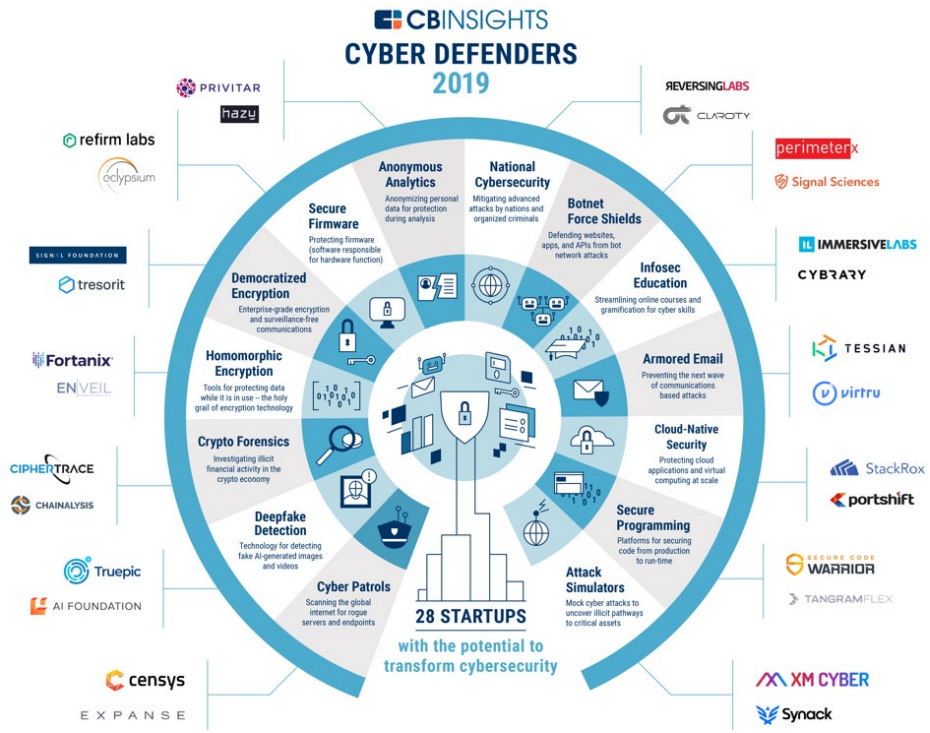
2019 Cyber Defenders

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

CBINSIGHTS

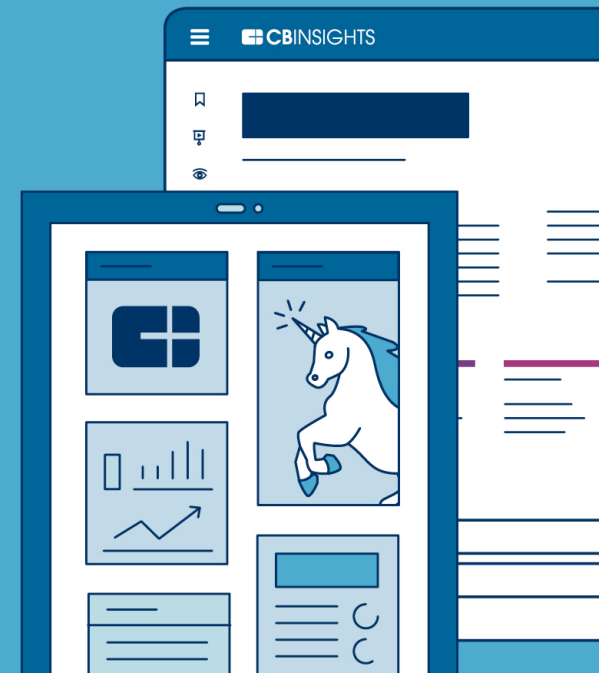


CBINSIGHTS

WHAT IS CB INSIGHTS?

CB Insights is a tech market intelligence platform that analyzes millions of data points on venture capital, startups, patents, partnerships and news mentions to help you see tomorrow's opportunities, today.

CLICK HERE TO LEARN MORE



Contents

CYBERSECURITY IS TOP OF MIND

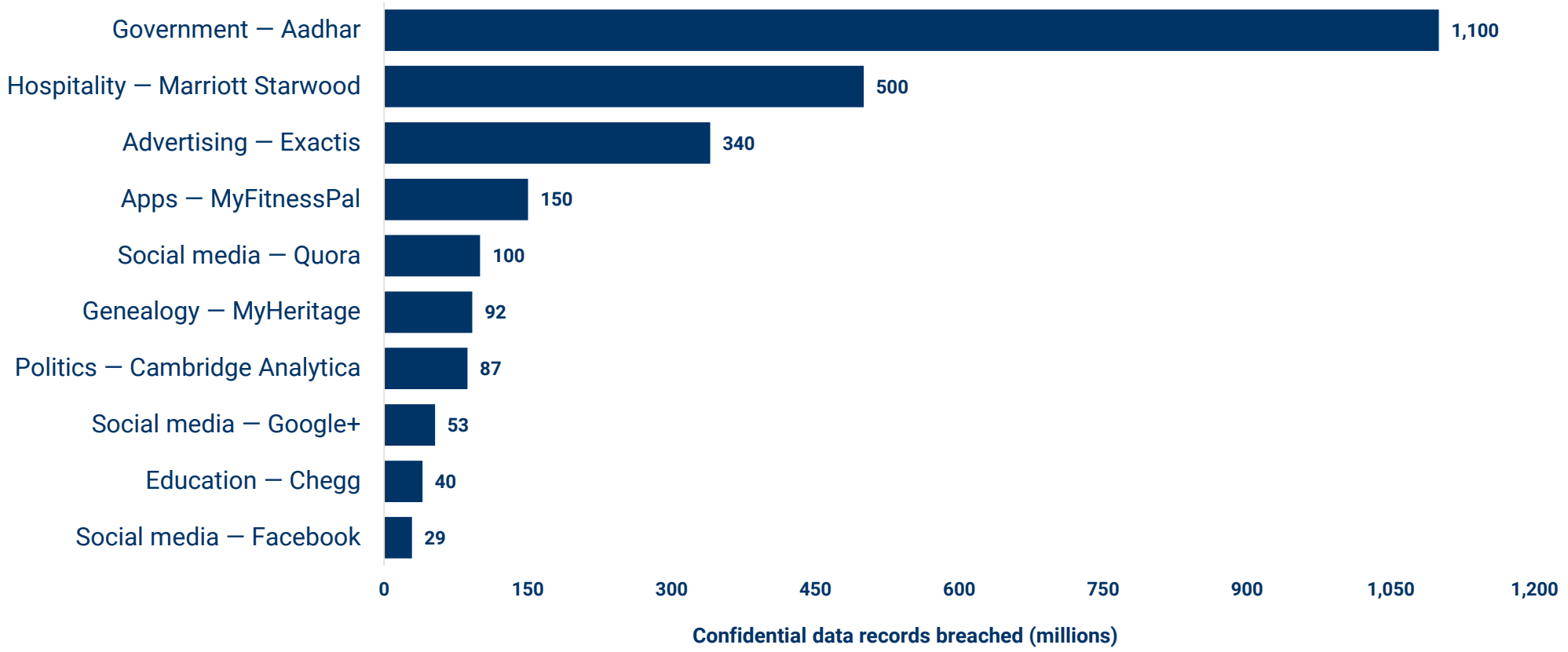
Over 800 **data breaches** were disclosed in 2018.*

Each new breach raises fears that **trust in the global digital economy is eroding**.

* Privacy Rights Clearinghouse

CYBER INSECURITY IS FELT ACROSS INDUSTRIES

NUMBER OF COMPROMISED DATA RECORDS IN SELECT BREACHES IN 2018



THE C-SUITE IS TALKING MORE ABOUT CYBERSECURITY

NUMBER OF EARNINGS CALLS MENTIONS OF "CYBERSECURITY" Q2'14 – Q1'19 YTD

“Cybersecurity is a central challenge.”

- Satya Nadella, CEO Microsoft, Q1’19 earnings call

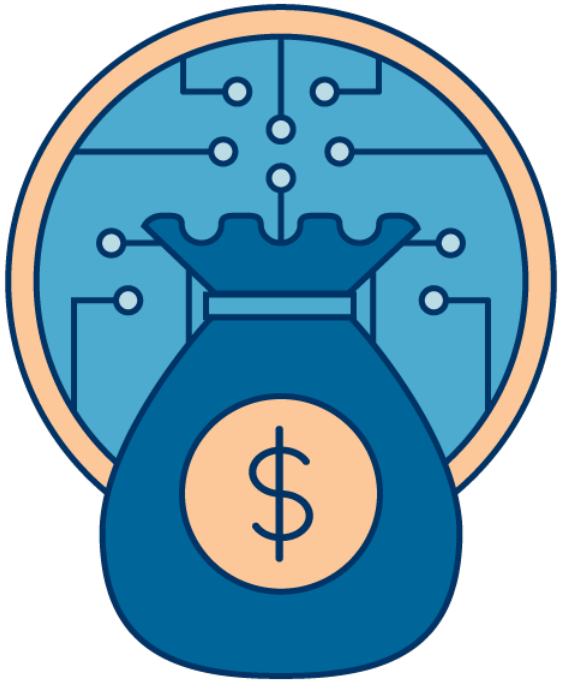
CHALLENGES = OPPORTUNITIES

In tandem, investors are seizing the opportunity to back **the next generation of cybersecurity startups**.

But first, some funding trends…

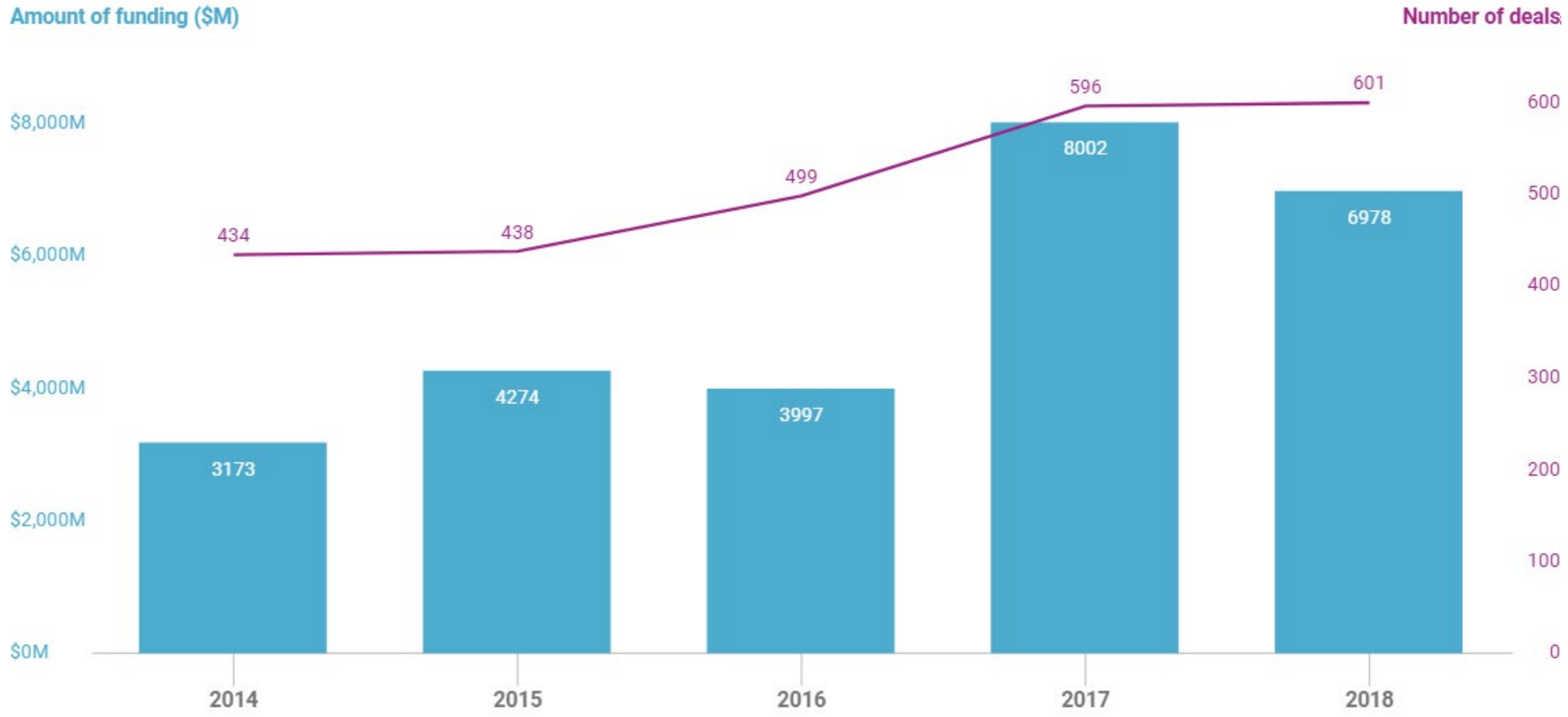
CYBERSECURITY

Global equity funding trends



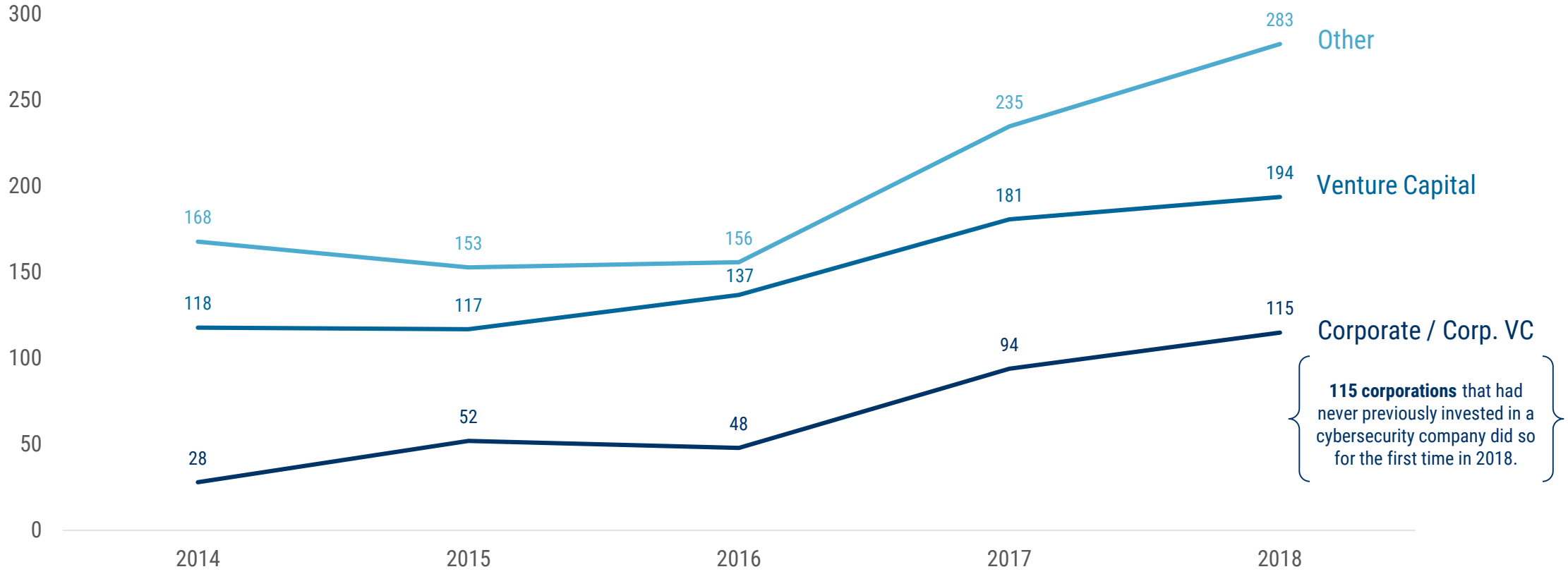
Cybersecurity deals hit a record high in 2018

