Houlihan Lokey

Cybersecurity Quarterly Update

Third Quarter 2024

Global Cybersecurity Team

U.S. Cyber Team

Keith Skirbe
Managing Director
San Francisco

Bobby Wolfe
Director
Miami

Joseph Miller
Vice President
San Francisco

Patrick Wong
Associate
San Francisco

Alex Maffei
Financial Analyst
San Francisco

Capital Markets

Sean Fitzgerald
Managing Director
New York

Chris Hebble
Managing Director
Los Angeles

David Kelnar
Managing Director
London

Greg Werntz
Director
San Francisco

Global Cyber Reach

Mark Smith
Director
Cyber Europe
U.K.

Malte Abrams
Managing Director
Cyber Europe
Frankfurt

Sara Napolitano
Managing Director
Cyber Europe
Paris

Ido Zakai
Managing Director
Tel Aviv

Raymond Fröjd
Managing Director
Stockholm

Sameer Jindal
Managing Director
Mumbai

Gabrielle Worrall
Vice President
U.K.

Christie Adams
Associate
Paris

Samuel Pattison
Financial Analyst
U.K.

Cybersecurity Technology Expertise

Joshua Holmes
Head of Cyber and Tech Due Diligence
Dallas

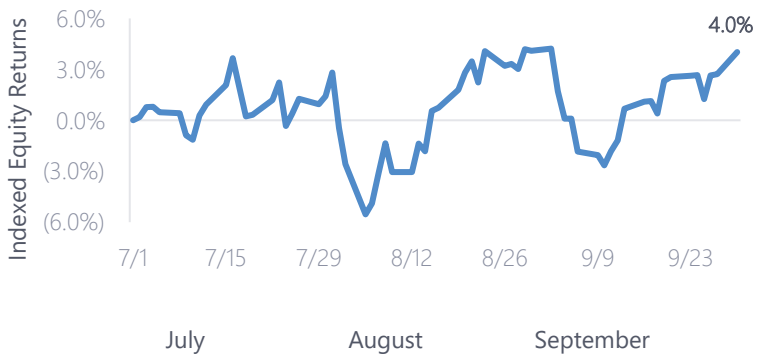
Executive Summary: Q3 2024 in Review

Executive Summary

- Q3 saw a **substantial recovery in M&A activity** propelled by a significant uptick in deal volume, primarily composed of small to medium sized transactions (<$100M).
- Capital invested experiences strong growth as investors exhibit more **conviction in the macroeconomic outlook**, with the highest amount of Q3 financing since 2021.
- We anticipate activity to continue rising in 2025, driven by an improving economy and lower interest rates with a high accumulation of dry powder.
- This past quarter, **Trend Micro** and **CrowdStrike** saw the greatest stock price movements, with the former surging 41.1%—near its all-time high—and the latter falling 28.5% as a result of its global platform outage.

A Strong Quarter for Public Companies

Houlihan Lokey Cybersecurity Index[1]



Q3 2024 Report Themes

The MDR landscape is fragmented, consisting of subscale and under-optimized players, presenting an attractive consolidation opportunity

Cybersecurity insurance offers a compelling value proposition as attacks have become more costly and occur more frequently.

Many organizations are assessing their cybersecurity posture as they consider a transition to the cloud.

Proliferation of APIs has led to increased vulnerabilities to be exploited by threat actors.

Generative AI has become a priority security implementation as threat actors seek to leverage the technology with malicious intent.

Securing the entire IoT ecosystem has become a top priority, as organizations look to innovative and zero-trust solutions.

M&A Volume Rebounds

	Q3 '24	VS. Q3 '23	VS. Q3 '22
Volume	$10.9B	↗ 18.1%[2]	↘ 13.8%
# of Deals	102	↗ 64.5%	↗ 61.9%

Acronis $4,000M

Recorded Future® $2,650M

Own $2,111M

Financing Volume Spikes, Underscored by More Deals

	Q3 '24	VS. Q3 '23	VS. Q3 '22
Volume	$3.2B	↗ 38.3%	↗ 3.1%
# of Deals	209	↗ 111.1%	↘ 5.9%

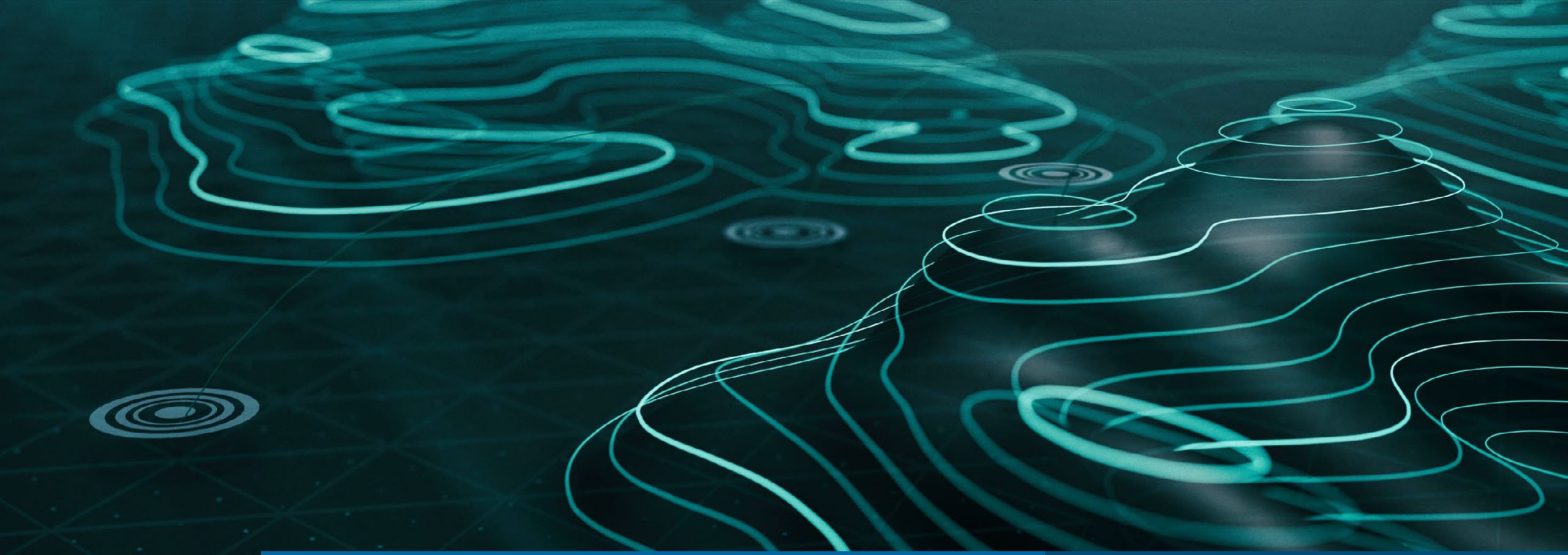
Kiteworks $456M

Cribl $319M

Abnormal $250M

Source: S&P Capital IQ as of September 30, 2024.
(1) Houlihan Lokey Cybersecurity Index includes S, CYBR, ZS, CRWD, PANW, OKTA, TENB, FTNT, AVGO, MITK, RSKD, RPD, GEN, CHKP, FFIV, QLYS, 4704, SWI, CGNT, SCWX, OSPN, TLS, FSECURE, WITH.
(2) Figure excludes the acquisition of Splunk.

Table of Contents



Perspectives From the Front

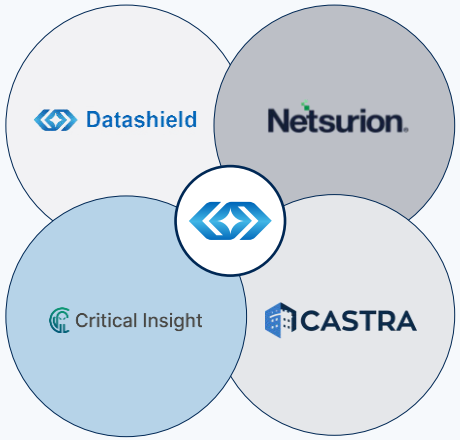
01

Rolling-Up the MDR Sector With a Technology-First Approach

lumifi Lumifi is a software-driven MDR consolidator purpose-built to unlock value by driving rapid and profitable growth through M&A while leveraging cutting-edge technology to extract synergies and maintain software-like gross margins.

Strong M&A Strategy Execution to Date

With **four strategic acquisitions** completed in the past three years, Lumifi has already established itself as **a leader in MDR** across a breadth of end markets.



> *Lumifi's consolidation strategy is built on more efficient delivery, improved client management, and greater sales enablement driven by the breadth and flexibility of the platform—with the combination of ShieldVision and a SOC triad-led perspective on security data visibility, Lumifi has optimized the MDR model and created the blueprint for profitability at scale.*

Michael Malone, Founder and CEO

Key Thesis for MDR Consolidation

Relentless Cyber Attacks and Talent Shortage Driving MDR Services Growth

By 2025, the global cost of cybercrime is projected to reach **$10.5 trillion, with 50% of organizations using MDR services** for threat monitoring, detection, and response functions.

MDR at Scale With a Strong Financial Profile Has Been Elusive

Vendors have experimented with various operating strategies to address industry pitfalls, but challenges have arisen elsewhere. Lumifi is cracking the code on a **scaled, highly profitable MDR model**.

Tech Powering MDR Is Commoditized and Creates Tech Debt for Operators

Thirteen vendors have been identified as SIEM leaders by Gartner since 2011, but **only one has maintained that classification.** Specialization or proprietary SIEMs leave MDRs with tech debt; **true BYOT platforms hold a competitive advantage.**

Fragmentation Presents an Opportunity for Profitable, Tech-Enabled Consolidation

Gartner estimates that **nearly 600 organizations offer MDR services**, most of which are **subscale or overstaffed and unprofitable.** The bar for market leadership is low, and the current nature of the industry makes it an attractive segment for consolidation.

Lumifi at a Glance

A Differentiated Approach to MDR

- Full-spectrum, correlated visibility across SOC triad.
- Powered by 400+ proprietary D&R rules and 50% SOC automation.
- High efficacy, flexible BYOT approach to technology.
- Robust SOC powered by world-class ShieldVision technology.
- Delivering unmatched performance.

2022
Founded

4
Acquisitions to Date

55+
Cyber/Technical Team SOC

ShieldVision
Powered by Industry-Leading Technology

Source: Company website, Gartner, Pitchbook.

SentinelOne: 2024 Cloud Security Report

SentinelOne

Many organizations are currently navigating a transition to the cloud, presenting opportunities for threat actors to identify vulnerabilities and disrupt operations through malicious cyber attacks, requiring teams to establish a comprehensive cloud security plan which often encounters issues through fragmented functionalities and inefficiencies.

Key Insights

1. **Cloud Security Is No Longer a Niche**

   Migrations to the cloud have presented new challenges, enabling nearly every cybersecurity domain to play a role in the adoption of cloud security.

2. **Organizational Confidence, Balanced by Concern**

   Core functions (threat detection, incident investigation, and vulnerability assessment) provide organizations reassurance in their cloud security capabilities. However, cloud asset discovery and configuration security remain areas of concern.

3. **Several Factors Are Inhibiting Effective Responses**

   A shortage of experienced IT security personnel, overwhelming volumes of security data, and insufficient automation are preventing comprehensive responses.

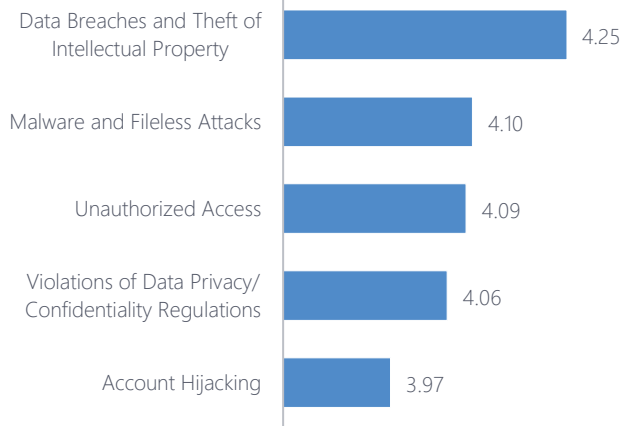
4. **A Unified Platform Is Desired for Simplicity**

   The highly tailored nature and narrow use cases of cloud security solutions have led organizations to struggle with managing multiple-point products and are now seeking out unified platforms which will integrate data silos, simplify management, and automate workflows.

