

Momentum

CYBER

David DeWalt
Chairman

Eric McAlpine
Managing Partner

Michael Tedesco
Managing Partner

Keith Skirbe
Managing Director

Dino Boukouris
Managing Director

Alexander Krongold
Vice President

Chris McDowell
Senior Associate

Alex Szejnberg
Associate

Vilyam Yegikyan
Senior Analyst

Rachel Joseph
Analyst

John Gould
Research Associate



The Cybersecurity Almanac | 2022

Momentum Cyber Is Pleased To Release Its Fourth Annual Cybersecurity Almanac.

Intended Audience	<ul style="list-style-type: none">▪ CEOs▪ Board of Directors▪ Venture Capitalists▪ Private Equity▪ Corporate Development▪ M&A Professionals▪ Hedge Funds▪ Public Investors▪ CISOs▪ Security Teams▪ Governments & Defense▪ Regulators
Purpose	<ul style="list-style-type: none">▪ We are dedicated to consistently providing valuable insights on the dynamic and rapidly evolving Cybersecurity landscape▪ We maintain the industry leading proprietary M&A and Financing Transaction Database – unrivaled in its accuracy, quality, and scale (“CYBERcloud”)▪ We complement our proprietary database with data from various industry leading databases and research publishers, primarily from North America and around the world, representing millions of data points and decades of institutional industry knowledge and experience
Background	<ul style="list-style-type: none">▪ The 2022 Almanac takes a deep dive into the year and decade that were and puts focus to key topics and trends▪ This year’s edition is our most in-depth industry review ever, as we present a detailed view on key industry trends, private and public market activity, major news and events, and all things “Cyber”. Some key highlights include:<ul style="list-style-type: none">- Highlighted key M&A and financing transactions as well as IPOs and public market performance- The latest version of our often-referenced CYBERScape to accurately capture the continuously evolving industry taxonomies- An examination of the past decade of Cybersecurity transactions (M&A and VC / PE) to provide valuable insights and identify key trends- Spotlighted our favorite content in 2021, sharing our own original content, as well as others’- Focused on key breaches and regulatory changes, as well as industry sectors that are center stage for strategic activity- Spotlighted leading, Cyber-focused buyers and investors that increasingly play an integral role in the industry’s most innovative startups

The Authors

World-Class Advisors, Operators, & Investors In Cybersecurity.

Momentum Cyber Team



Dave DeWalt
Founder & Chairman
david@momentumcyber.com



Eric McAlpine
Founder & Managing Partner
eric@momentumcyber.com



Michael Tedesco
Founder & Managing Partner
michael@momentumcyber.com



Keith Skirbe
Founder & Managing Director
keith@momentumcyber.com



Dino Boukouris
Founder & Managing Director
dino@momentumcyber.com



Alexander Krongold
Vice President
alexx@momentumcyber.com



Chris McDowell
Senior Associate
chris@momentumcyber.com



Alex Szejnberg
Associate
alexs@momentumcyber.com



Vilyam Yegikyan
Senior Analyst
vilyam@momentumcyber.com



Rachel Joseph
Analyst
rachel@momentumcyber.com



John Gould
Research Associate
john@momentumcyber.com



Michael Deal
Fall '21 & Spring '22 Analyst



Shubham Sharma
Fall '21 Analyst



Norsang Tseten
Fall '21 Analyst



Kevin Wang
Fall '21 Analyst

Table of Contents | Client vs Public Edition

Momentum Offers Readers A Condensed Public Edition & Client Edition Of The Cybersecurity Almanac.

		Client	Public
I.	About Momentum Cyber	5	5
II.	Foreword	18	18
III.	Executive Summary	24	24
IV.	M&A Activity In Cybersecurity	32	32
V.	Financing Activity In Cybersecurity	54	41
VI.	Public Company Trading Analysis	75	51
VII.	Cybersecurity Industry Perspectives	89	65
VIII.	Investor Spotlight	145	121
IX.	Transaction Profiles	158	123
	<div><div><ul style="list-style-type: none">▪ Highlighted Cybersecurity IPOs▪ Highlighted M&A Transactions</div><div><ul style="list-style-type: none">▪ Highlighted Financing Transactions</div></div>		
X.	Contact Momentum Cyber	422	130



ABOUT MOMENTUM CYBER

The Premier Strategic Advisor In Cybersecurity

The First And Only M&A And Strategic Advisory Firm Focused Exclusively On Cybersecurity.

Firm Highlights



Over A Century Of Experience
In Cybersecurity As World Class
Operators & Advisors

300+ **\$300B+**

Total M&A Transactions & Deal
Value As A Team Since 1994



Cyber Exit Savvy – Deep
Expertise Selling to Strategic
& Financial Buyers

50+ **\$16B**

Cybersecurity Transactions &
Total Deal Value Executed By
Team Members Since 2002

\$360M

Average
Cybersecurity
Deal Value



Unparalleled Access with
Executives, Board Members,
Investors, & CISOs

1M+

Categorized Data Points On
>3,500 Cybersecurity
Companies (**CYBERcloud**)

CYBER 

Unrivaled Thought Leadership
In Cybersecurity Through
Insightful Research

Firm Values

Empathy

Objectivity

Action

Tenacity

Innovation



**Long-Term
Loyalty**

**Sense of
Humor**

A Holistic Strategic Advisory Approach

Momentum Cyber Is A High-Impact Advisory Boutique With An Exceptional Client Focused Service Model.

Momentum's Advisory Approach

-  Bespoke, Targeted, & Discrete
-  Collaborative Approach With Management
-  No Broad Auctions
-  Industry Thought Leadership / Company Positioning
-  Unmatched Senior Level Dedication
-  Execution Experience & Excellence
-  Exceptional Outcomes For Clients

Deep Knowledge Capital & Relationships Across Cyber

Active Dialogue With Top Strategic And Financial Buyers
On Client Engagements

Strategic Buyers



Financial Buyers



CYBERcloud | Momentum's Proprietary Cybersecurity Data Platform

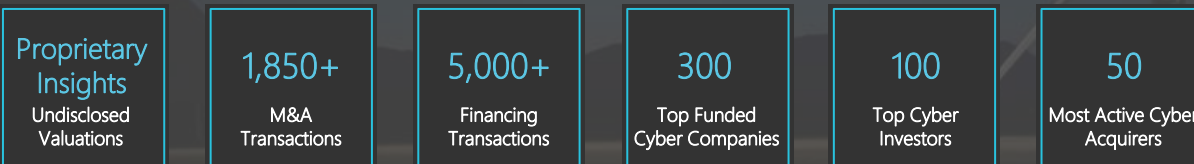
Unparalleled Proprietary Access & Insights Provides A Significant Competitive Advantage For Our Clients.

Thousands Of Hours Dedicated To Building A Robust Cyber Big Data Platform | Deep Relationships, Strategic Market / Industry Insights, & Proprietary Content

Unrivalled Industry Network



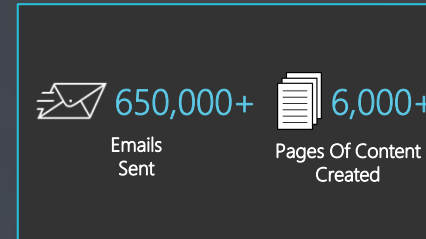
Transaction Database | 6,850+ Cybersecurity Transactions



Key Ecosystem Partners



Proprietary Industry Content



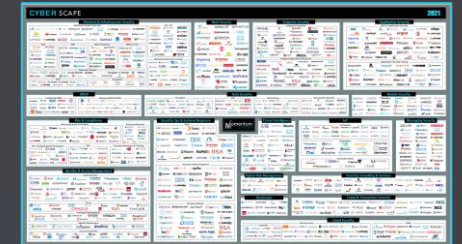
Frequent Releases Of Content To Highly Engaged Subscriber Base



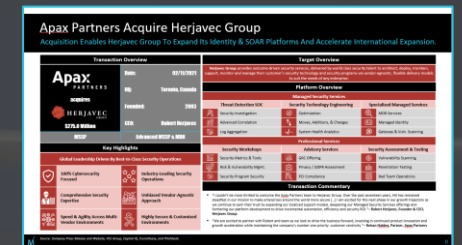
Monthly, Quarterly, Mid-Year, & Annual Reports



Bespoke Industry & Sub-Sector Coverage (45+ Sectors)



CYBERScope (800+ Companies)



Detailed Transaction Profiles (1,000+ Profiles)



Channel Reports / Whitepapers

Balanced & Highly Experienced Advisors

A Bespoke High-Impact Advisory Boutique With Unique Senior-Level Access.

Advice.

Bespoke Client Advisory Services



Mergers & Acquisitions

- Sellside
- Buyside
- Divestitures
- Joint Ventures
- Dual Track



Corporate Finance



Board & Special
Situation Advisory



Corporate Strategy &
Development



Partnerships & Business
Development



PE / Growth
Financing

Access.

Network Of Key Cyber Decision Makers



Executives



Entrepreneurs



Board
Members



Policy
Influencers






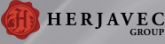































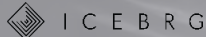





















Investors



Chief Security
Officers

Tremendous Advisory Track Record In Cybersecurity

Unrivalled Deal Experience And Comprehensive Coverage Across The Cybersecurity Landscape.

 acquired by  Managed Detection & Response	 merged with  a portfolio company of  Managed Security Service Provider	 acquired by  Extended Detection & Response	 acquired by  Vulnerability Management	 acquired by  Managed Security Service Provider	 acquired by  Kubernetes Security	 acquired by  a portfolio company of  Extended Detection & Response	 strategic investment by   Secure Access Service Edge	  acquired  Bot Mitigation & Fraud Prevention
  strategic investment in  Bot Mitigation & Fraud Prevention	 acquired by  Security Operations	 Strategic Advisor Diversified Security	 acquired by  Security Analytics	  strategic investment in  IoT Security	 acquired  Managed Security Service Provider	 acquired by  Network Security	 acquired by  Network Security	 acquired by  Web Security
 acquired  Managed Detection & Response	 acquired Undisclosed Consumer Security Company Consumer Security	 acquired by  Security Analytics	 acquired by  Cloud Security	 acquired by  Secure Cloud Orchestration	 acquired  MDM	 acquired  Mobile Security	 acquired  Endpoint Security	 acquired  Data Security

2021 Momentum Transactions



Fishtech Group Merges With Herjavec Group Via Apax Funds

Momentum Cyber Served As Exclusive Financial Advisor To Fishtech.



has merged with



a portfolio company of



Momentum Cyber served as exclusive financial and strategic advisor to Fishtech Group



December 30th, 2021

Transaction Overview

- On December 30th, 2021, Fishtech Group ("Fishtech") and Herjavec Group ("Herjavec") announced their merger, backed by funds advised by Apax Partners LLP (the "Apax Funds"). The two innovative companies will operate as a single entity under a new brand to be announced in early 2022. The Apax Funds will hold a majority stake in the new company while Robert Herjavec, Founder & CEO of Herjavec and star of ABC's Emmy award winning ratings giant "Shark Tank", and Gary Fish, Founder and CEO of Fishtech, will each maintain significant equity in the new business.
- "We're exceptionally proud of our results to date and even more excited about the growth to come. We're honored that so many organizations trust Fishtech to be their managed solutions provider. With complementary offerings from Herjavec, we will transform the security industry globally." – Gary Fish, CEO of Fishtech Group
- "We could not be more thrilled to join forces with industry pioneer Gary Fish, whom I have known for decades. We are very impressed by Fishtech's MDR offerings and its proprietary platform built on Google Chronicle, which we consider highly differentiated." – Robert Herjavec, CEO of Herjavec Group
- "By putting together two best-in-class organizations, we are confident that the combined platform will become an undisputed leader in Cybersecurity services in the enterprise segment and have an opportunity to redefine the market category." – Rohan Haldea, Partner at Apax

Transaction Significance

- The deal brings together the **complementary strengths** of both organizations, resulting in an **industry powerhouse** with a broad, holistic suite of **best-in-class managed detection and response capabilities (MDR)**, **professional services**, and **identity offerings** with a global perspective to address enterprise customers' increasingly complex information security needs
- Joining the forces of **Herjavec**, a **market leader in cloud and tech-enabled co-managed SIEM**, with **Fishtech**, a **market leader in enterprise MDR**, will allow the new company to provide customers with **unparalleled security and cloud expertise**, driving security maturity as a **competitive differentiator** via **advanced technology and services** across the industry landscape

Momentum Cyber's Role

- Momentum Cyber acted as exclusive financial & strategic advisor to Fishtech Group
- Momentum Cyber previously advised Herjavec Group on its February 2021 acquisition by Apax Funds

Notable MSSP & MDR Strategic Activity

Apax acquires **HERJAVEC GROUP**

Date: 02/11/21
HQ: Toronto, Canada
Founded: 2003
EV: Undisclosed

Barracuda acquires **SKOUT CYBERSECURITY**

Date: 07/01/21
HQ: Melville, NY
Founded: 2012
EV: Undisclosed

RELIAQUEST PE Growth Financing

Date: 12/01/21
HQ: Tampa, FL
Founded: 2007
Investors: KKR, FTV, TENELEVEN

eXpel \$140M Series E Financing

Date: 11/18/21
HQ: Herndon, VA
Founded: 2016
Investors: CapitalG, PALADIN CAPITAL GROUP

LogPoint Acquires SecBI

Momentum Cyber Served As Exclusive Financial & Strategic Advisor To SecBI.



has been acquired by



Momentum Cyber served as exclusive financial and strategic advisor to SecBI



September 1st, 2021

Transaction Overview

- On September 1st, 2021, LogPoint, the global Cybersecurity innovator, announced it will acquire Tel Aviv-based SecBI, a disruptive player in automated cyber threat detection and response. The acquisition is subject to customary legal requirements and approvals and is expected to be finalized by the end of Q3 2021.
- "Combining SecBI with LogPoint SIEM and UEBA will immediately drive tremendous value to our current and future customers. As organizations large and small face the most critical cyber threats, security teams need solutions that will help them be more effective and efficient in protecting their organization. This integration will allow customers to quickly launch automated notifications and security remediations using our full-native SOAR capabilities. This is a major step forward in delivering our XDR-enabled operations platform giving our partners and customers one of the most innovative, intuitive, and proven solutions available."
 - Jesper Zerlang, CEO of LogPoint
- "We are excited to join LogPoint and integrate seamlessly to further extend the company's foundational Cybersecurity solution. With the inclusion of the SecBI technology, LogPoint takes automation to the next level to address the challenges organizations and Cybersecurity analysts are facing in responding rapidly to an exponentially rising number of incidents."
 - Gilad Peleg, CEO of SecBI

Transaction Significance

- The acquisition will enhance LogPoint's core Cybersecurity stack, delivering an integrated, foundational security operations platform
- The acquisition will enable customers to eliminate false positives and automate incident response
- Together, these comprehensive, complementary platforms will automate repetitive tasks, orchestrate threat remediation workflows, and autonomously investigate, prioritize, and execute playbooks that reduce human involvement — allowing analysts to focus on real threats to protect organizations better

Momentum Cyber's Role

- Momentum Cyber** acted as exclusive financial & strategic advisor to SecBI
- This transaction highlights Momentum Cyber's continued success in advising innovative, next generation Cybersecurity companies and further establishes the firm's leadership position as the "go to" advisor exclusively focused on Cybersecurity

Notable XDR Strategic Activity

Hunters. \$30.0M Series B Financing

Date: 08/24/21

HQ: Tel Aviv, Israel

Founded: 2018

Investors: Bessemer Venture Partners, BLUMBERG CAPITAL, Y. VENTURES

cybereason acquires **empow**

Date: 07/21/21

HQ: Boston, MA

Founded: 2014

EV: Undisclosed

CROWDSTRIKE acquires **humio**

Date: 03/05/21

HQ: London, UK

Founded: 2016

EV: \$392.0M

exabeam \$200.0M Series F Financing

Date: 06/23/21

HQ: Foster City, CA

Founded: 2013

Investors: Acrew, Lightspeed, NORWEST

Ivanti Acquires RiskSense

Momentum Cyber Served As Exclusive Financial Advisor To RiskSense.



has been acquired by



Momentum Cyber served as exclusive financial and strategic advisor to RiskSense



August 2nd, 2021

Transaction Overview












- On August 2nd, 2021, Ivanti, the automation platform that discovers, manages, secures, and services IT assets from cloud to edge, today announced it has acquired RiskSense, a pioneer in risk-based vulnerability management and prioritization, to drive the next evolution of patch management. The terms of the transaction were not disclosed.
- “Ivanti and RiskSense are bringing two powerful data sets together. RiskSense has the most robust data on vulnerabilities and exploits, including the ability to map them back to ransomware families that are evolving as ransomware-as-a-service, along with nation states associated with APT groups and Ivanti has the most robust data on patches. Together, Ivanti and RiskSense will enable customers to take the right action at the right time and effectively defend against ransomware, which is the biggest security threat today.”
– Srinivas Mukkamala, CEO of RiskSense
- “Ivanti has been a leader in patch management for many years, but the acquisition of RiskSense will take our capabilities to an even higher level. This combination will allow us to provide our customers with a holistic view of vulnerabilities and exposures, and then enable them to take fast action through Ivanti Neurons for Patch Intelligence. Customers will be able to greatly reduce their attack surface and risk of breach because of the vulnerability intelligence and the resulting remediation prioritization based on actively trending exploits and ransomware attacks.” – Jim Schaper, Ivanti Chairman & CEO

Transaction Significance

- Together, Ivanti and RiskSense will provide security and IT teams with context and adaptive intelligence regarding what their organization’s exposures are to vulnerabilities that are being actively exploited, including whether those vulnerabilities are tied to ransomware, and then enable them to quickly remediate those threats
- Solutions from the combined companies are expected to reduce the mean time to detect, discover, remediate, and respond to cyber threats, particularly critical vulnerabilities linked to or associated with ransomware

Momentum Cyber’s Role

- Momentum Cyber acted as exclusive financial & strategic advisor to RiskSense

Notable Vuln. Mgmt. Strategic Activity		
		PE Growth
Date:	06/08/21	
HQ:	Austin, TX	
Founded:	2009	
Investors:		
	acquires	
Date:	05/14/21	
HQ:	Chicago, IL	
Founded:	2010	
EV:	Undisclosed	
	acquires	
Date:	05/11/21	
HQ:	Roseville, CA	
Founded:	1999	
EV:	Undisclosed	
		Series B Financing
Date:	02/26/21	
HQ:	Tel-Aviv, Israel	
Founded:	2018	
Investors:	   	

Apax Funds Acquire Herjavec Group

Momentum Cyber Served As Exclusive Financial Advisor To Herjavec Group.



has been acquired by



Momentum Cyber served as exclusive financial and strategic advisor to Herjavec Group



February 11th , 2021

Transaction Overview

- On February 11th, 2021, funds advised by Apax Partners (the "Apax Funds") today announced the majority acquisition of Herjavec Group ("HG"), an award-winning global Managed Security Services Provider (MSSP) and cyber operations leader. Founder & CEO, Robert Herjavec, will remain as a significant stakeholder and the firm's active Chief Executive Officer (CEO). The financial terms of the transaction (which is subject to applicable regulatory approvals) were not disclosed
- "I couldn't be more thrilled to welcome the Apax Partners team to Herjavec Group. Over the past seventeen years, HG has remained steadfast in our mission to make enterprises around the world more secure. We have succeeded in that effort by developing an industry-leading 24/7 Managed Security Services practice, by advancing our proprietary IP, by diversifying our offerings to include Advisory, Managed Detection & Response, Identity and Incident Response services, and by hiring what I fundamentally believe is the very best team in the world. This acquisition and the growth funding that results is a testament to our entire team, and to our loyal customer base who has entrusted us with their mission critical assets. I am excited for this next phase in our growth trajectory as we continue to earn their trust by expanding our localized support models, deepening our Managed Security Services offerings and furthering our platform development to drive incremental automation, efficiency and security ROI." – Robert Herjavec, Founder & CEO of Herjavec Group
- "Under Robert's leadership, HG has grown into an impressive business, providing critical cybersecurity solutions with a special focus on customer service. In an increasingly complex cybersecurity and IT market, where we are seeing ever more sophisticated cyber-crime, HG is a trusted partner that relieves the burden from internal enterprise security teams. We are excited to partner with Robert and team as we look to drive the business forward, investing in continued product innovation and growth acceleration while maintaining the company's number one priority: its customer centricity." – Rohan Haldea, Partner at Apax Partners

Transaction Significance

- The Apax Funds, in partnership with HG's management team, will look to build on the company's impressive growth rate by accelerating international expansion efforts, augmenting HG's talented team with additional threat & identity resources, and further advancing the HG Identity and HG SOAR proprietary platforms

Momentum Cyber's Role

- Momentum Cyber acted as exclusive financial & strategic advisor to Herjavec Group

Notable MSSP Strategic Activity

deepwatch \$53M Series B Financing

Date: 10/07/20

HQ: Denver, CO

Founded: 2019

Investors: Goldman Sachs

paloalto acquires **CRYPsis**

Date: 09/17/20

HQ: McLean, VA

Founded: 2015

EV: \$265M

RELIAQUEST PE Growth Financing

Date: 08/25/20

HQ: Tampa, FL

Founded: 2007

Investors: **KKR** TENELEVEN

Apax acquires **COALFIRE**

Date: 04/22/20


HQ: Westminster, CO

Founded: 2001


EV: Undisclosed

Rapid7 Acquires Alcide


Momentum Cyber Served As Exclusive Financial & Strategic Advisor To Alcide.



has been acquired by



Momentum Cyber served as exclusive financial & strategic advisor to Alcide



February 1st, 2021

Transaction Overview

- On February 1st, 2021, Rapid7, Inc. (NASDAQ: RPD) ("Rapid7"), a leading provider of security analytics and automation, announced it has acquired Alcide, a leading provider of Kubernetes security based in Tel Aviv, Israel
- This is the second acquisition Rapid7 has made in the cloud security market in the past nine months, having acquired DivvyCloud, a leader in Cloud Security Posture Management (CSPM) this past April. Together, these acquisitions will enhance Rapid7's ability to provide a cloud native security platform to its customers and facilitate continuous management of risk and compliance across their cloud environments
- "We are thrilled to welcome Alcide to Rapid7. The technical talent within Israel's Cybersecurity ecosystem is unparalleled and we look forward to working together with the Alcide team to provide organizations with comprehensive cloud security that drives business growth and innovation."
– Corey Thomas, CEO, Chairman, Rapid7
- "Today marks the beginning of an exciting new journey for Alcide. We are excited to join Rapid7 not only because of our shared commitment to providing customers with innovative and accessible cloud security solutions, but this also gives us an opportunity to bring our market-leading Kubernetes security platform to a broader set of customers. I am especially proud of having another multinational company join the Israeli ecosystem and enjoy the great cyber talent and innovation it has to offer." – Amir Ofek, CEO, Alcide



Transaction Significance

- With this acquisition, Rapid7 will expand and strengthen its cloud security offering, bringing together Alcide's cloud workload protection (CWPP) capabilities with the company's existing cloud security posture management (CSPM) and infrastructure entitlements (CIEM) capabilities, to provide customers with a more holistic, unified experience for managing the challenges of cloud-native application security
- The transaction represents Rapid7's first-ever acquisition in Israel, giving the Company strategic access to industry-leading thought leadership, domain expertise, and talent present within the Israeli cyber ecosystem


Momentum Cyber's Role



- Momentum Cyber acted as exclusive financial & strategic advisor to Alcide
- This transaction highlights Momentum Cyber's continued success in advising innovative, next-generation Cybersecurity companies and further establishes the firm's leadership position as the "go to" advisor exclusively focused on Cybersecurity



Notable Cloud Security Strategic Activity

 acquires 


Date:	01/07/21
HQ:	Mountain View, CA
Founded:	2014
EV:	Undisclosed



 \$525M Series D Financing

Date:	01/07/21
HQ:	San Jose, CA
Founded:	2015
Investors:	 

 acquires 

Date:	10/01/20
HQ:	Tel Aviv, Israel
Founded:	2018
EV:	\$100M

 \$30M Series D Financing

Date:	05/20/20
HQ:	Ramat Gan, Israel
Founded:	2015
Investors:	 

LogRhythm Acquires MistNet

Momentum Cyber Served As Exclusive Financial & Strategic Advisor To MistNet.



has been acquired by



a portfolio company of



Momentum Cyber served as exclusive financial & strategic advisor to MistNet



January 13th, 2021

Transaction Overview

- On January 13th, 2021, LogRhythm, Inc. (“LogRhythm”) announced the acquisition of Mistnet.IO, Inc. (“MistNet”), a cloud-based analytics platform that delivers vast network visibility and accurate threat detection
- “I am thrilled to announce the acquisition of MistNet. Their solution will facilitate our goal of addressing current and emerging endpoint security needs for our global customers and partners. MistNet complements our existing SIEM platform by enhancing deep network visibility, behavior analytics and threat detection capabilities and will accelerate LogRhythm’s reach into the XDR market.” – Mark Logan, President & Chief Executive Officer, LogRhythm
- “We are excited to join a company as committed to innovation and customer success as LogRhythm. The acquisition creates significant product synergy at the convergence of XDR and SIEM that will positively impact the industry, including the potential for accelerating detection based on open frameworks such as MITRE ATT&CK and driving additional use cases for supply chains, public cloud, and IoT / OT security.” – Geoffrey Mattson, President & Chief Executive Officer, MistNet


Transaction Significance

- The acquisition will allow LogRhythm to deliver intelligent, machine-learning based detection and response capabilities that incorporate network detection, user and entity behavior analytics (UEBA), endpoint detection and response (EDR), and additional MITRE ATT&CK detection to solve current and emerging security and risk problems
- The acquisition delivers the ability to collect and enrich tremendous amounts of security data ‘on location’ generating exceptionally accurate behavioral models and threat models without having to move any of the data. MistNet’s patent-pending TensorMist-AI™ technology also brings powerful AI capabilities to LogRhythm by constructing a geo-distributed meshed data pipeline that combines scale-out data management with distributed processing analytics



Momentum Cyber’s Role

- Momentum Cyber acted as exclusive Financial & Strategic Advisor to MistNet.
- This transaction highlights Momentum Cyber’s continued success in advising innovative, next-generation Cybersecurity companies and further establishes the firm’s leadership position as the “go to” advisor exclusively focused on Cybersecurity.



Notable XDR / NDR Strategic Activity

 acquires 

Date: 11/19/20
HQ: Mountain View, CA
Founded: 2016
EV: \$186M

 acquires 

Date: 09/28/20
HQ: Santa Clara, CA
Founded: 2014
EV: Undisclosed

 acquires 

Date: 06/04/20
HQ: San Mateo, CA
Founded: 2011
EV: \$160M

 DARKTRACE \$100M Later Stage VC Funding

Date: 06/15/20
HQ: England, UK
Founded: 2013
Investors: KKR 

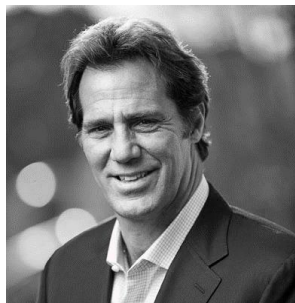


FOREWORD



The State Of Cyber | Highlights From Three Cybersecurity Titans

In Collaboration With Dave DeWalt, Gary Fish, And Robert Herjavec.



Dave DeWalt

Founder of Momentum Cyber & NightDragon

- Cybersecurity icon with over 30 years of experience as an investor and an operator of best-in-class companies



Looking Ahead To 2022



Growth Continuing to Accelerate



Sub-Sectors To Watch In The Coming Year



Founders Searching For Value



The Great Shift-Left In Security



Industrial Security's Importance



Cryptocurrency's Emergence



Gary Fish

CEO of Fishtech Group

- Serial entrepreneur, investor, and a Cybersecurity pioneer with over 25 years of industry experience



MDR & MSSP Market Trends



Security Staffing Shortage



Exciting Emerging Technologies



Highly Distributed Workforce



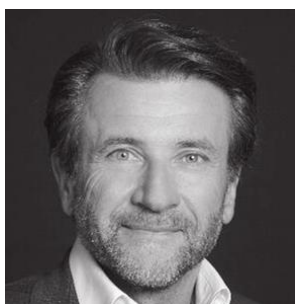
Increasing Sophistication of Attacks



Complying With Increasing Regulation



Third-Party Risk At The Forefront



Robert Herjavec

Founder & CEO of Herjavec Group

- Business leader, investor, and dynamic entrepreneur who built and sold several IT companies



Cybersecurity Challenges To Address



The Rise Of Ransomware



Cybersecurity Is Everyone's Responsibility



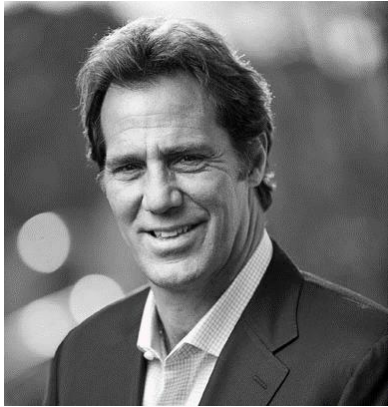
Inculcating A Culture Of Security-Driven Business



Cybersecurity Skills Gap

Dave DeWalt | Outlook In The Golden Age Of Cybersecurity

Cybersecurity Had A Record-Smashing Year In 2021 And Is Expected To Continue Its Upward Trajectory.








Dave DeWalt

Founder of Momentum Cyber & NightDragon

- Cybersecurity icon with over 30 years of experience having held leadership positions in some of the industry's most innovative and successful companies
- Dave has helped create more than \$20 billion of shareholder value during his 15+ years as President and CEO of three major companies

“ We are seeing a *perfect storm* of factors coming together to create the *most aggressive threat landscape in history* for commercial and government organizations around the world. ”

Dave's Track Record Of Success

Company	Background
 documentum	President and CEO of Documentum from 1999-2007; sold to EMC for \$1.9B
 McAfee	President and CEO of McAfee from 2007-2012; acquired by Intel Corp. for \$7.7B
 FIREEYE	Chairman and CEO of FireEye from 2012-2016; Executive Chairman from 2016-2017
 NIGHTDRAGON	Current Founder and Managing Director of NightDragon
 Momentum CYBER	Current Founder and Executive Chairman of Momentum Cyber

Cybersecurity Outlook Entering 2022



Growth Continuing To Accelerate

The necessity to protect digitized businesses, consumers, and devices from malicious threat actors will propel Cybersecurity spending further in 2022



Sub-Sectors To Watch

Identification management, threat hunting, managed XDR, vulnerability management, and security awareness training sub-sectors are all expected to grow significantly



Founders Looking For Value

Founders are looking for “real value-add” from their investors and specialization with an abundance of capital in the current market



The Great Shift-Left In Security

DevOps teams are guaranteeing security at the earliest stages in the development lifecycle as the market focuses on developers' needs



Industrial Security's Importance

Enterprises Of All Sizes Are Demanding A Different Approach To Industrial Security As Threats Increase and key infrastructure is tested



Cryptocurrency And Blockchain's Emergence

Cybersecurity will play an important role in cryptocurrency's mainstream adoption

Gary Fish | Key Trends In The MDR & MSSP Market

MDR Is Currently One Of The Hottest Sectors In Cybersecurity Attracting Tremendous Amounts Of Capital.








Gary Fish

CEO of Fishtech Group

- Serial entrepreneur, investor, and a Cybersecurity pioneer with over 25 years of industry experience
- Gary’s history includes over ten successful Cybersecurity startups, including Fishnet Security, the first security integrator in the world to reach \$700M in annual revenue

“ My team and I previously built the largest cybersecurity services provider in North America, but today’s security challenges are no longer effectively addressed by those legacy solutions. ”

Gary’s Track Record Of Success

Company	Acquirer / Merger	Background
 fishnet SECURITY	INVESTCORP (Majority Stake)	Founded Fishnet, sold majority stake to Investcorp
 FIREMON	INSIGHT PARTNERS	Founded Firemon, sold company to Insight Partners
 fishnet SECURITY	OPTIV	Sold remaining stake in Fishnet to Accuvant
 PERCH	ConnectWise	Invested in Series A, sold company to ConnectWise
 fishtech	HERJAVEC GROUP	Merged with Herjavec Group via Apax Funds

MDR & MSSP Market Trends



Security Staffing Shortage

Massive shortage of skilled professionals and in-house security expertise



Emerging Technologies

The rapid adoption of emerging technologies and proliferation of workloads is exponentially expanding organization’s attack surfaces



Distributed Workforce

The global pandemic has driven enterprises to increase security spending to protect the significant increase of remote workers



Increasing Sophistication of Attacks

Security gap is widening as increasingly sophisticated threats continue to bypass the first line of defense



Complying With Increasing Regulation

Enterprises continue to face challenges to comply with a continually increasing regulatory presence (GDPR, HIPAA, CCPA, NYCRR)

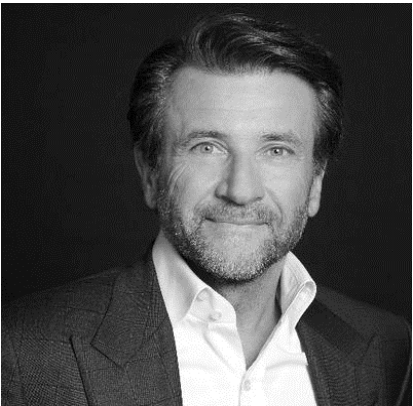


Third-Party Risk

Enterprises are sharing data with an increasingly complex network of 3rd parties including contractors, suppliers, and vendors, an attack surface that is difficult to protect

Robert Herjavec | Cybersecurity Threats Are At An All-Time High

Companies Should Assess Their Cybersecurity Posture And Ensure They Are Ready For The Challenges Ahead.












Robert Herjavec
Founder & CEO of Herjavec Group

- Business leader, investor, and dynamic entrepreneur who built and sold several successful IT firms
- Robert founded Herjavec Group and it quickly became one of North America’s fastest growing technology companies and is now a global leader in information security operating across USA, UK, and Canada

“ You have to stay laser focused when driving a car over 200 miles an hour, and the same approach is required when growing a business in today’s world of rapidly changing technology. ”

Robert’s Track Record Of Success

Company	Acquirer / Merger	Background
 brak Innovations Inc.	 AT&T	Founded BRAK Systems, sold company to AT&T Canada
 HERJAVEC GROUP	 Apax PARTNERS	Founded Herjavec Group, sold company to Apax Funds
 HERJAVEC GROUP	 fishtech	Merged with Fishtech Group via Apax Funds
Organization	Background	
 Government of Canada	Served as Cybersecurity Advisor for the Government of Canada	
 U.S. Chamber of Commerce	Member of the US Chamber of Commerce Task Force for Cybersecurity	
 SHARK TANK	Leading Shark on ABC’s Emmy Award-winning hit show, “Shark Tank”	

Cybersecurity Challenges To Address



The Rise Of Ransomware

Steep increases in the frequency and sophistication of attacks that have trickle-down impacts on communities, industries, and nations continue to threaten the world



Cybersecurity Is Everyone’s Responsibility

Defending a company from Cyber threats is no longer on the IT department’s shoulders alone – every person in the company must be Cybersecurity savvy as they can be the weakest link or the strongest first line of defense



Inculcating A Culture Of Security-Driven Business

Cybersecurity should be included in a company’s strategy & development and teams must have access to the resources, support, and infrastructure that allow them to prioritize Cybersecurity in their everyday tasks



Cybersecurity Skills Gap

Labor shortage of Cybersecurity professionals has been exacerbated by the pandemic and the increased speed of digital transformation, making it harder to maintain essential information security protocols

A Look Ahead: Discussion On Cyber In 2022

Join Us On February 24th At 10am PT For A Live Webinar.

Momentum
CYBER

+



NIGHTDRAGON

Join us on **February 24th** online for a lively discussion between Momentum Cyber and a panel of Cybersecurity industry icons including Dave DeWalt, Gary Fish, Robert Herjavec, and Bob Ackerman.

Gary and Robert's companies, Fishtech Group and Herjavec Group, recently merged to form one of the largest managed security organizations in the world that will operate as a single entity under a new brand to be announced in early 2022.



Dave, Gary, Robert, Bob, and Eric will recap themes they saw in 2021 across Cybersecurity, discuss challenges to address in the market, speak to trends in the MSSP & MDR space, and offer opinions on what to expect in 2022 across the industry.

Event is free to all to attend and will include a Q&A portion

When: Tuesday, February 24th from 10am –11am PT

[Click Here To Register For The Event](#)



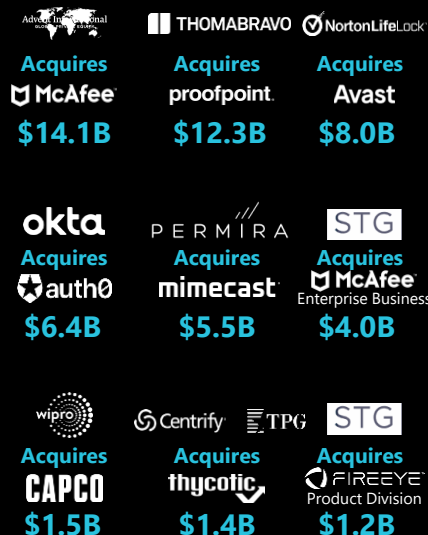
EXECUTIVE SUMMARY

Momentum Cyber's Snapshot of 2021

A Record Year For Cybersecurity Featured All-Time Highs Across The Industry.