Annual global cybersecurity deals and financing 2014 – 2018



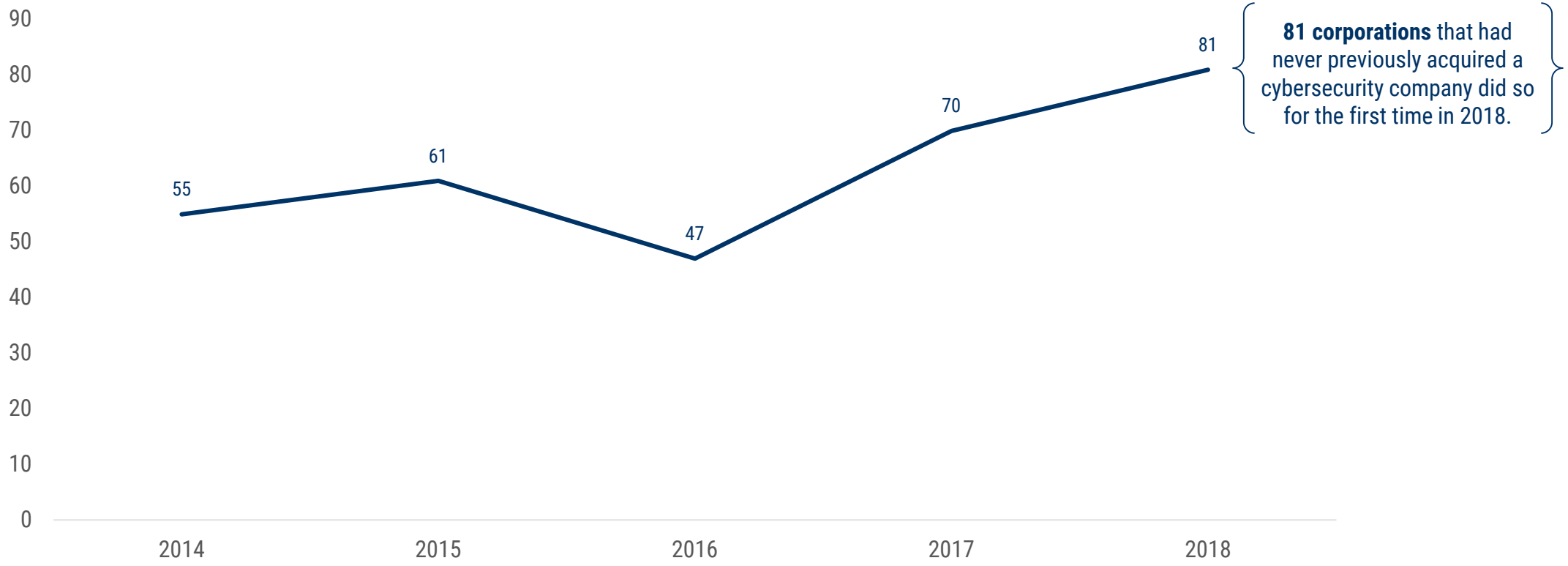
2018 was a record year for 1st time investors

Annual number of 1st time investors in cybersecurity 2014 - 2018



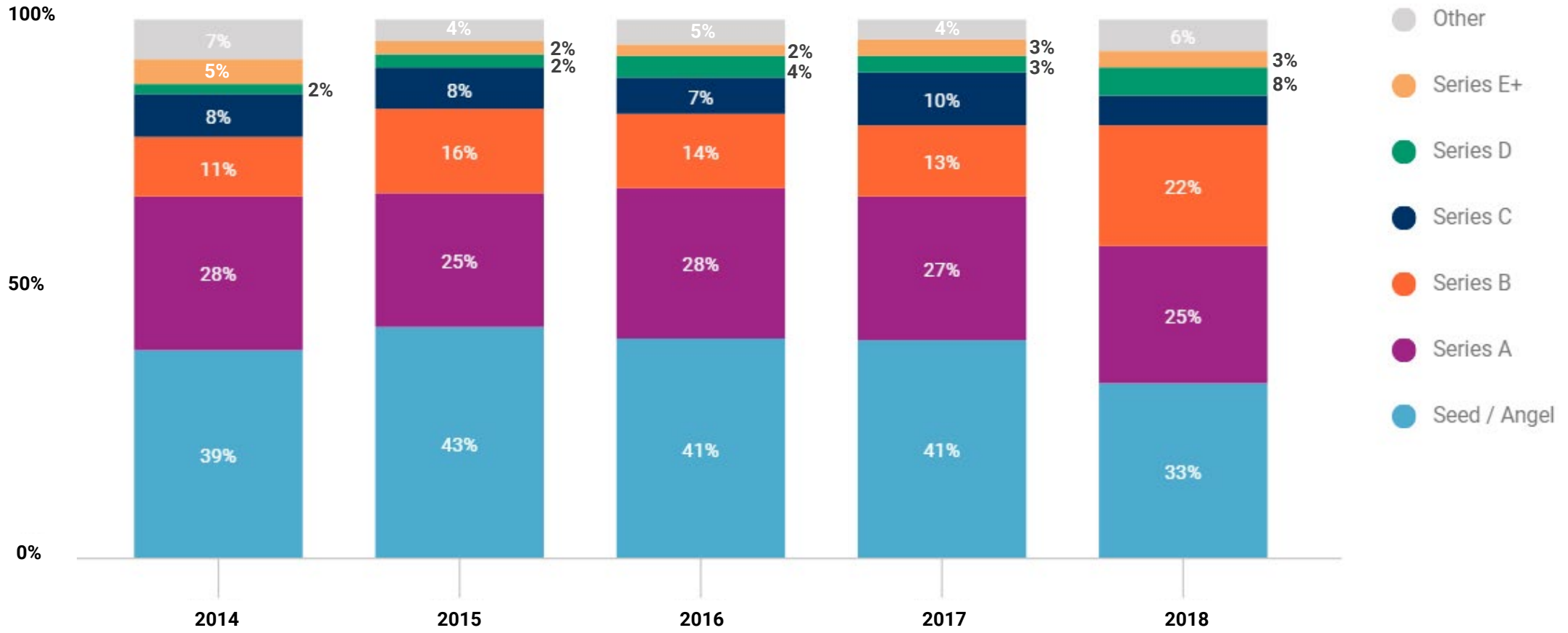
2018 was a record year for 1st time acquisitions

Annual number of corporations acquiring a cybersecurity company for the 1st time 2014 - 2018



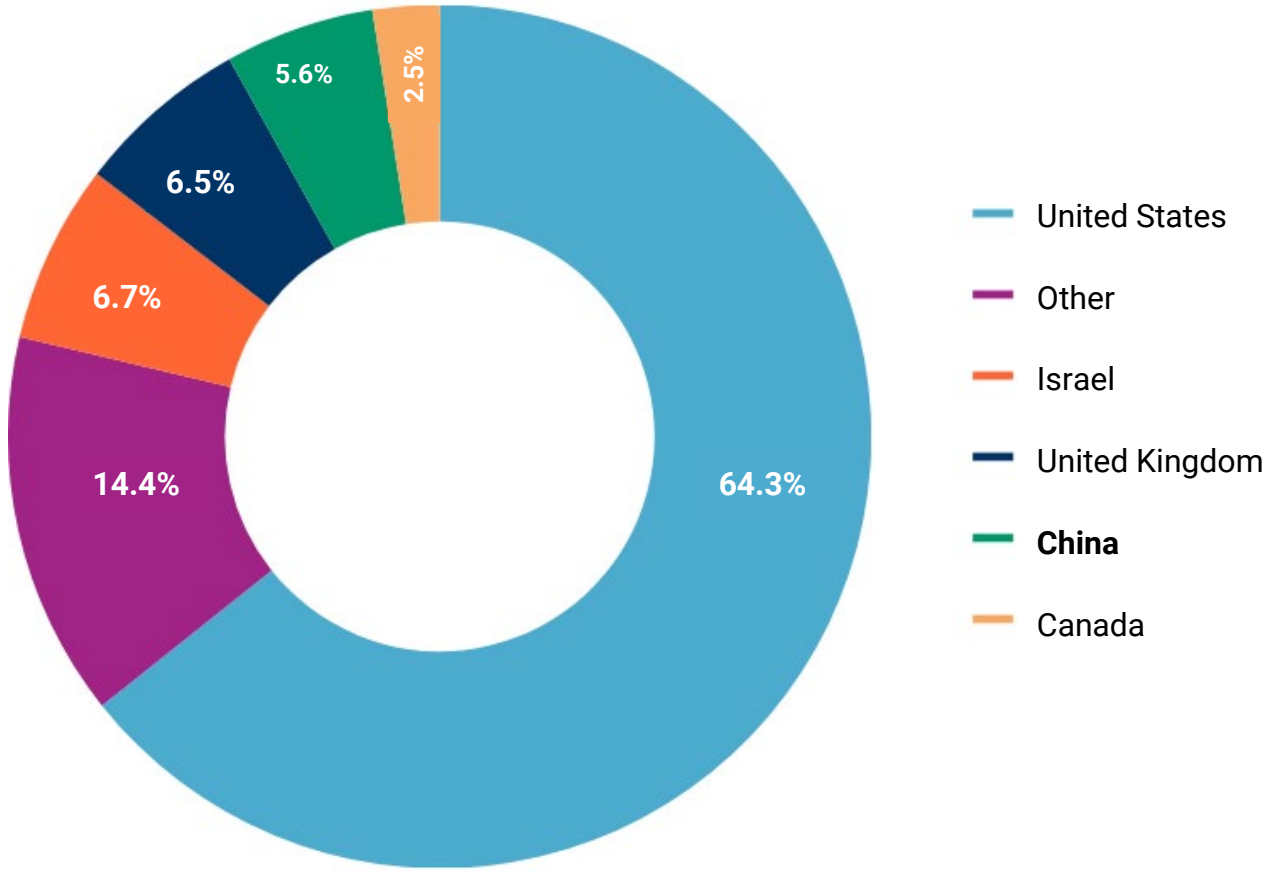
Early-stage deals fell to a 5-year low

Annual deal share by stage to private cybersecurity companies 2014 - 2018



China sees fourth-highest deal share globally

Cybersecurity global deal share by country 2014 – 2019 YTD (3/21/2019)



PRIVATE MARKET LEADERS

There are now 8 cybersecurity unicorns

Private cybersecurity companies valued at $1B+ as of 3/21/2019:

CHINA

- 4Paradigm 第四范式
- 同盾科技 www.tongdun.cn

UNITED STATES

- TANIUM™
- illumio
- Lookout
- CLOUDFLARE
- CROWDSTRIKE
- netskope

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 2017 are excluded.

This year's Cyber Defender categories

Cyber Patrols
Scanning the global internet for rogue servers and endpoints

Deepfake Detection
Technology for detecting fake, AI-generated images and videos

Crypto Forensics
Investigating illicit financial activity in the cryptocurrency economy

Homomorphic Encryption
Tools for protecting data while it is in use — the "holy grail" of encryption

Democratized Encryption
Enterprise-grade encryption and surveillance-free communications

Secure Firmware
Protecting firmware (software responsible for hardware function)

Anonymous Analytics
Anonymizing personal data for protection during analysis

National Cybersecurity
Mitigating advanced attacks by nations and organized criminals

Botnet Force Shields
Defending websites, apps, and APIs from bot network attacks

Infosec Education
Streaming online courses and gamification for cyber skills

Armored Email
Preventing the next wave of communications based attacks

Cloud-Native Security
Protecting cloud apps and virtual computing at scale

Secure Programming
Platforms for securing code from production to run time

Attack Simulators
Mock cyber attacks to uncover illicit pathways to critical assets

