attack**, putting data at greater risk."

- David Warburton, Senior Threat Research Evangelist, 2020

Source: Computer Weekly

Securing the container lifecycle

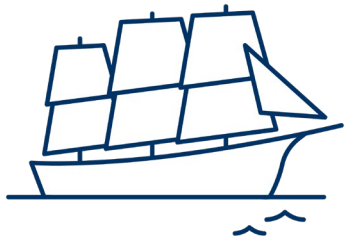
As with non-containerized applications, its crucial to secure containers from the point of development through to execution. Many startups are developing security solutions specifically for containers, whether its vulnerability scanning, access management, or runtime monitoring.

Container security lifecycle

Build

When building containers, vulnerabilities (e.g., malware, exposed information) must be identified.

Ship



Once built, containers ready for deployment must be secured to ensure only privileged access.

Run

Containers in operation must be monitored to protect against malicious activity.

Container security

CAPSULE8

Capsule8 offers an end-point protection solution, including attack detection, response, and investigation for Linux production environments on the cloud or on-premise.

Capsule8, founded in 2016, announced a partnership last year with Google to provide runtime protection to users of its cloud platform.

Investors include Intel Capital, Bessemer Venture Partners, and ClearSky, among others.

Most recent financing: $6.5M Series C (8/7/2019)

Total disclosed funding: $30M

Location: Brooklyn, NY

anchore

Anchore provides tools for inspecting container security and compliance.

Tech entrepreneurs Saïd Ziouani and Daniel Nurmi, who sold companies to Red Hat and HPE, respectively, founded Anchore in 2016.

In June 2020, the company was awarded a contract with the United States Air Force to help secure software containers as part of a DevSecOps workflow.

Investors include Menlo Ventures and SignalFire.

Most recent financing: $20M Series B (1/22/2020)

Total disclosed funding: $47.5M

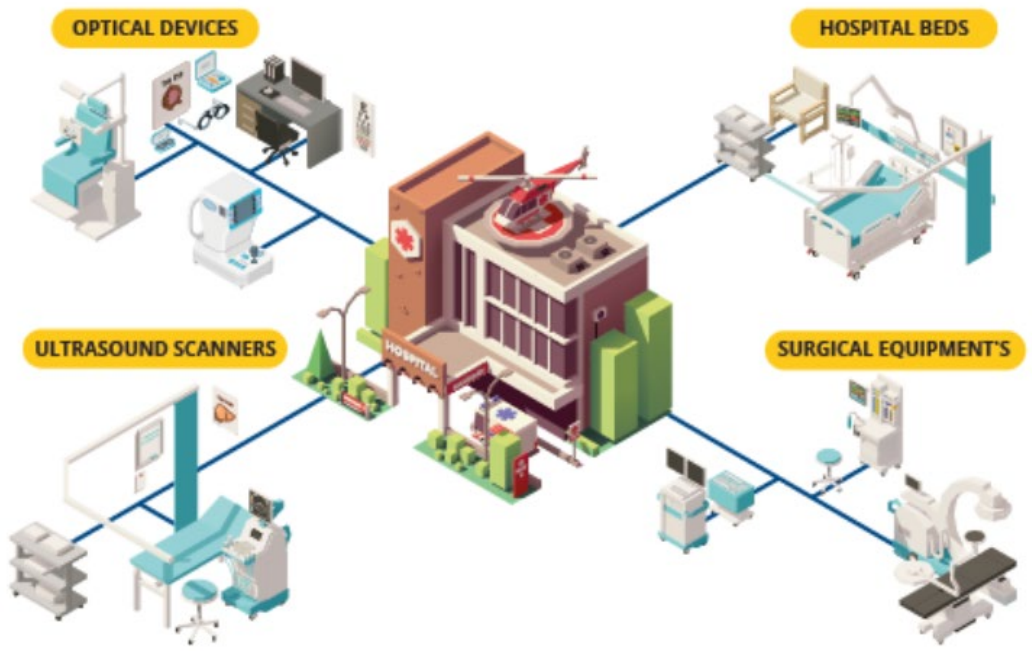
Location: Santa Barbara, CA

Medical device security

Connected devices increase cyber risk

Hospitals are connecting equipment and devices to the internet for real-time visibility into patient and machine health. If they are not protected, these sprawling networks could provide a way in for hackers.