14 \$1B+ M&A Deals Including



\$119M

Median 2021
Disclosed M&A
Deal Value



Security Consulting
Was The Most
Active Sector In
M&A With **50** Deals

2021 Was A Record-
Breaking Year For
Deal Making

\$77.5B

Total M&A
Volume

\$29.3B

Total Financing
Volume

2021 Was The Most
Active Year On Record

1,042

Financing
Deals

286

M&A
Deals



Risk & Compliance
Was The Most Active
Sector In Financing
With **170** Raises

5 Cybersecurity IPOs in 2021



Prominent Cyber Companies Taken Private



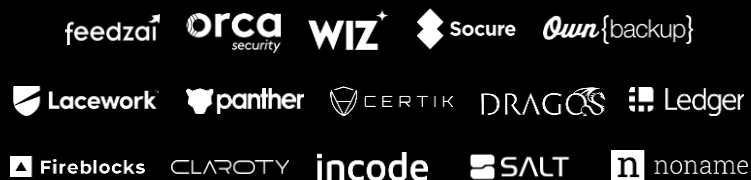
Private Equity's Cybersecurity

130 Completed Deals in 2021



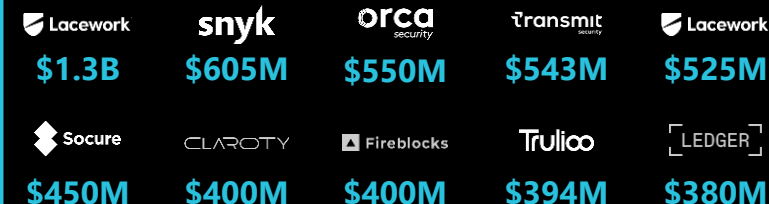
30+ New Cyber Unicorns

Including



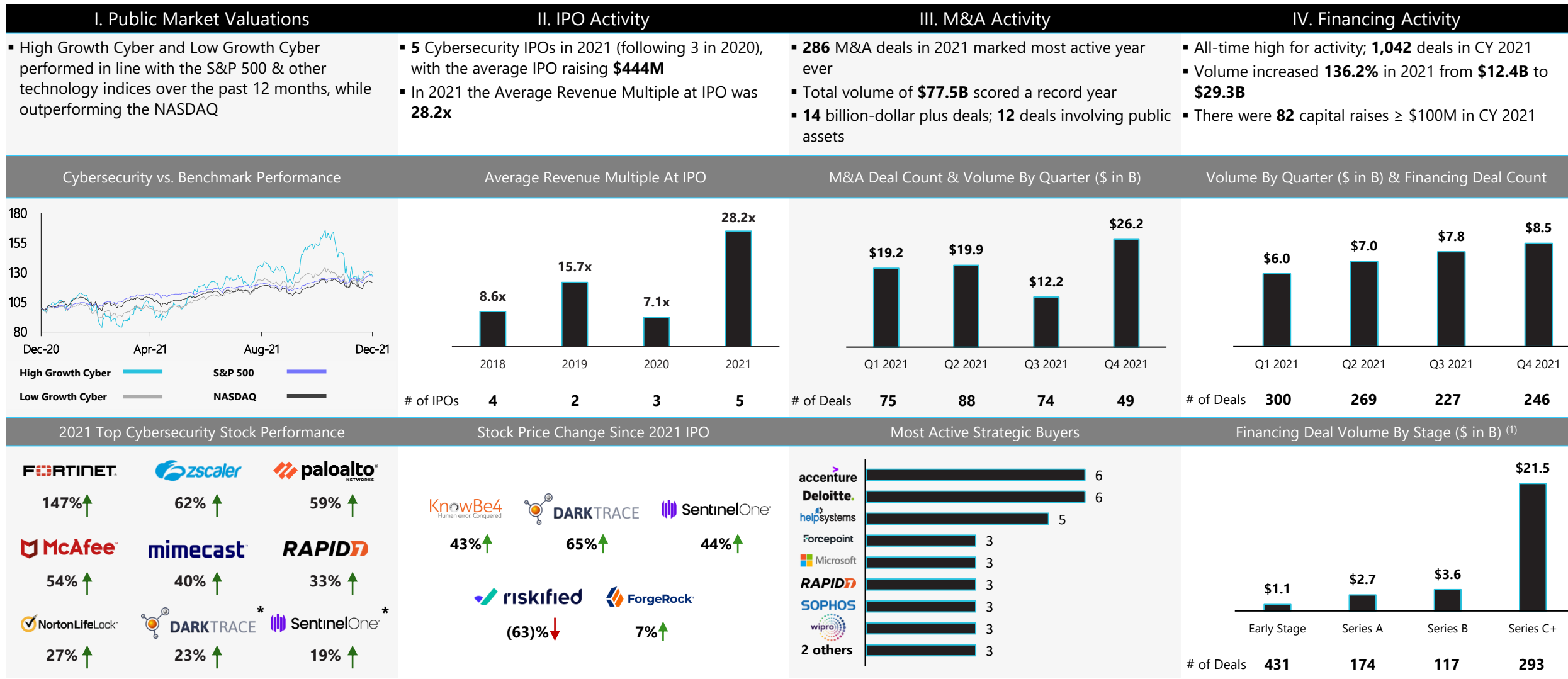
82 Capital Raises ≥ \$100M

Including



Cybersecurity Market Year in Review | CY 2021

Cybersecurity Continues To Be One Of The Most Active Sectors Of Technology Across The Public & Private Markets.



Source: Momentum Cyber Proprietary M&A & Financing Transaction Database.

* Since IPO

(1) Excludes grants and straight debt / loan financings. Follow-on financings (e.g., A, A1) in same year combined to represent one deal for that stage.

[Return To Table Of Contents](#)

The Cybersecurity Dashboard | CY 2021

\$29.3B
Financing Volume

1,042
Financing Transactions

\$77.5B
M&A Volume

286
M&A Transactions

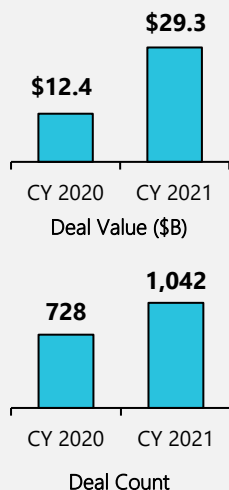
5
Initial Public Offerings

\$2.2 Billion
Gross IPO Proceeds

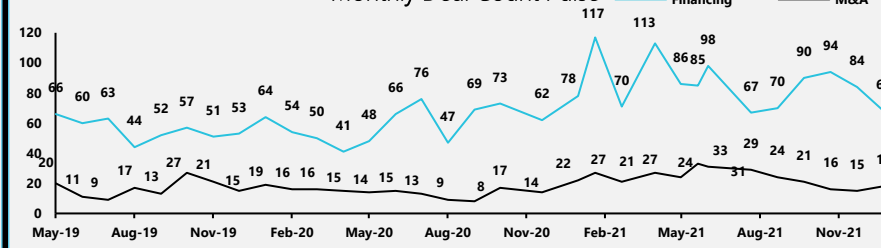
Notable Financing Transactions CY 2021

Date	Company	Amt. (\$M)
08/12/21	RSA	\$2,075.0
11/18/21	Lacework	\$1,300.0
09/08/21	snyk	\$605.0
10/05/21	orca security	\$550.0
06/22/21	transmit security	\$543.0
01/07/21	Lacework	\$525.0
11/09/21	Socure	\$450.0
12/08/21	CLAROTY	\$400.0
12/01/21	Fireblocks	\$400.0
06/07/21	Truicoo	\$394.0

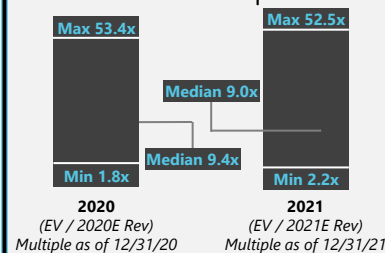
Financing Activity



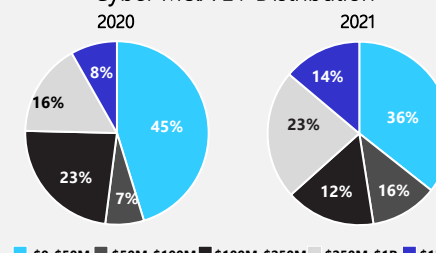
Monthly Deal Count Pulse



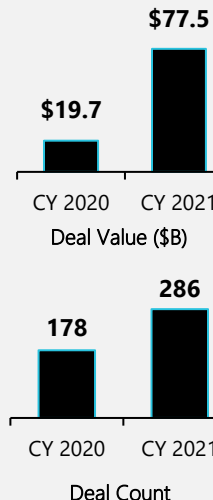
Public Comps



Cyber M&A EV Distribution



M&A

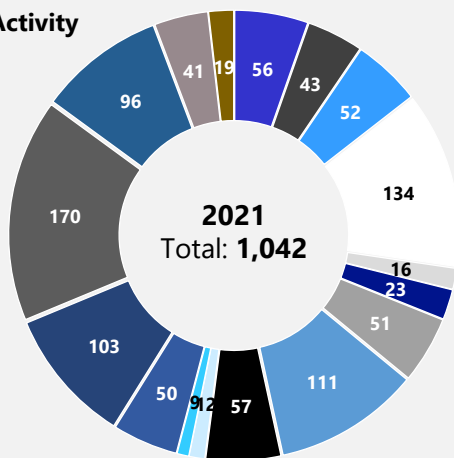
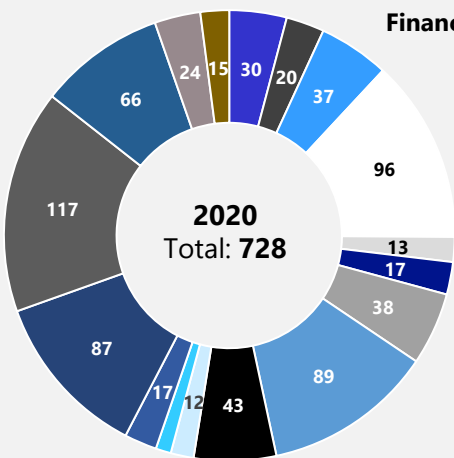


Notable M&A Transactions CY 2021

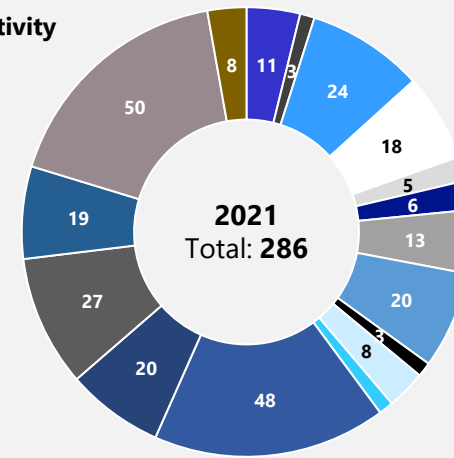
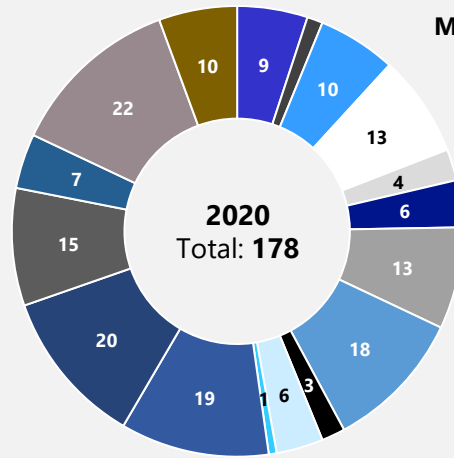
Target	Acquirer	EV (\$M)
McAfee	Advent International	\$14,085
proofpoint	THOMABRAVO	\$12,300
Avast	NortonLifeLock	\$8,020
auth0	okta	\$6,408
mimecast	PERMIRA	\$5,516
McAfee (Enterprise Business)	STG	\$4,000
appgate	NEWTOWN LANE MARKETING	\$1,575
CAPCO	wipro	\$1,450
thycotic	Centrify / TPG	\$1,400
TeleSign	NAAC	\$1,300

- Application Security
- Blockchain
- Cloud Security
- Data Security
- Digital Risk Management
- Endpoint Security
- Fraud & Transaction Security
- Identity & Access Management
- IoT
- Messaging Security
- Mobile Security
- MSSP
- Network & Infrastructure Security
- Risk & Compliance
- SecOps / IR / Threat Intel
- Security Consulting & Services
- Web Security

Financing Activity











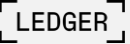




M&A Activity








A Summary Of Strategic Activity | CY 2021

14 Billion-Dollar-Plus M&A Deals, 82 Capital Raises ≥\$100M, & 5 Cyber IPOs Highlighted CY 2021 Strategic Activity.

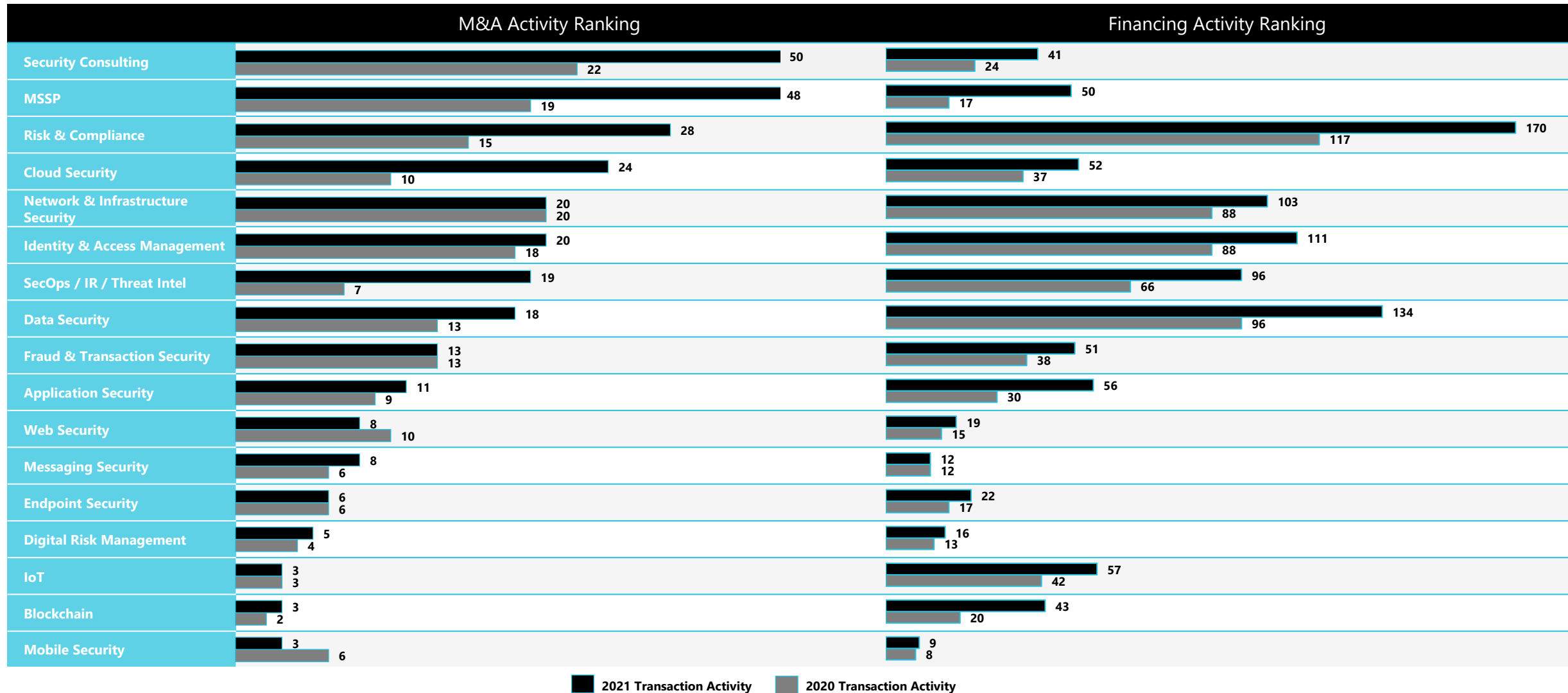
Selected Acquisition Activity (Date (M/DD): Implied Enterprise Value)		
 12/30: ND	 12/16: \$1,300M	 12/07: \$5,516M
 11/22: \$722M	 11/08: \$14,085M	 08/10: \$8,020M
 08/02: ND	 07/12: \$650M	 06/08: \$900M
 06/02: \$1,200M	 04/26: \$12,300M	 03/08: \$4,000M
 03/04: \$1,450M	 03/03: \$6,408M	 03/02: \$1,400M
 02/11: ND	 02/09: \$1,575M	 01/28: \$900M

Selected Financing Activity (Date (M/DD): \$ Raised / Funding Stage)		
 12/08: \$400M / E	 12/01: \$400M / E	 11/29: \$300M / PE Growth
 11/18: 1,300M / D	 11/09: \$450M / E	 10/05: \$550M / C
 09/08: \$605M / F	 08/10: \$240M / E	 07/16: \$355M / F
 07/09: \$300M / H	 06/22: \$543M / A	 06/10: \$380M / C
 06/07: \$394M / D	 05/25: \$300M / F	 04/06: \$210M / C
 03/05: \$180M / E	 02/22: \$270M / E	 01/07: \$525M / C

IPO Activity (IPO Date (M/YY): \$ Proceeds)
 Human error. Conquered. Market Cap: \$3,931M 04/22/21: \$152M Pre-IPO Funding: \$384M
 Market Cap: \$3,652M 04/30/21: \$198M Pre-IPO Funding: \$238M
 Market Cap: \$13,476M 06/30/21: \$1,225M Pre-IPO Funding: \$697M
 Market Cap: \$1,284M 07/29/21: \$368M Pre-IPO Funding: \$231M
 Market Cap: \$2,186M 09/16/21: \$275M Pre-IPO Funding: \$273M

M&A And Financing Activity By Sector

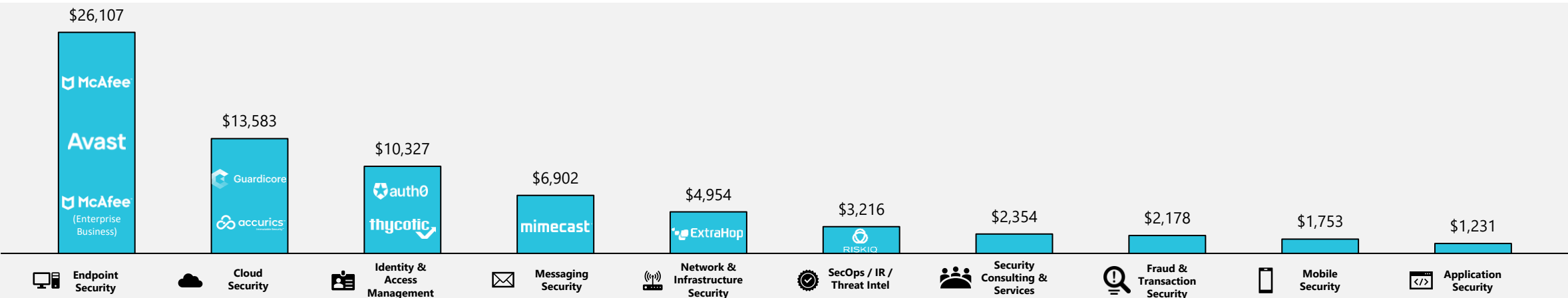
SecOps / IR / Threat Intel M&A Activity Increased By 171% From 2020, While Risk & Compliance Remained The Most Active Financing Sector (45% YoY Growth).



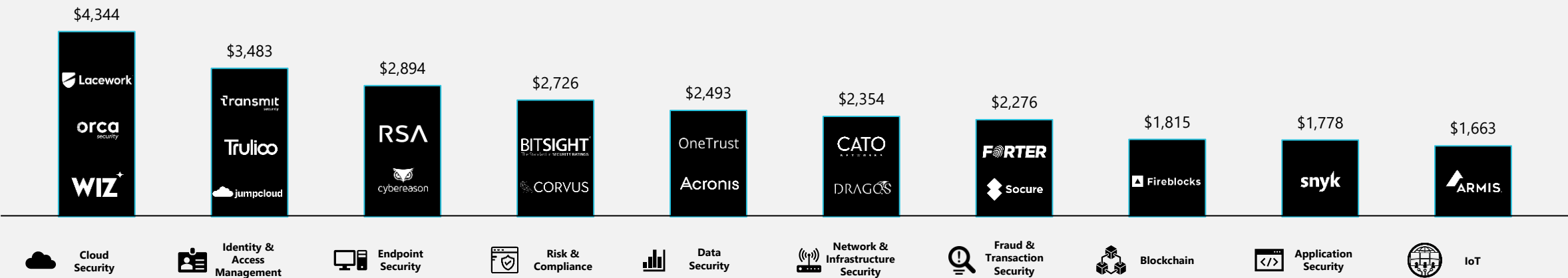
CY 2021 Top 10 Most Active M&A & Financing Volume By Sector

Endpoint Security Accounted For 34% Of Total M&A Volume, While Cloud Security Accounted For 15% Of Financing Volume.

Top 10 Sectors By Total M&A Volume (\$M) With Select Representative Targets



Top 10 Sectors By Total Financing Volume (\$M) With Select Representative Targets



Application Security

The diagram displays a comprehensive list of cybersecurity vendors, organized into several functional categories:

- Advanced Threat Protection:** Includes vendors like Barracuda, BlueFygon, BlueVector, Broadcom, Check Point, Cisco, Corsica, FireEye, Fortinet, Huawei, Hysolate, JoeSecurity, Juniper, Lastline, McAfee, Mimecast, OPSWAT, Palo Alto, Resec, Sasa Software, SonicWall, Sophos, VMware, Votiro, and WatchGuard.
- Network Security:** Includes vendors like Aruba, Cisco, Cybera, Cytera, ForeScout, Geniux, NetScout, Portnox, Pulse Secure, Trustwave, Versa, Zentara, and Zscaler.
- Network Firewall:** Includes vendors like Alcatel, Cisco, Fortinet, Imperva, NetScout, NetGuard, NetFocus, Oracle, Secure64, and StackPath.
- SASE:** Includes vendors like Cisco, Fortinet, Palo Alto, and Versa.
- Deception:** Includes vendors like CyberTrap, MimicScreen, and TrapX.
- Network Analysis & Forensics:** Includes vendors like Awake, Elictra, GCS, Cisco, Core, Corelight, Darktrace, and others.
- ICS & OT:** Includes vendors like Apero, Bayshore, Beden, Camtence, Endian, Dimerline, Owl, Radliff, SCADAance, and Verve.

A collage of various technology company logos, including Akamai, auronpro, AUTHENTiCE, Barracuda, BROADCOM, copy, CEQUESS, Check Point, cisco, ContentKeeper, CYREN, DEFiant, Forcepoint, FORTINET, GoSecure, HUMAN, iboss, imperva, McAfee, Micro Focus, NAMO-GO-GO, perimeterx, Menlo Security, proofpoint, randed, Reblaze, reflectiz, SECUREDIGITAL, SHIELD SQUARE, smoothwall, SOPHOS, TREND MICRO, Trustwave, and veritas.

Endpoint Protection

Endpoint Detection & Response

[illegible]

MSSP

[illegible]

Data Security

[illegible]

Risk & Compliance

The diagram illustrates the cybersecurity ecosystem, categorized into four main functional areas:

- Risk Assessment & Visibility:** Includes companies like Avea Networks, Axonius, Balbix, Cavirin, CAIR FIE, Coalition, CyberServer, CyberCube, CyberGuard, CyberSant, Delve, FIVEQ, InoSec, JupiterOne, KENNA, LOCALIER, Mastercard, NEMESYS, noetic, NIPSEC, Outpost, Panaseer, Prevalint, REDSEAL, riskrecon, and RiskSense.
- Risk Quantification:** Includes ARCEAO, Avea Networks, BIGSTIG, CORAX, FICO, GYREVIEW, HUMAN, Panoays, Prevalint, RiskLens, riskrecon, and SecurityScorecard.
- Pen Testing & Breach Simulation:** Includes ATTACK2U, bugcrowd, Cobalt, CROHUS, CYBERBAT, CYCINO, CYCVULNATE, DEPTH, FIREYE, KPMG, MAZEBOULT, NIPSEC, CYCIS, PICUS, RAPID7, SafeBreach, TMLite, and XM CYBER.
- Security Awareness & Training:** Includes Bannock, CyberSant, CyberSista, HOOK SECURITY, IMMERSIVE PASS, JONSCAL, KnowBe4, PHISHLABS, proofpoint, and RAINFORCE.

Other notable logos include SANS, Securonix, and Sinspace.

Security Ops & Incident Response

SIEM

AT&T Cybersecurity BLACKSTARGATE bmc CYBIRLANT

DEVO DNF SECURITY exabeam FORTINET

HanSight Huntman INTELLIGENCE IBM insight

LOGPOINT LogRhythm logz.io McAfee "Together is power." MICRO FOCUS

Netsurion EventTracker Palantir RAPID7 RSA SAMWILL

SECURIX solarwinds splunk > sumo logic TIBCO Trustwave

Veracode

Threat Intelligence

Century
CYBER

4iQ ANOMALI Bluebird
Cisco

Cyberint

Cyberint digital shadows. DOMAINTOOLS Eclectic

FORESIGHT PRODUCE FLASHPOINT InSight HanSight

HYAS INTEL 471 INTSIGHTS KELA

KING OF THE HILL LexisNexis LOOKING GLASS Malware Patrol

NUCLEON Recorded Future REVERSING LABS RiskIQ

RISKIQ Securify SIXGILL SKUR

SnowCloud ThreatConnect

IoT



































































The collage features logos for various companies in the IoT and security space, organized into two main sections:

- IoT Devices:** This section includes logos for Agileo, Xplorewell, Armis, Bastille by BlackBerry, CENTRI, Cymate, MDX, and Moxian. Below these are Deliffir, Gartner, Iconix Labs, INtuit, KeyFactor, Level, MagicCube, Migrate, and Moxian.
- Automotive:** This section includes logos for BlackBerry, BlueU, C2A, Continental, Cymotive, Enigmatos, Foretellix, G2Circ, Harman, Karamba Security, NNG, Otonomo, Cijerc, Knox, Safetide, Trillium, and Upstream.
- Connected Home:** This section includes logos for Bitdefender, CUJO AI, F-Secure, and Fortress.

Messaging Security

A collage of various technology company logos, including AGARI, AREA 1, BAE SYSTEMS, Barracuda, BlackBerry, CIBYONET, CISCO, CLEARSWIFT, CYREN, FIREYE, FOREPOINT, GREAT HORN, INKYE, IRONMASS, MICRO FOCUS, MIMESMART, NORTON LIFELOCK, PANGLOSS, PHISHLABS, PROOFPOINT, SONICWALL, SOPHOS, TRUSTWAVE, VADIA SECURE, VINTAGE, and VULNERABILITY.

Identity & Access Management

Authentication									
       									
      									
       									
       									
      									
Identity Governance									
      									
Privileged Management									
      									
Identity Governance									
     									
Consumer Identity									
       									

360 SECURITY DARKLIGHT DEMISTO DPL LABS NMAP ENCODE

FIREEYE IBM I V U McAfee Together is power. Microsoft

netScope paloalto Queryai RADAR Cyber Security RAPID7

Raytheon SEC3 servicenow SEMIFY splunk>

SWIMLANE 360 SECURITY ThreatConnect VERINT witfoo

Security Analytics

AWAKE BROADCOM CYCLRAFT DARKTRACE DTEX

exabeam Fluency FEARTINET

HanSight haystack IMVISION IT4U NOLOGISTICS IronNet Community

LogRhythm MICRO FOCUS observeIT a division of Posttension paloalto

patternsec Reservoir Labs RVIDIUM RSA

Sec3 SECURONIX sumo logic Veriato ERAMIND

THETARAY VECTRA vmware

Digital Risk Management

Blockchain

ANCHAINAI BLOCK ARMOUR CRAXEL edge
guardtime IDEE Inter/stellar NuID
Ping remmo valid.network Zamna.

Security Consulting & Services

accenture | ADAPTURE | ALIGN | AON | appsec | BishopFox | BlackBelt | Bluebird | BT | COALITION | COINTELEGRAPH | Cymon | Deloitte | Digi | EY
 FIREYE | iSchtech | GreyScale | HackingTeam | IBM | IOActive | KIVU | Komodo | KPMG | KRÖLL | KUNISBERG | leidos | Lend | LivePoint | nccgroup |
 NEC | NIS | NISG | NNTI | OPTIV | praetorian | pwc | RAVEN | REALVULNERABILITY | SecurityConcepts | SERAPHIN | SIBUR | SYGMA | VERIPUT | VERITY
 Fraud & Transaction Security
 BIOCATCH | BLOCK FRAUD | Brighterion | CARDINAL | DATAVISOR | DEFUSE | EARLY WARNING | emailage | ethoca | FICO | feedzai | FISERV | FORTER | GARDIAN | HUMAN | IdentityMind | IDenTrust | Kount | LexisNexis | MagicCube | MAXIMIO | NetGuards | NICE | NuData Security | OUTSEER | RISKIFIED | SECUREDOUCH | Shift Technology | SIFT | SIGNIFYD | SIMILITY | Secure | TokenID | TransUnion | UNIKEN | technology

Fraud & Transaction Security

Cloud Security

A hand-drawn diagram in light blue on a dark blue background. It features several 'X' marks and curved arrows. One 'X' is at the top, one in the middle, and two at the bottom. Arrows point from the top 'X' towards the center, from the middle 'X' towards the bottom, and from the bottom 'X' towards the top, creating a circular flow. There are also some faint, larger 'X' marks in the background.

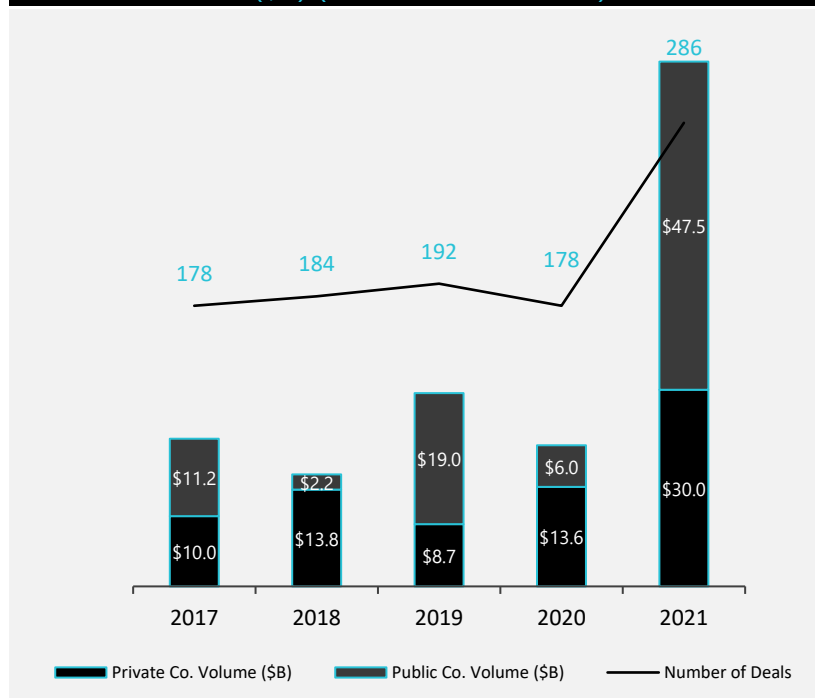
IV.

M&A ACTIVITY IN CYBERSECURITY

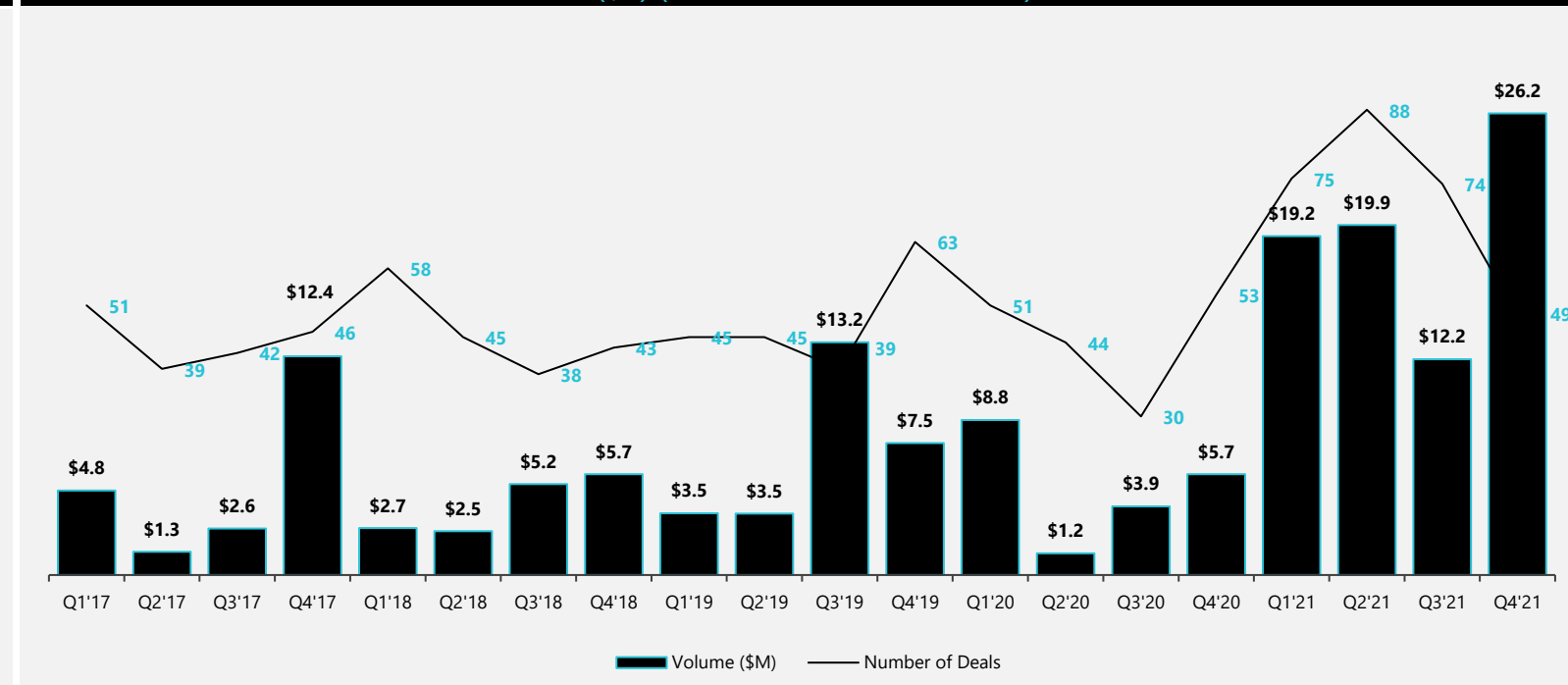
Cybersecurity M&A Activity | CY 2017 – CY 2021

Cybersecurity M&A Totaled \$162B Across 1,018 Deals Since 2017.

Annual M&A Deals And Volume
(\$B) (CY 2017 – CY 2021)



Quarterly M&A Deals And Volume
(\$B) (Q1 CY 2017 – Q4 CY 2021)



- M&A deal volume in 2021 reached **\$77.5B (294.6% YoY increase)**, across 286 deals (**60.7% YoY increase**)
- Acquisitions of public Companies / Assets totaled **\$47.5B**; transactions include **McAfee by Advent International** and Other Investors, **Avast and NortonLifeLock's merger**, and **Mimecast by Permira**
- After a blistering pace set in 1H 2021, Cybersecurity activity continued strong through Q3 2021 and Q4 2021 reaching **\$12.2B** and **\$26.2B**, respectively, while the total number of deals dipped from Q2 record highs
- Activity was primarily driven by Private Equity investments totaling **\$42.3B** across **34 deals**; Notable acquisitions included **McAfee by Advent International and Other Investors**, **Mimecast by Permira**, and **Proofpoint by Thoma Bravo**

































Source: Momentum Cyber Proprietary M&A & Financing Transaction Database.

Note: Includes private and public company M&A transactions including acquisitions of public companies and divestures of assets / operations / business units from public companies.

[Return To Table Of Contents](#)

M&A Deal Spotlight | 1H 2021

Select M&A Transactions Of Highly Strategic And Potentially Transformational Assets.

































Highlighted M&A Transactions						Large Cybersecurity Platforms Were Active Acquirers In 1H 2021 Across Multiple Sectors While Deal Volume Doubled from 1H 2020		
Date	Target	Acquirer	EV (\$M)	Sector	Impact	Sector	Target(s)	Acquirer
04/26/21	proofpoint.	 THOMABRAVO	\$12,300	Cloud Security	<ul style="list-style-type: none"> Demonstrates the significant Cybersecurity demand from the private equity space 			
03/08/21			\$4,000	Endpoint Security	<ul style="list-style-type: none"> Enables STC to combine parts of McAfee's Enterprise Business with another portfolio company, RSA Security Effectively cuts McAfee's offerings in half 			
03/03/21			\$6,408	Identity & Access Management	<ul style="list-style-type: none"> The acquisition enables Okta to expand its IAM offerings and begin catering to developer-focused customers 			
03/02/21			\$1,400	Identity & Access Management	<ul style="list-style-type: none"> Enables TPC to combine Centrify and Thycotic to provide a comprehensive PAM offering and grow IAM market share 			
02/11/21			ND	MSSP	<ul style="list-style-type: none"> Accelerates Herjavec Group's international expansion efforts, augmenting their talented team with additional threat & identity resources, and further advancing the HG Identity and HG SOAR proprietary platforms 			
02/09/21			\$1,575	Network & Infrastructure Security	<ul style="list-style-type: none"> SPAC deal brings Appgate's pure play Zero Trust solution to the public markets and accelerate expansion 			
								

Source: Momentum Cyber Proprietary M&A & Financing Transaction Database, Capital IQ, 451 Group, and Pitchbook.

[Return To Table Of Contents](#)

M&A Deal Spotlight | 2H 2021

Select M&A Transactions Of Highly Strategic And Potentially Transformational Assets.

Highlighted M&A Transactions						Large Cybersecurity Platforms Continued To Be Active Acquirers Across Multiple Sectors In 2H 2021		
Date	Target	Acquirer	EV (\$M)	Sector	Impact	Sector	Target(s)	Acquirer
12/30/21			ND	MSSP	<ul style="list-style-type: none"> Creates an industry powerhouse with a broad, holistic suite of best-in-class managed detection and response capabilities (MDR), professional services, and identity offerings 			
12/07/21			\$5,516	Messaging Security	<ul style="list-style-type: none"> Allows Mimecast to leverage Permira's strong financial backing to compete in an increasingly competitive messaging security market 			
11/22/21			\$722	Risk & Compliance	<ul style="list-style-type: none"> Enables Schwarz Group to leverage XM Cyber for internal security and to grow the platform 			
11/08/21		Advent International & 5 Other Investors ¹	\$14,085	Endpoint Security	<ul style="list-style-type: none"> Largest Cybersecurity deal of all time as of announcement in November Provides McAfee with financial and operational resources to further improve its online protection product offerings 			
11/08/21			\$860	Messaging Security	<ul style="list-style-type: none"> Enables OpenText to provide customers with a powerhouse SMB platform for data protection, threat management, email security, and compliance solutions 			
08/10/21			\$8,020	Endpoint Security	<ul style="list-style-type: none"> Enhances the financial profile of the combined company through increased scale, long-term growth, cost synergies with reinvestment capacity and strong cash flow generation 			
								

Source: Momentum Cyber Proprietary M&A & Financing Transaction Database, Capital IQ, 451 Group, and Pitchbook.

1 – Includes consortium of investors led by Advent.

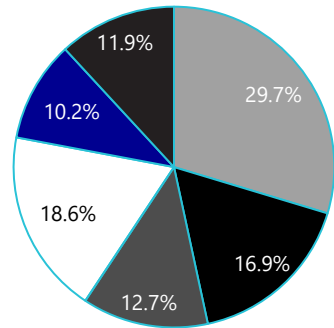
[Return To Table Of Contents](#)

Closer Look At Recent Cybersecurity "Exits" | Part 1

Breaking Down The Cybersecurity "Exits" From Q1 CY 2020 – Q4 2021.

Deal Value

- \$250M+: 26 companies; Median age of 7 years; Median Amount Raised of \$74M; Median EV / LTM Rev multiple of 14.2x
- \$50M-\$250M: 37 companies; Median age of 7 years; Median Amount Raised of \$23M; Median EV / LTM Rev multiple of 9.5x

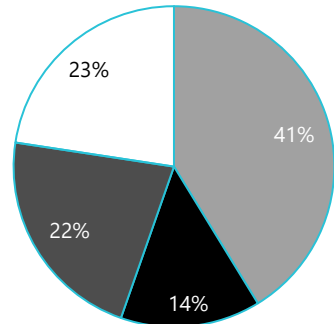


Selected Companies									
airloom	chameleonx	cloudneeti	DMARC Analyzer	EMSEC	Intalock	OPAQ Networks	POLYRIZE	observeIT	
CS CARVE SYSTEMS	CYBERPONSE	DATAGROUP	EDGEWISE	INTEGRIS SOFTWARE		Odo	Protego	SEGASEC	SYMPHONIC
ALSID	Cloud Conformity	idaptive	Indegy	IntelSecure	PERCH	portshift	preempt	threat stack	
accurics	AGARI	ampion	Aporeto	bridgecrew	CYBERX	DATAGUISE	lastline	SCALYR	sqreen
CRYP SIS	emailage	HERJAVEC GROUP	humio	INTSIGHTS	wandera				
auth0	EKCTO	FXPAPER	IronNet	QOMPLX:	SH-PE	Signal Sciences	VERAFIN		

Note: Excludes deals with undisclosed deal values (typically < \$50M). Deals with undisclosed deal values accounted for 52% of total exits.