The 2019 Cyber Defenders

Cyber Patrols

EXPANSE

censys

Deepfake Detection

AI FOUNDATION

Truepic

Crypto Forensics

CIPHERTRACE

CHAINALYSIS

Homomorphic Encryption

ENVEIL

Fortanix

Democratized Encryption

SIGNAL FOUNDATION

tresorit

Secure Firmware

refirm labs

eclypsium

Anonymous Analytics

PRIVITAR

hazy

National Cybersecurity

REVERSINGLABS

CLAROTY

Botnet Force Shields

perimeterx

Signal Sciences

Infosec Education

IMMERSIVELABS

CYBRARY

Armored Email

TESSIAN

virtru

Cloud-Native Security

StackRox

portshift

Secure Programming

SECURE CODE WARRIOR

TANGRAMFLEX

Attack Simulators

Synack

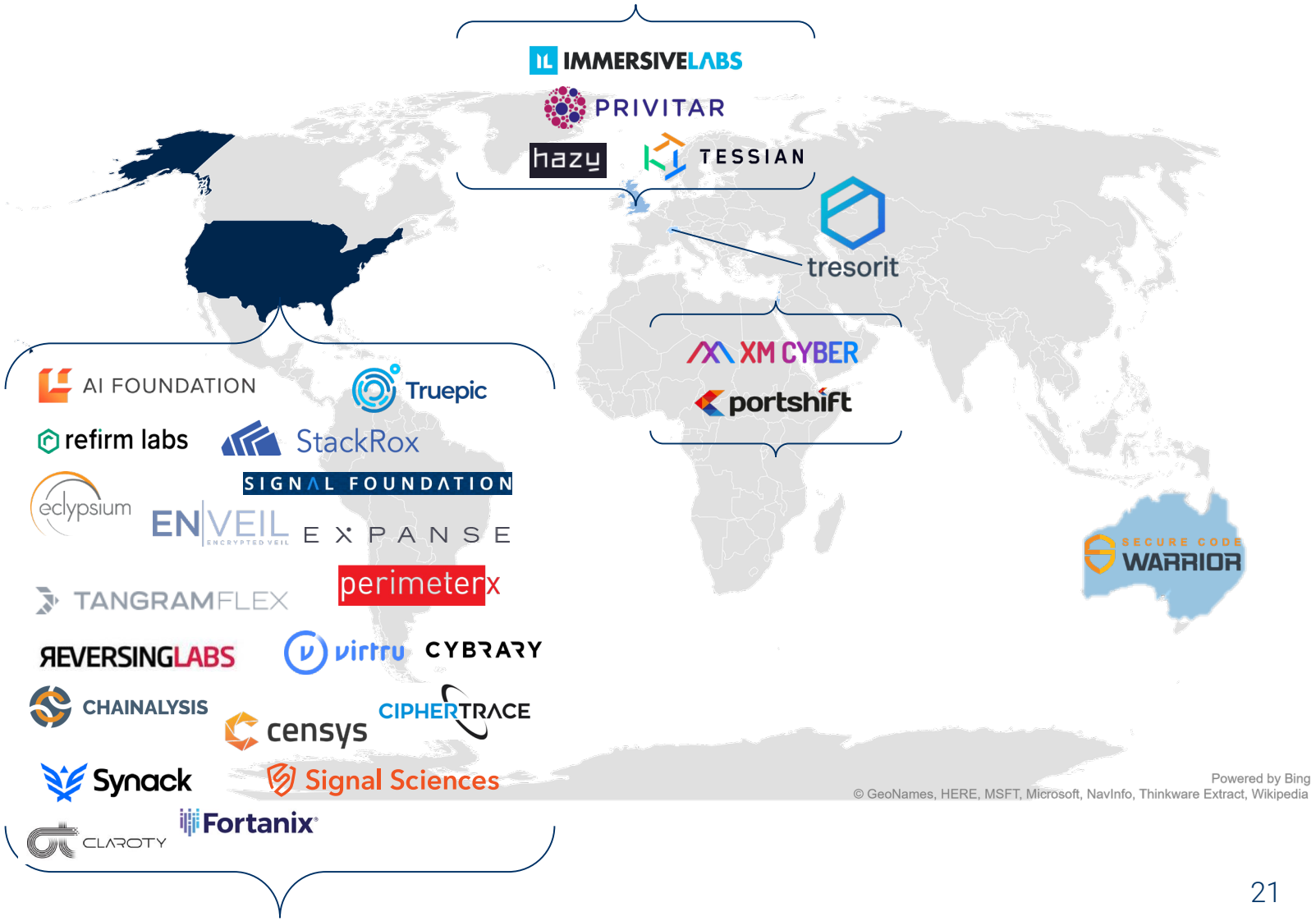
XM CYBER

The US has the most Cyber Defenders

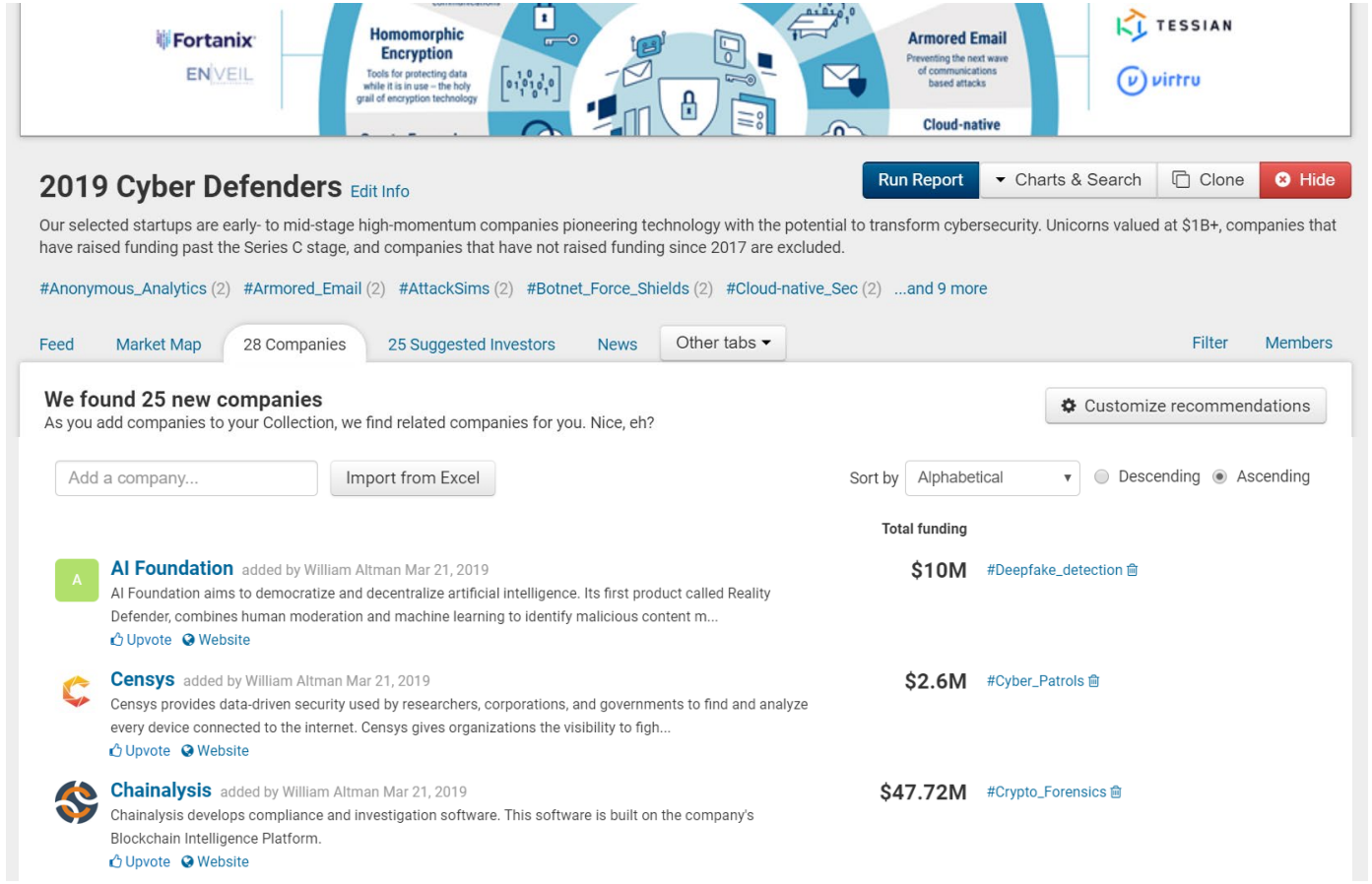
71% of the 2019 Cyber Defenders have their headquarters in the US — mostly in California.

The next highest concentration of Cyber Defenders are located in the UK, followed by Israel.

Switzerland and Australia are each represented with one Cyber Defender.



2019 Cyber Defenders expert collection on CBI

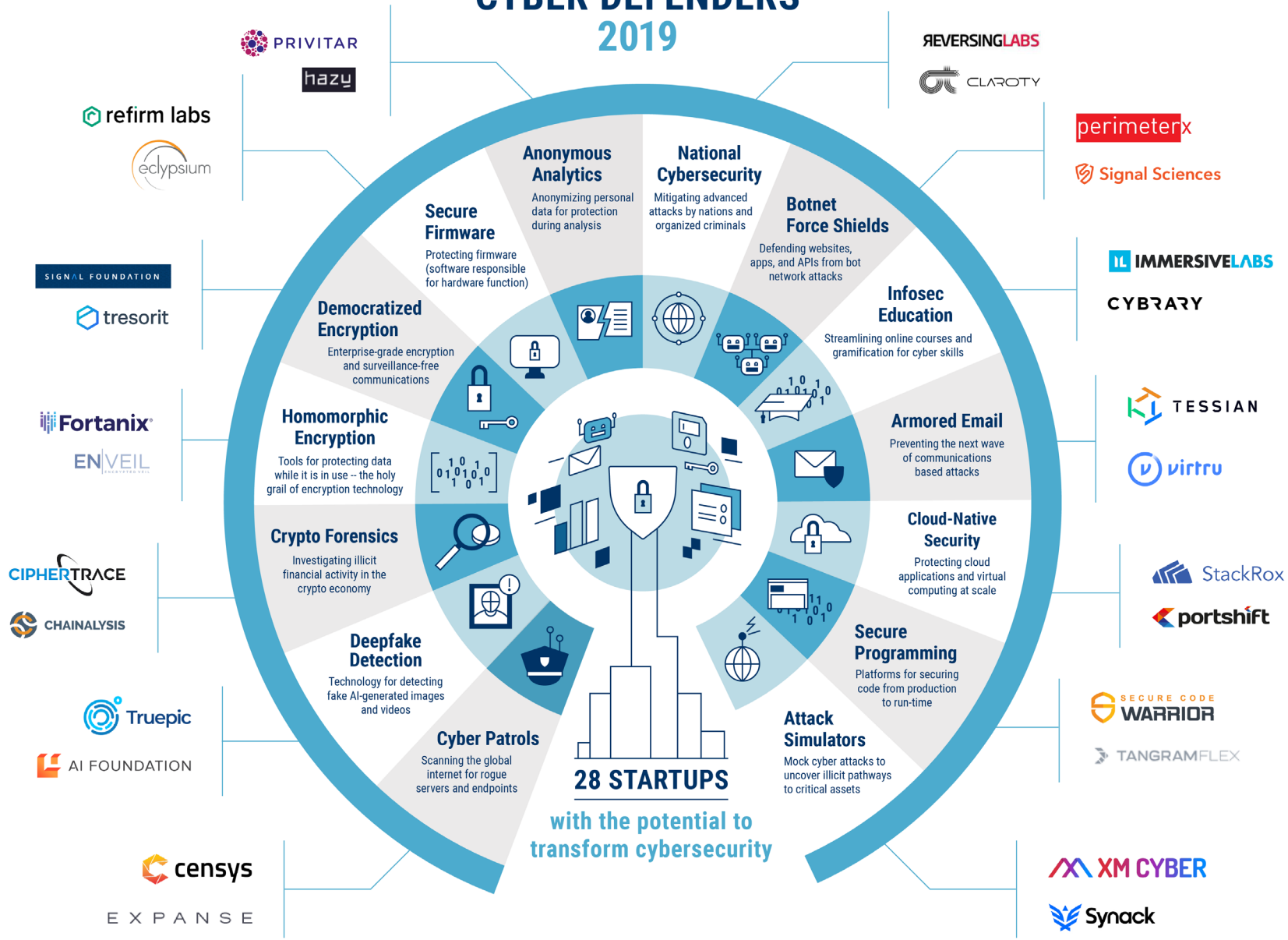


Track all of the startups in this presentation and many more on our platform using CB Insights' Collections.

Create dynamic market landscapes, collaborate within and beyond your organization, and ensure knowledge is not tied up in people's heads and inboxes.

CBINSIGHTS

CYBER DEFENDERS 2019



Cyber patrols

The enterprise attack surface is growing

Devices, critical infrastructure, apps, and services connected to the internet are all **potential network entry points that can be exploited** by adversaries.

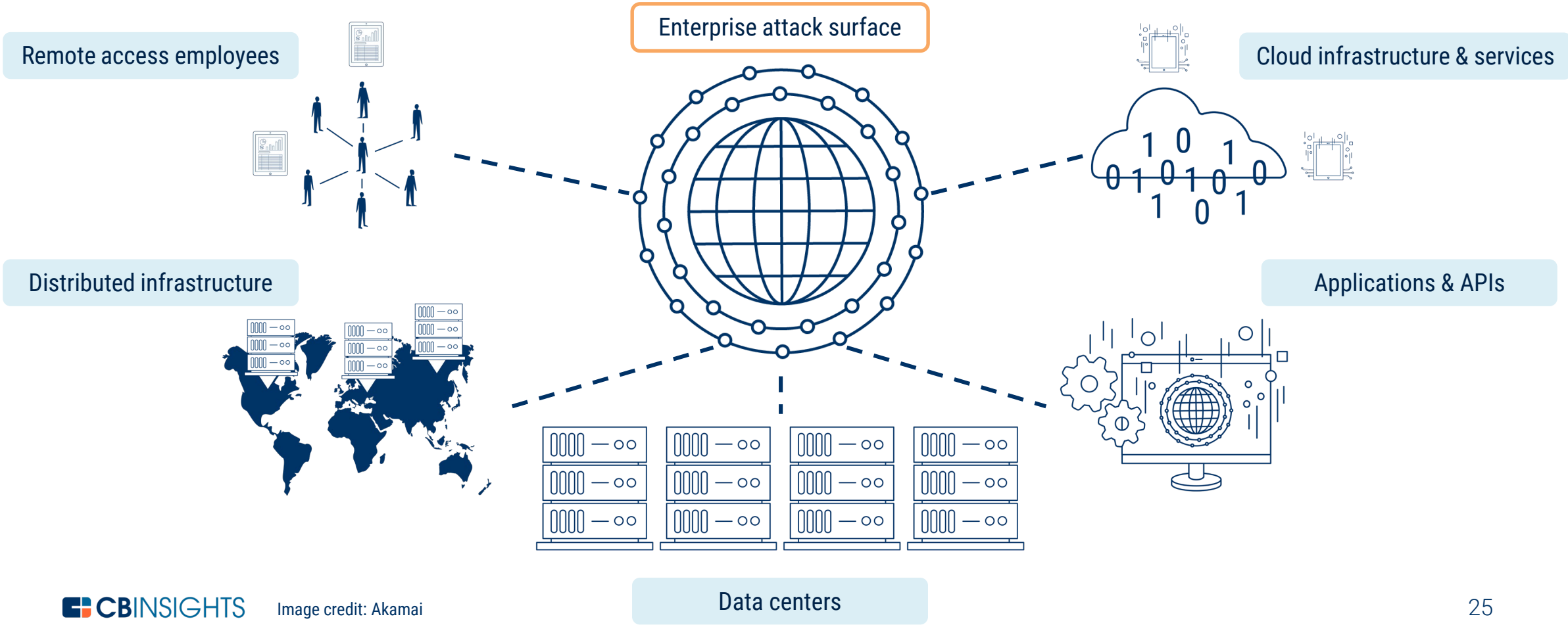


Image credit: Akamai

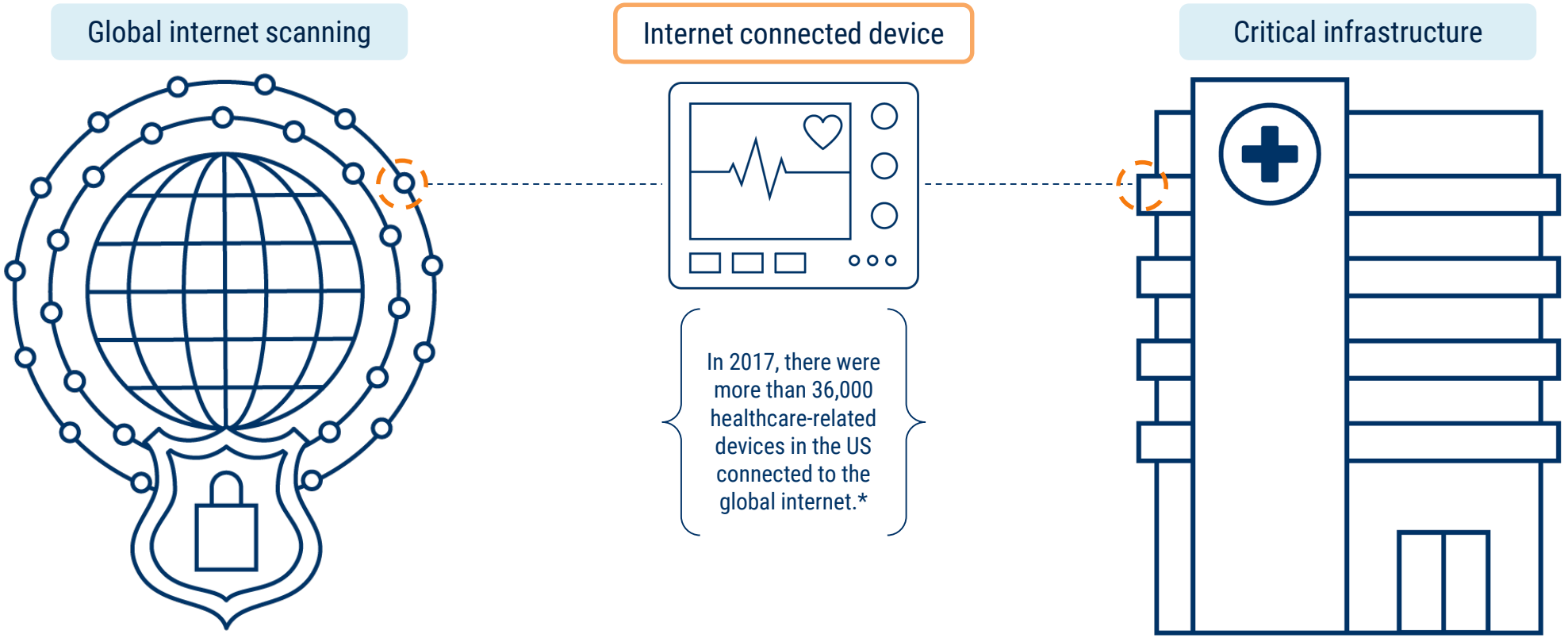
"Our power system, our transportation network, our communications systems, are **all on the internet. If it goes down, to a very real extent society grinds to a halt.**"

- Bruce Schneier, Berkman Klein Center for Internet and Society at Harvard University, 2018

Quote: MIT Technology Review

Patrolling the global internet can help

Startups are rising to help IT operations and security teams **manage the risk posed by all assets** running while connected to the global internet.



