2018 Cyber Defenders

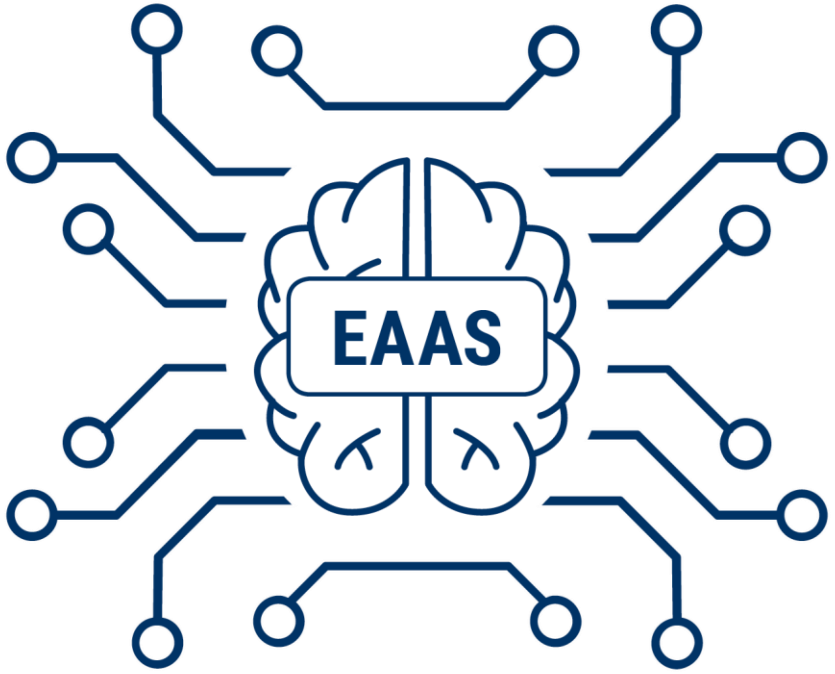
This year's trends, opportunities, and high-momentum startups with the potential to shape the future of cybersecurity.

CBINSIGHTS

WHO ARE WE

The technology market intelligence platform.

CB Insights software lets you predict, discuss, and communicate emerging technology trends using data in ways that are beyond human cognition.



Contents

CYBERSECURITY IS TOP OF MIND

Nearly 1,000 data-breaches occurred in the first-half of 2017.*

Each new breach raises fears that trust in the global digital economy is eroding due to death by a thousand hacks.

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

* breachlevelindex.com (Jan. – June '17)

CYBERSECURITY IS A C-SUITE ISSUE

"The battle against cybercrime will always continue, but we have made a great deal of improvement... What was once a field looked after only by CISOs, chief information security officers of major companies, is **now a hot topic of concern for CEOs and boards across the globe**."

AIRBUS

Markus Braendle

SVP, Head of Cybersecurity at Airbus CyberSecurity

WHAT MAKES A CYBER DEFENDER?

ˈSAɪBƏR DɪˈFƐNDƏR

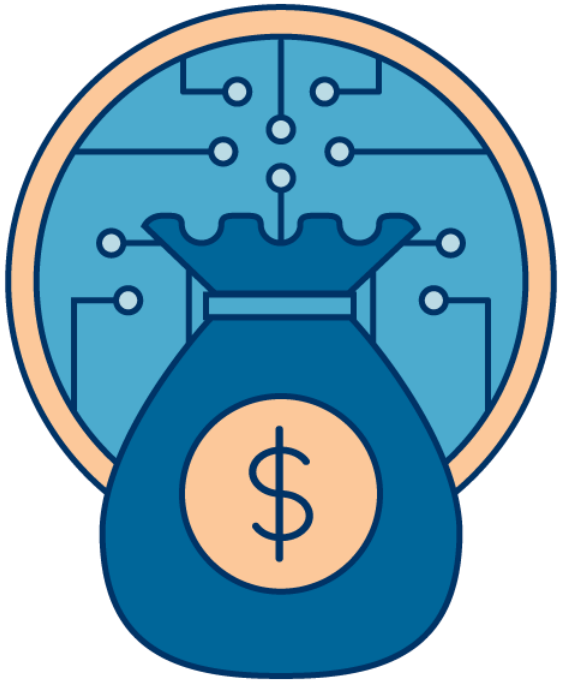
Our selected startups are early- to mid-stage high-momentum companies pioneering technology with the potential to transform cybersecurity.

Unicorns valued at $1B+, companies that have raised funding past the Series C stage, and companies that have not raised funding since 2016 are excluded.

But first some funding trends…

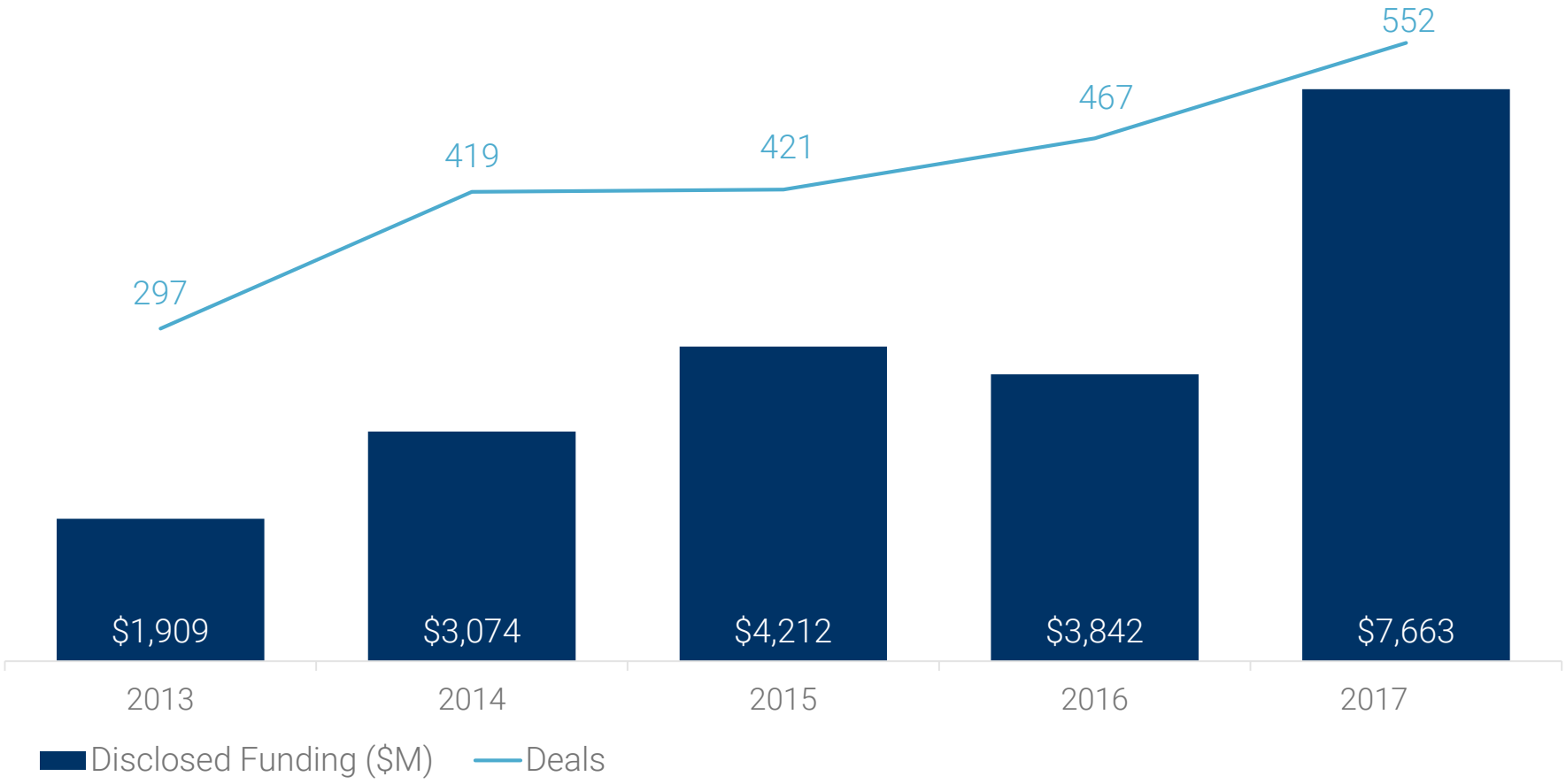
CYBERSECURITY

global equity funding trends



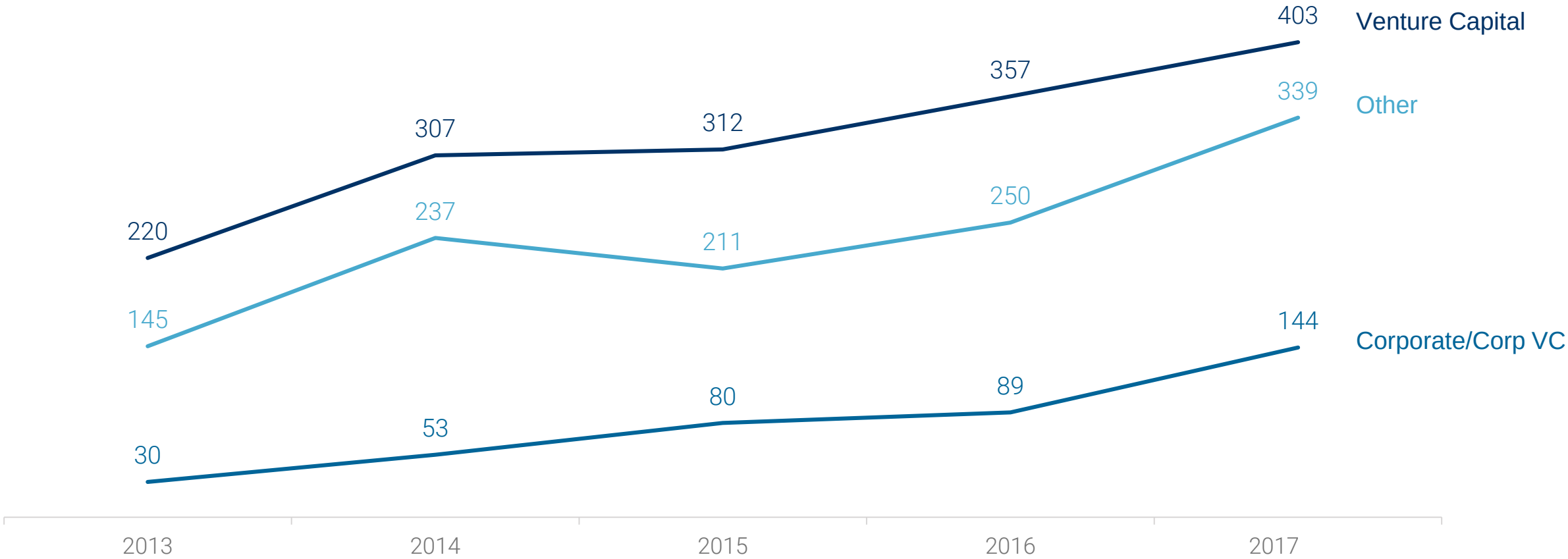
2017 was a record year for cybersecurity

