



Houlihan Lokey



Cybersecurity Quarterly Update

FIRST QUARTER 2023

Global Cybersecurity Team

U.S. Cyber Team



Keith Skirbe
Managing Director
Co-Head of U.S. Cyber
San Francisco



Bobby Wolfe
Director
Co-Head of U.S. Cyber
Miami



Tyler Deck
Vice President
Boston



Mark Smith
Director
Head of U.K. Cyber
U.K.



Malte Abrams
Managing Director
Head of DACH Cyber
Frankfurt



Sara Napolitano
Managing Director
Head of France Cyber
Paris



Ido Zakai
Managing Director
Head of Tech, Israel
Tel Aviv



Rishabh Bansal
Associate
San Francisco



Patrick Wong
Financial Analyst
San Francisco



Duncan Webber
Financial Analyst
New York



Gabrielle Worrall
Vice President
U.K.



Christie Adams
Financial Analyst
Paris



Samuel Pattison
Financial Analyst
U.K.

Capital Markets



Sean Fitzgerald
Managing Director
New York



Chris Hebble
Managing Director
Los Angeles

Global Cyber Reach

Financial Sponsors

20+

Senior Bankers
Covering

~1,400

Investors

Cybersecurity Technology Expertise



Stephen Lee
Tech and Cyber Due Diligence
Chicago



Edouard Viot
Cybersecurity Consultant
Paris

Executive Summary: Q1 2023 in Review

- The market slowdown continued with M&A and financing volume down YoY, reaching Q1 levels not seen since pre-pandemic
- This downtick can be attributed to the current macroeconomic environment and high interest rates, which have made it challenging for companies to secure funding and engage in M&A activity, especially after the collapse of prominent banks such as SVB
- Given the growing importance of cybersecurity, we anticipate activity to pick up in 2H 2023, driven by a rationalization of valuations, a build-up of dry powder from PEs/VCs, and strategics looking to be opportunistic

Q1 2023 Report Themes



Cyber storage is crucial in today's digital landscape where the risk of cyber attacks is high and can result in significant financial and reputational damage to businesses



A resurgence of old tactics, like malware and bots, reminds all that old threats do not die



Ransomware remains prevalent as threat actors extort public- and private-sector targets for large sums of money

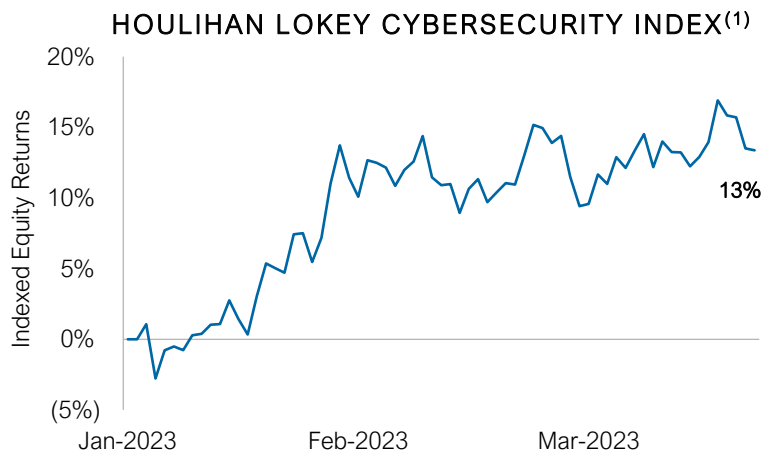


Access broker boom continues to grow at an unprecedented rate



Cyberattacks and information operations are thrust to the forefront of Russia's attack strategy against Ukraine

A Good Quarter for Public Companies



M&A Volume Faulters From 2022 Levels

	Q1 '23	VS. Q1 '22	VS. Q1 '21
Volume	\$5.9B	↓ (49%)	↓ (65%)
# of Deals	77	↑ 9%	↑ 43%

sumo logic

\$6.9B



\$1.1B

axis

\$500M

Financing Levels Pull Back

	Q1 '23	VS. Q1 '22	VS. Q1 '21
Volume	\$3.6B	↓ (45%)	↓ (34%)
# of Deals	125	↓ (61%)	↓ (52%)

SANDBOXAQ™

\$500M



\$300M

SAVIYNT

\$205M

Source: S&P Capital IQ as of March 31, 2023.

(1) Houlihan Lokey Cybersecurity Index includes S, CRWD, ZS, PANW, FTNT, SPLK, OKTA, FFIV, CYBR, QLYS, TENB, RPD, DARK, SUMO, RSKD, GEN, ABST, WITH, MITK, AVGO, CHKP, 4704, OTEX, BB, SWI, FSECURE, OSPN, TLS, and SCWX.

Table of Contents

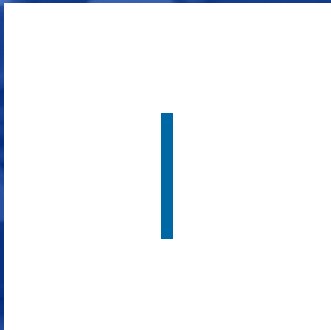
I Perspectives From the Front

II Capital Markets and Trends Update

III Conferences and Events

IV About Houlihan Lokey

V Appendix



Perspectives From the Front



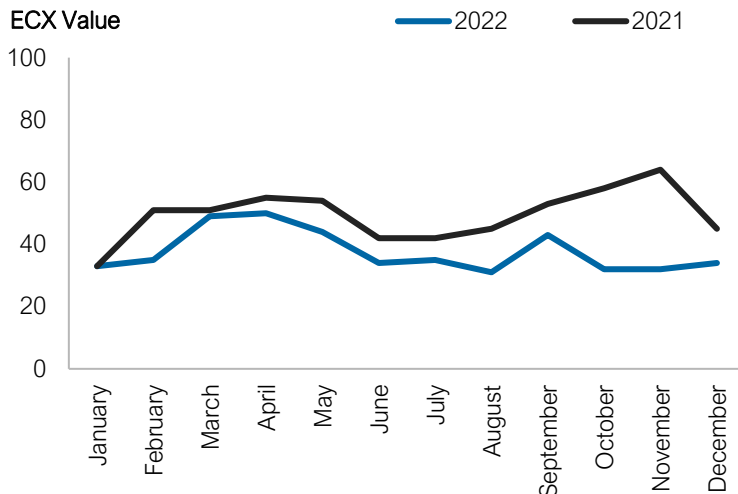
Houlihan Lokey

Critical Takeaways

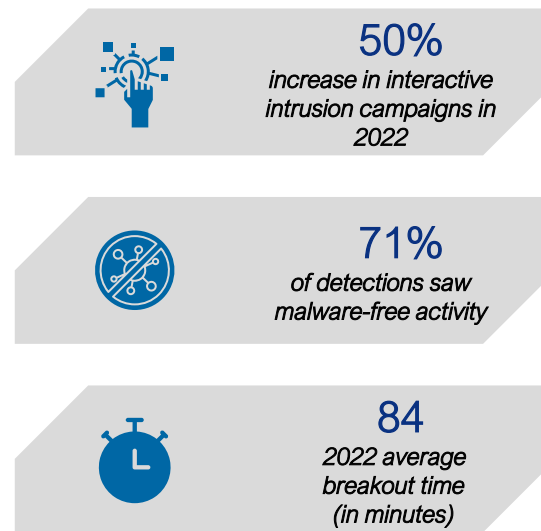
- A new, emerging class of eCrime threat actors are using fileless attacks to target high-profile organizations with devastating campaigns
- Identity protection continues to be a core requirement for risk mitigation as adversaries ramp up attacks on multifactor authentication
- Adversaries are accelerating cloud exploitation and the tactics they're using to compromise cloud infrastructures
- Adversaries have created new, "state-of-the-art" methodologies for vulnerability exploitation to sidestep patches, demonstrating why the industry needs to demand more secure software

CrowdStrike eCrime Index

Tracks activity across the eCrime ecosystem and calculates the total number of observed ransomware victims



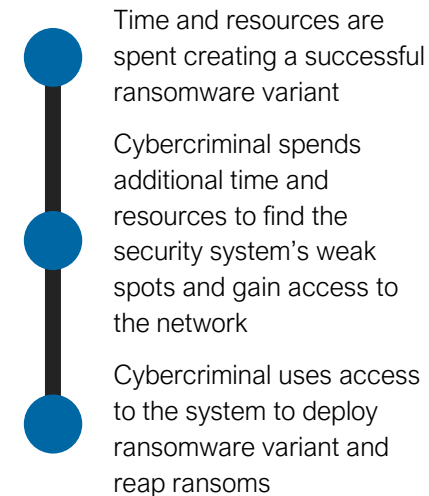
Key Stats



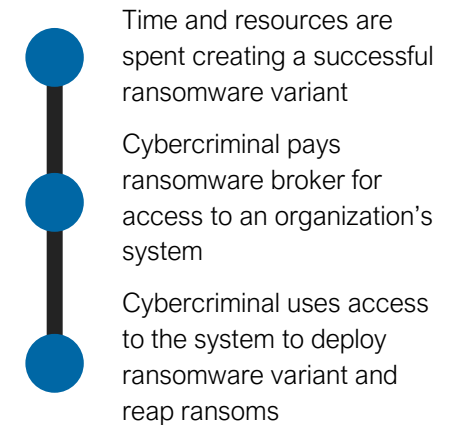
An Access Broker Boom

- Access brokers acquire access to organizations and provide or sell this access to other threat actors, including ransomware operators
- Brokers may engage in "access in bulk" (selling multiple at once), while others prefer to use the "one-access one-auction" (selling one access at a time)
- To combat access brokers, companies are heavily investing in ways to protect themselves from unauthorized access

TIMELINE WITHOUT ACCESS BROKERS



TIMELINE WITH ACCESS BROKERS



By paying initial access brokers, cybercriminals save time and money by having someone else do the hard work of gaining access to corporate networks, allowing them to produce more ransomware variants and reap more ransoms in total

FULL-THROTTLE CYBER AND INFORMATION WARFARE WITH LONG-TERM IMPLICATIONS



Russian-government-backed attackers have engaged in an aggressive, multipronged effort to gain a decisive wartime advantage in cyberspace, often with mixed results



Moscow has leveraged the full spectrum of information operations—from overt state-backed media to covert platforms and accounts—to shape the perception of the war



The invasion has triggered a notable shift in the Eastern European cybercriminal ecosystem that will likely have long-term implications for coordination between criminal groups and the scale of cybercrime worldwide

Key Stats

300%

increase in Russian phishing campaigns directed against users in NATO countries in 2022

250%

increase in Russian phishing campaigns directed against users in Ukraine in 2022

1,950

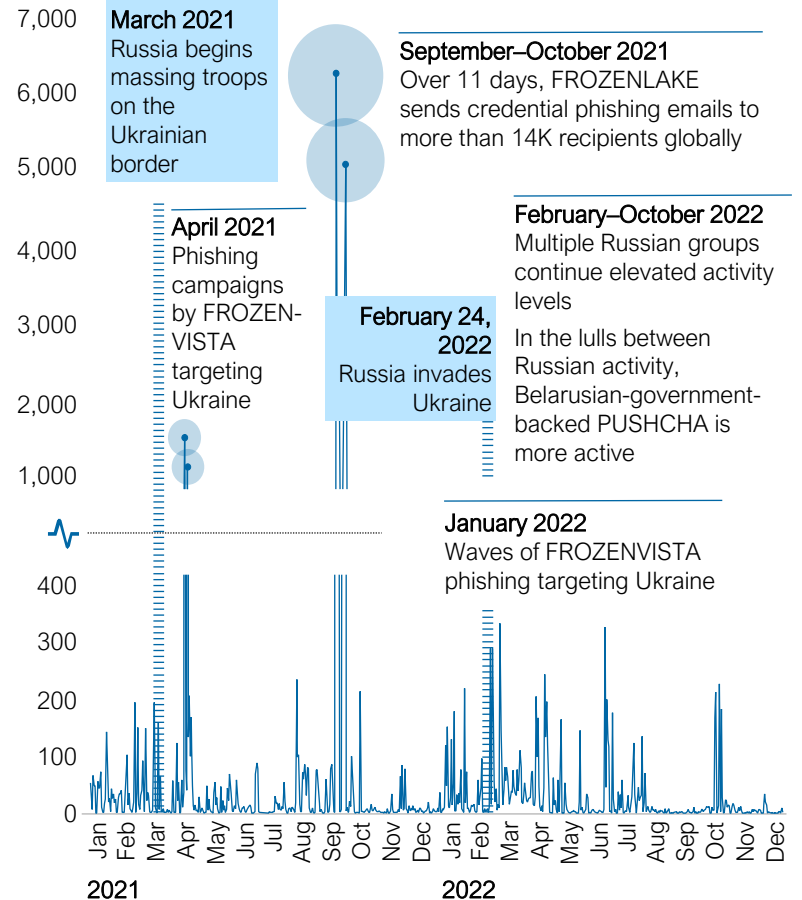
Russian IO activity disrupted by Google in 2022