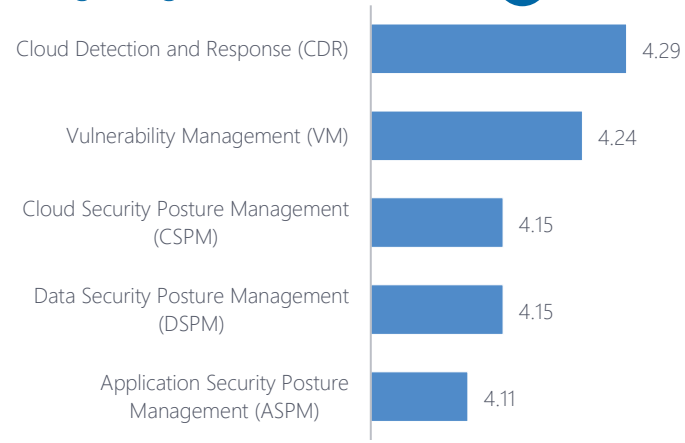
Key Conclusions

- Organizations will gravitate toward solutions that are easily deployed and can automate workflows.
- Secret scanning solutions are becoming increasingly popular as organizations seek to identify exposed credentials.
- Security budgets are adequate, but the desired results are not being achieved.
- The shortage of skilled cybersecurity professionals will continue to drive demand for automation, integrations, and the implementation of AI use cases.

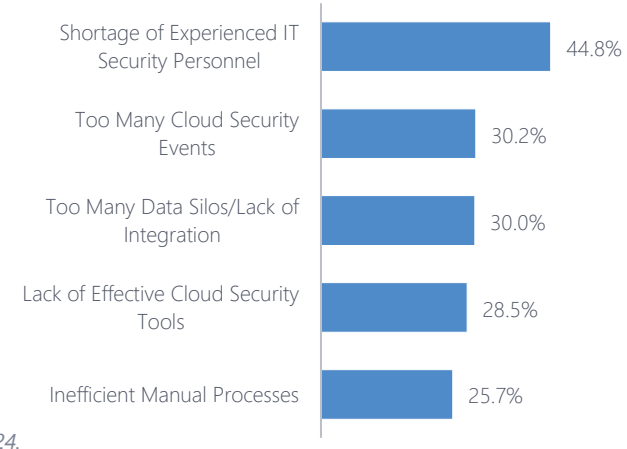
Perceived Concerns[1] 1



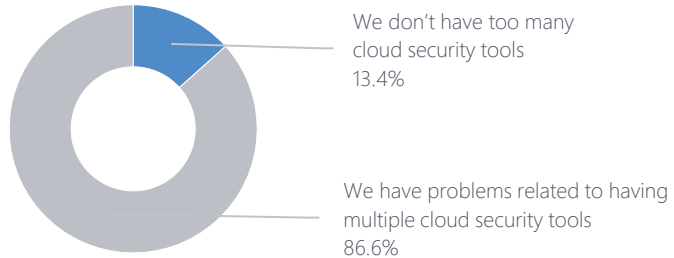
Recognizing the Desired Tools[2] 2



Barriers to Implementation 3



Defining the Need for a Unified Solution 4



Source: SentinelOne, "2024 Cloud Security Report," August 2024.
Note: The survey group consisted of 400 cybersecurity practitioners and managers who were knowledgeable about their organizations' cloud security strategy.
(1) Responses on a 1–5 scale, rating the organizational capabilities of each cloud security function.
(2) Responses on a 1–5 scale, rating the importance of each cloud security technology for protecting cloud infrastructure.

Akamai—2024 State of the Internet Report: Digital Fortresses Under Siege

The proliferation of APIs, serving as the bedrock for communication among applications, has revealed a new pillar of web application security that is a strategic imperative for any organization's security stack.

Key Findings

Threat actors are more frequently targeting web application and API vulnerabilities, **capitalizing on the growing pains of the API economy**.

Time-to-market pressures and the unique complexities of the API environment have left organizations with **cross-team visibility gaps in API footprints**, leading to an incomplete view of the security landscape and presenting an opportunity for cybercriminals.

Application-layer **(Layer 7) DDoS attacks are becoming increasingly prevalent**, exploiting flaws and loopholes in the business logic.

Contextualizing the Breadth of Attacks

49%

Increase in web attacks against applications and APIs between Q1 2023 and Q1 2024.

11 Trillion+

Application-layer DDoS attacks against the high technology, commerce, and social media industries.

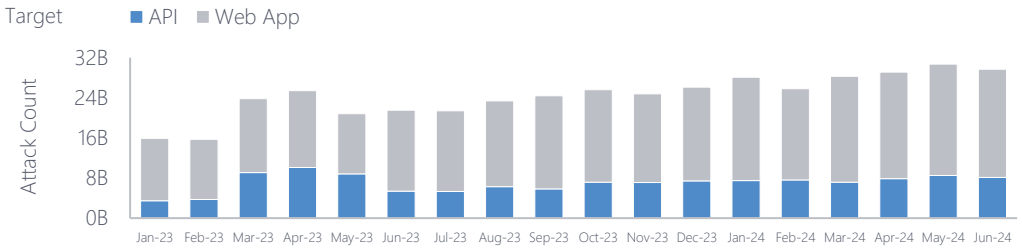
26 Billion+

Monthly web application and API attacks in June 2024, corroborating the vulnerabilities of an expanded attack surface.

Progression of Attacking Frequency(1)

Monthly Web Application and API Attacks
January 1, 2023 – June 30, 2024

Attackers Are Increasing Their Use of Traditional Web Attacks to Target Web Applications and APIs, as Exemplified by the 49% Year-Over-Year Growth

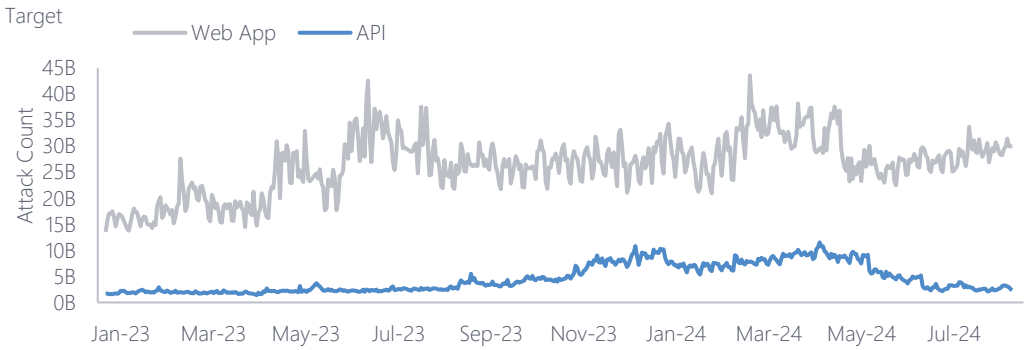


Most Targeted Industries

- Financial Services
- Commerce
- Social Media

Daily Layer 7 DDoS Attacks
January 1, 2023 – June 30, 2024

Layer 7 DDoS attacks on APIs increased significantly during Q4 of 2023 and persisted through Q1 of 2024



- Layer 7 refers to the application layer, which serves as the interface for communication between a network and its users—threat actors will exploit vulnerabilities in this layer, carrying out DDoS attacks to halt or disrupt operations.

Source: Akamai "Digital Fortresses Under Siege: Threats to Modern Application Architecture," August 2024.
(1) Figures are illustrative reconstructions, not exact data points.

Delinea: Identity Security Is Critical to Obtaining and Maintaining Cyber Insurance

Delinea

Cyber insurance is paramount to organizational risk management strategies, ensuring resiliency and recovery when confronted with data breaches, data losses, or revenue losses from interrupted operations; it becomes necessary to maintain insurability as security stacks adapt to more sophisticated adversaries.

Key Findings

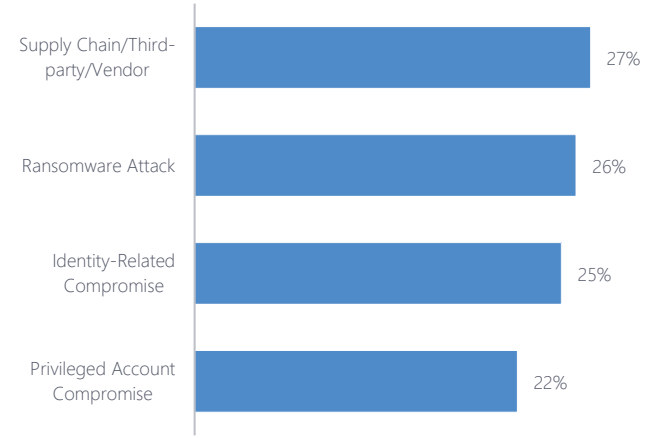
Identity and privilege compromises account for 47% of attacks that lead to insurance claims, highlighting the importance of comprehensive identity security solutions.

Identity security is often regarded as a prerequisite to obtaining an insurance policy, with roughly **40%** of insurance companies **requiring privileged access controls and authorization**.

Cyber insurance premiums are increasing; however, there is an opportunity for policyholders to **leverage AI-supported threat detection and monitoring** to reduce these obligations.

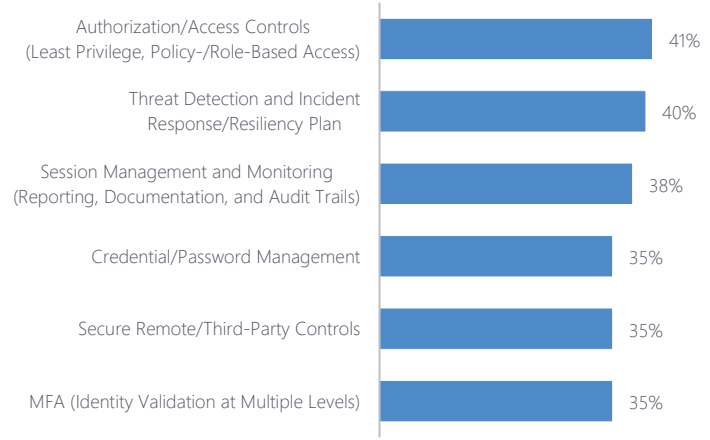
Determining the Source of Claims

What caused the cyber incident related to the cyber insurance claim?(1)



Defining the Prerequisites

What security controls, activities, and processes are required by your cyber insurance policy?(1)



Understanding the Frequency of Claims

77%

Of firms with cyber insurance have **previously filed** a claim, underscoring the importance of insurance policies.

50%

Of U.S. companies **utilizing AI-supported threat monitoring and detection tools** to drive down insurance premiums.

27%

Of organizations **filed more than one cyber insurance claim** in the past 12-month period.

> When I think about insurance carriers' and underwriters' expectations, identity security has become table stakes… You must have a good narrative of integrated controls and a holistic story on how you're mitigating unauthorized access risk and protecting identities.

CJ Dietzman, Senior Vice President, Alliant Insurance Services

> The greater portion of cybersecurity incidents that have reached the level of a claim are root-caused back to harvesting a credential, compromising an insider, using a third party that had access to your systems, etc., so when organizations are being evaluated for renewals, these are the questions that are asked.

Myrna Soto, CEO, Apogee Executive Advisors

Source: Delinea, "Identity Security is Critical to Obtaining and Maintaining Cyber Insurance," September 2024.
(1) Research study consisting of 300 decision-makers.

Cybersecurity Predictions for 2024

Industry Predictions

Generative AI

- Threat actors are leveraging generative AI to carry out fraudulent activities, accelerating the volume and targeted nature of phishing and malware creation.
- Generative AI is expected to address talent shortages by enhancing security professionals' efficiency, particularly regarding vulnerability investigation and tool creation.

IoT Security Is an Imperative

- By 2025, 27 billion IoT devices are predicted to be in use, resulting in additional attack surfaces for threat actors to target.
- Zero-trust security, API security, and innovative security solutions combating AI and quantum threats are all becoming security stack imperatives.

What Happened

- Organizations are feeling the pressure to incorporate AI solutions, resulting in rushed and incomplete implementation processes, exposing security vulnerabilities and underscoring an overall misuse of generative AI in cybersecurity contexts. Further, more than 50% of executives will attribute their weakening cybersecurity posture to the expanded attack surface due to the complexity of AI applications.
- With the EU and the U.S. enacting legislation to address concerns over consumer data privacy and IoT cybersecurity, IoT security is no longer an unregulated frontier. However, a comprehensive IoT legal framework still does not exist.
- The shift towards IoT security is underscored by the proliferation of connected devices/data as firms do more to address the costly nature of data breaches, which are estimated to cost an organization approximately $4.88 million on average.

Unintended Consequences

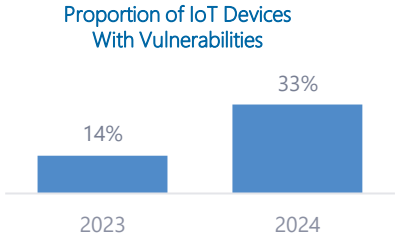
45%

Of organizations have experienced unintended data exposures since AI implementation.