Annual global deals and financing 2013 – 2017



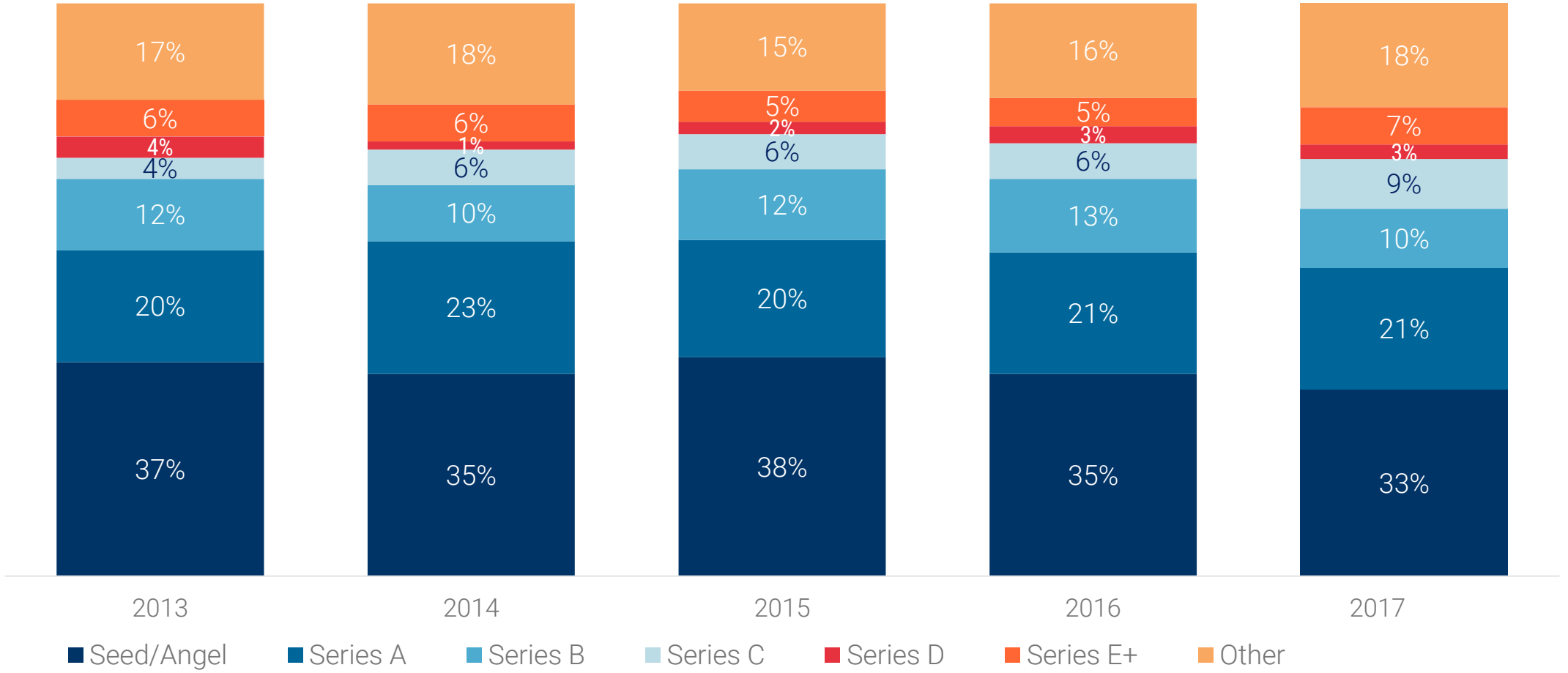
2017 was a record year for 1st time investors

Annual number of 1st time investors in cybersecurity 2013 - 2017



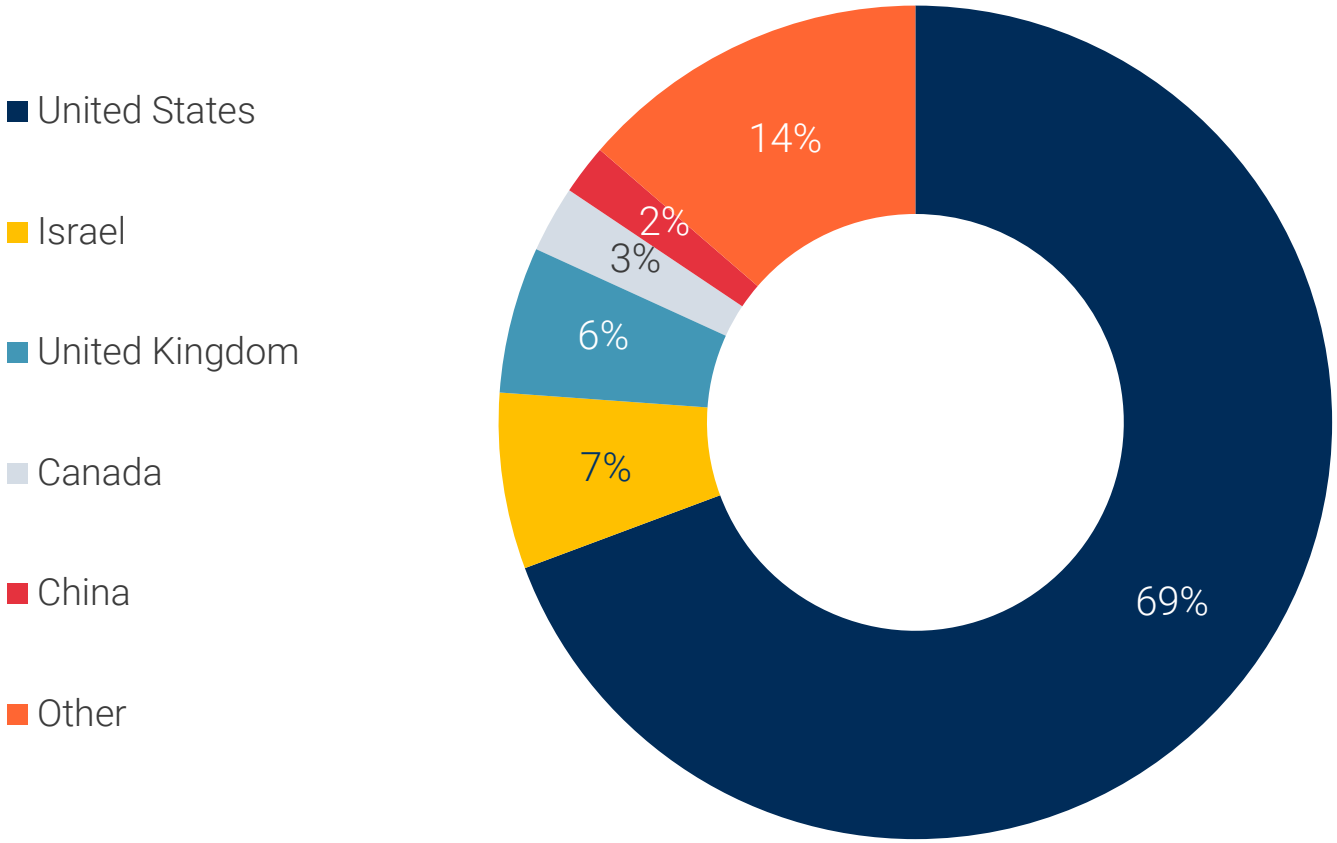
Early-stage (Seed – Series A) deals fell to a 5-year low

Annual deal share by stage to private cybersecurity companies 2013 - 2017



Well behind the US, Israel now tops the UK

Cybersecurity global deal share by country 2013 - 2017



PRIVATE MARKET LEADERS

There are now nine cybersecurity unicorns

Private cybersecurity companies valued at $1B+ as of 4/12/2018:

WHAT MAKES A CYBER DEFENDER?

ˈSAɪBƏR DɪˈFƐNDƏR

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 2016 are excluded.

Highlights from the 2017 Cyber Defenders

Since we released the first edition of this report on 3/29/2017, 21 out of the 30 companies we featured were involved in deals (**15 financings totaling ~$270M, and 6 exits** as of 4/10/2018).

Select financings:

Darktrace	$75M Series D
Sift Science	$53M Series D
Anomali	$40M Series D
Auth0	$30M Series C
CyberX	$18M Series B
Nozomi Networks	$15M Series B
Karamba Security	$12M Series B
Karamba Security	$10M Series C
Protectwise	$6M Convertible Note
Illusive Networks	$5M Series C-II
TrapX	Undisclosed Series C

Exits:

IDQ	Acquired by SK Telekom
Skycure	Acquired by Symantec Corporation
CYENCE	Acquired by Guidewire Software
ARGUS CYBER SECURITY	Acquired by Continental
PHISHME (fka Cofense)	Acquired by BlackRock and Pamplona Capital Management
FORTSCALE	Acquired by RSA

This year's Cyber Defender categories

Fraud hunters
Finding and eliminating synthetic identity fraud

DIY digital privacy
Tools to help consumers take digital privacy back into their own hands

Identity vaults
Preserving the secrecy of enterprise customers' personal information (PII)

Continuous authentication
Identifying people based on behaviors throughout a work session

Human-factor security
Training and technology to thwart email-based attacks known as phishing

Next-gen cloud security
Source code- and policy-driven approaches to secure complex cloud environments

Security by design
Embedding security controls into software development operations

Fileless-attack security
The future of fighting malware on endpoints and protecting enterprise networks

Autonomous watchdogs
Software that automatically executes security protocols

Dark web intelligence
Startups monitoring illicit activity in the hidden corners of the Internet

Web policing
Patrolling websites, apps, and online services for malicious Internet traffic

IIoT shields
Defending connected critical infrastructure against espionage and sabotage

Cyber actuaries
Startups offering tools for quantifying cyber risk and sizing insurance premiums

Crowdsourced security
Ethical hackers employed to discover software vulnerabilities

