Cybersecurity Startups:

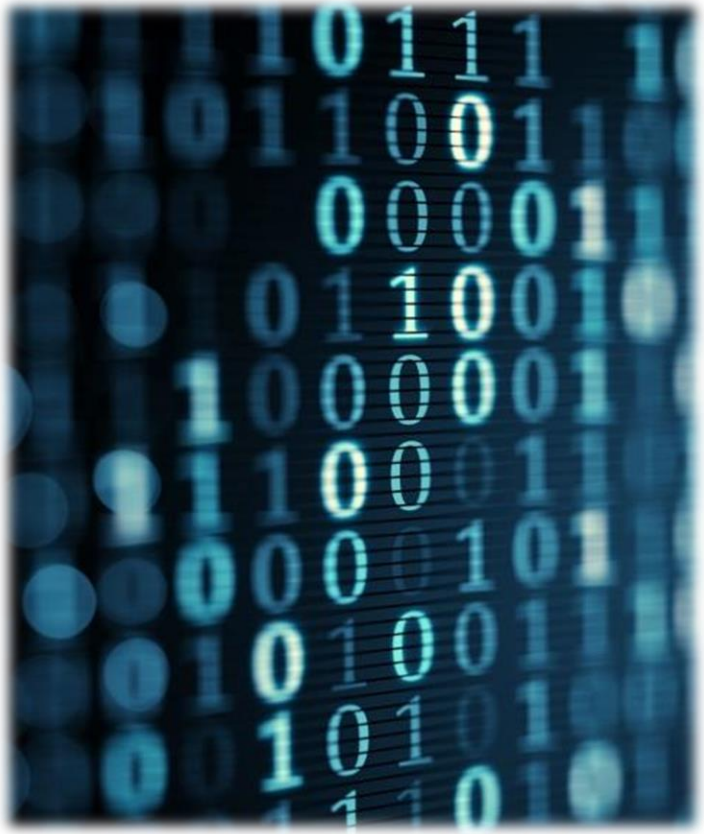
Hacking into a Growing Market Opportunity

September 14, 2017

EQUITYZEN

Cybersecurity Startups | Executive Summary

- **Cybersecurity landscape shifting.** The cybersecurity market has grown to $120B, underpinned by an increase in the frequency and severity of cybercrime over recent years. As cyber threats have increased, though, legacy technology has become increasingly less effective at mitigating them.
- **A wave of startups are driving innovation within the sector to meet new security challenges.** Key "next gen" technologies include: cloud/IoT security, predictive analytics, deception-based security, autonomous systems and segmentation.
- **Robust venture capital funding private cybersecurity sector.** VC funding for cybersecurity firms totaled $3.5B in 2016 and has continued at record levels into 2017. Over 1,500 startups are currently operating in the sector according to Crunchbase, including a handful of "unicorns" (Tanium, illumio, CrowdStrike, Cylance and Zscaler).
- **Key investment positives for investors looking at cybersecurity start-ups** incl. (1) strong revenue growth prospects, driven primarily by higher enterprise spending, (2) a market ripe for disruption given the emergence of new security threats and (3) the likelihood of increased consolidation as incumbents try to stay relevant. Growing competition as well as technological obsolescence are risks.



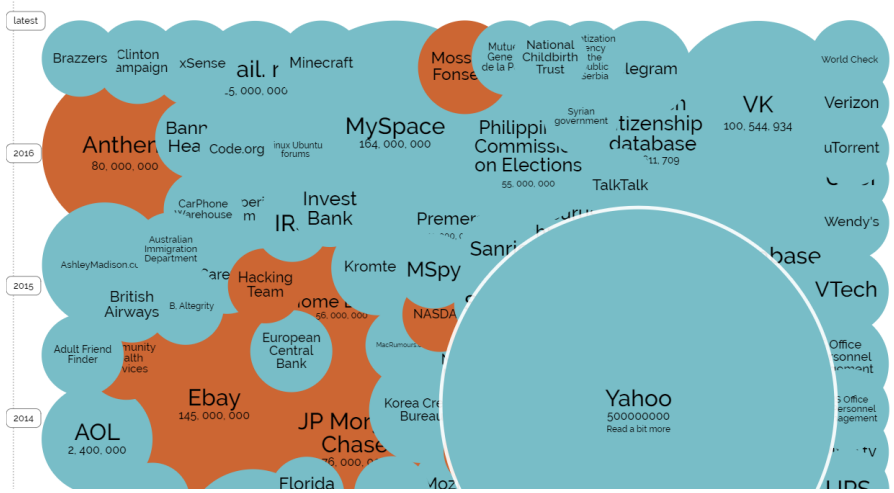
Cybersecurity – A Shifting Landscape

Cybersecurity is poised to become a key challenge for the modern economy. A staggering 4B records were exposed to data breaches last year, including notable attacks on Yahoo (twice), Dyn and the Democratic National Committee. This number is expected to increase – Cybersecurity Ventures estimates cybercrime could cost the global economy $6T annually by 2021, up from $3T in 2015.