Country-Backed Threat Actors and Their Targets

	FROZENBARENTS	FROZENLAKE	COLDRIVER	FROZENVISTA	PUSHCHA	SUMMIT
Espionage	•	•	•	•	•	•
Information Operations	•	•	•	—	•	—
Destruction	•	—	—	•	—	—
Targeted Nations	<ul style="list-style-type: none"> Ukraine NATO Countries Georgia 	<ul style="list-style-type: none"> Ukraine NATO Countries 	<ul style="list-style-type: none"> Ukraine NATO Countries 	<ul style="list-style-type: none"> Ukraine NATO Countries 	<ul style="list-style-type: none"> Ukraine NATO Countries Russia 	<ul style="list-style-type: none"> Ukraine NATO Countries Australia South America Middle East Central Asia

Phishing Campaigns by Government-Backed Attackers

Targets



- Ransomware attacks have become more sophisticated and targeted, with attackers using advanced techniques such as spear phishing, supply chain attacks, and zero-day exploits to gain access to networks and infect systems
- The emergence of ransomware-as-a-service (RaaS) platforms has made it easier for criminals to launch ransomware attacks, with individuals and groups able to purchase and customize ready-made ransomware kits to carry out attacks with minimal technical expertise
- Ransomware gangs are demanding larger ransoms than ever before, with some demanding millions of dollars from high-value targets such as large corporations, hospitals, and government agencies
- Ransomware attacks increasingly target critical infrastructure, such as healthcare systems, transportation networks, and utility companies, impacting public safety and the economy

Notable Ransomware Attacks



- The financial trading service group was hit by a ransomware attack in the beginning of February by notable group LockBit
- The information stolen in the attack was not revealed, but all affected servers were disconnected, forcing several banks and brokers to trade manually
- LockBit claimed that the ransom was eventually paid
- In February, LockBit launched a successful ransomware attack against the U.K.'s Royal Mail, demanding \$80 million in ransom
- The information stolen included human resources and staff records and details on salaries
- The data was eventually released online along with images of negotiations after Royal Mail refused to pay the ransom



New Ransomware Groups



Medusa

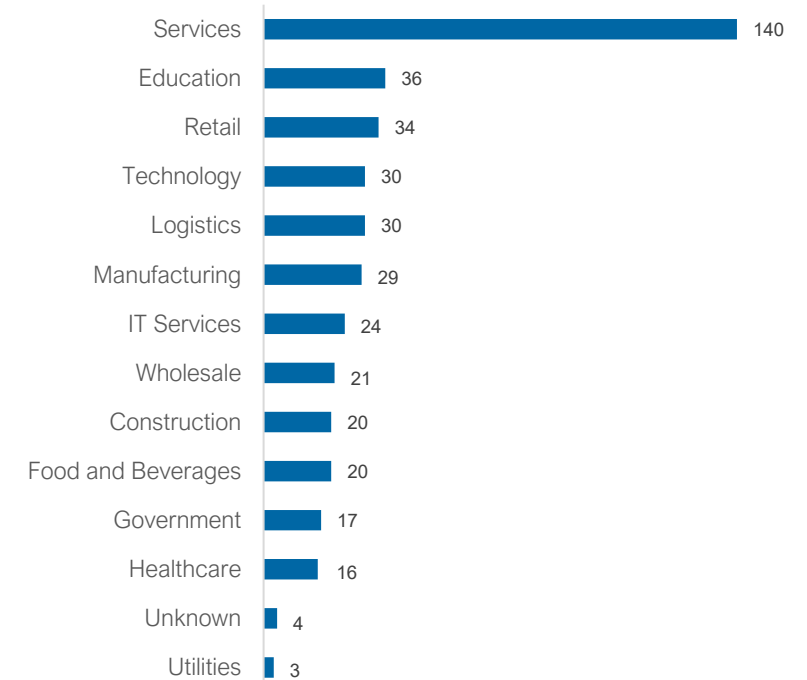
- The group published 20 victims on its leak site, making it the third most active ransomware group in February
- To date, its victims included Tonga Communications Corporation (TCC) and PetroChina Indonesia



V is Vendetta

- A newcomer that published three victims in February, including Tudor Watch

Ransomware Attacks by Segment



DataCentre: Uniting Cybersecurity and Cyber Storage Resilience

Cyber Research Summary

- Cybersecurity and cyber storage resilience are often treated separately in the enterprise, creating a critical gap that cyber attackers can exploit; when they are trending together, they cover each other's weaknesses, which cyber attackers have previously been able to exploit
- The exponential growth and intensity of cyber threats have escalated the need for cyber storage resilience to be part of every enterprise's cybersecurity strategy

2023 Prediction Tracking

- The predicted cost of cybercrime is staggering, with Cybersecurity Ventures forecasting that it will reach \$8 trillion USD in 2023 and rise to \$10.5 trillion by 2025
- The rising cost of cybercrime highlights the urgent need for organizations to invest in cybersecurity and cyber storage resilience; failure to do so can result in significant financial and reputational damage, making it essential for organizations to take proactive steps to protect their data and operations

Data Breaches

Baked-in Cyber Resilience



- The increasing frequency and severity of cyberattacks means that organizations need to adopt a more proactive approach to cybersecurity and ensure that their storage systems have intrinsic cyber storage resilience capabilities



- These capabilities include features such as rapid cyber recovery, immutable snapshots, air-gapping, and fenced forensic environments, which work together to provide a more comprehensive and robust approach to cybersecurity



- By deploying storage systems that have these capabilities built-in, organizations can more effectively protect their data, both at rest and in motion, and reduce the risk of data loss or theft due to cyberattacks



- Rapid cyber recovery is a critical aspect of cyber storage resilience, as it enables organizations to quickly restore their systems and data to a known good state after a cyberattack; to facilitate this, copies of critical data must be unalterable and data integrity must be preserved at all times



- Overall, the deployment of enterprise storage products with intrinsic cyber storage resilience capabilities is an important step in creating a more comprehensive and effective enterprise cybersecurity strategy

The Automation



- Enterprises are increasingly turning to machine-learning-based automation to enhance their cybersecurity infrastructures; this includes the adoption of autonomous automation to make storage infrastructures smarter and more resilient to cyberattacks



- However, cybercriminals are also using AI/ML to automate their attacks, making it a race between corporate automation and criminal automation on the security front

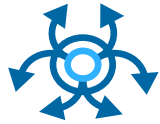


- The combination of cybersecurity and cyber-resilient storage is crucial to combatting cyberattacks; IT solutions providers can work with enterprise IT teams to identify security capabilities and the solutions needed to deliver them



- A cyber-resilient storage architecture is necessary to map to the broader data infrastructure, including features like cyber recovery, air-gapping, fenced forensic environments, and immutable snapshots; this can be achieved through integration via APIs and a resilient data infrastructure engine

KEY HIGHLIGHTS OF THE SECOND HALF OF 2022



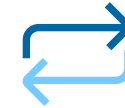
DON'T COUNT OUT THE OLD

The resurgence of familiar names in the malware, wiper, and botnet space—including Emotet and GandCrab, to name a few—in addition to code reuse (old code being recompiled into new variants) is a reminder that old malware and threats never die

ATT&CK

KEEP AN EYE OUT FOR PRE-ATT&CK

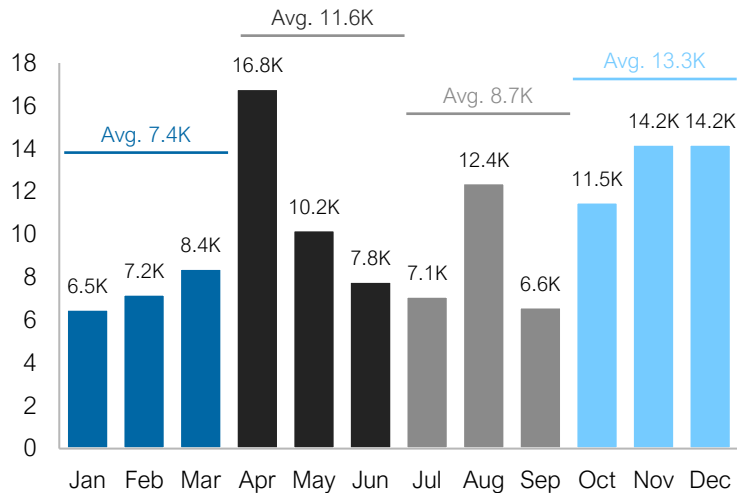
Adversaries are dedicating more resources to their attacks' recon and weaponization phase; as this approach becomes more “de facto” among threat actors, cyber defenders must keep using intelligence gathered from these phases



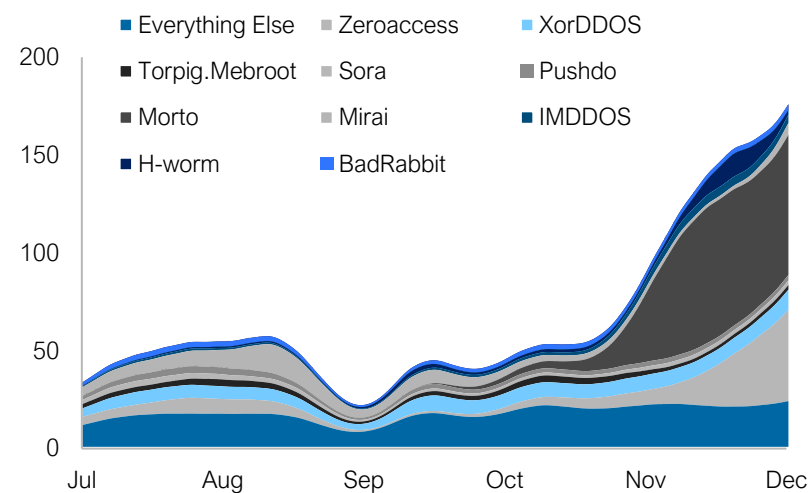
EXCHANGE BECOMES A POST-EXPLOITATION HOT POT

Hardening activities on exchange servers have thwarted much initial access targeting; adversary familiarity with associated services means Exchange servers have become a hotbed for post-exploitation activity

Quarterly Wiper Volume for 2022



Monthly Volume of Top 10 Botnets



Key Stats

- 44% of initial access techniques used valid credentials
- 21% of initial access techniques exploited public-facing applications
- 16% increase in ransomware and wipers in 2022

OUR PREDICTIONS

Phishing Escalations



- While phishing has become a top access vector in recent years, cybercriminals are moving toward SMS phishing (smishing) to infiltrate their targets
- Training initiatives for new compromising tactics will become increasingly important for organizations

State-Sponsored Attacks



- State-sponsored crime is a heightened threat when compared with previous years, as Russia, China, and Iran are all currently involved in conflict
- These and other nation-state actors will use cybersecurity tactics to advance their objectives as part of both outright conflict and covert operations

WHAT HAPPENED

- Phishing is the most common form of cyber crime, with an estimated 3.4 billion spam emails sent every day⁽¹⁾
- Only 23% of Americans can correctly define smishing, yet the average American receives up to 41 spam texts per month⁽²⁾⁽³⁾
- In 2023, 33 million data records are expected to be compromised due to phishing attacks⁽⁴⁾

- Foreign intelligence agencies are enhancing their abilities and presenting a challenge to U.S. defense by utilizing state-of-the-art technologies, including advanced cyber tools, unmanned systems, and improved technical surveillance equipment
- Many of these technologies are readily available in the market, allowing less technologically advanced agencies to become credible adversaries quickly

WHAT WE DID NOT PREDICT

AI Tech Has Made Phishing Easier

OpenAI's ChatGPT ability to produce grammatically correct and natural-looking writing would resolve one of the biggest challenges that scammers face when creating their phishing content



ChatGPT makes it very easy for them to impersonate a legitimate business without even having any of the language skills or other things necessary to write a well-crafted attack

– Chester Wisniewski, Field CTO at Sophos

- At the forefront, the ability for generative AI to mimic human text and speech means it can automate the phishing process for cybercriminals or write social engineering attacks or other types of malicious content
- Generative AI models are not limited to text-based applications; it can also be used to create a realistic-sounding speech for use in phone-based attacks
- AI-like VALL-E can match the voice and mannerisms of someone almost perfectly based on just three seconds of an audio recording of their voice

(1) AAG, "The Latest 2023 Phishing Statistics."

(2) Safety Detectives, "11 Facts + Stats on Smishing (SMS Phishing) in 2023."

(3) Earthweb, "Smishing Statistics."

(4) Truelist, "Phishing Statistics."