The 2018 Cyber Defenders

Fraud hunters

SIGNIFYD

feedzai

DIY digital privacy

Keybase

CIPHY

Identity vaults

BigID

D-ID

Continuous authentication

UNIFYID

BIOCATCH

Human-factor security

KnowBe4

IRONSCALES

Next-gen cloud security

TIGERA

ShiftLeft

Security by design

snyk

aqua

Fileless-attack security

Virsec

MINERVA

Autonomous watchdogs

RESPOND

JASK

Dark web intelligence

FLASHPOINT

TERBIUM LABS

Web policing

StealthSecurity

netsparker

IIoT shields

DRAGOS

CYLUS

Cyber actuaries

corax

cyberGRX

Crowdsourced security

hackerone

detectify

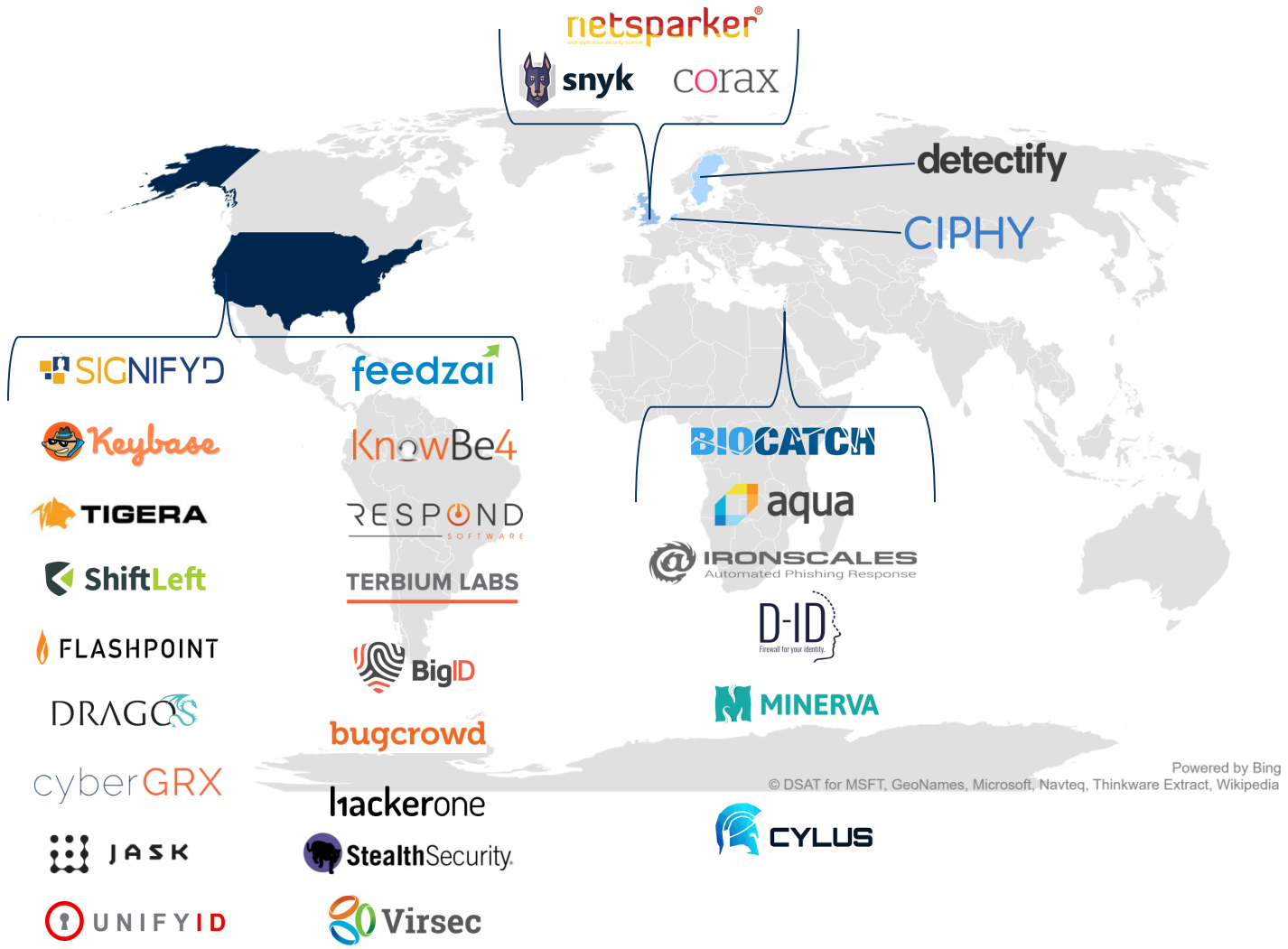
bugcrowd

The US has the most Cyber Defenders

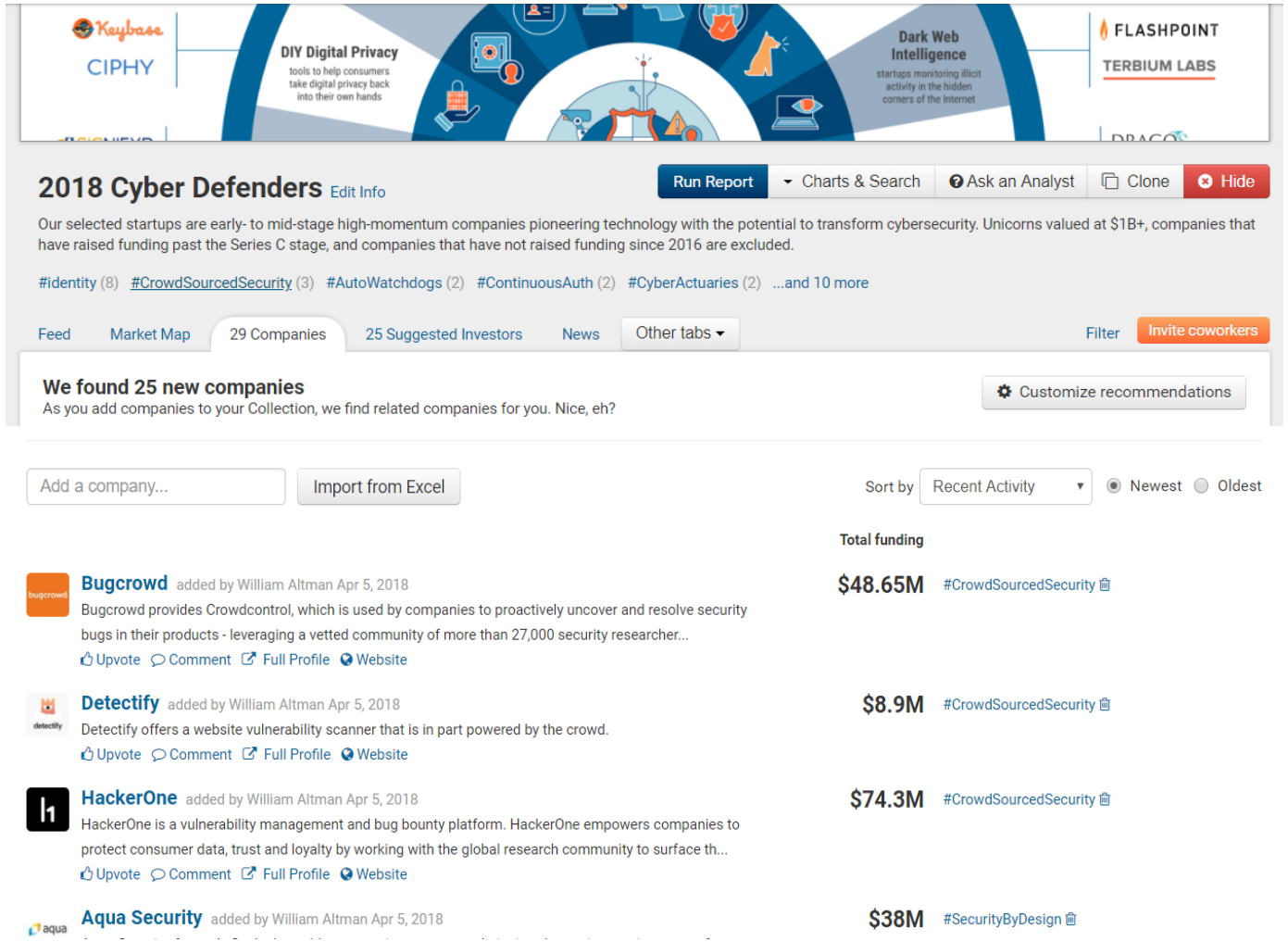
62% of the 2018 Cyber Defenders have their headquarters in the US, mostly in California.

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

Sweden and the Netherlands have one each.



2018 Cyber Defenders expert collection on CBI



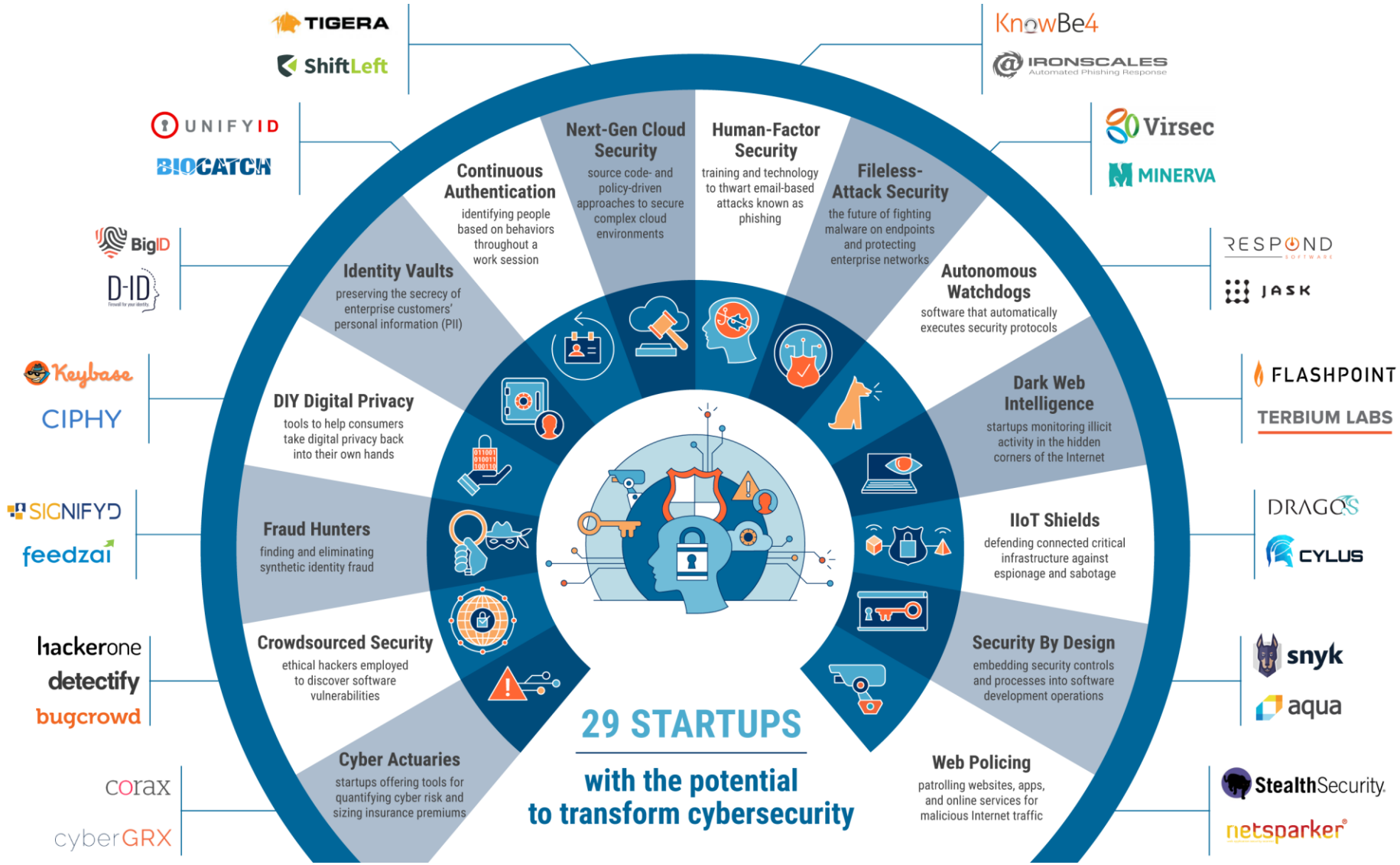
Track all of the startups in this presentation and many more on our platform using CB Insights' Collections.

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

CLICK HERE TO SEE THE COLLECTION

CBINSIGHTS

2018 CYBER DEFENDERS



Personally identifiable information (PII) is increasingly tracked and surrendered online. In tandem, massive data breaches have unleashed unprecedented amounts of PII into the wild.