40%

Of IT leaders indicate their security teams do not have the skills needed to protect AI workloads and applications.

IoT Vulnerability Tracking



136%

Growth in IoT devices containing vulnerabilities.

Sources: Cybersecurity Dive, "Generative AI Raises Security Concerns Among IT Leaders"; Dark Reading, "Friend or Foe? AI's Complicated Role in Cybersecurity"; IoT For All, "The Future of IoT Security: Trends and Predictions"; IBM, "Cost of a Data Breach Report 2024"; Infosecurity Magazine, "IoT Vulnerabilities Skyrocket, Becoming Key Entry Point for Attackers"; The Hacker News, "The State of the Virtual CISO Report: MSP/MSSP Security Strategies for 2025."
(1) Independent survey of 200 security leaders in MSPs and MSSPs.

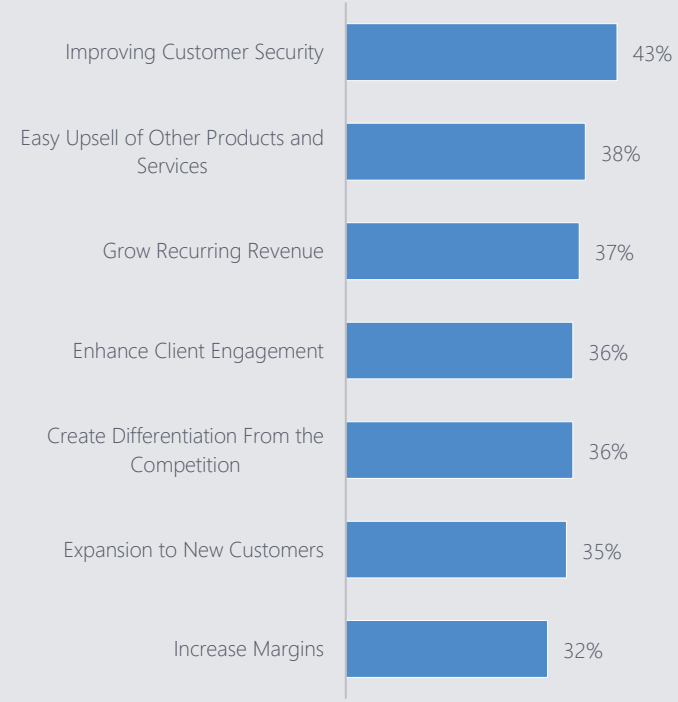
What Was Not Predicted: Growth of Virtual CISO Services

Currently, only **21% of MSPs and MSSPs are offering virtual CISO services**, indicating an opportunity for firms to establish themselves as key players within the ecosystem.

98% of MSPs and MSSPs that are not currently offering virtual CISO services **intend to integrate these services** into their portfolios, demonstrating an observed demand from SMBs for specialized cybersecurity and compliance expertise.

Defining the Strategic Opportunity: Perceived Benefits

Impact of offering virtual CISO services?(1)



RockYou2024

Breach Overview

Description	Compilation of plaintext passwords assembled from various breaches over the years, building upon RockYou2021.
Date of Discovery	July 4, 2024.
What Happened	A dataset was posted to a hacking forum, combining information across breaches from the past two decades and exposing nearly 10 billion unique plaintext passwords.
Outcome of Breach	A consolidated and searchable database of leaked passwords is now available to threat actors, heightening the risk of credential-stuffing attacks.

Key Stats

~10.0B

Unique plaintext passwords leaked.

~1.5B

New passwords since the previous RockYou2021 data leak.

Attack Methodology and Rationale

An anonymous user known as "ObamaCare" scraped information from previous data breaches, gathering leaked passwords and sensitive data.

By combining the previous and newly leaked plaintext passwords into one encompassing and easily accessible database, hackers can more effectively carry out brute-force attacks and gain unauthorized access to accounts and sensitive information.

Expert Opinion and Commentary

"Companies should assume all passwords are compromised and build the correct mitigating controls. Those include phishing-resistant MFA, passwordless authentication, and behavior-based detection and response programs to detect malicious use."

Chris Bates
Former Chief Security & Trust Officer, SentinelOne

The Outcome

The sheer size of the leaked list makes credential-stuffing impractical, given the time it would require to iterate through such a list as well as the many protection mechanisms such as rate limiting and multiple attempts limiting.

Some analyses suggest that a substantial portion of the dataset may consist of junk data, such as uncracked hashed passwords and random strings, potentially limiting its effectiveness for malicious use.

Key Takeaway

Stringent Password Protection and Protocol

This incident highlights the importance of rotating or maintaining a variety of passwords, preventing threat actors from gaining unauthorized access.

Given the frequency and severity of data leaks and breaches, it is critical for organizations to implement defensive password policies and require multifactor authentications to safeguard sensitive information.

Sources: IT Security Guru, "RockYou2024: 10 Billion Unique Passwords Exposed – What Now?"; Check Point Software, "How Big is Too Big (Of a Password List)? An Analysis of the RockYou2024 Password Leak".

CROWDSTRIKE

Outage Overview

Company Description	Cloud-native provider of a threat intelligence and endpoint protection platform.
Date of Breach	July 22, 2024.
What Happened	Faulty code in the Falcon Sensor software update files resulted in widespread tech outages for those customers using Microsoft Windows operating systems.
Outcome of Breach	Critical services and infrastructures were interrupted or halted entirely.

Key Stats

$0.3B–$1.0B

Estimated insured losses connected to the global IT outage.

$5.4B

Estimated financial impact on Fortune 500 from the disruption, excluding the impact on Microsoft.

10,000+

Flight cancellations affected an estimated 1.4 million passengers.

28.5%

Decrease in the stock price over Q3 2024.

Source of the Outage

CrowdStrike confirmed the outage originated from an internal source, re-establishing confidence in the firm's endpoint protection platform.

Cybersecurity experts are drawing their attention to the chain effects of single points of failure in the IT ecosystem.

Expert Opinion and Commentary

"The fact that something like this could happen should open people's minds to the real risks of technical monocultures."

Spencer Kimball
Chief Executive Officer, Cockroach Labs

The Outcome

The outage represents a stress test against first-line IT support teams, showcasing a reliance and susceptibility to third-party disruptions.

Following the CrowdStrike outage, Delta filed a lawsuit asking for damages to cover more than $500 million in losses. The lawsuit alleges disrupted operations and the cancellation of more than 7,000 flights within a week.

Key Takeaway

Impeccable Records Are a Must

Reputation is everything in cybersecurity and experiencing outages or breaches degrades customer trust and shifts the organizational perception.

The outage constitutes an opportunity for organizations to re-evaluate their level of preparedness and to consider shifting away from technical monocultures.

Sources: Cybersecurity Dive, "Top Takeaways from the CrowdStrike Outage for IT Teams"; Cybersecurity Dive, "Insured Loss Impact Could Reach $1B Following CrowdStrike Outage"; Reuters, "CrowdStrike Update that Caused Global Outage Likely Skipped Checks, Experts Say"; CNBC, "Delta, CrowdStrike Sue Each Other Over Widespread IT Outage that Caused Thousands of Cancellations"; Oxford Economics, "CrowdStrike Update Grounds Thousands of Flights."

National Public Data

Breach Overview

Description	National Public Data is a background-checking company that utilizes nonpublic sources to scrape personally identifiable information.
Date of Breach	August 19, 2024.
What Happened	A federal class-action lawsuit alleges that a hacking group has gained unauthorized access to the network of National Public Data, exposing nearly three billion people's personal information.
Outcome of Breach	Hackers have launched a sale of the stolen data, looking to fetch around $3.5 million in exchange for the database.

Key Stats

170.0M+

Individuals with highly sensitive personal data were exposed.

2.9B

Records were identified as being exposed during this breach.

Attack Methodology and Rationale

USDoD, the entity responsible for carrying out the breach, leveraged vendor system vulnerabilities and exploited third-party risk management practices.

The prompt auctioning of the compromised information on the dark web indicates the attack was financially motivated.

Expert Opinion and Commentary

"What makes this breach a little bit different is some of the data is also about relationships — so who are your family members, who are people that you've worked with — and this makes consumers susceptible to all sorts of other types of attacks."

Steve Grobman
Chief Technology Officer, *McAfee*

The Outcome

A database containing billions of highly sensitive records, including full names, Social Security numbers, phone numbers, and physical addresses, has been made available for purchase.

The scale and sensitive nature of the information compromised underscores an opportunity for threat actors to gain unauthorized access and carry out targeted phishing attempts.

Key Takeaway

Reinforce Cyber Posture and Maintain Vigilance

This breach spotlights how highly sensitive and identifiable information can be held by organizations unbeknownst to individuals. Thus, it is imperative to thoroughly vet third-party cybersecurity postures to secure the entire data journey.

Individuals should proactively monitor the use of their sensitive data, ensuring no fraudulent behavior is occurring, and remain aware of the increasingly targeted phishing attempts resulting from compromised data.

Sources: Scripps News, "Cybersecurity Expert Urges Consumers to Take Precautions After Massive Data Breach"; USA Today, "National Public Data Confirms Massive Data Breach Included Social Security Numbers."

Port of Seattle and Halliburton Oilfield

Entity Overview

Description	The Port of Seattle is a government agency overseeing both Seattle's seaport and the Sea-Tac airport, and Halliburton is the second-largest provider of energy services in the U.S.
Date of Discovery	August 21, 2024, and August 24, 2024.
What Happened	The Port of Seattle and Halliburton reported outages of internet and web-based systems due to alleged cyberattacks.
Outcome of Breach	System outages resulted in operational disruptions or required taking devices offline to isolate and investigate the issues.

Key Stats

$6.0M

Demanded in Bitcoin in exchange for the documents stolen from the Port of Seattle.

$4.4M

Precedent established among U.S. energy firms after Colonial Pipeline paid the amount in ransom due to a similar breach in 2021.

Attack Methodology and Rationale

Unauthorized access to Halliburton's IT environment enabled threat actors to steal sensitive data and disrupt certain Halliburton business applications.

A highly coordinated and sophisticated attack involving a combination of advanced persistent threats (APTs) and ransomware was used to infiltrate the Sea-Tac network, likely exploiting system vulnerabilities or compromised employee credentials to gain access to sensitive data.

Expert Opinion and Commentary

"Many companies still rely on outdated cybersecurity measures. All critical infrastructure operators must adopt zero-trust cybersecurity solutions, as this model has become essential in the fight against evolving threats."

Roman Arutyunov
Co-Founder and Senior Vice President, Xage Security

The Outcome

The Port of Seattle breach did not result in mass flight delays or cancellations, but interruptions were experienced with in-terminal screen and baggage services. The full scale of damages is still relatively unknown.

Halliburton was made aware of an unauthorized third-party access to its systems and was forced to take certain systems offline as part of the incident response.

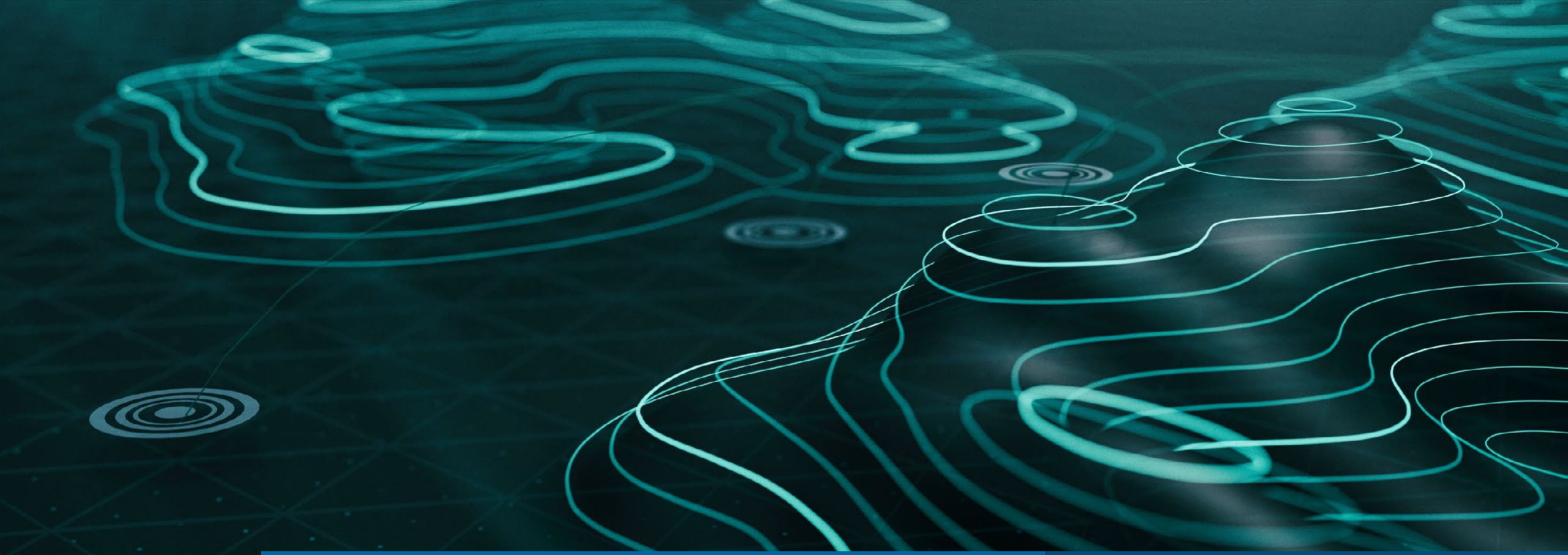
Key Takeaway

The Importance of Securing Critical Infrastructure

This incident highlights a substantial technological gap in the security posture of many organizations and underscores the need for rigorous security protocols and solutions.