Cyber Research Summary

Breach Overview

Company Description: Wireless carrier and service provider

Date of Breach: January 2023

What Happened: AT&T customer data was stolen via a data breach in one of its marketing vendors

Months Since Last Breach at AT&T: <1 Month

Key Stats⁽¹⁾⁽²⁾



9M
total users affected



37M
customer records accessed in an earlier data breach in January

2023 Prediction Tracking

Attack Methodology and Rationale



While the specifics of how the data was accessed is unknown, an unauthorized actor breached the vendor's network and gained access to AT&T customer information



While the data that was leaked did not include credit card information or account passwords, it did include customer names and phone numbers, which could be used in a variety of phishing and smishing scams

Expert Opinions and Commentary



"Customers should be on the lookout for scam phone numbers and text messages because now these folks have your account number—they may be able to fool other vendors."
– Leeza Garber, Cybersecurity Attorney and Expert



"Seeing AT&T experience a data breach involving a third-party company is a wakeup call for all businesses and highlights the need to revisit supply chains for security weak links."
– Matt Aldridge, Principal Solutions Consultant at OpenText

Data Breaches

The Outcome

AT&T has notified customers and federal law enforcement about the data breach



A small portion of impacted customers also had exposure of their rate plan name, past due amount, monthly payment amount, and various monthly charges on top of the other information that was leaked



Customers are advised to toggle off CPNI data sharing on their accounts to reduce exposure risks



AT&T has yet to comment on what vendor was breached for this data

Key Takeaways



Limiting the Damage

It is crucial for organizations that have experienced data breaches to promptly educate their customers on how to protect themselves from phishing and smishing attempts



Data Sharing Caution

Companies should restrict the disclosure of customer sensitive data to third parties unless they have a comprehensive understanding of their cybersecurity measures and protocols

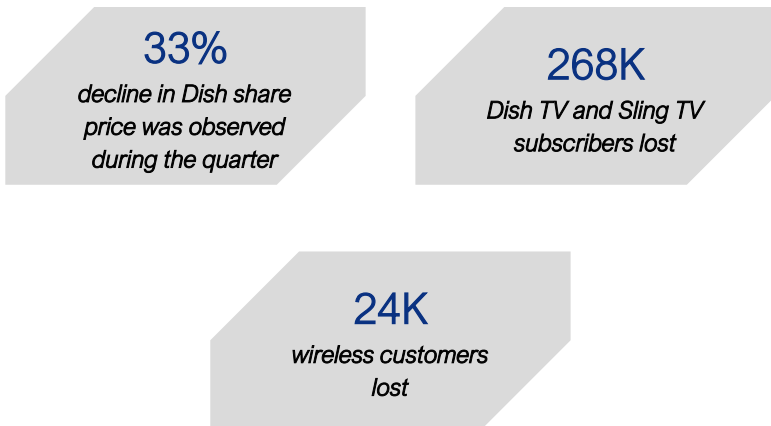
Data Breaches: Dish

Cyber Research Summary

Breach Overview

Company Description:	American television provider
Date of Breach:	February 2022
What Happened:	Ransomware attack breached Dish's networks, encrypted data, and caused a multiday outage of some services
Dish TV Subscribers:	7.42 Million ⁽¹⁾
Sling TV Subscribers:	2.42 Million ⁽¹⁾

Key Stats⁽¹⁾



2023 Prediction Tracking

Attack Methodology and Rationale



While unconfirmed, industry sources believe Black Basta, a ransomware-as-a-service gang, compromised the Windows domain controller and then encrypted VMware virtual machines



The rationale of the attack remains unknown, but Black Basta is known for its double extortion technique of demanding a ransom and threatening to release sensitive data if not paid

Expert Opinions and Commentary



"Ransomware attacks on such organizations can have a huge impact, as we are seeing with Dish's multiday outage and South Africa's RSAWEB, which had to shut down its telecommunication systems for a week."
– Rebecca Moody, Head of Data Research at Comparitech



"If the leaked memo is accurate and employees are being told not to log in to their VPN, this is one way Dish is attempting to protect its remote employees and curtail the spread of the ransomware."
– Alex Hoff, Co-Founder and CPO of Auvik Networks

Data Breaches

The Outcome



- Dish first blamed the outage on a VPN issue but later disclosed it was managing a ransomware attack, urging employees not to use the VPN in order to prevent the malware from spreading
- In late February, via a form 8-K, Dish said that it had determined that the outage was due to a cybersecurity incident



- Though Dish has worked to restore networks, some customers say that they are still experiencing network outages and long wait times to speak to customer support
- Customers and shareholders have lost confidence in Dish, as both the share price and the number of Dish subscribers have fallen since the outages began

Key Takeaways



Be Transparent

Companies should be transparent and honest with customers about any breaches; this includes providing clear and concise information about what happened, how it may affect customers, and what the company is doing to address the issue



More Advanced Security Measures

Implementing multifactor authentication or other identity-based access controls may decrease the risk of security breaches

Sources: Bleeping Computer, "Dish Network Confirms Ransomware Attack Behind Multi-Day Outage"; The Hill, "Dish Network Confirms Cybersecurity Breach."

Notes: Statistics from CPO Magazine reflect information posted in Dish's Q4 2022 SEC report.

(1) CPO Magazine: "Leading U.S. Satellite TV Provider Dish Network Yet to Recover From a Ransomware Attack."

Data Breaches: U.S. Marshals

Cyber Research Summary

Breach Overview

Agency Description: Federal Law Enforcement Agency

Date of Breach: February 2023

What Happened: U.S. Marshals Service (USMS) suffered a security breach that compromised sensitive law enforcement information

Information Stolen Supposedly Includes: Aerial footage and photos of military bases and other high-security areas, copies of passports, details of wiretapping on citizens, and more

Key Stats⁽¹⁾



\$150K
is the asking price for the dataset



350 GB
volume of stolen data

2023 Prediction Tracking

Attack Methodology and Rationale



The specific methodology used is unknown, but a compromised USMS system was identified and subsequently disconnected from the network



The attacker was able to successfully breach the software and gain access to sensitive personal information, including Personally Identifiable Information (PII), which they then used to enhance their identity fabric for further malicious activities



The information was taken from a stand-alone computer that did not have any connection to the broader network; it was quickly shut down when the breach was discovered

Expert Opinions and Commentary



“The theft of U.S. Marshal confidential data can compromise ongoing investigations, endanger the lives of law enforcement officers, and undermine public trust in our justice system.”

– Dimitri Nemirovsky, Co-Founder and COO of Atakama



“Based on the information we do have, the information stolen has the potential to compromise ongoing investigations, including witnesses and informants, put USMS employees in danger, and disrupt time-sensitive operations while the USMS recovers.”

– Darren Guccione, CEO at Keeper Security

Data Breaches

The Outcome



A threat actor came out on a Russian-speaking hacking forum claiming to have hundreds of gigabytes of data stolen from U.S. Marshals Service servers and is now selling the database



The system did not contain personal details about people enrolled in the Federal Witness Protection Program; however, the threat actor claims that the database includes details about witnesses in the protection program



The USMS has yet to comment on the validity of the threat actor's claims

Key Takeaways



Improving Cybersecurity Resources

Government agencies that have access to highly sensitive data should ensure that they have the latest security measures in place and should implement monitoring and threat intelligence gathering to detect and prevent future breaches



The Importance of IDPS

By implementing intrusion detection and prevention systems (IDPS), agencies can protect themselves by monitoring network traffic and identifying potential malicious activity

Data Breaches: T-Mobile

Cyber Research Summary

Breach Overview

Company Description: A mobile communications services provider offering voice, messaging, and data services

Date of Breach: January 2023

What Happened: T-Mobile customer data was stolen via an attack on its application programming interface (API)

Number of Customers: 113.6 million customers at the end of 2022⁽¹⁾

Total Users Impacted: 37 million⁽²⁾

Key Stats⁽³⁾⁽⁴⁾



8

security breaches since 2018



\$150M

investment dedicated to improving cybersecurity at T-Mobile

2023 Prediction Tracking

Attack Methodology and Rationale



According to T-Mobile, the threat actor did not breach any company systems but instead abused an API to mass harvest data



While sensitive customer data may not have been stolen, the information that was taken could still pose a threat; this stolen information could be utilized for malicious activities such as phishing or sold to the highest bidder on the dark web

Expert Opinions and Commentary



"While these cybersecurity breaches may not be systemic in nature, their frequency of occurrence at T-Mobile is an alarming outlier relative to telecom peers."

– Neil Mack, Senior Analyst at Moody's Investors Service



Federal Communications Commission

"Carriers have a unique responsibility to protect customer information. When they fail to do so, we will hold them accountable. This incident is the latest in a string of data breaches at the company, and the FCC is investigating."

– FCC Spokesperson

Data Breaches

The Outcome

24 hours after the T-Mobile team identified the breach, the attack was shut down



T-Mobile has restated its pledge to make a substantial, multi-year investment in strengthening its cybersecurity program



Due to the excessive number of breaches T-Mobile has faced over the years, experts theorize that these breaches may alienate customers and attract scrutiny by the Federal Communications Commission (FCC) and other regulators



T-Mobile contacted authorities and notified law enforcement about this breach; the FCC is now investigating the breach

Key Takeaways



Increasing Cybersecurity Investment

Organizations that experience frequent data breaches should prioritize allocating more resources to safeguarding customer data and enhancing their cybersecurity measures



Increasing Transparency

Companies should communicate transparently with affected customers about the breach and steps being taken to address it to maintain trust and credibility

(1) T-Mobile, "Preliminary Customer Results 2022."

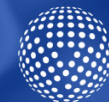
(2) Krebs on Security, "New T-Mobile Breach Affects 37 Million Accounts."

(3) TechCrunch, "T-Mobile Data Breach."

(4) USA Today, "In Latest T-Mobile Hack, 37 Million Customers Have Personal Data Stolen, Company Says."



Capital Markets and Trends Update



Cybersecurity Dashboard

Public Market Environment

In reverse from 2022, cybersecurity companies in 2023 experienced a rise in public performance



High-Growth Index Performance⁽¹⁾

↗ 18% | ↘ (47%)
Q1 '23 | LTM



Medium-Growth Index Performance⁽²⁾

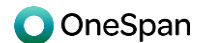
↗ 19% | ↘ (24%)
Q1 '23 | LTM



Low-Growth Index Performance⁽³⁾

↗ 14% | ↘ (3%)
Q1 '23 | LTM

Selected Cybersecurity Performance Q1 2023



↗ 56.4%

sumo logic

↗ 47.9%



↗ 43.1%



↗ 40.6%



↗ 35.9%



↗ 35.1%



↗ 34.1%

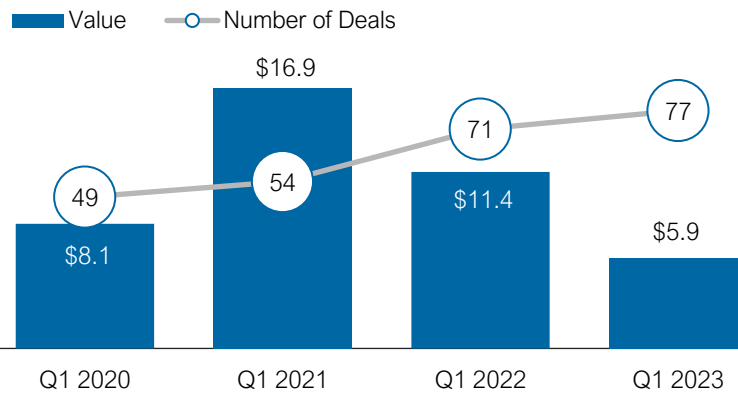


↗ 30.4%

M&A Environment

While the disclosed value fell from 2022, the number of transactions remains higher than in 2020, 2021, and 2022

(\$ in billions)



(\$ in millions)

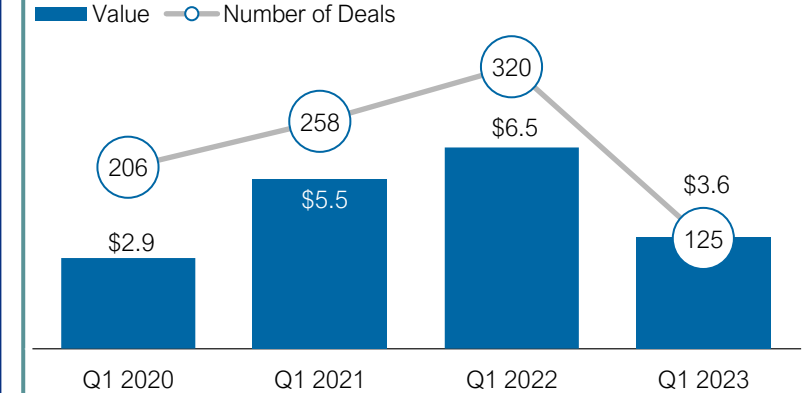
Selected Q1 Transactions

Ann. Date	Acquirer	Target	EV	EV/Rev
Mar-23	SUMMAEQUITY	LOGPOINT	\$150	6.0x
Mar-23	Hewlett Packard Enterprise	axis	\$500	NM
Feb-23	CISCO	VALTIX	\$200	NA
Feb-23	FP FRANCISCO PARTNERS	sumo logic	\$1,419	4.7x
Jan-23	THOMABRAVO	MAGNET FORENSICS	\$1,114	12.5x

Private Funding Environment

Despite an uncertain and volatile macroeconomic environment, cybersecurity funding hit \$3.6 billion in the first quarter of 2023, reflecting a normalization to pre-pandemic levels

(\$ in billions)



(\$ in millions)

Selected Q1 Financings

Ann. Date	Investor	Target	Amt.	Val.
Mar-23	breyer capital / TIME Ventures / Others	SANDBOX AQ+	\$500	\$4,000
Feb-23	Index Ventures / GREENOAKS / Lightspeed	WIZ+	\$300	\$10,300
Feb-23	splunk> / Springcoast / VISTA PARTNERS	deepwatch	\$180	NA
Jan-23	ALLIANCEBERNSTEIN	SAVIYNT	\$205	NA
Jan-23	servicenow	snyk	\$25	\$7,400

Source: S&P Capital IQ as of March 31, 2023.