Total \$ Raised Prior to Exit

- \$10M-\$50M: 64 companies; Median EV of \$98M; Median Age of 7 years; Active Sectors: Network & Infrastructure Security (9), Cloud Security (9), Identity & Access Management (6)
- \$50M+: 40 companies; Median EV of \$430M; Median Age of 9 years; Active Sectors: Cloud Security (7), Network & Infrastructure Security (5), Risk & Compliance (4)



Selected Companies									
chameleonx	Cloud Conformity	DFLABS	MESH7	OCTARINE	POLYRIZE	portshift	Protego	SEYTALE	STEALTHbits
accurics	ALSID	bridgecrew	CyGlass	{disrupt:Ops}	EDGEWISE	GRAMMATECH	IdentityMind	INTEGRIS SOFTWARE	privateinternetaccess
Aporeto	CYBERX	DATAGUISE	erp maestro	EXOSTAR	IntelSecure	SCALYR	securlly	SHIELDX	sqreen
AGARI	auth0	CipherCloud	CloudPassage	convercent	HYTRUST	IronNet	QOMPLX:	Signal Sciences	wandera

Source: Momentum Cyber Proprietary M&A & Financing Transaction Database, Capital IQ, 451 Group, and Pitchbook.

Note: "Exits" excludes targets that were previously acquired or listed on a public exchange; Median EV & EV / LTM Rev is inclusive of only disclosed deal values.

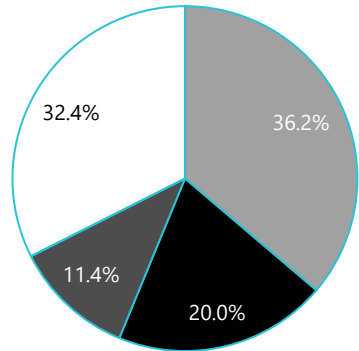
[Return To Table Of Contents](#)

Closer Look At Recent Cybersecurity "Exits" | Part 2

Breaking Down The Cybersecurity "Exits" From Q1 CY 2020 – Q4 2021.

Last Round Prior to Exit

- Series A & B: 58 companies, Median EV of \$98M; Median Age of 6 years; Median Amount Raised of \$16M
- Series C+: 60 companies, Median EV of \$190M; Median Age of 11 years; Median Amount Raised of \$49M

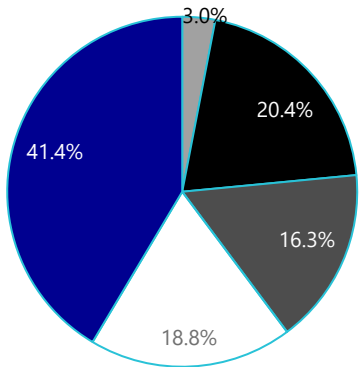


	Selected Companies									
Early Stage										
Series A										
Series B										
Series C+										

Note: Excludes debt financings and self-funded companies.

Time to Exit

- 7+ years: 218 companies; Median EV of \$100M; Median Amount Raised of \$26M; Active Sectors: Security Consulting & Services (46), MSSP (41), Network & Infrastructure Security (20)
- 7 years: 133 companies; Median EV of \$48M; Median Amount Raised of \$7M; Active Sectors: Risk & Compliance (21), Cloud Security (20), Identity & Access Management (14)



	Selected Companies									
<2 Years										
2 to 5 years										
5 to 7 years										
7 to 10 years										
10+ years										

Source: Momentum Cyber Proprietary M&A & Financing Transaction Database, Capital IQ, 451 Group, and Pitchbook.

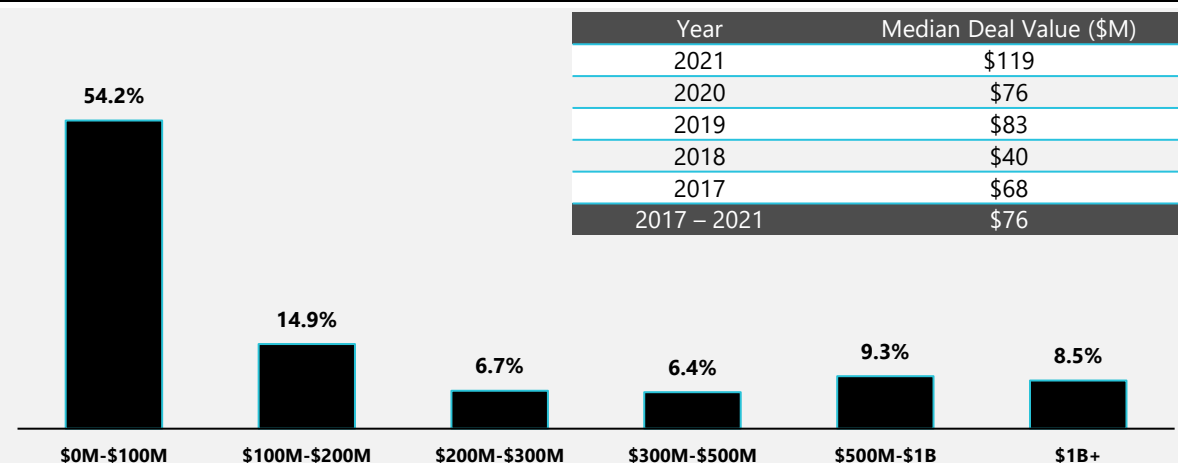
Note: "Exits" excludes targets that were previously acquired or listed on a public exchange; Median EV & EV / LTM Rev is inclusive of only disclosed deal values.

[Return To Table Of Contents](#)

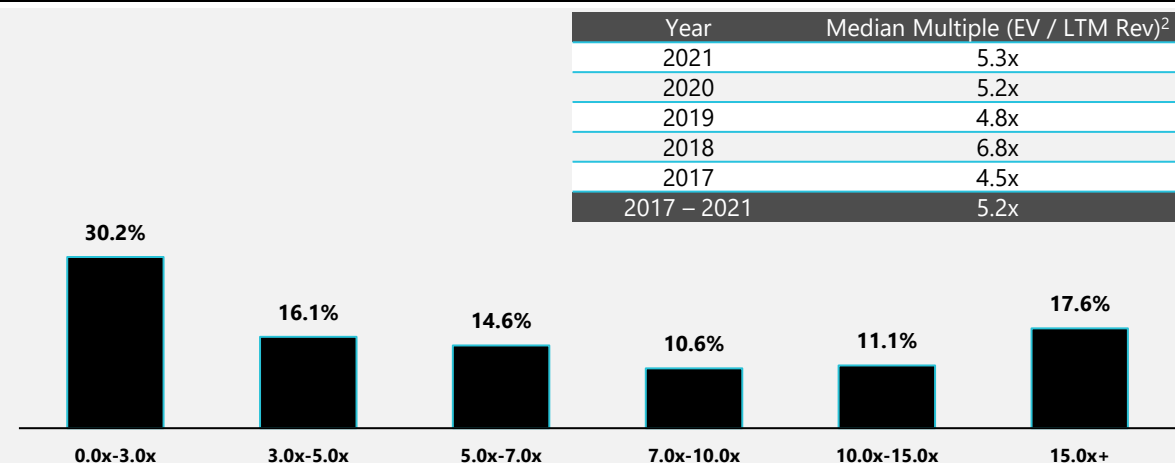
Cybersecurity M&A: A Closer Look At Deal Value & Multiples

Cybersecurity Companies Traded At Higher Valuations And Multiples From 2017-2021 Compared To 2012-2016.

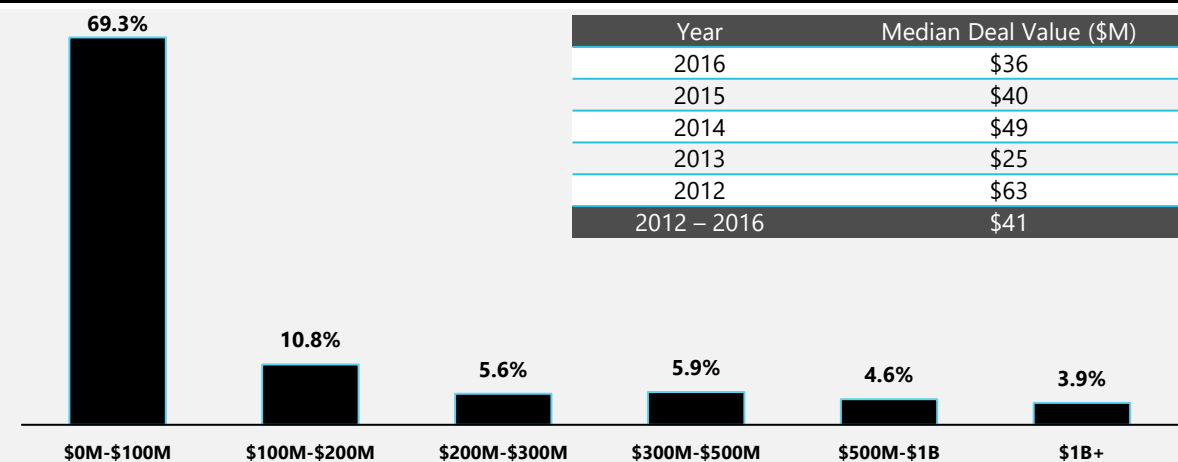
M&A By Deal Value | CY 2017 - CY 2021



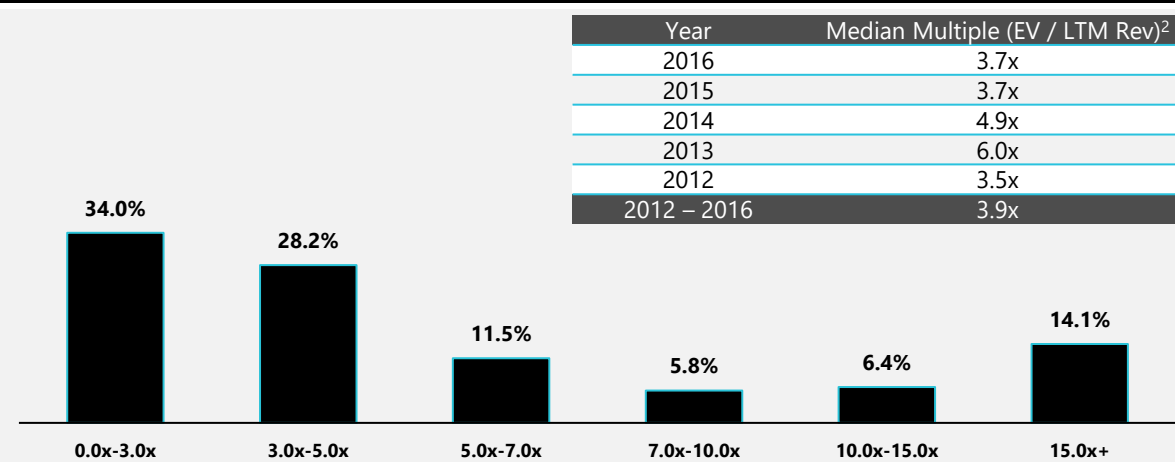
M&A By Valuation Multiples (EV / LTM Rev) | CY 2017 - CY 2021



M&A By Deal Value | CY 2012 - CY 2016



M&A By Valuation Multiples (EV / LTM Rev) | CY 2012 - CY 2016



Source: Momentum Cyber Proprietary M&A & Financing Transaction Database.

Note: ¹Includes acquisitions of public companies and divestitures of assets / operations / business units from public companies.

²EV / LTM Revenue Median Multiples cut off at 25.0x.

[Return To Table Of Contents](#)

Private Equity Continues To ❤️ Cybersecurity

PE Has A Growing Importance Throughout The Lifecycle Of A Cybersecurity Firm.

Recent Cybersecurity PE Activity

Target								
Acquirer	Advent International & 4 Other Investors	THOMABRAVO	PERMIRA	STG	Centrify / TPG	STG	BainCapital & CROSSPOINT	TPG
EV	\$14,085	\$12,300	\$5,516	\$4,000	\$1,400	\$1,200	\$900	\$900

- Private Equity firms remain serious players in the competitive market of Cybersecurity M&A, with a demonstrated ability to compete with strategic buyers for high quality assets

Funding The Next Cybersecurity Unicorns Towards IPO

							
Series D \$1,300	Series F \$605M	Series C \$550M	Series E \$450M	Series E \$400M	Series E \$400M	Series D \$394M	Series E \$380M
ALTIMETER	TIGERGLOBAL	CapitalG	Accel	SoftBank Partners	SEQUOIA	TCV	10T
							
Series F \$300M	Series H \$300M	Series F \$300M	Series C \$250M	Later Stage VC \$250M	Series E \$240M	Series F \$225M	Series C \$210M
TIGERGLOBAL	ICONIQ	SoftBank Partners	INSIGHT PARTNERS	CVC	ALKEON CAPITAL MANAGEMENT	SAPPHIRE VENTURES	SoftBank Partners

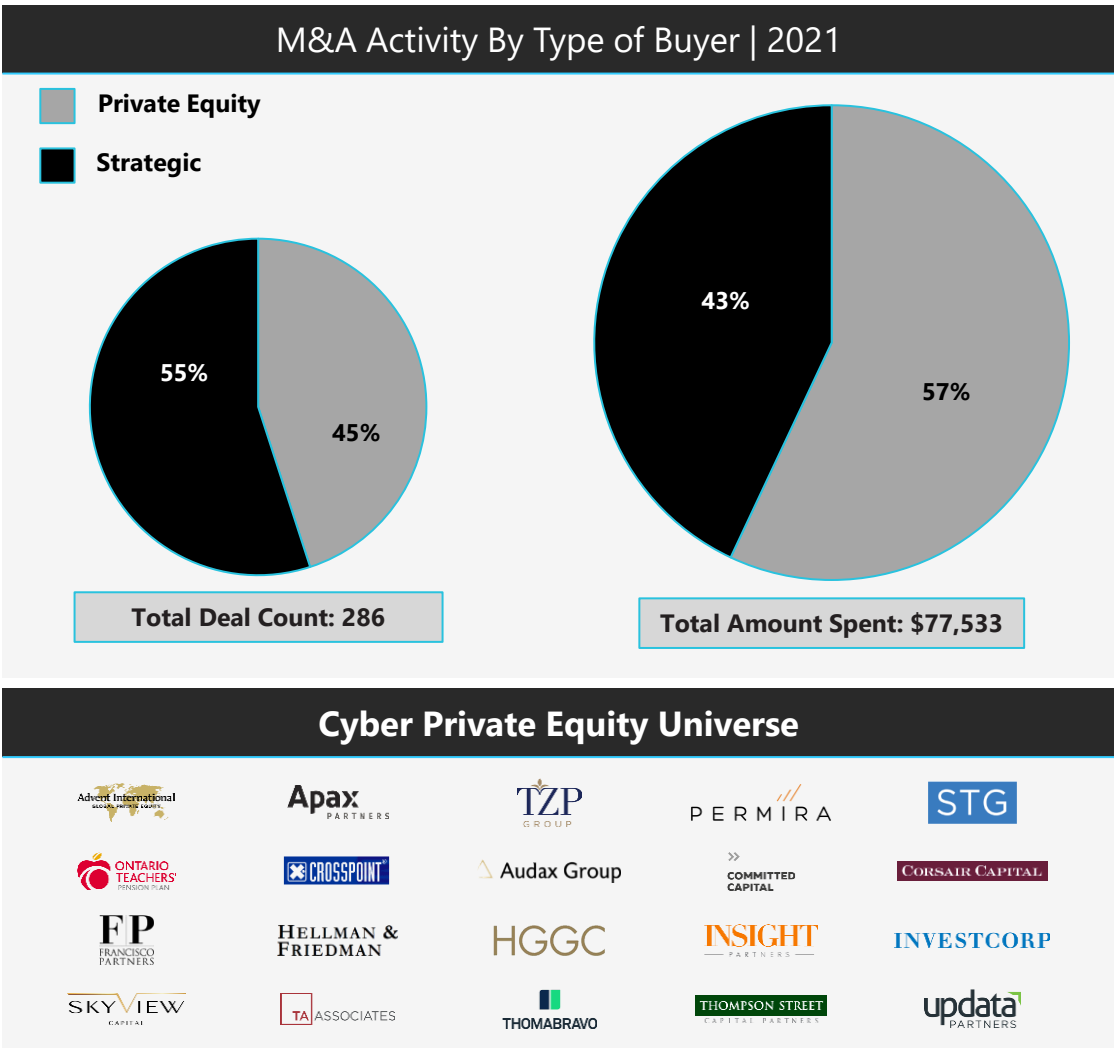
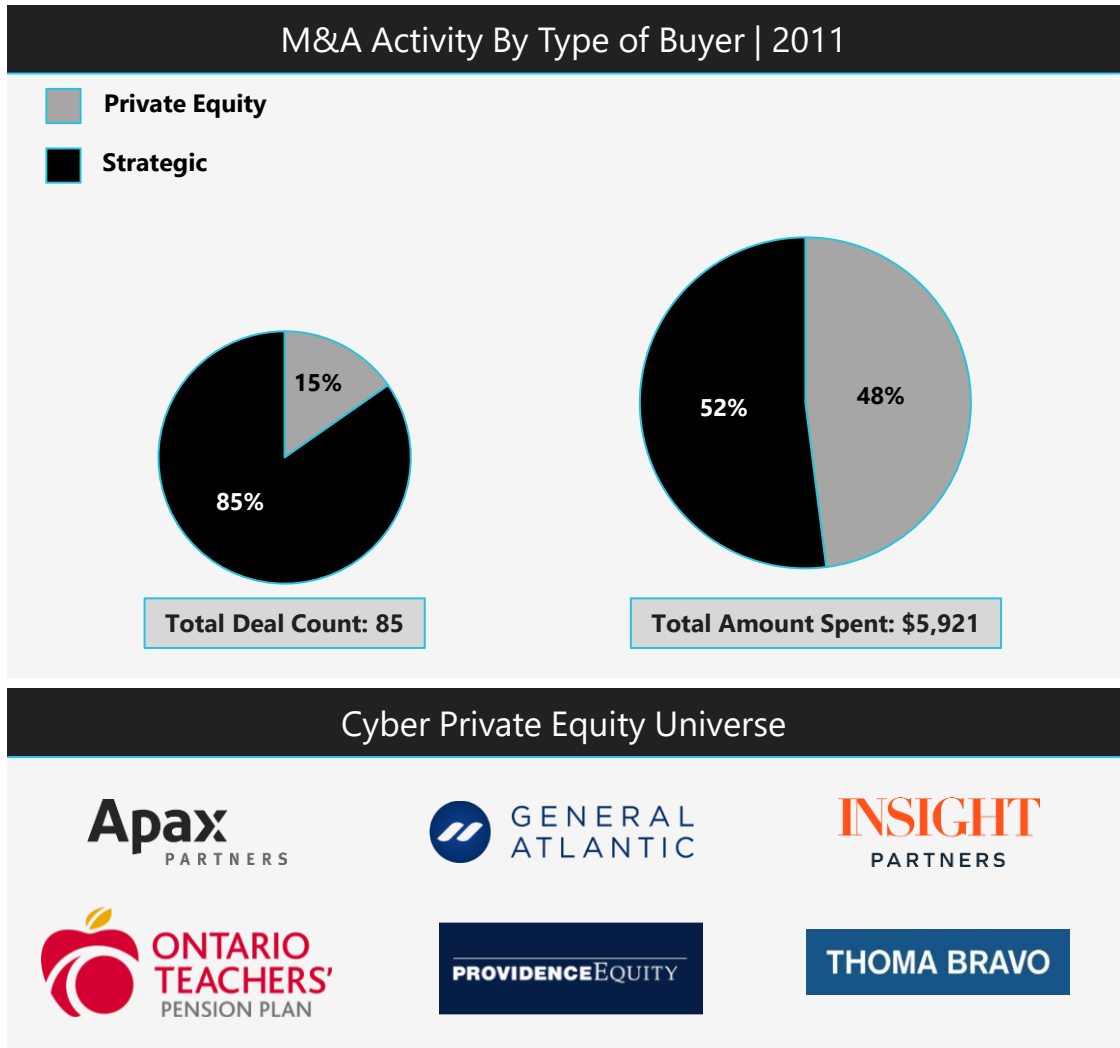
- PE / late stage and public / cross-over investors have strong appetite for break-out Cybersecurity stories that could exit via an IPO in 12 – 24 months

PE Firm → Platform → Add-Ons → Exit

	 (\$2.4B / 3.7x)	 Making the Public Cloud Private (\$45M)	 (\$280M)	 (\$4.7B / 7.8x)
HGGC	 (\$1.2B / 6.7x)	 (Assets)	 (\$38M)	 (\$219M)
THOMABRAVO	 (\$1.5B / 4.0x)	 (\$25M)	 (Managed Workplace RMM)	 (Bot Mitigation Assets)
THOMABRAVO	 (\$1.9B / 5.5x)	 (\$100M)	 CLOUDVECTOR	
TPG	 (\$900M / 8.6x)	 (\$1.4B)		
TPG	 (\$4.2B / NA)	 (\$600M / 16.2x)		 Light Point Security
				 (IPO: \$7.9B / 2.8x)

Private Equity By The Numbers

Private Equity's Market Share In Cybersecurity M&A Is Increasing Across Deal Volume And Count.



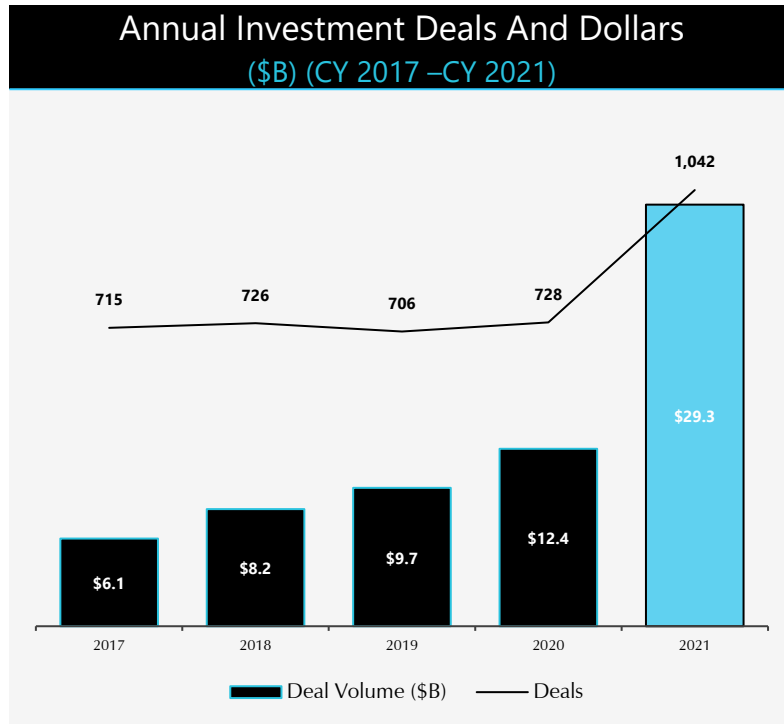


V.

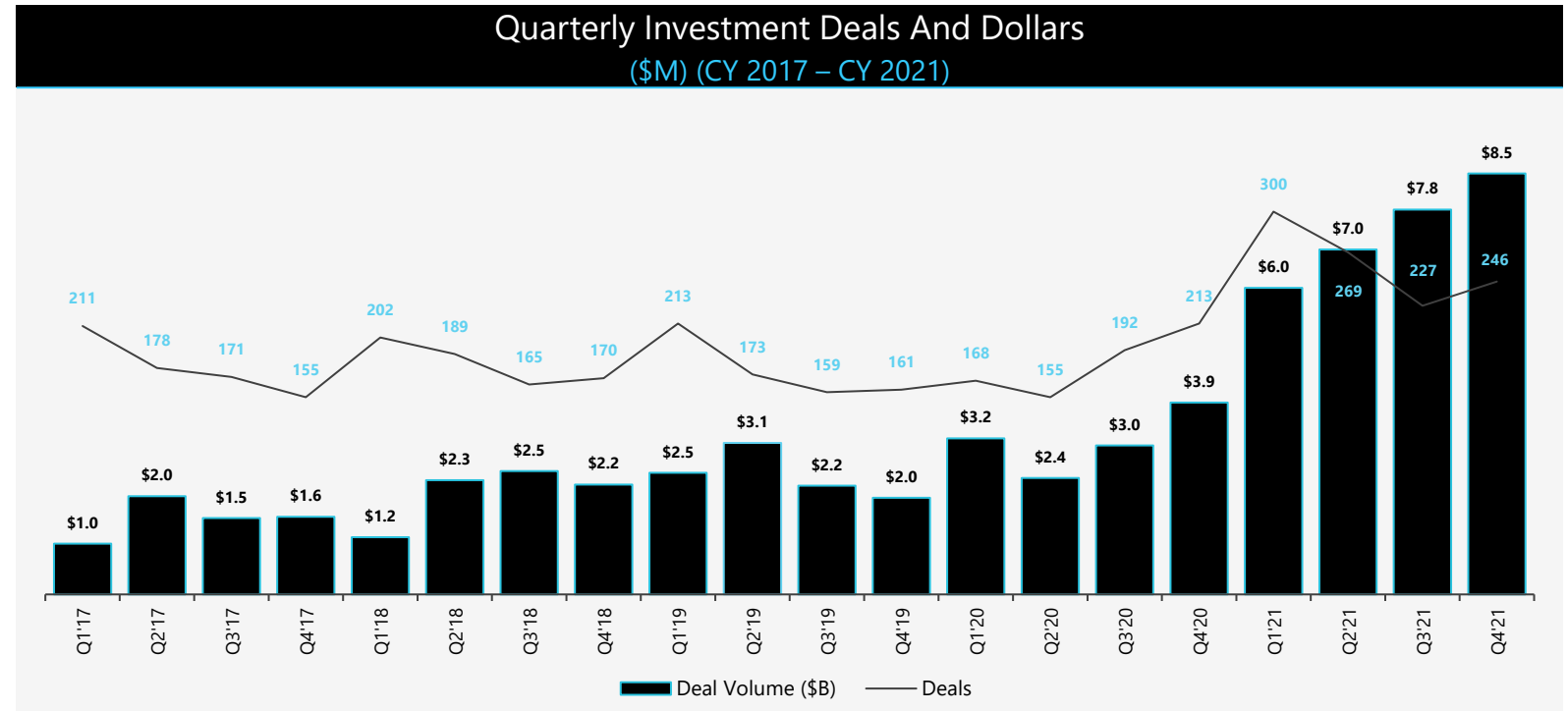
FINANCING ACTIVITY IN CYBERSECURITY

Cybersecurity Financing Activity | CY 2017 – CY 2021

Cybersecurity Startups Have Raised \$65.7 Billion Across 3,917 Deals Since CY 2017.



- **\$29.3B (+136.2% YoY increase)** was raised across **1,042 (+43.1%)** transactions in CY 2021
- Deal volume in CY 2021 alone almost equaled total volume from 2018-2020 combined (\$30.3B).

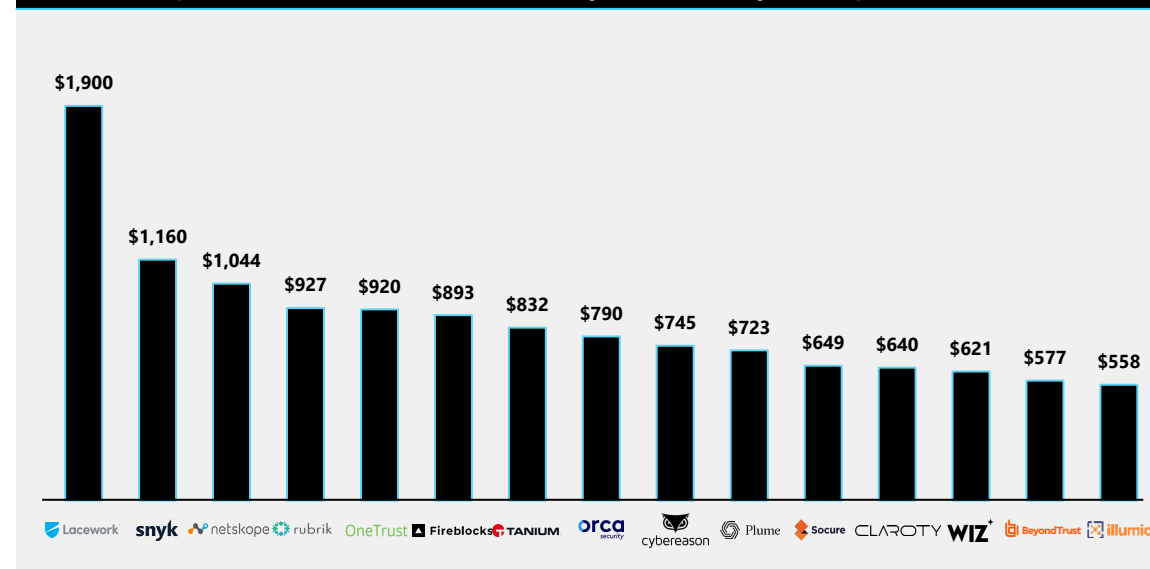


- Over the last eight quarters, investors have invested **\$41.7B** into Cybersecurity
- **\$29.3B** in CY 2021 was a new record, with **\$6.0B** invested in Q1 CY 2021 (**300** deals), **\$7.0B** invested in Q2 CY 2021 (**269** deals), **\$7.8B** invested in Q3 CY 2021 (**227** deals) & **\$8.5B** invested in Q4 CY 2021 (**246** deals)
- Q4 CY 2021 (**\$8.5B**) was a record setting quarter of funding in Cybersecurity by volume; CY 2021 was highlighted by **82 financings rounds** \geq **\$100M**, Average and Median round raised of **\$36.6M** and **\$7.6M**, respectively

Cybersecurity Venture-Backed Private Companies & Investors

List of Most Well-Funded Private Companies And Most Active Financial VC Investors.

Top 15 Well-Funded Private Cybersecurity Companies (\$M)



- The **top 15** funded private companies have raised **\$12.9B** during their lifespan
- Notable companies include Lacework which last raised **\$1.3B** in Q4 CY 2021, totaling **\$1.9B** since 2017 and Snyc, whose **\$605M** Raise in Q3 brings total raised to **\$1.1B**
- 145** other companies have raised \$100M+ in total funding (**\$33.4B**), including:

Coalition	transmit	ARCTIC WOLF	CATO	FORTER	Own{backup}	Truicoo
\$580.0	\$543.0	\$535.7	\$532.0	\$525.0	\$507.3	\$490.6
druva	LEDGER	Acronis	Signifyd	exabeam	jumpcloud	Chainalysis
\$475.0	\$464.6	\$421.7	\$421.2	\$393.0	\$380.9	\$366.7

Top 15 Most Active Financial Investors in Cybersecurity Since CY 2017 ⁽¹⁾

Investor	Number of Cyber Investments	Select Cybersecurity Investments Since 2017
INSIGHT PARTNERS	67	aqua, corelight, DARKTRACE, detectify, OneTrust, SentinelOne, transmit
Accel	66	callsign, netskope, pango, PRIVATAR, Shift Technology, snyk, TESSIAN, VECTRA
SEQUOIA	58	DASHLANE, druva, netskope, SafeBreach, SecurityScorecard, StackRox, TESSIAN
Bessemer Venture Partners	52	Auth0, AXONIUS, BigID, CAPSULE8, CLAROTY, cyberGRX, DASHLANE, HYSOLATE, KENNA
Lightspeed	50	aqua, ARCEOAI, ARCTIC WOLF, exabeam, netskope, rubrik
FORGEPOINT	44	ANITIAN, BISHOPFOX, HYTRUST, IronNet, NowSecure, Remediant, REVERSING LABS
TENELEVEN	44	cyberGRX, DARKTRACE, digital shadows, KnowBe4, ordr, sonrai, VULCAN
vertex VENTURES	40	ADAPTIVE SHIELD, AXONIUS, CYBERAVTA, IMENTIV, Own{backup}, SIGNIFYD, VERY GOOD SECURITY
BainCapital	36	Attivo Networks, BetterCloud, Nightfall, ShiftLeft, SIGNIFYD, Sysdig
ClearSky	34	BigID, CAPSULE8, INKY, INTSIGHTS, preempt, respond, SKOUT, ZERONORTH
PALADIN CAPITAL GROUP	33	bugcrowd, CALYPSO, expel, NISOS, nanaseer, TATGE-DEK, RiskLens, WARRIOR
NEA	33	bitglass, expel, FORTER, hackerone, THREATQUOTIENT, virtru, ZEROFOX
YL VENTURES	31	Karamba Security, cocode, PIANO, ORCA security, Hunters, satori
andreesen.horowitz	30	Matter Labs, SentiLink, Material, VERY GOOD SECURITY, ANCHORAGE DIGITAL
GGVCAPITAL	29	ORCA security, torq, Synack, DRATA, vdoo, idwall, HashiCorp




















Denotes pure-play Cybersecurity investors

Source: Momentum Cyber Proprietary M&A & Financing Transaction Database, Capital IQ, and Pitchbook.
 (1) Total number of investments made in rounds with a minimum of \$5 million raised; excludes strategic investors.

Cybersecurity Unicorns

Companies Reaching Unicorn Status Are Raising Increasingly Larger Rounds As Investors Continue To Make Bigger Bets On the Industry.

CY 2021 minted 37 new Cybersecurity unicorns (\$1B+ Valuation)

Current Private / Independent Cybersecurity Unicorns								
Date Of Unicorn Status	Company	Recent Lead Investor	Sector	Last \$ Raised (\$M)	Last Round	Total Raised (\$M)	⁽¹⁾ Post Money Valuation	
2021	12/26/21	 SALT	Alphabet	SecOps / IR / Threat Intel	\$135.0	Later Stage VC	\$265.7	\$1.5B
	12/15/21	 noname	Lightspeed	Application Security	\$135.0	Series C	\$220.0	\$1.0B
	12/07/21	 incode	GENERAL ATLANTIC	Identity & Access Management	\$220.0	Series B	\$270.0	\$1.3B
	12/02/21	 panther	COATUE	Cloud Security	\$120.0	Series B	\$140.5	\$1.4B
	11/30/21	 CERTIK	SEQUOIA	Blockchain	\$80.0	Series B2	\$152.2	\$1.0B
	11/18/21	 expe1	CapitalG	MSSP	\$140.3	Series E	\$257.8	\$1.0B
	11/09/21	 CONTRAST SECURITY	Liberty Strategic Capital	Application Security	\$150.0	Series E	\$272.0	\$1.4B
	11/08/21	 DRATA	ICONIQ	Risk & Compliance	\$100.0	Series B	\$128.2	\$1.0B
	10/28/21	 DRAGOS	BlackRock	Network & Infrastructure Security	\$200.0	Series D	\$358.2	\$1.7B
	10/19/21	 jumpcloud	SAPPHIRE PARTNERS	Identity & Access Management	\$225.0	Series F	\$380.9	\$2.6B
	09/15/21	 ALLOY	Lightspeed	Fraud & Transaction Security	\$100.0	Series C	\$157.5	\$1.4B
	09/15/21	 persona	FOUNDERS FUND	Identity & Access Management	\$150.0	Series C	\$217.5	\$1.5B
	09/13/21	 BITSIGHT [™] <small>THE STANDARD IN SECURITY RATINGS</small>	Moody's	Risk & Compliance	\$250.0	Series E	\$415.1	\$2.4B
	07/27/21	 1Password	Accel	Identity & Access Management	\$100.1	Series B	\$300.1	\$2.0B
	07/27/21	 Fireblocks	COATUE	Blockchain	\$310.0	Series D	\$892.5	\$2.2B
	06/22/21	 transmit security	GENERAL ATLANTIC	Identity & Access Management	\$543.0	Series A	\$543.0	\$2.7B
	06/15/21	 CLAROTY	Bessemer Venture Partners	Network & Infrastructure Security	\$140.0	Series D	\$640.0	\$1.0B
	06/10/21	 Ledger	10T	Blockchain	\$380.0	Series C	\$464.6	\$1.5B
	06/09/21	 AURA [™]	WARBURG PINCUS	Fraud & Transaction Security	\$150.0	Series E	\$350.0	\$1.0B

Source: Momentum Cyber Proprietary Financing Transaction Database, Pitchbook, Crunchbase, Company Website and Press Releases.











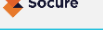

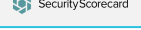
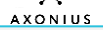


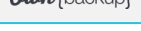

(1) Post-Money Valuation As Of The Company's Most Recent Disclosed Fundraising.

[Return To Table Of Contents](#)

Cybersecurity Unicorns

Companies Reaching Unicorn Status Are Raising Increasingly Larger Rounds As Investors Continue To Make Bigger Bets On the Industry.

CY 2021 minted 37 new Cybersecurity unicorns (\$1B+ Valuation)

Current Private / Independent Cybersecurity Unicorns								
Date Of Unicorn Status		Company	Recent Lead Investor	Sector	Last \$ Raised (\$M)	Last Round	Total Raised (\$M)	⁽¹⁾ Post Money Valuation
2021	06/07/21	 Truioo	TCV	Identity & Access Management	\$394.0	Series D	\$490.6	\$1.8B
	06/01/21	 exabeam	OWL ROCK	Security Ops & Incident Response	\$200.0	Series F	\$393.0	\$2.4B
	04/29/21	 VECTRA	Blackstone	Network & Infrastructure Security	\$130.0	Series F	\$356.6	\$1.1B
	04/22/21	 sift	INSIGHT PARTNERS	Fraud & Transaction Security	\$75.0	Series E	\$208.3	\$1.2B
	04/15/21	 Signifyd	OWL ROCK	Fraud & Transaction Security	\$205.0	Series E	\$421.2	\$1.4B
	03/26/21	 Chainalysis	Paradigm	Blockchain	\$100.0	Series D	\$366.7	\$2.1B
	03/24/21	 feedzai	KKR	Fraud & Transaction Security	\$200.0	Series D	\$282.0	\$1.0B
	03/23/21	 orca security	CapitalG	Cloud Security	\$550.0	Series C	\$790.0	\$1.2B
	03/18/21	 ID.me	Viking	Identity & Access Management	\$100.0	Series C	\$244.4	\$1.6B
	03/17/21	 WIZ+	Advent Ventures Partners	Cloud Security	\$130.0	Series B	\$600.0	\$1.7B
	03/16/21	 Secure	Accel	Fraud & Transaction Security	\$100.0	Series D	\$649.0	\$1.3B
	03/10/21	 aqua run	ION	Cloud Security	\$135.0	Series E	\$266.3	\$1.0B
	03/05/21	 SecurityScorecard	G/	Risk & Compliance	\$180.0	Series E	\$293.4	\$1.1B
	02/25/21	 AXONIUS	stripes	Risk & Compliance	\$100.0	Series D	\$195.0	\$1.3B
	02/22/21	 Plume	SoftBank	IoT	\$270.0	Series E	\$722.9	\$1.4B
	02/01/21	 Coalition	Index Ventures	Risk & Compliance	\$175.0	Series D	\$580.0	\$1.8B
	01/28/21	 Own{backup}	INSIGHT PARTNERS	Data Security	\$167.5	Series D	\$507.3	\$1.5B
	01/07/21	 Lacework	ACTIMETER	Cloud Security	\$525.0	Series D	\$1,900.0	\$1.0B









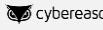











Source: Momentum Cyber Proprietary Financing Transaction Database, Pitchbook, Crunchbase, Company Website and Press Releases.

(1) Post-Money Valuation As Of The Company's Most Recent Disclosed Fundraising.