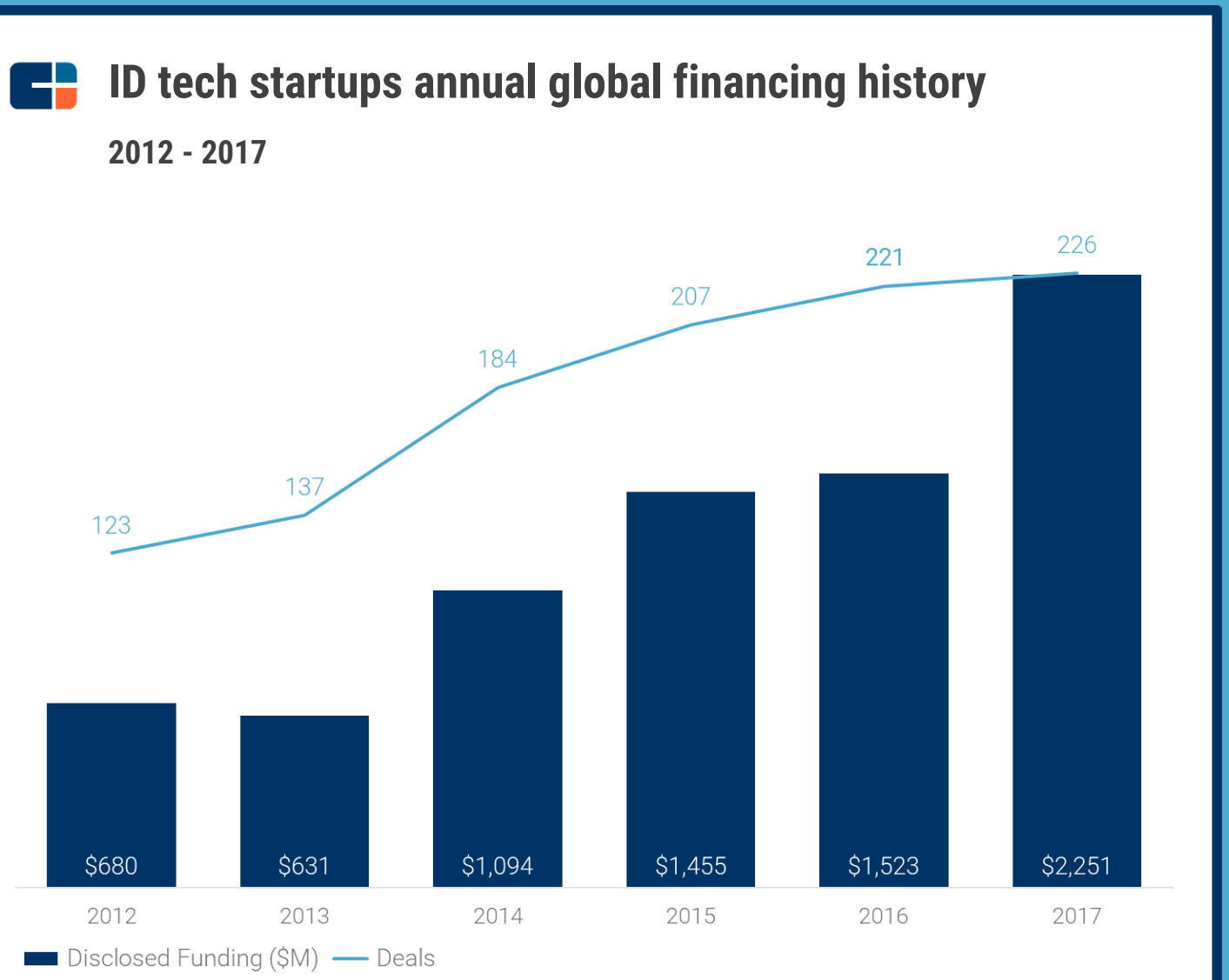
Alongside the rising insecurity of our PII, startups have begun to create solutions for protecting it.

The products these companies offer are broadly known as identity technologies or ID tech.

ID tech rising

Deals and dollars to private ID tech companies have risen annually since 2012.

The digitization of identity, and the use cases it enables, has ushered in a range of private sector players developing ID tech.



LOOK OUT FOR FOUR FAST-GROWING CATEGORIES OF ID TECH IN 2018

Fraud hunters

Finding and eliminating synthetic identity fraud

DIY digital privacy

Tools to help consumers take digital privacy back into their own hands

Identity vaults

Preserving the secrecy of enterprise customers' personally identifiable information (PII)

Continuous authentication

Identifying people based on behavioral traits throughout a work session

FRAUD IS GOING TO GET WORSE BEFORE IT GETS BETTER

There are two sides to the anti-fraud equation: (1) authenticate legitimate users and avoid false-positives, and (2) identify fraudsters.

Fraudsters are complicating the equation by switching up their tactics.

Fraudsters are going from obtaining illegitimate access to legitimate accounts to creating synthetic identities from stolen PII.

PII is increasingly in the wild…

3 billion: The number of user accounts compromised in the **Yahoo** breach, in which thieves stole names, emails, phone numbers, etc.

200 million: Personal information of almost 200 million **registered U.S. voters** was accidentally exposed online including: names, birth dates, addresses, voter registration details, and social media posts.

146 million: The number of people affected by the **Equifax** breach – in which names, birth dates, addresses, and Social Security numbers were leaked – that affected half the U.S. population.

57 million: In 2016, hackers stole the data of 57 million **Uber** customers, and the company paid them $100,000 to cover it up. The breach wasn't made public until November, 2017.

1 million: Fasten, a ride-sharing company whose app is primarily used in the Boston area saw a trove of PII get exposed online, albeit briefly. Leaked data included a year's worth of customer pick-up and drop-off points.

…and available for exploitation.

ACCOUNT TAKEOVER IS NO LONGER THE MOST SERIOUS CASE OF FRAUD

"When you look at things like the Equifax breach – and the other waves of breaches that have seen the full suite of consumer information go out the door – **accounts being taken over is becoming a less challenging threat than fraudulent accounts and synthetic identity frauds**, where stolen data is attached to fabricated accounts and identities."

KrebsonSecurity
In-depth security news and investigation

Brian Krebs

Journalist and investigative reporter

Fraud hunters

SIGNIFYD

Signifyd offers fraud protection for e-commerce.

Most anti-fraud solutions provide retailers with a cryptic score and rely on human expertise to decide whether or not to accept a transaction.

Signifyd's analytics engine offers online retailers a simple yes or no decision on whether or not to accept a transaction.

Investors include American Express Ventures, Allegis Cyber, and a16z backed the company's seed round in 2012.

Most recent financing: $56M Series C (5/4/2017)

Total disclosed funding: $106M

feedzai

Feedzai prevents fraud for banks, payment providers, and retailers.

Feedzai's platform ingests multiple data streams and fraud insights and enriches the data to create hyper granular risk profiles.

The company helps in predicting fraud by scoring risk in real-time using a combination of rules and machine learning models.

Investors include Capital One Growth Ventures and Citi Ventures.

Most recent financing: $50M Series C (10/17/2017)

Total disclosed funding: $77M

CONSUMERS ARE TAKING PRIVACY INTO THEIR OWN HANDS

From Equifax to Yahoo, major hacks show us that there is little guarantee that a business can protect its customers' data.

We're starting to see an interesting mindset crop up: cyber-safety for protecting PII begins with the user.

Startups are rising to create specific products and services for those who want to stop their data from getting outside of their control.

DIY digital privacy

Keybase offers a free app that makes public-key cryptography accessible for average internet users.

The company describes itself by saying, “Imagine a Slack for the whole world, except end-to-end encrypted across all your devices. Or a Team Dropbox where the server can't leak your files or be hacked.”

Keybase and Stellar (XLM) have partnered to make a payment protocol that requires customers to input their usernames rather than lengthy wallet addresses to execute monetary transfers.

Ideally the partnership could enable blockchain users to make international payments within minutes.

Most recent financing: Unattributed (3/9/2018)

Total disclosed funding: $10M

CIPHY

Ciphy is an early-stage company based in the Netherlands, developing a device that allows users to set up a secure internet connection through their home-router regardless of their location.

One of the easiest ways to eavesdrop and wiretap internet connections is to do so through public Wi-Fi hotspots.

CIPHY is connected to your home router. Every time you work on an unsecured public Wi-Fi connection your device will automatically set up a private connection to your CIPHY.

CIPHY then puts you through to your Internet provider’s connection instead of leaving you vulnerable to snoops on public Wi-Fi.

Most recent financing: N/A

Total disclosed funding: N/A

REGULATION PLACES DATA PRIVACY CONCERN IN THE C-SUITE

The EU's General Data Protection Regulation (GDPR) is a law that requires businesses to protect the personal data and privacy of European Union citizens.

Effective May 25, 2018 organizations in non-compliance will face heavy fines.

Executives must equate the survivability of their business with securing PII.

In tandem, a new class of cybersecurity startups is emerging to capitalize on the growing imperative for enterprises to protect the confidentiality of PII.

Enterprises are now legally bound to protect users' PII…

GDPR applies to all companies processing and holding the PII of citizens of the European Union, regardless of the company's location.

Key ideas in GDPR:

- **Right to Access:** The right to know if personal data concerning you is being processed, where, and why.

- **Right to be Forgotten:** The right to erase personal data, cease dissemination, and halt processing of your data.

- **Privacy by Design:** Privacy by design has existed for years, but is now a legal requirement with the GDPR. It calls for designing systems at the outset that protect user identity.

…and failure to do so is a punishable offense.

Identity vaults

BigID helps organizations manage the risk and privacy of customers' identity data.

BigID searches multiple data stores, finds private data, maps data relationships across sources and geographies, and helps customers comply with privacy regulations.

The company is still young with fewer than 20 employees spread across two offices in NYC and Tel Aviv.

Investors include Comcast Ventures and SAP.

Most recent financing: $14M Series A (1/29/2018)

Total disclosed funding: $16M

D-ID helps enterprises protect users' face-data from unauthorized use.

Face-data is becoming common across enterprises. For example, each of the Big 5 tech giants has at least one patent for facial recognition.

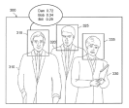
D-ID is an Israeli company backed by Y-Combinator.