Note: 2022 M&A deal volume includes Broadcom's pending acquisition of VMware.

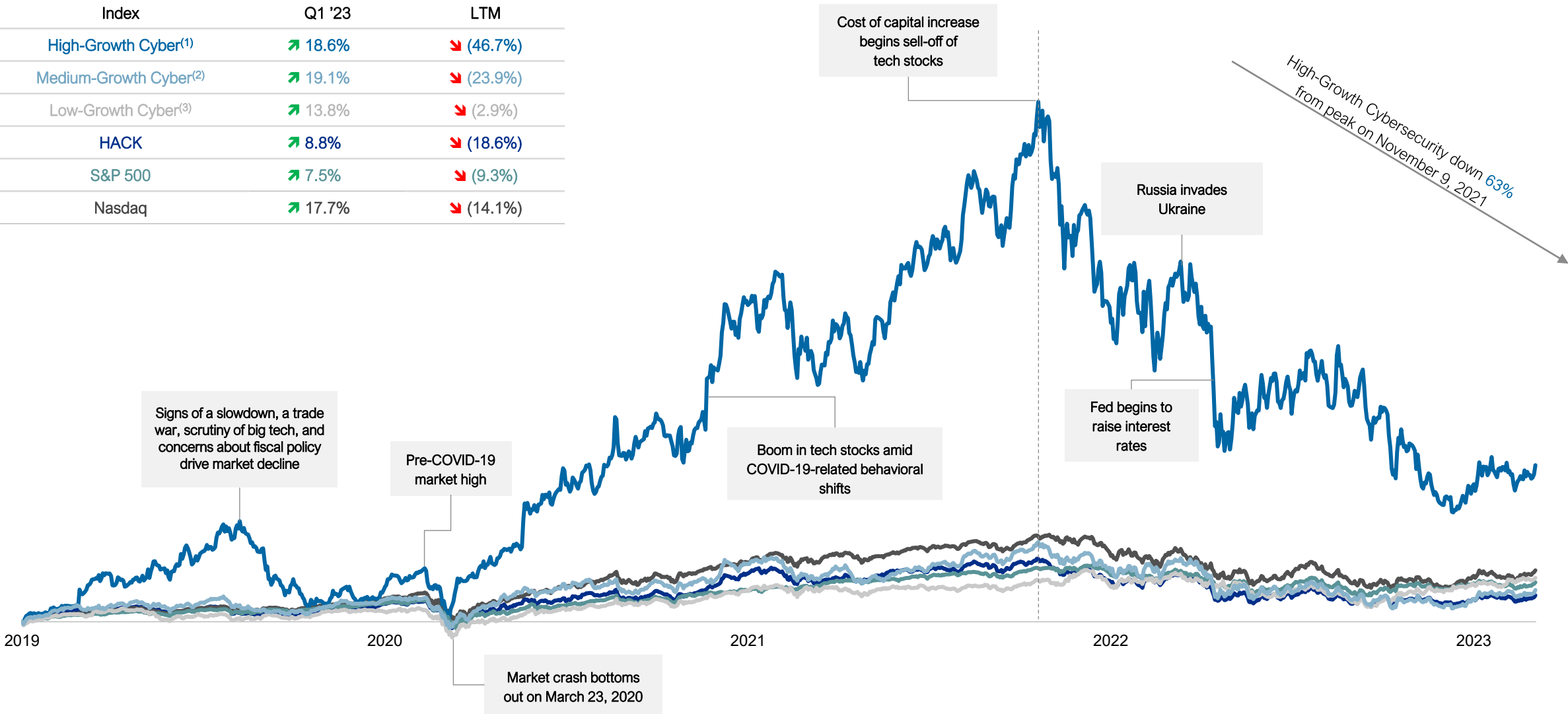
(1) High-Growth Cybersecurity includes S, CRWD, and ZS.

(2) Medium-Growth Cybersecurity includes PANW, FTNT, SPLK, OKTA, FFIV, CYBR, QLYS, TENB, RPD, DARK, SUMO, RSKD, ABST, WITH, GEN, and MITK.

(3) Low-Growth Cybersecurity includes AVGO, CHKP, 4704, OTEX, BB, SWI, FSECURE, OSPN, TLS, and SCWX.

Despite Correction, High-Growth Cybersecurity Remains Above Pre-COVID-19 Levels

Index	Q1 '23	LTM
High-Growth Cyber ⁽¹⁾	↗ 18.6%	↘ (46.7%)
Medium-Growth Cyber ⁽²⁾	↗ 19.1%	↘ (23.9%)
Low-Growth Cyber ⁽³⁾	↗ 13.8%	↘ (2.9%)
HACK	↗ 8.8%	↘ (18.6%)
S&P 500	↗ 7.5%	↘ (9.3%)
Nasdaq	↗ 17.7%	↘ (14.1%)

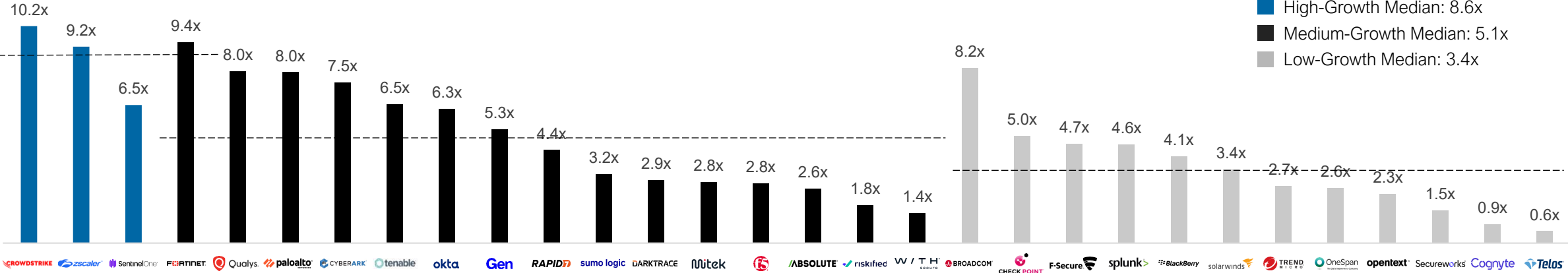


Source: S&P Capital IQ as of March 31, 2023.

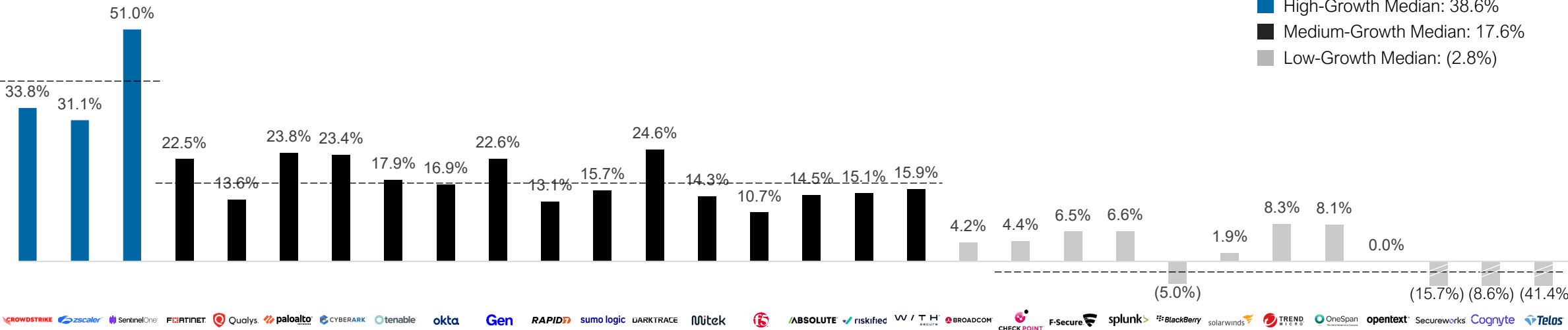
(1) High-Growth Cybersecurity includes S, CRWD, and ZS.
 (2) Medium-Growth Cybersecurity includes PANW, FTNT, SPLK, OKTA, FFIV, CYBR, QLYS, TENB, RPD, DARK, SUMO, RSKD, ABST, WITH, GEN, and MITK.
 (3) Low-Growth Cybersecurity includes AVGO, CHKP, 4704, OTEX, BB, SWI, FSECURE, OSPN, TLS, and SCWX.

Public Company Benchmarking: Cybersecurity Software

EV/2023E Revenue



CY 2022E-2023E Revenue Growth



Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of March 31, 2023.
 Note: All financials calendarized to a December year-end. Sorted by EV/2023E revenue.

Public Investors Remain Focused on Growth and Profitability

Low-Revenue Growth	Medium-Revenue Growth	High-Revenue Growth
--------------------	-----------------------	---------------------