*Source: Shodan via Trend Micro

Cyber patrols

EXPANSE

Expanse is an automated global internet intelligence company.

The company offers real-time detection and classification of connected digital assets and the risks they pose to organizations.

Expanse was awarded a $37.6M contract by the U.S. Department of Defense in July, 2018. The contract was awarded by the U.S. Navy's Space and Warfare Command after the Department of Defense validated the software.

Investors include Founders Fund, New Enterprise Associates, Peter Thiel, and TPG Growth, among others.

Most recent financing: $70M Series C (4/9/2019)

Total disclosed funding: $135.97M

Location: San Francisco, CA

Censys fights threats by analyzing real-time internet data.

The platform is used by researchers, corporations, and governments to analyze every device connected to the internet.

Censys is an early-stage company that started as a research project at the University of Michigan in 2015, and it was spun out in 2017. The startup is reportedly using its seed funding to collect more data and develop additional paid services.

Investors include Google Ventures and Greylock Partners.

Most recent financing: $2.6M Seed (11/27/2018)

Total disclosed funding: $2.6M

Location: Ann Arbor, MI

Deepfake detection

Deepfake **(a portmanteau of "deep learning" and "fake")** is type of fake synthetic image or video made with artificial intelligence (AI).

Deepfakes combine existing images and videos onto source images or videos using a machine learning technique called a **generative adversarial network (GAN)**.

AI is accelerating the fake media problem

GANs (generative adversarial networks) are a type of AI used to carry out unsupervised machine learning. In a GAN, opposed neural networks work together **to fabricate increasingly realistic audio, image, and video content**.

Sketch of a Generative Adversarial Network for creating fake images:

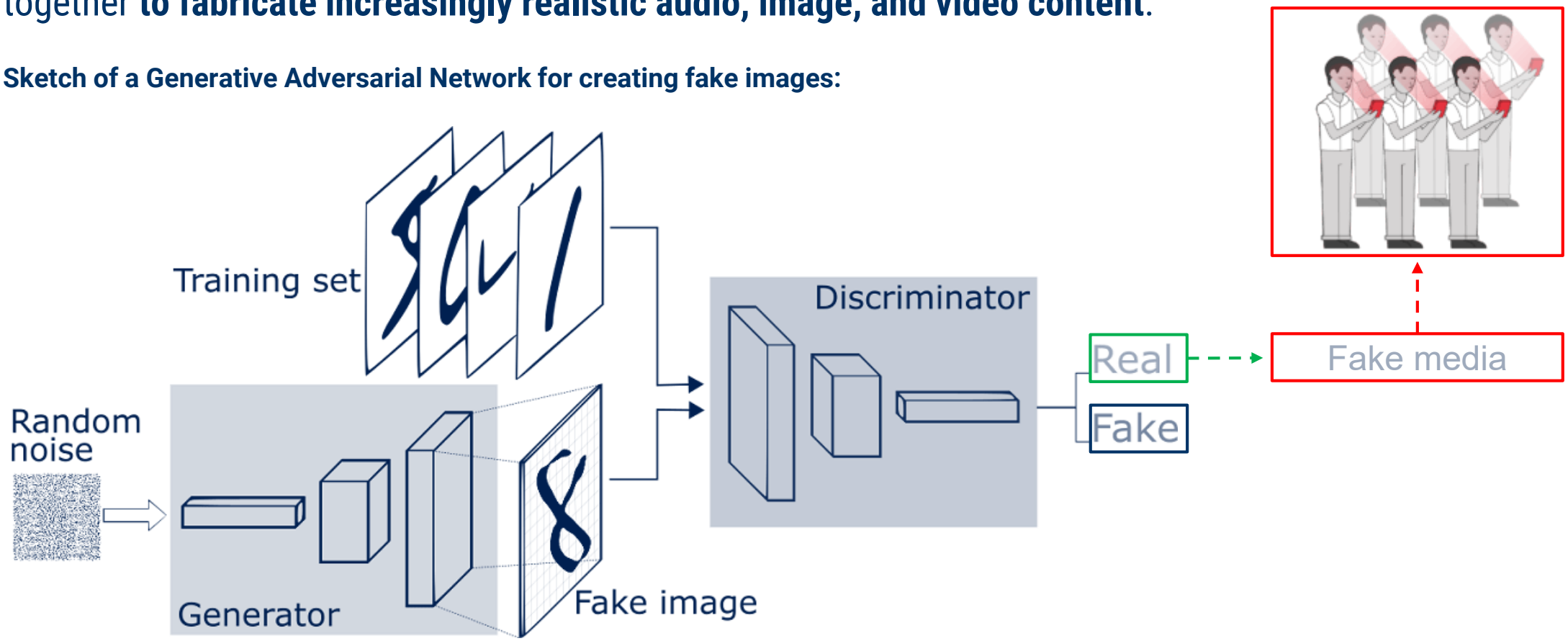


Image credit: DL4J

"It is almost **too late to sound the alarm** before this technology is released — **it has been unleashed**."

- Senate Intelligence Committee Vice Chairman Mark Warner (D-Va.), 2018

Quote: The Hill

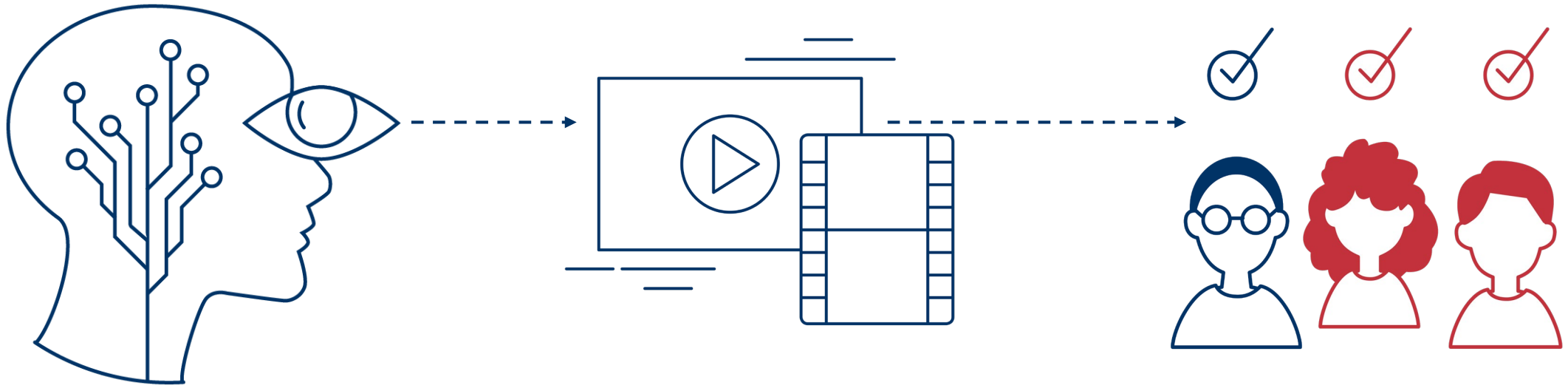
Emerging tech can help spot deepfakes

Startups are using AI, cryptography, and other **emerging technologies to authenticate real media** and help spot fake images, video, and audio.

Computer vision technology, etc.

Media scanning platform

Deepfakes spotted



Deepfake detection

TruePic is an online image and video authenticity provider.

The company authenticates digital photos and videos by verifying their origin, pixel contents, and metadata at capture.

The unique cryptographic signature of media captured using TruePic's app is written to the blockchain — creating an immutable record of authenticity in a distributed public ledger. TruePic is working on authentication for media captured outside the app.

Investors include Thompson Reuters, Dowling Capital Partners, and five angel investors.

Most recent financing: $8M Series A (6/20/2018)

Total disclosed funding: $11.21M

Location: La Jolla, CA

AI Foundation develops tools for fighting digital deceptions.

The company combines human moderation and machine learning to identify content meant to deceive people, such as deepfakes.

The software runs while browsing the web, similar to virus protection. It scans every image, video, and other media that a user encounters for known fakes, allows reporting of suspected fakes, and can detect signs of alteration or synthetic media generation.

Investors include Founders Fund, Endeavor, and angel investor Biz Stone, among others.

Most recent financing: $10M Seed (9/18/2018)

Total disclosed funding: $10M

Location: San Francisco, CA

Crypto forensics

Bad actors are using cryptocurrency

Cryptocurrencies such as Bitcoin enable money launderers and extortionists to **obfuscate the origin and receipt of funds**. Similarly, nations can use crypto to evade sanctions.

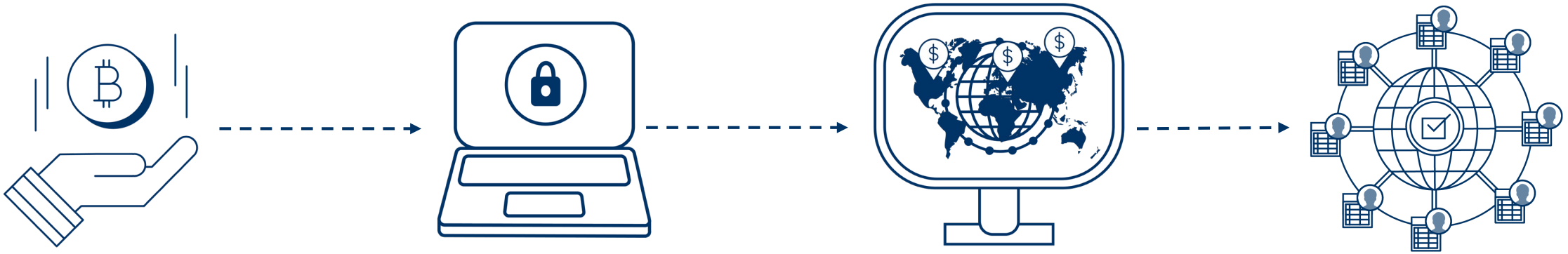
Public crypto wallet

Cryptocurrency laundering

Dark web crypto wallet

Crypto “coin-scrambler”

Clean crypto exchange



Dark wallets offer privacy and anonymity through encrypted transactions and coin-scrambling services.

Scramblers are a technology that mix cryptocurrencies to obscure audit trails back to the original source.

CBINSIGHTS

*According to Ciphertrace, 97% of criminal Bitcoin received by the top 20 exchanges flowed into unregulated countries.

"Cryptocurrencies can help bypass certain sanctions through **untraceable banking operations**."

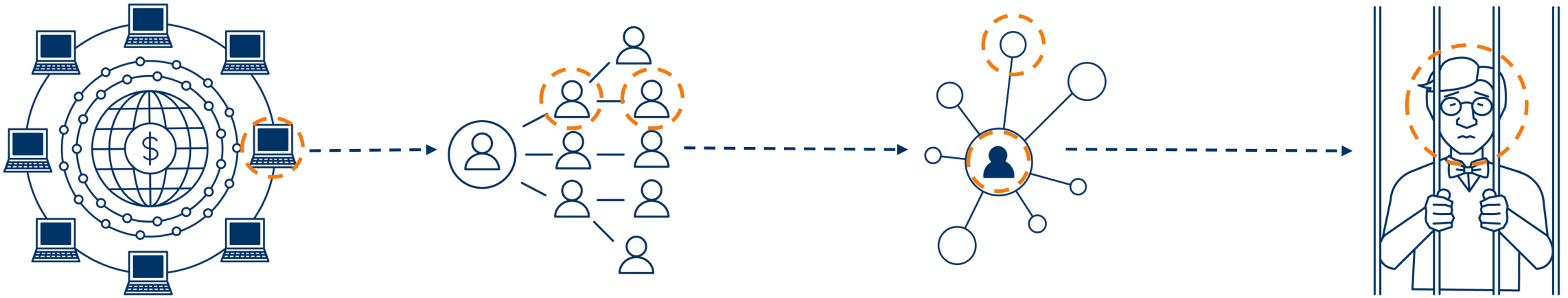
- Brigadier General Gholam Reza Jalali, head of Iran's Civil Defense Organization, 2018

Quote: Iran's Mehr news agency

Crypto transactions can be investigated

Startups are rising to help law enforcement agencies investigate the **sources and destinations of suspicious cryptocurrency transactions**.

Cryptocurrency economy | Suspicious transactions | Network analysis, etc. | Source identified



Most cryptocurrencies, other than dedicated privacy coins, are **only pseudonymous**.

Crypto transactions are recorded on **digital public ledgers** known as a blockchains.

Account balances and **activity can be traced** back to users' blockchain addresses.

Crypto forensics

CipherTrace offers tools for tracing cryptocurrency transactions.

The company develops cryptocurrency anti-money laundering, forensics, and blockchain threat intelligence solutions.

Exchanges, banks, law enforcement agencies, and others use CipherTrace to follow transactions and comply with regulations. The Malta Financial Services Authority has partnered with the startup to improve monitoring for cryptocurrency related risks.

Investors include Neotribe Ventures, Aspect Ventures, Galaxy Digital Ventures, and WestWave Capital.

Most recent financing: $15M Series A (2/19/2019)

Total disclosed funding: $18M

Location: Menlo Park, CA

Chainalysis sells crypto compliance and investigation software.

The company specializes in enhanced due diligence for tracing the flow of funds for a specific transaction, among other services.

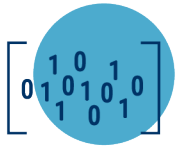
Chainalysis gained notoriety after investigating the now infamous Mt. Gox cryptocurrency heist in 2011. The startup has since moved on to work with institutions such as the IRS, to help the US government fight tax evasion and money laundering.

Investors include Barclays, Accel, Benchmark, Digital Currency Group, and Techstars Ventures, among others.