Old security models broken; new tools needed. As cyber risks grow, legacy technologies have become increasingly less effective in mitigating them. Several key changes are driving this trend: (1) the volume of data transmitted is growing rapidly, with global IP traffic projected to reach 3.3 ZB* by 2021 (vs. 1.2 ZB in 2016), (2) data is increasingly stored outside of datacenters, which traditional security systems were designed to protect and (3) hackers are becoming more sophisticated at undermining legacy security tools.

Startups stepping up to the challenge. Key innovations introduced by these companies to address emerging cybersecurity challenges include cloud/IoT security, segmentation, predictive analysis, deception security, autonomous systems, and quantum encryption.

Largest Data Breaches



Source: informationisbeatiful.net
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

* ZB = zettabyte. 1 ZB = $1e^{15}$ megabytes (MB).

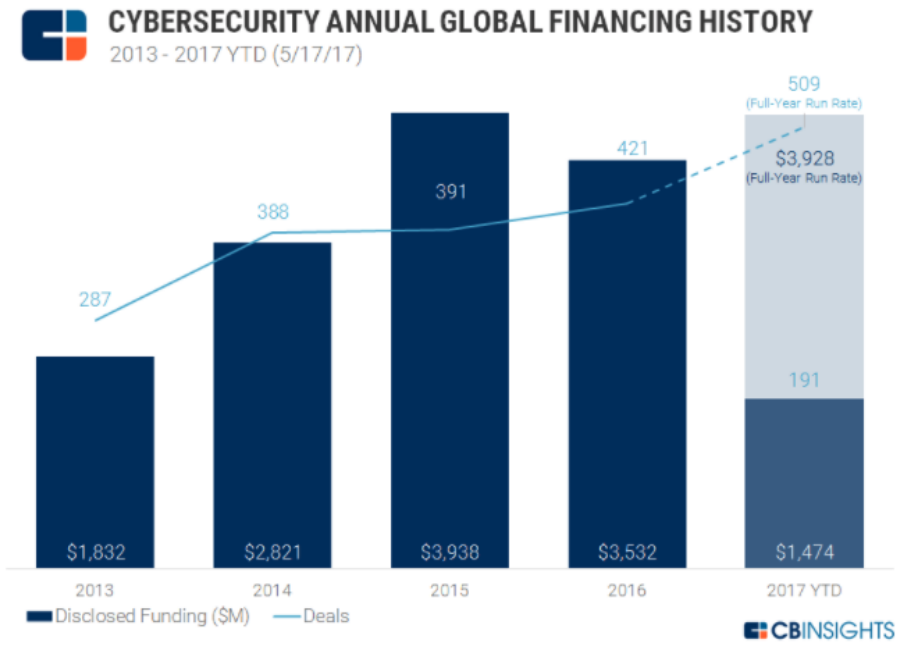
Startups Bolstered by Strong VC Interest

Cybersecurity has attracted robust venture funding. 2016 marked a robust year for private security financing, with $3.5B invested in 400 start-ups (CB Insights). This momentum continued into 2017, with 1Q17 marking a five-year record for VC-based cybersecurity deals. Prominent venture firms invested in the space include Andreessen Horowitz, Bessemer Venture Partners, Accel Partners, Intel Capital, and Lightspeed Venture Partners.

Cybersecurity-dedicated funds also arriving on the scene. Earlier in 2017, Trident Capital launched a $300M cybersecurity fund. The fund—which was oversubscribed at its debut—is one of the largest dedicated exclusively to cybersecurity. Allegis Capital and TenEleven Ventures also focus on the sector.

Over 1,400 cybersecurity start-ups are currently operating. Unicorns (companies valued at $1B or more) include Tanium ($3.8B), Illumio ($1B), CrowdStrike ($1B), Cylance ($1B) and Zscaler ($1B).