Mean: (4%) | 3.4x
Median: 3% | 3.1x

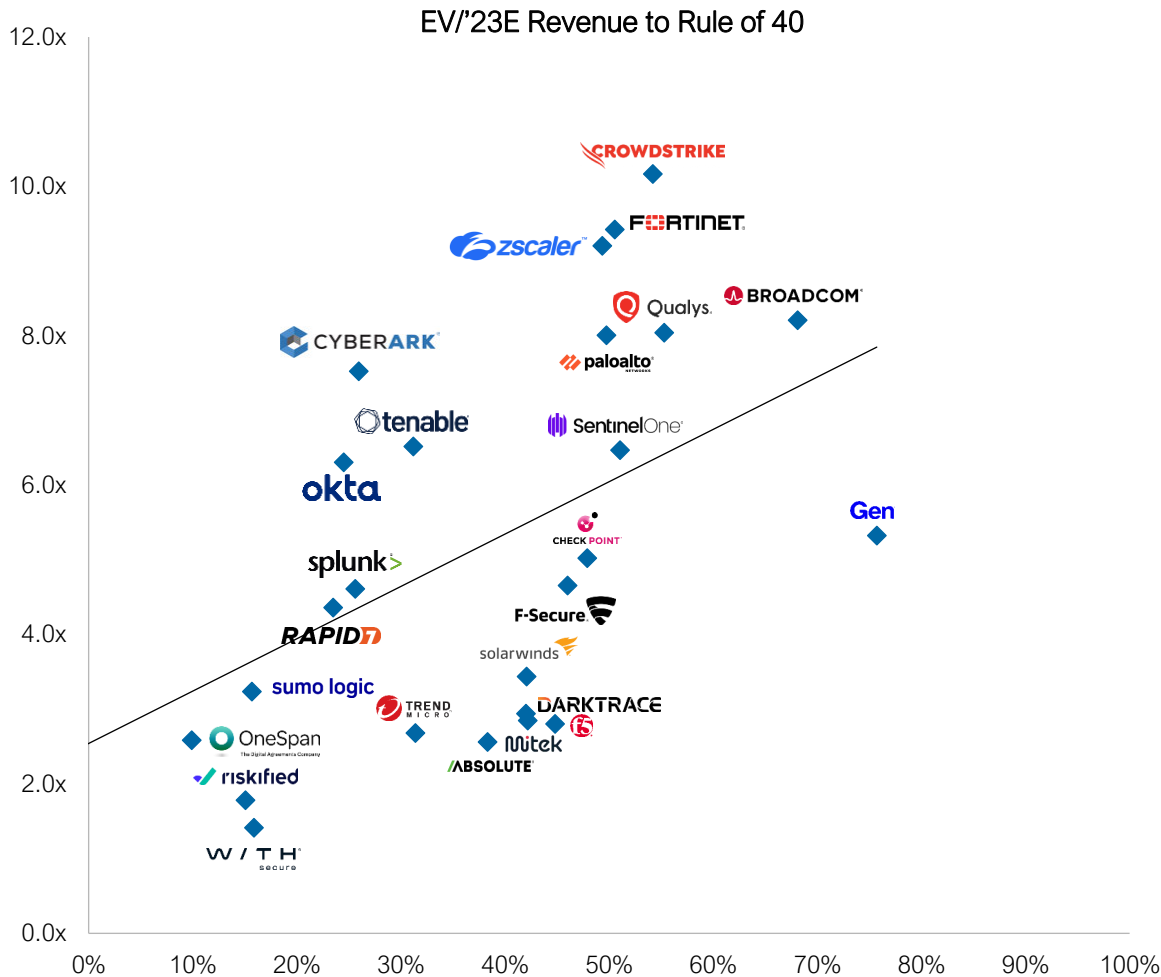
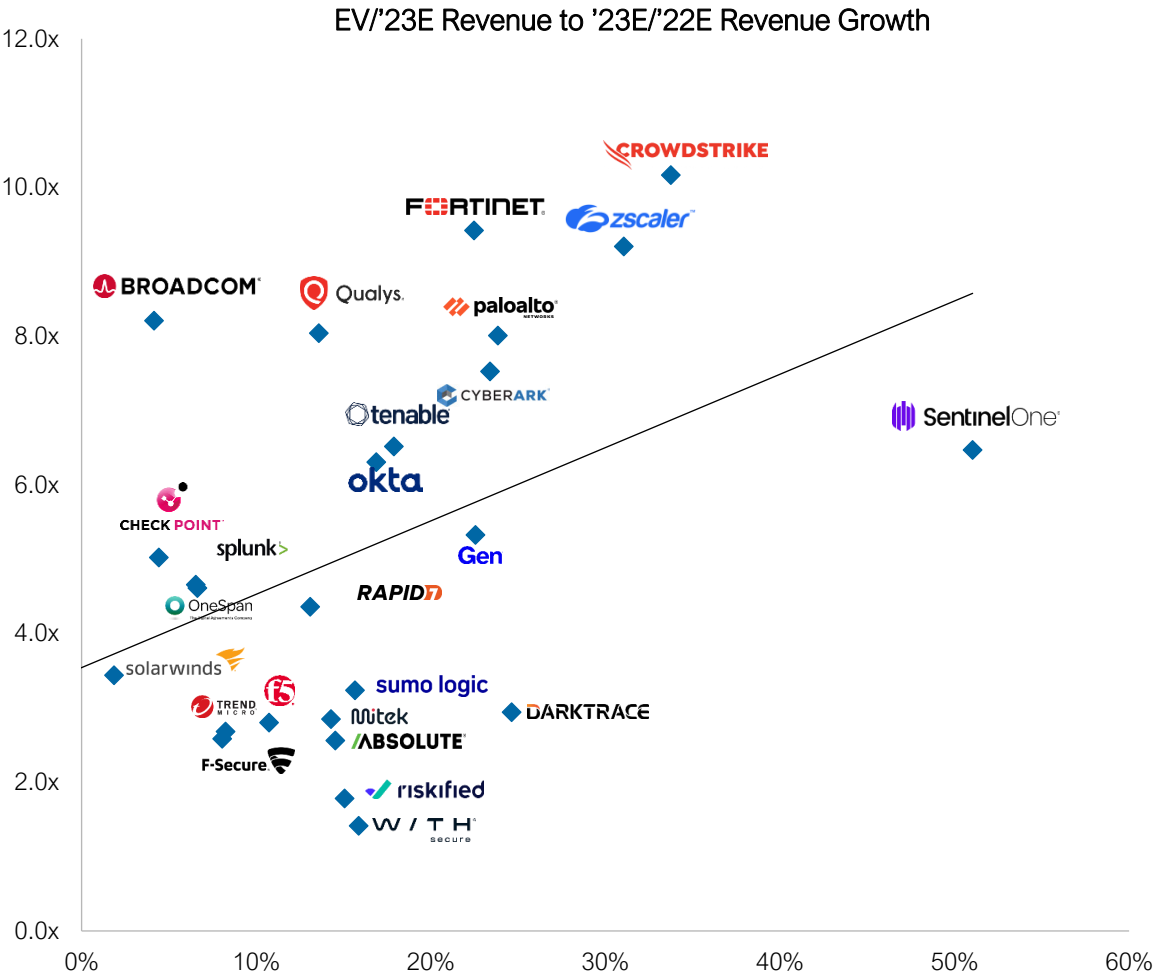
Mean: 17% | 4.8x
Median: 16% | 4.4x

Mean: 33% | 8.0x
Median: 32% | 7.8x

Below "Rule of 40"	Above "Rule of 40"
--------------------	--------------------

Mean: 6% | 3.4x
Median: 13% | 2.7x

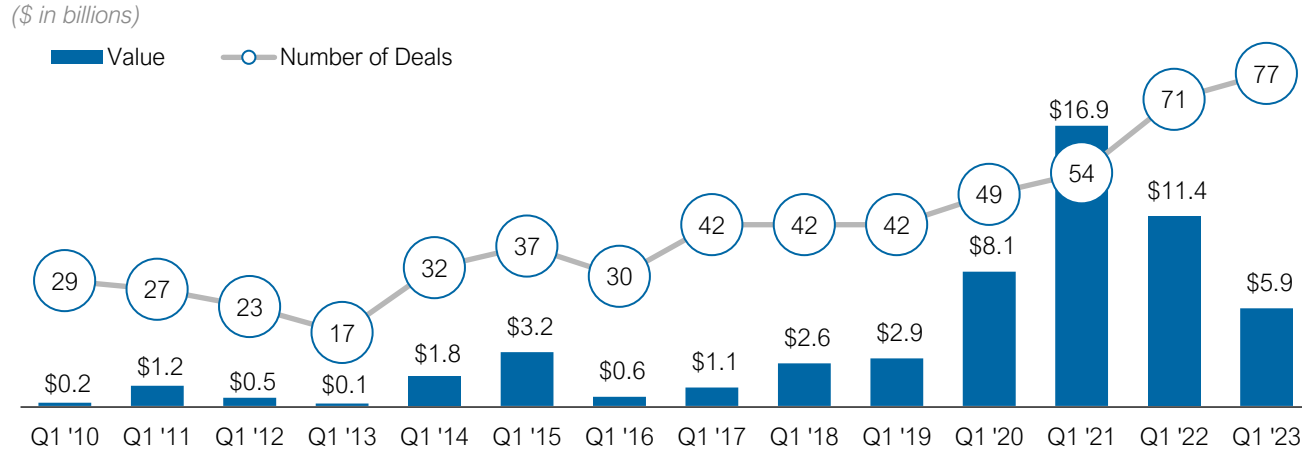
Mean: 19% | 6.2x
Median: 18% | 5.9x



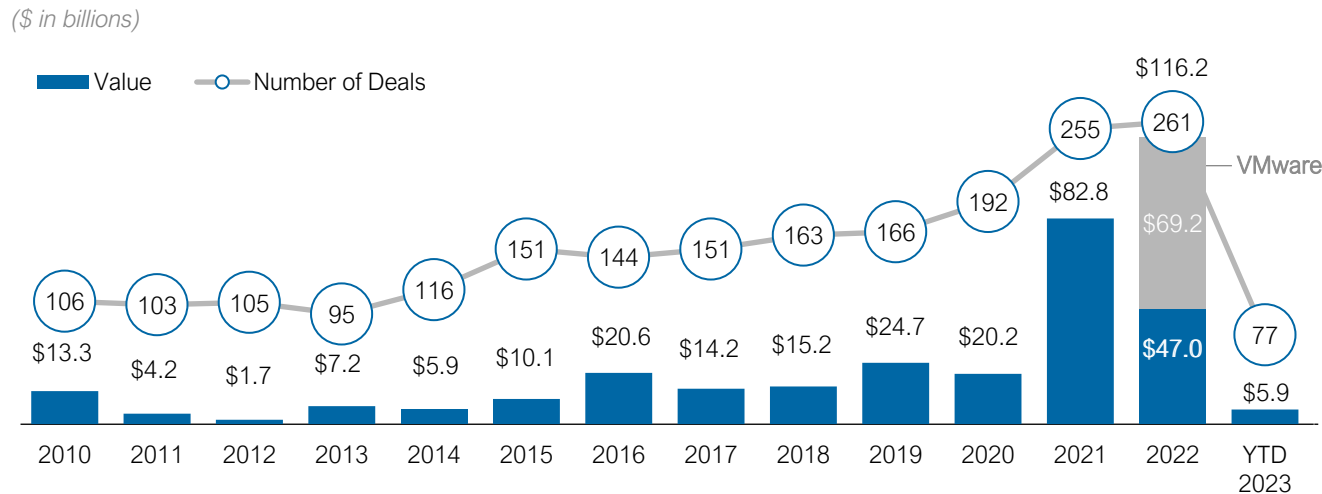
Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of March 31, 2023. All financials calendarized to a December year-end. Note: TLS, BB, and SCWX are included in the calculation for R² but are not included in the charts due to having negative values for either Revenue Growth or Rule of 40.

Cybersecurity M&A Activity

Historical Q1 M&A Summary



Annual M&A Summary



Selected M&A Transactions

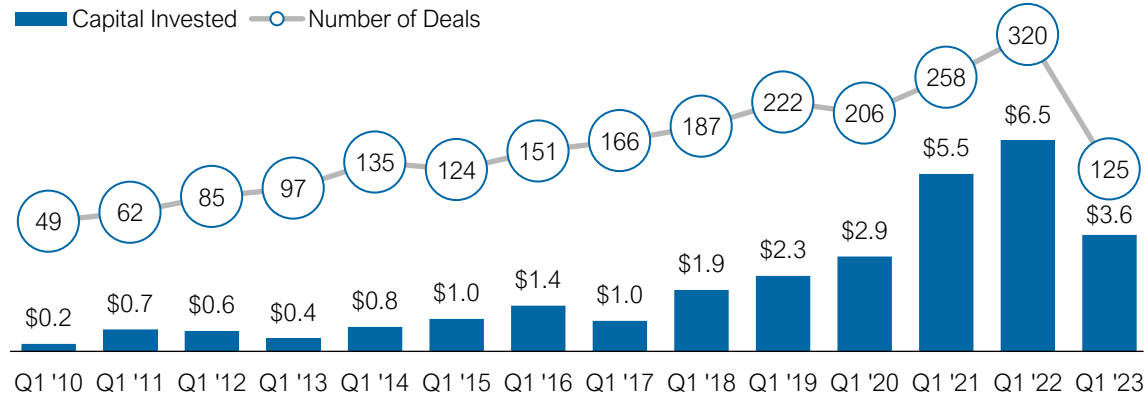
(\$ in millions)

Ann. Date	Acquirer	Target	EV	EV/Rev
Mar-23	CISCO	Lightspin	NA	NA
Mar-23	mastercard	BAFFIN BAY NETWORKS	NA	NA
Mar-23	RAPID7	MINERVA	\$38	0.8x
Mar-23	SUMMAEQUITY	LOGPOINT	\$150	6.0x
Mar-23	Hewlett Packard Enterprise	axis	\$500	NM
Feb-23	CISCO	VALTIX	\$200	NA
Feb-23	zscaler	CANONIC	NA	NA
Feb-23	FP FRANCISCO PARTNERS	sumo logic	\$1,419	4.7x
Jan-23	Vanta	Trustpage	NA	NA
Jan-23	THOMABRAVO	MAGNET FORENSICS	\$1,114	12.5x
Jan-23	SailPoint	SecZetta	NA	NA
Jan-23	NETSPI	nvisium	NA	NA

Cybersecurity Financing Activity

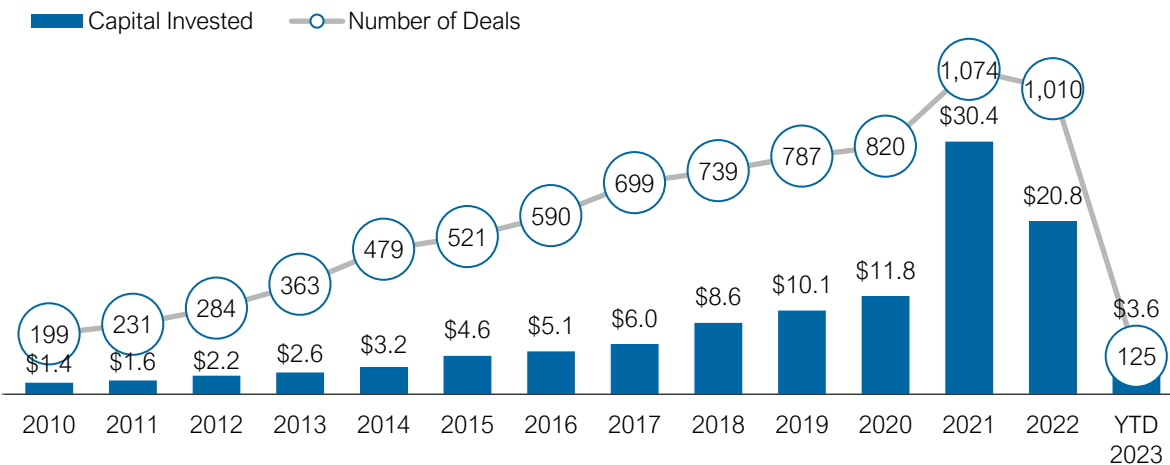
Historical Q1 Financing Summary

(\$ in billions)