Most recent financing: $30M Series B (2/12/2019)

Total disclosed funding: $47.72M

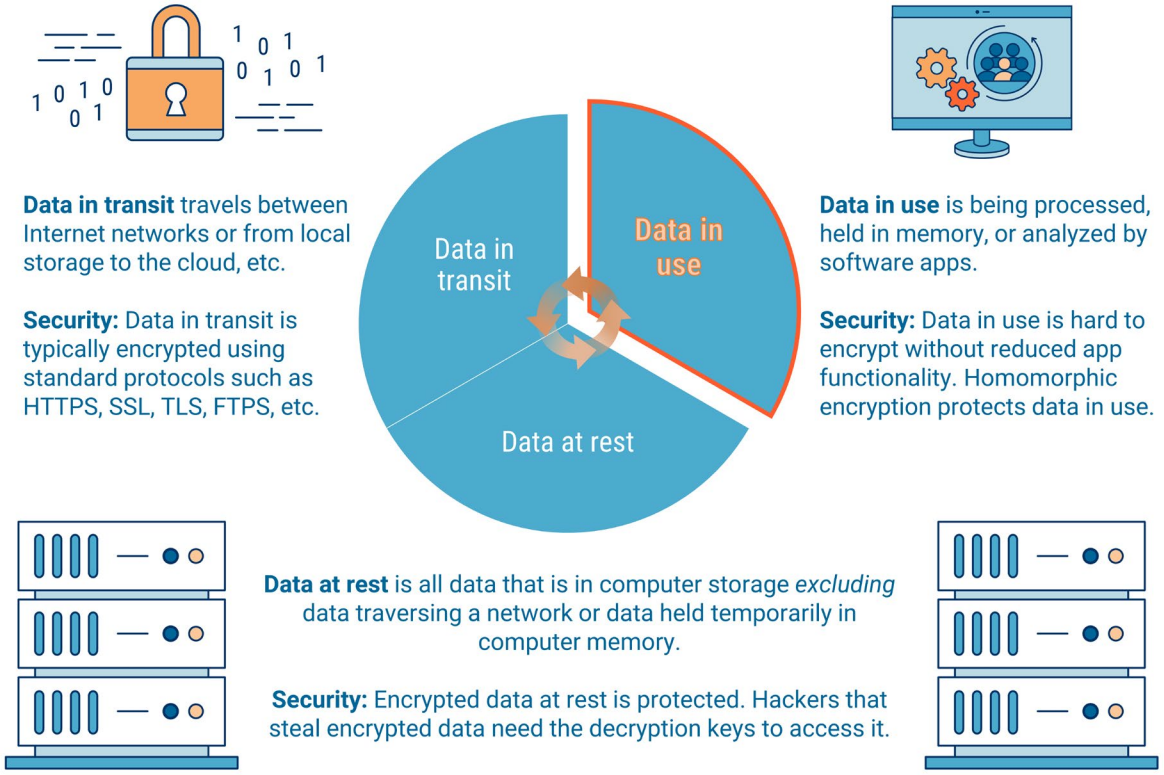
Location: New York, NY



Homomorphic encryption

Data in use is the hardest to secure

The enterprise data life cycle consists of three elements: data at rest, data in transit, and data in use.
Traditional encryption secures data while it is at rest and in transit, but struggles to secure data in use.
Actions like search and analytics have historically required decryption, creating points of exposure.



"Homomorphic encryption is at an **inflection point**, where several **real-world applications are now within reach.**"

- Shai Halevi, cryptographer at IBM's Thomas J. Watson Research Center, 2019

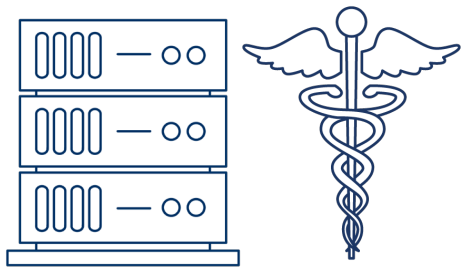
Quote: TheServerSide

It is now possible to secure data in use

Recent advances in cryptography make it possible to keep data encrypted while it's in use. **Homomorphic encryption** technology lets enterprises **operate on sensitive, encrypted data** — such as personal data — without decrypting it.

Emerging use cases for homomorphic encryption (HE)

Comparing private databases

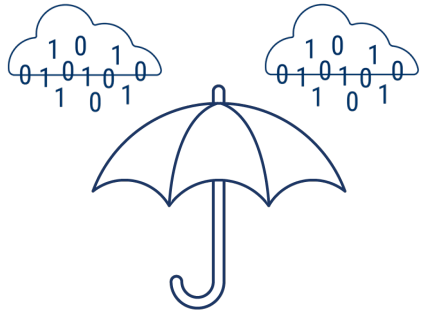


HE provides the ability to generate aggregated reports that **draw comparisons between separate, fully encrypted data sets** without revealing the underlying raw data.

Submitting private queries

HE makes private search engine queries possible. The user submits an encrypted query and the **search engine computes an encrypted answer without looking at the plain text query**.

Ensuring cloud privacy



HE lets cloud computing customers secure their cloud data while it's in use and **ensures that only authorized users — not the cloud provider — can access decryption keys**.

Preventing data breaches

HE can **help thwart speculative execution attacks** by protecting data currently being used in a computer's memory space.

Homomorphic encryption

Enveil is a data security company that protects data in use.

Enveil is an innovator in homomorphic encryption, which has been available for 30 years but not commercially viable — until now.

Founder and CEO Dr. Ellison Anne Williams has more than a decade of InfoSec experience at the National Security Agency. Enveil achieved Standard Technology Partner status in the Amazon Web Services (AWS) Partner Network (APN) in 2018.

Investors include Data Tribe, In-Q-Tel, USAA, Thompson Reuters, and Bloomberg Beta.

Most recent financing: $4M Series A (11/9/2017)

Total disclosed funding: $5M

Location: Fulton, MD

Fortanix allows users to run applications privately in public clouds.

The company offers run time encryption which enables applications to process and work with encrypted data.

Fortanix allows organizations with sensitive workloads to operate in untrusted environments such as the public clouds and remote clouds. Equinix, IBM Cloud, and Alibaba Cloud use Fortanix's security software, which runs on Intel's SGX hardware.

Investors include Intel Capital, Neotribe Ventures, and Foundation Capital.

Most recent financing: $23M Series B (12/14/2018)

Total disclosed funding: $31M

Location: Mountain View, CA

Democratized encryption

Encryption is essential for human rights

Encryption enables freedoms of expression and privacy, and protects intellectual and digital property.
However, access to high-grade encryption technology is rare and unevenly distributed.

Only six countries have a general right to encryption, 2019

A general right to encryption means national legislation **establishes a right** for individuals to use encryption products and services.

Source: Global Partners Digital, 2019

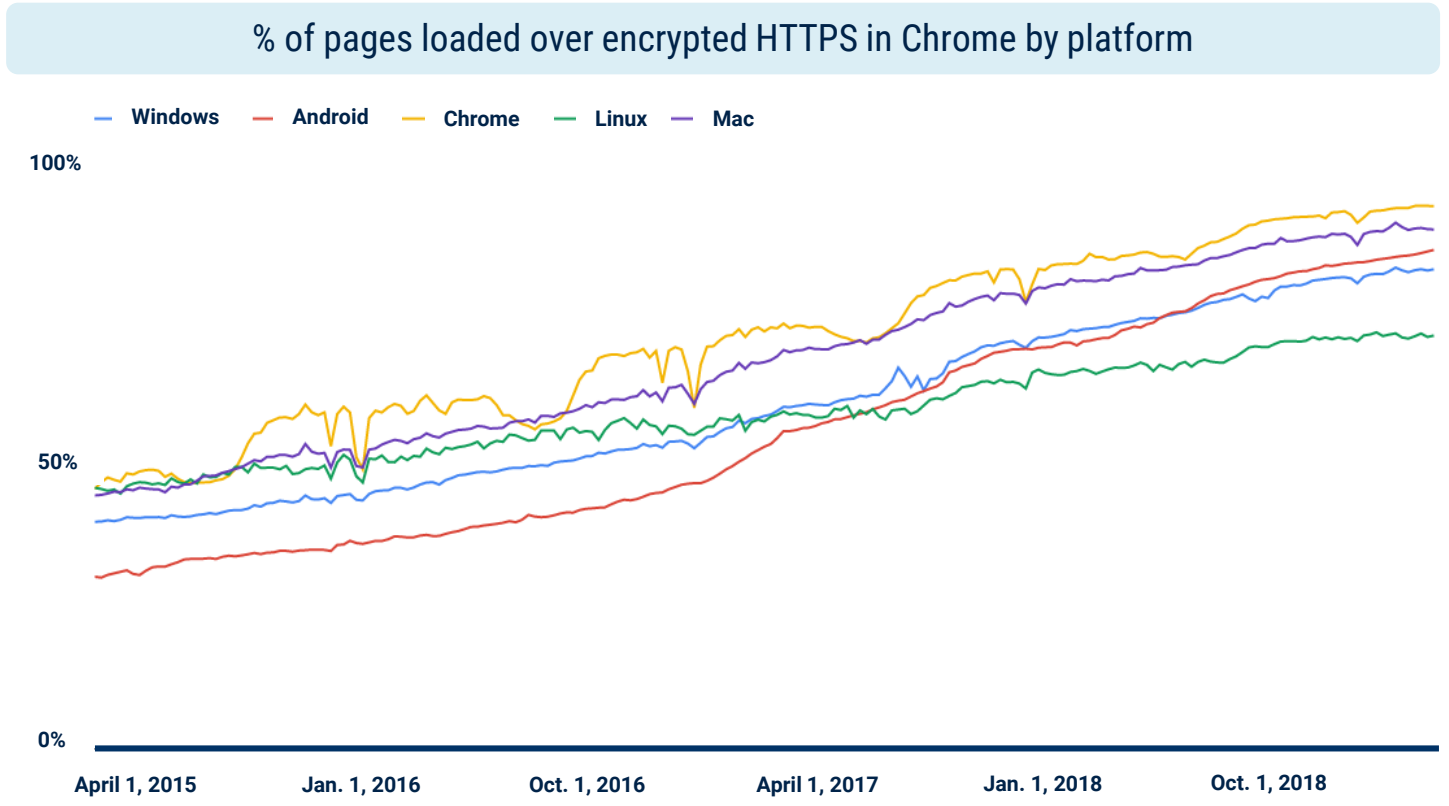
"I want all of my data to be encrypted — if somebody gets hold of my laptop, if it falls into the wrong hands, I don't want any of the charities I work with or people like myself to be targeted."

- Tauqir Sharif, humanitarian, activist, and frontline aid worker in Syria, 2019

Quote: ComputerWeekly

Use of encryption is growing

Individuals and small- and medium-size enterprises are increasingly using encryption for **stopping the interception of information and ensuring the integrity of online information**.



HTTPS encrypted web connections protect against eavesdroppers, man-in-the-middle attacks, and hijackers who attempt to spoof a trusted website.

Source: Google Transparency Report, 2019

Democratized encryption

SIGNAL FOUNDATION

The Signal Foundation supports access to private communications.

The non-profit focuses on developing open source privacy technology to enable access to secure global communications.

The Signal Foundation was founded in 2018 by Moxie Marlinspike and Brian Acton (co-founders of WhatsApp). The foundation shares its name with the Signal messaging app. Acton started the foundation with $50M after leaving WhatsApp's parent Facebook.

Investors include Brian Acton.

Most recent financing: $50M Angel (2/21/2018)

Total disclosed funding: $50M

Location: Palo Alto, CA

tresorit

Tresorit is a cryptographically secure cloud storage service.

The platform is designed for small- and medium-size enterprises that need compliance, security, and confidentiality.

Tresorit's document scanning feature was launched in 2019. Users can snap pictures of confidential data on whiteboards and in meetings, etc. The contents can then be stored and shared securely using Tresorit's end-to-end encrypted cloud service.

Investors include Euroventures, PortfoLion, 3TS Capital Partners, among others.

Most recent financing: $13.29M Series B (9/4/2018)

Total disclosed funding: $18.01M

Location: Zurich, Switzerland

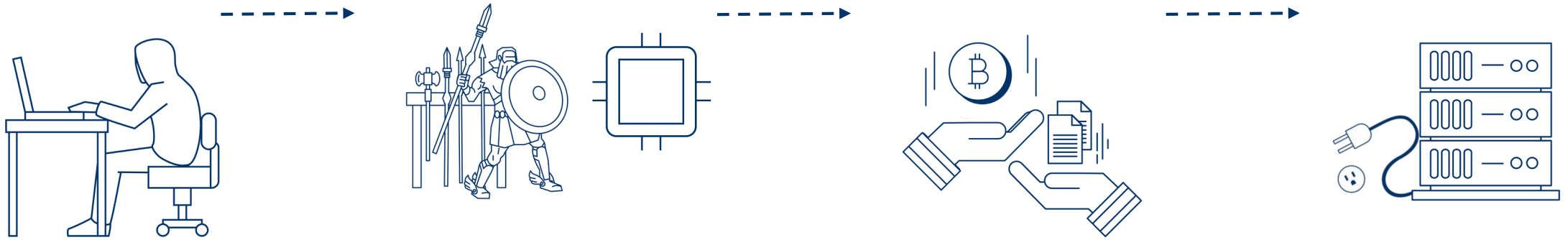
Secure firmware

Firmware attacks could be devastating

Firmware is software that provides the low-level control for a device's hardware functionality. **Firmware threats are gaining speed in the wild,** including remote and supply chain compromises that can destroy critical hardware that governs computer server functionality, and more.

Understanding the firmware threat: stages and effects

Firmware compromise		Devastation	
Infiltrate	Takeover	Exploit	Destroy
Attackers infiltrate targets with remote malware or via supply chain attacks.	**Attackers takeover** critical server firmware/hardware such as motherboards, etc.	**Corrupted firmware** leaves servers remotely vulnerable and open to ransomware.	Servers that operate in the world's largest data centers are **shutdown without mercy**.



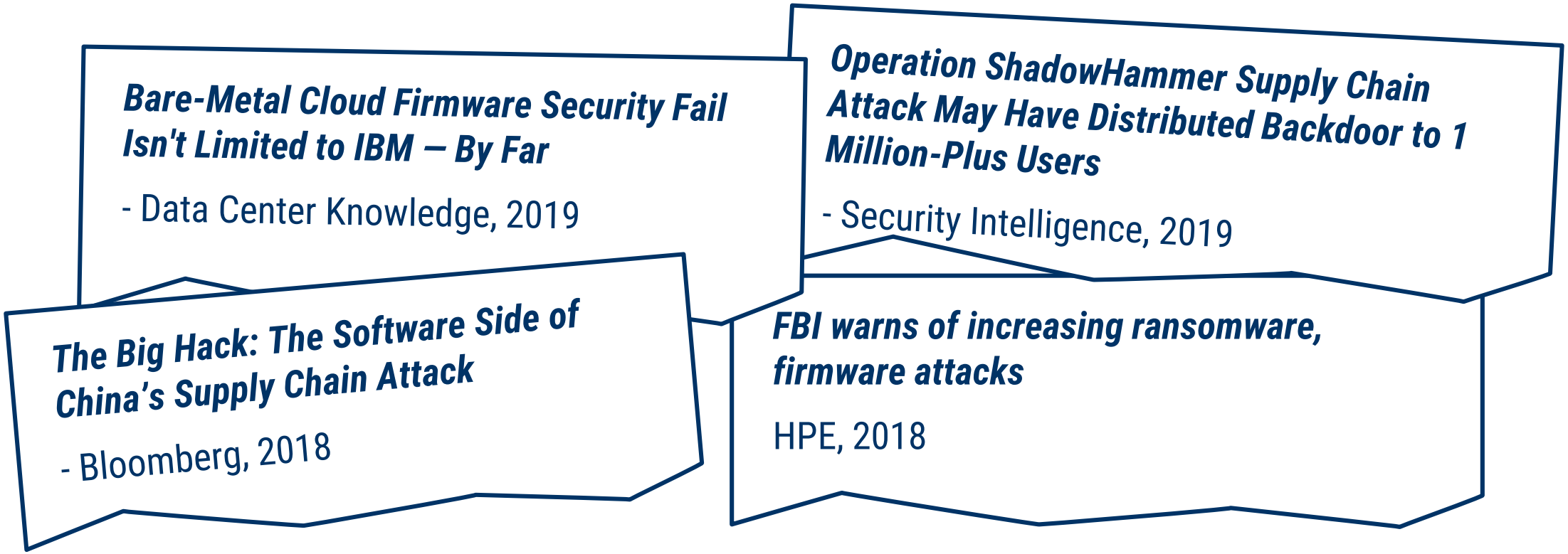
"There's firmware everywhere in your computer, and **all of it is risky**."