[Return To Table Of Contents](#)

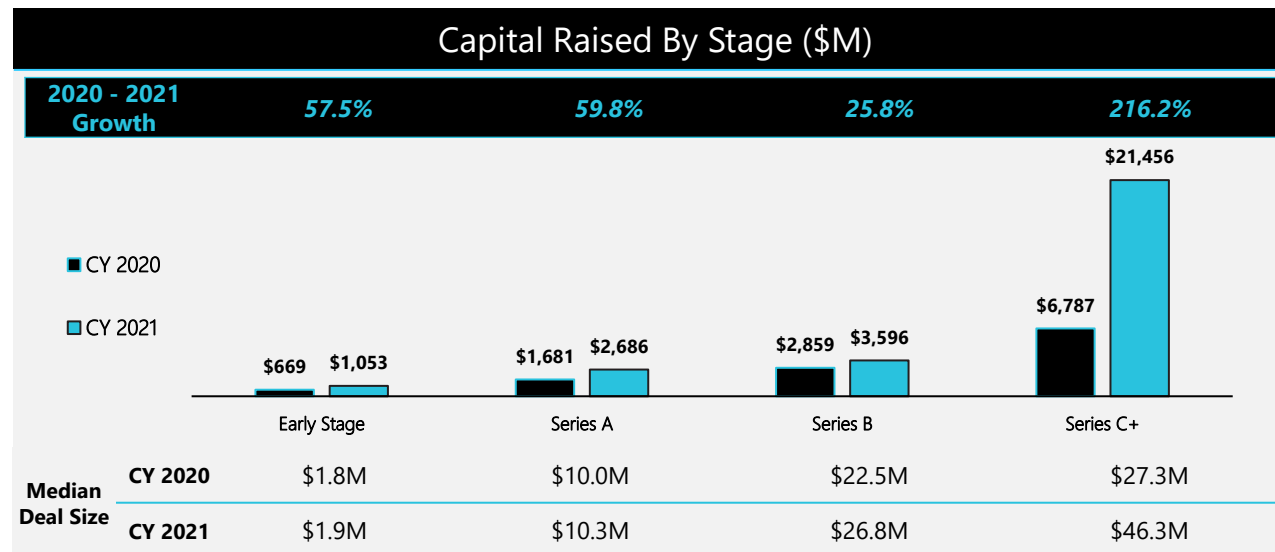
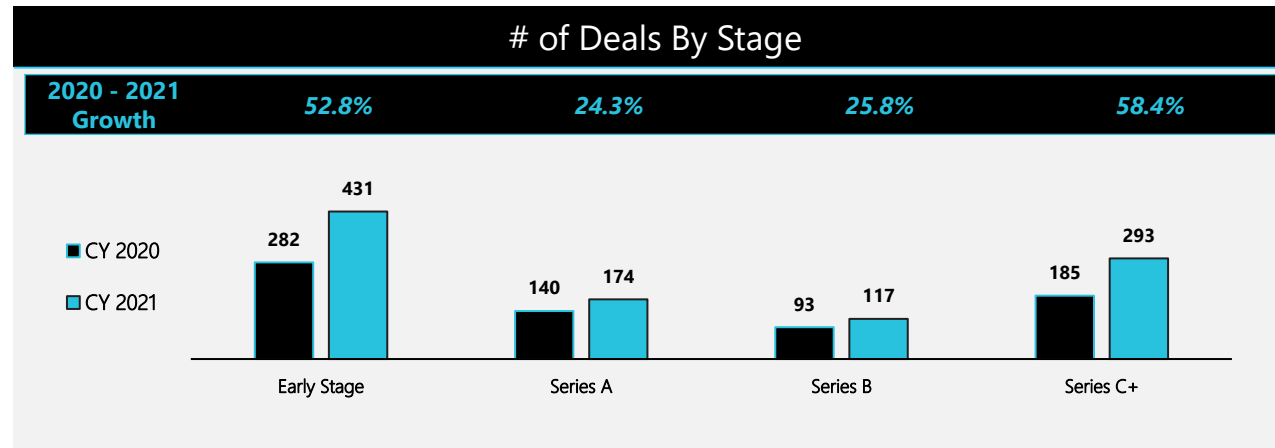
Cybersecurity Unicorns

Companies Reaching Unicorn Status Are Raising Increasingly Larger Rounds As Investors Continue To Make Bigger Bets On the Industry.

Current Private / Independent Cybersecurity Unicorns							
	Date Of Unicorn Status	Company	Recent Lead Investor	Sector	Last \$ Raised (\$M)	Last Round	(1)Post Money Valuation
2020	12/16/20	 BigID	TIGERGLOBAL	Data Security	\$70.0	Series D	\$1.0B
	12/10/20	 VENAFI	THOMABRAVO	Risk & Compliance	N/A	PE Growth	\$1.2B
	11/19/20	 FORTER	TIGERGLOBAL	Fraud & Transaction Security	\$300.0	Series F	\$3.0B
	11/17/20	 CATO	Lightspeed	Network & Infrastructure Security	\$130.0	Series E	\$1.1B
	10/22/20	 ARCTIC WOLF	Viking	MSSP	\$200.0	Series E	\$1.3B
	01/21/20	 snyk	Accel	Application Security	\$199.1	Series E	\$4.7B
2019	11/05/19	 riskified	GENERAL ATLANTIC	Fraud & Transaction Security	\$3.4	Later Stage VC	\$1.0B
	09/18/20	 Acronis	CVC	Data Security	\$250.0	Later Stage VC	\$2.5B
	08/05/19	 cybereason	SoftBank Group	Endpoint Security	\$200.0	Series E	\$1.0B
	07/13/19	 OneTrust	SoftBank Group	Data Security	\$210.0	Series C	\$5.1B
	06/20/19	 druva	CDPQ	Data Security	\$147.0	PE Growth	\$2.0B
	05/20/19	 Auth0	salesforce ventures	Identity & Access Management	\$120.0	Series F	\$1.9B
2018	11/13/18	 netskope	SEQUOIA	Cloud Security	\$340.0	Series G	\$1,044.0
	11/01/18	 HashiCorp	FRANKLIN TEMPLETON	Cloud Security	\$175.0	Series E	\$5.3B
2017	10/10/17	 同盾科技 www.tongdun.cn	GGVCAPITAL	Fraud & Transaction Security	\$115.0	Series E	\$361.6
	04/28/17	 rubrik	Undisclosed	Data Security	\$373.5	Series E	\$926.5
Unicorn Pipeline (1)Post-Money Valuation in \$M)							
		 pindrop	 Menlo Security	 corelight	 sparkcognition		
		\$900.0	\$800.0	\$825.0	\$750.0		

A Breakdown Of Cybersecurity Capital Raises By Stage

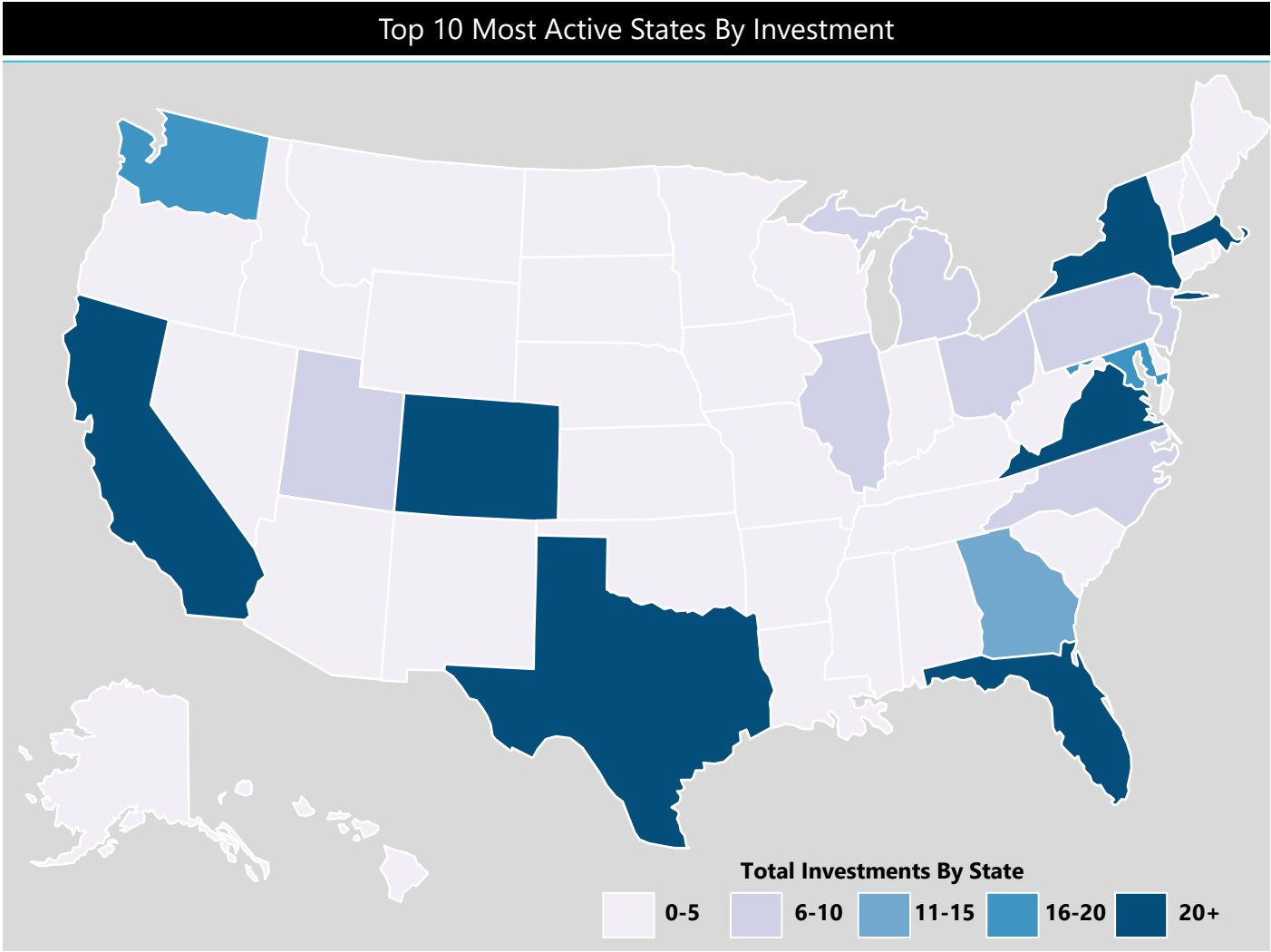
Investments Over The Past 2 Years | CY 2020 – CY 2021.













Selected Companies By Stage				
Early Stage	ACTIVEFENCE	ANAPAYA	BreachQuest	CipherStash
	32e-assure	FLOW	TALON	PRIVATE AI
	Q5id	Threat Key	toposware	
Series A	TripleBlind	TRUSTDOCK	WITESAND	ZAMA
	COWBELL CYBER	cycode	CYE	HYPORI
	incode	monad	neosec	QUANTUMXCHANGE
Series B	satori	secureframe	StackPulse	Stairwell
	Tausight	transmit security	Vanta	VISIBLERISK
	1Password	AppOmni	Armorblox	CYWARE
Series C+	DATA DOME	DATA GRAIL	envelop	JupiterOne
	Material	persona	PRIVACERA	STERNUM
	strongdm	UpGuard	vdoo	WIZ
Series C+	Acronis	Aware	Coalition	exabeam
	feedzai	FORTER	Lacework	Ledger
	OneTrust	orca security	Own{backup}	Plume
	SecurityScorecard	Signifyd	snky	Truilio

U.S. Cybersecurity Funding By State













































































































































































































Investments Are Still Concentrated In Traditional Hubs, But New Hubs Are Continuing To Attract Investment.



Funding Ranking Detail – 567 Total Investments In USA In 2021				
Ranking	State		# of Investments	Total \$ Invested (\$M)
1.	California		195	\$10,042
2.	New York		54	\$3,305
3.	Massachusetts		43	\$4,969
4.	Virginia		42	\$607
5.	Texas		31	\$402
6.	Colorado		21	\$630
7.	Florida		21	\$283
8.	Maryland		18	\$403
9.	Washington		17	\$58
10.	Georgia		11	\$261
Total			453	\$20,960

Notable Cybersecurity Funded Companies

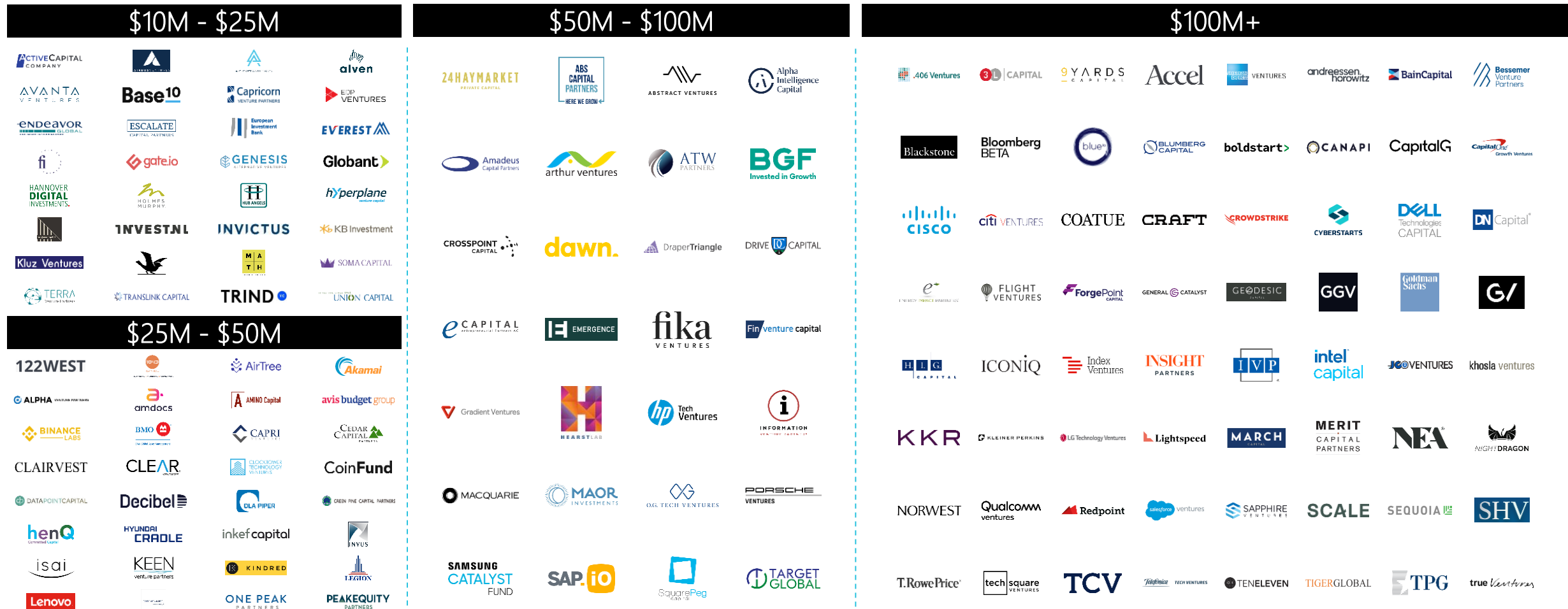
Select Companies That Have Raised \$10M+ | CY 2017 – CY 2021.

\$10M - \$25M					\$50M - \$100M					\$100M+														
																								
																								
																								
																								
																								
																								
																								
																								
\$25M - \$50M																								
																								
																								
For Additional Information On Backup Data Supporting Transaction Data, Please Contact Momentum Cyber.										Total Amount Raised (\$M)										\$65,657.4				
										Median Amount Raised (\$M)										\$5.8				

Source: Momentum Cyber Proprietary M&A & Financing Transaction Database, Capital IQ, and Pitchbook.
□ Denotes companies that have been acquired since CY 2017; □ Denotes companies that have IPO-ed and SPAC-ed since CY 2017

Active Cybersecurity Investors

Select Firms That Have Investments Totaling \$10M+ | CY 2017 – CY 2021.



For Additional Information on Backup Data Supporting Transaction Data, Please Contact Momentum Cyber.

VI.

PUBLIC COMPANY TRADING ANALYSIS

	Buy	Sell	Grow
Gold	\$285.00	\$314.07	10.20%
Silver	\$175.00	\$480.75	28.20%
Platinum	\$625.00	\$663.75	6.20%
Steel	\$769.00	\$828.98	7.80%
Aluminum	\$424.00	\$552.90	30.40%
Tungsten	\$326.00	\$419.89	28.80%
Manganese	\$400.00	\$448.80	12.20%
Uranium	\$588.00	\$726.77	23.60%
Nickel	\$351.00	\$442.26	26.00%
Cobalt	\$517.00	\$578.01	11.80%
Resin	\$583.00	\$753.24	29.20%

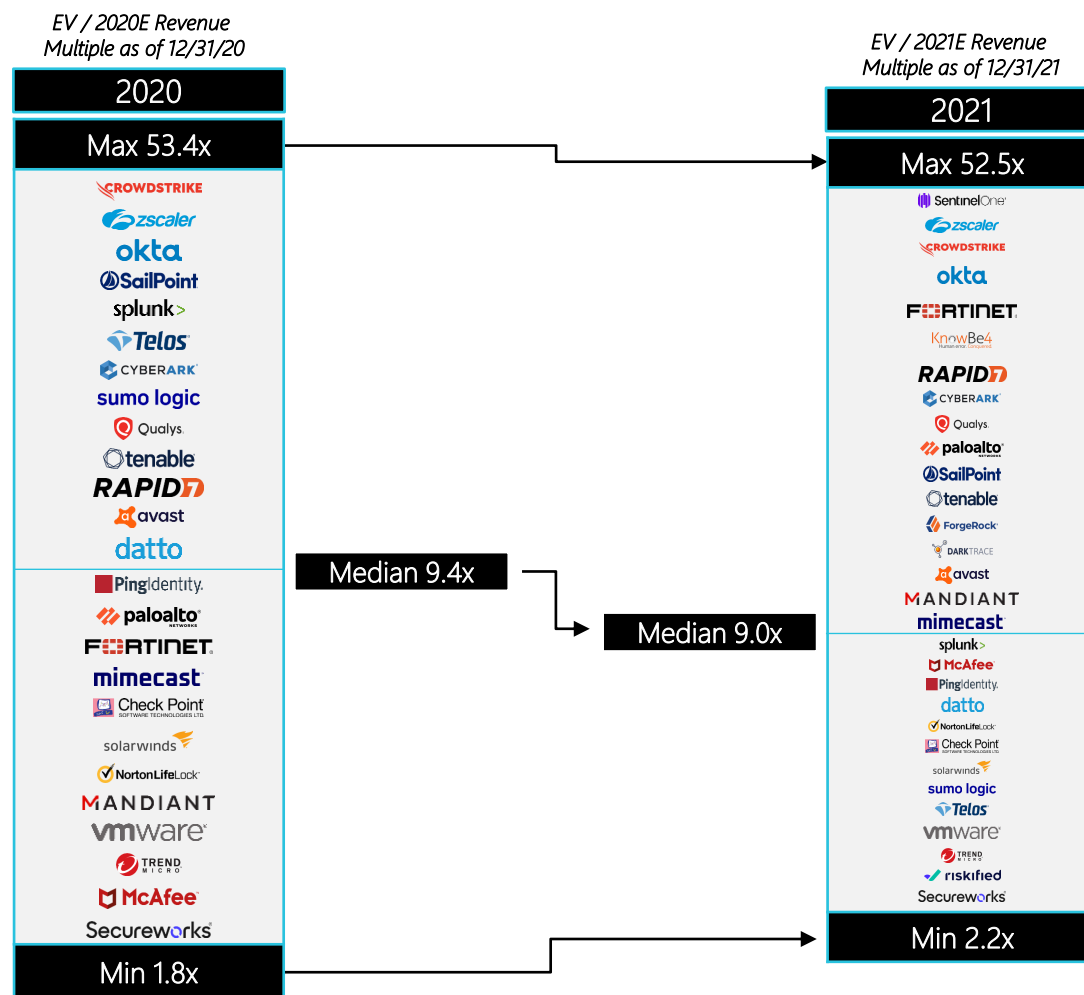
Cotton	\$162.60	\$162.60	37.80%
Flax	\$191.35	\$191.35	18.60%
Textiles	\$173.03	\$173.03	21.60%
Wool	\$241.00	\$241.00	24.00%
Fur	\$109.00	\$151.07	38.60%
Screen	\$789.00	\$935.75	18.60%
Silk	\$722.00	\$877.95	21.60%
Electric Pow	\$602.00	\$746.48	24.00%



Cybersecurity Multiples Year-Over-Year

Majority Of Public Company Valuations Have Slightly Decreased Along With Broader Market Indices.

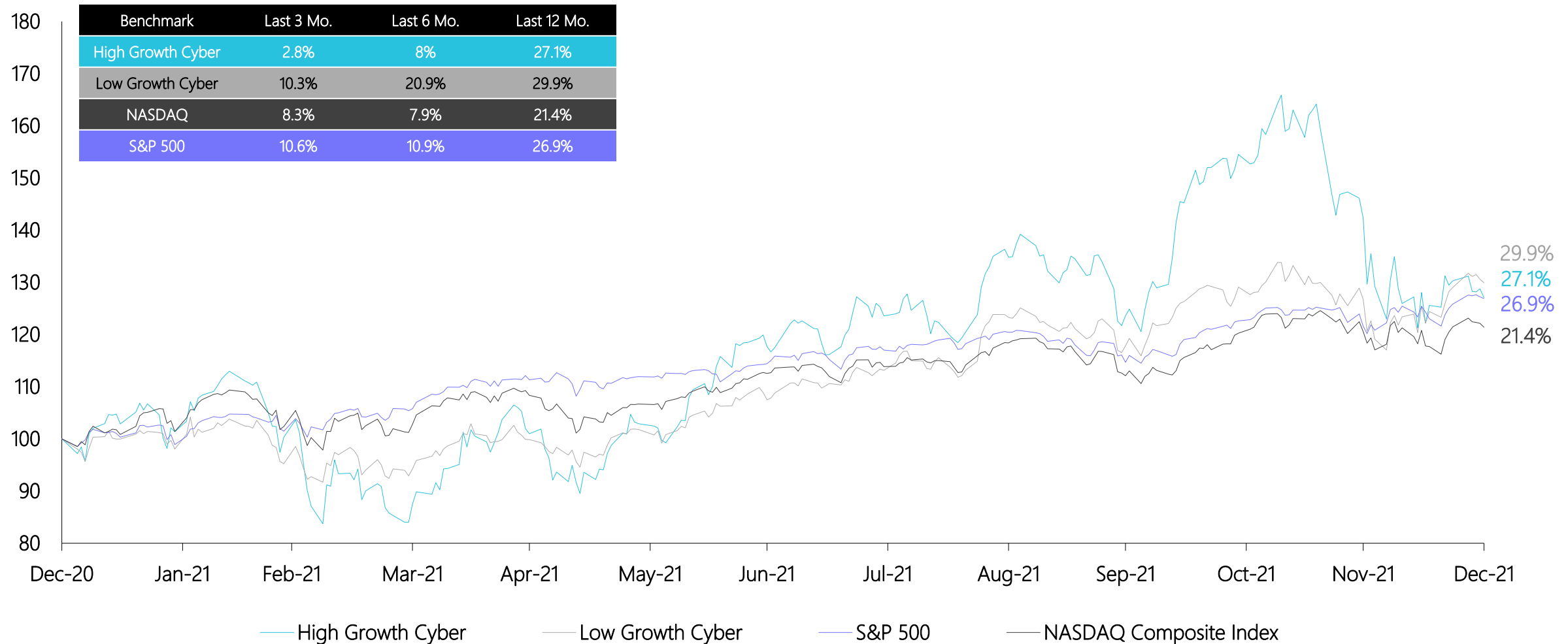
In-Step With The Broader Market, The Majority Of Cybersecurity Revenue Multiples Have Slightly Declined Over The Past 12 Months



Company	EV / 2020E Revenue	EV / 2021E Revenue	% Change
McAfee	2.5x	6.8x	172%
FORTINET	8.8x	17.0x	94%
MANDIANT	5.7x	9.2x	60%
paloalto	9.2x	11.5x	25%
Secureworks	1.8x	2.2x	20%
RAPID7	11.8x	13.9x	18%
mimecast	7.6x	9.0x	17%
NortonLifeLock	6.0x	6.4x	6%
zscaler	50.0x	52.5x	5%
Avast	9.5x	9.5x	1%
CYBERARK	12.6x	12.5x	(1%)
Qualys	12.0x	11.9x	(1%)
TREND MICRO	3.7x	3.5x	(5%)
tenable	11.9x	10.6x	(11%)
SailPoint	13.2x	10.8x	(18%)
solarwinds	6.2x	5.0x	(20%)
Check Point	7.2x	5.4x	(24%)
Ping	9.3x	6.8x	(27%)
vmware	5.2x	3.7x	(28%)
datto	9.4x	6.7x	(29%)
okta	39.3x	26.9x	(31%)
splunk	13.0x	7.9x	(40%)
CROWDSTRIKE	53.4x	32.0x	(40%)
sumo logic	12.5x	4.9x	(61%)
Telas	12.9x	3.8x	(71%)

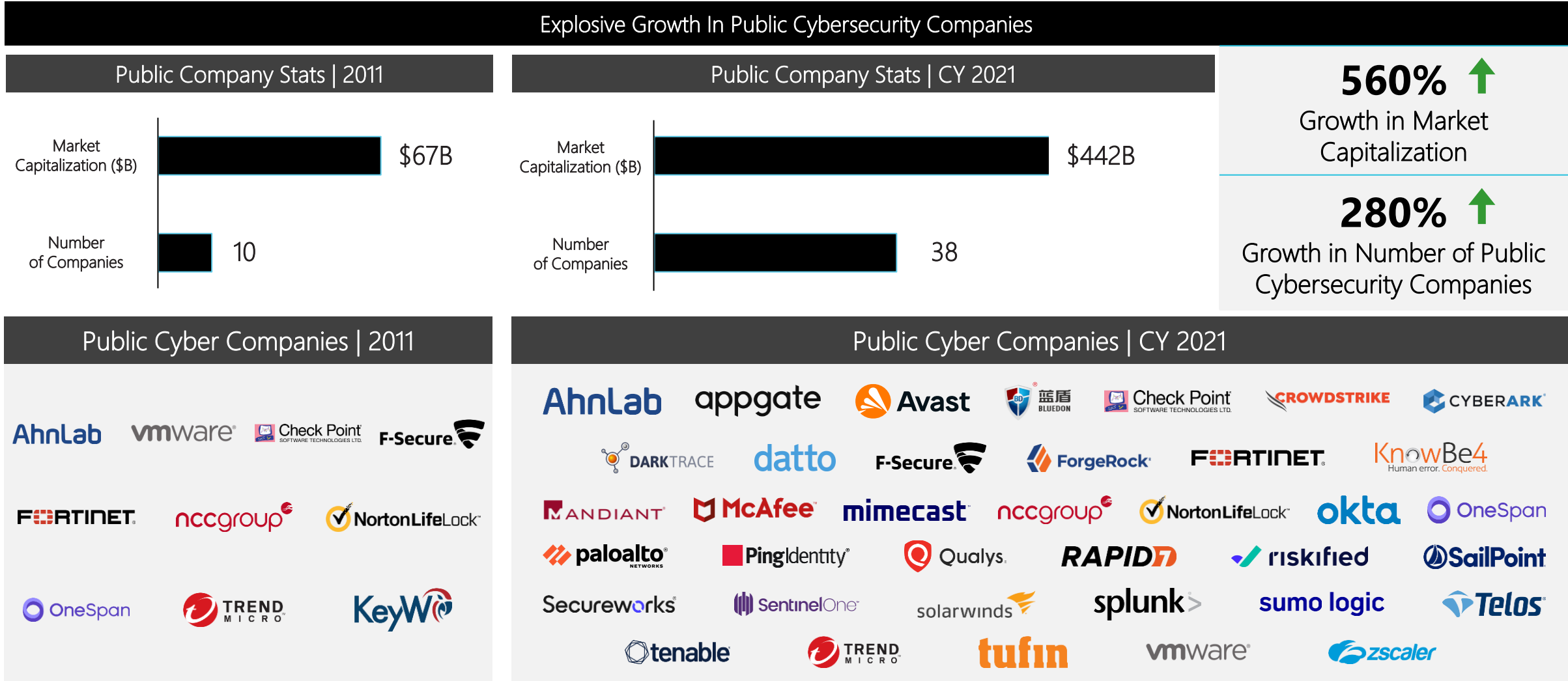
Cybersecurity vs. The Benchmarks

Cybersecurity Stocks Have Exceeded Broader Market Benchmarks.



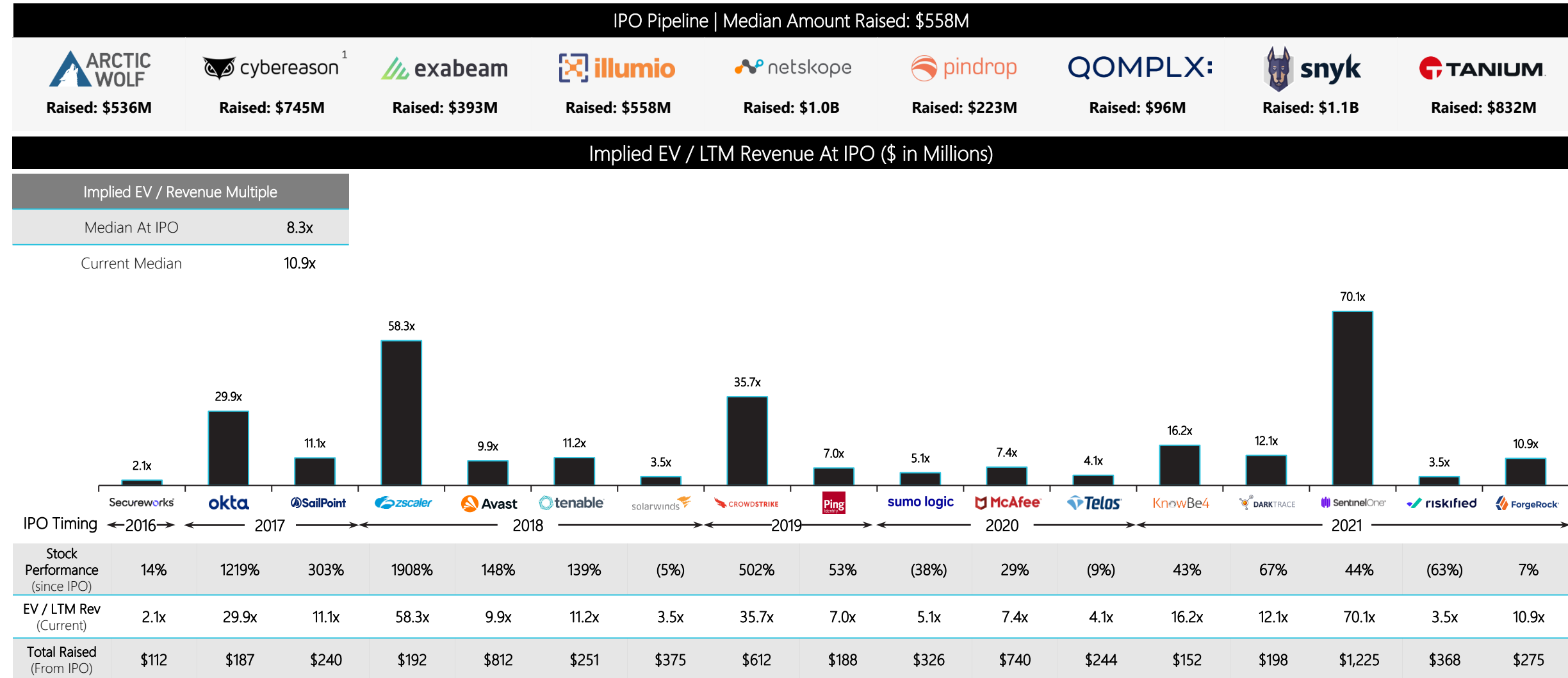
Significant Growth in Public Cyber Companies | 2011 – CY 2021

Aggregate Market Capitalization For Cybersecurity Has Grown Considerably Over The Last Decade.



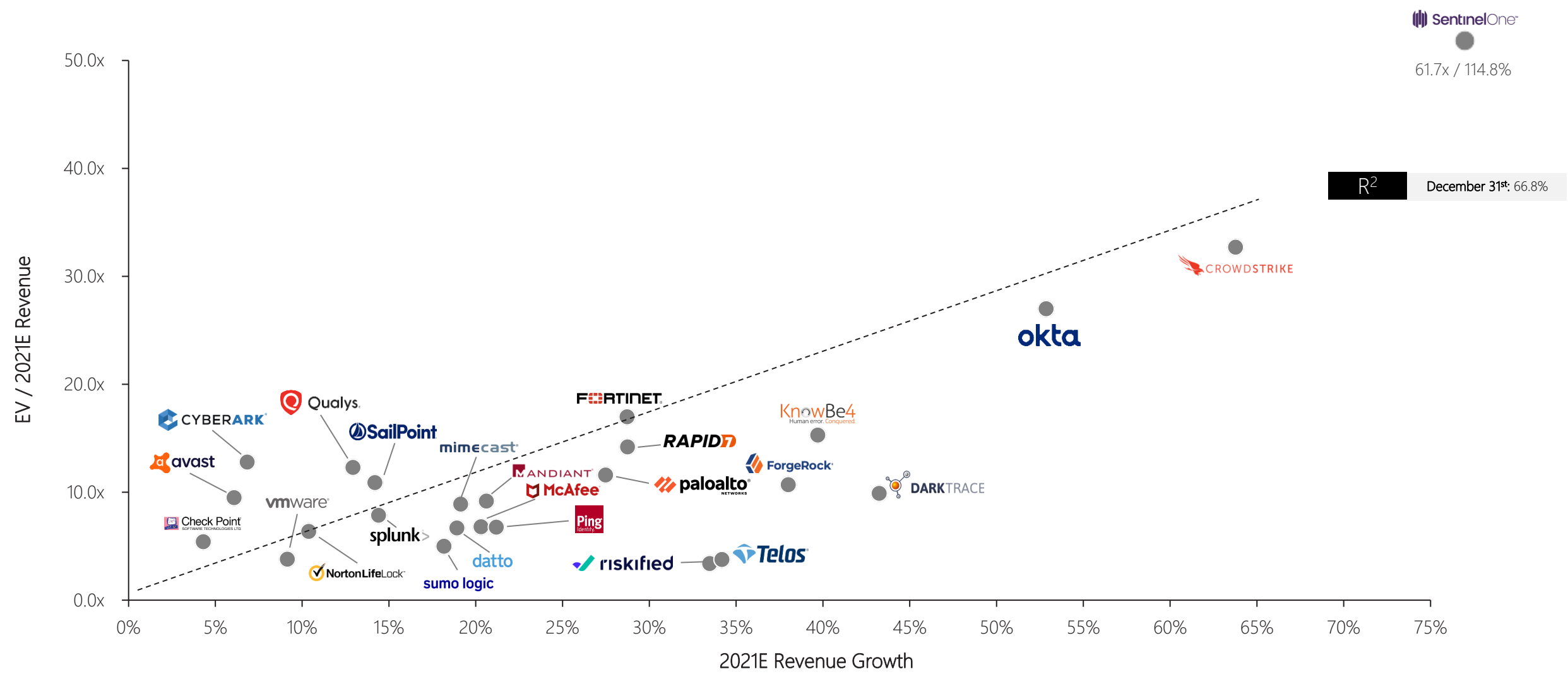
Cybersecurity IPO Insights

Several High-Potential IPO Candidates Remain, But The Rate Of Public Filings Or SPAC Mergers Is Accelerating Across Cyber.



Revenue Growth Is Correlated To Value...

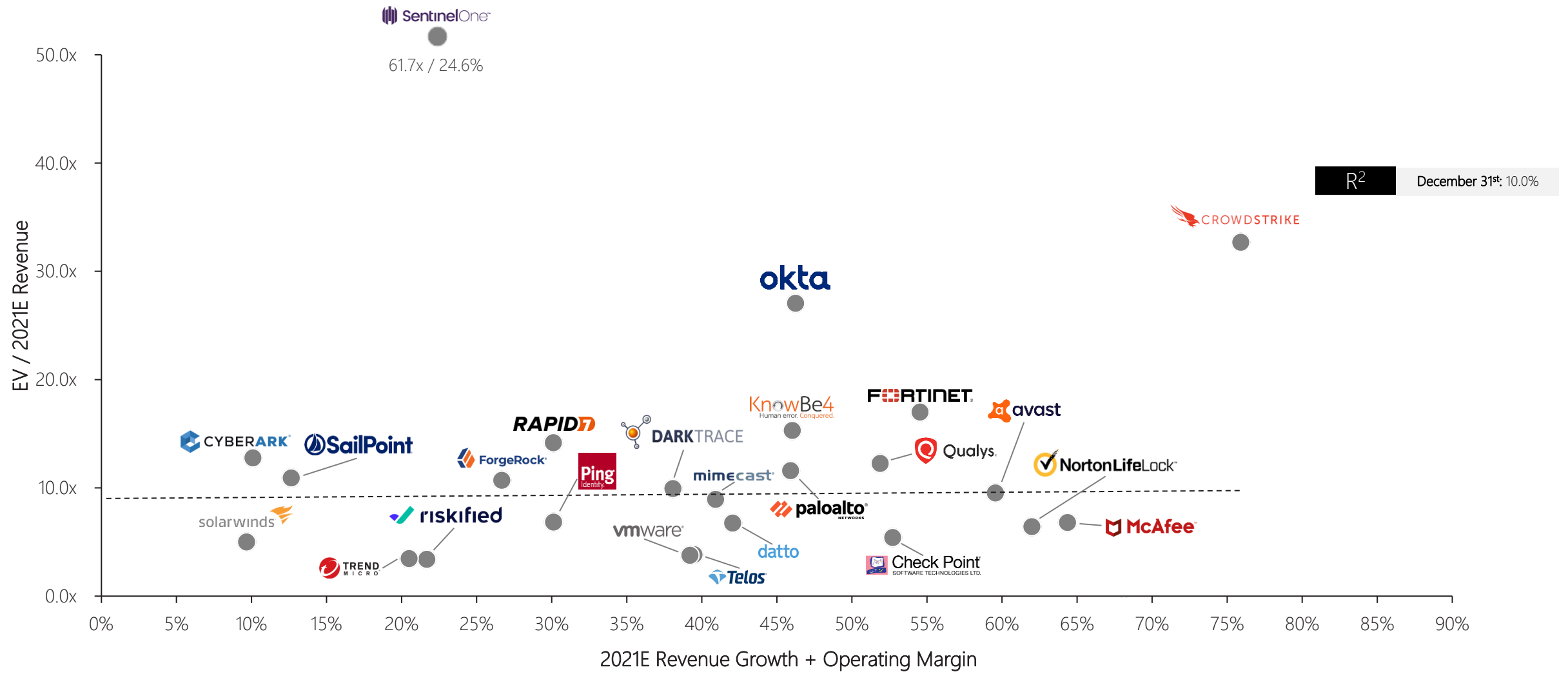
Public Markets Today Are Focused On Growth.



Source: Capital IQ. Public Market Data as of December 31st, 2021. Using Latest Spot Exchange Rate. Trend Micro, Tenable, SolarWinds, and SecureWorks have been excluded from the output.










...While The Correlation To Growth and Profitability Is Much Weaker

Public Markets Today Are Focused On Growth.



The Current IPO Pipeline | 2022

The Current Backlog Of Well-Funded Companies Positions 1H 2022 As Another Active Half For Cybersecurity IPOs.