VC-backed cybersecurity deals



Source: Bloomberg, CB Insights

Investment Themes and Risks for Cybersecurity Startups

Key Themes

> Large and growing market

> Limitations of incumbent software opening market to innovators

> Consolidation likely as incumbents play catch up

Key Risks

> Technological obsolescence

> Competition heating up

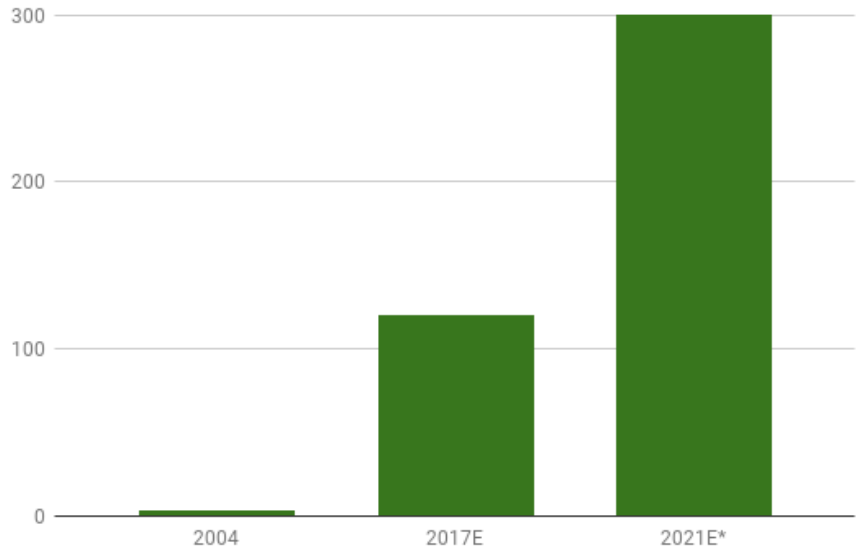
> Theme: Large and growing market

The global cybersecurity market stands at ~$120B currently according to Cybersecurity Ventures, underpinned by an uptick in the severity and frequency of cyber attacks over recent years. The firm projects this spending will grow to over $1T cumulatively through 2021, which we estimate would equate to a ~26% CAGR. We believe this estimate is reasonable assuming cybercrime and security costs rise proportionally with IP traffic.

Enterprise market is the largest driver of spend, with companies rushing to safeguard digital assets. Cybersecurity budgets are growing more than double the pace of overall IT budgets. Expectedly, industries with the largest exposure to sensitive data -- telecom, finance, government, healthcare and utilities -- are the largest contributors to overall security spending.

"Blank check" attitudes towards fighting cybercrime are increasing. Bank of America is the most notable example of this, recently putting no cap on its cybersecurity budget. Other enterprises/entities that have notably stepped up budget allocations include JP Morgan (to $500M annually from $250M previously) and the US government ($19B from $14B last year).

Cybersecurity Ventures spending forecast



Source: Cybersecurity Ventures and EquityZen estimates
*2021 spending estimated using Cybersecurity Ventures total 2017-2021 spending estimate ($1T) and assuming a constant growth rate between 2017 and 2021.

> Theme: Limitations of incumbent software opening market to innovators

We believe the cybersecurity market is ripe for disruption as changes in the IT/security landscape have undermined the effectiveness of incumbent tools:

- Most were designed for on-premise server environments and traditional endpoints (e.g. desktops) and cannot protect the cloud and IoT devices (e.g. phones, tablets, smart devices) – two key components of the emerging IT landscape.
- Many are static and reactive and best used to thwart known security threats. Hackers have become more sophisticated at bypassing these controls. For example, polymorphic malware can change its electronic signature to avoid detection by traditional anti-malware programs and "zero day" attacks exploit vulnerabilities in existing code to penetrate a network undetected.
- Legacy tools often require significant human resources to implement. This model will become less tenable, in our view, as data volumes continue to expand. A projected 2m global shortage of cybersecurity talent by 2019 will only add to this problem.

Startups have introduced several key innovations to address these challenges (summarized in table at right).

Incumbent technology issue	Innovation	How it helps
Designed for on-premise server / desktop infrastructure	Cloud/ IoT Security	Secures new IT landscape of cloud computing and alternative endpoints (tablets, mobile phones, etc.)
Designed to protect against known attacks and vulnerabilities, which hackers can increasingly circumvent	Predictive analytics	Can identify known and previously unknown threats by looking at anomalous behavior in a network
	Deception-based security	Seeks to trap hackers that do manage to penetrate network
	Segmentation	Sets up obstacles that make it more difficult for intruders to access a company's most sensitive information
Requires significant human resources	Artificial intelligence/ automation	Can automate incident detection and response to reduce human workload; offers more efficient security for large volumes of data/traffic
Traditional encryption keys (RSA, SSL, DES and AES) can be broken with enough computing power	Quantum encryption	Quantum encryption leverages principles of quantum mechanics; a quantum key is theoretically unbreakable

> Theme: Consolidation likely as incumbents play catch-up

Start-ups have led recent wave of technological innovation within cybersecurity. Many of these companies focus narrowly on niche markets within the broader sector (e.g. cloud security, predictive analytics, deception-based security, etc.) and do not provide comprehensive solutions for customers.

We believe larger players will look to roll up smaller rivals to maintain relevance. Leading vendors such as Cisco, Symantec and Oracle have all used M&A to augment their market position historically. These acquisitions can generate meaningful synergies for large corporations as they apply more expansive data to the innovative, acquired technology.

Cloud security and predictive analytics have been key areas of focus for consolidation in the past. We believe autonomous systems companies could also prove attractive targets going forward given the ongoing proliferation of data along with the growing shortage of cybersecurity professionals.