- Karsten Nohl, Chief Scientist at Security Research Labs, 2015

Quote: WIRED

Firmware security awareness is growing

Startups are rising to help protect the firmware in critical devices and infrastructure. In tandem, government agencies, investigative journalists, and others are **calling for improved firmware security**.



Secure firmware

refirm labs

ReFirm Labs focuses on firmware security in IoT devices.

The company offers enterprises the ability to automatically vet, validate, and monitor firmware security in connected devices.

In 2017, the cybersecurity startup incubator DataTribe took a corporate minority stake in ReFirm Labs. ReFirm Labs leverages expertise from the US intelligence community and national laboratories. Derick Naef was appointed ReFirm Labs CEO in 2019.

Investors include Data Tribe.

Most recent financing: $1.5M Corp. Min. (11/15/2017)

Total disclosed funding: $1.5M

Location: Fulton, MD

eclypsium

Eclypsium fights firmware, hardware, and supply chain attacks.

The company specializes in gaining full visibility into an organization's devices and their underlying hardware components.

Eclypsium gained notoriety after a 2019 disclosure in which the company proved that it could compromise firmware embedded in IBM's bare metal cloud computing equipment. Eclypsium works closely with Intel to secure firmware inside cloud infrastructure.

Investors include Intel Capital, Andreessen Horowitz, Madrona Venture Group, and Ubiquity Ventures.

Most recent financing: $8.75M Series A (12/4/2018)

Total disclosed funding: $11.05M

Location: Beaverton, OR

Anonymous Analytics

Personal information needs protection

Surveillance capitalism is the dominant paradigm shaping the way today's internet giants make money. The world's largest **tech companies and others increasingly profit from personal data**.

Data companies have extensive information on billions of people

			Large Online Platforms
Facebook	has profiles on	1.9 billion	Facebook users
		1.2 billion	Whatsapp users
		600 million	Instagram users
Google	has profiles on	2 billion	Android users
		1+ billion	Gmail users
		1+ billion	YouTube users
Apple	has profiles on	1 billion	iOS users
			Credit Reporting Agencies
Experian	has credit data on	918 million	people
	marketing data on	700 million	people
	„insights" on	2.3 billion	people
Equifax	has data on	820 million	people
		1 billion	devices
TransUnion	has data on	1 billion	people
			Consumer Data Brokers
Acxiom	has data on	700 million	people
		1 billion	cookies and mobile devices
	it manages	3.7 billion	consumer profiles for clients
Oracle	has data on	1 billion	mobile users
		1.9 billion	website visitors
	provides access to	5 billion	"unique" consumer IDs

Source: Cracked Labs, *Corporate Surveillance in Everyday Life*, 2017

"Our own information, from the everyday to the deeply personal, is being **weaponized against us** with military efficiency."

- Tim Cook, CEO of Apple, 2018

Quote: Reuters

Anonymous analytics can help protect us

Startups are creating **tech for anonymizing data**. Anonymized data offers privacy, reduces the risk of data breaches, and lets enterprises ethically derive insights and profit from personal data.

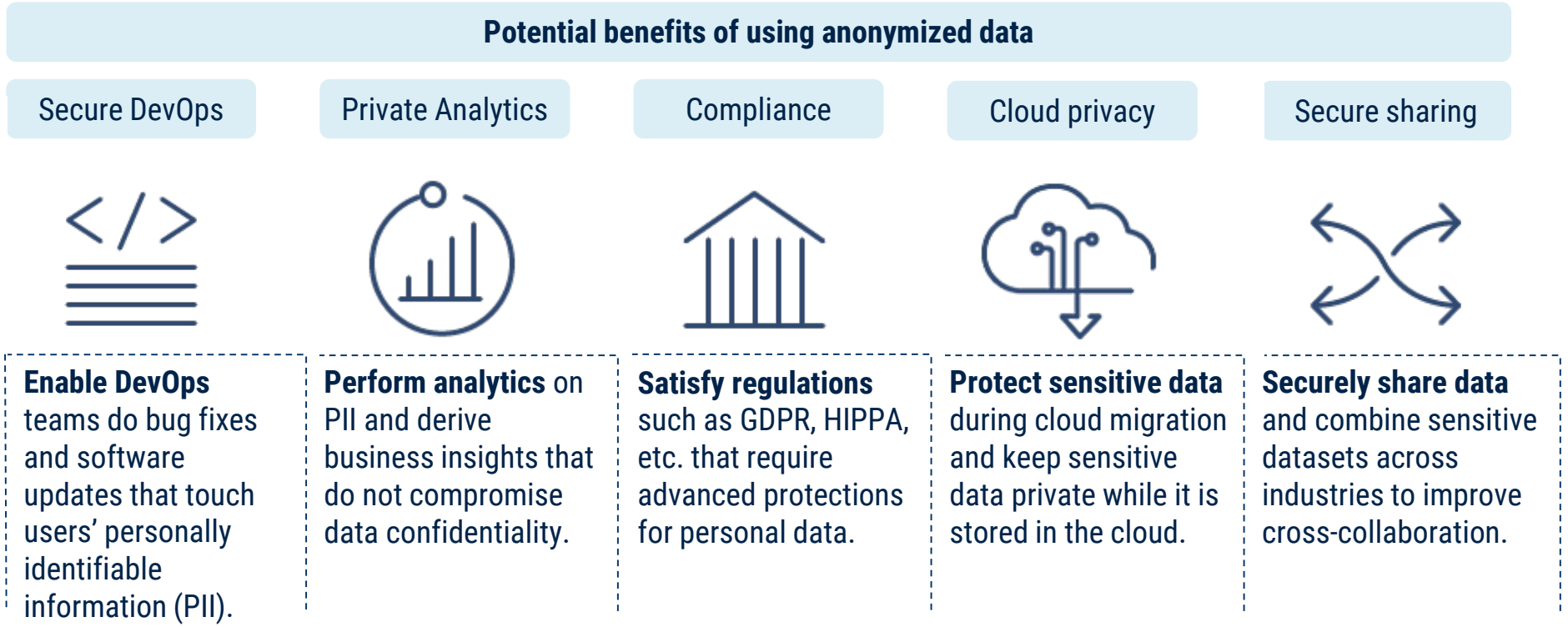


Image credit: Privitar

Anonymous analytics

PRIVITAR

Privitar offers tools for data privacy and ethical data analysis.

The company offers a mix of privacy tech, governance, and data management for enterprises to safely derive insights from PII.

In 2018, Citigroup took a corporate minority stake in Privitar for an undisclosed amount. Privitar achieved Standard Technology Partner status in the Amazon Web Services (AWS) Partner Network (APN), and the company's Singapore office opened in 2019.

Investors include Citigroup, Salesforce Ventures, CME Ventures, the Bank of England, among others.

Most recent financing: $16M Series A (7/18/2017)

Total disclosed funding: $21M

Location: London, UK

hazy

Hazy is developing tech that automates synthetic data creation.

The company works with financial clients that conduct fraud investigations and generate risk models with PII.

Hazy spun out of University College London (UCL) in 2017. The company is backed in part by Microsoft's corporate venture arm M12. Alongside financial services the company also works with clients in the utilities, telecoms, and government sectors.

Investors include M12, Ascension Ventures, Vertex Ventures, Nationwide Building Society, among others.

Most recent financing: $1.8M Seed (8/1/2018)

Total disclosed funding: $3.27M

Location: Shropshire, UK

National cybersecurity

Cyber threats are more advanced than ever

Enterprises increasingly face threats from nations in cyber space. Among the top threats are espionage and extortion. Advanced hacking tools developed by the NSA and CIA have been leaked into the wild and made available to rogue nations and organized criminals.

Select nation-state sponsored hacking campaigns 2015 – 2019 YTD (3/27/2019)

WannaCry

WannaCry and NotPetya leveraged an exploit developed by the NSA, called **EternalBlue**, which was stolen in 2017.

NotPetya

OPM, Marriot

Attributed to North Korea, the WannaCry ransomware attack froze IT systems worldwide in 2017.

Attributed to Russia, the NotPetya cyber attack targeted computer systems throughout Ukraine in 2017.

Attributed to China, attacks on the US Office of Personnel Mgmt. (2015) and Marriott (2018) exfiltrated identity data.

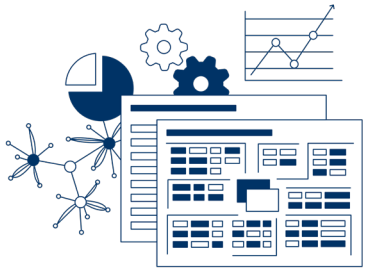
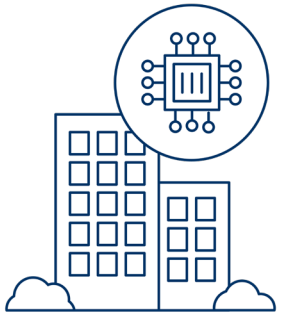
"The potential for surprise in the cyber realm will increase in the next year and beyond as **both nation states and malign actors become more emboldened and better equipped** in the use of increasingly widespread cyber toolkits."

- US Director of National Intelligence Daniel R. Coats

Cyber startups are stepping up their game

Startups are rising to develop cyberthreat detection and mitigation products **addressing nation-state directed attacks**, advanced persistent threats, and ways to classify unknown and evasive types of malware.

Cybersecurity technologies and tactics for countering nation-state level threats

File reputation & intel	Malware analysis & hunting	OT security systems
		
Sourcing intelligence and storing reputation data on troves of files helps threat researchers classify unknown and evasive malware.	**Reverse engineering new threats** and correlating threat intelligence helps researchers hunt for polymorphic malware.	**Securing operational technology (OT)** inside critical infrastructure systems can prevent nation-state attacks.

National cybersecurity

REVERSINGLABS

ReversingLabs fights advanced threats and polymorphic malware.

The company's customers include antivirus vendors, security vendors, government agencies, and commercial enterprises.

In 2011, ReversingLabs entered into a partnership agreement with the US intelligence community's strategic venture arm In-Q-Tel (IQT), to work with a number of government agencies. ReversingLabs has employees in the US, Switzerland, and Croatia.

Investors include J.P. Morgan Chase & Co. and ForgePoint Capital.

Most recent financing: $25M Series A (11/29/2017)

Total disclosed funding: $25M

Location: Cambridge, MA

Claroty's platform helps protect critical industrial control systems.

The company specializes in visibility into the a range of ICS, SCADA, and other control devices, protocols, and OT networks.

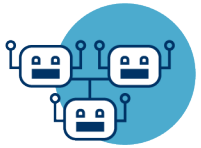
In 2019, Claroty selected U.S. Navy Admiral (Ret.) Michael S. Rogers as the Chairman of the company's Board of Advisors. Strategic investors include former leaders of the Israeli Defense Force's technology and intelligence Unit 8200.

Investors include BMW i Ventures, GM Ventures, Team 8, next 47, and Bessemer Venture Partners, among others.

Most recent disclosed financing: $60M Series B (6/11/2018)

Total disclosed funding: $92M

Location: New York, NY



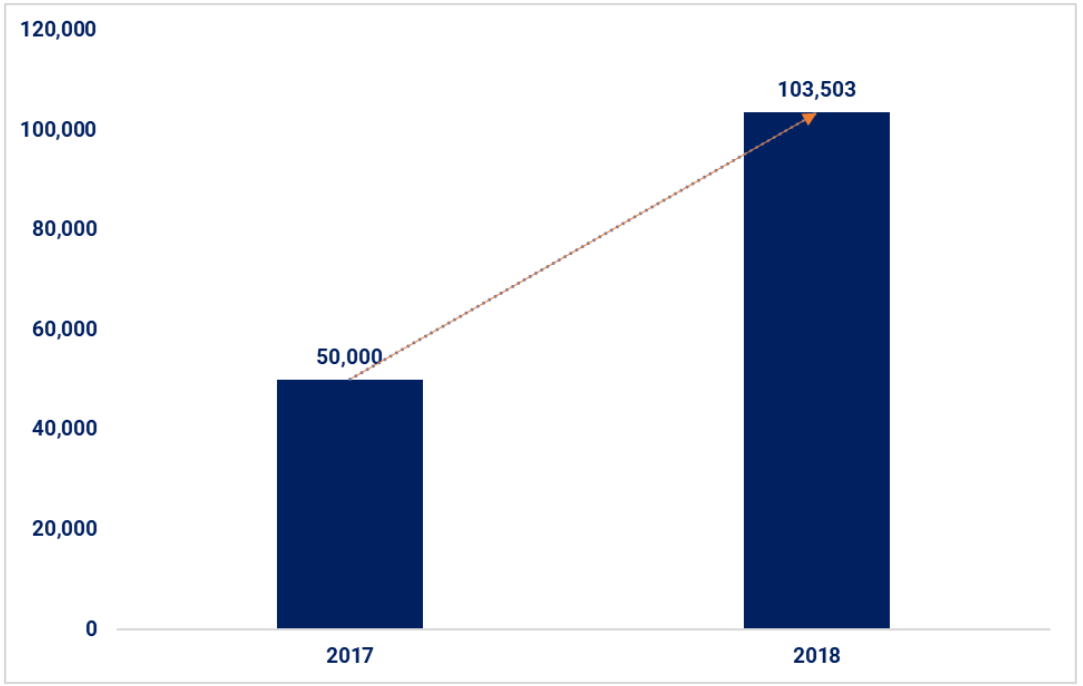
Botnet force shields

Botnets are a rising threat

Botnets are **armies of networked, infected devices** that simultaneously attack and overwhelm websites, online businesses, and other devices. Domain names registered solely to control **botnets are skyrocketing**.

Last year, compared to 2017, there was ***a 100% increase*** in the number of the domain names registered and set up by cybercriminals for the sole purpose of commanding and controlling botnets.

Number of botnet control domain names registered in 2017 vs. 2018



CBINSIGHTS Source: Spamhaus Botnet Threat Report, 2019

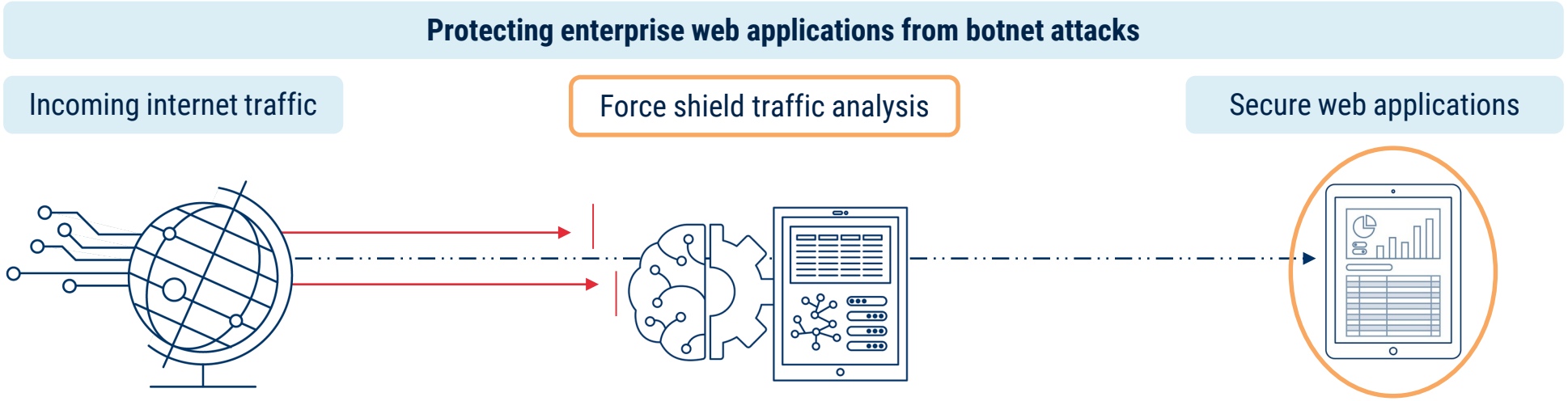
"The bad guys are experimenting with how they can **use IoT botnets to make money**."