Most recent financing: $4M Seed (1/22/2018)

Total disclosed funding: $4.12M

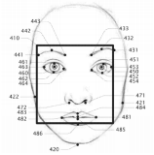
amazon

"Image analysis for user authentication"



facebook

"Facial recognition using social networking information"

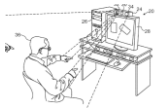


Microsoft

"Creation of representative content based on facial analysis"

Google

"Automatic transition of content based on facial recognition"



Apple

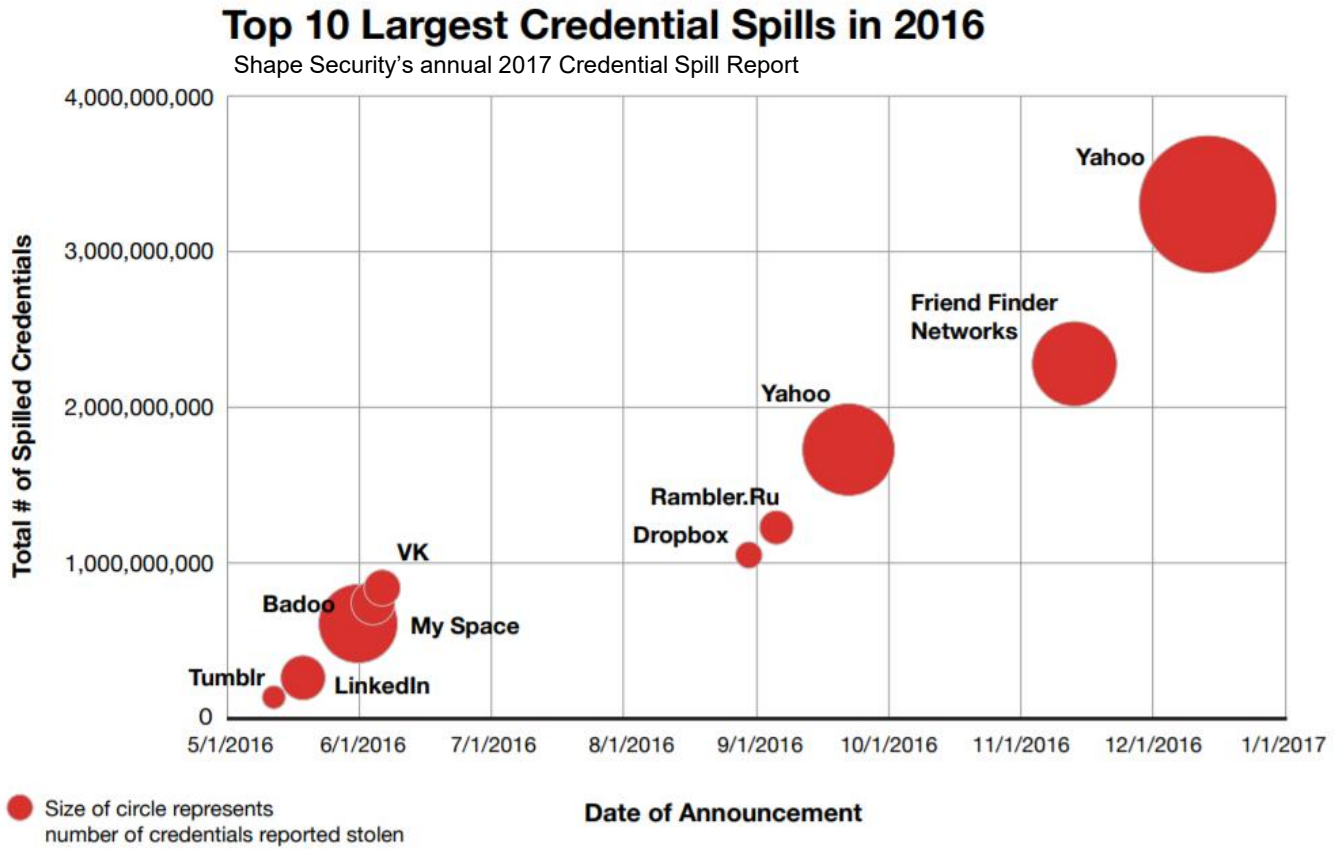
"Enhanced face detection using depth information"

PASSWORDS ARE EASY TO STEAL, BEHAVIORS ARE NOT

Continuous authentication techniques turn the ability to identify someone into a process vs. a single login event such as entering a password or other static-credential.

The continuous authentication process happens the entire time a user is on a network by monitoring their implicit behaviors such as: typing cadence, mouse movements, and more.

3B+ login credentials were reported stolen worldwide in 2016…



…this effects every organization operating a public or private web or mobile application in 2018.

Continuous authentication

UNIFYID

UnifyID is an authentication platform with an approach that uses behavioral and environmental factors from smartphones to identify users.

The company's technology can identify users based on inherent factors such as walking gait, typing speed, etc.

Investors include a16z and NEA, among others.

Most recent financing: $20M Series A (8/1/2017)

Total disclosed funding: $20M

BIOCATCH

BioCatch collects and analyzes behavioral, cognitive, and physiological parameters to generate a unique user profile for identifying and stopping fraudsters.

BioCatch can measure factors such as palm size, hand tremor and eye-hand coordination, combined with behavioral traits, to authenticate users on mobile devices.

Investors include American Express Ventures, CreditEase, and the Monetary Authority of Singapore, among others.

Most recent financing: $30M Series B (3/12/2018)

Total disclosed funding: $46M

MOST CYBER ATTACKS START BY TARGETING PEOPLE

Phishing is a social engineering scam that involves obtaining login credentials of privileged insiders by posing as a trustworthy entity in an electronic communication.

Most data breaches are traced back to phishing and the theft of login credentials that enable attackers to gain entry into proprietary systems.

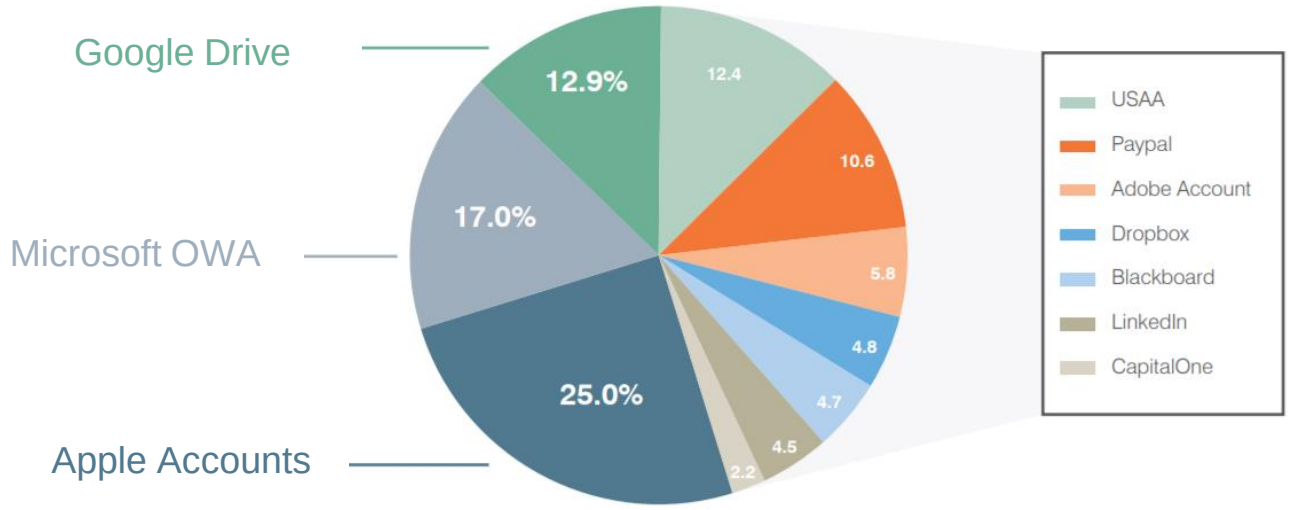
The most popular products are the bait

A phishing lure is a fake customer support account that promises to help users but secretly steals their credentials.

According to cybersecurity company Proofpoint, “while large phishing campaigns designed to steal Apple account credentials may be the most common, the most effective in terms of click rate are emails targeting Dropbox credentials.”

Top 10 Credential Phishing Lures of 2016

Proofpoint’s annual 2017 report “The Human Factor”



Human-factor security

KnowBe4 offers security awareness training and a simulated phishing platform.

The company provides training that allows organizations to thwart social engineering schemes by equipping users to recognize red flags and by testing employees with simulated phishing emails.

Investors include Goldman Sachs and Elephant VC, among others.

Most recent financing: $30M Series B (10/24/2017)

Total disclosed funding: $43M

Ironscales offers awareness training, phishing detection, incident response, and intelligence sharing to combat phishing.

The company uses mailbox-level anomaly detection combining human input and machine learning algorithms to analyze employees' mailbox behavior to protect against hyper-targeted attacks.

The company was born out of Israel's 8200 EISP.

Most recent financing: $6.5M Series A (12/5/2017)

Total disclosed funding: $8M

CLOUD SECURITY IS THE FUTURE OF DATA SECURITY

Corporations are increasingly storing sensitive data in both public and private clouds, which creates new security concerns.

Chief among the concerns are the security of data when migrating to the cloud, and the protection of data in a hybrid-cloud environment.

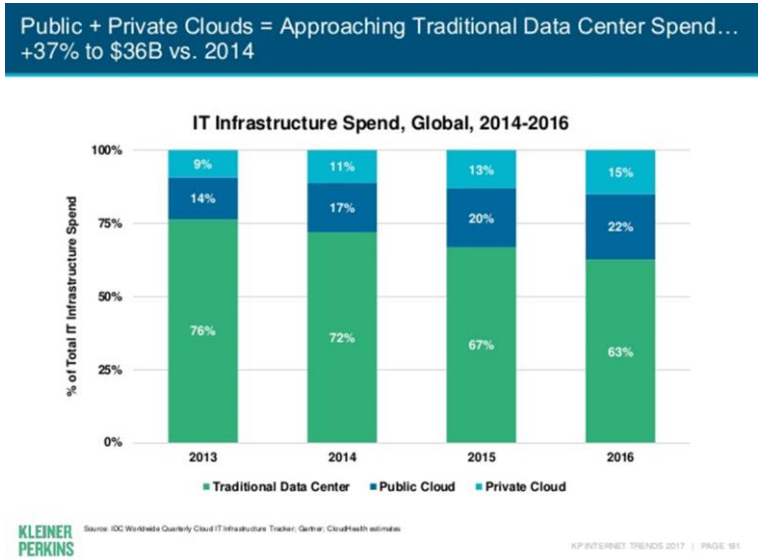
Developers in particular are responsible for ensuring that custom applications do not accidently reveal critical data in public clouds.

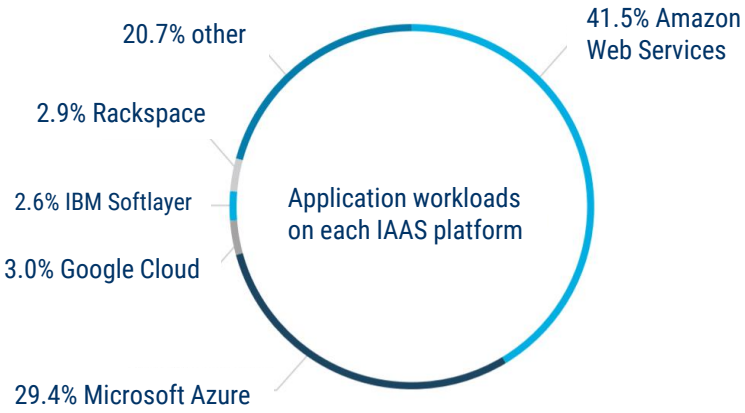
We are on the brink of a cloud-security tipping-point

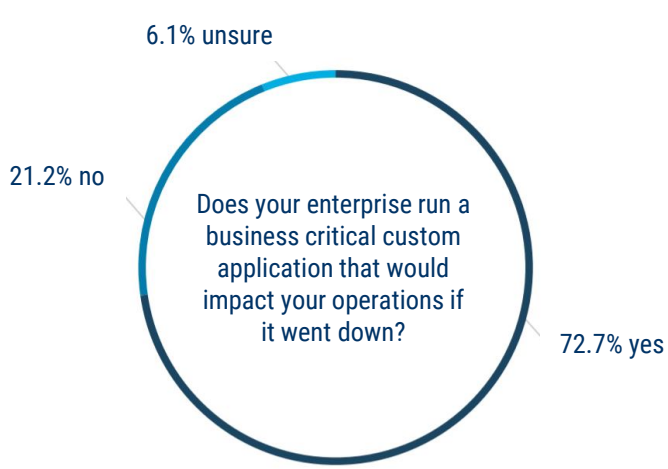
In 2018, more custom enterprise applications will reside in public infrastructure-as-a-service (IaaS) platforms such as those in AWS, rather than in private corporate datacenters.