The breach also reinforces the need for swift and comprehensive incident response practices to minimize the potential consequences of such attacks.

Sources: Industrial Cyber, "Critical Infrastructure Continues Under Threat, as Hackers Strike at Port of Seattle and Halliburton Oilfield" ; Reuters, "Top US Oilfield Firm Halliburton Hit by Cyberattack, Source Says"; AP News, "Hackers Demand $6 Million for Files Stolen From Seattle Airport Operator in Cyberattack".



Capital Markets and Trends Update

02

Cybersecurity Dashboard

Public Market Environment

The cybersecurity sector experiences moderate decline; however, low-growth candidates experience outsized growth.

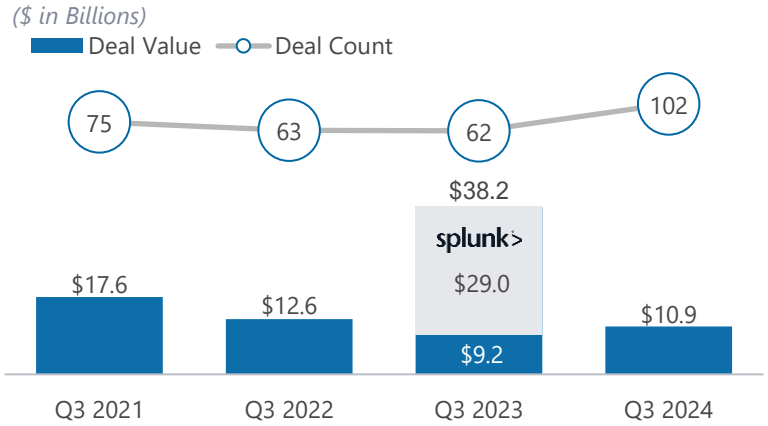
High-Growth	High-Growth Index Performance[1]	↘ 4.2% | ↗ 47.7% Q3 '24 | LTM
Medium-Growth	Medium-Growth Index Performance[2]	↘ 5.7% | ↗ 21.8% Q3 '24 | LTM
Low-Growth	Low-Growth Index Performance[3]	↗ 11.7% | ↗ 30.6% Q3 '24 | LTM

Selected Cybersecurity Performance Q3 2024

TREND MICRO ↗ 41.1%	OneSpan ↗ 30.3%
FORTINET ↗ 29.6%	f5 ↗ 28.6%
Secureworks ↗ 28.3%	SentinelOne ↗ 17.5%
CHECK POINT ↗ 16.9%	F-Secure ↗ 15.6%

M&A Environment

A significant increase in the volume of transactions underscores the thawing dealmaking environment.



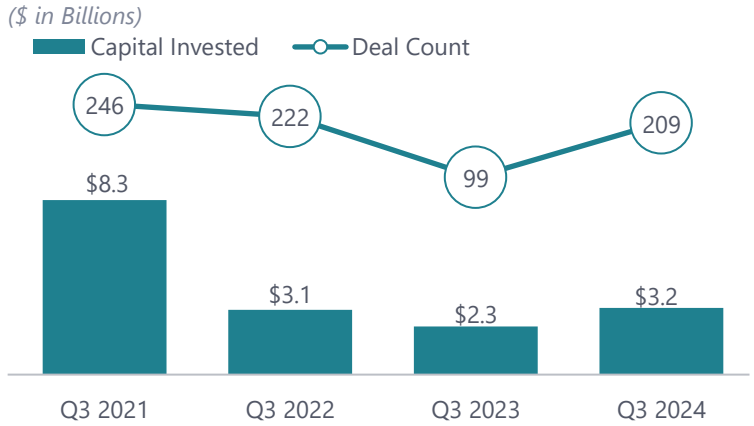
Selected Q3 Transactions

($ in Millions)

Ann. Date	Acquirer	Target	EV	EV/Rev
Sep. 12	mastercard	Recorded Future	$2,650	7.8x
Sep. 05	salesforce	Own	$2,111	8.4x
Aug. 26	CHECK POINT	Cyberint	$200	8.0x
Aug. 26	CISCO	ROBUST INTELLIGENCE	$350	NM
Aug. 07	EQT	Acronis	$4,000	NA

Private Funding Environment

Private funding environment rebounds, as investors look to deploy capital in an improving dealmaking environment.



Selected Q3 Financings

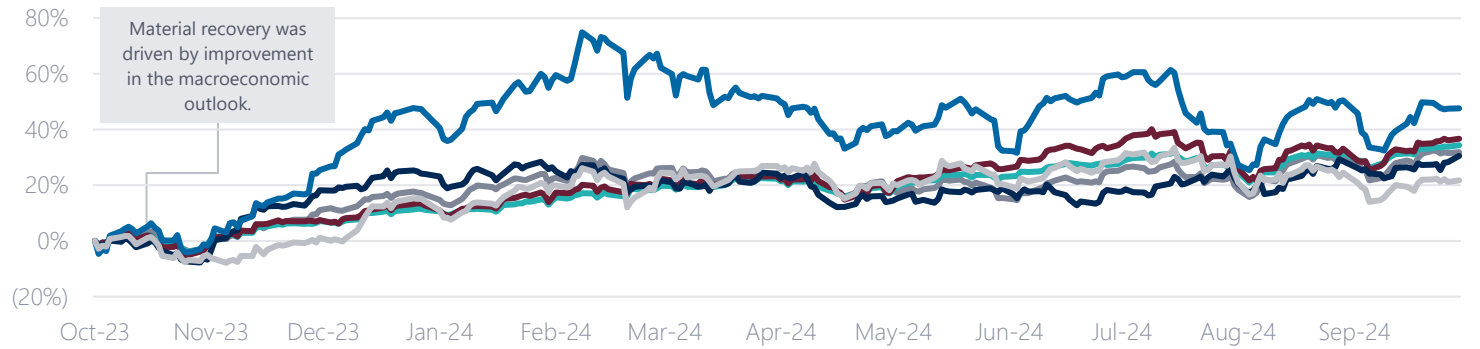
($ in Millions)

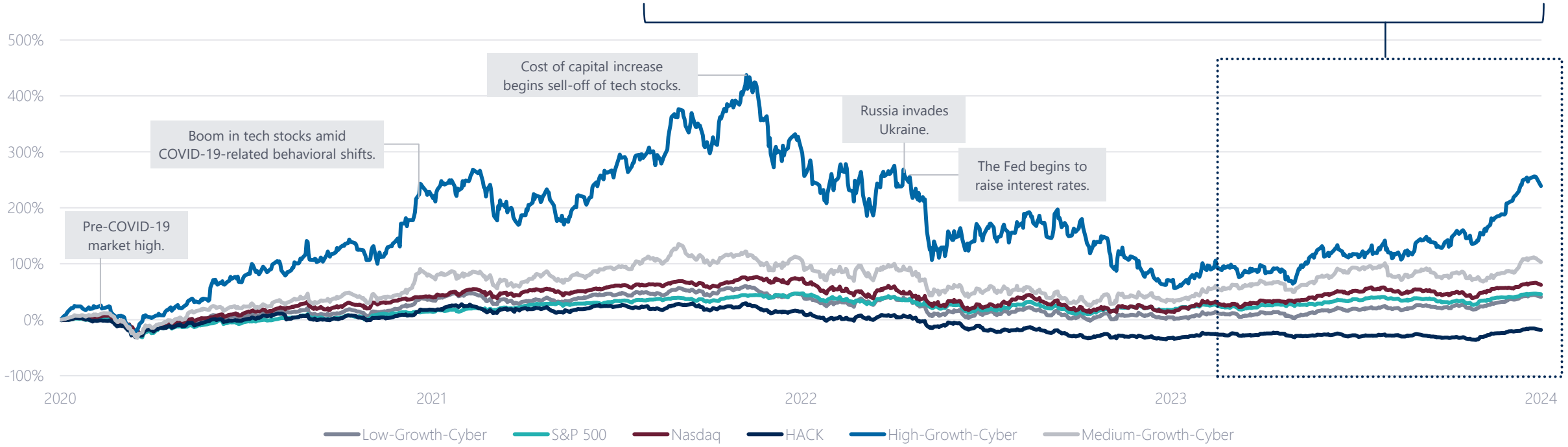
Ann. Date	Investor	Target	Amount	Val.
Sep. 13	salesforce ventures	SECOND FRONT SYSTEMS	$70	$785
Aug. 27	G/	Cribl	$319	$3,500
Aug. 14	SIXTH STREET INSIGHT PARTNERS	Kiteworks	$456	NA
Aug. 6	WELLINGTON MANAGEMENT	Abnormal	$250	$5,100
Jul. 25	ivp Lightspeed Redpoint	Chainguard	$140	$1,120

Source: S&P Capital IQ as of September 30, 2024.
Notes: NA indicates not available. NM indicates not meaningful.
(1) High-growth cybersecurity includes S, CRWD, ZS, and CYBR. (2) Medium-growth cybersecurity includes AVGO, PANW, FTNT, TENB, MITK, OKTA, and RSKD. (3) Low-growth cybersecurity includes RPD, QLYS, CGNT, 4704, WITH, CHKP, FFIV, OSPN, SWI, SCWX, FSECURE, GEN, TLS, and OTEX.

Segments of Cybersecurity and Broader Indexes

Index	Q3 '24	LTM
High-Growth Cyber[1]	↘ 4.2%	↗ 47.7%
Medium-Growth Cyber[2]	↘ 5.7%	↗ 21.8%
Low-Growth Cyber[3]	↗ 11.7%	↗ 30.6%
HACK[4]	↗ 5.3%	↗ 31.9%
S&P 500	↗ 5.3%	↗ 34.4%
Nasdaq	↗ 1.7%	↗ 36.7%

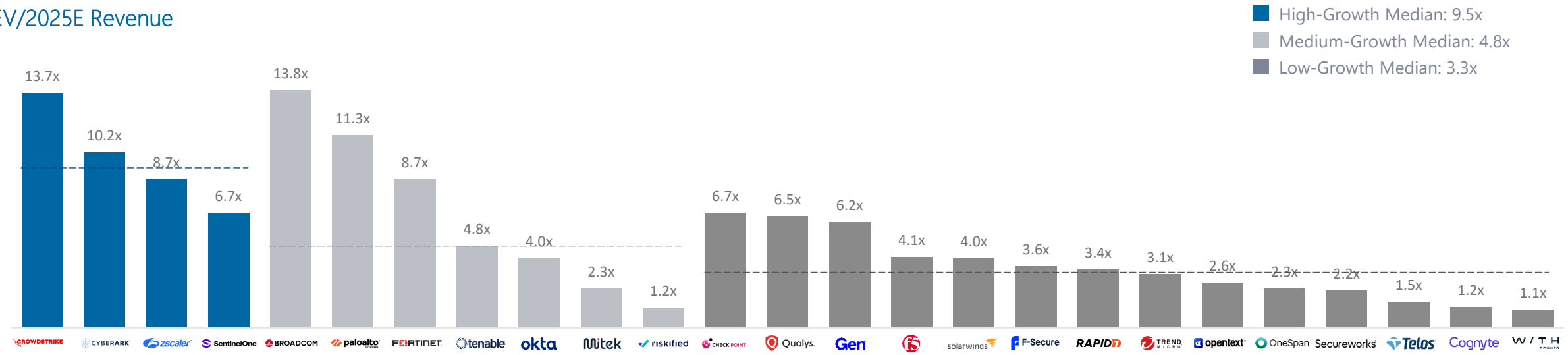




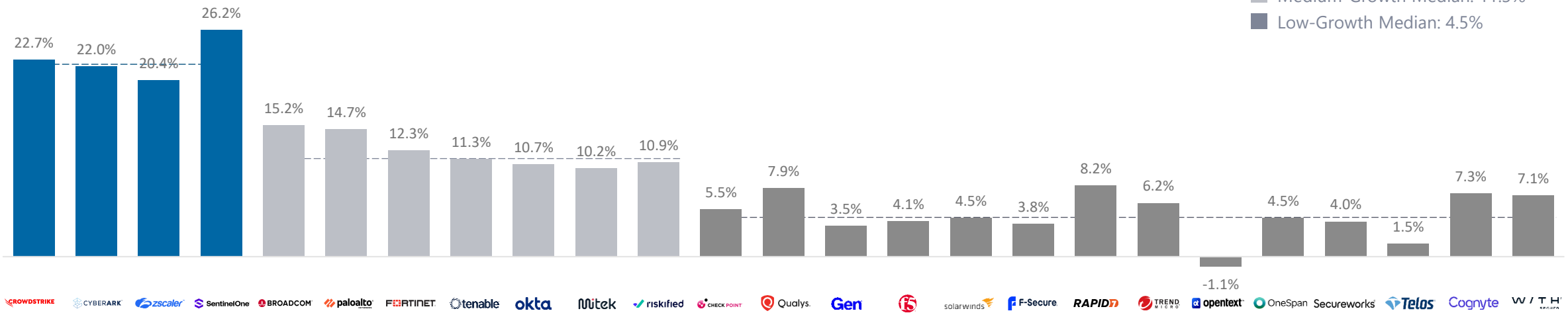
Source: S&P Capital IQ as of September 30, 2024.
(1) High-growth cybersecurity includes S, CRWD, ZS, and CYBR.
(2) Medium-growth cybersecurity includes AVGO, PANW, FTNT, TENB, MITK, OKTA, and RSKD.
(3) Low-growth cybersecurity includes RPD, QLYS, CGNT, 4704, WITH, CHKP, FFIV, OSPN, SWI, SCWX, FSECURE, GEN, TLS, and OTEX.
(4) Amplify Cybersecurity ETF (ARCA:HACK).