Incumbents have a history of rolling up smaller rivals…

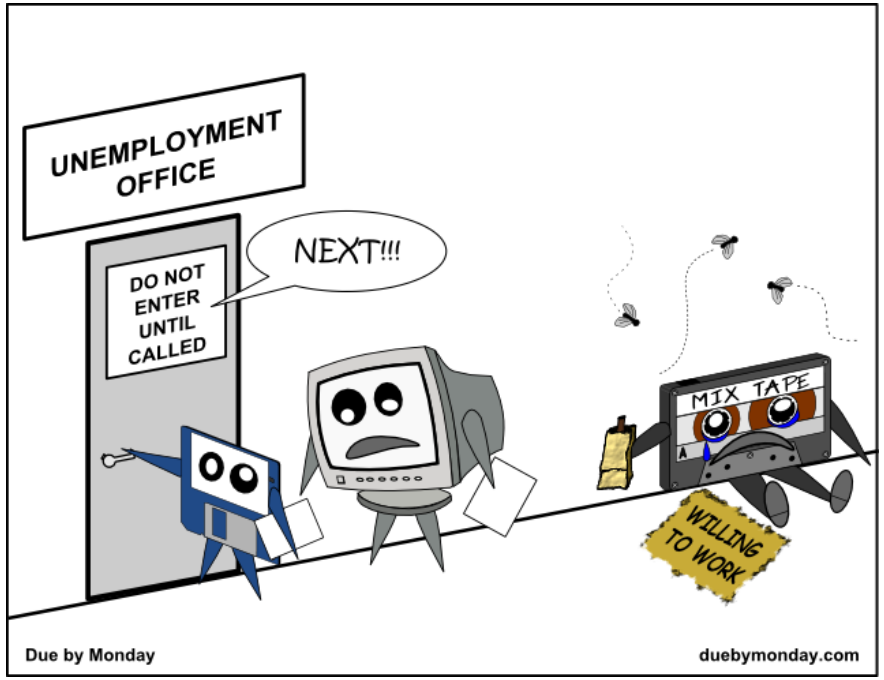
Date	Acquirer	Target	Sector	Price
Feb 2017	Sophos	Invincea	Predictive Analytics	$100M
Feb 2017	Palo Alto Networks	LightCyber	Predictive Analytics	$105M
Feb 2017	HPE	Niara	Autonomous systems	NA
Jan 2017	Amazon	Harvest.ai	Autonomous systems	$20M
Sep 2016	Oracle	Palerra	Cloud Security	NA
Aug 2016	Symantec	BlueCoat	Cloud Security	$4.65B
Aug 2016	Cisco	CloudLock	Cloud Security	$293M
Oct 2015	Cisco	Lancope	Predictive Analytics	$453M
Jun 2015	Cisco	OpenDNS	IoT Security	$635M

Source: Crunchbase and EquityZen estimates

> Key Risks

Competition heating up. The influx in venture capital funding has led to a surge in the number of cybersecurity startups, with over 1,500 in operation currently. Some sub-sectors are more exposed to higher competition than others. Endpoint security has started to show signs of increasing saturation and cloud/IoT security has seen a growing number of new entrants recently. That said, many solutions (even within subsectors) are complementary, rather than substitute, technologies.

Technological obsolescence. Cybercrime and security has become a hotly contested arms race, with new technologies being developed and hackers continually seeking to circumvent them. Current technologies could be rendered obsolete or irrelevant as new technologies replace them or as new threats emerge.



Appendix A: The New Cybersecurity Landscape

> Cloud/IoT Security

> Segmentation

> Predictive Analytics

> Deception-Based Security

> Autonomous Systems

> Quantum/Post-Quantum Encryption

> Anti-Phishing

> Cloud/IoT Security

What is it?	Cloud/IoT security tools bring key security infrastructure to cloud-based computing environments and internet-connected devices.
Why is it important?	Traditional security tools are no longer sufficient as cloud, IoT expand security perimeters beyond traditional on-premise servers and equipment.
Market commentary	• IoT has seen a huge uptick in early –stage companies in recent years • Cloud security growth pegged at a ~26% CAGR through 2022.
Key Players^	CipherCloud™ Building Trust in the Cloud; zscaler; ForeScout

^ Companies may compete in more than one sub-sector. Key players in a category can specialize in different security areas and listed companies may not directly compete against each other.

> Segmentation

What is it?	Segmentation vendors separate computer networks so that each network component is only visible to authorized viewers.
Why is it important?	Attackers that penetrate a segmented network encounter a series of “locked doors” as they try to move through the system, thus impeding their path to sensitive/critical data and reducing the damage they can inflict.
Market commentary	• Companies in the segment continue to report strong growth: • illumio reported 400% growth in bookings during 2016, its second year in operation • vmware’s NSX grew bookings by 50% in 4Q16, pushing its annualized revenue run rate over $1B
Key Players^	  

^ Companies may compete in more than one sub-sector. Key players in a category can specialize in different security areas and listed companies may not directly compete against each other.

> Predictive Analytics

What is it?	Looks for unusual behavior and traffic in a network that might signal the presence of malware. Unlike legacy systems that scan network traffic for known threats, predictive intelligence solutions often rely on signature-less or anomaly-based indicators to detect harmful behavior in real time.
Why is it important?	Threat signatures are increasingly becoming a thing of the past as hackers use more sophisticated tools to circumvent cybersecurity defenses. For example, point-and-click exploit kits enable attackers to create unique signatures for every attack.
Market commentary	• Prominent startups in this category have reported strong growth in recent years: • Cylance recently reported 283% YOY revenue growth; 2016 revenue estimated at ~$45m. • Crowdstrike reported a 400% increase in transactions valued at >$1m.
Key Players^	ANOMALI, CYLANCE, CROWDSTRIKE, Carbon Black.