Cloud providers such as Amazon offer microservices to help secure customer data. However, **enterprises still own the bulk of the responsibility for securing custom applications regardless of where they are hosted.**

Enterprises that utilize hybrid-clouds have to worry about how to orchestrate the complex balance between legacy and cloud-native infrastructure as well as ensure that the code in the apps they are releasing is not vulnerable once deployed.







Data from Cloud Security Alliance & SkyHigh Networks "Custom Applications and IaaS Trends 2017"

Next-gen cloud security

ShiftLeft

ShiftLeft is a cloud security solution specific to each version of each application, without focusing on threats.

The company's software allows for the protection of a workload by understanding its source code. The code is scanned for vulnerabilities and patched until developers can step in to make the fix.

Note, ShiftLeft protects cloud-apps but is also applicable to the "security by design" category featured in this report.

Most recent financing: $9.3M Series A (10/11/2017)

Total disclosed funding: $9.3M

TIGERA

Tigera provides policy-driven security for enterprises deploying applications and workloads in the cloud.

Tigera is solving the networking problems inherent in deploying and enforcing policy in complex private, public, and hybrid enterprise cloud environments.

Most recent financing: $10M Series B (1/24//2018)

Total disclosed funding: $23M

DEVELOPMENT OPERATIONS AND SECURITY ARE ONE

Truly secure systems are designed with security in mind.

Security must be a part of the software development process from coding to release, operation, and even updating.

Developers have to balance demands for rapid deployment cycles with the need to make vulnerability-free-software.

DevOps failures lead to data-breaches

In 2016, Uber leaked the data of 57 million people. The data was hosted Amazon Web Services (AWS) and neither Amazon or Uber could protect it. Why? Because **Uber's contract-developers accidentally published code that included AWS keys** on GitHub. The AWS login-credentials gave hackers access to privileged files on Uber's AWS account.

From a security perspective (not PR), Uber's breach is both a reminder of the significance of what can happen when attackers breach a privileged account, and a reminder that development operations teams are often the first line of defense.

Uber is not alone. Throughout 2017 a number of firms reportedly leaked sensitive data as a result of a common issue: developers misconfiguring AWS accounts for public access.

"IT, DevOps and security teams must come together to better understand the immediate threat from hackers, future trends and the gaps in their security policies. Only then can they build a strategy to effectively protect themselves against threats."

CYBERARK®

Elizabeth Lawler

VP DevOps, CyberArk

Security by design

Snyk is a software service startup that aims to help developers find and fix vulnerabilities in their open-source code before it goes into production.

The company also collects data on known vulnerabilities across the internet for the open source projects it monitors.

Snyk can identify libraries and certain coding languages to determine if versions of code are out-of-date.

Most recent financing: $7M Series A (3/6/2018)

Total disclosed funding: $10M

Aqua Security enables enterprises to secure their virtual container environments from development to production, accelerating container adoption and bridging the gap between DevOps and IT security.

Aqua's platform provides full visibility into container activity, allowing organizations to detect and prevent suspicious activity and attacks in real time.

The newest version of the Aqua's container security platform focusses on automating Kubernetes-based controls to secure the growing number of cloud-native applications and micro-services.

Most recent financing: $25M Series B (9/19/2017)

Total disclosed funding: $38M

ONCE THEORETICAL ATTACKS ARE NOW OPERATIONAL

The Shadow Brokers leak of highly-classified NSA cyber exploits opened the door to hackers seeking elite cyber warfare tools of nation-states.

Today's cybersecurity tools can stop attacks that use data files to deploy malware. However, new attacks are fileless and more adept at dodging conventional security systems.

Modern cybersecurity tools that claim zero-day effectiveness are largely obsolete against fileless attacks.

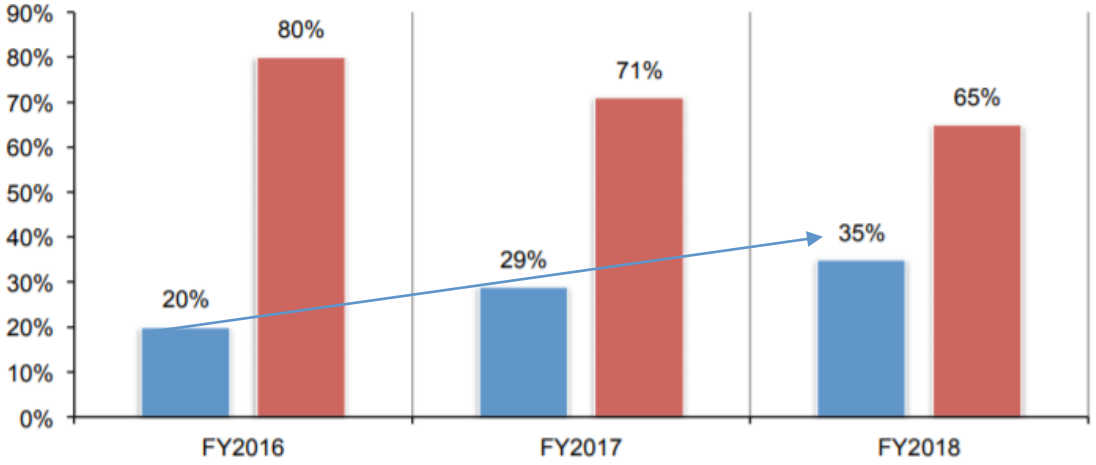
Fileless cyber attacks are on the rise

Recent attacks including WannaCry, Petya, and Apache Struts all leveraged fileless memory-based attacks to penetrate systems, hunt, and steal valuable data.

Fileless and memory corruption tool-kits enable hackers to run malicious code or launch scripts directly from memory, infecting endpoints and their networks without a trace.

The Growth Of Fileless And File-based Attacks 2016 - 2018

The 2017 State of Endpoint Security Risk Report (Ponemon Institute for Barkly)



Fileless attacks

File-based attacks

Fileless attacks are proliferating and causing real damage:

BOEING

Boeing Is The Latest **WannaCry** Ransomware Victim
Forbes - Mar 30, 2018

MERCK

Petya cyberattack cost Merck $135 million in revenue
Healthcare IT News - Oct 27, 2017

EQUIFAX

Equifax Ignored **Apache Struts** Patch For Months
EnterpriseTech - Sep 15, 2017

Fileless-attack security

Virsec specializes in defending networks against fileless memory-based attacks.

Virsec's software maps acceptable application execution, and detects deviations caused by attacks.

Virsec obtained a grant from the National Science Foundation in 2007.

Most recent financing: $24M Series B (3/20/2018)

Total disclosed funding: $29M

Minerva offers a deception security tool to thwart evasive malware and memory-based attacks.

Minerva's software works by deceiving malware about its ability to interact with other processes.

Minerva's deception tool prevents malware from gaining a foothold on the endpoint, rendering its evasion technique ineffective.

Most recent financing: $7.5M Series A (6/7/2017)

Total disclosed funding: $7.5M

AI IN CYBERSECURITY IS NOT ALL HYPE

AI is common in pitch-decks these days but real progress is being made to augment the job of security analysts.

An ideal security operations center (SOC) fuses data-streams to give analysts an overview of a company's systems. However, analysts report being fatigued by the number of attacks and alerts they have to process.

Autonomous systems help analysts prioritize which alerts to address.

Alert fatigue plagues even the largest SOCs

The number of security alerts and false-positives means analysts can't find strong signals among limitless noise.

For example, a survey conducted by the research firm Ovum shows that large financial institutions -- especially those in North America -- receive an overwhelming number of cybersecurity alerts each day. In fact, big banks reported receiving more than 200,000 alerts daily.

Financial institutions tend to employ some of the largest SOC teams of any industry. Yet, even giants report being overwhelmed and in need of autonomous solutions.

"Volumes of alerts will continue to climb until organizations implement the appropriate technology and overlay them with operational innovations that allow the organization to **rapidly sift through the mountains of data to find the actionable alerts**."

WELLS FARGO

Rich Baich

CISO, Wells Fargo

Autonomous watchdogs

RESPOND SOFTWARE

Respond Software offers automated cybersecurity judgements for the security operations team.

The platform looks at data sources used in a SOC and makes a determination about risk and impact.

Based on the analysis, events are escalated and prioritized for a human security analyst to investigate.

Most recent financing: $12M Series A (8/16/2017)

Total disclosed funding: $12M

JASK

JASK Labs is developing algorithms to deliver end-to-end network monitoring by surfacing and triaging the most relevant attacks and visualizing the attack surface for SOC teams.

The company specializes in learning how highly-trained security workers respond to threats to build an AI model around that data.

Investors include Stuart McClure, and Dell Technologies, among others.

Most recent financing: $12M Series A (6/27/2017)

Total disclosed funding: $14M

LEAKED DATA SHOWS UP FOR SALE ON THE DARK WEB

The dark web is a hidden group of illicit and untraceable marketplaces.

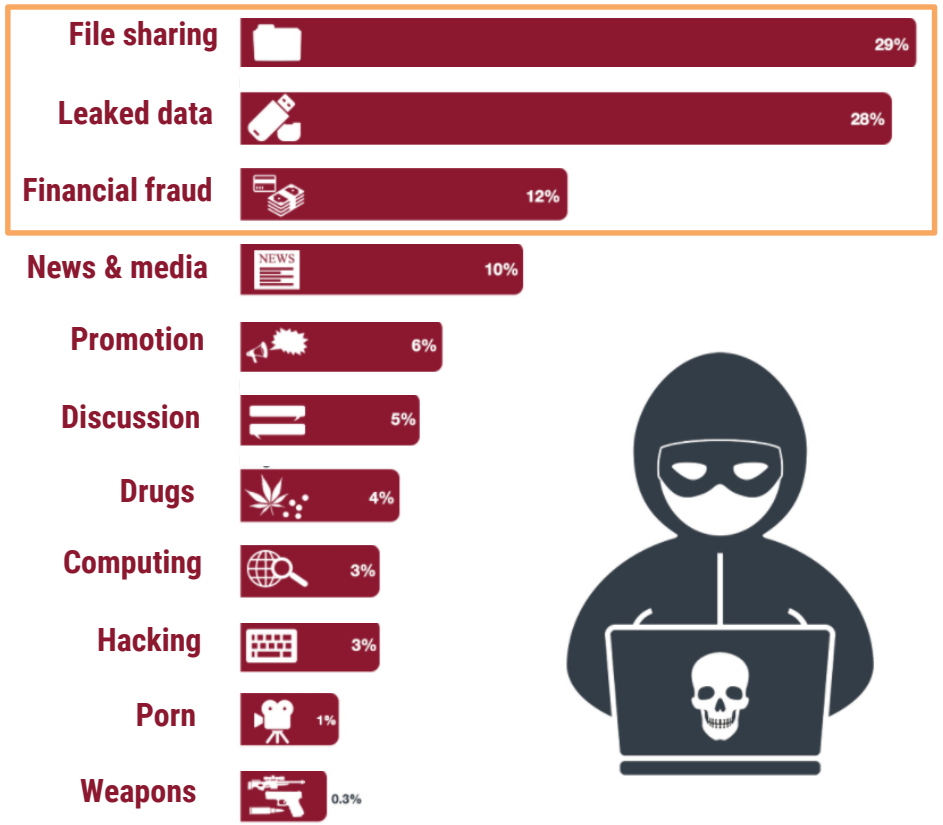
Average Internet users never see the dark web. This layer of the Internet is only accessible with specialized expertise and is the realm of criminals.