Public Company Benchmarking Cybersecurity Software

EV/2025E Revenue



CY 2024E–2025E Revenue Growth



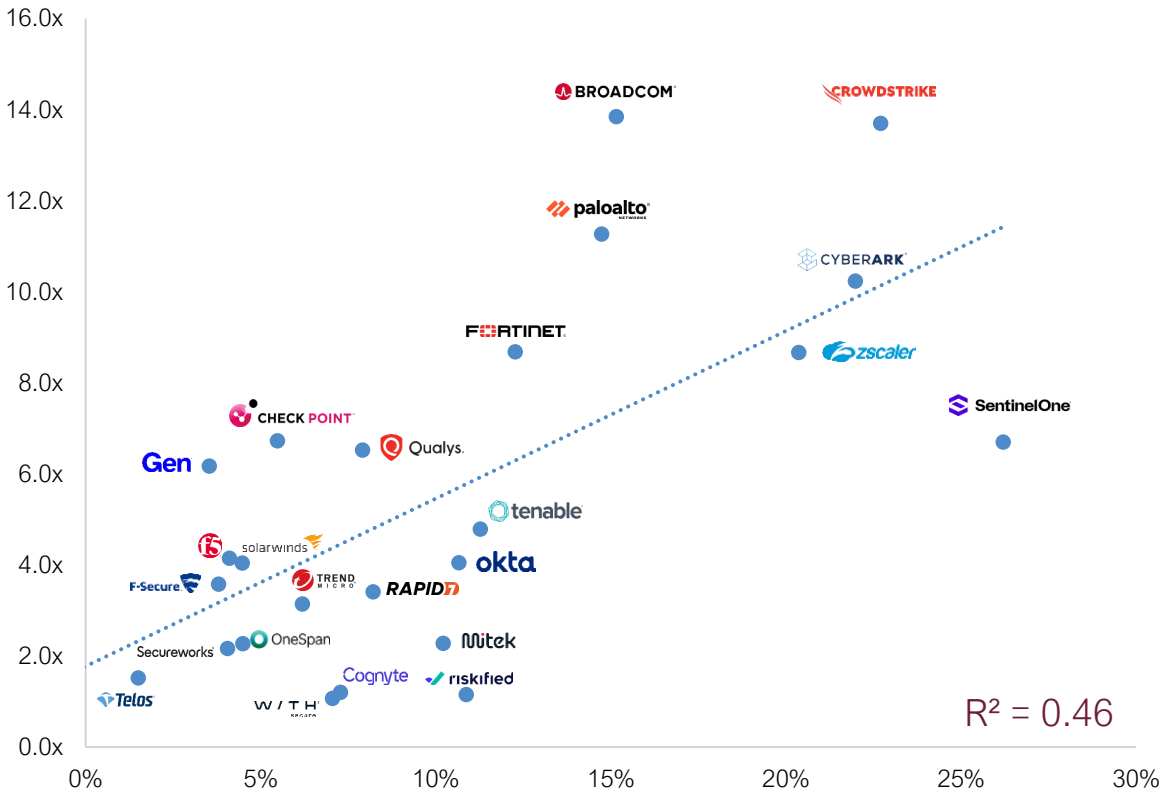
Source: Trading multiples are based on share price, other market data, and broker consensus future-earnings estimates from S&P Capital IQ as of September 30, 2024.
Notes: All financials are calendarized to December year-end and sorted by EV/2024E revenue. Broadcom's figures have been pro forma adjusted for its acquisition of VMware.

Public Investors Have Preference for a Balance of Profitability and Growth

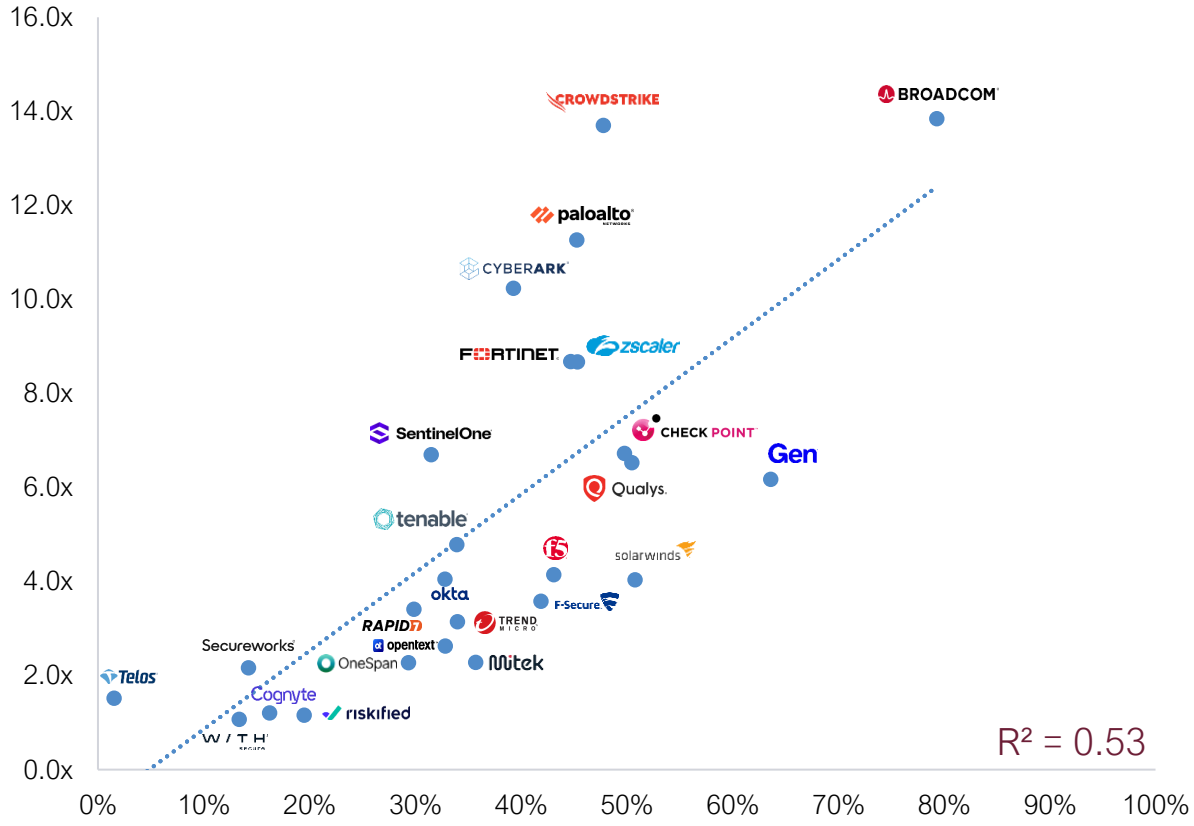
Low-Revenue Growth Rate	Medium-Revenue Growth Rate	High-Revenue Growth Rate
Mean: 5% | 3.5x Median: 4% | 3.3x	Mean: 12% | 6.6x Median: 11% | 4.8x	Mean: 23% | 9.8x Median: 22% | 9.5x

Below Rule of 40	Above Rule of 40
Mean: 9% | 3.3x Median: 8% | 2.5x	Mean: 10% | 7.9x Median: 8% | 6.7x

EV/'25E Revenue to '25E/'24E Revenue Growth



EV/'25E Revenue to Rule of 40

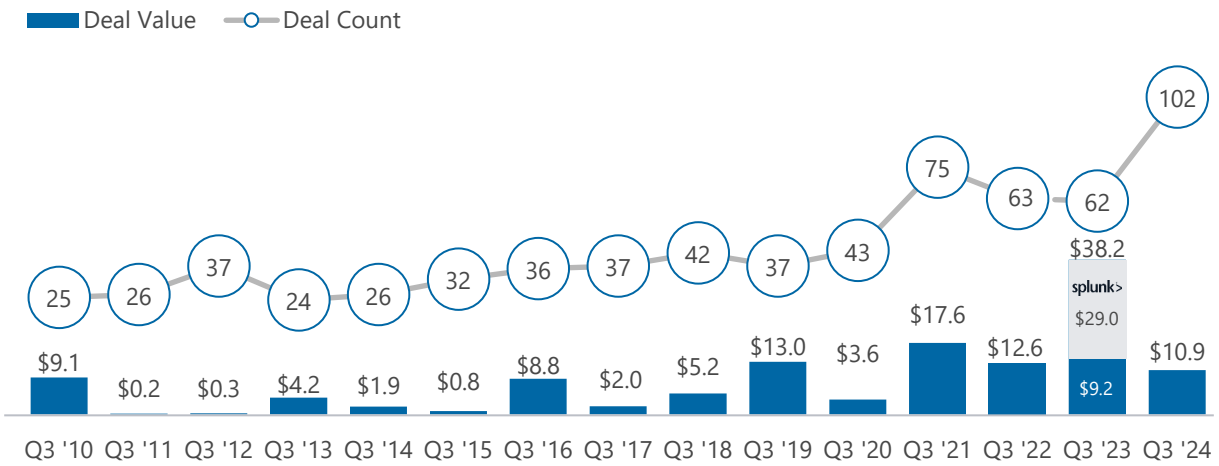


Source: Trading multiples are based on share price, other market data, and broker consensus future-earnings estimates from S&P Capital IQ as of September 30, 2024.
Notes: All financials are calendarized to a December year-end. Companies with negative values for revenue growth are included in the calculation for R2 but are not included in the charts.