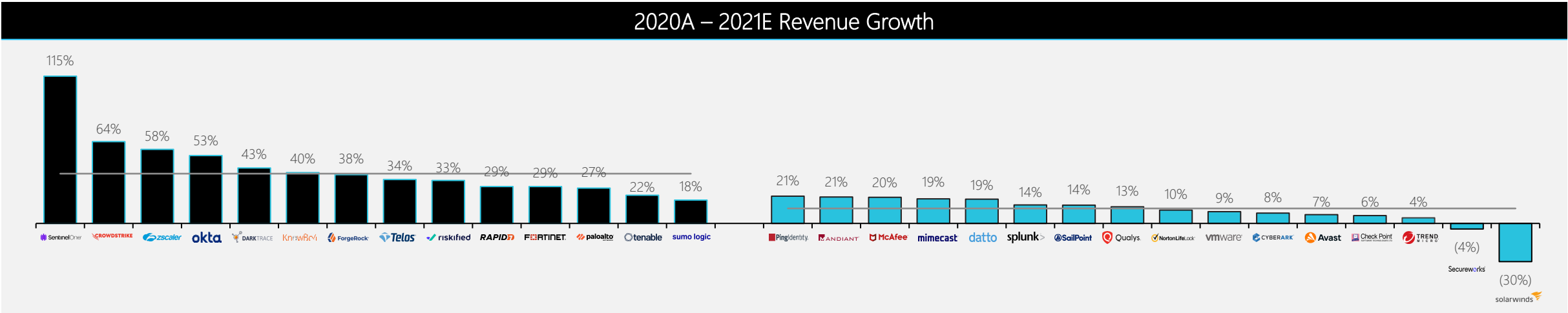
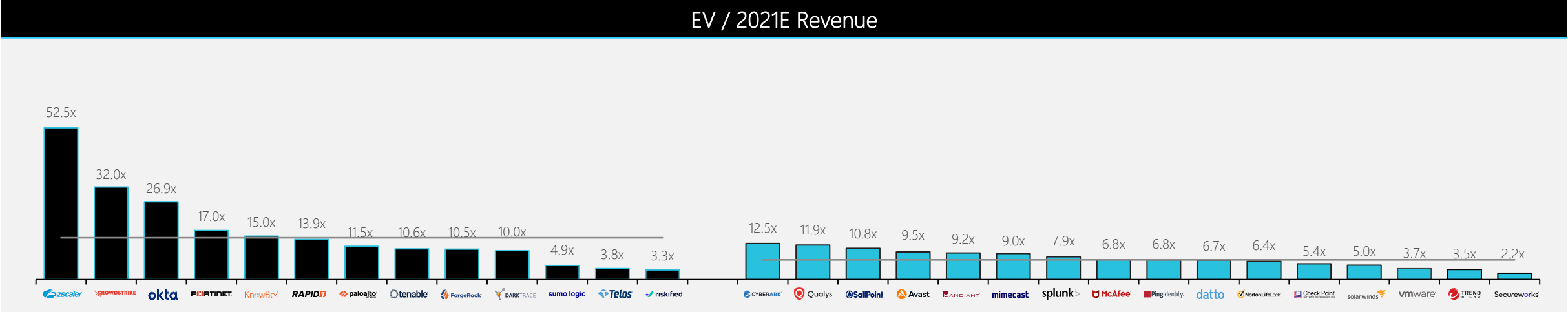
2022 IPO Watchlist									
Company	Sector	Founded	Location	CEO	Select Investors			Raised To Date	Select Public Competitors
 ARCTIC WOLF	MSSP	2012	Eden Prairie, Minnesota	Nick Schneider	DTCP	OWL ROCK	Viking	\$536M	RAPID7 red canary SentinelOne
 cybereason ¹	Endpoint Security	2012	Boston, MA	Lior Div	IRVING INVESTORS	Liberty Strategic Capital	NEUBERGER BERMAN	\$745M	CROWDSTRIKE BlackBerry
 exabeam	SecOps & Incident Response	2013	San Mateo, CA	Nir Polak	cisco investments	Lightspeed	SAPPHIRE VENTURES	\$393M	MICRO FOCUS solarwinds splunk
 illumio	Cloud Security	2013	Sunnyvale, CA	Andrew Rubin	Accel	ANDREESSEN HOROWITZ	GENERAL CATALYST	\$558M	Check Point paloalto zscaler
 netskope	Cloud Security	2012	Santa Clara, CA	Sanjay Beri	Accel	Lightspeed	SEQUOIA	\$1.0B	Check Point paloalto zscaler
 pindrop	Identity & Access Management	2011	Atlanta, GA	Vijay Balasubramaniyan	ANDREESSEN HOROWITZ	BlackRock	J.P.Morgan	\$223M	okta SailPoint Ping
 QOMPLX	Risk & Compliance	2014	Tysons, VA	Jason Crabtree	exponential	Fidelity		\$96M	tenable FORTINET
 snyk	Application Security	2015	Boston, MA	Peter McKay	Accel	SANDS CAPITAL	TIGERGLOBAL	\$1.1B	GitHub VERACODE WhiteSource
 TANIUM	Endpoint Security	2007	Emeryville, CA	Orion Hindawi	ANDREESSEN HOROWITZ	TPG	WELLINGTON MANAGEMENT	\$832M	CROWDSTRIKE BlackBerry

Source: Capital IQ. Amount raised to date as of December 31st, 2021.
1 – Cybereason has confidentially filed an IPO.

[Return To Table Of Contents](#)

2021E Trading Multiples: High Growth & Low Growth

Valuation Multiples For High Growth & Low Growth Cybersecurity Companies.



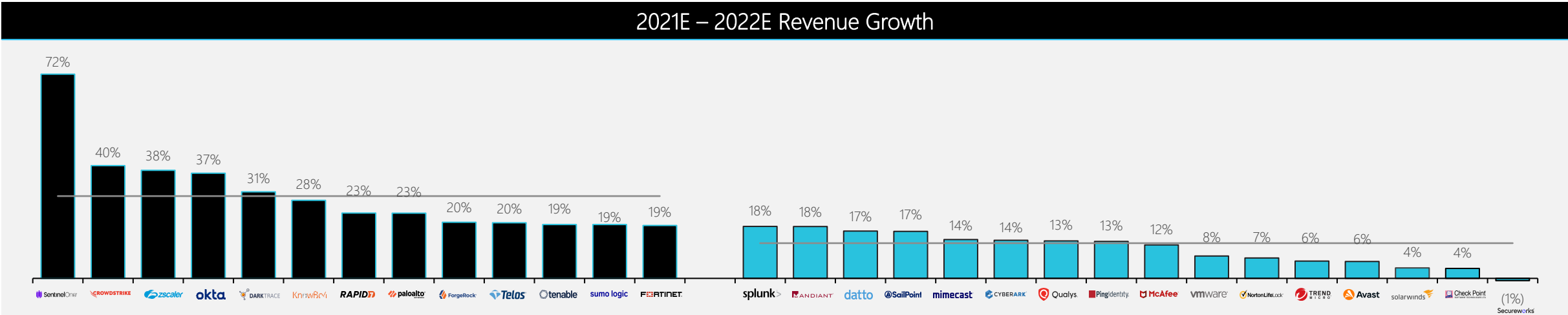
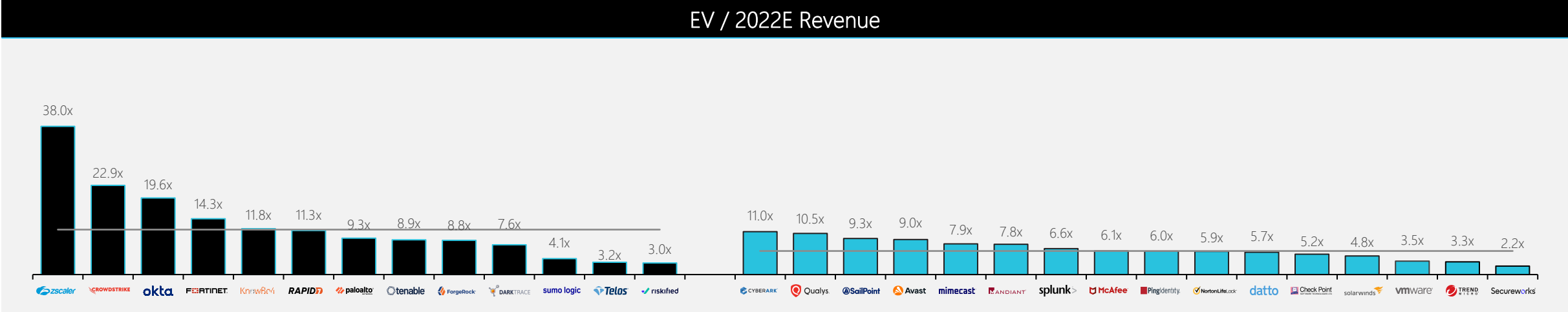
■ High Growth ■ Low Growth



Source: Capital IQ. Public Market data as of December 31st, 2021.
Note: High Growth represented by companies with >20% revenue CAGR; Low Growth represented by companies with <20% revenue CAGR.

2022E Trading Multiples: High Growth & Low Growth

Valuation Multiples For High Growth & Low Growth Cybersecurity Companies.

















High Growth Low Growth



Source: Capital IQ. Public Market data as of December 31st, 2021.
Note: High Growth represented by companies with >20% revenue CAGR; Low Growth represented by companies with <20% revenue CAGR.

Public Company Trading Analysis

High-Growth Cybersecurity Comps (\$ In Millions Excl. Stock Price).

Company	Stock Price	LTM Price Performance	Market Cap	Enterprise Value	Revenue Growth			EV / Revenue			EV / EBITDA		
					LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E
High-Growth Cybersecurity (>20% 2019A – 2022E CAGR)													
 FORTINET	\$359.40	147%	\$58,762	\$56,729	21%	29%	19%	18.1x	17.0x	14.3x	NM	NM	NM
 paloalto	\$556.76	59%	\$54,934	\$55,444	27%	27%	23%	12.2x	11.5x	9.3x	NM	NM	NM
 CROWDSTRIKE	\$204.75	(2%)	\$46,957	\$45,838	69%	64%	40%	35.7x	32.0x	22.9x	NM	NM	NM
 zscaler	\$321.33	62%	\$45,012	\$44,406	58%	58%	38%	58.3x	52.5x	38.0x	NM	NM	NM
 okta	\$224.17	(12%)	\$34,868	\$34,403	50%	53%	37%	29.9x	26.9x	19.6x	NM	NM	NM
 SentinelOne *	\$50.49	19%	\$13,476	\$11,841	264%	115%	72%	NM	NM	NM	NM	NM	NM
 RAPID7	\$117.69	33%	\$6,728	\$7,358	21%	29%	23%	14.8x	13.9x	11.3x	NM	NM	NM
 tenable	\$55.07	6%	\$5,917	\$5,692	16%	22%	19%	11.2x	10.6x	8.9x	NM	NM	NM
 KnowBe4 *	\$22.94	(6%)	\$3,931	\$3,672	29%	40%	26%	16.2x	15.0x	11.9x	NM	NM	NM
 DARKTRACE *	\$5.69	23%	\$3,652	\$3,350	20%	43%	31%	11.9x	10.0x	7.6x	NM	NM	NM
 ForgeRock *	\$26.69	(25%)	\$2,186	\$1,852	33%	38%	20%	10.9x	10.5x	8.8x	NM	NM	NM
 sumo logic	\$13.56	(52%)	\$1,519	\$1,165	19%	18%	19%	5.1x	4.9x	4.1x	NM	NM	NM
 riskified *	\$7.86	(71%)	\$1,284	\$755	27%	33%	12%	3.5x	3.3x	3.0x	NM	NM	NM
 Telos	\$15.42	(53%)	\$1,029	\$911	24%	34%	20%	4.1x	3.8x	3.2x	NM	NM	NM
				Mean	48%	43%	29%	17.8x	16.3x	12.5x	NM	NM	NM
				Median	27%	36%	23%	12.2x	11.5x	9.3x	NM	NM	NM

Source: Capital IQ. Market data updated as of December 31st, 2021














Note: NM – Not Meaningful, NA – Not Available; analysis only includes companies with an enterprise value greater than \$1B.

* Stock price performance from IPO price.

[Return To Table Of Contents](#)




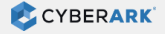






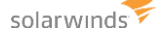


Public Company Trading Analysis | Operating Metrics

High-Growth Cybersecurity Comps.

Company	Revenue			Revenue Growth			EBITDA			EBITDA Margin		
	LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E
High-Growth Cybersecurity (>20% 2019A – 2022E CAGR)												
 FORTINET	\$3,127	\$3,339	\$3,966	20.5%	28.7%	18.8%	\$676	\$947	\$1,101	21.6%	28.3%	27.8%
 paloalto	\$4,558	\$4,822	\$5,936	27.2%	27.5%	23.1%	(\$86)	\$1,123	\$1,359	(1.9%)	23.3%	22.9%
 CROWDSTRIKE	\$1,286	\$1,432	\$2,004	68.8%	63.8%	40.0%	(\$78)	\$237	\$334	(6.1%)	16.6%	16.6%
 zscaler	\$761	\$845	\$1,169	58.5%	57.7%	38.3%	(\$213)	\$122	\$166	(28.0%)	14.4%	14.2%
 okta	\$1,152	\$1,277	\$1,753	50.0%	52.9%	37.3%	(\$467)	(\$38)	(\$27)	(40.5%)	(3.0%)	(1.5%)
 SentinelOne	\$169	\$200	\$345	263.7%	114.8%	72.4%	(\$226)	(\$163)	(\$163)	(133.8%)	(81.7%)	(47.2%)
 RAPID7	\$497	\$530	\$652	20.8%	28.7%	23.1%	(\$62)	\$25	\$50	(12.5%)	4.8%	7.7%
 tenable	\$510	\$537	\$639	15.9%	21.9%	19.1%	(\$10)	\$59	\$75	(1.9%)	11.0%	11.7%
 KnowBe4	\$226	\$244	\$312	29.4%	39.7%	27.7%	(\$8)	\$29	\$39	(3.4%)	11.8%	12.4%
 DARKTRACE	\$281	\$336	\$439	20.0%	43.2%	30.7%	(\$5)	\$17	\$14	(1.7%)	5.1%	3.1%
 ForgeRock	\$169	\$176	\$211	32.5%	38.0%	19.9%	(\$18)	(\$19)	(\$18)	(10.9%)	(10.7%)	(8.7%)
 sumo logic	\$229	\$239	\$285	18.9%	18.2%	19.1%	(\$103)	(\$44)	(\$48)	(44.9%)	(18.5%)	(16.9%)
 riskified	\$216	\$227	\$254	27.5%	33.5%	11.9%	(\$18)	(\$25)	(\$60)	(8.4%)	(10.9%)	(23.5%)
 Telos	\$223	\$241	\$289	24.1%	34.2%	19.7%	(\$42)	\$18	\$27	(18.7%)	7.6%	9.4%

Public Company Trading Analysis

Low-Growth Cybersecurity Comps (\$ In Millions Excl. Stock Price).

Company	Stock Price	LTM Price Performance	Market Cap	Enterprise Value	Revenue Growth			EV / Revenue			EV / EBITDA		
					LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E
Low-Growth Cybersecurity (<20% 2019A – 2022E CAGR)													
 vmware	\$115.88	(16%)	\$48,712	\$47,909	9%	9%	8%	3.8x	3.7x	3.5x	15.8x	10.0x	9.6x
 splunk	\$115.72	(32%)	\$18,375	\$20,068	11%	14%	18%	8.0x	7.9x	6.6x	NM	NM	NM
 Check Point	\$116.56	(11%)	\$15,479	\$11,673	3%	4%	4%	5.5x	5.4x	5.2x	12.5x	11.0x	10.8x
 NortonLifeLock	\$25.98	27%	\$15,117	\$17,536	9%	10%	7%	6.5x	6.4x	5.9x	13.8x	12.0x	11.5x
 Avast	\$8.22	12%	\$8,529	\$9,040	4%	6%	6%	9.7x	9.5x	9.0x	18.7x	17.4x	16.4x
 TREND MICRO	\$55.50	(2%)	\$7,748	\$5,664	(1%)	(3%)	6%	3.4x	3.5x	3.3x	9.5x	10.3x	10.3x
 CYBERARK	\$173.28	8%	\$6,890	\$6,197	7%	7%	14%	12.5x	12.5x	11.0x	NM	NM	NM
 Qualys	\$137.22	16%	\$5,327	\$4,895	9%	13%	13%	12.4x	11.9x	10.5x	41.2x	25.8x	24.5x
 mimecast	\$79.57	40%	\$5,302	\$5,146	15%	19%	14%	9.3x	9.0x	7.9x	54.7x	32.1x	28.7x
 McAfee ¹	\$25.79	54%	\$4,717	\$12,755	11%	20%	12%	7.4x	6.8x	6.1x	19.6x	15.3x	13.2x
 SailPoint	\$48.34	(9%)	\$4,508	\$4,506	11%	14%	17%	11.1x	10.8x	9.3x	NM	NM	NM
 datto	\$26.35	(2%)	\$4,297	\$4,131	14%	19%	17%	7.0x	6.7x	5.7x	37.4x	23.5x	22.8x
 MANDIANT ²	\$17.54	(24%)	\$4,178	\$4,426	21%	21%	18%	10.3x	9.2x	7.8x	NM	NM	NM
 solarwinds	\$14.19	(52%)	\$2,257	\$3,542	0%	(30%)	4%	3.5x	5.0x	4.8x	21.2x	11.8x	11.6x
 Ping	\$22.88	(20%)	\$1,912	\$1,999	18%	21%	13%	7.0x	6.8x	6.0x	NM	NM	51.6x
 Secureworks	\$15.97	12%	\$1,345	\$1,164	(3%)	(4%)	(1%)	2.1x	2.2x	2.2x	NM	NM	NM
Mean					9%	9%	11%	7.7x	7.6x	6.8x	25.4x	17.7x	20.2x
Median					9%	13%	13%	7.4x	6.8x	6.1x	19.6x	14.9x	14.8x

Source: Capital IQ. Market data updated as of December 31st, 2021














Note: NM – Not Meaningful, NA – Not Available; analysis only includes companies with an enterprise Value greater than \$1B.

* Price performance from IPO price; ¹ Pro forma for the divestiture of McAfee's Enterprise business to Symphony Technology Group; ² Pro forma for divestiture of FireEye's Products business to Symphony Technology Group

[Return To Table Of Contents](#)

Public Company Trading Analysis | Operating Metrics

Low-Growth Cybersecurity Comps.

Company	Revenue			Revenue Growth			EBITDA			EBITDA Margin		
	LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E	LTM	CY 2021E	CY 2022E
Low-Growth Cybersecurity (<20% 2019A – 2022E CAGR)												
 vmware	\$12,614	\$12,843	\$13,860	9.2%	9.1%	7.9%	\$3,034	\$4,806	\$5,013	24.1%	37.4%	36.2%
 splunk >	\$2,518	\$2,550	\$3,020	10.6%	14.4%	18.4%	(\$987)	(\$287)	(\$112)	(39.2%)	(11.3%)	(3.7%)
 Check Point <small>SOFTWARE TECHNOLOGIES LTD.</small>	\$2,132	\$2,154	\$2,230	3.2%	4.3%	3.5%	\$935	\$1,061	\$1,077	43.9%	49.3%	48.3%
 NortonLifeLock	\$2,689	\$2,752	\$2,950	8.8%	10.4%	7.2%	\$1,275	\$1,461	\$1,531	47.4%	53.1%	51.9%
 Avast	\$931	\$947	\$1,004	4.3%	6.1%	6.0%	\$482	\$521	\$553	51.8%	55.0%	55.0%
 TREND MICRO	\$1,632	\$1,634	\$1,734	(1.0%)	(3.1%)	6.1%	\$586	\$548	\$548	35.9%	33.6%	31.6%
 CYBERARK	\$496	\$496	\$563	6.8%	6.8%	13.5%	(\$30)	\$31	\$4	(6.0%)	6.2%	0.6%
 Qualys	\$396	\$410	\$464	9.2%	12.9%	13.3%	\$119	\$189	\$200	30.0%	46.2%	43.0%
 mimecast	\$553	\$574	\$653	14.9%	19.1%	13.8%	\$94	\$160	\$179	17.0%	27.9%	27.4%
 McAfee ¹	\$1,730	\$1,874	\$2,096	11.0%	20.3%	11.8%	\$652	\$854	\$963	37.7%	45.6%	46.0%
 SailPoint	\$407	\$417	\$487	11.3%	14.2%	16.7%	(\$25)	\$9	\$1	(6.1%)	2.2%	0.3%
 datto	\$593	\$617	\$720	14.4%	18.9%	16.8%	\$110	\$176	\$181	18.6%	28.5%	25.1%
 MANDIANT ²	\$428	\$482	\$571	20.6%	20.6%	18.4%	(\$73)	(\$47)	(\$60)	(17.1%)	(9.7%)	(10.5%)
 solarwinds	\$1,020	\$715	\$741	0.1%	(29.9%)	3.7%	\$167	\$300	\$305	16.4%	42.0%	41.1%
 Ping	\$287	\$295	\$334	17.9%	21.2%	13.1%	(\$39)	\$30	\$39	(13.4%)	10.1%	11.6%
 Secureworks	\$547	\$537	\$532	(2.9%)	(4.4%)	(0.8%)	(\$11)	\$10	(\$3)	(2.0%)	1.9%	(0.6%)

Source: Capital IQ.

Note: NM – Not Meaningful, NA – Not Available.

¹ Pro forma for the divestiture of McAfee's Enterprise business to Symphony Technology Group; ² Pro forma for divestiture of FireEye's Products business to Symphony Technology Group

[Return To Table Of Contents](#)



VII.

CYBERSECURITY INDUSTRY PERSPECTIVES

Developers Take Center Stage

A Look At The Shift-Left Of Security



What Is Shift Left DevOps?

DeveOps Teams Are Incorporating Security At Early Stages In The Development Lifecycle.

What is Shift Left DevOps?

The term “**shift left**” refers to the efforts of a DevOps team to **guarantee application security** at the **earliest** stages in the **development lifecycle**, as part of an organizational pattern known as DevSecOps (collaboration between **development**, **security**, and **operations**).

Important Reasons to Shift Left

More code gets tested during the DevOps process

- Bringing security forward in the SDLC increases opportunities for code to be scanned and threats to be remediated
- By automating (SAST) at every code commit, for example, can ensure that all code has been scanned at least once

Planning becomes more well-rounded

- Bring a security DRI into initial planning meetings ensures accounting for security needs in all stages of the SDLC
- Helps to streamline end-of-cycle security reviews, reduces friction between teams, and accelerates Speed-to-Market

Better accountability among non-security team members

- The entire team is expected to take security seriously and make it a part of their daily work
- Integrated security into every job function results in less threats across the entire digital landscape

Key Benefits

Shift Left

=



Faster Delivery



Improved Security Posture



Reduced Costs



Improved Security Integration



Greater Business Success

Shift Left: Supporting Stats

6x

Cheaper to address security issues during the design process

42%

Of developers said testing happens too late in the development lifecycle

1/4

Of developers think their organizations have “good” security practices

60%

Of security teams do not run Static AST scans at all within the design process

Getting Started with Shift Left Testing

1

Implement Security Policies


2

Integrate testing early in the SDLC


3

Embrace security automation


Tips for Efficient Shift Left DevOps




Look for patterns in the type or source of vulnerabilities and adjust for improvement.




Make small code changes. Smaller updates are easier to review and secure.




Build security scans into the developer’s workflow.



Reduce or eliminate any waterfall-style security processes within your SDLC.



Give the security team visibility into both resolved and unresolved vulnerabilities.



Streamline your toolchain so that employees can focus their attention on a single interface.

Security's Shift-Left

High Level Coverage Of How The Security Market Is Focusing More On Developers' Needs.

Application Security Testing (AST)



Overview

- Process of **discovering and fixing application vulnerabilities throughout the development lifecycle (DLC)** to protect applications against potential threats
- AST tools service various vectors including **cloud, IoT, networks, mobile applications, and critical infrastructure**
- **Large variation in vendor offerings** depending on which stage of the DLC they target and which application platforms they support



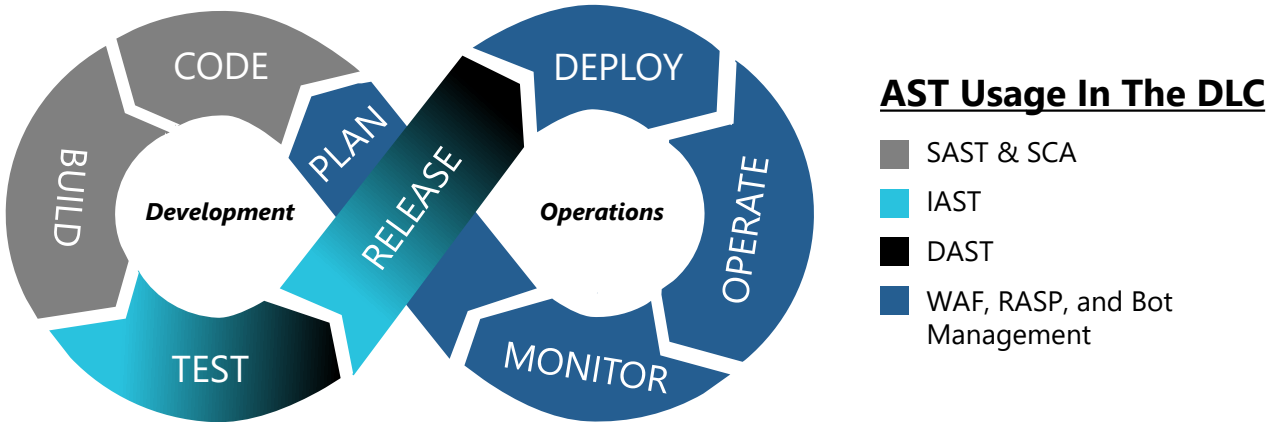
Tools Offered

Security Scanning Tools	Runtime Protection Tools
<ul style="list-style-type: none">▪ Software Composition Analysis (SCA)▪ Static AST (SAST)▪ Interactive AST (IAST)▪ Dynamic AST (DAST)	<ul style="list-style-type: none">▪ Web Application Firewall (WAF)▪ Bot Management▪ Runtime Application Self-Protection (RASP)



Looking Ahead

- **Strong growth is expected to continue over the next 12 months** as evident by growing user needs, new entrants, transaction activity, and investment dollars
- **Vendors should move towards delivering testing capabilities across the DLC** as customers are leaning towards fulfilling their AST needs through a single vendor
- Many vendors are adding in **developer enablement and education tools** to their platforms



	Static AST (SAST)	Interactive AST (IAST)	Dynamic AST (DAST)
Overview	Developer-approach testing that checks source code from the inside	QA-approach testing that is triggered by human or automated app interactions	Hacker-approach testing that simulates real-life attacks from the outside
App Status	Application is stopped	Application is running	Application is running
Type	Proactive	Reactive	Proactive
Pros	<ul style="list-style-type: none">▪ Comprehensive analysis▪ Promotes secure coding	<ul style="list-style-type: none">▪ Real-time analysis▪ Low false positive rate	<ul style="list-style-type: none">▪ Language independent▪ Low false positive rate
Cons	<ul style="list-style-type: none">▪ High false positive rate▪ No real-time analysis	<ul style="list-style-type: none">▪ Limited language scope▪ Slows app performance	<ul style="list-style-type: none">▪ Needs test environment▪ No real-time analysis

Incorporating Product-Led Growth In Go-To-Market Strategies

Snyk Is A Good Case Study Of How Using Product-Led Growth Principles Can Help Scale Businesses.

Product-Led Growth Is Becoming An Increasingly Important GTM Strategy

Catering directly to the needs of developers, rather than competing for approval from executives, is the most important factor for many go-to-market strategies. In order to strengthen their GTM campaigns, companies can consider incorporating Product-Led Growth (PLG) principles. PLG, a term coined by OpenView Partners, focuses on using the product as the main driver of acquiring and retaining customers.

Product-Led Growth Model			
1	2	3	4
Companies build and distribute products directly to developers – the end users	Good products gain popularity in tightknit developer communities through word-of-mouth	Developer trust and adoption grows, creating a use case for executives with purchasing power	Software purchases are more likely to be approved, leading to more paying accounts

Product-Led Growth Principles, by OpenView Partners

1. Design For The End User	2. Deliver Value Before Capturing Value	3. Invest In The Product With Go-To-Market Intent
Listen to the user	Put the product first	Invest in product data
Personalize where possible	Deliver value quickly	Build a growth team
Build a culture of continuous, rapid improvement	Introduce customer success before sales	Run experiments

Company Spotlight: snyk Is Successfully Executing A PLG Model



Peter McKay
CEO



Guy Podjarny
Founder & President



Ken MacAskill
CFO

Year Founded:
HQ:
Total Raised:
Select Investors:

2015
Boston, MA
\$1.11B
Accel SANDS CAPITAL TIGERGLOBAL

What Is snyk?

Developer security platform that integrates directly into development tools, workflows, and automation pipelines

Supported by industry-leading application and security intelligence

Makes it easy for teams to find and fix security vulnerabilities in code, dependencies, containers, and infrastructure as code

PLG Model In Action

- Currently has a community of 2.2M developers using the products
- Leverages the developer community to receive live feedback which then results in subsequent product enhancements
- Growth has compounded exponentially, as evidenced by its recent capital raises and \$8.5B valuation

The Year Of Industrial Cybersecurity

Sector Analysis | Overview, Trends,
& Capital Markets Activity Across
ICS + OT



A New Wave Of Threats To Industrial Devices

Enterprises Of All Sizes Are Demanding A Different Approach To Industrial Security As Threats Increase.

Key ICS + OT Challenges

- > Need To Overcome Cultural & Technical Differences Between IT & OT Teams
- > Effectively Integrate Technical Implementations With Legacy OT Environments
- > Face A Worsening OT Labor Shortage Crisis

Gartner

“

By 2025, **75%** of OT security solutions will be delivered via multifunction platforms interoperable with IT security solutions

ICS + OT Market Trends In 2021

Increasing Attacks On Infrastructure



2021 saw several high-profile attacks on critical infrastructure impacting industrial operations including Colonial Pipeline and JBS Foods, with no end in sight to attacks as more devices go online

Convergence Of OT & IT As More Companies Connect ICS Devices



IT and OT environments are quickly becoming intertwined, with visibility into network assets becoming an absolute necessity to protect against threats and prevent software and firmware vulnerabilities

Emergence Of Vertical-Specific ICS + OT Vendors



Vendors are recognizing that certain verticals like healthcare, defense, and the transportation industries often have specialized needs and are catering their services to these unique environments

Highlighted Need For Multi-Functional Platforms In A Growing Sector










Vendors are increasingly expected to offer users a multitude of features including threat intelligence, vulnerability management, risk analysis, and more across their entire environments










Key ICS + OT Sector Activity

ICS + OT Companies Of All Sizes Are Benefiting From Increased Sector Activity.

ICS + OT M&A Activity

Date	Target	Acquirer	Enterprise Value (\$M)	Target HQ
11/24/21	 Applied Risk	 DNV	ND	Amsterdam, Netherlands
07/19/21	 BAYSHORE	OPSWAT.	ND	Durham, NC
06/22/20	CYBERX	 Microsoft	\$165	Waltham, MA
02/06/20	 FORESCOUT	 Advent International  Crosspoint Capital Partners	\$1,625	San Jose, CA

ICS + OT Financing Activity

Date	Company	Deal Type	Amount Raised (\$M)	Total Amount Raised (\$M)	HQ	Select Investors
12/08/21	CLAROTY	Series E	\$400	\$640	New York, NY	 SE VENTURES  SoftBank
12/06/21	 NOZOMI NETWORKS	Series D	\$100	\$154	San Francisco, CA	 Honeywell  Triangle Peak
10/28/21	DRAGOS	Series D	\$200	\$358	Hanover, MD	 BlackRock  KOCH
06/15/21	CLAROTY	Series D	\$140	\$240	New York, NY	 40north ventures  Bessemer Venture Partners

Key Stats

\$1.6^B

Amount of capital raised across the ICS + OT space since January 2019

\$1.0^B

Amount of capital raised across ICS + OT in 2021 alone

29

Financing Raises in 2021 across ICS + OT

Sector Unicorn Spotlights

DRAGOS

Delivers a software platform that collects, detects, and automates asset inventorying and visualization, and detects threats through behavioral analytics, security operations, and incident response workflows.

\$1.7B
Valuation

\$358M
Total Raised

2016
Founded

CLAROTY

Offers a unified platform that integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

\$2.0B
Valuation

\$640M
Total Raised

2014
Founded

Industry Perspectives



Log4j Exploit

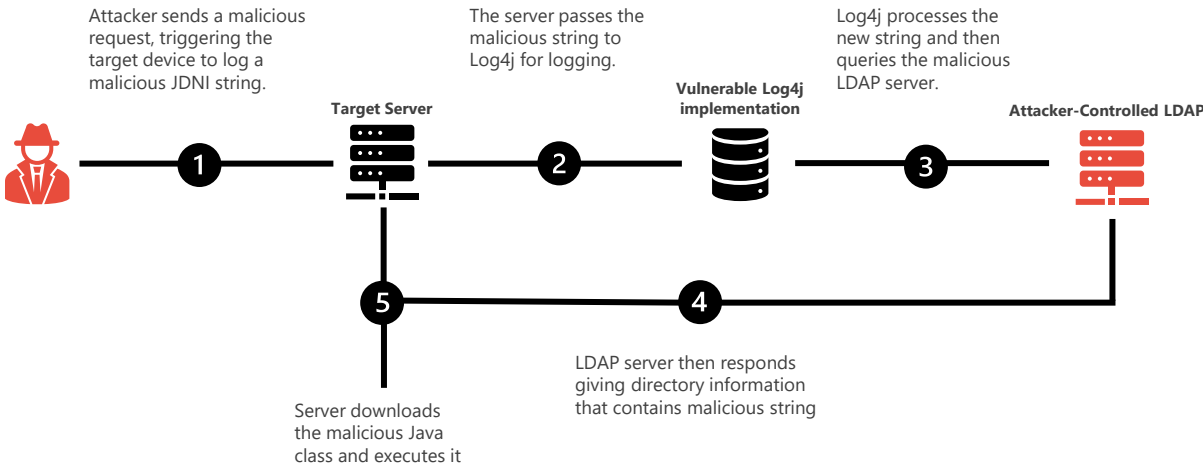
Critical Vulnerabilities Leave The Security Community Scrambling In “Apocalyptic” Flaw Discovery.



On December 9th, 2021, a zero-day vulnerability was publicly disclosed in Log4j, a Java-based data logging utility that allows requests to arbitrary Lightweight Directory Access Protocol (LDAP) and Java Naming and Directory Interface (JNDI) servers. The vulnerability enables hackers to remotely execute code and gain access to machines, potentially affecting hundreds of millions of devices.

Because Log4j is so widely used, the vulnerability could impact a wide range of software and services from many major vendors. Organizations with products known to be vulnerable include Atlassian, Amazon, Microsoft Azure, Cisco, Commvault, ESRI, Exact, Fortinet, JetBrains, Nelson, Nutanix, OpenMRS, Oracle, Red Hat, Splunk, Soft, and VMware.

Exploit Overview



Global Response & Key Stats



Apache Software Foundation released a new version 2.15.0 to address the flaw, but companies will still need to update devices, along with downstream customers.



Threat actors have already begun to target affected devices, with malicious activity appearing in Iran, China, and elsewhere.



While patches are being developed, attackers are expected to have months if not years to find and exploit vulnerable devices.

~40%

Of corporate networks have been targeted by the exploit

10M+

Attempts to exploit the Log4j vulnerability every hour

100M+

potentially affected devices

Expert Commentary



“ We will only minimize potential impacts through collaborative efforts between government and the private sector. We urge all organizations to join us in this essential effort and take action.”
- Jen Easterly, Director - CISA



“ I cannot overstate the seriousness of this threat. On the face of it, this is aimed at crypto-miners but we believe this creates just the sort of background noise that serious threat actors will try to exploit in order to attack a whole range of high-value targets such as banks, state security and critical infrastructure.”
- Lotem Finkelstein, Director of Threat Intelligence & Research – Check Point

NSO Group's Pegasus Exploit And Zero-Click Attacks

Zero-Click Exploitation Technique Presents An Alarming New Attack Vector In Cybersecurity.

Exploit Overview

Pegasus, a spyware developed by Israeli Cybersecurity company NSO, has recently come under fire for offering "zero-click exploitation technology" called ForcedEntry which allows attackers to exploit devices with no user interaction required. Researchers at Google Project Zero recently provided a deep dive into the exploit and its many potential effects on users



Attack targets users through iMessage, where a PDF file disguised as a fake GIF image is sent to a user with malicious code



This malicious code then executes a breach on a user's phone without any input from the victim, with the code hidden on a pixel-level



The attacker can gain full control of a victim's phone after sending the message to a helpless target



While one-click exploits are common, zero-click exploits are a new threat posing a dangerous threat

Industry Commentary

“ Based on our research and findings, we assess this to be one of the most technically sophisticated exploits we've ever seen, further demonstrating that the capabilities NSO provides rival those previously thought to be accessible to only a handful of nation states.”

- Ian Beer & Samuel Groß – Google Project Zero



“ It's really sophisticated stuff, and when it's wielded by an all-gas, no-brakes autocrat, it's totally terrifying. And it just makes you wonder what else is out there being used right now that is just waiting to be discovered. If this is the kind of threat civil society is facing, it is truly an emergency.”

- John Scott-Railton, Researcher – Citizen Lab

Key Takeaways



A Dangerous Precedent

Exploits continue to advance in terms of technical ability and clever intrusion techniques. While users should always practice good Cyber hygiene practices, zero-click exploitation represents a dangerous precedent in a potential rise of attacks for which social engineering techniques are unnecessary.



Not Just NSO

While NSO's exploit was discovered publicly, many companies are developing similarly destructive offensive exploitation techniques unbeknownst to the public. While NSO has been admonished for its history of providing spyware products to foreign nation-states and potential threat actors, they are far from the only threat.



What About Defense?

Zero-click exploitation techniques are able to set up their own virtualized environments and run javascript-like code, with no need to connect to an outside server once inside a device, giving attackers access to user data, passwords and more. Extremely hard to detect, researchers call it “a weapon against which there is no defense” at the moment.

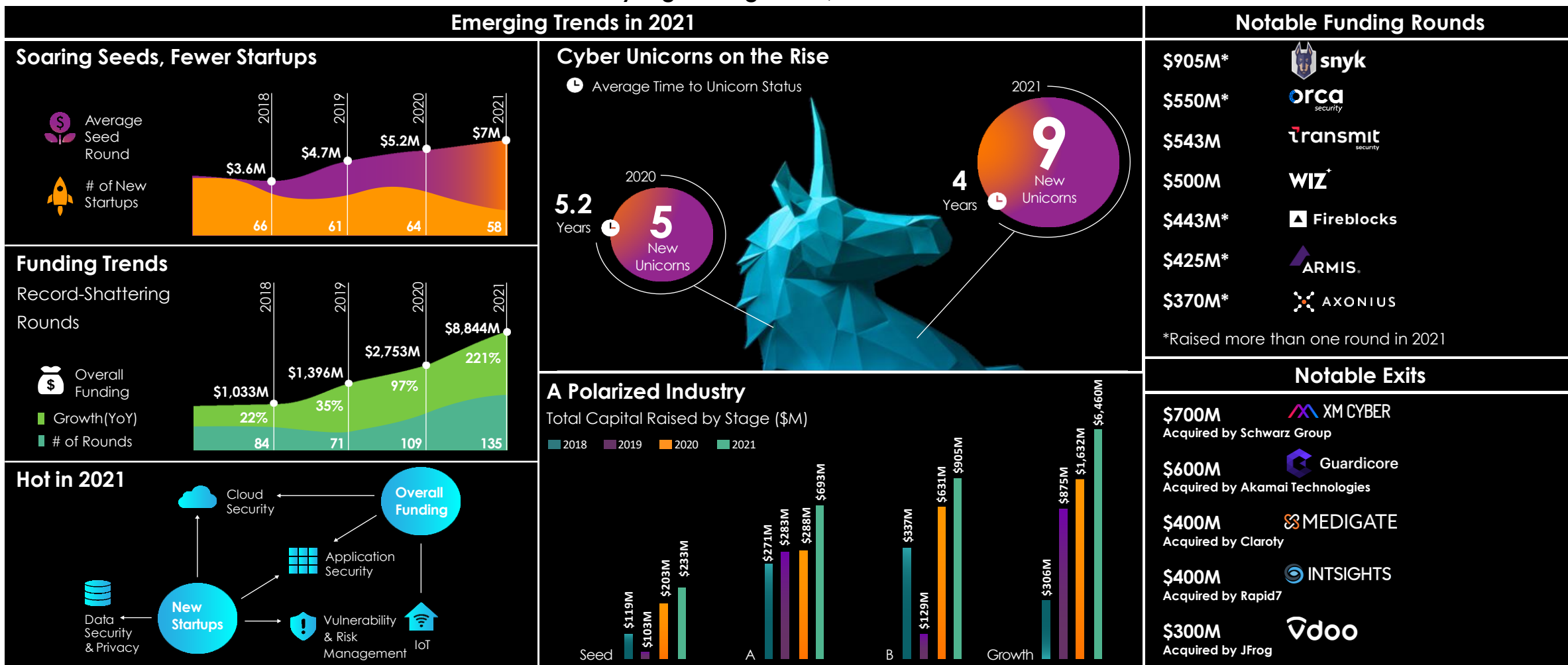
Forward-Looking Action

- Tech giant Apple has sued NSE Group for targeting users of its devices, seeking a permanent injunction to ban NSO group from using any Apple software, services, or devices.
- The US Government has recently black-listed NSO Group based on their prior involvement in providing spyware to foreign nation-states and other threat actors
- It remains to be seen how zero-click exploit techniques will be combatted by both the private sector and governments alike, however the powerful technology in the wrong hands poses a threat to citizens around the globe

YL VENTURES | State of the Cyber Nation 2021

By Yonit Wiseman (Associate, YL Ventures).