^ Companies may compete in more than one sub-sector. Key players in a category can specialize in different security areas and listed companies may not directly compete against each other.

> Deception-Based Security

What is it?	Uses advanced luring technology to deceive attackers and entice them away from sensitive information and critical infrastructure.
Why is it important?	Deception-based security can step in when traditional prevention methods fail, identifying attackers and tricking and/or trapping them before they cause harm. They can also provide valuable insight into the data hackers are looking for as well as their techniques.
Market commentary	• Research & Markets projects the deception-based security market will grow to $1B by 2021, equating to a ~10% revenue CAGR
Key Players^	TRAPX SECURITY, illusive™, Cymmetria

^ Companies may compete in more than one sub-sector. Key players in a category can specialize in different security areas and listed companies may not directly compete against each other.

> Autonomous Systems

What is it?

Uses machine-learning and AI to police networks and automate attack/intrusion detection and response without human intervention. Can be used in conjunction with other cybersecurity tools (e.g. predictive analytics).

Why is it important?

Data is growing at an exponential rate, far outpacing the capacity of IT teams to analyze this data and monitor for anomalies. A shortage of cybersecurity talent will only further compound this problem, with a shortfall of 2.0M professionals expected by 2019. Autonomous systems address these issues directly by automating aspects of security operations. Vectra Networks, for example, claims its product can reduce threat investigation workloads by up to 29X.

Market commentary

- Market still nascent; however, we see this as a key emerging frontier in cybersecurity.
- Available disclosures suggest strong traction: sift science experienced its third consecutive 250%+ revenue growth year in 2016, Endgame ranked as one of the 500 fastest growing firms in North America by Deloitte.

Key Players^

ENDGAME. VECTRA exabeam PROTECTWISE™ sift science

^ Companies may compete in more than one sub-sector. Key players in a category can specialize in different security areas and listed companies may not directly compete against each other.

> Quantum Encryption

What is it?	Utilizes principles of quantum mechanics in encryption technology – uses photons of light to physically transfer cryptographic keys securely between two parties (e.g. browsers and web servers).
Why is it important?	Traditional encryption keys are prone to compromise. In theory, quantum encryption makes it impossible for an attacker to copy data encoded in a quantum state.
Market commentary	• Promising technology, but still in early stages and has yet to see broad-based adoption. • Likely to see most demand from industries that handle a lot of sensitive data (finance, government, healthcare and utilities).
Key Players^	Post-Quantum, id Quantique, labs Quintessence

^ Companies may compete in more than one sub-sector. Key players in a category can specialize in different security areas and listed companies may not directly compete against each other.

> Anti-Phishing Tools

What is it?	Anti-phishing tools attempt to identify phishing content. Phishing is a form of fraud, where cyber criminals send emails under the guise of being a reputable company to induce individuals to review personal information (passwords, credit card numbers, etc.).
Why is it important?	Phishing has become a primary attack tool among hackers to penetrate both individuals and corporations. According to PhishMe, 91% of breaches start with spear phishing.
Financial Data/ Projections	• PhishMe reported an annual revenue run rate of $50M in early 2017, with its flagship product experiencing 350% YOY sales growth. • KnowBe4 has similarly shows substantial revenue increases, with 1Q17 sales up 261% from the prior year.
Key Players^	PHISHME KnowBe4

^ Companies may compete in more than one sub-sector. Key players in a category can specialize in different security areas and listed companies may not directly compete against each other.

Appendix B: Select Cybersecurity Startup Profiles*

- > Anomali
- > CipherCloud
- > Carbon Black
- > CloudPassage
- > CrowdStrike
- > Cylance
- > Endgame
- > Exabeam
- > ForeScout
- > illumio
- > PhishMe
- > ProtectWise
- > Sift Science
- > Tanium
- > vArmour
- > Vectra Networks
- > Zscaler

* Includes select companies with $50M+ of total funding

> Anomali

ANOMALI

Description	Anomali's technology facilitates cyber risk detection and identification by correlating tens of millions of threat indicators against real time network activity logs and up to a year or more of forensic log data. The company was founded in 2013.
Business Model	Anomali generates revenue from sales of on-premise and SaaS threat intelligence products, including Anomali ThreatStream and Anomali Enterprise. A subscription to Anomali ThreatStream, which accounts for the bulk of revenues, starts at $5,000.
Management Team	Hugh Njemanze — CEO Colby DeRodeff — Co-Founder and Chief Strategy Officer Wei Huang — Chief Technology Officer
Financials	Anomali does not disclose financial data. The company announced record adoption rates among large enterprises in 2016. Anomali now counts 25% of the Fortune 100 and four of the largest five US banks among its customers.
Total Funding: $56M	**Key Investors** GENERAL CATALYST · G/ · IVP Institutional Venture Partners · IQT In-Q-Tel