- Anthony Giandomenico, Senior Security Strategist and Researcher at Fortinet, 2019

Quote: CIO

Botnet defense is getting better

Artificial intelligence and machine learning technologies are being applied to botnet security. Startups are using AI to analyze incoming internet traffic to **flag potentially malicious activity at machine speed**.



Incoming threats from botnets include distributed denial of service attacks (DDoS), SQL injection, among others.

Flagging malicious activity before incoming traffic reaches the web application protects critical digital assets.

Critical web applications can include eCommerce shopping carts, online banking portals, email services, and more.

Botnet force shields

perimeterx

PerimeterX offers behavior-based threat detection for websites.

The company uses AI and behavioral fingerprinting technologies to detect and defend websites from various types of botnet attacks.

Behavioral fingerprinting involves analyzing the user and distinguishing normal behavior and an anomalous behavior that looks like it's coming from an automated tool. PerimeterX has a presence in the US and Israel.

Investors include Scale Venture Partners, Adams Street Partners, Vertex Ventures, Data Collective, and Canaan Partners.

Most recent financing: $43M Series C (2/11/2019)

Total disclosed funding: $78M

Location: San Mateo, CA

Signal Sciences

Signal Sciences helps defend high-traffic web applications.

The company specializes in visibility into the a range of ICS, SCADA, and other control devices, protocols, and OT networks.

Signal Sciences is a DevOps security company. This means the platform is deployed in the software programming arena and is meant to aid developers in the creation of secure web applications. The company has a presence in California, New York, and Tokyo.

Investors include Alex Stamos, Harrison Metal, CRV, and Index Ventures, among others.

Most recent disclosed financing: $35M Series C (2/5/2019)

Total disclosed funding: $61.7M

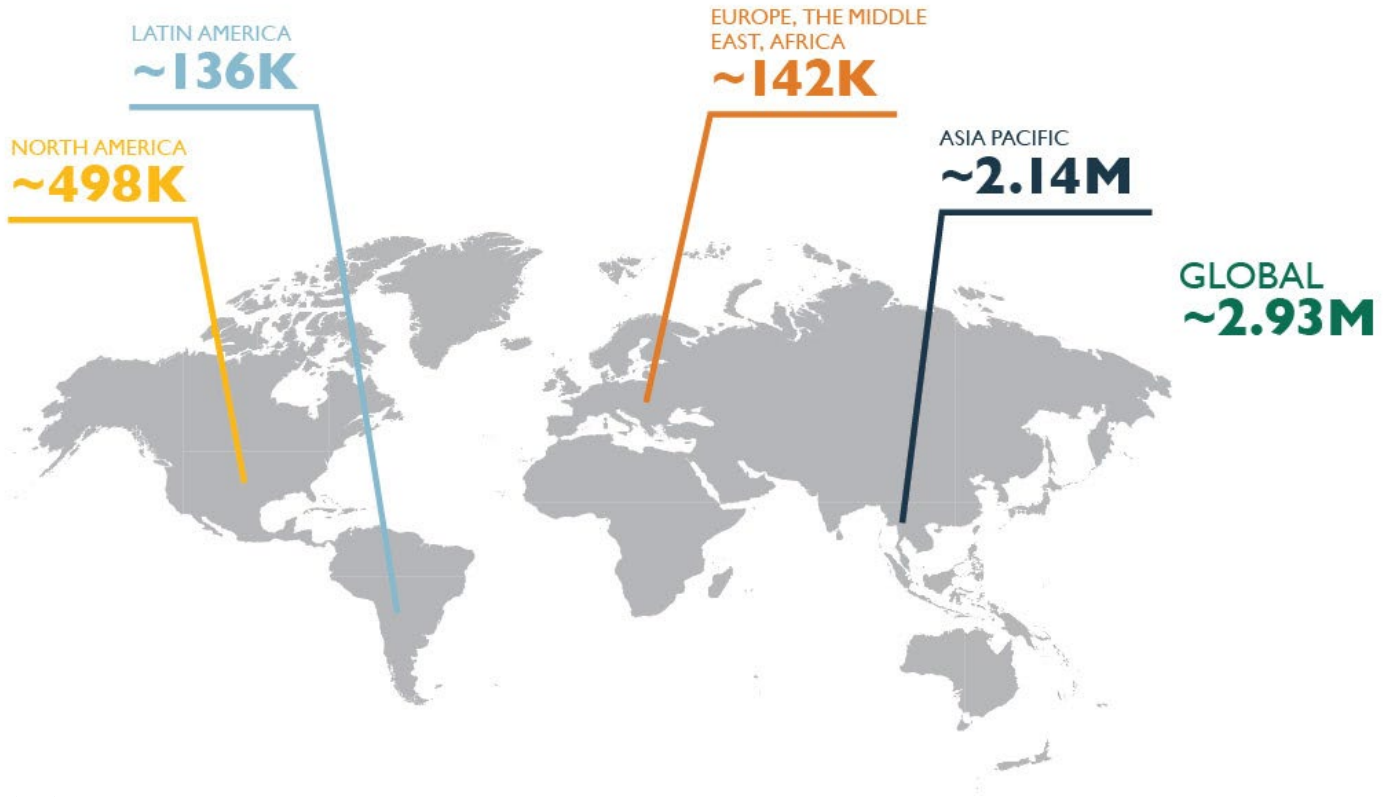
Location: Venice, CA

Infosec education

Cybersecurity needs more qualified people

There is a global shortage of qualified personnel available for employment in the cyber security industry. In fact, estimates say **the world is short roughly 3 million cybersecurity professionals**.

Number of additional cybersecurity personnel needed around the world, 2018



CBINSIGHTS

Source: (ISC)² Cybersecurity Workforce Study, 2018

"… industry reports almost unanimously depict **the education and training system** as the main culprit behind the shortage…"

- Tommaso De Zan, PhD, Centre for Doctoral Training in Cyber Security, University of Oxford, 2019

Quote: Council on Foreign Relations via Net Politics

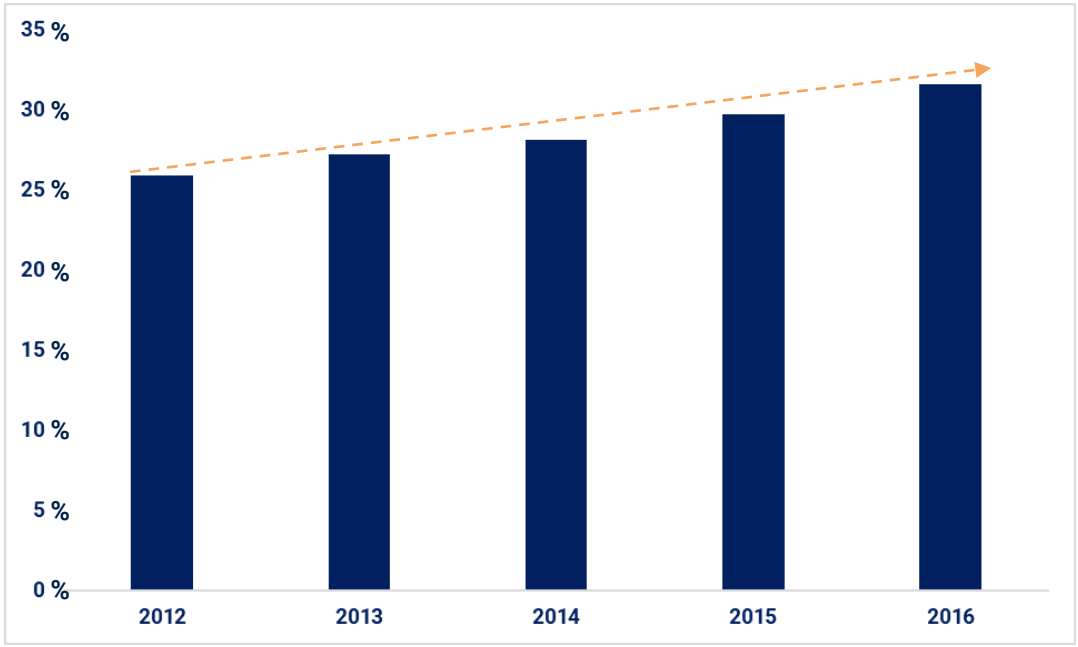
Cyber training opportunities are spreading

Startups are rising to capitalize on the need for qualified cybersecurity personnel. Companies are **leveraging the popularity of online courses** and gamification techniques to compel more people to train in cyber.

The proportion of the higher education student body taking advantage of **online education courses increased each year from 2012 - 2016**.

As of fall 2016, there were 6M+ students taking at least one online education course, comprising **31.6% of all higher education enrollments**.

Percentage of US students taking online courses 2012 - 2016



Source: Grade Increase: Tracking Distance Education in the United States, Babson Survey Research Group, 2018

Infosec education

IMMERSIVELABS

Immersive Labs streams gamified cyber training labs on demand.

The startup offers multiple disciplines: secure coding, reverse engineering, ethical hacking, security investigation, and more.

In 2019, financial services giant Goldman Sachs led Immersive Labs' Series A round. Goldman Sachs intends to deploy Immersive Labs' virtual cybersecurity learning platform to incentivize its 8,000+ software developers and other employees to train cyber.

Investors include Goldman Sachs, and the UK Department for Digital, Culture, Media and Sport, among others.

Most recent financing: $8M Series A (1/14/2019)

Total disclosed funding: $8.02M

Location: Bristol, UK

CYBRARY

Cybrary is an online cyber classroom and professional network.

The startup provides free cyber training classes, from beginner to advanced, and is starting to charge for premium course materials.

In 2019, Cybrary teamed up with nonprofit Melwood. Melwood will provide students with technical training provided by Cybrary, job search assistance, placement, and on-the-job coaching.

Investors include Arthur Ventures, Ron Gula, New Stack Ventures, and Inner Loop Capital.

Most recent financing: $2.5M Series A-II (9/5/2018)

Total disclosed funding: $7.7M

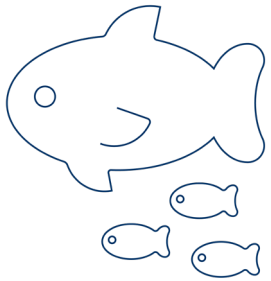
Location: Greenbelt, MD

Armored email

Email is increasingly vulnerable

Email continues to be the #1 threat facing IT security. Alongside the growth of email-based social engineering attacks known as phishing, other **sophisticated email threats are rising.**

Rising email-based cybersecurity threats

Whaling	Misdirected emails	Man-in-the-middle
		
Attacks targeting the "big fish" inside an organization generally involve fake financial requests sent on behalf of real executives.	**Insider data privacy threats** whereby a sender accidentally inputs an incorrect recipient into any of the recipient fields.	**Eavesdropping and altering** the communication between two unwitting parties who believe they have privacy.

"Employees are one of the top cybersecurity risks to organizations **by merely clicking malicious URLs or bypassing security controls**, however unintentional."

- Dr. Salvatore Stolfo, professor of computer science at Columbia University, 2018

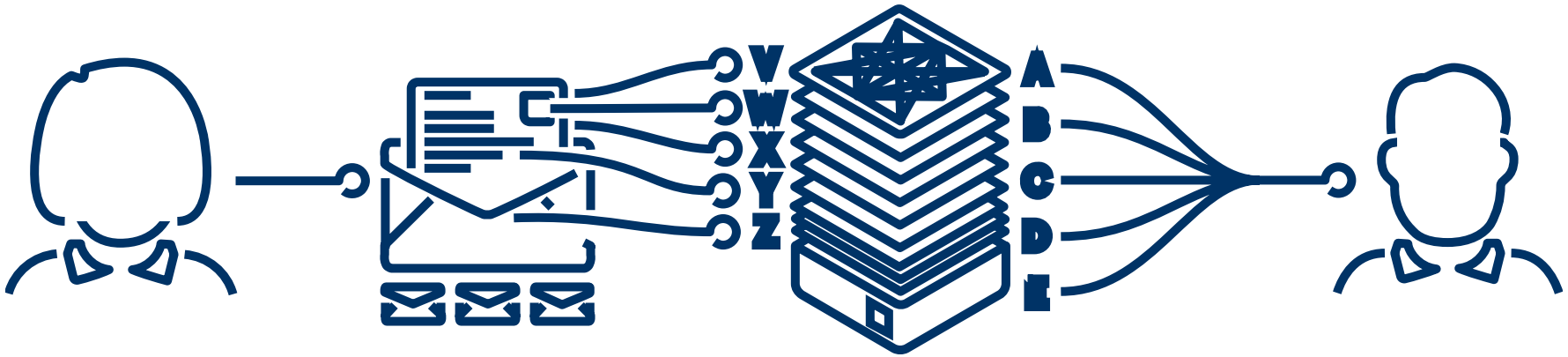
Quote: PhoenixNAP

Email is getting armored

Startups are rising to help enterprises protect their email-based communications. **Emerging technologies such as AI and machine learning, and advances in cryptography, are boosting email security**.

AI & machine learning, advanced cryptography, are the future of email security

Encrypted & tracked | Analyzed & flagged | Received & verified



Encrypting and tracking messages helps ensure confidentially and integrity.

AI and machine learning pattern recognition enables advanced email threat flagging services.

Encryption mechanisms can help verify that emails have come from trusted sources.

Image credit: Tessian

Armored email

TESSIAN

Tessian specializes in analyzing emails for security threats.

The startup is protecting enterprises against inbound spear phishing emails and flagging employees' misdirected emails.

Tessian uses AI and machine learning to analyze historical email data and identify potential security threats early. By knowing what normal email activity looks like, it can automatically detect any anomalies that may imply a security threat.

Investors include Sequoia Capital, Accel, Amadeus Capital Partners, among others.

Most recent financing: $42M Series B (2/27/2019)

Total disclosed funding: $58M

Location: London, UK

virtru

Virtru offers an email encryption and data privacy platform.

The company gives enterprises control over who receives, reviews, and retains their sensitive digital information.

Virtru was co-founded by Will Ackerly, a former lead security architect for the National Security Agency's first cross-domain cloud. There he invented advanced encryption techniques for dynamically securing individual pieces of moving data sets.

Investors include Samsung Ventures, Bessemer Venture Partners, and Soros Fund Management, among others.

Most recent financing: $37.5M Series B (5/31/2018)

Total disclosed funding: $76.5M

Location: Washington, DC

Cloud-native security

Cybersecurity needs to be cloud-native

Enterprises are migrating infrastructure and services to the cloud. In tandem, the **complex virtual and legacy on-premise IT environments** being created demand cybersecurity that is built for the cloud.