YL Ventures releases the “State Of The Cyber Nation 2021” report, which focuses on Israel's Cybersecurity ecosystem over the past year, analyzing funding trends, rounds and exits.



2022 Threat Report

SOPHOS

Report Centers On 5 Aspects Of Cybersecurity Under Threat Of Attack In 2022.

The Future Of Ransomware

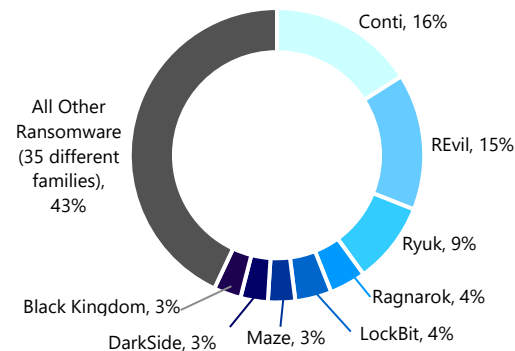
Ransomware Leasing Model Emerges

- More attackers are creating and then leasing out ransomware to specialists who then use the pre-made ransomware
- This model opposes traditional groups who make and then attack organizations using their own bespoke products

Expanding Extortion

- Large organizations are increasingly susceptible to threat actors moving valuable company secrets to a cloud backup and then demanding payment
- Extortion leaves companies open to customer backlash, privacy laws, and loss of trade secrets

Ransomware Families Investigated By Sophos Rapid Response, 2020-2021



Malware Begets Malware



The Rise of Cobalt Strike

Cobalt Strike is a commercial threat-emulation product suite with a customizable Beacon-backdoor to execute several commands. Hacked copies of Cobalt Strike are all over the internet with ample training available for use making it a favorite among recent attackers



Malware Distribution Frameworks

Several malware families are switching business models to a Malware Distribution Network (Ex: IcedID, TrickBot, Dridex) – Criminals can contact networks to distribute malware out with ease and scale



Shotgun Attacks with pinpoint targeting

Shotgun or spam attacks were prominent until recent years. Threats are now only firing off their attacks after luring and screening a larger population (Ex: Language, Location & Operating System filtering)



Trouble for Malware Researchers

Bad actors will continue to spread attacks widely and then quality-filter results to keep under the radar which will be troublesome for security researchers

Security & AI In 2022 And Beyond



AI in 2021

- Transitioned from a specialized discipline to a technology ecosystem
- Recognition and shift towards integrating ML into the space



AI & Threats

- Open-source AI is accessible by anyone
- Adoption of Generative adversarial networks (GANs) will directly lead to neural network voice and video synthesis tech



Cybersecurity & AI

- User-facing security ML will make IT security products intuitive, easier and more efficient
- Deep learning at scale using supercomputers will help revisit missed problems

Unstoppable Mobile Malware



Flubot

- Major banking trojan affecting Android in 2021
- Steals details through fake bank login screens
- Spreads through SMS & stolen contact lists with mimicked URLs



Fake iOS app Scams

- Victims download applications through 3rd party site (Apple ad hoc distribution method)
- A more personal attack (targets people on dating apps & media)



Joker

- SMS subscription billing fraud malware
- Deployed in the form of utility applications (Ex: QR scanners, wallpaper apps, flashlight apps)



Initial Access Brokers

- As threats concentrate jobs to specialize, the emergence of IABs sell gateways into company servers
- IABs gain foothold into networks through RDPs, VPNs, or lackluster zero trust safety



Linux & IoT

- Linux Bash scripts target Debian or Red Hat distributions to perform reconnaissance, lateral movement & encryption
- Attackers will target IoT devices on Linux shells



Commercial Tools

- Attackers are relying on bootleg copies of commercial/open-source software
- Old Conti attacks show usage of TeamViewer, Splashtop, Routerscan & more

Infrastructure Under Attack

Cyber Predictions For 2022 And Beyond

Increasingly Aggressive Ransomware Attacks And Nation-State Threat Actors Will Compound Cyber Threats.

Ransomware & Multi-Faceted Extortion



No End In Sight To Breaches

Ransomware threats have no end in sight, likely continuing their upward trend from outside the U.S. against critical industries where there is greater urgency to pay ransoms and avoid significant impacts



No Honor Among Thieves

Ransomware-as-a-Service (RaaS) operations often involve multiple actors that perform a portion of the attack for a portion of the proceeds, which can lead to conflict among actors



US Government's Role In Ransomware

Currently, U.S. organizations are not allowed to pay threat actors on a "no-pay" list and the government may look to make an example out of a large organization that makes a payment from an extortion demand



Cyber Physical Systems Vulnerabilities

Attacks on OT environments can cause serious disruption and increase pressure on organizations to pay a ransom given the potential of serious consequences from a breach



More Public Breaches In APAC and Japan

APJ organizations are often inexperienced with extortion operators threatening to publish sensitive data which will likely lead to many more breaches being made public in the coming year

Key Nation-State Threat Actors



Russia

Likely to maintain an aggressive posture into 2022 and target NATO, Eastern Europe, Ukraine, Afghanistan, and the energy sector



Iran

Expected to leverage destructive malware to promote regional interests and continue to target Israel and others in the Middle East



China

Looking to scale espionage operations and potentially flex destructive capabilities as geopolitical tensions continue to rise



North Korea

Aiming to take risks going into 2022 by leveraging Cyber capabilities to make up for the lack of other instruments

Select Commentary



“ The reality of doing incident response work remotely is more important than it's ever been. I think we need to anticipate a world moving forward where the offices that we work in will very likely be virtual.
- *Charles Carmakal, SVP & CTO, Mandiant*



“ When I think about 2022, the thing that's top of mind for me and for my colleagues continues to be ransomware. It's simply too lucrative. The business model makes it such that a threat actor has a lot more to gain than to lose.
- *Sandra Joyce, EVP & Head of Global Intelligence, Mandiant*

Cybersecurity Is Core To Google Cloud's Strategy



Growing Security Ecosystem Continues To Drive Google Cloud Momentum & Differentiation.



On 8/25/21, Google announced its intent to invest **\$10 billion** over the next five years to **strengthen Cybersecurity**, including expanding zero-trust programs, helping secure the software supply chain, and enhancing open-source security, all largely through cloud security efforts.

Additional Exciting Trends at Google

BigQuery & Looker Integration

- Chronicle's integration into Looker and BigQuery signals Google's commitment to embedding security in all cloud products
- Merges security telemetry with other organizational data
- Enables businesses to quickly analyze and find meaningful insights in datasets, enhancing security and visibility

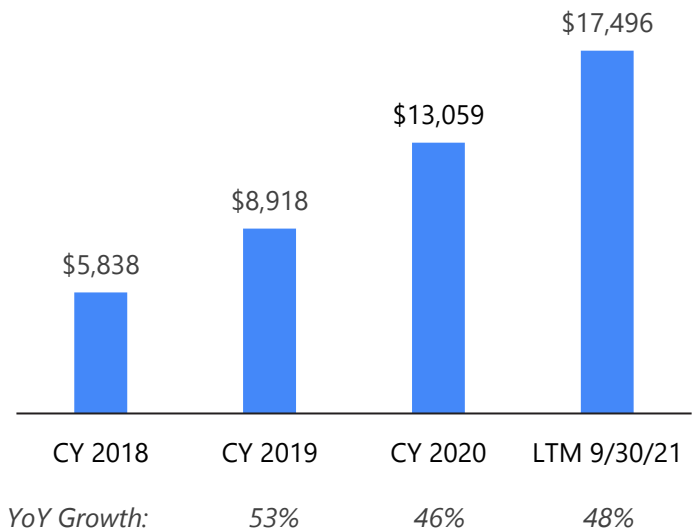
Investment in Security Tools

- Launched a new Cloud Intrusion Detection System (IDS) which provides cloud-native network threat detection
- Launched Google Cloud's Web App and API Protection (WAAP) in April 2021
- Announced three new solutions across data analytics, Dataplex, Analytics Hub, and Datastream

Partner / Channel Focus

- GCP has shifted to a 100% partner attachment strategy for customer deals
- Partners brought 85% more new customers to Google Cloud in 2019 relative to the prior year
- "We believe that partners have both a set of skills and reach that we don't have direct" – Thomas Kurian, CEO GCP

GCP Revenue



Key Commentary

Sundar Pinchai, Google CEO
July 2021 Earnings Release

“Google Cloud’s **security offering** is our **strongest product portfolio**, and we are continuing to enhance our solutions speed, integrating Chronicle, BeyondCorp and all the product components we have there. **You will continue to see us invest in Google Cloud Security.**”


2021 CISO Survival Guide

Trending Areas In 2021 Include SASE, DevSecOps, Privacy & Compliance, And Security Automation.

Report Overview

Cisco Investments, in partnership with Norwest Venture Partners, YL Ventures, and ForgePoint Capital, conducted CISO interviews and surveys and identified SASE, DevSecOps, Privacy & Compliance, and Security Automation as the key areas of focus for CISOs in 2021.

Key Findings



98% of survey respondents see clear benefits from SASE and are committed to directing future spend towards it



DevSecOps, while in a relatively nascent stage, is emerging as a trend with many new startups moving onto the scene



140+ privacy laws across the globe are making the regulatory landscape more and more complex



Many CISOs identified inventorying network access and protecting databases as priority areas for automation across their security stack

CISO Survey Key Stats

42%

Have ZNTA as top spending priority within SASE

60%

See the network as the most difficult to inventory

Up To
↑ 75%
intend to prioritize their future IT security budget on SASE

44%

Say that data access control is top priority

93%

Challenged to transition to being governance focused in app dev

Emerging Trends For CISOs In 2021



SASE

- Among the SASE pillars, ZTNA and cloud-native firewalls are the key priorities
- Most enterprises have already embraced cloud-based SWG and view cloud-native security and adaptive user access as critical focus areas



DevSecOps

- The role of security teams is changing with regards to DevOps security practices and security policies as code are increasingly prevalent
- CISOs are actively expanding software-driven security policies, adopting security tools for developers and applying security tools across the entire DevOps pipeline



Privacy & Compliance

- Data access control is ranked as the top privacy concern for nearly half of CISOs surveyed
- CISOs recommend building awareness of privacy and compliance across an entire organization through dedicated training and board-level visibility



Security Automation

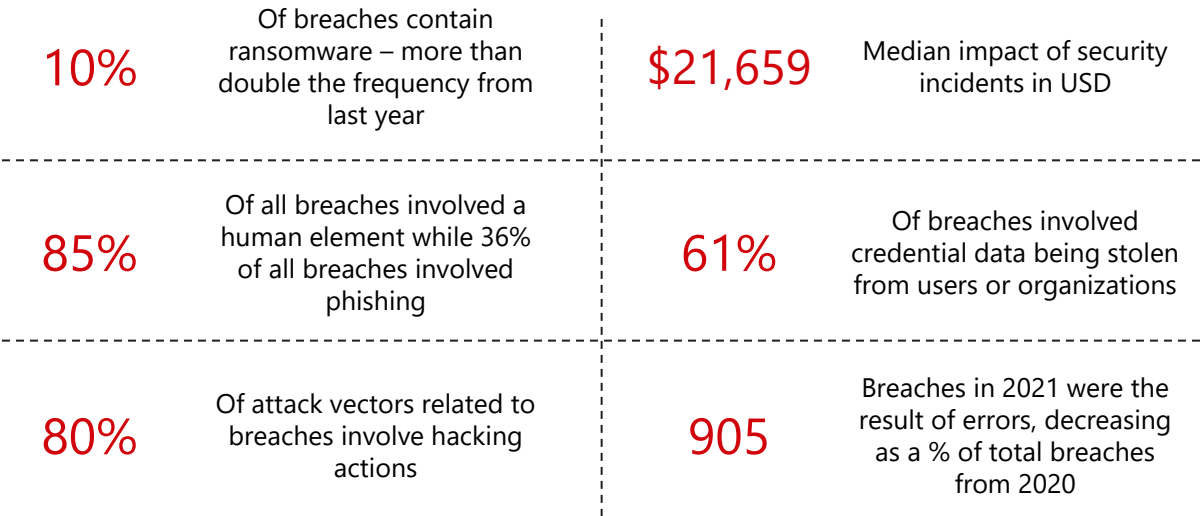
- While DevSecOps solutions are “shifting left” and “shifting everywhere,” overall financing has “shifted right” towards detecting and responding
- Startup innovation is continuing to “shift right” to address the needs of the industry during and post incident

2021 Data Breach Investigations Report (DBIR)



Verizon Provided Insights From Investigated Breaches To Demonstrate How Cybersecurity Threat Patterns Are Evolving.

DBIR By The Numbers



Key Takeaways



Ransomware is Still on the Rise
The upward move in ransomware has been influenced by new tactics, where some ransomware now steals the data as they encrypt it



The Human Element Accounts for a Majority of Breaches
A large majority of breaches involve user error, as many threat actors use social engineering attacks. Business Email Compromises also rose in 2021, reflecting the rise in misrepresentation



Financially Motivated Threat Actors Remain Persistent
Compromised external cloud assets were more common than on-premises assets in both incidents and breaches in 2021 as breaches move toward Social and Web application vectors, such as gathering credentials and using them against cloud-based email systems



Breaches Have Price Tags
While 14% of all breaches had no financial impact, organizations incurred heavy losses due to breaches in 2021 through losses, insurance costs, and stock price fluctuations

Security Control Best Practices



Secure Configuration

- Focus on solutions that are secure from the outset rather than tacking security on later
- Secure configurations help reduce error-based breaches such as misconfiguration and loss of assets



Account Management

- Centralize previous account management practices to manage access to all accounts
- Account management control is useful against brute force and credential stuffing attacks



Access Control

- Manage not only user account access, but also rights and privileges for these accounts
- Enforce multifactor authentication on key components, a useful tactic against the use of stolen credentials



Awareness & Skills Training

- Invest money into technical training and awareness programs to support organizational control over cognitive hazards
- Important due to a high prevalence of errors and social engineering attacks

SaaS Security Survey Report

The Need For SSPM Is Recognized As SaaS Misconfigurations Pose A Top Threat To InfoSec Professionals.

Survey Overview

By surveying 300+ InfoSec professionals, Adaptive Shield provides insight into Gartner's new category of cloud security, SaaS Security Posture Management (SSPM). The survey identifies how teams are currently handling their SSPM and their main concerns when dealing with SaaS applications.



By The Numbers



SaaS Security Trends

- SaaS Misconfigurations Are Considered A Top Threat
- Companies Struggle With Maintaining SaaS Security Hygiene With No Solution In Place
- As SaaS Use Grows, Security Checks Lessen
- App Owners Find Themselves Responsible For Security

SaaS Security: Challenges & Concerns In 2021

SaaS Stack Misconfigurations Create Security Blind Spots

- | Inconsistent Security Checks | Configuration Concerns |
|--|--|
| <ul style="list-style-type: none">As companies implement more SaaS applications, security checks become harder to manage73% of those surveyed only check security weaknesses either monthly, quarterly, or annually | <ul style="list-style-type: none">Constant app changes give rise to security concernsDespite 60% of companies worrying about 25% of their applications, the frequency of security checks has declined |

Increases In Applications Result In Mismanaged Security

- | Responsibility For Security | Poor Access Controls |
|---|--|
| <ul style="list-style-type: none">Over half of surveyed companies reported that security settings are monitored by the SaaS ownerSaaS security management is often delegated to less-trained staff who are not tied to the company's security department | <ul style="list-style-type: none">Giving security access to SaaS owners not trained in security can lead to an increase in security misconfigurations1 in 4 companies reported giving non-security departments access to SaaS app security settings |

SaaS Security Planning And Priorities

- | Top Security Priority | SSPM Planning |
|--|---|
| <ul style="list-style-type: none">SSPM tools give companies full visibility over their SaaS security ecosystem, when compared to other security tools48% of companies list SSPM as their top priority in 2021 | <ul style="list-style-type: none">Companies lacking SSPM face greater risk as they increase their use of SaaS applications63% of companies are already using or planning to implement SSPM tools |

YL VENTURES | The CISO Circuit

By Naama Ben Dov (Associate, YL Ventures).

YL Ventures releases their sixth edition of "The CISO Circuit Report - IAM", which outlines IAM domain challenges, such as the rise in enterprise assets requiring access and various identities to manage, technology's failure to keep up with concerted user demands, and management reluctance to implement updated IAM projects.

Most Significant Emerging Challenges

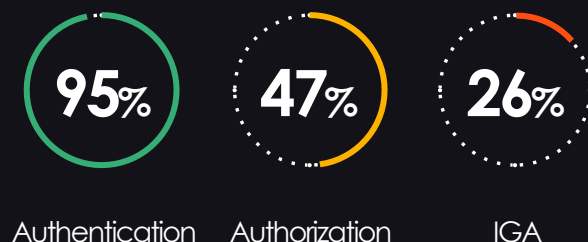
47%
Authentication scalability

26%
Authorization scalability

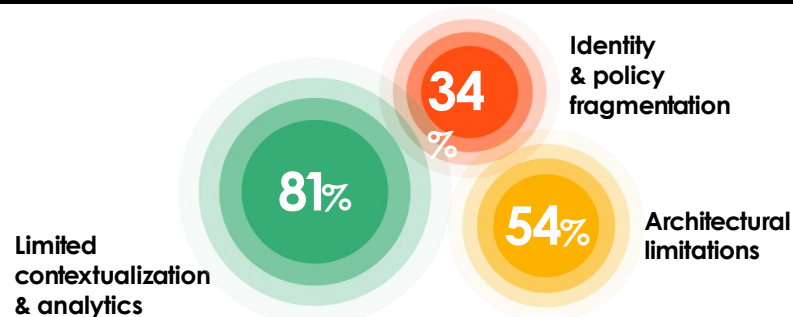
19%
Need for a single source of truth



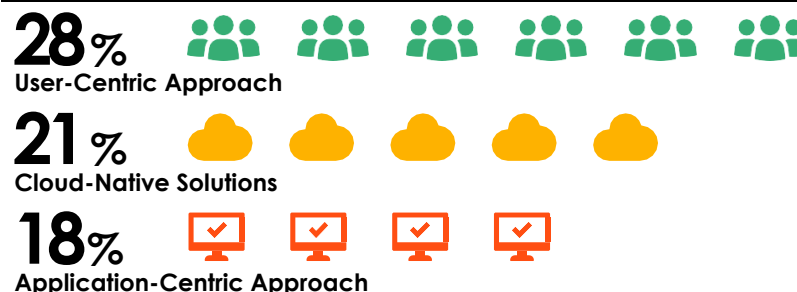
Most Used IAM Tools



Most Prevalent Difficulties With IAM Tools



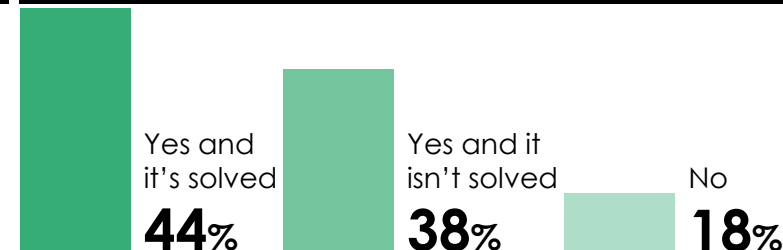
How Should Privileged Access Be Managed?



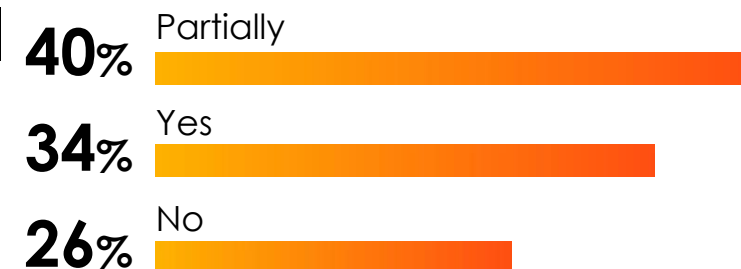
Are You Currently Using Passwordless Controls?



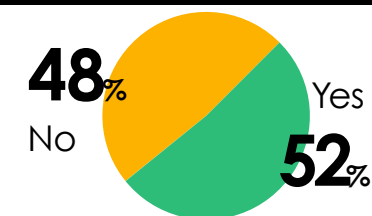
Is Developer Access To Production Environments A Priority?



Have You Centralized And / Or Automated Access Provisioning?



Would You Like To Add Additional Granular Access Controls?



Evolution Of The CISO Position

The Global Pandemic Has Drastically Increased The Scope Of The CISO Role.

Hitch Partners Overview

Hitch Partners is a retained executive search firm that specializes in Security Engineering, Product Security, and Physical Security leaders. The Company has expertise in rapidly identifying talented candidates while enhancing the skills and productivity of current Cybersecurity executives.

Services Provided

Search Capabilities

- Connections with skilled minds to help companies build an optimal CISO team
- Customized search strategies to effectively identify top notch candidates who satisfy the requirements laid out by the companies

Leadership Advisory

- Executive career coaching to help CISOs increase their confidence, presence, and impact
- On-demand chief of staff to consult with when making unfamiliar decisions
- Training on culture navigation and messaging to build trust and rapport

30%+

Placed Candidates in
D, I & B Category

50+

CISO
Placements

73%

Of Private Technology
Unicorn Clients

Key Trends & Statistics



Security teams have been growing due to the increasing importance of Cybersecurity



The number of CISOs given the responsibility to manage IT has increased by 39% YoY



~75% of CISOs report directly to the C-Suite



42% of CISO teams present to the Board of Directors on a quarterly basis at minimum

Growth Of CISO Position

Overview



“Since the COVID-19 pandemic started, the job market for new and existing CISOs has become more competitive. This is due to every aspect of the CISO’s role, scope, and positioning expanding – the CISO has become *the* critical hire for many organizations regardless of industry, company size, or location. Whether a company is hiring a CISO to secure its product platform, achieve compliance or governance standards, build customer trust, drive customer acquisition, or demonstrate executive leadership, the opportunities are plenty.”

– Michael Piacente, Managing Partner & Co-Founder, Hitch Partners

Changes To CISO Role



Shift In CISO Positioning Within Organizations

- Rather than being a traditional IT-centric deputy, the CISO role is now evolving into a product, cloud, and customer-facing standalone executive leader with substantial executive sponsorship



Increased Exposure And Interaction With Executives

- Many BoDs require CISOs to regularly present on the state of data protection, privacy, and company brand protection, as well as strengthen levels of awareness and education across the organization
- Greater elevation to reporting structures will be expected in the future due to the increased scope



Higher Levels Of Communication Within An Organization And With Customers

- CISOs are now the designer, driver, and communicator of a company’s overall security program
- There will be heavier customer acquisition responsibilities due to an overall expansion of an evolving audience



More Nuances In The CISO Role

- The increase in specialization will be driven by how a company builds, deploys, and maintains its products and/or services
- CISOs will need to rapidly gain new skills to effectively manage the increased scope

The Biden Administration's Cybersecurity Executive Order

Washington Continues To Devote Resources Toward The Growing Threat Of Cyber Attacks In The Public And Private Sectors.

Overview Of Executive Order

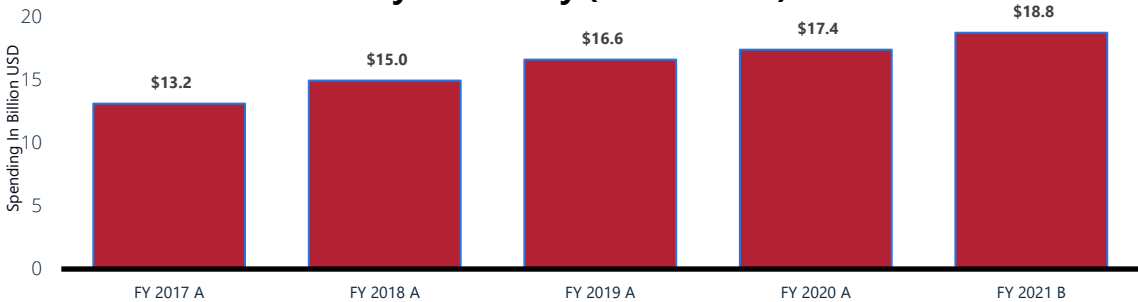


On May 12, 2021, the President signed an executive order to galvanize public and private efforts to help identify, deter, protect against, detect, and respond to persistent and increasingly malicious cyber campaigns. It sets a goal for more effective and agile federal government responses, along with increased security and protection of IT and OT.

Key Elements Of Executive Order

-  Removes Barriers To Threat Information Sharing Between The Public And Private Sectors
-  Modernizes And Implements Stronger Cyber Standards Throughout The Federal Government
-  Strengthens Security Measures Across The Software Supply Chain
-  Establishes A Cybersecurity Safety Review Board
-  Institutes a Standardized Federal Playbook For Responding To Cyber Incidents
-  Enhances The Government's Ability To Detect Cybersecurity Incidents On Its Networks
-  Improves Investigative And Remediation Capabilities

US Government Spending on Cybersecurity (2017 – 2021)



Significant Cyber Events In The US

- January 2021**
Hackers linked to Hezbollah breached telecommunications companies, internet service providers, and hosting providers in the US, UK, Egypt, Israel, Lebanon, Jordan, Saudi Arabia, and the UAE
- February 2021**
The Department of Justice indicted three North Korean hackers for conspiring to steal and extort more than \$1.3 billion in cash and cryptocurrencies
- March 2021**
Hackers backed by the Chinese government targeted Microsoft's enterprise email software to steal data from over 30,000 organizations around the world, including government agencies, infectious disease researchers, and legislative bodies
- April 2021**
Two state-backed hacking groups – one of which works on behalf of the Chinese government – exploited vulnerabilities in a VPN service to target organizations across the US and Europe, with a particular focus on US defense contractors
- May 2021**
Colonial Pipeline, the largest fuel pipeline in the United States, was the target of a ransomware attack and paid \$4.4 million to the Russian hackers to regain control of its computer systems; \$2.8M of ransomware was later recovered by the FBI
- June 2021**
Notorious Russian cybercrime group, REvil, exfiltrated 5 terabytes of data from the world's largest meat processing company, JBS, resulting in an \$11 Million ransom payout and the halting of 23% of the United States' meat supply

Source: The White House: [Executive Order on Improving the Nation's Cybersecurity](#), Center For Strategic And International Studies: [Significant Cyber Incidents](#), GovInfo: [Cybersecurity Funding](#)

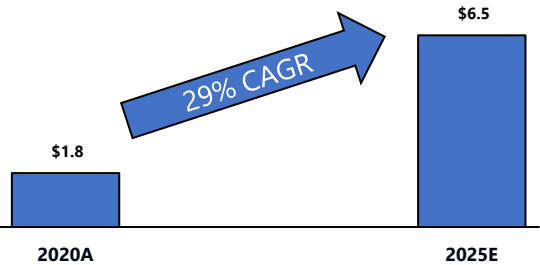
Market Opportunity For DevSecOps

DevOps Practitioners Are Shifting Left Towards Security, Creating An Opportunity To Sell Security Applications To Software Developers.

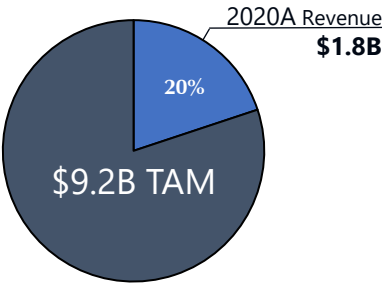
Market Overview

Over the past decade, there has been a “shift left” of IT operations towards the planning phase of software development. While traditional IT Ops processes have shifted left, security has remained far right in the deployment and maintenance phase. As a result, software engineering teams have quickly emerged as the next end market for Cybersecurity tools, giving rise to DevSecOps.

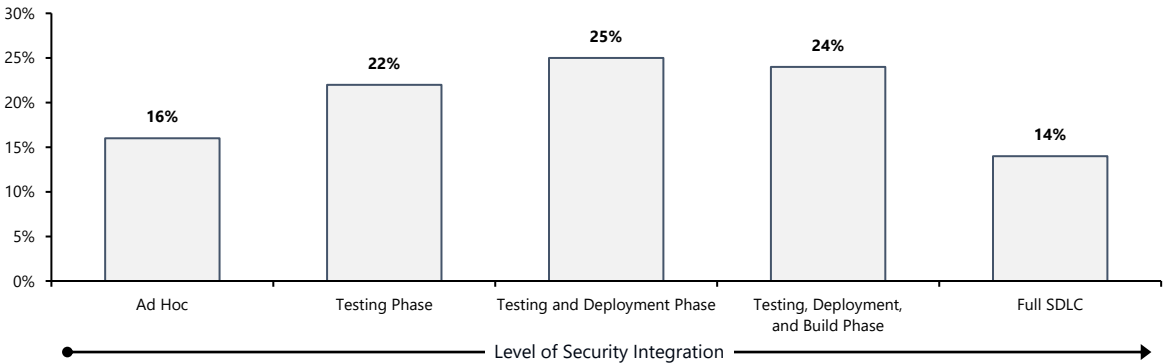
DevSecOps Growth Trajectory



Current Market Opportunity Captured








Security Integration Of DevOps Practitioners By SDLC Phases



Solutions Overview

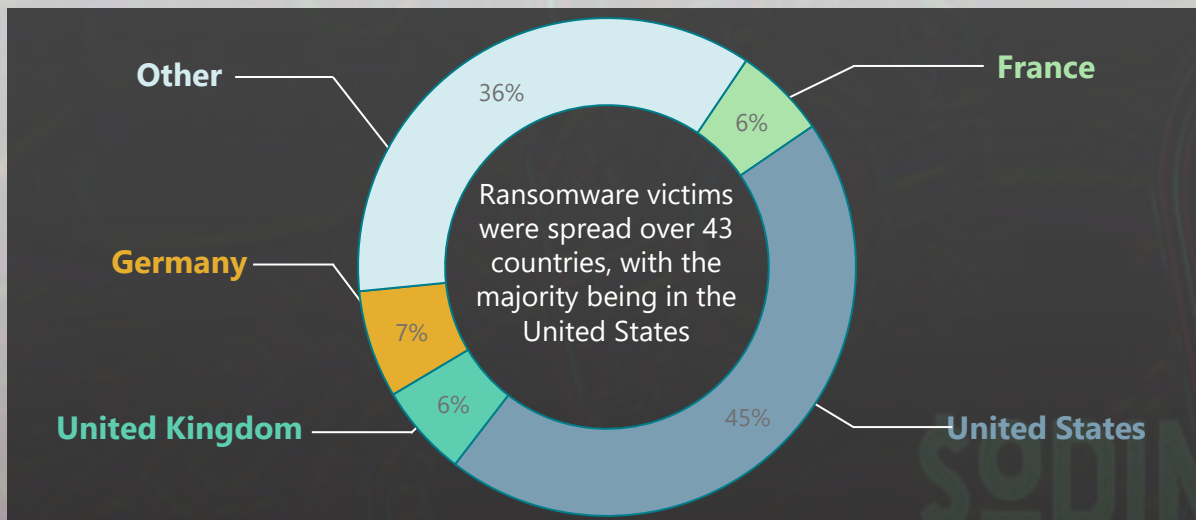
The **DevSecOps** market is highly fragmented into multiple point solutions that plug into specific phases of the SDLC. Significant opportunity exists to consolidate service providers and horizontally integrate their solutions into a single unified platform.

	Threat Modeling Automation	<ul style="list-style-type: none">Inspects production environments for vulnerabilities and quantifies various levels of risk to an organization based on various attack vectors
	Software Composition Analysis	<ul style="list-style-type: none">Identifies dependencies on open-source libraries in code bases and flags vulnerabilities found in modern applications
	Application Security Testing	<ul style="list-style-type: none">Plugs into and surveys integrated developer environments, alerting developers to vulnerabilities before they deploy applications
	CI / CD Pipeline Security Integration	<ul style="list-style-type: none">Scans for vulnerabilities during the build phase and embeds security policies to prepare applications for deployment
	Chaos Engineering	<ul style="list-style-type: none">Automatically tests applications against various failure and outage scenarios based on potential security threats





Ransomware Round-Up May 2021

Tetra Defense Observed 231 Total Ransomware Attacks In The Month Of May.

Geographic Breakdown of Attacks – May 2021






Industry Breakdown




	Manufacturing	Most highly impacted industry for the month of May with a total of 29 attacks
	Education	Industry with the highest revenue, totaling \$2.8 Billion
	Technology	Encountered 23 attacks for the month of May
	Construction	Encountered 20 attacks for the month of May

Most Prevalent Threat Actor Behavior & Intel

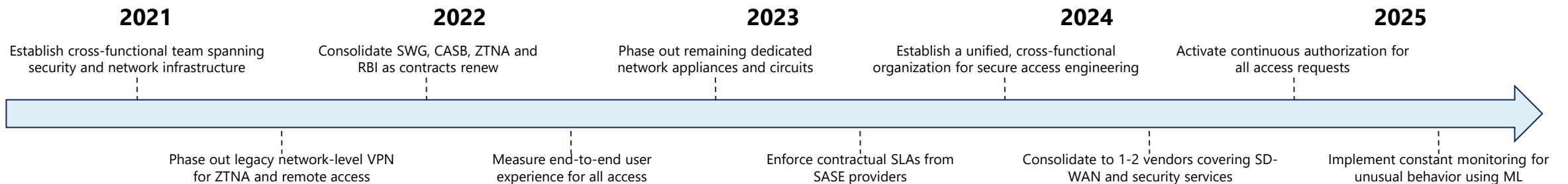
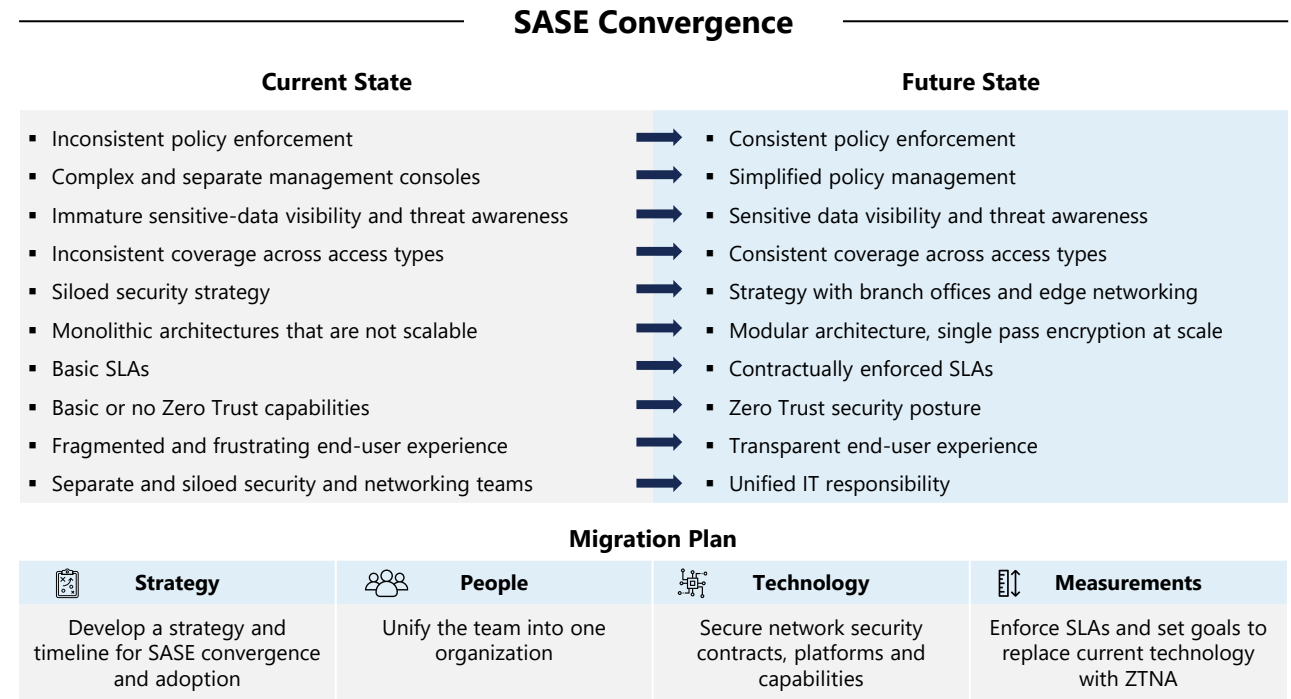
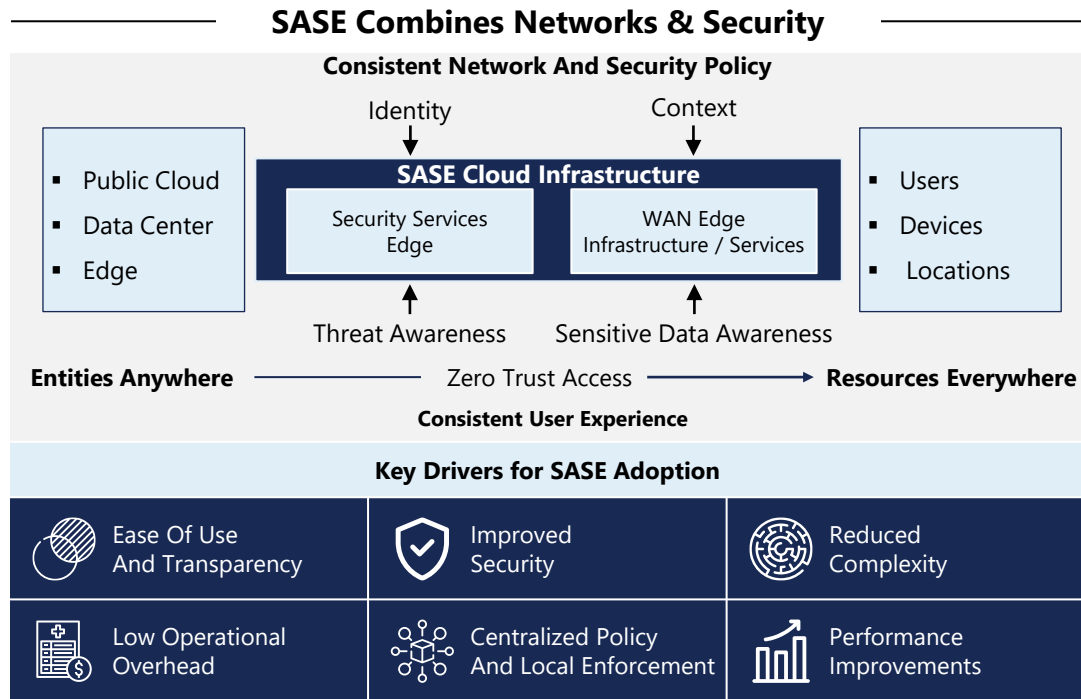
Avaddon, Conti, and Sodinokibi had the highest number of disclosed ransomware attacks among major threat actors. Intel from Tetra Defense has indicated that, for the month of May, Thursday is the most common day for a new victim to be posted on the dark web.