Cybersecurity M&A Activity

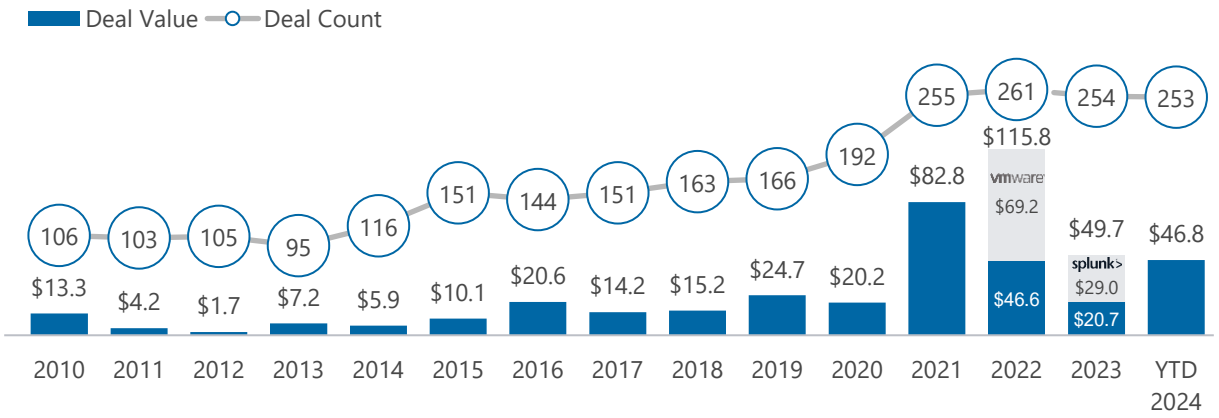
Historical Q3 M&A Summary

($ in Billions)



Annual M&A Summary

($ in Billions)



Featured M&A Transactions

($ in Millions)

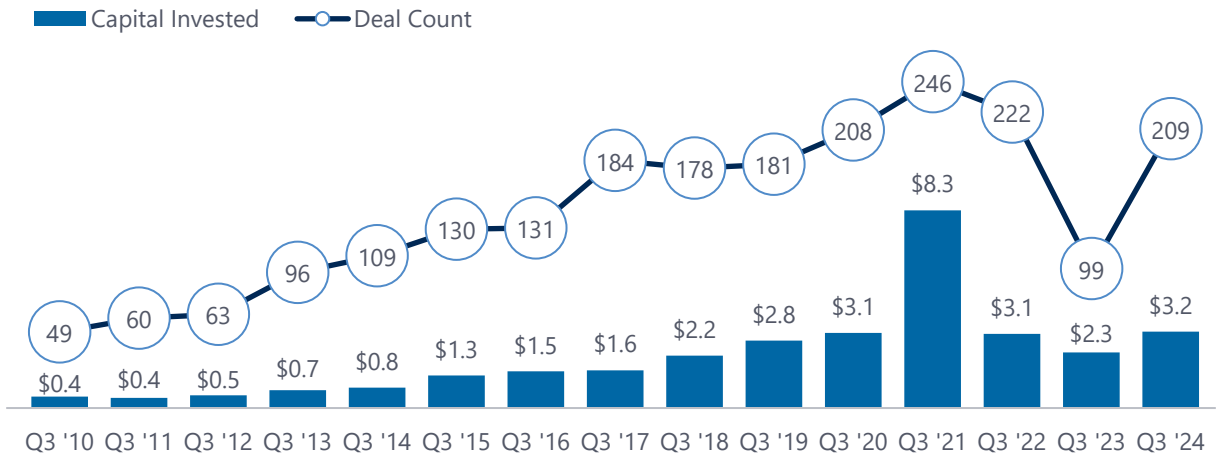
Ann. Date	Acquirer	Target	EV	EV/Rev
Sep. 24	Commvault	CLUMIO	$47	1.9x
Sep. 18	DESCARTES	MyCarrierPortal	$24	NA
Sep. 12	mastercard	Recorded Future	$2,650	7.8x
Sep. 5	salesforce	Own	$2,111	8.4x
Aug. 27	CHECK POINT	Cyberint	$200	8.0x
Aug. 26	CISCO	ROBUST INTELLIGENCE	$350	NM
Aug. 23	VINCI ENERGIES	fernao	NA	NA
Aug. 7	EQT	Acronis	$4,000	NA
Aug. 6	FORTINET	next	$96	NA
Jul. 23	Trailblazer	Cyabra	$70	NA
Jul. 9	VISTA	NASUNI	$1,200	NA
Jul. 1	RAPID7	noetic	$57	NA

Sources: S&P Capital IQ, PitchBook, Altitude Cyber, 451 Research as of September 30, 2024.
Notes: NA indicates not available. NM indicates not meaningful.

Cybersecurity Financing Activity

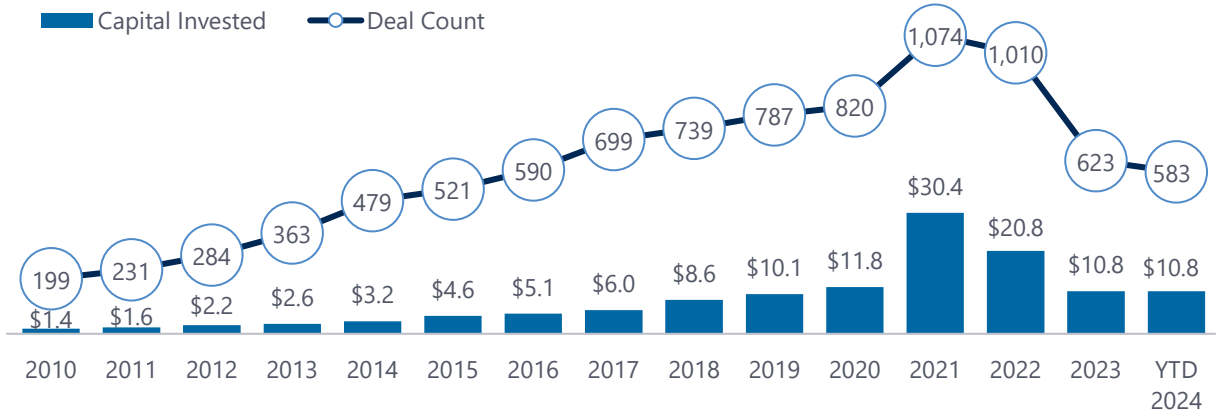
Historical Q3 Financing Summary

($ in Billions)



Annual Financing Summary

($ in Billions)

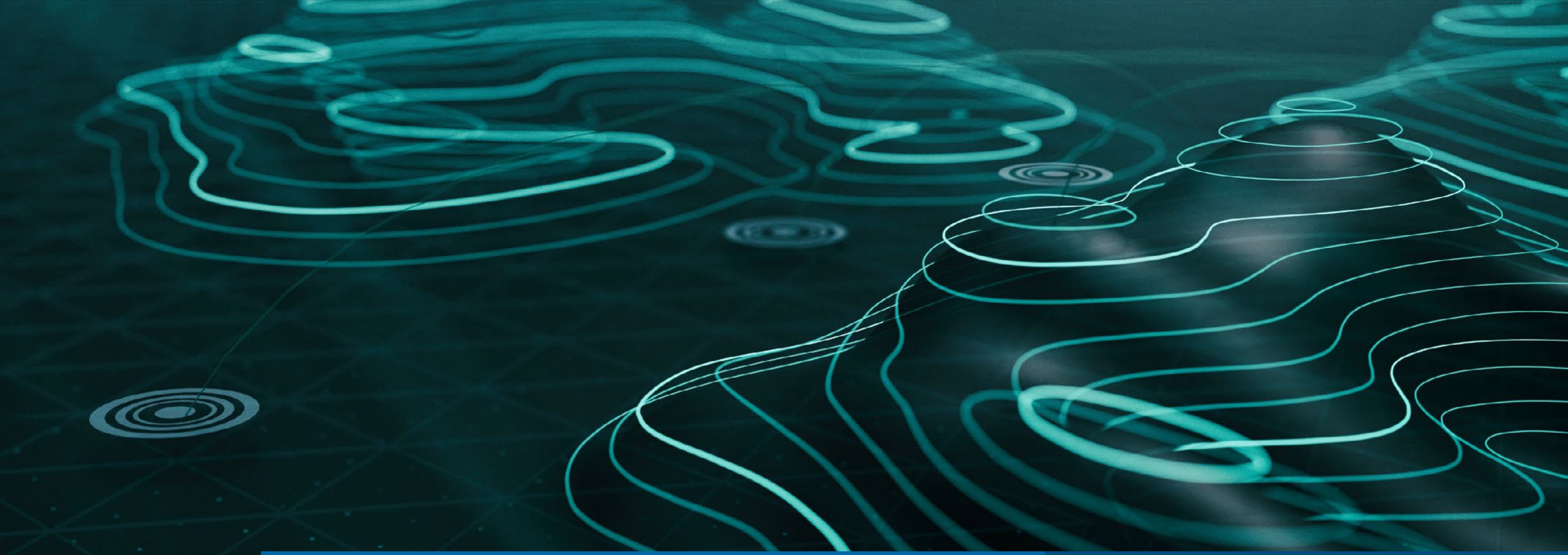


Featured Minority Transactions

($ in Millions)

Ann. Date	Investor	Target	Amount	Valuation
Sep. 20	TENELEVEN	eclypsium	$20	$164
Sep. 19	RIVERWOOD CAPITAL	PICUS	$45	$245
Sep. 17	NORWEST	INTEZER	$33	NA
Sep. 13	salesforce ventures	SECOND FRONT SYSTEMS	$70	$785
Aug. 27	GV	Cribl	$319	$3,500
Aug. 14	SIXTH STREET, INSIGHT PARTNERS	Kiteworks	$456	NA
Aug. 13	TAU Capital Group	SEPIO	$48	NA
Aug. 6	WELLINGTON MANAGEMENT	Abnormal	$250	$5,100
Aug. 1	evolution EQUITY PARTNERS	PROTECT AI	$81	$500
Jul. 25	ivp, Lightspeed, Redpoint	Chainguard	$140	$1,120
Jul. 24	SEQUOIA	Vanta	$150	$2,450
Jul. 18	PELION	STRIDER	$40	$462

Sources: PitchBook, 451 Research as of September 30, 2024.
Notes: Valuation reflects estimated post-money valuation. NA indicates not available.



Conferences and Events

03

Recent Conferences and Events
Houlihan Lokey Global Tech Conference
New York: October 23, 2024

Selected Sponsor Attendees

abry partners, AKKR, Apax Digital Growth, BainCapital, BregalSagemount, Brighton Park Capital, Charlesbank, Dragoneer, FTV Capital, General Atlantic, Great Hill Partners, GrowthCurve, HGGC, ICONIQ, JMI Equity, KKR, Long Ridge, Providence Equity Partners, Sixth Street Growth, Springcoast Partners, Sumeru, TA, TCV, ThomaBravo, TPG, Vector Capital, Vista, Vitruvian, Warburg Pincus

Participating Cybersecurity Companies

Authentic8, Cyfirma, everc, Human, NoFraud, SAFE, SecurityHQ, Shufti, virtru

What Happened

- **Panel Discussions From CEOs at High-Growth Companies:** A wide range of speakers shared their insights about navigating current market conditions and positioning their companies for future success across a variety of technology sectors.
- **Featured Speakers:** The conference featured high-profile speakers and candid panel discussions with distinguished tech thought leaders, discussing a variety of topical themes.
- **Targeted One-on-One Meetings:** Houlihan Lokey arranged targeted one-on-one meetings for presenting companies over the course of the conference, advising on prospects, meeting structure, and materials and coordinating any follow-up.
- **Networking Opportunities:** An audience of strategic, financial, and institutional investors, as well as other capital providers, gathered for lunch and end-of-day cocktails.

Conference Highlights

70+
Participating Companies

8 to 10
Targeted One-on-One Meetings Per Presenting Company

600+
Conference Attendees

Recent Conferences and Events
Black Hat USA 2024
Las Vegas: August 3–8, 2024

- Black Hat is an internationally recognized cybersecurity event series providing the most technical and relevant security research.
- These multi-day 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.

Sustaining Partners

ARMIS, AXONIUS, Carbon Black., CROWDSTRIKE, KnowBe4, ManageEngine, Qualys., SentinelOne, snyk, SOPHOS, sysdig, TREND MICRO

Source: Black Hat USA 2024 website.

Core Black Hat 2024 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 Business Hall	Solution providers and startups showcase the latest technologies and security services.

Black Hat CISO Summit

CISO Chief Information Security Officer

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

- AI and ML
- AppSec
- Cloud Security
- Cryptography
- Human Factors
- Malware
- Mobile Security
- Network Security
- Policy
- Privacy

black hat USA 2024

Four Days
Training

Two Days
Main Conference

100+
Selected Briefings

Dozens
Open-Source Tool Demos in Black Hat Arsenal, Dark Reading, and More

Upcoming Conferences and Events
AWS re:Invent
Las Vegas: December 2–6, 2024

- AWS re:Invent is a learning conference hosted by AWS for the global cloud computing community. It offers technical training sessions, workshops, and opportunities to connect with peers and experts.
- The conference features keynote announcements, training and certification opportunities, access to 2,000+ technical sessions, and numerous after-hours events.

Innovation Talks: Deep-dive into cloud computing topics with AWS subject matter experts across analytics, databases, developer experience, and much more.

Keynotes: Hear from AWS leaders about what's top of mind for them, from innovations in infrastructure and AI/ML to the latest trends and breakthroughs in cloud computing.

Peer Talk Platform: Find, connect, and network with other attendees who share similar interests.

Source: AWS re:Invent website.