Annual Financing Summary

(\$ in billions)



Selected Minority Transactions

(\$ in millions)

Ann. Date	Lead Investor	Target	Amount	Valuation	Total Raised
Mar-23	INFRAVIA	DATA DOME	\$42	NA	\$81
Mar-23	breyer capital TIME Ventures / Others	SANDBOX AQ™	\$500	\$4,000	\$500
Mar-23	ATLANTIC BRIDGE ClearSky dnx ventures	MITIGA	\$45	\$145	\$52
Mar-23	J.P.Morgan KeyBanc Capital Markets	Socure	\$95	NA	\$744
Feb-23	Index Ventures GREENOAKS Lightspeed	WIZ	\$300	\$10,300	\$921
Feb-23	splunk > Springcoast VISTA PARTNERS	deepwatch	\$180	NA	\$381
Feb-23	Lightspeed GGVCAPITAL	descope	\$53	NA	\$53
Feb-23	CVC PANTHEON J.P.Morgan	SKYBOX SECURITY	\$50	NA	\$200
Jan-23	[A/B] ALLIANCEBERNSTEIN	SAVIYNT	\$205	NA	\$245
Jan-23	servicenow	snyk	\$25	\$7,400	\$1,356
Jan-23	Felicis GENERAL CATALYST POINT72 VENTURES	VANNEVAR Labs	\$75	\$575	\$91
Jan-23	Morgan Stanley	netskope	\$401	NA	\$1,450

FINANCIAL SPONSORscape: Cybersecurity Portfolio Companies





Conferences and Events



Recent Conferences and Events

“Digital Warfare With One of the World's Greatest Hackers”

To hear the conversation recording, please follow the link by clicking on the text above



Dmitri Alperovitch
Chairman of Silverado Policy Accelerator
Co-Founder of CrowdStrike

in
conversation
with



Sid Trivedi
Partner at Foundation Capital

Upcoming Conferences and Events

Topics Covered

Russia-Ukraine Conflict Q: “What do you predict is going to happen next?”



A: “Well, this war has really become a war of attrition on both sides. [Putin] has gambled his regime on it. Obviously, for Ukraine, it is an existential fight, and they have the same willpower to keep on fighting. So, unfortunately, I think it’s going to continue on for quite some time.”

Digital Warfare

Q: “Could you talk about the attack on Viasat and why it matters?”



A: “They hacked into Viasat. And because they timed it with the invasion, the effect was really dramatic because they were able to disable Ukrainian communications that were using satellites.”

Successful Companies Q: “What do you think are the traits that define successful founders?”



A: “I think the key characteristic is perseverance. I mean, look at founders today dealing with [SVB] issues. Who right now wants to deal with the question of how do I make payroll, how do I access my money in a bank that I thought was completely safe, right? Life deals you lemons; make lemonade.”

Questions From the Audience



Q: “To what extent do you see TikTok as being a threat? And if so, what kind of threat?”

A: “Out of all the things that they’re doing to us with technologies like Huawei and with stealing intellectual property and so forth, TikTok is at the bottom of my list of concerns. We know that China has the ability—or TikTok has the ability—to collect information from the device, track locations, and so forth. I’m not thrilled about government officials having TikTok on their phone, and Congress just passed a bill last year banning that.”



Q: “Russia had an extremely sophisticated understanding of the West in the 2016 election. What role do you think they played?”

A: “Americans elected Donald Trump, and I think we have to recognize that, whether you like that or not. But Russia did not change votes. I believe that both the 2016 elections were secure, as I believe the 2020 elections were secure. I think we have polarization that they’re trying to amplify. But I think it’s a cop-out to say our problem is Russia in this sphere.”

Recent Conferences and Events



- RSA Conference (RSAC) is the premier series of global events and year-round learning for the cybersecurity community
- RSAC is the ultimate marketplace for the latest technologies and hands-on educational opportunities that help industry professionals discover how to make their companies more secure while showcasing the most enterprising, influential, and thought-provoking thinkers and leaders in cybersecurity today
- This year's theme is "Stronger Together": a theme to show that none of the breakthroughs in the cybersecurity space could have been achieved without working together, sharing ideas, and examining past failures

Upcoming Conferences and Events

Innovation Programs



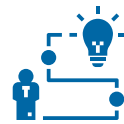
Innovation Sandbox

Cybersecurity's boldest new innovators compete to put the spotlight on their game-changing ideas



Launch Pad

Early-stage startups can pitch their new ideas *Shark Tank*-style to industry veterans for advice and strategy



Sandbox

Hosts eight villages for head-to-head interactive activities and games for hands-on experience



Early-Stage Expo

An opportunity to see up-and-coming companies and the cybersecurity leaders of tomorrow



Security Scholar

Hand-selected cybersecurity students are able to connect with the RSAC community



Inclusive Security

Focuses on how changes to cultures and hiring practices can promote a new type of thought within cybersecurity

Selected Keynote Speakers



Rohit Ghai
CEO
RSA Security



Tom Gillis
Senior Vice President and
General Manager
Cisco Security Business Group



Tanya Janca
CEO and Founder
We Hack Purple



George Kurtz
Co-Founder and CEO
CrowdStrike



Brad Maiorino
CISO
Raytheon Technologies



Phyllis Schneck
Vice President and Chief
Information Security Officer
Northrop Grumman



Kevin Mandia
CEO
Mandiant, Google Cloud



Lisa Monaco
U.S. Deputy Attorney General
United States Government

Recent Conferences and Events

Infosecurity Europe

- Infosecurity Europe is the biggest gathering of the information security industry in Europe
- Each year, the community comes together to share innovation, learn from each other, test and benchmark solutions, build relationships to drive new business, and connect with colleagues

258

Exhibitors

23

Strategy Talks
Sessions

250+

Speakers Across
Three Days

Conference Offerings

Keynote Stage

Innovation Showcase

Strategy Talks

Geek Street

Insight Stage

Start-Up Showcase

Talking Tactics

Security Workshops

Technology Showcase

Security Training

Upcoming Conferences and Events

Selected Keynote Speakers



Andrew Rose
Resident CISO, EMEA
Proofpoint Ltd.



Ilona Simpson
CIO EMEA
Netskope



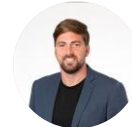
Yuval Wollman
President
CyberProof



Bentsi Benatar
CMO, Co-Founder
Sepio



Brad Freeman
Director of Technology
SenseOn



Nadir Izrael
CTO, Co-Founder
Armis



Dan Benjamin
CEO, Co-Founder
Dig Security



Dr. Niklas Hellemann
CEO
SoSafe



Henning Christiansen
CISO
Ottobock



Stephen Boyer
CTO, Co-Founder
BitSight

Beyond the Conference



Department
for Business
Innovation & Skills

- For the eighth year running, the Department for Science, Innovation and Technology (DSIT) is looking for the most creative and original cybersecurity companies in the country, one of which will be crowned the U.K.'s Most Innovative Cyber SME 2023
- The winner, along with the 13 runners-up, will be invited to join the Cyber Innovation Zone at Infosecurity Europe 2023

PREVIOUS WINNERS



Recent Conferences and Events

- Black Hat is an internationally recognized cybersecurity event series providing the most technical and relevant security research
- These multiday events provide the security community with the latest cutting-edge research, developments, and trends
- Attendees can gain hands-on experience and deepen their knowledge through a variety of training opportunities, including beginner- and advanced-level courses

Black Hat USA 2023



The event includes four days of trainings and a two-day main conference featuring Briefings, Black Hat Arsenal, Dark Reading, and more



Black Hat CISO Summit is an approval-only event that brings together top security executives from global corporations and government agencies for a full day of unique discussions



Key topics in the conference include AI and ML, AppSec, cloud security, cryptography, human factors, malware, mobile security, network security, policy, and privacy

SUSTAINING PARTNERS



Upcoming Conferences and Events



Core Black Hat 2023 Features



Black Hat Briefings

Provides security professionals with a place to learn the very latest in information security risks, research, and trends



Black Hat Trainings

Offers individual technical courses with topics ranging from the latest in penetration testing to exploiting web applications and defending and building SCADA systems



Black Hat Certified Pentester

In partnership with The SecOps Group, Black Hat now has its own certification: Black Hat Certified Pentester



Black Hat Business Hall

Solution providers and startups showcase the latest technologies and security services

A hand is shown from the right, holding a glowing digital globe. The globe is composed of a network of white nodes connected by thin lines, set against a dark blue background with faint, larger-scale network patterns. The overall aesthetic is futuristic and technological.

IV

About Houlihan Lokey



Houlihan Lokey



Houlihan Lokey is the trusted advisor to more top decision-makers than any other independent global investment bank.

~2,610 Global Employees ⁽¹⁾	36 Locations	\$6 Billion Market Cap ⁽²⁾	HLI LISTED NYSE	\$1.8 Billion Revenue ⁽³⁾	~25% Employee-Owned	No Debt
---	-----------------	--	------------------------------	---	------------------------	------------

Corporate Finance

- No. 1 Global M&A Advisor Under \$1 Billion
- Leading Capital Markets Advisor Raising More Than \$100 Billion in Past Five Years

Rank	Advisor	Deals
1	Houlihan Lokey	381
2	Rothschild	369
3	JP Morgan	217

Source: Refinitiv. Excludes accounting firms and brokers.

Financial Restructuring

- No. 1 Global Restructuring Advisor
- \$3.0 Trillion of Aggregate Transaction Value Completed

Rank	Advisor	Deals
1	Houlihan Lokey	58
2	PJT Partners	30
3	Lazard	29

Source: Refinitiv.

Financial and Valuation Advisory

- No. 1 Global M&A Fairness Opinion Advisor Over the Past 25 Years
- 1,000+ Annual Valuation Engagements

Rank	Advisor	Deals
1	Houlihan Lokey	1,232
2	JP Morgan	1,030
3	Duff & Phelps, A Kroll Business	938

Source: Refinitiv. Announced or completed transactions.

Financial Sponsors Coverage

- No. 1 Global Private Equity M&A Advisor
- 1,000+ Sponsors Covered Globally

Rank	Advisor	Deals
1	Houlihan Lokey	242
2	Lincoln International	192
3	Deloitte	190

Source: PitchBook.

Houlihan Lokey + **Oakley Advisory**

Houlihan Lokey has acquired Oakley Advisory, an independent advisory firm that provides a range of services to clients across the digital infrastructure, communications services, and cloud landscape.

With the addition of Oakley, Houlihan Lokey will cover the full spectrum of digital infrastructure and connectivity in the U.S. and Europe.

- Broadband and Connectivity
- Towers and Shared Infrastructure
- Data Centers and Managed Services
- Wireless and Spectrum
- Telecom Services
- Telecom Software

(1) As of April 2023. Excludes corporate MDs
 (2) As of April 2023.
 (3) LTM ended March 31, 2023.

Our Tech M&A Team Is No. 1 Globally With Unparalleled Reach

Americas

- Atlanta
- Baltimore
- Boston**
- Chicago
- Dallas
- Houston
- Los Angeles**
- Miami**
- Minneapolis
- New York**
- San Francisco**
- São Paulo
- Washington, D.C.

Europe and Middle East

- Amsterdam
- Antwerp
- Dubai
- Frankfurt**
- London**
- Madrid
- Manchester**
- Milan**
- Munich
- Paris**
- Stockholm**
- Tel Aviv**
- Zurich

Asia-Pacific

- Beijing
- Fukuoka
- Gurugram
- Hong Kong SAR
- Mumbai**
- Nagoya
- Shanghai
- Singapore
- Sydney
- Tokyo**

No. 1

GLOBAL TECH
M&A ADVISOR*

14

LOCATIONS
WORLDWIDE

231+

TECHNOLOGY
BANKERS

40+

MANAGING
DIRECTORS

























































115+

TECHNOLOGY
DEALS IN CY22

Local Technology Team

*Source: Refinitiv. Excludes accounting firms and brokers.