		
Publishes a large number of victims over two consecutive days followed by a week of silence	Posts large number of victims twice throughout the month, with a steady stream of smaller releases	Displays a consistent stream of smaller victim releases throughout the month

New Threat Actor Groups

	<ul style="list-style-type: none"> Engages similar targets as the established ransomware group Astro Team – which has gone offline since Xing's formation Sophos, has investigated the mounting evidence between the groups for indications of a first-degree connection
	<ul style="list-style-type: none"> Discourages negotiations and takes an aggressive approach to ransomware through periodic releases of user data Claims to be "the new generation" of threat actors that no longer engages in discounts or provides data proofs
	<ul style="list-style-type: none"> Employs automation by means of a chat bot which handles everything from sample file decryption to payments

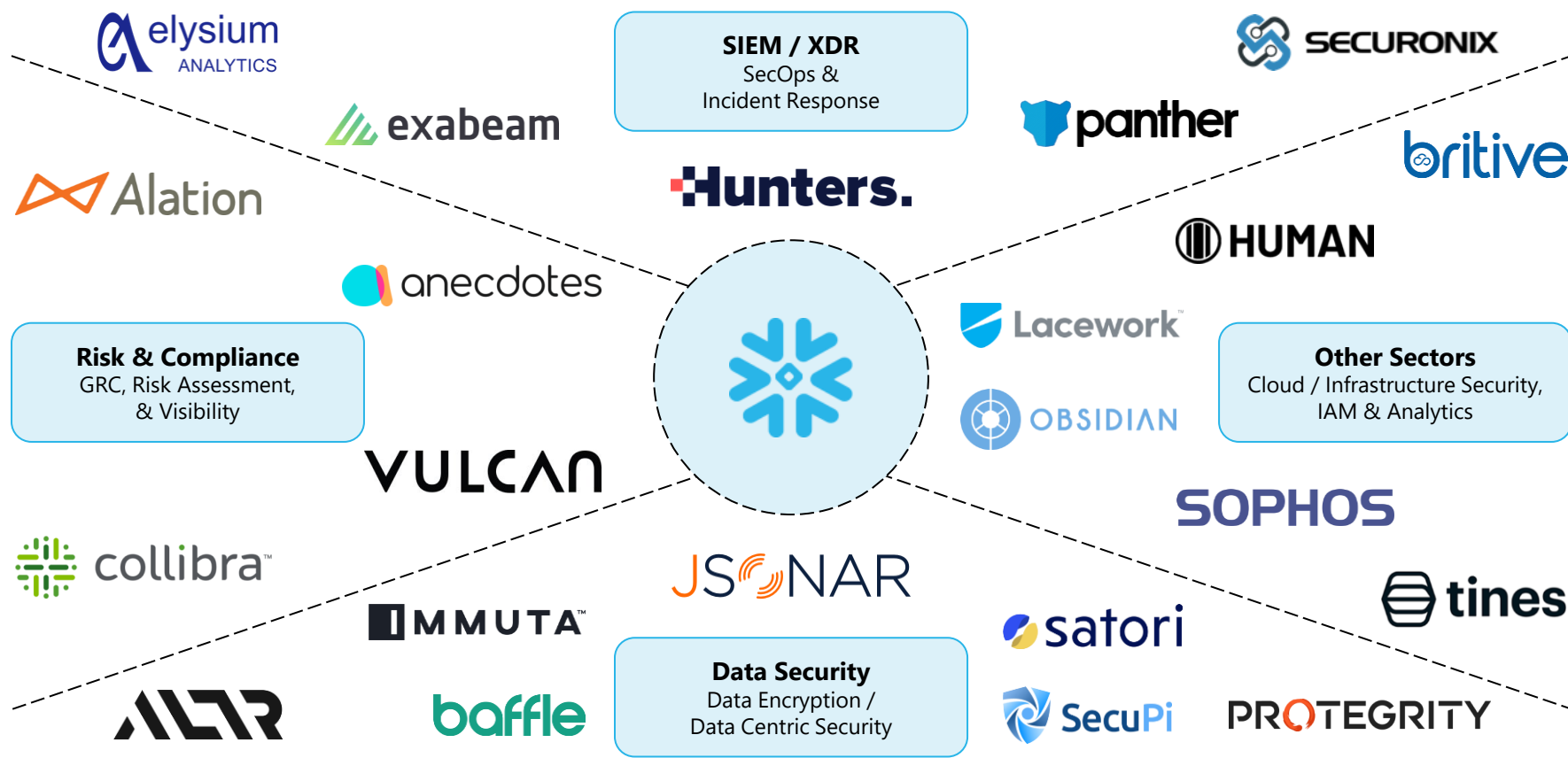
Gartner®







snowflake | Cybersecurity Partner Ecosystem

Snowflake Is Helping Cybersecurity Vendors Simplify Their Architectures & Enhance GTM Efforts Through Their “Powered By Snowflake Program”.

Snowflake's Cybersecurity Ecosystem



Partner Spotlight

	Enables data migration to Snowflake and provides active data governance
Elite Partner	
	Ingests standardized data from Snowflake to automate data privacy governance
Elite Partner	
	Provides advanced security, access-control, auditing, and privacy management
Premier Partner	
	Analyzes data with code-driven automation to replace legacy SIEM architecture
'20 Partner of The Year	

Snowflake Ventures

Corporate VC Arm Of Snowflake Investing In The Data Cloud Industry

Select Cybersecurity Investments



Forbes | Artificial Intelligence Predictions

Vendors Will Out Innovate Attackers by Combining Human And Machine Insights In An Escalating AI-Based Arms Race.

Emerging AI Trends



Unsupervised machine learning approaches will continue to advance, finding patterns and structure in data rather than training classifiers



Gaining more visibility into **open-source contributors** will be critical in 2021 for developers to vet who they're trusting & the packages they're leveraging



Privacy regulations like the GDPR explicitly limit the use of automated technologies in processing and profiling using personal data



Pervasive intelligence and **enterprise automation** will have significant impacts on business growth and strategy in 2021



AI Ops will heat up to enhance the customer experience and deliver on application assurance and optimization



AI, machine learning, and BIOS-level technologies enable more **resilient endpoint connections** that can keep up with this rapid rate of change

Highlighting AI Increasing Use In Authentication Frameworks



Authentication Frameworks

- AI will be embedded into more authentication frameworks for **less friction** and to guarantee **real-time decisions**
- High use in **multi-factor authentication** (MFA) will dynamically reduce risk by establishing real-time risk scores and stop threats at the authentication stage



AI As Authentication

- Shift away from passwords to **mobile-centric zero trust** security approach
- AI and machine-learning** validates devices, establishes user context, checks app authorization, verifies the network, and detects and remediates threats before granting access

Organizational Drivers Fueling Increased AI Integration

Shift to vulnerable remote offices and online services key areas

Cybersecurity skills shortage will cause firms to automate protection with AI

Quickly changing employer and employee IT and security needs

Sophisticated Cyber Attacks Require Advanced Solutions



Phishing Attacks

Threat actors are relying on machine learning to automate and reduce costs of phishing attacks



Training Stage Attack

Organizations must adjust algorithms to both detect and react to attacks in both the training and production stages of AI



Large Datasets

Organizations are increasingly aggregating large amounts of highly sensitive data, creating easy targets

Enterprise Response Plans



Cloud Adoption

- Solves **entitlement challenges** related to cloud adoption by leveraging AI
- Helps detect access related **risk in IaaS and PaaS** landscapes



Catalyst Against Malware

- AI and ML** will be a catalyst for weeding out malicious intent
- Enterprises will **identify and flag scenarios** where it's the first open-source project a user has contributed to to verify their credibility and if the user alters code in sensitive areas of the system



Increased Investing Into AI

- Security vendors are spending more time and money than ever on **specialists in artificial intelligence and data science** to mine their data and enhance their products

snowflake | Leading Companies Are Adopting A Security Data Lake

Snowflake Provides A Robust Data Lake That Can Serve As A Single Source For All Security / Compliance Data.

Cybersecurity Is A Big Data Problem...

As key industry trends continue to grow data volumes exponentially... **Snowflake's** cloud built multi-clustered architecture is purposely built to store petabytes of shared data, scale compute resources up or down, and enable full visibility across security logs at massive scale.



Increased Shift To Cloud Infrastructure

The shift to cloud infrastructure is highly instrumented and generates detailed logs across the enterprise, often resulting in a 10x+ increase in machine data



Move From Endpoint Antivirus to EDR Solutions

Companies shifting from traditional endpoint antivirus to EDR products must manage not just alerts but also complete "flight recorder" logs on every server and laptop

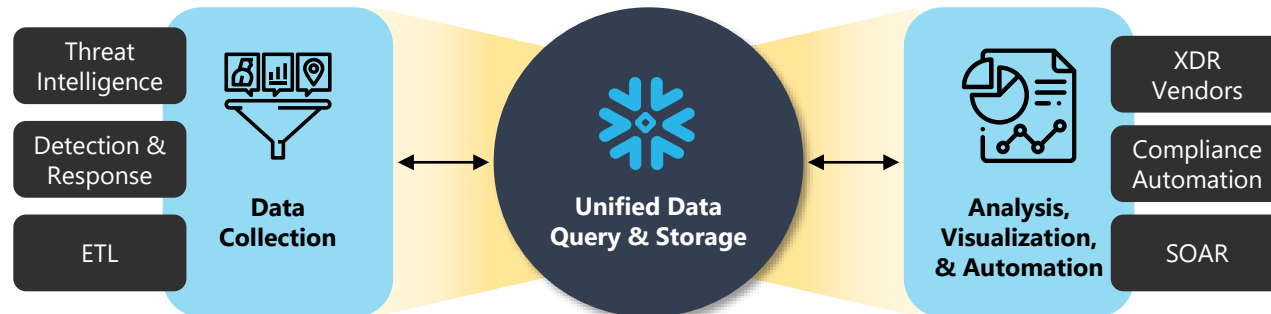


High Cost Of Centralized Data / Legacy SIEMs

Large data sets are expensive to centralize and standardize within legacy architecture, often resulting in an incomplete/fragmented landscape as well as SIEM sticker shock

Snowflake | The New Security Stack Tied Together By The Data Cloud

Legacy SIEM architecture tends to be fragmented and limits security teams across dimensions such as data ingestion and retention time. The shift to a data lake architecture takes vertically integrated components of SIEM and breaks them into three parts that are tied together through the Data Cloud.



The new security stack won't mirror the vertically integrated SIEMs of the past – rather the data platform will play an essential role supporting specialized solutions that deliver better security, lower costs and more automation.

...That Snowflake Plays An Essential Role In Solving

Cybersecurity Use Cases



Incident Response

- Integrates and analyzes high-volume data logs in seconds
- Scales resources up and down accelerating incident response
- Compiles structured and semi-structured logs



Threat Detection

- Supports detection rules that are unavailable in legacy SIEMs
- Allows for partnerships with integrated detection solutions
- Enables the creation of custom SIEMs on Snowflake



Security Metrics

- Generates actionable reports based on compliance metrics
- Identifies visibility gaps and out-of-compliance machines
- Resolves out-of-compliance issues across IT and security

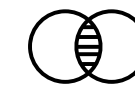
As data moves to petabyte scale – sophisticated security analysts are increasingly demanding new platform features such as smart indexes, relationship graphs, lower latency, and incremental languages that **Snowflake** specializes in...

...**Snowflake** provides a holistic data platform that bridges the gap between data platforms and domain security requirements. The platform enables the lateral integration of SIEM capabilities and a unified data layer while supporting niche data solutions in an ecosystem that delivers both data centralization and optimization.

Key Platform Benefits



Capture and Efficiently Store Data From All Sources – Gaining Full Visibility



Run Analytics On Security Logs & Enterprise Data – Reducing SIEM Cost

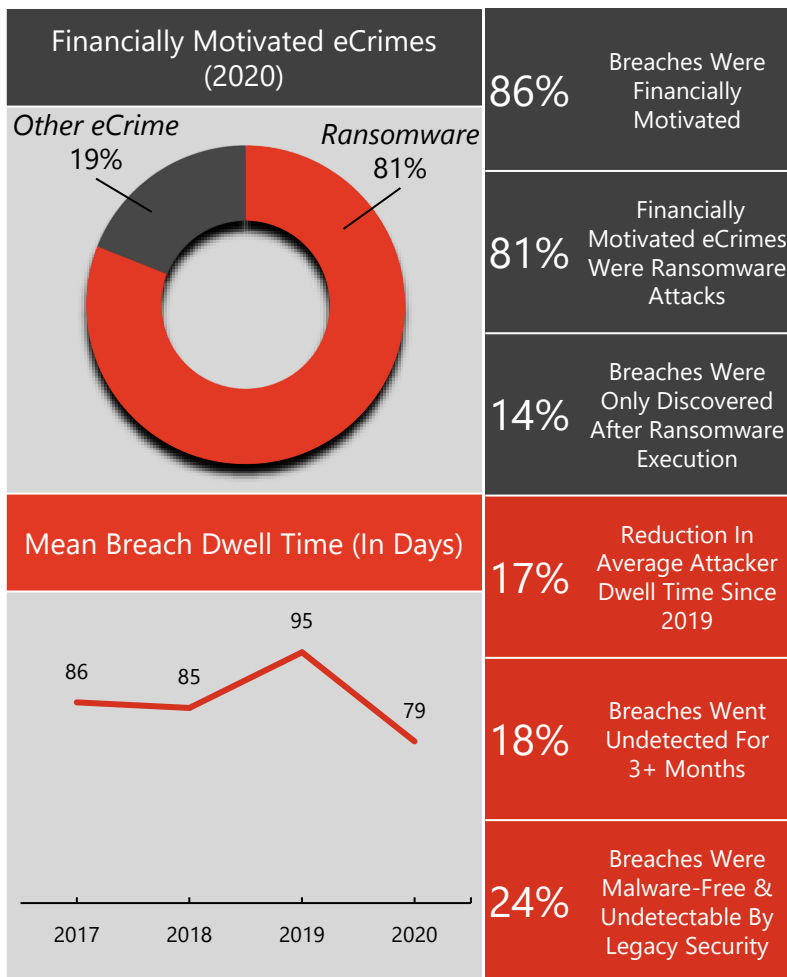


Provide Partners Seamless Governed Access To Data And Robust Cyber Integrations
















CROWDSTRIKE Services | Cyber Front Lines Report

COVID-19 Leaves Organizations Battling To Address Public-Facing Weaknesses & Improve Post-Breach As Threat Actors Evolve & Adapt.

By The Numbers | Key Takeaways



Cybersecurity Themes For 2021

As Threat Actors Advance & New Security Practices Emerge...		...Organizations Must Adapt & Respond Proactively	
 Evolution Of Ransomware	<ul style="list-style-type: none">Big game hunting (BGH) ransomware variants are increasing with formal collaboration and copycats among threat actorsMultiple eCrime groups popularized data-leak extortion and follow-up DDoS attack threats for ransomware in 2020	 Invest In A Bulletproof Backup Security Strategy	 Implement MFA, PAM, & Next-Gen Endpoint Security
 Cloud-Native Cyberthreats	<ul style="list-style-type: none">Cloud infrastructure slated for retirement or neglected from maintenance and updates is a prime targetThreat actors leverage cloud to launch attacks using the lack of outbound restrictions and workload protection	 Set Up A Cloud Account Creation Factory	 Incorporate CSPM & CWP Solutions
 Public-Facing Weaknesses	<ul style="list-style-type: none">Attacks on perimeter-facing vulnerabilities wrought immense financial impact with consistent system downtimeSuccessful attacks on public-facing applications resulted in a 36% ransomware rate and 16% PII / PHI / PCI data leak rate	 Leverage Third-Party Web Application Pen Testing	 Upgrade Security On Internet-Facing Systems
 State-Sponsored Threat Evolution	<ul style="list-style-type: none">Nation-state actors are employing heavy use of N-day vulnerability exploits to compromise external applicationsLiving off the land (LOTL) techniques, commodity toolsets, and multi-stage implants contribute to long dwell times	 Establish Plans For A CRE Against TTP Modifications	 Adopt Cloud-Focused Security Assessments
 Post-Breach Improvements	<ul style="list-style-type: none">An emerging goal is to achieve continuous monitoring and response where new threats are solved in near real-timeOrganizations are turning the incident response cycle into an upwards spiral where future incidents are less severe	 Expedite Business Recovery For Security Advancements	 Garner Executive Buy-In For Security Investments

What's Behind The Surge In Cybersecurity Unicorns?

Security Industry Experts Share Thoughts On Why Cybersecurity Unicorns Are No Longer Rare Sightings.

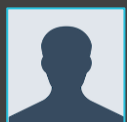


Will Lin



Managing Director, ForgePoint Capital

"Coupled with public market valuation highs, startups have been well-poised to succeed in this valuation environment. When looking at multiple multi-stage and cross-sector funds, **Cybersecurity has been identified by many investors as a significant contribution to their returns over the past cycle.**"



Venture Capital Investor

Anonymous

"I believe we are seeing 'Synthetic Unicorns.' I would define these as early-stage companies where the **unicorn valuation is being driven by optimistic investors that are intent on building a new platform company that can compete against existing platform leaders** such as Palo Alto Networks."



Brendan Burke



Sr. Emerging Technology Analyst, PitchBook

"**While several years ago a startup might need to reach \$100 million in annual recurring revenue to become a unicorn, only a fraction of that sum is required now.** Startups can achieve unicorn status soon after finding product-market fit with the expectation of growth to much higher valuations in public markets."



Hank Thomas



CEO, Strategic Cyber Ventures

"You now have a much clearer two class system of haves and have nots all competing for the same security budgets. **The haves actually help secure key Cyberspace terrain in a security environment that has changed radically in the past year.**"



Yoav Leitersdorf



Managing Partner, YL Ventures

"**The increase in the valuation of Cybersecurity companies is commensurate with the increasing number of breaches and compromises that we see in the headlines...**COVID drove a rapid shift towards digital transformation. As digital transformation grows, we should see the security market grow with it."



John Funge



Managing Director, DataTribe

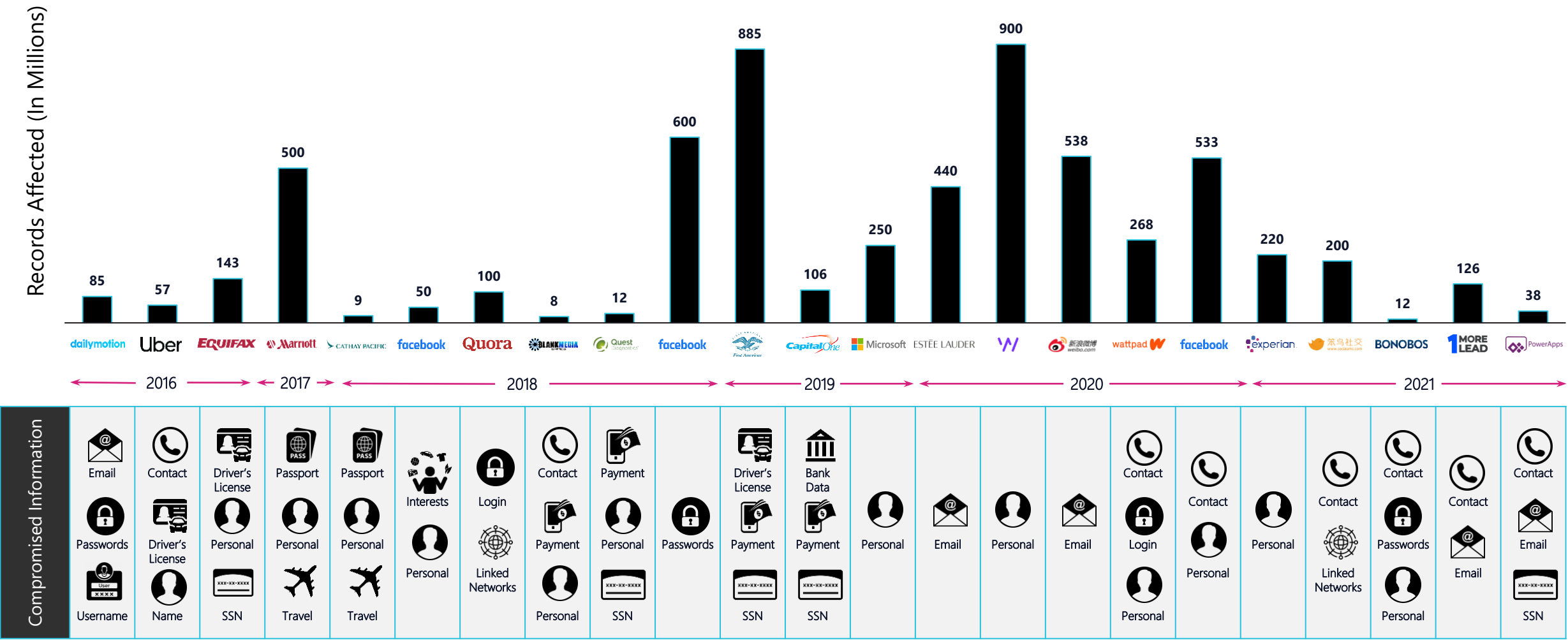
"Cyber is a very large market that generally doesn't exhibit strong winner-take-all dynamics like other parts of tech, such as social media. So, **there is space in the market for multiple unicorn-scale companies to form.**"

Breach Spotlight



Timeline Of Major Data Breaches








Large Breaches Have Been A Consistent Factor Over The Past Decade, While The Severity Continues To Escalate.



Sources: Visual Capitalist: [The 15 Biggest Data Breaches In The Last 15 Years](#), CRN: [The 13 Biggest Data Breaches Of 2019](#), Identify Force: [2020 Data Breaches | The Worst So Far](#), Security: [The Top 10 Data Breaches Of 2020](#), UpGuard: [Biggest Data Breaches This Year](#), IdentityForce: [2021 Data Breaches](#).

Cuban Ransomware Gang Targets US

Cuban Ransomware Group Disrupts 49 Organizations From Critical US Infrastructure Sectors.


US Infrastructure Breach Overview			Key Takeaways	
Key Details		Attacker Profile & Activity		Current Implications
Critical Sectors Affected:	Financial, government, manufacturing, and information technology	<div><div>Background</div></div> <div><div>Attack Method</div></div> <div><div>Extortion</div></div>	<ul style="list-style-type: none">The group was first detected when they attacked payment processor Automatic Funds Transfer Services, forcing multiple US states to send out breach notification letters	<div>Rise in Ransomware</div> <ul style="list-style-type: none">Despite the alerts, we continue to see a rise in the number of ransomware attack victimsMany organizations give in to these demands to safeguard their reputation, critical information, data, and financial status <div>Security Patches Remain Ineffective</div> <ul style="list-style-type: none">90% of vulnerabilities exploited by ransomware have patches associated with them10% attacks are vulnerabilities for which patches are not available
Attack Location:	Across the United States			
Date Announced:	December 3, 2021			
Breach Profile:	Cuba ransomware is delivered on victims' networks through the Hancitor malware downloader			
How It Happened:	Widespread Ransomware Attack exploited primarily through Phishing attacks			
Current Status:	Unconfirmed As Of Publication			
Contextualizing The Attack				
Cyber Expert Commentary		Key Stats		
<p>"This really highlights how much money there is to be made from ransomware. Cuba is a relatively small player, and if they made \$49 million, other outfits will have made considerably more."</p> <p>– Brett Callow, Threat Analyst, Emsisoft</p> <p>"Critical infrastructure will remain a highly lucrative target. There is a subtle but massive change in attacker tactics that is taking place and we are at risk of being totally blindsided."</p> <p>– Satya Gupta, Cofounder and CTO, Virsec</p>		<div>\$44M</div> <div>Total Payout Received by Cuban Ransomware Actors in latest attack</div>	<div>105</div> <div>Cuban Ransomware Submissions according to Emsisoft's Research Report</div>	
		<div>\$590M</div> <div>In Ransomware activity in the First Half of 2021 as Identified by the US Treasury Department</div>		
Suggested Ransomware Mitigations				
<div><div>Runtime Security Controls</div></div> <ul style="list-style-type: none">Provide active protection for an enterprise's container applications while in useThese controls will stop attackers, in milliseconds, from successfully exploiting vulnerabilities		<div><div>Login Security Protocols</div></div> <ul style="list-style-type: none">Require multi-factor authentication for all services, particularly for webmail, virtual private networks, and accounts that access critical systems		
<div><div>Segment Networks</div></div> <ul style="list-style-type: none">Network segmentation can help prevent the spread of ransomware by controlling traffic flows between — and access to — various subnetworks and by restricting adversary lateral movement		<div><div>Control Access Points</div></div> <ul style="list-style-type: none">Restrict privileges to only the necessary service or user accounts and perform continuous monitoring for anomalous activityImplement time-based access for accounts set at the admin level and higher		

FBI Hacker Returns For Robinhood




Robinhood Has 7 Million Users' Data Breached And Listed On The Dark Web.



Breach Overview

Robinhood 	
Company Description:	Mobile Trading Platform
Company Location:	Menlo Park, CA
Date Announced:	November 8, 2021
Breach Profile:	Social Engineering via Customer Service Hotline
How It Happened:	Hacker gained access to the Robinhood customer support systems after tricking a help desk employee into installing remote access software
Current Status:	Remediation efforts were made by Mandiant shortly after being notified of the breach

Attacker Profile & Activity

 Background	<ul style="list-style-type: none">The hacker seems to be the same threat actor responsible for taking advantage of the FBI's email servers to send threatening emails
 Attack Method	<ul style="list-style-type: none">The hacker convinced a customer service employee to install a remote access software on his computer that he then used to access sensitive customer data and exfiltrate itData stolen included: names, email addresses, DOB, and zip code
 Previous Activity	<ul style="list-style-type: none">Prior FBI server breach was possible via a bug found in the FBI's Law Enforcement Enterprise Portal to send emails from their IP address

Key Takeaways




Current Implications

Attacks Are Becoming More Targeted	Phishing Attacks Remain Successful
<ul style="list-style-type: none">In the face of ongoing cyber attacks, hackers are becoming more targeted in exploiting security weak points45% of SMBs say that their processes are ineffective at mitigating attacks69% say that cyber attacks are becoming more targeted	<ul style="list-style-type: none">Phishing attacks are on the rise as the employees shift to WFH and security training to a minimum85% of breaches involved the human element36% of breaches involved phishing, 11% more than 2020

Breached Data Leads to More Targeted Phishing Attacks

- Hackers can use leaked information to carry out more attacks against the victims, like targeted phishing emails, as names and dates of birth can often be used to verify a person's identity

Defense Against Social Engineering Attacks

 A.I. Driven Security	<ul style="list-style-type: none">Leveraging A.I. to perform automated system checks, software updates, password changes, network maintenance, and limits on administrative access
 Education & Training	<ul style="list-style-type: none">Utilize cybersecurity platforms to train employees for social engineering attacksActive training using mock scenarios to ready all levels of employees against attacks
 Multifactor Authentication	<ul style="list-style-type: none">Deploying a multifactor authentication approach for employee credentials makes gaining increased access to your system harder for hackers with some stolen information

Contextualizing The Attack

Cyber Expert Commentary

"Once that attack occurs and you are compromised, the speed in which you can respond today is primarily gated by human effort — which is not fast enough because the attack is definitely coming from something that's enabled by machine intelligence, advanced automation."

—John Roese, CTO, Microsoft

"We can expect that attackers will continue to target people in these roles and invest in more sophisticated social engineering efforts in order to gain a privileged foothold within organizations that they target."

— Josh Yavor, CISO, Tessian

Key Stats

7M	Total amount of Robinhood users affected by the data breach
\$10k+	The hacker was looking to sell the stolen information for on a dark web forum
500%	Increase in threat activity for the payment services industry in Q2 of 2021

Data Breach of Cellphone Giant

21-Year-Old American Compromises 50+ Million Customers' Data As Cyber Crime Continues To Ramp.



T

T-Mobile | Breach Overview

Background

Company Description:

3rd Largest Telecommunications Company in the US

Date of Breach:

August 17, 2021

Company HQ:

Bellevue, Washington

Threat Actor:

American John Binns & possible unknown associates

Data Stolen:

Personal data, as well as IMEI and IMSI information

How It Happened:

T-Mobile network accessed via an unprotected router

Attacker Profile

Background

21-year-old American, John Binn, executed the data breach from Turkey as a form of retaliation following an alleged kidnapping by the CIA and Turkish Intelligence. He stated his overall goal was to generate noise and harm US infrastructure.

Method

Binn gained access to T-Mobile's systems through "production, staging, and developmental servers" before hacking into the Oracle database containing customer data. He claimed to copy 106GB of customer data before being kicked off the server.

Key Stats

Customers Affected

Category	Percentage
Current Customers	14%
Prospective Customers	74%
Current Postpaid Customers	9%
Former Customers	2%
Active Prepaid Customers	1%

Current Customers

Prospective Customers

Current Postpaid Customers

Former Customers

Active Prepaid Customers

*Stolen Information included names, addresses, phone numbers, DLN, SSN, as well as IMEI & IMSI used to track individuals' cellphones

Aftermath

Customer Risk

Sim-Swap

The stolen personal info can be used to convince T-Mobile to swap phone service to a sim they control

Having control of the individual's number allows them to bypass the 2FA process most applications require to reset passwords

T-Mobile's Response

T-Mobile is offering free access to McAfee's ID Theft Protection Service for two years and advanced spam-blocking

They provided postpaid customers Account Takeover Protection service to protect their accounts from being ported out and stolen

T-Mobile reset PIN numbers for all prepaid customers

T-Mobile plans to beef up security and overall strategic cyber security initiatives with the help of KPMG and Mandiant

Impact By The Numbers

30 million

Customers' info listed on a dark web marketplace at a price of 6 BTC

23 Lawsuits

Filed against T-Mobile calling for compensation for the victims

Source: [CNET](#), [CyberScoop](#), [ZDNet](#), [ClassAction](#), [Yahoo Finance](#), [TechRadar](#), [Usenix](#)

[Return To Table Of Contents](#)

99

Accenture Client Data Leaked By Hackers

Accenture Downplays Ransomware Hack As Attackers LockBit 2.0 Demand Record \$50M.

accenture

Accenture Incident Overview		Contextualizing The Breach		Key Takeaways	
accenture		Cyber Expert Commentary		Safety Steps	
Company Description:	Multinational Firm Providing Consulting and Professional Services	<div></div> <div></div> <div></div> <div></div>	"While the perpetrators were able to acquire certain documents that reference a small number of clients ... none of the information is of a highly sensitive nature." – Accenture Internal Memo	<div>Employees</div> <div></div> <div><div>1) Establish corporate security awareness campaigns to stress personal safety online</div><div>2) Restrict administrative rights for company employees</div><div>3) Avoid clicking on email links and attachments from unknown senders</div><div>4) Download a VPN and only use secured networks to protect employees online</div></div>	<div>Software</div> <div></div> <div><div>1) Update operating systems and software when available</div><div>2) Download anti-ransom software such as virus scanners and content filters on mailing servers</div><div>3) Backup data to restore during ransomware attacks</div><div>4) Incorporate cloud-based technologies to restore older versions of files</div></div>
Company Location:	Dublin, Ireland		<div></div> <div>"These attacks highlight the importance of 24x7 threat coverage. Yet in-house security teams struggle to keep up with threat alerts and afford, find and retain enough Cybersecurity experts" – Ric Longenecker, CISO, Open Systems</div>		
Date Announced:	August 11, 2021		<div></div> <div>Every enterprise should expect attacks like this – perhaps especially a global consulting firm with links to so many other companies. It's how you anticipate, plan for and recover from attacks that counts" – Hitesh Sheth, President and CEO, Vectra</div>		
Breach Profile:	LockBit ransomware attack releases 6 TB of client information, threatens to continue leak		<div></div> <div>"Rather than having a concrete 'always' or 'never,' think about the criteria you will use to make that decision, should you find yourself in a ransomware crisis." – Michael S. Rogers, Former Commander, U.S. Cyber Command</div>		
How It Happened:	Experts claim the hack was insider job; attackers compromises the domain controller				
Current Status:	Accenture completes forensic view of hacked documents; states LockBit's claims are false				
Key Stats		Attacker Profile		Moving Forward	
\$50M	Amount demanded by LockBit 2.0 to return company data	<div>Background</div> <div>"Crypto Virus" Ransomware as a Service (RaaS) Founded September 2019</div>	<div>Breach Victims</div> <div>Software and Services</div> <div>Professional Services</div> <div>Transportation</div> <div>Manufacturing</div>	<div>Operations</div> <div>1) Exploit weaknesses in a network</div> <div>2) Infiltrate deeper to complete attack</div> <div>3) Deploy the encryption payload</div> <div>After the attack, the victim may choose to contact LockBit and pay the ransom</div>	<div>Company</div> <div></div> <div>Accenture's existing clients will likely be more cautious working with the firm</div> <div>Accenture will continue to increase investments in Cybersecurity and intelligence</div>
2,000	Number of stolen files leaked to the dark web for a few minutes	<div>3rd</div> <div>Largest RaaS by Earnings</div>			<div>Stats</div> <div></div> <div>49% of companies reported their Cybersecurity strategy is fully implemented across their organization</div> <div>40% of businesses that suffered a breach lost some business opportunities</div> <div>29% of respondents stated their companies were forced to remove jobs following a ransomware attack</div>
6	Terabytes of data stolen by LockBit 2.0	<div>7.5%</div> <div>Ransomware Market Share</div>			
		<div>\$85K</div> <div>Average Ransom Amount</div>			

Ransomware Attack Sets New Mark

REvil Attack On Kaseya Ends With \$70M Ransom Demand And Thousands Of Companies Breached.



Kaseya Breach Overview		Key Takeaways	
Kaseya		REvil Attacker Profile & Activity	
Company Description:	Provider of IT Management Software to MSPs and IT Teams to improve efficiency and security	<div>Background</div> <div>Attack Model</div> <div>Disappearance</div>	Current Implications
Company Location:	Miami, FL		Rising Ransoms
Date Announced:	July 2, 2021		RaaS Attacks Grow
Breach Profile:	Ransomware-As-A-Service (RaaS) Attack Carried Out By Cybercrime Organization REvil		US Response to Russian Interference
How It Happened:	Highly Sophisticated "Zero Day" Attack That Targeted Kaseya's virtual systems/server administrator (VSA)		
Current Status:	Unconfirmed As Of Publication		
Contextualizing The Attack		Forward-Thinking Ransomware Prevention	
Cyber Expert Commentary		Key Stats	
<div></div> <div></div>	"They [REvil] are among the top in terms of ransom sums, big game hunters and typically try to ask for ransom amounts in the millions, based on the data they are able to exfiltrate and the size of the organization." – John Martineau, Consultant, Palo Alto Networks	\$70M	Amount demanded by REvil to decrypt Kaseya's data
	"This attack is a lot bigger than they expected and it is getting a lot of attention. It is in REvil's interest to end it quickly." – Allan Liska, Analyst, Recorded Future	70%	Percentage Of Affected Customers That Are MSPs Using Hacked Software To Manage Down-Stream Customers' Applications
		1,500	Number Of Total Businesses Potentially Affected By The Attack
		<div></div> <div>Focus on Zero-Trust</div>	<ul style="list-style-type: none">Everything trying to connect to a company's systems must be verified before granting accessHelps to prevent singular breaches and network-wide attacks
		<div></div> <div>Offline Backup Plan</div>	<ul style="list-style-type: none">In order to combat a large-scale breach, companies should create a plan for backing up data.Back-ups should be tested, encrypted, and have a copy stored off-site with a unique digital key
		<div></div> <div>Security Awareness</div>	<ul style="list-style-type: none">Employees should be trained on common phishing techniques in order to reduce the chances of breaches involving human error

Ransomware Attacks Continue To Be A Prevalent Threat

Attackers Are Accelerating Their Efforts To Extort Money From Vulnerable Institutions.



Accellion Breach Overview

Attacker Profile

Identity

Threat actors with connections to FIN11, the financial crimes group, and Clop, the ransomware gang

Method

Utilized email threats to extorts money from impacted organizations

Point of Entry

Zero-Day vulnerabilities in Accellion's legacy File Transfer Appliance (FTA)

Targets

Legacy FTA customers

Timeline Of Key Events

Jan 20, 2021	Accellion was exploited for the first time without any knowledge
Jan 22, 2021	Accellion learnt of exploit through multiple customer service inquiries
Jan 22, 2021 (cont.)	Accellion issued a critical security alert advising FTA customers to shut down their FTA systems
Jan 22-25, 2021	Accellion identified Server-Side Request Forgery and OS Command Execution vulnerabilities
Jan 25, 2021	Accellion released patch FTA 9.12.416 which remediates vulnerabilities
Jan 28, 2021	Accellion increased the frequency of anomaly detector checks to every 10 minutes

Aftermath

Large Scale Effects

- Attack affected more than 3,000 organizations, including government agencies, hospitals, and schools
- Additional victims are still coming out more than six months after the attack occurred

Costly Response

- The average breach costs \$4 million
- At least 14 lawsuits seeking class-action status have been filed against Accellion in the wake of the breaches and its outdated systems

Impacted Organizations

Ireland's Health System Breach Overview

Irish Health Service Executive

Background

Date

May 14th, 2021

Overview

Forced to shut down major technology systems belonging to Ireland's health system after receiving a ransomware attack, causing disruption at hospitals and COVID-19 testing centers

Method

Implemented CONTI ransomware which immediately connects to computers on the network and spreads malware

Aftermath

Nationwide Delays

Severely affected x-rays and negated the ability for individuals to make new online appointments to receive COVID-19 tests nationwide, causing delays and unforeseen interruptions

Broader Implications

Highlights the concerning advancement of ransomware capabilities as this is the first cyber attack to disable a country's centralized health system during the COVID-19 pandemic

Road to Recovery

Recovery will rely on a variety of factors including access to backup data, security of private records, and the integrity of the data available

AXA Insurance Company Breach Overview

AXA Insurance Company

Background

Targets

IT operations in in Asia

Impact

Stole 3TB of patient data, including passport copies and medical records

Method

Implemented Avaddon ransomware which launched a DDoS attack

Commentary

"Ransomware and targeted breaches are a threat to all organizations and can be extremely difficult to protect against." – **Martin Jartelius, CSO, Outpost 24**

Solutions To Deter Data Breaches

Endpoint Protection

Network Security Review

Identity Access Management

Multi-Factor Authentication

Third-Party Risk Management Program

Employee Education & Training

Source: Company Press Releases, Public Press Releases, Fireeye: [Accellion Breach](#), Kroger: [Accellion Incident](#), NYTimes: [Irish Health System Breach](#), Security Magazine: [AXA Ransomware Attack](#)

[Return To Table Of Contents](#)

102

International Meat Supplier Attack:

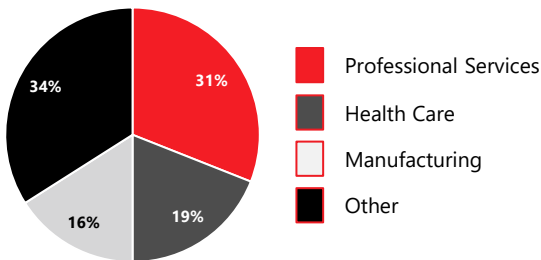


REvil Continues String Of Attacks With Shutdown Of A Quarter Of US Meat Supply And \$11M Ransomware Payout.