Selected Event Sponsors

accenture, COHESITY, CONFLUENT, databricks, DATADOG, Deloitte., elastic, FORTINET, HashiCorp, intel, IBM, MongoDB., NVIDIA, paloalto NETWORKS, rubrik, SentinelOne, solarwinds, splunk>, tenable, TREND MICRO, WIZ

Conference Offerings

Bootcamps

Chalk Talks

Code Talks

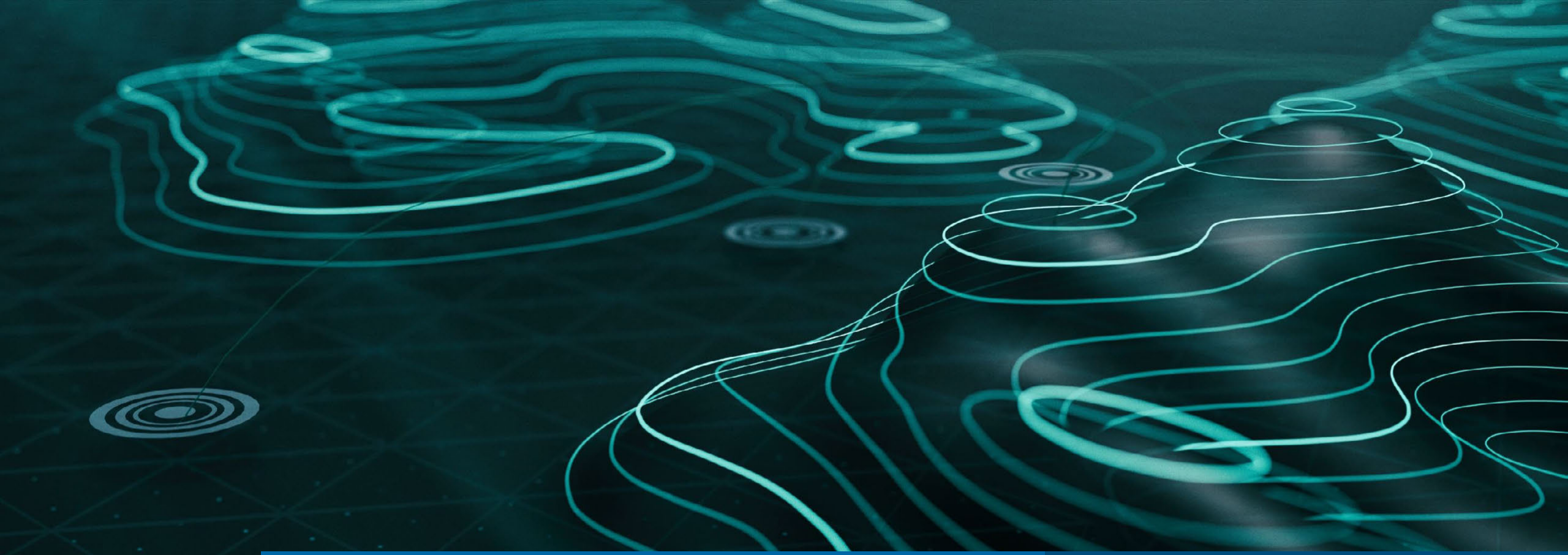
Dev Chats

Workshops

2023 Conference Highlights

50,000+
Attendees

2,250
Sessions and Hands-On Labs



About Houlihan Lokey

04

Leading Independent, Global Advisory Firm

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

2,691 Global Employees

36 Locations Worldwide

$13B Market Cap[1]

$2.1B Revenue[2]

~25% Employee-owned

No Debt

HLI LISTED NYSE

CORPORATE FINANCE

2023 M&A Advisory Rankings
All Global Transactions

	Advisor	Deals
1	**Houlihan Lokey**	**352**
2	Rothschild	349
3	Goldman Sachs	300
3	JP Morgan	300
5	Morgan Stanley	253

Source: LSEG (formerly Refinitiv).
Excludes accounting firms and brokers.

No. 1
Global M&A Advisor

Leading
Capital Markets Advisor

FINANCIAL RESTRUCTURING

2023 Global Distressed Debt &
Bankruptcy Restructuring Rankings

	Advisor	Deals
1	**Houlihan Lokey**	**73**
2	PJT Partners	64
3	Rothschild	51
4	Lazard	37
5	Evercore Partners	27

Source: LSEG (formerly Refinitiv).

No. 1
Global Restructuring Advisor

1,700+
Transactions Completed Valued at More Than $3.5 Trillion Collectively

FINANCIAL AND VALUATION ADVISORY

1999–2023 Global M&A
Fairness Advisory Rankings

	Advisor	Deals
1	**Houlihan Lokey**	**1,247**
2	JP Morgan	1,035
3	Duff & Phelps, A Kroll Business	977
4	UBS	884
5	Morgan Stanley	716

Source: LSEG (formerly Refinitiv).
Announced or completed transactions.

No. 1
Global M&A Fairness Opinion Advisor Over the Past 25 Years

2,000+
Annual Valuation Engagements

FINANCIAL SPONSORS COVERAGE

2023 Most Active Investment Banks to
Private Equity– Globally

	Advisor	Deals
1	**Houlihan Lokey**	**217**
2	Lincoln International	156
3	William Blair	112
4	Lazard	96
5	Raymond James Financial	85

Source: PitchBook. Excludes accounting firms and brokers.

No. 1
Global Private Equity M&A Advisor

1,300+
Sponsors Covered Globally

Source: (1) As of November 29, 2024. (2) LTM ended September 30, 2024.

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

No. 1
Tech M&A Advisor

14
Locations Worldwide

145+
Technology Financial Professionals

28
Managing Directors

116
Technology Deals in CY23

AMERICAS
Atlanta
Baltimore
Boston
Charlotte
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
Shanghai
Singapore
Sydney
Tokyo

No. 1 Global Tech Team

2023 M&A Advisory Rankings
All Global Technology Transactions

	Advisor	Deals
1	**Houlihan Lokey**	**89**
2	Rothschild	76
3	JP Morgan	68
4	Goldman Sachs	63
5	Morgan Stanley	59

Source: LSEG (formerly Refinitiv).
Excludes accounting firms and brokers.

2023 M&A Advisory Rankings
U.S. Technology Transactions Under $1 Billion

	Advisor	Deals
1	**Houlihan Lokey**	**36**
2	Canaccord Genuity Grp	31
3	Lincoln International	25
4	Raymond James Fin	24
5	Generational Equity	20

Source: LSEG (formerly Refinitiv).

Deep Cybersecurity Experience Across the Ecosystem

Procilon Group a portfolio company of Harald Quandt Industriebeteiligungen has been acquired by Main Capital Partners Sellside Advisor	Transaction Pending HID Citizen Identity Solutions Business has agreed to be acquired by Toppan Sellside Advisor	NEVERHACK a portfolio company of CARLYLE has acquired INNOVERY a portfolio company of WISE EQUITY Buyside Advisor	ALCHEMY TECH GROUP has received a strategic investment from AVANCE Sellside Advisor	CYBOLT has integrated Cyber Guards Security Made Simple Buyside Advisor	nuspire a portfolio company of abry partners has been acquired by PDI Technologies a portfolio company of INSIGHT PARTNERS · TA ASSOCIATES · GENSTAR Sellside Advisor	CLANGO has merged with MajorKey a portfolio company of acacia Exclusive Placement Agent
CYBOLT has integrated PRI pontis research Buyside Advisor	CARLYLE has acquired a majority stake in NEVERHACK formerly known as PROPHECY a portfolio company of IK Partners Buyside Advisor	PRIVITAR has been acquired by Informatica Sellside Advisor	Armorblox has been acquired by Cisco Sellside Advisor	XALIENT accelerate your business has received investment from VOLPi CAPITAL Sellside Advisor	THRIVE a portfolio company of COURT SQUARE HoldCo PIK Notes Acquisition Financing Exclusive Placement Agent	ROHDE&SCHWARZ Cybersecurity SAS has been acquired by total specific solutions Sellside Advisor
proov has received a growth equity investment of $70,000,000 from SEP · Sumeru Equity Partners Financial Advisor	SVERICA has made a strategic investment in SHADOWDRAGON Buyside Advisor	Acumera has received a strategic growth investment from PEAK ROCK CAPITAL® Sellside Advisor*	AnaCap Financial Partners has acquired a majority stake in WebID Your True Identity Company Buyside Advisor*	tresorit has been acquired by SWISS POST Sellside Advisor*	CVC has invested in Acronis Financing Advisor*	IDIQ has sold a majority stake to Corsair Capital Sellside Advisor*
netwrix has received an equity investment from updata PARTNERS Financial Advisor	Threema. has entered into a partnership with Afinum Sellside Advisor*	LIVINGBRIDGE has invested in TitanHQ Buyside Advisor*	DSwiss has sold a minority stake to Verium Sellside Advisor*	Acronis structured equity investment led by Goldman Sachs Financing Advisor*	NC4 has been acquired by everbridge® Sellside Advisor	MARLIN EQUITY PARTNERS has sold a majority stake in QUALITEST to Bridgepoint Sellside Advisor*

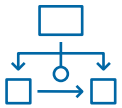
Tombstones included herein represent transactions closed from 2017 forward.
**Selected transactions were executed by Houlihan Lokey professionals while at other firms acquired by Houlihan Lokey or by professionals from a Houlihan Lokey joint venture company.*

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

Corporate Finance 	› Mergers and Acquisitions › Capital Markets › Private Funds Advisory › Board and Special Committee Advisory	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.
Financial Restructuring 	› Creditor 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 1,700 restructuring transactions (with aggregate debt claims in excess of $3.5 trillion). We served as an advisor in 12 of the 15 largest bankruptcies from 2000 to 2023.
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 more than 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 All Global M&A and All Global Tech M&A in 2023*

Significant Experience With Financing Markets

Senior-Level Commitment and Dedication

Deep, Industry-Specific Expertise

Superior Work Product/ Technical Abilities

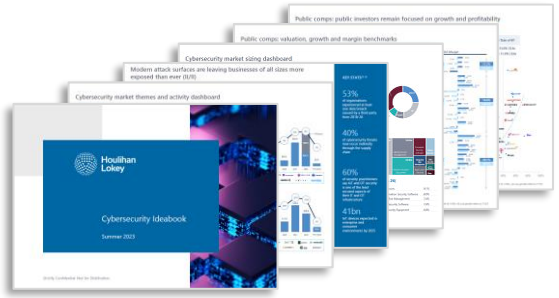
Creativity, Imagination, Tenacity, and Positivity

*Sources: *LSEG (formerly Refinitiv). Excludes accounting firms and brokers. BankruptcyData.com and Debtwire, January 2024.*

Other Houlihan Lokey Cyber Sector Reports

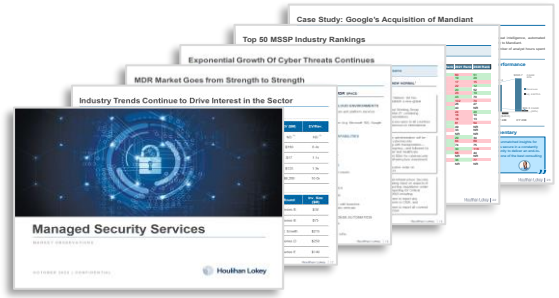
Generative AI in Cybersecurity Report

European Cybersecurity Ideabook



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
San Francisco
Keith.Skirbe@HL.com

Bobby Wolfe
Director
Miami
BWolfe@HL.com

Joseph Miller
Vice President
San Francisco
JJMiller@HL.com

Patrick Wong
Associate
San Francisco
Patrick.Wong@HL.com

Global Cyber Reach

Mark Smith
Director
Cyber Europe
Manchester
Mark.Smith@HL.com

Malte Abrams
Managing Director
Cyber Europe
Frankfurt
Malte.Abrams@HL.com

Ido Zakai
Managing Director
Head of Tech, Israel
Tel Aviv
Ido.Zakai@HL.com

Sara Napolitano
Managing Director
Cyber Europe
Paris
Sara.Napolitano@HL.com

Capital Markets

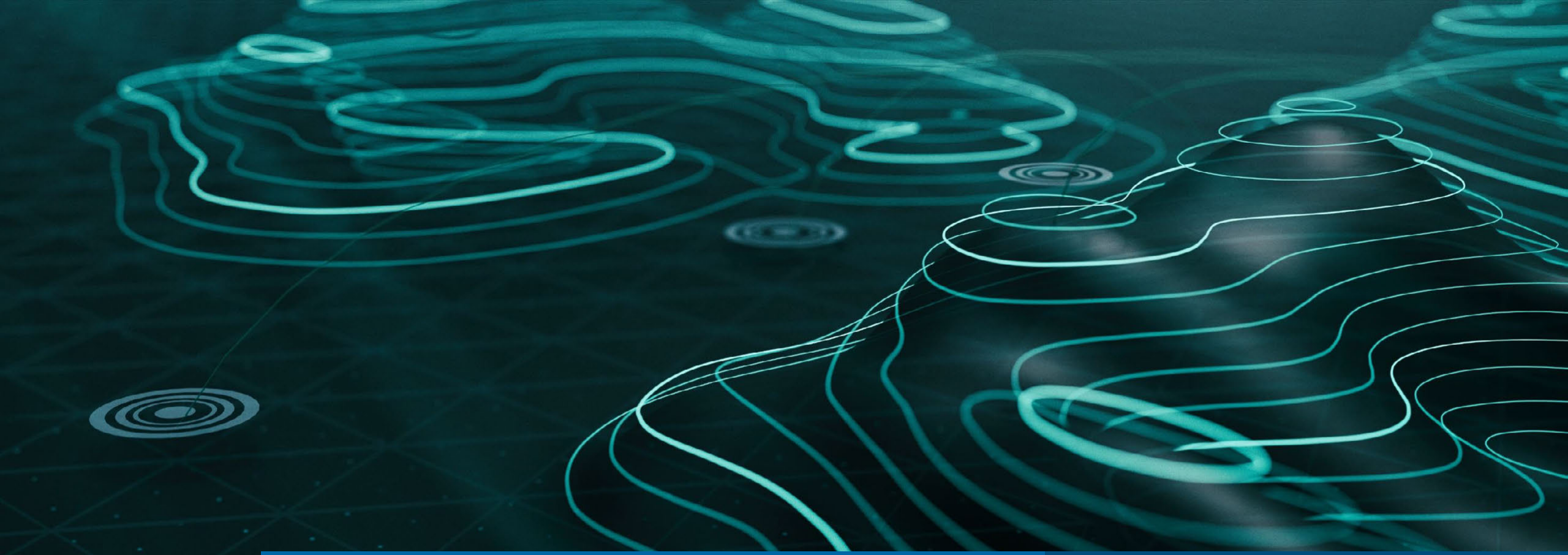
David Kelnar
Managing Director
London
David.Kelnar@HL.com