> CipherCloud

Description	CipherCloud is a cloud security platform that protects against data loss and security compliance violations. The company was founded in 2010 and was a pioneer in cloud encryption and tokenization. CipherCloud was also the first Cloud Access Security Broker (CASB) vendor to offer an integrated mobile app.
Business Model	CipherCloud's product suite is sold on a subscription basis and includes out of the box security solutions for Salesforce, SAP SuccessFactors, ServiceNow, Adobe Analytics Cloud, Office 365, Box, Dropbox and Google Drive. The company also offers implementation, training and management services related to its products.
Management Team	Pravin Kothari — Founder & CEO Dev Ghoshal — SVP, Global Alliances & Customer Success Simon Pius — CFO
Financials	CipherCloud does not disclose financials or pricing. When CipherCloud was first launched in 2011, it charged $5-20 per user monthly, typically under a three to five year contract.
Total Funding: $74M	**Key Investors** Andreessen Horowitz, Index Ventures, Transamerica Ventures

> Carbon Black

Carbon Black.

Description	Carbon Black offers cyber threat detection and response. The company offers "streaming prevention" technology to thwart both malware and non-malware attacks. Carbon Black was founded in 2003 by former offensive security hackers for the US government.
Business Model	Carbon Black offers both SaaS and on-premise security solutions. The company has three product offerings: Cb Defense, Cb Response and Cb Protection.
Management Team	Patrick Morley — President & CEO Tom Barsi — SVP, Corporate and Business Development Roman Brozyna — Chief Information Security Officer Thomas Hansen — EVP and Chief Revenue Officer
Financials	Carbon Black generated ~$70M of revenue in 2015. The company confidentially filed for an IPO last year.
Total Funding: $190M	**Key Investors** SEQUOIA .406 Ventures KPCB | KLEINER PERKINS CAUFIELD BYERS HIGHLAND CAPITAL PARTNERS

> CloudPassage

Description	CloudPassage offers next-gen server security and compliance solutions. CloudPassage Halo, its flagship product, provides instant visibility and continuous protection for servers in data centers, private clouds and public clouds. The company was founded in 2009.
Business Model	CloudPassage Halo is sold on a subscription basis. The company does not disclose pricing, which reportedly starts at $350 per year.
Management Team	Robert Thomas — CEO Carson Sweet — Co-Founder and CTO Vitaliy Geraymovych — Co-Founder and SVP, Advanced Engineering
Financials	CloudPassage does not disclose financials. The company's customer base includes over 100 major enterprises, including GE, Xero, Dollar Shave Club, and FHLBank San Francisco.
Total Funding: $89M	**Key Investors** Lightspeed Venture Partners, Benchmark, Tenaya Capital, Shasta Ventures

> CrowdStrike

Description	Founded in 2011, CrowdStrike specializes in next-generation endpoint protection designed to prevent, detect and mitigate security breaches. The company's security platform is 100% cloud delivered.
Business Model	CrowdStrike sells security software and services. The company's key product is CrowdStrike Falcon, which features a next-gen anti-virus, endpoint detection and response, managed threat hunting and threat intelligence. Pricing is subscription-based and reportedly starts at $50 per endpoint.
Management Team	George Kurtz — Co-Founder, President & CEO Dmitri Alperovitch — Co-Founder & CTO Colin Black — CIO Burt Podbere — CFO
Financials	CrowdStrike does not disclose financials. The company continues to see strong growth, recently reporting a 476% increase in new endpoint protection subscriptions and a 400% increase in transactions valued at >$1m. CrowdStrike has endpoint deployments in 176 countries and processes 40B security events each day.
Total Funding: $256M	**Key Investors** ACCEL PARTNERS · WARBURG PINCUS · T VENTURES · capitalG

Signifies company with $1B+ valuation

> Cylance

Description	Cylance applies artificial intelligence, algorithmic science and machine learning to identify malware before it can execute. The company was founded in 2012.
Business Model	Cylance earns revenue through software sales and consulting services to enterprises. The company's product-suite includes CylancePROTECT (its flagship anti-malware software) as well as CylanceOPTICS and CylanceV. CylancePROTECT is also available in a home edition for employees who connect to work networks from home.
Management Team	Stuart McClure — Founder, President & CEO Ryan Permeh — Founder & Chief Data Scientist Daniel Doimo — COO Brian Robins — CFO
Financials	Cylance recently reported 283% YOY revenue growth. 2016 revenue has been estimated at ~$45m. The company's technology is deployed on over 10M endpoints.
Total Funding: $177M	**Key Investors** khosla ventures, Blackstone, FAIRHAVEN CAPITAL, INSIGHT VENTURE PARTNERS, DFJ GROWTH

Signifies company with $1B+ valuation

> Endgame

ENDGAME.