Today's enterprises face challenges securing complex cloud environments

Public cloud	Hybrid cloud	Private cloud
		
Public clouds are hosted by AWS, Azure, etc., but **server configurations are often left up to customers'** developer and security teams.	**Hybrid clouds spread resources** over both public and private infrastructure, creating **unique data security challenges** when switching between clouds.	**Private clouds are restricted** to being accessed exclusively by a single organization. Private control means **data security falls entirely on the enterprise**.

"With more and more data — and with more of that data deemed mission critical — created, stored, and managed in the cloud, **bad actors will naturally take aim.**"

- Ann Johnson, Vice President of Microsoft's Enterprise Cybersecurity Group, 2018

Quote: SecurityRoundTable.org

Cloud-native security is here

Startups are rising to help secure the future of could computing with solutions that **increase network visibility and control**, pinpoint vulnerabilities early, and help achieve compliance and manage risk.

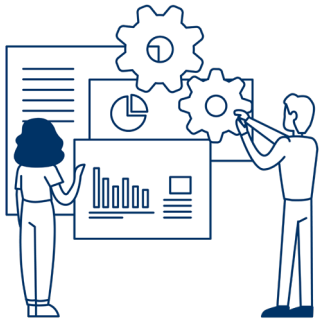
Emerging technologies and tactics for securing the future of cloud computing

Container visibility

Monitoring container activity and use architectures at the scale and speed of modern applications.

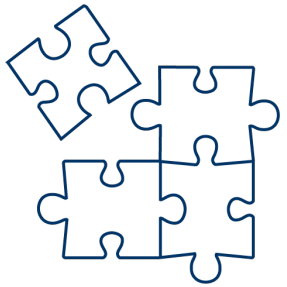
In 2018, more than 70M records were stolen or leaked from poorly configured S3 buckets.*

Vulnerability management



Equipping DevOps teams to secure entire container life cycles from design through to run time.

Micro segmentation



Separating cloud resources to granularly secure communication between microservice workloads.

*Source: Symantec Internet Security Threat Report, 2019

Cloud-native security

StackRox provides cyber threat protection for cloud containers.

The company helps DevOps teams map container environments from services to applications, and monitors for vulnerabilities.

In 2018, StackRox obtained an undisclosed investment from the US intelligence community's strategic venture arm In-Q-Tel (IQT). StackRox focuses on securing Kubernetes, an open-source container orchestration system for application deployment.

Investors include In-Q-Tel, Sequoia Capital, Amplify Partners, and Redpoint Ventures.

Most recent disclosed financing: $25M Series B (4/10/2018)

Total disclosed funding: $39M

Location: Mountain View, CA

Portshift offers a platform for securing cloud-based applications.

The company helps enterprises deploy, manage, and secure application workloads by infusing security into DevOps.

Portshift's core technology uses digital signing techniques to provide threat prevention capabilities for cloud applications. Essentially, when a policy violation is found with an improperly signed application, Portshift can isolate the offending application.

Investors include Team8.

Most recent financing: $5.3M Seed (11/20/2018)

Total disclosed funding: $5.3M

Location: Tel Aviv, Israel

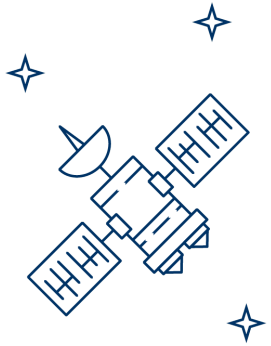
Secure programming

Some software can't afford to fail

Software operating inside critical infrastructure, autonomous vehicles, satellites, and more needs to work perfectly. **Safeguarding mission critical software** saves money and can prevent the loss of human life.

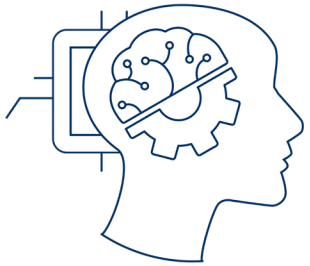
The world runs on mission critical software

Communications & GPS



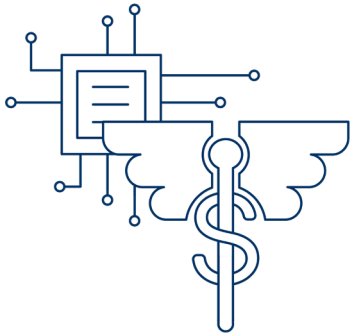
Software inside satellites is critical to communications and geographic positioning systems that underpin the global economy.

Artificial Intelligence



AI is tasked with decision making for devices and infrastructure such as smart speakers, factories, autonomous vehicles, and more.

Healthcare



The number of medical device **recalls** in the United States spiked 126% in 2018, mostly due to device software issues.*

Software is eating healthcare, which means patient outcomes can increasingly be directly linked to proper digital health programming.

*Source: Stericycle Recall Index, 2018

"**Boeing was going to have a software fix** in the next five to six weeks… we told them, 'yeah, it can't drag out.' And well, here we are."

The New York Times

- Michael Michaelis, safety official at the American Airlines Pilots Union and a Boeing 737 captain, 2019

Quote: The New York Times

Mission critical cybersecurity is ‘shifting left’

Secure programming startups are rising to help enterprises ‘shift left’ and prioritize **cybersecurity earlier in the software development timeline**. Traditionally, bugs are identified later in the timeline and as a costly step after product deployment.

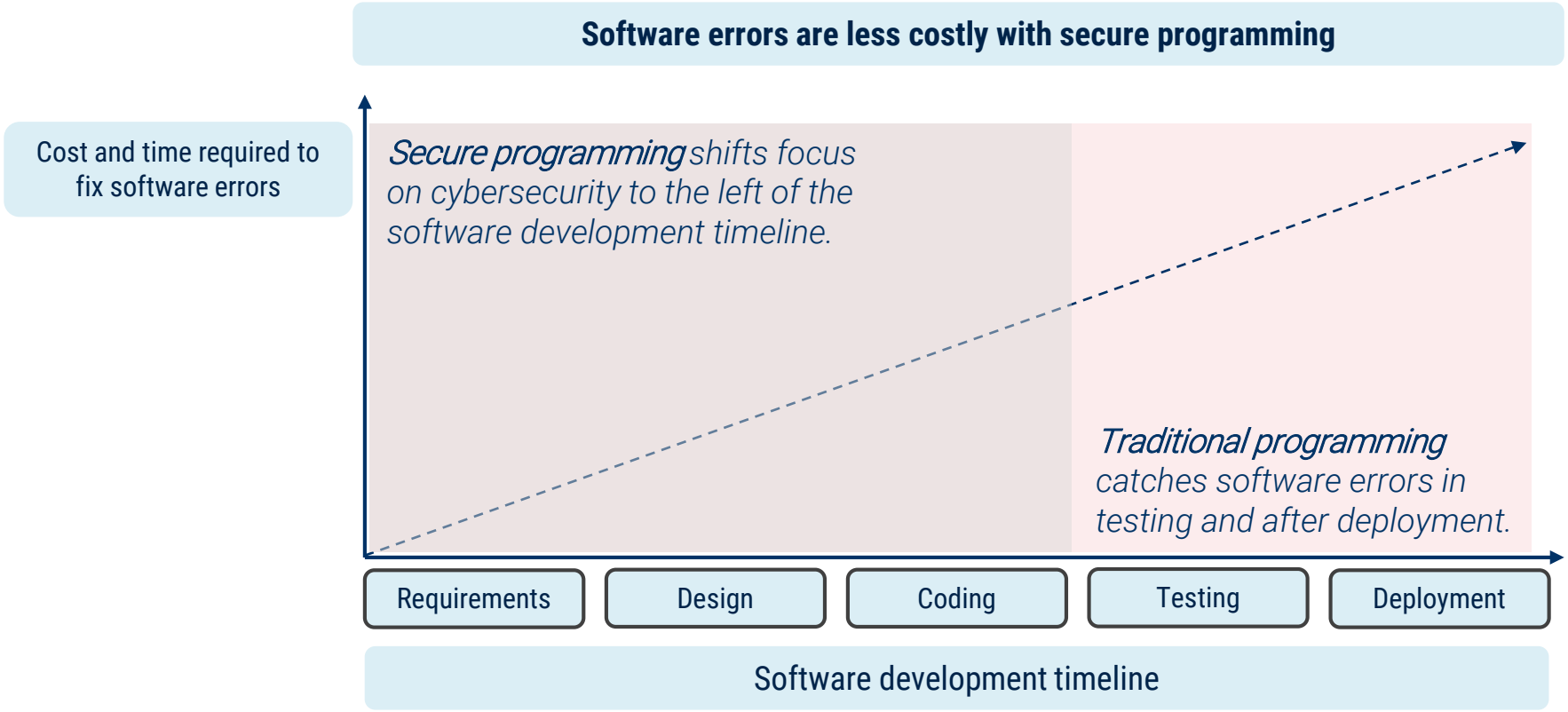


Image credit: Software Testing Help

Secure programming

TANGRAMFLEX

Tangram Flex secures mission critical software used for defense.

The company's customers include the DOD and contractors that make embedded systems used in aircraft, missiles, and more.

In 2018, Tangram Flex spun out of Galois' computer science and cryptography work for DARPA, the Intelligence Community, Navy, Air Force, and NASA. CTO John Launchbury, previously served as Director of the Information Innovation Office (I2O) at DARPA.

Investors include Hale Capital Partners.

Most recent financing: $4.5M Series A (12/18/2018)

Total disclosed funding: $4.5M

Location: Dayton, OH

SECURE CODE WARRIOR

Secure Code Warrior helps train developers to write secure code.

The company offers hands-on, interactive learning scenarios that enable developers to master cybersecurity coding techniques.

In 2019, Secure Code Warrior partnered with the crowdsourced cybersecurity startup Bugcrowd to teach developers new programming techniques and languages that correspond with fixing Bugcrowd's latest discovered software vulnerabilities.

Investors include AirTree Ventures, Paladin Capital Group, Wayra, NCSC Cyber Accelerator, and FinTech Innovation Lab.

Most recent financing: $3.5M Series A (9/11/2018)

Total disclosed funding: $3.53M

Location: Sydney, New South Wales, Australia

Attack simulators

The rise of active enterprise cyber defense

We are witnessing a paradigm shift in enterprise cybersecurity. **Organizations are shifting from passive defense to active defense,** including **embracing white-hats** for simulating cyber attacks and more.

The shift from passive to active cyber defense

Passive	Active	Offensive

Reactive cybersecurity includes finding invading code, unplugging affected systems, patching, and applying patches network-wide.

Proactive cybersecurity includes threat intelligence, disruption of ongoing attacks, **embracing white-hats for attack simulations**, etc.

Directly engaging adversaries by stealing-back data, executing "good guy" malware, striking preemptively, and more.

"Now, in 2019 more than ever, **I need to prove to my board, executives and customers that they can trust that our security is working**, and therefore trust our brand."

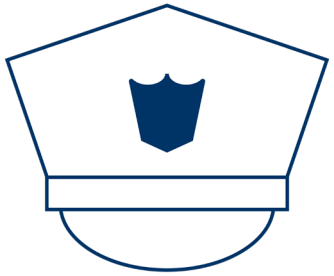
- Ethan Steiger, Vice President & Chief Information Security Officer at Domino's, 2019

Quote: Synack, The 2019 Trust Report

Attack simulations are active cybersecurity

Startups are rising to help enterprises simulate cyber attacks to **proactively uncover attackers' pathways to critical digital assets**. In turn, enterprises can **validate cybersecurity tools and garner trust**.

The benefits of conducting active cyber threat simulations

Police vulnerabilities	Validate cybersecurity	Garner trust
		
Identify weaknesses in IT systems that present opportunities for attackers to circumvent controls and find critical enterprise assets.	**Prove cybersecurity tools work** by continuously testing your vendors' products and flagging when simulated attacks are successful.	**Openly simulating attacks** helps the public and clients know that your organization is taking a more proactive approach to security.

Attack simulators

Synack

Synack offers crowdsourced cybersecurity penetration testing.

The company scans an organization's network and alerts researchers of vulnerabilities, changes, or unknown events.

Synack serves US defense agencies including the Pentagon, Army, and Air Force, among others. In 2016, Synack was awarded the Department of Defense's first cyber attack simulation program "Hack the Pentagon." The DoD granted Synack the contract again in 2018.

Investors include Allegis Cyber, M12, Google Ventures, Kleiner Perkins Caufield Byers, and Intel Capital, among others.

Most recent disclosed financing: $21.25M Series C (4/11/2017)

Total disclosed funding: $55.27M

Location: Redwood City, CA

XM CYBER

XM Cyber provides an automated cyber threat simulator.

The company specializes in applying AI to automatically simulate system exploits and find vulnerabilities for early remediation.

XM Cyber was co-founded by Tamir Pardo, who served as chief of Mossad, Israel's elite security intelligence service between 2011 and 2016. Customers are mainly in the banking, insurance, and critical infrastructure industries.

Investors include Nasdaq Ventures, ING Belgium, UST Global, and Shaul Shani, among others.

Most recent financing: $22M Series A (11/13/2018)

Total disclosed funding: $37M

Location: Herzliya, Israel

APPENDIX

Cyber patrols on top

Global internet intelligence startup **Expanse** is the only 2019 Cyber Defender to raise over $100M.

All of the top 10 most well-funded 2019 Cyber Defenders raised over $30M.

All four startups in the Botnet Force Shields and Armored Email categories are in the top 10 most well-funded.

2019 Cyber Defenders most well-funded companies

as of 2019 YTD (4/9/2019)

Rank	Company	Disclosed Funding ($M)	2019 Cyber Defender category
1	**Expanse**	135.97	Cyber patrols
2	Claroty	$92	National cybersecurity
3	PerimeterX	$78	Botnet force shields
4	Virtru	$76.5	Armored email
5	Signal Sciences	$61.7	Botnet force shields
6	Tessian	$58	Armored email
7	Synack	$55.3	Attack simulators
8	Signal Foundation	$50	Democratized encryption
9	Chainalysis	$47.7	Crypto forensics
10	StackRox	$39	Cloud-native security

Two VCs on top

The California based investors **Bessemer Venture Partners**, and **O'Reilly AlphaTech Ventures** are the only VCs to participate in 5 deals to 2019 Cyber Defenders.

No investors outside of the 8 listed participated in more than 4 deals to 2019 Cyber Defenders.

2019 Cyber Defenders most active investors

Measured by number of deals to the cohort as of 2019 YTD (4/2/2019)

Rank	Investor	Number of deals to 2019 Cyber Defenders:
1	**Bessemer Venture Partners**	5
1	**O'Reilly AlphaTech Ventures**	5
3	New Enterprise Associates	4
3	Founders Fund	4
3	Intel Capital	4
3	Accel	4
3	Vertex Ventures	4
3	Neotribe Ventures	4

METHODOLOGY

How the categories were selected: To identify our categories, we used CB Insights' Trends tool, which mines and organizes million of media articles to quantify rising media attention to tech trends.

How the companies were selected: We used CB Insights' Mosaic Score, which uses data to track private company health based on recency of financing, total 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 in some detail.

CBINSIGHTS

WHERE IS ALL THIS DATA FROM?

The CB Insights platform has the underlying data included in this report

CLICK HERE TO SIGN UP FOR FREE

cbinsights.com

@cbinsights