The connected hospital



10 to 15 connected medical devices per patient bed

82% of healthcare organizations have experienced an IoT-focused cyberattack

$346,000 is the average cost an IoT-focused attack

Source: L&T Services; Fierce Healthcare

"While advanced devices can offer safer, more convenient and timely health care delivery, a **medical device connected to a communications network** could have **cybersecurity vulnerabilities** that could be exploited resulting in **patient harm**."

- Dr. Amy P. Abernethy, M.D., Ph.D, Principal Deputy Commissioner of Food and Drugs, 2019

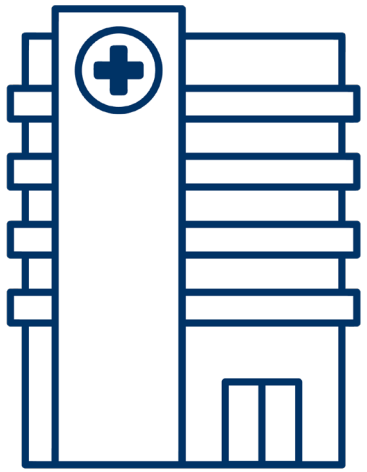
Source: FDA

Strengthening connected devices

Startups are aiming to help hospitals protect connected devices critical to delivering patient care. Solutions that provide visibility into device activity could help mitigate attacks.

Securing connected medical devices

Hospital

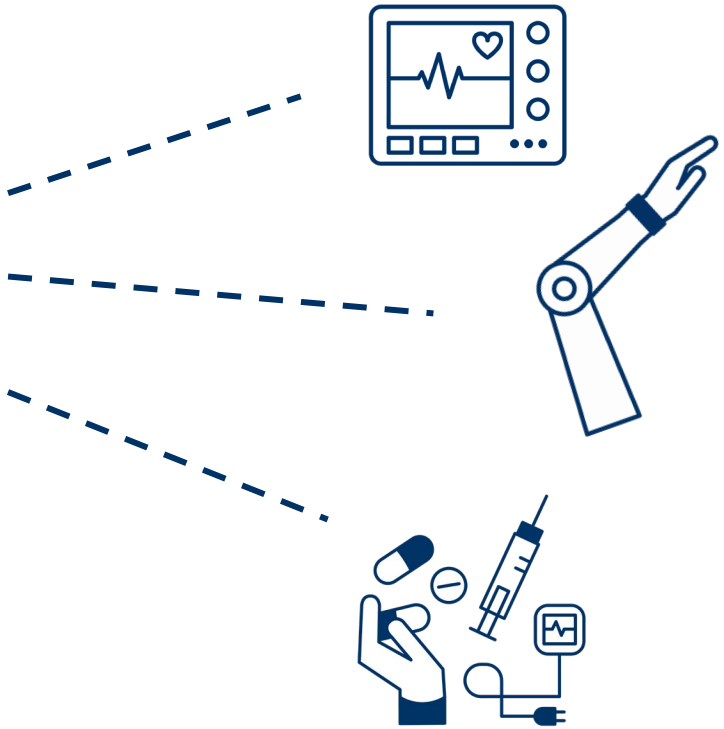


Identify devices

Monitor device activity

Manage security policies

Provide alerts of suspicious activity



Medical device security

Ordr uses machine learning to identify anomalous behavior across a company's network of connected devices.

The company was founded in 2015 by veterans of wireless networking company Aruba Networks.

Investors include Kaiser Permanente Ventures, Battery Ventures, and Mayo Clinic Ventures, among others.

Most recent disclosed financing: $2M Series B (3/5/2020)

Total disclosed funding: $50M

Location: Santa Clara, CA

Medigate monitors and enforces security policies on connected devices across a company's network.

Since its founding in 2017, Medigate has developed an ecosystem of partners that includes electronic medical records (EMR) provider Cerner and networking provider Cisco.

Investors include YL Ventures, US Venture Partners, and Blumberg Capital.

Most recent financing: $15M Series A (1/29/2019)

Total disclosed funding: $20.4M

Location: New York, New York

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 categories.

How the companies were selected: We used CB Insights' 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.

We've gathered this data via our machine learning technology (dubbed The Cruncher) as well as via several thousand direct submissions from firms and individual professionals using The Editor.

The CB Insights Mosaic page walks through the factors considered in the algorithm.