Description	Endgame uses machine learning and data science to prevent and detect cyber attacks. All prevention and detection functions occur autonomously. The company was founded in 2008 by Christopher Rouland.
Business Model	Endgame earns revenue through software sales and add-on services.
Management Team	Nathaniel Fick — CEO Jamie Butler — CTO Hyrum Anderson — Technical Director of Data Science
Financials	Endgame does not disclose financials. The company recently secured a $19M contract with the US Air Force, one of the largest cybersecurity deals in 2016.
Total Funding: $93M	**Key Investors** BESSEMER VENTURE PARTNERS PALADIN CAPITAL GROUP KPCB | KLEINER PERKINS CAUFIELD BYERS COLUMBIA CAPITAL

> Exabeam

exabeam

Description	Founded in 2013, Exabeam is a big data security analytics company that leverages machine learning to home in on attackers in a network. The company's software service tracks user activity in a network using a customer's existing log data and then alerts IT security teams of anomalous events.
Business Model	Exabeam charges by user, with pricing ranging from $5 to $50 per user, depending on the total number of users in an organization (larger organizations will have lower per user costs).
Management Team	Nir Polak — CEO & Co-Founder Domingo Mihovilovic — CTO & Co-Founder Sylvain Gil — VP, Products & Co-Founder
Financials	Exabeam does not disclose financials. The company has enjoyed strong growth in recent years, with 2016 revenue nearly tripling year-over-year.
Total Funding: $65M	**Key Investors** Lightspeed Venture Partners, Norwest Venture Partners, ICON Ventures, Cisco Investments

> ForeScout

Description	ForeScout is focused on IoT security. The company's products allow customers to view all IoT devices (e.g. mobile phones, tablets, other smart devices) connected to their respective networks. Customers can then ensure that these devices meet their security protocols or choose to remove the devices from their network. ForeScout was founded in 2000.
Business Model	ForeScout's product portfolio includes CounterACT, Orchestrate (an extended module) and Enterprise Manager. CounterAct and Enterprise Manager are sold as appliances with a license for a maximum number of devices (between 100 to 10,000). Similarly, extended modules are licensed for a maximum number of devices.
Management Team	Michael DeCesare – CEO and President Pedro Abreu – Chief Strategy Officer Oded Comay – Co-Founder and CTO Dror Comay – Co-Founder and Chief Architect
Financials	ForeScout has not disclosed recent financials. The company reported revenues of ~$125M in 2015, with growth of 50% year over year since 2012. It was also estimated to be be cash neutral as of 2015. Through June 2017, ForeScout has sold ~43M enterprises licenses. The company confidentially filed for an IPO earlier this year.
Total Funding: $163M	**Key Investors** pitango VENTURE CAPITAL, ACCEL PARTNERS, MERITECH CAPITAL PARTNERS, Amadeus Capital

Signifies company with $1B+ valuation

> illumio

illumio

Description	Illumio is a data center and cloud security vendor. The company specializes in microsegmentation, which walls off a network to reduce the attack surface for cyber threats and keep intruders away from sensitive data. Illumio was founded in January 2013.
Business Model	Illumio prices its Adaptive Security Platform based on the number of virtual enforcement notes in a network. The company does not disclose pricing on its website.
Management Team	Andrew Rubin — CEO PJ Kirner — CTO & Founder Alan Cohen — Chief Commerical Officer
Financials	Illumio does not disclose financials. The company has seen strong demand growth, announcing 400% year-over-year bookings growth in 2016.
Total Funding: $313M	**Key Investors** Andreessen Horowitz, Accel Partners, General Catalyst, J.P.Morgan Asset Management, BlackRock

Signifies company with $1B+ valuation

> PhishMe

Description	PhishMe provides solutions help companies protect themselves against phishing attacks. The products uses a customer's employees as an active line of defense against these attacks, enabling them to identify, report and mitigate threats. The company was founded in 2011.
Business Model	PhishMe offers four SaaS products: PhishMe Simulator, PhishMe Reporter, PhishMe Intelligence and PhishMe Triage. The company also offers consulting services for training and threat management. PhishMe Triage is the company's flagship product and automates phishing incident response for emails reported as suspicious by a customer's employees.
Management Team	Rohyt Belani — Co-Founder and CEO Aaron Higbee — Co-Founder and CTO Jim Hansen — COO
Financials	PhishMe reported an annual revenue run rate of $50M in early 2017, with PhishMe Triage experiencing 350% YOY sales growth.
Total Funding: $58M	**Key Investors** Bessemer Venture Partners, Paladin Capital Group, Aldrich Capital Partners