Deep Cybersecurity Experience Across the Ecosystem

 <p>accelerate your business</p> <p>has received investment from</p>  <p>Sellside Advisor</p>	 <p>a portfolio company of</p>  <p>HoldCo PIK Notes Acquisition Financing</p> <p>Exclusive Placement Agent</p>	 <p>has been acquired by</p>  <p>Sellside Advisor</p>	 <p>has received a growth equity investment of \$70,000,000 from</p>  <p>Financial Advisor</p>	 <p>has made a strategic investment in</p>  <p>Buyside Advisor</p>	 <p>has received a strategic growth investment from</p>  <p>Sellside Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>
 <p>has invested in</p>  <p>Financing Advisor*</p>	 <p>has received an investment from</p>  <p>Sellside Advisor*</p>	 <p>has sold a majority stake to</p>  <p>Sellside Advisor*</p>	 <p>has received an equity investment from</p>  <p>Financial Advisor</p>	 <p>has entered into a partnership with</p>  <p>Sellside Advisor*</p>	 <p>has invested in</p>  <p>Buyside Advisor*</p>	 <p>has sold a minority stake to</p>  <p>Sellside Advisor*</p>
 <p>structured equity investment led by</p>  <p>Financing Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor</p>	 <p>has sold a majority stake in</p>  <p>Sellside Advisor*</p>	 <p>has acquired</p>  <p>Buyside Advisor</p>	<p>Acquisition Financing</p>  <p>has acquired</p>  <p>Financing Advisor*</p>	 <p>has sold substantially all its assets, pursuant to Section 363 of the U.S. Bankruptcy Code, to</p>  <p>Company Advisor</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>
 <p>has been acquired by</p>  <p>Sellside Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor</p>	 <p>a portfolio company of</p>  <p>Financial Advisor</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>	 <p>has been recapitalized in partnership with</p>  <p>Sellside Advisor</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>

*Selected transactions were executed by Houlihan Lokey professionals while at other firms acquired by Houlihan Lokey or by professionals from a Houlihan Lokey joint venture company. Tombstones included herein represent transactions closed from 2010 forward.

How Houlihan Lokey Can Help


Our firm is extremely well equipped to help our clients navigate uncertain times. We respond quickly to challenging situations and are constantly helping clients to analyze, structure, negotiate, and execute the best possible solutions from both a strategic and a financial perspective.

What We Offer

1  Corporate Finance

- Mergers and Acquisitions
- Capital Markets
- Private Funds Advisory
- Board Advisory Services

We are widely recognized as a leading M&A advisor to the mid-cap and have long-standing relationships with capital providers, including commercial banks and other senior credit providers, insurance funds, asset managers, and mezzanine fund investors. Few other investment banks maintain the breadth of relationships and capital markets intelligence that we do.

2  Financial Restructuring

- Company Advisory
- Special Situations
- Distressed M&A
- Liability Management
- Creditor Advisory

We have the largest restructuring practice of any global investment bank. Since 1988, we have advised on more than 1,500 restructuring transactions (with aggregate debt claims in excess of \$3.0 trillion). We served as an advisor in 12 of the 15 largest bankruptcies from 2000 to 2022.

3  Financial and Valuation Advisory

- Portfolio Valuation and Fund Advisory
- Transaction Opinions
- Corporate Valuation Advisory Services
- Transaction Advisory Services
- Real Estate Valuation and Advisory
- Dispute Resolution Consulting

Over five decades, we have established ourselves as one of the largest financial and valuation advisory firms. Our transaction expertise and leadership in the field of valuation help inspire confidence in the financial executives, boards of directors, special committees, investors, and business owners we serve.

Why We're Different



No. 1 for U.S. and Tech M&A*



Significant Experience With Financing Markets



Senior-Level Commitment and Dedication



Deep, Industry-Specific Expertise



Superior Work Product/Technical Abilities



Creativity, Imagination, Tenacity, and Positivity

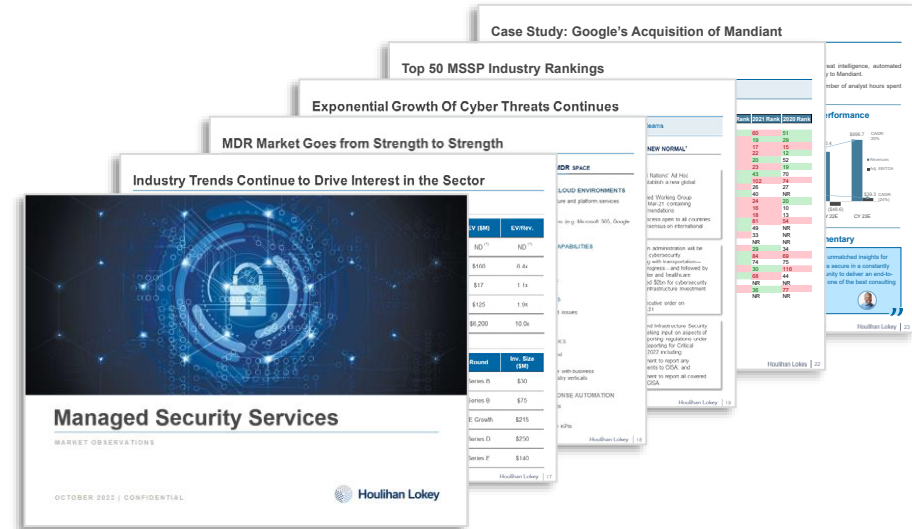
*Source: Refinitiv. Excludes accounting firms and brokers.

Other Houlihan Lokey Cyber Sector Reports

Identity Sector Report



Managed Security Services Report



To gain access to these decks, please reach out to the following:

U.S. Cyber Team



Keith Skirbe
Managing Director
Co-Head of U.S. Cyber
San Francisco
Keith.Skirbe@HL.com



Bobby Wolfe
Director
Co-Head of U.S. Cyber
Miami
BWolfe@HL.com



Tyler Deck
Vice President
Boston
TDeck@HL.com

Global Cyber Reach



Mark Smith
Head of U.K. Cyber
U.K.
Mark.Smith@HL.com



Malte Abrams
Head of DACH Cyber
Frankfurt
Malte.Abrams@HL.com



Ido Zakai
Head of Tech
Tel Aviv
Ido.Zakai@HL.com



Sara Napolitano
Head of France Cyber
Paris
Sara.Napolitano@HL.com

Capital Markets



Sean Fitzgerald
Managing Director
New York
SFitzgerald@HL.com



Chris Hebble
Managing Director
Los Angeles
CHebble@HL.com

Cyber Tech Expertise



Stephen Lee
Tech and Cyber Due Diligence
Chicago
SJLee@HL.com



Edouard Viot
Cybersecurity Consultant
Paris

Yearly Conferences



A hand is shown holding a glowing digital globe. The globe is composed of a network of interconnected nodes and lines, creating a mesh-like structure. The background is a deep blue with faint, abstract patterns of circles and lines, suggesting a digital or data environment.

V




Appendix



Houlihan Lokey

High-Growth Cybersecurity Trading Metrics

(\$ in millions)

Company	Stock Price	52-wk High	% of 52-wk High	YTD Stock Performance	Cash & ST Inv	Equity Mkt Cap	Enterprise Value	EV / Revenue			EV / EBITDA		
								CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E
 CROWDSTRIKE	\$137.26	\$242.00	56.7%	32.9%	\$2,705	\$32,024	\$30,477	13.6x	10.2x	7.9x	NM	49.7x	36.2x
 zscaler	116.83	253.74	46.0%	6.0%	1,905	16,700	16,265	12.1x	9.2x	7.2x	NM	NM	35.5x
 SentinelOne	16.36	41.68	39.3%	12.3%	624	4,545	4,125	9.8x	6.5x	4.5x	NM	NM	NM

Top Quartile	\$24,362	\$23,371	12.8x	9.7x	7.5x	NM	49.7x	36.0x
Mean	17,757	16,956	11.8x	8.6x	6.5x	NM	49.7x	35.8x
Median	16,700	16,265	12.1x	9.2x	7.2x	NM	49.7x	35.8x
1st Quartile	10,623	10,195	10.9x	7.8x	5.8x	NM	49.7x	35.6x

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of March 31, 2023.
 Note: All financials calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Financials are valued in millions except for share price.
 Sorted by Enterprise Value.

Medium-Growth Cybersecurity Trading Metrics

(\$ in millions)







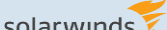





Company	Stock Price	52-wk High	% of 52-wk High	YTD Stock Performance	Cash & ST Inv	Equity Mkt Cap	Enterprise Value	EV / Revenue			EV / EBITDA		
								CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E
paloalto NETWORKS	\$199.74	\$213.63	93.5%	44.3%	\$3,347	\$63,148	\$61,051	9.9x	8.0x	6.7x	NM	30.9x	26.1x
FORTINET	66.46	71.52	92.9%	37.0%	2,211	53,520	50,984	11.5x	9.4x	7.9x	47.7x	33.6x	28.2x
Gen	17.16	27.33	62.8%	(20.6%)	812	10,476	20,283	6.5x	5.3x	5.1x	14.0x	10.0x	9.1x
okta	86.24	161.61	53.4%	24.0%	2,580	13,628	13,696	7.4x	6.3x	5.3x	NM	NM	NM
f5	145.69	215.28	67.7%	0.6%	660	8,847	8,410	3.1x	2.8x	2.7x	16.7x	8.2x	7.5x
CYBERARK	147.98	180.01	82.2%	17.2%	954	6,005	5,495	9.3x	7.5x	6.1x	NM	NM	NM
tenable	47.51	63.61	74.7%	25.4%	567	5,289	5,250	7.7x	6.5x	5.5x	NM	49.0x	36.3x
Qualys	130.02	162.36	80.1%	16.6%	321	5,116	4,474	9.1x	8.0x	7.1x	27.1x	19.3x	17.1x
RAPID7	45.91	118.25	38.8%	31.3%	291	2,688	3,379	4.9x	4.4x	3.8x	NM	42.0x	31.1x
DARKTRACE	3.19	6.94	46.0%	0.0%	380	2,092	1,774	3.7x	2.9x	2.3x	NM	16.9x	12.1x
sumo logic	11.98	12.60	95.1%	51.6%	302	1,412	1,126	3.7x	3.2x	2.9x	NM	NM	NM
ABSOLUTE	7.81	12.71	61.5%	(27.5%)	50	402	632	2.9x	2.6x	2.2x	NM	10.8x	8.4x
riskified	5.64	6.73	83.8%	22.3%	476	946	536	2.1x	1.8x	1.5x	NM	NM	NM
Nitek	9.59	15.20	63.1%	(1.2%)	71	441	492	3.3x	2.8x	NA	11.3x	10.2x	NA
W / T H ⁺ SECURE	1.66	6.05	27.4%	13.4%	74	284	236	1.6x	1.4x	1.3x	NM	NM	43.6x

Top Quartile	\$9,661	\$11,053	8.4x	7.0x	6.0x	27.1x	32.9x	30.4x
Mean	11,619	11,855	5.8x	4.9x	4.3x	23.4x	23.1x	21.9x
Median	5,116	4,474	4.9x	4.4x	4.4x	16.7x	18.1x	21.6x
1st Quartile	1,179	879	3.2x	2.8x	2.4x	14.0x	10.4x	9.8x

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of March 31, 2023.
 Note: All financials calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Financials are valued in millions except for share price.
 Sorted by Enterprise Value.

Low-Growth Cybersecurity Trading Metrics

(\$ in millions)




Company	Stock Price	52-wk High	% of 52-wk High	YTD Stock Performance	Cash & ST Inv	Equity Mkt Cap	Enterprise Value	EV / Revenue			EV / EBITDA		
								CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E
 BROADCOM	\$641.54	\$648.50	98.9%	15.9%	\$12,647	\$271,371	\$294,222	8.5x	8.2x	7.8x	14.7x	12.8x	12.3x
 splunk	95.88	150.79	63.6%	10.4%	2,007	15,569	17,972	4.9x	4.6x	4.1x	NM	24.3x	19.6x
 opentext	38.55	43.61	88.4%	28.2%	2,824	10,424	12,927	3.7x	2.3x	2.2x	13.3x	7.0x	5.8x
 CHECK POINT	130.00	145.55	89.3%	2.5%	1,638	16,419	12,223	5.2x	5.0x	4.8x	13.5x	11.6x	11.1x
 TREND MICRO	48.67	68.83	70.7%	3.7%	1,842	6,812	4,927	2.9x	2.7x	2.5x	11.5x	11.6x	10.9x
 BlackBerry	4.58	6.84	67.0%	37.9%	426	2,930	2,661	3.9x	4.1x	3.4x	NM	NM	NM
 solarwinds	8.60	13.72	62.7%	(8.7%)	149	1,383	2,520	3.5x	3.4x	3.3x	13.1x	8.6x	8.0x
 OneSpan <small>The Digital Agreement Company</small>	17.50	19.25	90.9%	50.9%	99	703	612	2.8x	2.6x	2.4x	NM	NM	NM
 Secureworks	8.57	13.54	63.3%	36.5%	144	723	603	1.3x	1.5x	1.5x	NM	NM	NM
 F-Secure	3.47	3.74	92.9%	16.9%	25	606	589	5.0x	4.7x	4.5x	14.3x	11.8x	10.7x
 Cognyte	3.39	11.80	28.7%	6.3%	57	244	252	0.8x	0.9x	0.9x	NM	NM	NA
 Telos	2.53	12.51	20.2%	(51.3%)	119	171	71	0.3x	0.6x	0.5x	NM	NM	NM

Top Quartile	\$11,710	\$12,399	4.9x	4.6x	4.2x	14.1x	12.3x	11.7x
Mean	27,280	29,132	3.6x	3.4x	3.2x	13.4x	12.5x	11.2x
Median	2,157	2,591	3.6x	3.1x	2.9x	13.4x	11.6x	10.9x
1st Quartile	678	600	2.4x	2.1x	2.0x	13.2x	10.1x	9.4x

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of March 31, 2023.
 Note: All financials calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Financials are valued in millions except for share price.
 Sorted by Enterprise Value.