Leaked data often shows up on the dark web and tracking its sale can help security analysts and law enforcement measure risk, remediate attacks, identify perpetrators, and more.

Dark web markets are mostly illicit data-economies

A variety of vice and contraband are available on the dark web. However, file sharing is the top activity, trafficking leaked data comes in second, followed by financial fraud. Increasingly, the means to commit identity theft are for sale on the dark web.

Activities on the dark web by % share



Source: Intelliagg

Dark web actors are capitalizing on selling stolen data:

"Active Network data breach: Info sold on the dark web"

- BBC News March 22, 2018

"The Dark Web: How Much is Your Bank Account Worth?"

- ZDNet March 20, 2018

"Your Facebook Data is Only Worth $5.20 On The Dark Web"

- MarketWatch March 16, 2018

"Your Identity is For Sale On The Dark Web For Less Than $1200"

- NBC News March 12, 2018

"UK Top 500 Legal Firm Credentials Leaked On The Dark Web"

- ZDNet January 22, 2018

Dark web intelligence

FLASHPOINT

Flashpoint offers business risk intelligence gleaned from expertise and monitoring technology for the dark web.

The company offers a variety of services including: synthesized intelligence reports, searchable dark web datasets, as well as the ability to augment security teams' existing data streams.

Flashpoint can also spot emerging cyber threats being developed and traded on the dark web.

Most recent financing: $28 Series C (7/12/2017)

Total disclosed funding: $43M

TERBIUM LABS

Terbium Labs models the dark web, finds new markets, and predicts where illegal data is likely to appear.

The company gives users the ability to know when and where fingerprints of their actual data appear online.

Terbium's data fingerprinting technology creates a one-way digital signature of any type of data, enabling organizations to search for their sensitive information without revealing it.

Most recent financing: $6M Series B (11/8/2017)

Total disclosed funding: $16M

THE WORST OF THE WEB-ATTACKS IS STILL OUT THERE

Off-the-shelf web-attack-kits are also available on the dark web. These kits include tools for launching both distributed denial of service (DDoS) and web application-based attacks. DDoS attacks are designed to flood a victim's servers with enough requests to effectively take a website offline.

Attacks can be customized and configured for almost any site, allowing a B-grade attacker to unleash a sophisticated and automated web-attack.

Consequently, we are seeing the largest DDoS attacks ever recorded and instances of web application attacks are prominent.

GitHub just survived the biggest DDoS attack ever

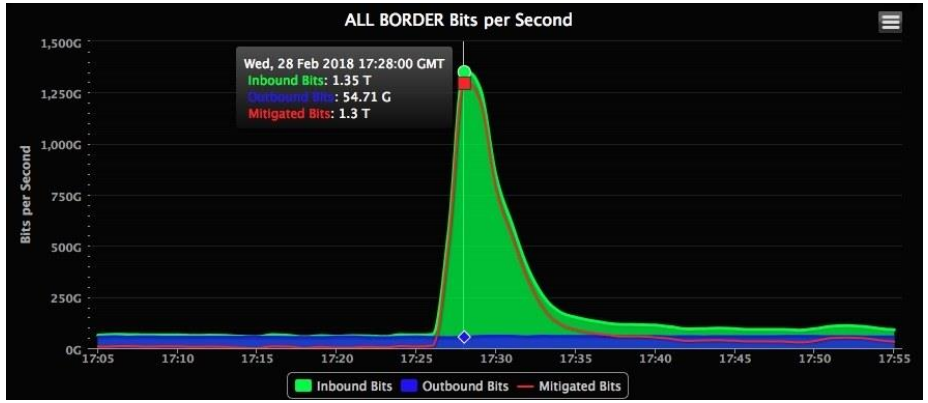
Famous DDoS attacks such as Mirai used malware-driven botnets to overwhelm websites into shutting down. However, DDoS attacks are evolving and newer memcached DDoS attacks like the one against GitHub no longer require the use of botnets.

The first memcached DDoS attacks were reported nearly five years ago, but they are now growing in sophistication and popularity.

The open-sourcing of these tools and their frequent use makes subsequent attacks easier to launch, tweak, and try again.

The biggest DDoS attack ever recorded:

Real-time traffic from the DDoS attack on GitHub, courtesy Akamai:



ON WEDNESDAY, AT about 12:15 pm EST, 1.35 terabits per second of traffic hit the developer platform GitHub all at once. It was the most powerful distributed denial of service attack recorded to date—and it used an increasingly popular DDoS method, no botnet required.

WIRED

Web-app attacks and DDoS are more popular

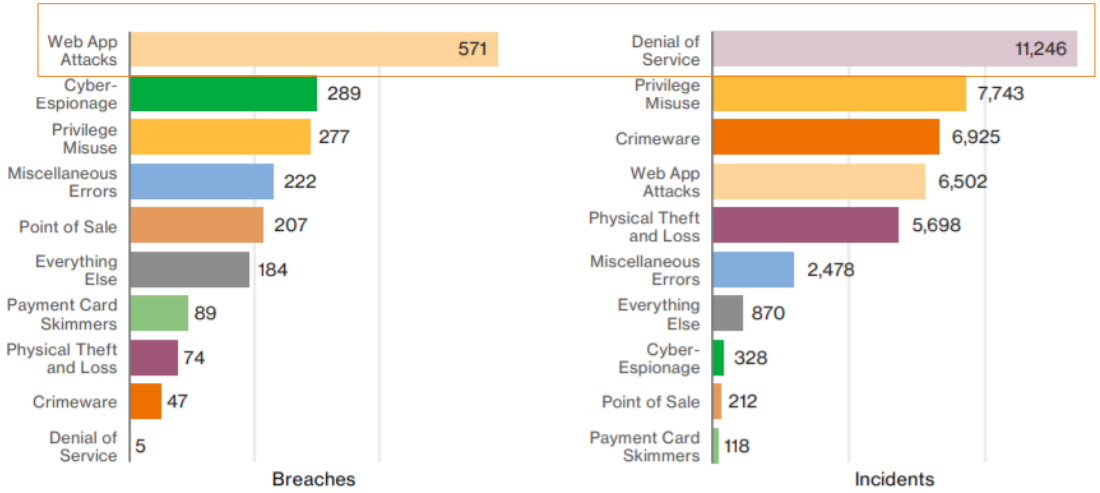


Figure 33: Percentage and count of breaches per pattern (n=1,935)

Figure 34: Percentage and count of incidents per pattern (n=42,068)

Source: Verizon's 2017 Data Breach Investigations Report

Web policing

Stealth Security protects enterprise websites, mobile apps, and APIs from automated attacks.

The company's technology can continuously monitor all web, mobile, and API traffic, providing real-time visibility and analytics of automated attacks and unwanted traffic.

Stealth Security is purpose-built to deploy to on-premise, hybrid, and public cloud environments.

Most recent financing: $8 Series A (2/13/2018)

Total disclosed funding: $8M

Netsparker develops desktop and cloud-based automated web application security scanners.

The company's vulnerability scanning technology enables users to automatically detect SQL Injection, cross-site scripting and other vulnerabilities in websites, web applications and web services.

The company has its head office in the U.K. with branch offices in Austin, Texas and Turkey.

Most recent financing: $40M Private Equity (3/8/2018)

Total disclosed funding: $40M

CRITICAL INFRASTRUCTURE IS MORE VULNERABLE THAN EVER

Critical infrastructure such as power plants, water, and other utilities that are connected to the Internet are vulnerable to cyber-attacks.

The types of attacks waged against IIoT facilities are increasingly severe.

Attackers used to be interested in espionage, they are now shifting toward hijacking and even sabotage -- creating new security concerns.

IIoT attacks are becoming more severe

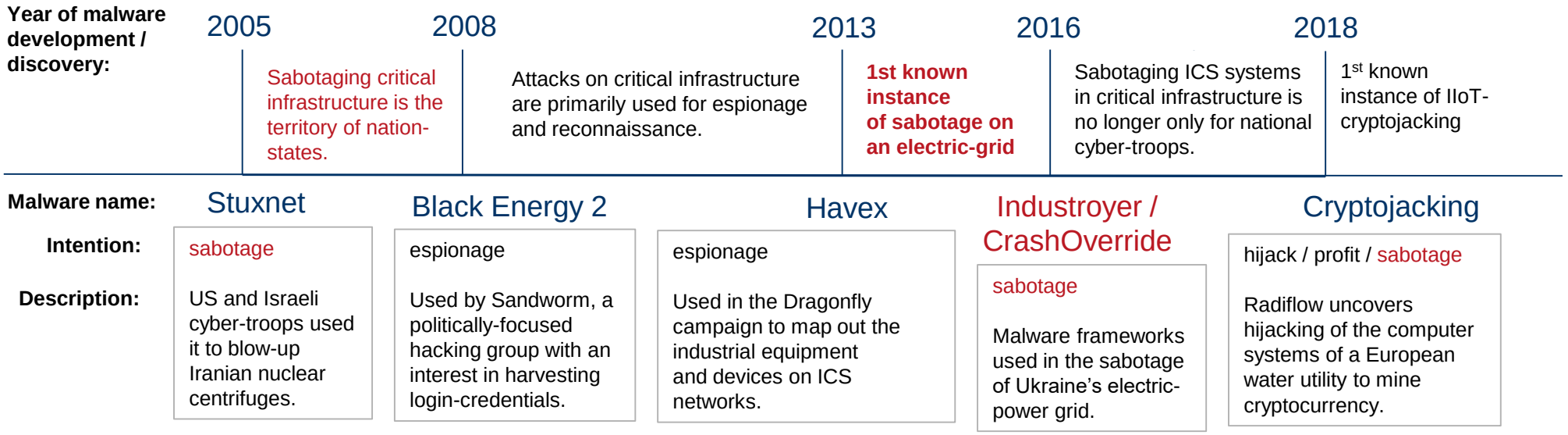
Utilities and industrial companies have always been targeted due to the potential impact of an attack and their relative insecurity due to the general antiquity of these systems, especially when their industrial control systems (ICS) are connected to the Internet.

The proliferation of malware intent on sabotaging critical infrastructure is relatively new. The tools for waging these attacks were previously the purview of militaries or national cyber-troops but they are now available to a wider range of threat-actors.

There have been at least four malware attacks found in the wild that target ICS: Stuxnet, Black Energy2, Havex, and Industroyer / CrashOverride.

The timeline below uses those attacks to show how the malware-threat to critical infrastructure has evolved.

Since 2016, threats to critical infrastructure are trending away from espionage and towards sabotage and cryptojacking.



IIoT shields

DRAGOS

Dragos is an industrial (ICS/IIoT) cybersecurity company.

The company offers an industrial cybersecurity automation platform that sits on-premise with customers to provide them visibility into their assets, detection of threats through behavioral analytics, collection and correlation of various data sets, automated workflows that reach across incident response scenarios, and compliance checks.