> ProtectWise

Description	Founded in 2013, ProtectWise facilitates threat protection through its ProtectWise Grid platform. Akin to a security camera, ProtectWise Grid records live-streams of a customer's network activity and then helps them analyze data for potential threats. Customers can even rewind the recording if needed to see how hackers penetrated their network. ProtectWise Grid is 100% cloud delivered.
Business Model	ProtectWise is delivered as a subscription service. Pricing reportedly starts at $40,000 a year, but varies with the amount of network traffic as well as the length of time historical network data is retained for analysis.
Management Team	Scott Chasin — Co-Founder and CEO Gene Stevens — Co-Founder and CTO Ramon Peypoch — Chief Product Officer Michael Lipfield — CFO
Financials	ProtectWise does not disclose financials. CEO Scott Chasin has suggested that the company continues to double its customer count quarter-over-quarter.
Total Funding: $62M	**Key Investors** TOLA CAPITAL ARSENAL VENTURE PARTNERS PALADIN CAPITAL GROUP

> Sift Science

Description	Sift Science uses machine learning technology to analyze data and detect fraudulent behavior. The company has a full suite of fraud prevention products including account takeover, payment fraud, content abuse, promo abuse and account abuse. The service is primarily targeted towards areas where fraud is most prevalent (e-commerce, payment networks, online marketplaces). Sift science was founded in 2011 by former Google engineers.
Business Model	Sift Science's products are sold on a subscription basis. Pricing varies from $1,000/month for 15,000 billable events to $10,000/month for 225,000 billable events (see plans here). The company also offers an enterprise products for clients with more intense usage. Prominent customers include: Airbnb, Zoosk, HotelTonight and OpenTable.
Management Team	Jason Tan — Co-Founder and CEO Russell Fujioka — President and COO Fred Sadaghiani — CTO
Financials	Sift Science does not disclose financials. The company's products are used by over 6,000 websites and apps. Assuming most of these customers are smaller and mid-sized companies that use Sift Science's smaller pricing plans (up to $2,500), we estimate revenue would be as high as ~$180M.
Total Funding: $54M	**Key Investors** INSIGHT VENTURE PARTNERS, SPARK CAPITAL, First Round

> Tanium

Description	Tanium is a security and systems management solution that allows customers to scan all endpoints in a network in real-time to detect vulnerabilities. The company was founded in 2013.
Business Model	Tanium employs a subscription-based model for its security solutions. The company does not disclose pricing on its website.
Management Team	David Hindawi — Co-Founder and Executive Chairman Orion Hindawi — Co-Founder and CEO Chris Bream — CTO
Financials	Tanium does not disclose financials. The company claims its revenue has grown over 100% a year, with 150% net renewals.
Total Funding: $306M	**Key Investors** Andreessen Horowitz, Franklin Templeton Investments, IVP Institutional Venture Partners, Geodesic Capital

Signifies company with $1B+ valuation

> vArmour

Description	vArmour offers data defined perimeter security solutions for mobile, virtual, and cloud platforms. The company focuses on enterprises, offering security policy management, software-based segmentation and microsegmentation and cyber deception. vArmour was founded in 2011.
Business Model	vArmour employs a subscription-based model . Pricing starts at $5,000/hypervisor for an annual subscription.
Management Team	Tim Eades — CEO Roger Lian — Co-Founder and VP of Engineering Michael Shieh — Co-Founder and CFO
Financials	vArmour does not disclose financials. The company had 165 customers last year, and was targeting 450 customers in 2017 (173% growth).
Total Funding: $83M	**Key Investors** HIGHLAND CAPITAL PARTNERS Menlo REDLINE Capital Management

> Vectra Networks

Description	Vectra Netowkrs offers security software that uses machine learning and behavioral analytics to automate cyber attack detection and response. The company was founded in 2010.
Business Model	Vectra Networks earns revenue through sales of hardware and software. The Vectra X-series platform is reportedly priced at $68,000 for the hardware and software. Hardware support costs an additional $1,600 while software support and updates are provided with no additional costs.
Management Team	Hitesh Sheth — President & CEO Oliver Tavakoli — CTO Howie Shohet — CFO
Financials	Vectra Networks does not disclose their financials and has not provided recent operating metrics. The company announced that they recorded bookings growth of nearly 400% in 2015 over 2014.
Total Funding: $93M	**Key Investors** khosla ventures, ACCEL PARTNERS, DAG VENTURES, IA VENTURES

> Zscaler

Description	Zscaler is a cloud security company that enables companies to move to the cloud with secure, policy-based access to the internet and private apps. The companies services are 100% cloud delivered. Zscaler was founded in 2008 by Jay Chaudhry.
Business Model	Zscaler offers five products through a subscription-based service: its flagship solutions, Zscaler Internet Access and Zscaler Private Access, as well as Cloud Sandbox, Cloud Firewall and Zscaler App. Pricing varies based on number of features and users protected.
Management Team	Jay Chaudhry — Founder & CEO William Welch — COO Remo Canessa — CFO Amit Sinha — EVP of Engineering and Cloud Operations, CTO
Financials	Zscaler has not disclosed recent financials. The company saw 2x growth in sales in 2015 and was cash flow neutral as of that year. According to Crunchbase, the company has over 5,000 customers, including 50 Fortune 500 companies. Zscaler is reportedly considering an IPO.
Total Funding: $185M	**Key Investors** Lightspeed Venture Partners, capitalG, TPG Growth

Signifies company with $1B+ valuation