High-Growth Cybersecurity Operating Metrics

(\$ in millions)

Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E	2021-2022A	2022A-2023E	2023-2024E	CY 2022A	CY 2023E	CY 2024E
 CROWDSTRIKE	\$137.26	\$32,024	\$30,477	\$2,241	\$2,998	\$3,872	(\$118)	\$613	\$841	54.4%	33.8%	29.2%	NM	20.4%	21.7%
 zscaler	116.83	16,700	16,265	1,348	1,767	2,274	(272)	323	459	56.8%	31.1%	28.7%	NM	18.3%	20.2%
 SentinelOne	16.36	4,545	4,125	422	638	915	(374)	(144)	(6)	106.1%	51.0%	43.6%	NM	NM	NM

Top Quartile	\$24,362	\$19,818	\$1,954	\$2,378	\$2,897	(\$234)	\$395	\$554	69.2%	38.1%	32.8%	NM	19.4%	21.0%
Mean	17,757	16,141	1,467	1,893	2,409	(357)	239	388	63.8%	33.2%	30.0%	NM	15.4%	17.3%
Median	15,164	14,981	1,603	1,969	2,423	(323)	244	358	55.6%	32.4%	28.9%	NM	18.3%	20.2%
1st Quartile	11,357	11,304	1,117	1,484	1,934	(446)	88	192	50.2%	27.5%	26.1%	NM	12.9%	15.1%

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of March 31, 2023.
 Note: All financials calendarized to a December year-end. NM indicates not meaningful or not disclosed. Financials are valued in millions except for share price.
 Sorted by Enterprise Value.

Medium-Growth Cybersecurity Operating Metrics

(\$ in millions)

Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E	2021-2022A	2022A-2023E	2023-2024E	CY 2022A	CY 2023E	CY 2024E
paloalto	\$199.74	\$63,148	\$61,051	\$6,156	\$7,624	\$9,121	\$245	\$1,974	\$2,341	26.7%	23.8%	19.6%	4.0%	25.9%	25.7%
FORTINET	66.46	53,520	50,984	4,417	5,410	6,462	1,069	1,518	1,808	32.2%	22.5%	19.4%	24.2%	28.1%	28.0%
Gen	17.16	10,476	20,283	3,107	3,808	3,985	1,454	2,024	2,228	12.9%	22.6%	4.6%	46.8%	53.1%	55.9%
okta	145.69	8,847	8,410	2,709	3,000	3,158	502	1,022	1,127	1.6%	10.7%	5.3%	18.5%	34.1%	35.7%
F5	86.24	13,628	13,696	1,858	2,172	2,573	(662)	165	257	37.7%	16.9%	18.5%	NM	7.6%	10.0%
CYBERARK	147.98	6,005	5,495	592	730	898	(136)	19	78	17.7%	23.4%	23.0%	NM	2.5%	8.7%
tenable	47.51	5,289	5,250	683	805	955	(43)	107	145	26.3%	17.9%	18.6%	NM	13.3%	15.2%
Qualys	130.02	5,116	4,474	490	556	631	165	232	261	19.1%	13.6%	13.4%	33.7%	41.7%	41.4%
RAPID7	45.91	2,688	3,379	685	775	898	(70)	80	109	28.0%	13.1%	15.9%	NM	10.4%	12.1%
DARKTRACE	3.19	2,092	1,774	484	603	758	35	105	147	38.5%	24.6%	25.7%	7.2%	17.4%	19.4%
sumo logic	11.98	1,412	1,126	301	348	394	(110)	(30)	(20)	24.2%	15.7%	13.3%	NM	NM	NM
ABSOLUTE	7.81	402	632	215	247	292	9	59	75	38.7%	14.5%	18.3%	4.0%	23.8%	25.7%
riskified	5.64	946	536	261	301	356	(105)	(23)	(3)	14.0%	15.1%	18.4%	NM	NM	NM
Mittek	9.59	441	492	151	173	-	43	48	-	19.5%	14.3%	NA	28.7%	27.9%	NA
W / T H [®] secure	1.66	284	236	144	167	187	(44)	(9)	5	(2.6%)	15.9%	12.1%	NM	NM	2.9%

Top Quartile	\$20,531	\$19,818	\$1,954	\$2,378	\$2,897	(\$234)	\$395	\$554	69.2%	38.1%	32.8%	NM	19.4%	21.0%
Mean	16,724	16,141	1,467	1,893	2,409	(357)	239	388	63.8%	33.2%	30.0%	NM	15.4%	17.3%
Median	15,164	14,981	1,603	1,969	2,423	(323)	244	358	55.6%	32.4%	28.9%	NM	18.3%	20.2%
1st Quartile	11,357	11,304	1,117	1,484	1,934	(446)	88	192	50.2%	27.5%	26.1%	NM	12.9%	15.1%

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of March 31, 2023.
 Note: All financials calendarized to a December year-end. NM indicates not meaningful or not disclosed. Financials are valued in millions except for share price.
 Sorted by Enterprise Value.

Low-Growth Cybersecurity Operating Metrics

(\$ in millions)

Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2022A	CY 2023E	CY 2024E	CY 2022A	CY 2023E	CY 2024E	2021-2022A	2022A-2023E	2023-2024E	CY 2022A	CY 2023E	CY 2024E
BROADCOM	\$641.54	\$271,371	\$294,222	\$34,412	\$35,843	\$37,500	\$20,005	\$22,921	\$23,828	20.7%	4.2%	4.6%	58.1%	63.9%	63.5%
splunk	95.88	15,569	17,972	3,654	3,896	4,409	(126)	739	918	36.7%	6.6%	13.2%	NM	19.0%	20.8%
opentext	38.55	10,424	12,927	3,534	5,607	5,952	972	1,851	2,221	2.9%	NM	6.1%	27.5%	33.0%	37.3%
CHECK POINT	130.00	16,419	12,223	2,330	2,433	2,534	909	1,057	1,099	7.5%	4.4%	4.1%	39.0%	43.5%	43.4%
TREND MICRO	48.67	6,812	4,927	1,697	1,837	1,975	429	425	453	2.6%	8.3%	7.5%	25.3%	23.1%	22.9%
BlackBerry	4.58	2,930	2,661	690	656	773	(91)	(61)	46	(7.1%)	(5.0%)	18.0%	NM	NM	5.9%
solarwinds	8.60	1,383	2,520	719	733	764	192	295	316	0.1%	1.9%	4.2%	26.7%	40.2%	41.4%
OneSpan <small>The Digital Agreements Company</small>	17.50	703	612	219	237	258	(7)	4	12	2.1%	8.1%	8.8%	NM	1.8%	4.7%
Secureworks	8.57	723	603	463	391	404	(111)	(35)	2	(13.4%)	(15.7%)	3.4%	NM	NM	0.5%
F-Secure	3.47	606	589	119	126	132	41	50	55	(1.8%)	6.5%	4.6%	34.8%	39.4%	41.4%
Cognyte	3.39	244	252	315	288	295	(64)	0.1	-	(33.6%)	(8.6%)	2.6%	NM	0.03%	NM
Telos	2.53	171	71	217	127	134	(49)	(23)	(7)	(10.5%)	(41.4%)	5.7%	NM	NM	NM

Top Quartile	\$8,618	\$8,575	\$2,013	\$2,135	\$2,255	\$669	\$741	\$776	2.8%	6.0%	6.8%	37.9%	41.0%	41.4%
Mean	28,344	30,146	4,065	4,389	4,611	2,020	2,408	2,548	(2.8%)	(3.7%)	6.3%	35.2%	30.6%	29.0%
Median	1,383	2,520	690	656	764	41	50	55	0.1%	3.0%	4.6%	31.2%	36.2%	37.3%
1st Quartile	654	596	267	262	276	(57)	(11)	7	(8.8%)	(7.7%)	4.2%	26.9%	17.8%	5.9%

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of March 31, 2023.
 Note: All financials calendarized to a December year-end. NM indicates not meaningful or not disclosed. Financials are valued in millions except for share price.
 Sorted by Enterprise Value.

Disclaimer

© 2023 Houlihan Lokey. All rights reserved. This material may not be reproduced in any format by any means or redistributed without the prior written consent of Houlihan Lokey.

Houlihan Lokey is a trade name for Houlihan Lokey, Inc., and its subsidiaries and affiliates, which include the following licensed (or, in the case of Singapore, exempt) entities: in (i) the United States: Houlihan Lokey Capital, Inc., and Houlihan Lokey Advisors, LLC, each an SEC-registered broker-dealer and member of FINRA (www.finra.org) and SIPC (www.sipc.org) (investment banking services); (ii) Europe: Houlihan Lokey Advisory Limited, Houlihan Lokey EMEA, LLP, Houlihan Lokey (Corporate Finance) Limited, and Houlihan Lokey UK Limited, authorized and regulated by the U.K. Financial Conduct Authority; Houlihan Lokey (Europe) GmbH, authorized and regulated by the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht); (iii) the United Arab Emirates, Dubai International Financial Centre (Dubai): Houlihan Lokey (MEA Financial Advisory) Limited, regulated by the Dubai Financial Services Authority for the provision of advising on financial products, arranging deals in investments, and arranging credit and advising on credit to professional clients only; (iv) Singapore: Houlihan Lokey (Singapore) Private Limited and Houlihan Lokey Advisers Singapore Private Limited, each an “exempt corporate finance adviser” able to provide exempt corporate finance advisory services to accredited investors only; (v) Hong Kong SAR: Houlihan Lokey (China) Limited, licensed in Hong Kong by the Securities and Futures Commission to conduct Type 1, 4, and 6 regulated activities to professional investors only; (vi) India: Houlihan Lokey Advisory (India) Private Limited, registered as an investment adviser with the Securities and Exchange Board of India (registration number INA000001217); and (vii) Australia: Houlihan Lokey (Australia) Pty Limited (ABN 74 601 825 227), a company incorporated in Australia and licensed by the [Australian Securities and Investments Commission](http://www.afsl.gov.au) (AFSL number 474953) in respect of financial services provided to wholesale clients only. In the United Kingdom, European Economic Area (EEA), Dubai, Singapore, Hong Kong, India, and Australia, this communication is directed to intended recipients, including actual or potential professional clients (UK, EEA, and Dubai), accredited investors (Singapore), professional investors (Hong Kong), and wholesale clients (Australia), respectively. Other persons, such as retail clients, are NOT the intended recipients of our communications or services and should not act upon this communication.

Houlihan Lokey gathers its data from sources it considers reliable; however, it does not guarantee the accuracy or completeness of the information provided within this presentation. The material presented reflects information known to the authors at the time this presentation was written, and this information is subject to change. Any forward-looking information and statements contained herein are subject to various risks and uncertainties, many of which are difficult to predict, that could cause actual results and developments to differ materially from those expressed in, or implied or projected by, the forward-looking information and statements. In addition, past performance should not be taken as an indication or guarantee of future performance, and information contained herein may be subject to variation as a result of currency fluctuations. Houlihan Lokey makes no representations or warranties, expressed or implied, regarding the accuracy of this material. The views expressed in this material accurately reflect the personal views of the authors regarding the subject securities and issuers and do not necessarily coincide with those of Houlihan Lokey. Officers, directors, and partners in the Houlihan Lokey group of companies may have positions in the securities of the companies discussed. This presentation does not constitute advice or a recommendation, offer, or solicitation with respect to the securities of any company discussed herein, is not intended to provide information upon which to base an investment decision, and should not be construed as such. Houlihan Lokey or its affiliates may from time to time provide investment banking or related services to these companies. Like all Houlihan Lokey employees, the authors of this presentation receive compensation that is affected by overall firm profitability.



Houlihan Lokey



CORPORATE FINANCE
FINANCIAL RESTRUCTURING
FINANCIAL AND VALUATION ADVISORY

HL.com