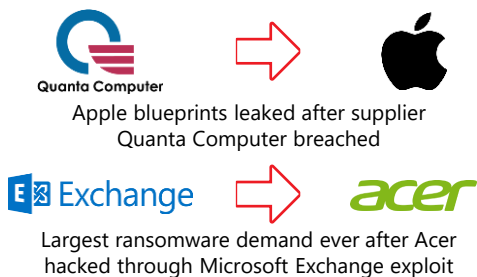
REvil | Attacker Profile

After breaching the system using leaked employee credentials in February, REvil began exfiltrating data from March 1st to May 29th. The attackers encrypted the environment on June 1st with over 5 terabytes of stolen data and were eventually paid an \$11M ransom.

REvil Historically Targeted Sectors



Other Notable REvil Breaches



Poor Security Hygiene In The Food Industry Is Enabling Adversaries To Capitalize



>20%

of food companies are hosting a CVE in their exposed Internet assets



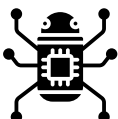
2,400+

food company IPs communicating with malware sinkholes



360+

food companies suffered a breach and / or attack



2,500

food industry assets exploited by ransomware on the Internet

Future Challenges For The Food Industry



Consolidation

- Highly consolidated industries such as food will continue to attract potential attackers
- High consolidation necessitates stronger defenses as breaches will have greater impacts as seen by the JBS hack halting 23% of US meat supply production



Shifting Sector Focus

- Improved security measures in other industries discourages attackers who will shift their sights to industries with less sophisticated Cybersecurity infrastructure
- Limited Cybersecurity regulations in food emboldens adversaries to capitalize



Rising Scale of Attacks

- Organized cybercriminals are targeting large supply-chain business evidenced by recent disruptions in food and oil
- As targets have increased in size, the average ransomware demand has also increased 43% since the start of 2021

Ransomware Prevention Mechanisms



Cybersecurity IR Planning

- JBS audit in 2018 discovered weaknesses that were not addressed
- Over 77% of businesses lack a Cybersecurity Incident Response Plan



Zero-Trust Architecture

- All users must provide verification before accessing any controls
- Prevents singular breaches and network-wide attacks



Cloud Security Access Broker

- Adds extra layer of security between enterprises and cloud providers
- Manages policy enforcement for an organization's cloud infrastructure



Awareness & Training

- Raising awareness about ransomware is a baseline security measure
- 95% of cybersecurity breaches are caused by human error

Cyber Attack Against U.S. Critical Infrastructure:
DarkSide Demands \$4.4M From The Colonial Pipeline Company Following A Double-Extortion Ransomware Attack.

Colonial Pipeline Company

Colonial Pipeline | Incident Overview

Company Description:

Refined Petroleum Products Transportation Company

Company Location:

Alpharetta, Georgia

Date Announced:

May 7, 2021

Threat Actor:

DarkSide

Type Of Breach:

Double-Extortion Ransomware Attack

How It Happened:

VPN without 2FA was accessed through a leaked password found on the dark web

Key Stats

\$4.4M

demanded as ransom for the decryption of Colonial Pipeline’s data; **\$2.8M** was later seized by the FBI who held the bitcoin **private keys**

~45%

of **all fuel** provided to the East Coast of the United States was cut off while in transport

12 Hours

elapsed before CEO Joe Blount decided to pay the ransom for the **decryption tool** enabling Colonial Pipeline to resume operations

Attacker Profile | DarkSide

Background

DarkSide is a Russian hacker group that was founded in August 2020. DarkSide sells Ransomware-as-a-Service to other groups and takes a fee of the ransom. The group claims that they are not political and only want to make money, and even have a list of acceptable targets.

Method

DarkSide uses double extortion ransomware which involves finding a weak entry point into a network and stealing sensitive files to leak. DarkSide then laterally moves to the domain controllers where they can distribute ransomware throughout an entire network and disable any data backups.

DarkSide Business Model

50% of the 100 attacks resulted in a ransom payment

~80% of each ransom payment goes to DarkSide Affiliates

The DarkSide RaaS model is run like a **business model**. DarkSide only takes a small portion of each ransom while their affiliates that spearhead the attacks take anywhere from **75% - 90%** of the total profits.

DarkSide Developer

17.2%

\$15.5M

DarkSide Affiliates

82.8%

\$74.7M

Key Takeaways

Ransomware Growth

62%

Global ransomware growth from 2019 through 2021

158%

Growth in ransomware usage in North America

268,362

New malware variants were discovered in 2020

Double Extortion Defenses

Penetration Testing

Simulating attacks will highlight network vulnerabilities and enable CISOs to proactively defend organizations from threats

Continuous Monitoring

Monitoring network data logs can produce a window of opportunity to detect and stop a primary infection before it spreads

Backup Capabilities

Employing robust backup plans can ensure that business continuity is saved in the event of entire network encryptions

Source: [Technology Review](#); [CNBC](#); [Bank of InfoSecurity](#); [Security Magazine](#); [Computer Weekly](#); [Gemini Advisory](#); [ThreatPost](#); [Colonial Website](#).

Return To Table Of Contents

104

The Largest Ransomware Demand In History: **acer**

REvil Demands \$50M From Acer In Double-Extortion Ransomware Attack On Microsoft Exchange Vulnerabilities.

Acer | Incident Overview



Company Description:	Advanced Electronics Company & Global PC Market Leader With \$2.5B Market Cap
Company Location:	New Taipei City, Taiwan
Date Announced:	March 18, 2021
Breach Profile:	Double-Extortion Ransomware Attack Carried Out By Cybercrime Organization REvil
How It Happened:	Exploitation of Zero-Day Microsoft Exchange Vulnerabilities
Current Status:	Ongoing As Of Publication

Key Stats

\$50M	Amount demanded by REvil to decrypt Acer's data, the largest ransomware demand in history
2 Weeks	Time from negotiation that Acer has to pay \$50M, after which the ransom will increase to \$100M
21M	Number of PCs that Acer shipped out in 2020, representing a massive threat if REvil chooses to carry out a supply chain attack

Contextualizing The Breach

Cyber Expert Commentary



"Targeted ransomware actors like REvil will see this as a particular boon as the many bespoke steps of an attack can be short-circuited with a direct attack on an organization's Exchange server."
– **Oliver Tavakoli, CTO, Vectra**



"The large demand suggests that REvil likely exfiltrated information that is highly confidential, or information that could be used to launch Cyberattacks on Acer's customers."
– **Ivan Righi, Cyber Threat Intelligence Analyst, Digital Shadows**



"Attackers who saw the payoff from these supply chain attacks left a gap where ransomware operators have more available attack surface, meaning ransomware will become a bull market again."
– **Brandon Hoffman, CISO, Netenrich**



"Ransomware is just another type of malware. It's very important to employ multiple layers of security and monitoring controls in your environment to help prevent this type of exposure."
– **Brent Johnson, CISO, Bluefin**

Attacker Profile



Background

Private Ransomware as a Service (RaaS) Organization
Founded In April 2019

\$81M

Profit In 2020

33%

Ransomware Involves REvil

\$1M

Spent In 2020 On Expansion



Breadth

140

Organizations Attacked Across



Wholesale



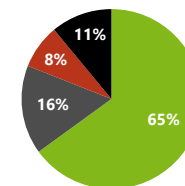
Professional Services



Manufacturing



Attack Vectors



- RDP Sessions
- Phishing
- Software
- Other

Key Takeaways

Current Implications



Rising Ransoms

- REvil's enormous ransom indicates even higher and more high-profile ransoms are in store
- Acer's response will set a precedent for future breaches and demands



Microsoft Exchange

- Microsoft Exchange vulnerabilities have led to exploits on **30,000+** U.S. organizations
- It took only weeks for this particular Microsoft Exchange hack to arise and be used on the high-profile Acer



Double Extortion Attacks

- Ransomware attacks are shifting from data encryption to data exfiltration
- More than **1,000** companies had their data leaked from not paying ransomware demands in 2020 alone



Ransomware as a Service

- 2 out of 3** ransomware attacks are Ransomware as a Service (RaaS)
- RaaS demand is increasing, and **15** new affiliates emerged in 2020 alone
- RaaS allows anyone who can pay to access Cybercrime technology

Forward-Thinking Prevention



Privileged Access

- Privileged access abuse continues to be a primary route for ransomware breaches
- Organizations should seek a PAM solution and ensure their data is properly access-controlled and encrypted



Multilayer Networks

- To reduce human error and increase visibility during a breach, organizations should implement a multilayer network infrastructure with various security checks
















Security Awareness

- Human error is still a primary security concern, causing **90%** of successful breaches
- Employees should actively recognize unusual behavior, such as data transfer events during odd hours

Municipal Water Treatment Attack: **OLDSMAR** FL

Threat Actors Leveraged TeamViewer To Access A Water Treatment Plant's Controls To Modify Lye Concentration.

Bruce T. Haddock Water Treatment Plant Incident Overview		IT / OT Security Issues & Recommended Remediation	
Background	Attacker Profile & Methodology	Industry Challenges	Why Cybersecurity In Infrastructure Matters
<p>Assumed Motive: Poison the town residents by raising the lye content of water from 100 ppm to 11,100 ppm</p> <p>Point of Entry: Identical User Passwords / TeamViewer VM</p> <p>Target: OLDSMAR FL Bruce T. Haddock Water Treatment Plant</p>	<p> Attacker Profile</p> <ul style="list-style-type: none">Unidentified individual / group using noisy & haphazard techniques which points to a less sophisticated actorThere is not enough information to identify who caused the attack, but FBI and Secret Service are still investigating <p> Assumed Motives</p> <ul style="list-style-type: none">Full attack rationale is unknown; the actions during the attack point to a deadly intentContaminate Oldsmar, Florida's water supply, poisoning residents and disabling the water treatment plant <p> Method</p> <ul style="list-style-type: none">Connected to the SCADA system, which was accessible through a single password used by all employeesLeveraged TeamViewer to access system controls and manipulate lye content to extreme levels <p> Potential Ramifications</p> <ul style="list-style-type: none">Could act as a catalyst for other threat actors to target infrastructure with weak security measuresDemonstrates the ease at which some pieces of infrastructure can be breached and manipulated <p>Avoided Fallout</p> <p>Lye, or sodium hydroxide, is a caustic substance and can cause chemical burns to the skin or internal corrosive damage if ingested</p> <p>If the concentration change had gone undetected, it could have resulted in the mass poisoning of Oldsmar, a town of 15,000 people</p>	<p> The OT space faces increasing vulnerabilities through the convergence of IT & OT environments, compromising the traditional security of the air gap technique used to isolate separate domains</p> <p> 2,000% Increase in OT attacks from 2019 to 2020</p> <p> 90% organizations experienced at least one OT system intrusion in 2020</p> <p>33% Of OT attacks in 2020 were committed via Ransomware</p> <p>15% Of OT attacks in 2020 were attributed to Remote Access Trojans (RAT)</p>	<p> SCADA Breaches</p> <p>Recently, threat actors have been distributing access to SCADA and ICS systems on dark web markets, which are increasingly vulnerable to attacks</p> <p> Digital Transition</p> <p>It is expected that the number of internet connected devices will double through 2025 increasing the attack surface for critical infrastructure</p> <p> Debilitating Outcomes</p> <p>The potential consequences of a successful attack on critical infrastructure could disrupt other essential systems and entire industries</p> <p>Infrastructure Security Best Practices</p> <p> VPN & Firewall</p> <p>Enable bidirectional communication between IT & OT environments, best deployed in a demilitarized zone for a secured and regulated access protocol</p> <p> Network Segregation</p> <p>Ensure employees are extended access to only the systems they need, and place systems on separate networks with privileged access</p> <p> Unidirectional Gateways</p> <p>Extract & send key information, while preventing inbound communication from OT environments without opening critical systems to unwanted infiltration</p>

2022 Conferences & Events



Major Industry Conferences | 2022

Momentum Cyber Will Be Attending & Speaking At A Number Of Cybersecurity Conferences Worldwide.

 San Francisco & Digital February 7 – 10 Jun. 6 - 9, 2022	<ul style="list-style-type: none">▪ RSA Conference provides an opportunity to learn from 42,000+ attendees about new approaches to information security, discover the latest technologies, and interact with top security leaders and pioneers		<ul style="list-style-type: none">▪ Black Hat is the world's leading information security event. For more than 20 years, it has provided 17,000+ annual attendees with the very latest in information security research, development, and trends in a strictly vendor-neutral environment
	<ul style="list-style-type: none">▪ Infosecurity Europe is the region's number one information security event featuring over 400 exhibitors showcasing the most relevant information security solutions and products to 19,500+ information security professionals		<ul style="list-style-type: none">▪ Cyber Week, hosted by Tel Aviv University in Israel, offers a unique gathering of Cybersecurity experts, industry leaders, startups, investors, academics, diplomats, and government officials
	<ul style="list-style-type: none">▪ CyberUK is the authoritative event for the UK's Cybersecurity community attended by 2,500+ delegates. The event features content themed around key emerging issues: the fast-evolving technology landscape, and threat & national resilience		<ul style="list-style-type: none">▪ DefCon is one of the oldest and largest continuously running hacker conventions around. The event consists of several tracks of speakers about computer and hacking related subjects, as well as Cybersecurity challenges and competitions
	<ul style="list-style-type: none">▪ SANS 2022 attracts 1,200+ Cybersecurity professionals who are looking to improve their security systems against the most dangerous threats. SANS provides practical training that addresses the challenges security professionals face daily		<ul style="list-style-type: none">▪ Gartner Security & Risk Management Summit provides attendees with proven practices and strategies needed to maintain cost-effective security and risk programs to support digital businesses

RSA®Conference | Innovation Program for Start-Ups

High-Value Platform For Companies To Showcase The New Ways They Are Tackling Present & Future Cybersecurity Issues.

RSA Conference 2022 Innovation Programs Overview

RSA®Conference2022
San Francisco & Digital | June 6 – 9

Behind every great Cybersecurity company is a stroke of genius that started it all. When it comes to getting those ideas off the ground, there's no better place than RSA Conference. RSAC Early Stage Expo and RSAC Innovation Sandbox Contest are part of the RSA Conference Innovation Programs, which present an opportunity for start-up companies to compete in and showcase their brilliant industry solutions.

[Click here to learn more about the RSAC Innovation Programs.](#)

RSAC Innovation Sandbox Contest | Monday, June 6, 2022

The **RSAC Innovation Sandbox Contest** brings out cybersecurity's boldest new innovators who have made it their mission to minimize risk. Each year, 10 finalists grab the spotlight for a three-minute pitch while demonstrating groundbreaking security technologies to the broader RSA Conference community.

Event Details

RSA Conference 2022 Full Conference Pass and Expo Plus Pass holders can watch this event live on **Monday, June 6 at 12:00 PM PT.**

Moderator



Hugh Thompson
RSA Conference
Program Committee
Chair

Judges Panel



Dorit Dor
Check Point
SOFTWARE TECHNOLOGIES LTD.



Niloofar Howe
e-
ENERGY IMPACT PARTNERS



Paul Kocher
Independent
Researcher



Shlomo Kramer
CATO
NETWORKS



Christopher Young
Microsoft

RSAC 2022 Top 10 Innovation Sandbox Contest Finalists

The lucky top 10 finalists will be announced early May 2022.

RSAC Early Stage Expo | June 8 – 9, 2022

The **RSA Conference Early Stage Expo** is an innovation space dedicated to promoting up-and-comers in the industry. With emerging talent at every kiosk, this is an opportunity to meet 30 of the industry's most promising newcomers. Learn about their innovative products and solutions by visiting their kiosks or sitting in on a short demo at the Early Stage Expo Briefing Center.

Event Details



RSA Conference 2022 Full Conference Pass, Expo Plus Pass, and Expo Pass holders can access the RSAC Early Stage Expo on Wednesday, June 8 and Thursday, June 9.

RSAC 2022 Early Stage Expo Participants



Explore the **RSAC Early Stage Expo participants** you'll find at RSAC 2022.

Registration Information



[Click here to register for RSA Conference 2022.](#)

Past Conferences & Events



Advancing Cybersecurity In The Global Health Sector

In Person Summit Discussing Information Regarding Preventing Cybersecurity Attacks On The Health Sector.

Selected Sessions

Segmenting OT Systems in a Cloud First World

This panel-style presentation by Booz Allen and a Top-5 Global Pharma client will provide the audience with real-world examples of how Next-Generation Cyber Operations are being built to meet the challenge of global coverage and around-the-clock protection. From 24x7 Tier1 through Tier 3 IR triage, to strategies for OT detect & response, to building, testing and maintaining crisis response capabilities from factories to board rooms.

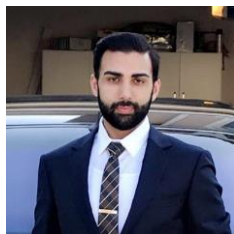
Software Build and Distribution Threat Model

Threat models are used to systematically identify Cybersecurity weaknesses in products as well as processes. Supply-chain activities such as software build and distribution can be critical attack vectors for the Cybersecurity of a product. This presentation will demonstrate application of threat modeling to a mobile application build and distribution process using the STRIDE methodology.

Selected Session Speakers



Karthikeyan Bose
Associate Director
Organon



Omar Sheikh
Sr. Software Developer
Medtronic



Myles Wright-Walker
Security Engineer
Medtronic

2021 Health – ISAC Fall Summit Overview

About Health - ISAC

Health – ISAC is a trusted community of critical infrastructure owners and operators within the Healthcare and Public Health sector. The community is primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities.

Session Highlights



Data Sources Logs Prioritization



Financial Exposure: The Common Language of Cyber Risk



Mobile Messaging Apps and Retention Policy



Symbiotic Vulnerability Management & Response



Modernization of Security Operations



The Ethics of Analytics



Government Response to Ransomware



Networking Breaks

Gartner | Enabling Innovation: Secure The Future While Managing Risks








Virtual Summit Providing Valuable Insights On New Complexities And Risks Brought By Accelerating Digital Innovation.

Gartner Security & Risk Management Summit Overview



16-18 NOV. 2021
VIRTUAL SUMMIT

Whether its a chief information security officer (CISO) looking to improve his or her leadership skills, a security professional who needs practical advice to accelerate progress on their next initiative or a risk management leader trying to optimize the value of risk management investment, anybody will find their program, peers and strategic partners at this virtual conference.

Summit Coverage Topics				Agenda / Track				
	Advanced Threat Protection		Application Security					
	Cloud Security		Cybersecurity	CISO Circle	Management & Leadership	Digital Risk Management	Security Technology & Architecture	Infrastructure Protection Strategies
	Data Security		Identity and Access Management					
	Risk Management		Vulnerability Management	Business Enablement	Market Dynamic & Evolution	Technical Insights: Architecture	Midsize Enterprise	Diversity, Equity and Inclusion

Featured Gartner Experts						
						
Jeffrey Wheatman VP, Advisory Gartner	Patrick Hevesi VP, Analyst Gartner	Katell Thielemann VP, Analyst Gartner	Roberta Witty VP, Analyst Gartner	Zaira Pirzada Principal, Advisory Gartner	Neil MacDonald Distinguished VP, Analyst Gartner	Jay Heiser VP, Analyst Gartner

Sources: Gartner Website.

Protecting Energy Through Cybersecurity

Hybrid Platform Providing Attendees With Insightful Conversations, Best Practices, & Innovative Ideas Against Risks.

2021 API Conference Overview

For 16 years, the Annual API Cybersecurity Conference has been the only Cybersecurity conference dedicated to the oil and natural gas industry and has a loyal and dedicated attendee base. It is also volunteer-driven, both at the planning committee and speaker level. The API Conference has consistently produced a compelling program, with a focus on safety, best practices, and innovation.

API 2021 Conference Program

	Regulatory Panel		Legal Panel		CIO Panel
	CISO Panel		API Cybersecurity Update		Pandemic Response Track
	Cybersecurity Programs		ICS Security: Collaboration, Standards, and Models		Next Generation SOC / Security Orchestration
	Governance, Board Communications, Risk Management		Application Security and SecDevOps		Threat Intelligence Sharing
	Cybersecurity Architecture		Emerging / Recent Threats		Cybersecurity Policy and Law
	Industrial Internet of Things Including Edge Computing		Incident Response Management		Supply Chain

2021 Cybersecurity Conference Sponsors



Keynote Speaker



Robert M. Lee is a recognized pioneer in the industrial security incident response and threat intelligence community. He gained his start in security as a US Air Force Cyber Warfare Operations Officer tasked to the National Security Agency where he built a first-of-its-kind mission identifying and analyzing national threats to industrial infrastructure. He went on to build the industrial community's first dedicated monitoring and incident response class at the SANS Institute (ICS515) and the industry recognized cyber threat intelligence course (FOR578).

| Defending The New Normal

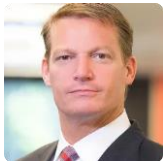
Hybrid Platform Providing Attendees With Insightful Conversations, Best Practices, & Innovative Ideas Against Risks.

Cyber Defense Summit 2021 Overview

Mandiant's 2021 Cyber Defense Summit is held from October 5-7, with a focus on defending the new normal in Cybersecurity as the industry moves towards remote working and remote learning, as well as increased reliance on the cloud. The summit is held as a hybrid event, both in-person and virtual, and features an agenda allowing Cybersecurity professionals to hold insightful conversations, as well as discuss best practices and innovative ideas that can help protect against today's threats and tomorrow's risks.

Event Agenda

Select Speakers



Kevin Mandia
CEO,
Mandiant



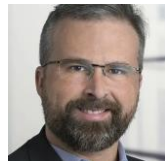
Sue Gordon
Former Principal Deputy Director of
National Intelligence, US



Christopher Krebs
Former Director, CISA, Dept. of
Homeland Security



Sara Andrews
SVP & CISO,
PepsiCo



Matthew Byrne
Senior Manager Threat Intelligence,
PwC



Raymond Canzanese
Director of Threat Research,
Netskope

Breakout Session Tracks

Executive Track

- Business-level view into critical cyber security topics
- Targeted for executives, managers, board of directors, and lawyers and what they need to know about Cybersecurity

Mandiant Solutions Track

- Mandiant in real-world security environments
- Focused on how Mandiant solutions are used on the front lines of Cybersecurity

Technical Track

- Real-world intrusion scenarios at a technical level.
- Targeted for security practitioners and what they need to know to mitigate, detect, and respond to Cyber attacks.

FireEye Solutions Track

- FireEye in real-world security environments
- Focused on how FireEye solutions are used on the front lines of Cybersecurity

Enabling A Secure Future In Cybersecurity

Virtual-Only Platform Hosting Senior Experts To Discuss The Cybersecurity & Cloud Ecosystem.

Cybersecurity & Cloud Congress 2021 Overview



Presented by TechEx, the North America Cyber Security & Cloud Congress 2021 is hosted virtually on the 29-30 September, covering two days of top-level content and thought leadership discussions looking at the Cyber Security & Cloud ecosystem. The event focuses on a series of top-level keynotes, interactive panel discussions and solution-based case studies with a focus on learning and building partnerships in the emerging cyber security and cloud space.

Event Agenda

Day 1: Enterprise Security

- Focused on security strategy for the modern enterprise
- Events center around Network & Infrastructure, Building a SecOps Team, Incident Response, SASE, Cloud Security, Data Security, and IoT Security

Day 2: Privacy & Data

- Focused on secure development for the agile enterprise
- Events center around Future-proofing, Digital Transformation, Resilience, Application Security, SDLC Security, and Data-Centric Cloud Security

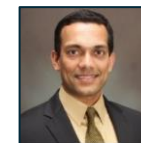
Select Speakers



Manish Gupta
Director, Global Cyber Services



Kurt John
Chief Cybersecurity Officer



Sujeet Bambawale
CISO



Doug Glair
Principal Consultant, NA



Hillery Hunter
VP & CTO, IBM Cloud



Event Stats

5000+

Attendees

63%

Speakers at
Director-Level+

21

Conference Tracks

250+

Speakers

Select Partners & Sponsors

anJUNA

(ISC)²

digital element

ProcessUnity

FRSECURE

RedTeam
SECURITY CONSULTING

IBM

skyflow

Acclaimed International Cybersecurity Event

Platform Providing Expert-Driven Content, High-Level Networking, And The World's Best Cybersecurity Speakers.

Cyber Week 2021 Overview

Cyber Week 2021, hosted by Tel Aviv University in Israel, offers a unique gathering of Cybersecurity experts, industry leaders, startups, investors, academics, diplomats, and government officials. The event in 2021 was hosted in a hybrid format, with opportunities for local and online audiences to attend.

Select Cyber Week Programs



Jonathan Fischbein
Global CISO,
Check Point

The CISO Flix



David Warshavski
VP Enterprise Security,
Sygnia

Attack from Hell: A View From the Frontlines of a Heavyweight Ransomware Extortion Attack



Yigal Unna
Director General,
Israel National Cyber Directorate

2021 and Beyond, Threats and Opportunities



Maty Siman
Founder & CTO,
Checkmarx

Appsec is More than Application Security

Select Speakers



Naftali Bennett
Prime Minister



Wendy Nather
Head, Advisory CISO Team



Ofer Schreiber
Partner



YL VENTURES



Ubi Mokady
Co-Founder, CEO



CYBERARK



Flavio Aggio
CISO



World Health Organization

Cyber Week Resources Overview

Event Highlights



Connect

Interact with Cybersecurity peers, investors, and decision makers



Learn

Hear from international trail-blazers about Cyber's best practices and game changing ideas



Discover

Unearth some of the latest technology and Cyber solutions for organizations

Cyber Week Hot Topics



Ransomware



Cyber & COVID-19



Cloud Security



Secure Supply Chains



FraudCon



BSides



Maritime Security



Aviation



Critical Infrastructure



Startups



Intl. Collaboration



Policy & Regulation

blackhat® | Convening Modern Information Security

Comprehensive Platform For Industry Leaders And New Players To Sync On InfoSec Trends & Developments.

Black Hat Conference 2021 Overview



JULY 31 - AUGUST 5, 2021

INFOSEC
KNOWLEDGE & NETWORKS

The annual Black Hat Conference convenes InfoSec experts from around the world to share their latest findings, open-source tools, zero-day exploits, and other cutting-edge research on information security risks & trends. Additionally, the conference provides hands-on offensive and defensive skill-building opportunities for InfoSec as well as information on various current events.

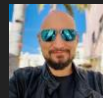
Briefings, Research, & Trainings

Black Hat **Briefings** provide Cybersecurity professionals with the latest in information security risks, research, and trends. Security experts present research on topics ranging from vulnerabilities within popular consumer devices, to critical infrastructure threats, and everything in between.

Black Hat's **Research Arsenal** is a space for independent researchers and developers to showcase their latest open-source tools and products. Participants are introduced to new tools that strengthen their security toolkits.

Black Hat **Trainings** offer attendees technical hands-on courses on a vast array of attack and defense InfoSec topics. These courses are led by global security experts with the goal of defining and defending tomorrow's InfoSec landscape.

Keynote Speakers



Safeguarding
UEFI Ecosystem

Alexander
Matrosov, Nvidia



Next-Gen DFIR

Sherri Davidoff,
LMG Security

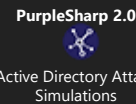
Notable Products



Cloud Security
Operations Platform

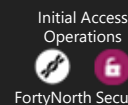


Zero Infrastructure
Password Cracking



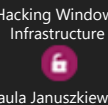
Active Directory Attack
Simulations

Prominent Courses



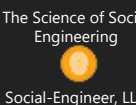
Initial Access
Operations

FortyNorth Security



Hacking Windows
Infrastructure

Paula Januszkiewicz



The Science of Social
Engineering

Social-Engineer, LLC

Key Topics Represented



Business Hall

Black Hat's Business Hall allows attendees to network with **security experts**, **cutting-edge researchers**, and InfoSec's **leading solution providers**. The Business Hall includes sponsored sessions and events by major security players, as well as the ability to discover new open-source tools at **Arsenal** sessions.

Contests



Participants compete in a virtual jeopardy-style capture the flag event. Competitors will use LogRhythm Web UI, alarms, and investigations to find answers to the questions.



Sponsored Sessions



Scholarships



Black Hat Student Scholarship



Black Hat Veteran's Scholarship



EWf Women In Security
Scholarship

| Ensuring A Secure Supply Chain Network

Platform That Provides Companies With Case Studies On Third-Party Cybersecurity Implementation Practices.

Third-Party & Supply Chain Cybersecurity Virtual Summit Overview



Led by the top information security professionals from leading companies, this summit provides attendees the opportunity to discover case studies on optimizing enterprise vendor risk management programs as well as embedding and reviewing Cybersecurity practices within the supply chain. Through this summit, participants will be able to understand the risks associated with third-party vendors from various perspectives, thereby enabling them to identify the right processes and solutions to implement in their own supply chains.

Summit Coverage Topics

 Technology Bifurcation & Supply Chain Compliance	 Measuring Cyber Risk of Vendor Ecosystems	 Residual Risk in Third-Party Cyber Risk Ratings	 The Future of Third-Party Risk Management	 Evaluation of Third-Party Security Resources & Standards
 Implementing Continuous Cyber Risk Monitoring	 Building Third-Party Risk Management Programs	 Effective Oversight to Mitigate Potential Risks	 Potential Risks of Shared Assessments	 Overview of IT Vendor Risk Management Tools
 Building a Functional Sourcing Model	 European Framework for Cybersecurity Risk Assessments	 Blockchain Technology in Supply Chain Security	 Risk Assessment of 5G Networks	 Evaluating and Auditing IT Security
 Practical Tools for Data Breach Response	 Cloud Security Challenges & Supply Chain Risks	 Third-Party Due Diligence at the Global Scale	 Insider Threats in Remote Environments	 Cyber Risks of IoT and AI Automation

Technology Partners



KB4-CON | KnowBe4's Fourth Annual Conference

Discussion Platform For Cybersecurity Experts To Increase Awareness Of Hacking Methods And Provide Insights For Defense.

KB4-CON 2021 Overview

KB4-Con is a Cybersecurity-focused event **designed for CISOs, security awareness training administrators, and InfoSec professionals** that promotes engagement across the industry and hosts over 11,000 participants.

Select Virtual Agenda Programs



Greg Kras
Chief Product Officer

2021 Product Roadmap: Looking To The Road Ahead



Roger Grimes
Data-Driven Defense Evangelist

Hacking Multifactor Authentication



Katie Brennan
Senior Director, Product Services

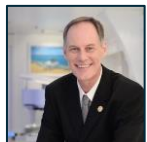
Live Bait – Phish Better Than The Bad Guys



Jason Kelley
VP, Product Support

Stronger Together: Partner Enablement Through Technical Training

Select Speakers



Stu Sjouwerman
Chief Executive Officer

KnowBe4

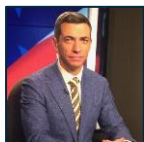


Kevin Mitnick
Chief Hacking Officer

KnowBe4



Theresa Payton
Former White House CISO & Author



Clint Watts
National Security Contributor



Keri Pearson
Executive Director of Cybersecurity



KB4-CON 2021 Resources Overview

Courseware Content



Security Culture and Assessments (SCS & SAPA)



Creating Hyper-Engagement through Deep Storytelling



eLearning for All: Inclusive Security Awareness Training



Benefits of Game-Based Learning



Security Awareness Training Planning and Deployment



Two Truths and a Lie About Your Compliance Program

IT Security Tools



Compliance Audit Readiness Assessment

Gauges an organization's readiness for Cybersecurity Maturity Model Certification (CMCC) audit



MFA Authentication Security Assessment

Helps organizations understand their MFA security readiness and identifies specific risks against MFA hacks



Domain Doppelganger

Identifies malicious domain twins and combines search, discovery, reporting, risk indicators, and end-user agreements with training



Phish Alert Button

Gives users safer and easier way to forward email threats to security team for analysis



Browser Password Inspector

Provides identification of users saving weak, reused, or old passwords



Weak Password Test

Checks organizations' Active Directory for 10 types of weak password-related threats

RSAConference | Innovation Program Start-Up Contests

A High-Value Platform For Companies To Showcase The Innovative Ways They Are Addressing Present & Future Cybersecurity Issues.

RSA Conference 2021 Innovation Programs Overview

RSAConference2021
May 17 – 20 | Virtual Experience



RSAC Innovation Sandbox RSAC Early Stage Expo

For 30 years, RSA Conference has helped organizations build an unshakable foundation of resilience to overcome the impact of events that threaten the way of progress. RSA Conference Innovation Sandbox Contest presents an opportunity for start-up companies to compete and showcase their brilliant industry solutions. Learn more about RSAC Innovation Programs [here](#).

RSAC 2021 Innovation Sandbox

RSAC Innovation Sandbox Contest puts the spotlight on Cybersecurity's boldest new innovators to compete with their potentially game-changing ideas. 10 finalists have 3 minutes to make their pitch to a panel of judges. Over the last 16 years, the top 10 finalists have collectively seen over 50 acquisitions and received \$5.2 billion in investments. To learn more from this year's RSAC Innovation Sandbox Contest, click [here](#).

RSAC 2021 Innovation Sandbox Winner



Apiiro is a leader within DevSecOps and risk visibility. Its Industry-first Code Risk Platform provides a 360-degree view of security and compliance risks across applications, infrastructure, developers' knowledge, and business impact from design to production.

HQ: Tel Aviv-Yafo, Israel

“ It's so hard to invent something completely new and get such recognition from the market, customers, and the industry-expert RSAC Innovation Sandbox judges. We are honored by this recognition. ”



Idan Plotnik
CEO

RSAC 2021 Top 10 Innovation Sandbox Contest Finalists



Past Winners



2020



2019



2018



2017



2016



2015

Moderator



Hugh Thompson
Program Committee
Chair
RSAConference

Judges Panel



Dorit Dor
VP, Products
Check Point
SOFTWARE TECHNOLOGIES LTD



Niloofer Howe
Principal &
Founder
RAZI VENTURES



Paul Kocher
Security Entrepreneur
& Researcher



Shlomo Kramer
Co-Founder & CEO
CATO
NETWORKS



Christopher Young
EVP, Bus Dev
Microsoft

RSAC 2021's Interactive Sandbox Experiences



**Aerospace
Sandbox**

Discover how aerospace companies are creating a secure environment



**AppSec
Sandbox**

Learn how to exploit & secure vulnerabilities from the best of the best



**Biohacking
Sandbox**

Find out how security research is developing solutions for healthcare



**ICS
Sandbox**

Engage with a curated hack on an industrial process using TTP



**IoT
Sandbox**

Uncover innovative techniques to hack and secure IoT devices



**Red Team
Sandbox**

A community of Red-Teaming and Adversarial attack simulation tactics



**SANS
NetWars**

Compete with peers in a cybersecurity challenge to enhance skills



**Supply
Chain Village**

Explore how to impact and manage cyber supply chain issues



VIII.






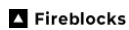


































INVESTOR SPOTLIGHT

RETURN
ON
INVESTMENT

ROI

Top Cybersecurity Investors Of 2021

Investors Continue To Capitalize On Investment Opportunities Across Specific Sectors.

Investor	Founded Date	HQ	No. of Cyber Investments	Recent Fund Size (\$M)	Highlighted Investments			Recent Sector Investments	
 INSIGHT PARTNERS	1995	New York, NY	31	\$9,542	 persona Series C	 Plume Series E	 WIZ Series C	<ul style="list-style-type: none"> Risk & Compliance Cloud Security 	<ul style="list-style-type: none"> Data Security Identity & Access Mgmt.
 SEQUOIA	1972	Menlo Park, CA	21	\$999	 Fireblocks Series E	 CERTIK Series B2	 SALT Series C	<ul style="list-style-type: none"> Cloud Security Endpoint Security 	<ul style="list-style-type: none"> Risk & Compliance Data Security
 Accel	1983	Palo Alto, CA	16	\$650	 Socure Series E	 netskope Series H	 snyk Series F	<ul style="list-style-type: none"> Cloud Security Data Security 	<ul style="list-style-type: none"> Network & Infra. Security Risk & Compliance
 TENELEVEN	2014	Burlingame, CA	16	\$175	 AURA Series F	 feedzai Series D	 ANCHORAGE DIGITAL Series C	<ul style="list-style-type: none"> Cloud Security Fraud & Transaction Security 	<ul style="list-style-type: none"> Identity & Access Mgmt. SecOps & Incident Response
 COATUE	1999	New York, NY	15	\$707	 panther Series B	 persona Series C	 Chainalysis Series E	<ul style="list-style-type: none"> Blockchain Cloud Security 	<ul style="list-style-type: none"> Application Security Identity & Access Mgmt.
 TIGERGLOBAL	2001	New York, NY	14	\$175	 Lacework Series D	 snyk Series F	 FORTER Series F	<ul style="list-style-type: none"> Fraud & Transaction Security Data Security 	<ul style="list-style-type: none"> Blockchain Application Security
 vertex VENTURES	2013	Palo Alto, CA	14	\$175	 ADAPTIVE SHIELD Series A	 SAYATA LABS Series A	 AXONIUS Series D	<ul style="list-style-type: none"> Risk & Compliance Data Security 	<ul style="list-style-type: none"> SecOps / IR / Threat Intel Digital Risk Management
 Lightspeed	2000	Menlo Park, CA	13	\$890	 noname Series C	 netskope Series H	 aqua Series E	<ul style="list-style-type: none"> Cloud Security Risk & Compliance 	<ul style="list-style-type: none"> Application Security Identity & Access Mgmt.
 GGVCAPITAL	2000	Menlo Park, CA	12	\$1,830	 torq Series B	 DRATA Series B	 ORCA security Series C	<ul style="list-style-type: none"> SecOps / IR / Threat Intel Data Security 	<ul style="list-style-type: none"> IoT Risk & Compliance
 ForgePoint CAPITAL	2015	San Mateo, CA	11	\$450	 noname Series C	 ermetic Series B	 HUNTRESS Series B	<ul style="list-style-type: none"> Data Security Identity & Access Mgmt. 	<ul style="list-style-type: none"> Application Security MSSP



IX.

TRANSACTION PROFILES

2021 Cybersecurity Initial Public Offerings



9,500,000 Shares



Common Stock

\$16.00 Per Share

\$152,000,000

April 22nd, 2021

57,376,000 Shares



Common Stock

\$3.45 Per Share

\$197,947,200

April 30th, 2021

14,800,000 Shares



Common Stock

\$35.00 Per Share

\$1,225,000,000

June 30th, 2021

17,500,000 Shares



Common Stock

\$21.00 Per Share

\$367,500,000

July 29th, 2021

11,000,000 Shares



Common Stock

\$25.00 Per Share

\$275,000,000

September 16th, 2021

Highlighted 2021 M&A Transactions



2021 M&A Snapshot

\$77.5B
Deal Volume



286
Transactions



**Security
Consulting**
was the most
active sector



Deal Volume
in 2021
increased
295% YoY



Highlighted 2021 Financing Transactions



2021 Financing Snapshot





MOMENTUM CYBERSECURITY GROUP, LLC
101 2nd Street, Suite 1275, San Francisco, California 94105
8601 Ranch Road 2222, Building 1, Suite 290, Austin, TX 78730

For Inquiries Or Information On The Cybersecurity Almanac Please Contact Momentum Cyber at: almanac@momentumcyber.com
Securities transactions offered through Momentum Capital Markets, LLC, Member FINRA and SIPC