Most recent financing: $10M Series A (8/7/2017)

Total disclosed funding: $11M

Cylus is an early-stage Israeli company developing cybersecurity solutions for railways and metros.

Cylus provides a platform that enables rail companies to detect cyber-attacks in their operational network, including their signaling systems and rolling stocks, and blocks attackers before they can cause any damage.

Most recent financing: $4.7M Seed VC (1/25/2018)

Total disclosed funding: $4.7M

CYBER INSURANCE IS GROWING BUT CHALLENGES PERSIST

Global cyber insurance premiums grew at a rate of 30% every year for the past five years.*

As the market grows and carriers take on more cyber-risk, it becomes equally important to accurately model risk and predict outcomes.

* Aon Inpoint Global Cyber Market Overview June 2017

Underwriters struggle to quantify risk amidst growth

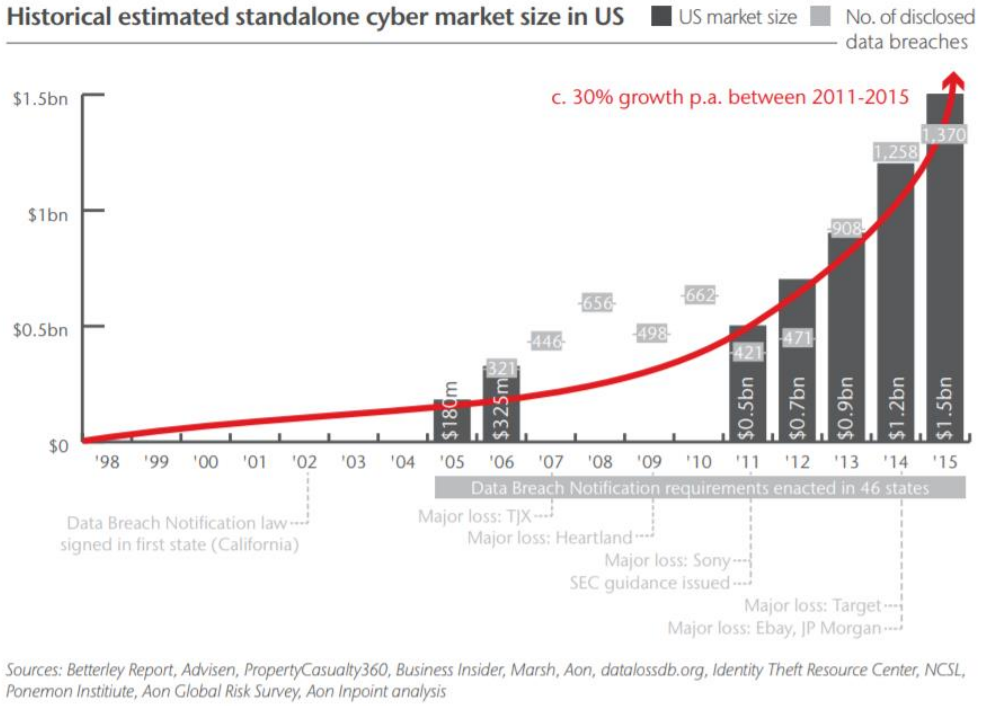
Quantifying cyber-risk is difficult for three reasons:

(1) The cybersecurity threat landscape is constantly shifting. It is said that once the good guys have it, so do the bad guys.

(2) A lack of breach-reporting and standards prevents the flow of accurate data from ever reaching an underwriter's desk.

(3) Large organizations are often exposed to third-party cyber-risk based on contracts and partnerships that are hard to investigate.

Underwriters are challenged to accurately forecast the costs and frequency of cyber attacks. Nevertheless, the industry is growing.



Sources: Betterley Report, Advisen, PropertyCasualty360, Business Insider, Marsh, Aon, datalossdb.org, Identity Theft Resource Center, NCSL, Ponemon Institiute, Aon Global Risk Survey, Aon Inpoint analysis

Key growth drivers

Legislation — Data breach legislation has been enacted in 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands

Awareness — In 2015, US firms ranked cyber as their 5th most important risk, compared to 18th back in 2011

# of breaches — More companies are uncovering data breaches and reported breaches in the US have risen by c.325% since 2006

Higher cost — On average, the cost of a data breach is 60% higher than it was in 2006

Cyber actuaries

corax

Corax Cyber Security is a software company helping organizations and the insurance community make better decisions on cyber security risk and investment.

Corax's analytics platform quantifies cyber risk for organizations and their surrounding ecosystem and automatically shows how much insurance cover and what security measures offer the best return on investment.

Most recent financing: $0.95M unattributed (2/12/2018)

Total disclosed funding: $3M

cyberGRX

CyberGRX provides a comprehensive third-party risk management platform to identify, assess, mitigate and monitor an enterprise's risk exposure across its entire partner ecosystem.

Through automation and analytics, CyberGRX enables enterprises to collaboratively mitigate threats presented from their increasing interdependency on vendors, partners, and customers.

Most recent financing: $20M Series B (4/18/2017)

Total disclosed funding: $29M

CROWDSOURCING COULD HELP FILL THE CYBERSECURITY TALENT-GAP

The cybersecurity industry does not have enough qualified people to satisfy rising demand for expertise.

Organizations that need to fortify their systems are harnessing the crowdsourced work of thousands of trusted hackers to find flaws in devices, software, and systems.

Today there are three types of cyber-crowdsourcing

(1) **Product collabs:** The most common form of cyber-crowdsourcing involves collaborating on a specific product. Generally this involves teams of white hat hackers getting hired to ensure that specific products don't contain vulnerabilities.

(2) **Threat intelligence sharing:** Often, organizations will subscribe to threat-data-feeds that are fed with crowdsourced intelligence to help defend against a wider-attack surface than if the organization was collecting intelligence on its own.

(3) **Bug-bounty teams:** Increasingly, institutions and corporations are hosting bug-bounty challenges in which white-hat hackers try to penetrate proprietary systems with authorized simulated attacks. Today, startups are capitalizing on the rising value of bug-bounty rewards and pooling white-hat expertise in crowdsourced bug-bounty operations.

"The DoD has seen tremendous success to date working with hackers to secure our vital systems, and we're looking forward to taking a page from their playbook. **We're excited to be working with the global ethical hacker community**, and the diverse perspectives they bring to the table, to continue to secure our critical systems."

Jack Messer

Director, Defense Manpower Data Center (DMDC)

Crowdsourced security

hackerone

HackerOne is a vulnerability coordination and bug bounty platform that connects businesses with cybersecurity researchers.

Investors include Facebook, GitHub, Ford Foundation, among others

Most recent financing: $0.3M Grant (7/21/2017)

Total disclosed funding: $74M

detectify

Detectify is a Swedish company offering a website vulnerability scanner that is in part powered by the crowd.

The company was founded in 2013 by a group of white-hat hackers who had discovered vulnerabilities in Google, Facebook, and PayPal, etc.

Most recent financing: $6.13M Series A (3/16/2018)

Total disclosed funding: $8M

bugcrowd

Bugcrowd uncovers and resolves security bugs in clients' products by leveraging a vetted community of security researchers.

The company also provides customized security testing programs that fit specific requirements.

Investors include Salesforce Ventures and Stanford University, among others.

Most recent financing: $26M Series C (3/1/2018)

Total disclosed funding: $48M

APPENDIX

Fraud hunters on top

The fraud hunter Signifyd is the only Cyber Defender to have raised over $100M.

Feedzai, another fraud hunter raised $77.8M.

Two crowdsourced security startups: HackerOne and Bugcrowd are in the top ten most well-funded.

2018 Cyber Defenders most well-funded companies

2012 – 2018 YTD (4/10/2018)

Rank	Company	Disclosed Funding	2018 Cyber Defender category
1	Signifyd	$106.2M	Fraud hunters
2	Feedzai	$77.8M	Fraud hunters
3	HackerOne	$74.3M	Crowdsourced security
4	Bugcrowd	$48.6M	Crowdsourced security
5	BioCatch	$46.6M	Continuous auth.
6	KnowBe4	$43.2M	Human-factor security
7	Flashpoint	$43M	Dark web intel.
8	Netsparker	$40M	Web policing
9	Aqua Security	$38M	Security by design
10	Virsec Systems	$29.7M	Fileless attack security

Rally Ventures on top

The Minnesota based investor Rally Ventures is the only VC to participate in 6 deals to 2018 Cyber Defenders.

No investors outside of the five listed participated in more than four deals to 2018 Cyber Defenders.

2018 Cyber Defenders most active investors

Measured by number of deals to the cohort 2012 – 2018 YTD (4/10/2018)

Rank	Investor	Investments:
1	Rally Ventures	Bugcrowd (Seed, A, B, C) / CyberGRX (A, B)
2	Allegis Cyber	Dragos (A) / CyberGRX (A, B) / Signifyd (A, B)
3	NEA	Tigera (A, B) / UnifyID (A) / HackerOne (B)
3	Paladin Capital Group	Bugcrowd (Seed, A, B, C)
3	BOLDstart Ventures	Snyk (Seed, A) / BigID (Seed, A)

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.

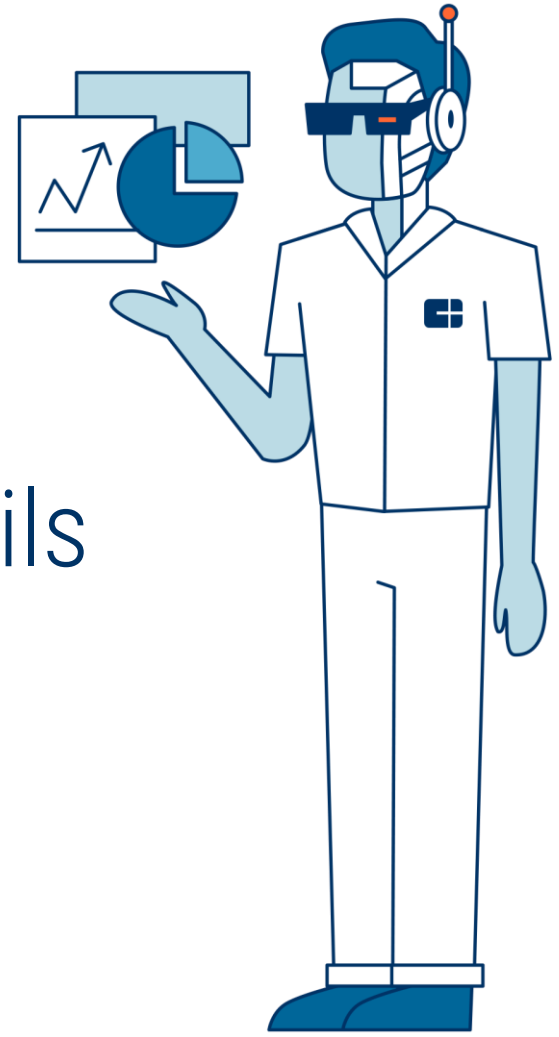
How the companies were selected: We used CB Insights' Company Mosaic, which uses data to track private company health based on recency of financing, total raised, and investor quality.

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.

WHERE IS ALL THIS DATA FROM?

The CB Insights platform has the details on all the data included in this report



CLICK HERE TO SIGN UP FOR FREE

cbinsights.com

@cbinsights