Greg Werntz
Director
San Francisco
Greg.Werntz@HL.com

Cybersecurity Technology Expertise

Joshua Holmes
Head of Cyber and
Tech Due Diligence
Dallas
JLHolmes@HL.com

Yearly Conferences



Appendix

05

High-Growth Cybersecurity Trading Metrics

($ in Millions, Except Price per Share)

Company	Stock Price	52-Wk High	% of 52-Wk High	YTD Stock Performance	Cash and ST Inv	Equity Mkt Cap	Enterprise Value	EV/Revenue			EV/EBITDA		
								CY 2023A	CY 2024E	CY 2025E	CY 2023A	CY 2024E	CY 2025E
CROWDSTRIKE	$280.47	$398.33	70.4%	13.6%	$4,039	$69,680	$65,542	21.5x	16.8x	13.7x	NM	NM	NM
zscaler	170.94	259.61	65.8%	(19.5%)	2,410	25,570	24,899	13.1x	10.4x	8.7x	NM	43.4x	34.7x
CYBERARK	291.61	293.31	99.4%	34.9%	1,400	12,338	11,725	15.6x	12.5x	10.2x	NM	NM	NM
SentinelOne	23.92	30.76	77.8%	(7.5%)	708	7,289	6,900	11.1x	8.5x	6.7x	NM	NM	NM
Top Quartile					$36,598		$35,060	17.1x	13.6x	11.1x	NM	43.4x	34.7x
Mean					29,021		27,266	15.3x	12.0x	9.8x	NM	43.4x	34.7x
Median					19,558		18,312	14.4x	11.5x	9.5x	NM	43.4x	34.7x
First Quartile					11,981		10,519	12.6x	9.9x	8.2x	NM	43.4x	34.7x

Source: Trading multiples are based on share price, other market data, and broker consensus future-earnings estimates from S&P Capital IQ as of September 30, 2024.
Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >50x or <0x. Sorted by enterprise value. Growth categorizations are based on 2024E–2025E revenue growth breakpoints; high-growth ≥ 20%, medium-growth >10% and <20%, low-growth ≤ 10%.

Medium-Growth Cybersecurity Trading Metrics

($ in Millions, Except Price per Share)

Company	Stock Price	52-Wk High	% of 52-Wk High	YTD Stock Performance	Cash and ST Inv	Equity Mkt Cap	Enterprise Value	EV/Revenue			EV/EBITDA		
								CY 2023A	CY 2024E	CY 2025E	CY 2023A	CY 2024E	CY 2025E
BROADCOM	$172.50	$185.16	93.2%	58.9%	$9,952	$799,710	$865,681	22.3x	15.9x	13.8x	42.4x	25.6x	21.6x
paloalto NETWORKS	341.80	380.84	89.7%	18.3%	2,579	120,997	110,122	14.6x	12.9x	11.3x	NM	42.7x	36.9x
FORTINET	77.55	78.18	99.2%	34.2%	3,701	59,805	57,056	10.8x	9.7x	8.7x	42.3x	29.5x	26.8x
okta	74.34	114.50	64.9%	(14.6%)	2,358	12,387	11,490	5.1x	4.5x	4.0x	NM	20.8x	18.3x
tenable	40.52	53.50	75.7%	(7.8%)	548	4,783	4,751	5.9x	5.3x	4.8x	NM	25.9x	21.1x
Mitek	8.67	16.24	53.4%	(32.7%)	123	402	425	2.6x	2.5x	2.3x	19.6x	9.9x	NA
riskified	4.73	6.65	71.2%	6.5%	390	827	413	1.4x	1.3x	1.2x	NM	27.3x	13.4x
Top Quartile					$90,401	$83,589		12.7x	11.3x	10.0x	42.3x	28.4x	25.5x
Mean					142,702	149,991		9.0x	7.5x	6.6x	34.8x	26.0x	23.0x
Median					12,387	11,490		5.9x	5.3x	4.8x	42.3x	25.9x	21.4x
First Quartile					2,805	2,588		3.8x	3.5x	3.2x	30.9x	23.2x	19.0x

Source: Trading multiples are based on share price, other market data, and broker consensus future-earnings estimates from S&P Capital IQ as of September 30, 2024.
Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >50x or <0x. Sorted by enterprise value. Growth categorizations are based on 2024E–2025E revenue growth breakpoints; high-growth ≥ 20%, medium-growth >10% and <20%, low-growth ≤ 10%.

Low-Growth Cybersecurity Trading Metrics

($ in Millions, Except Price per Share)

Company	Stock Price	52-Wk High	% of 52-Wk High	YTD Stock Performance	Cash and ST Inv	Equity Mkt Cap	Enterprise Value	EV/Revenue			EV/EBITDA		
								CY 2023A	CY 2024E	CY 2025E	CY 2023A	CY 2024E	CY 2025E
Gen	$27.43	$27.53	99.6%	20.4%	$737	$17,336	$24,816	6.5x	6.4x	6.2x	14.9x	10.7x	10.3x
CHECK POINT	192.81	196.56	98.1%	26.6%	1,469	22,081	18,184	7.5x	7.1x	6.7x	19.5x	16.0x	15.2x
opentext	33.28	45.47	73.2%	(18.1%)	1,002	9,039	14,192	2.5x	2.6x	2.6x	9.9x	7.9x	7.7x
F5	220.20	223.74	98.4%	24.9%	1,075	13,071	12,159	4.3x	4.3x	4.1x	16.8x	11.5x	10.6x
TREND	59.23	64.41	92.0%	11.3%	1,374	7,771	6,314	3.6x	3.3x	3.1x	14.6x	12.8x	11.3x
Qualys.	128.46	206.35	62.3%	(33.1%)	386	4,823	4,224	7.6x	7.0x	6.5x	22.2x	16.1x	15.3x
solarwinds	13.05	13.43	97.2%	7.7%	199	2,236	3,306	4.4x	4.2x	4.0x	14.6x	8.9x	8.7x
RAPID7	39.89	61.88	64.5%	(27.4%)	444	2,834	3,081	4.0x	3.7x	3.4x	NM	17.1x	15.7x
Secureworks	8.85	9.76	90.7%	23.9%	48	771	744	2.0x	2.3x	2.2x	NM	32.4x	21.3x
F-Secure	2.41	2.60	92.7%	10.3%	15	409	611	4.2x	3.7x	3.6x	16.0x	10.2x	9.4x
OneSpan	16.67	16.68	99.9%	57.7%	77	649	577	2.5x	2.4x	2.3x	NM	9.8x	9.1x
Cognyte	6.79	8.70	78.0%	8.8%	92	502	445	1.4x	1.3x	1.2x	NM	17.5x	13.5x
WITH secure	1.17	1.39	84.3%	2.2%	24	205	193	1.2x	1.1x	1.1x	NM	47.3x	17.1x
Telos	3.59	5.03	71.4%	(11.8%)	70	256	190	1.3x	1.8x	1.5x	NM	NM	NM
Top Quartile					$8,722	$10,698		4.4x	4.3x	4.1x	17.4x	17.1x	15.3x
Mean					5,856	6,360		3.8x	3.7x	3.5x	16.1x	16.8x	12.7x
Median					2,535	3,193		3.8x	3.5x	3.3x	15.5x	12.8x	11.3x
First Quartile					539	585		2.1x	2.3x	2.2x	14.6x	10.2x	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 September 30, 2024.
Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >50x or <0x. Sorted by enterprise value. Growth categorizations are based on 2024E–2025E revenue growth breakpoints; high-growth ≥ 20%, medium-growth >10% and <20%, low-growth ≤ 10%.

High-Growth Cybersecurity Operating Metrics

($ in Millions, Except Price per Share)

Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2023A	CY 2024E	CY 2025E	CY 2023A	CY 2024E	CY 2025E	2022A–2023A	2023–2024E	2024–2025E	CY 2023A	CY 2024E	CY 2025E
CROWDSTRIKE	$280.47	$69,680	$65,542	$3,056	$3,899	$4,785	$106	$958	$1,199	36.3%	27.6%	22.7%	3.5%	24.6%	25.1%
zscaler	170.94	25,570	24,899	1,896	2,386	2,872	(153)	574	717	40.6%	25.9%	20.4%	NM	24.1%	25.0%
CYBERARK	291.61	12,338	11,725	752	939	1,146	(100)	128	198	27.1%	24.9%	22.0%	NM	13.6%	17.3%
SentinelOne	23.92	7,289	6,900	621	816	1,030	(340)	(14)	54	47.1%	31.3%	26.2%	NM	NM	5.3%
Top Quartile	$36,598	$35,060	$2,186	$2,765	$3,351	($48)	$670	$838	42.2%	28.6%	23.6%	3.5%	24.3%	25.0%	
Mean	29,021	27,266	1,581	2,010	2,458	(122)	412	542	37.8%	27.4%	22.8%	3.5%	20.8%	18.2%	
Median	19,558	18,312	1,324	1,663	2,009	(127)	351	458	38.5%	26.8%	22.3%	3.5%	24.1%	21.1%	
First Quartile	11,981	10,519	719	908	1,117	(200)	93	162	34.0%	25.6%	21.6%	3.5%	18.9%	14.3%	

Source: Trading multiples are based on share price, other market data, and broker consensus future-earnings estimates from S&P Capital IQ as of September 30, 2024.
Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >50x or <0x. Sorted by enterprise value. Growth categorizations are based on 2024E–2025E revenue growth breakpoints; high-growth ≥ 20%, medium-growth >10% and <20%, low-growth ≤ 10%.

Medium-Growth Cybersecurity Operating Metrics

($ in Millions, Except Price per Share)

Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2023A	CY 2024E	CY 2025E	CY 2023A	CY 2024E	CY 2025E	2022A–2023A	2023–2024E	2024–2025E	CY 2023A	CY 2024E	CY 2025E
BROADCOM	$172.50	$799,710	$865,681	$38,865	$54,297	$62,525	$20,404	$33,812	$40,113	12.9%	39.7%	15.2%	52.5%	62.3%	64.2%
paloalto NETWORKS	341.80	120,997	110,122	7,527	8,523	9,779	973	2,580	2,984	22.3%	13.2%	14.7%	12.9%	30.3%	30.5%
FORTINET	77.55	59,805	57,056	5,305	5,855	6,574	1,350	1,937	2,131	20.1%	10.4%	12.3%	25.4%	33.1%	32.4%
okta	74.34	12,387	11,490	2,263	2,564	2,837	(376)	553	628	21.8%	13.3%	10.7%	NM	21.6%	22.1%
tenable	40.52	4,783	4,751	799	893	993	(11)	183	225	16.9%	11.8%	11.3%	NM	20.5%	22.7%
Mitek	8.67	402	425	164	169	186	22	43	0	3.6%	3.1%	10.2%	13.2%	25.5%	NM
riskified	4.73	839	413	298	322	357	(73)	15	31	13.9%	8.1%	10.9%	NM	4.7%	8.6%
Top Quartile		$90,401	$83,589	$6,416	$7,189	$8,176	$1,161	$2,258	$2,558	20.9%	13.3%	13.5%	32.2%	31.7%	31.9%
Mean		142,702	149,991	7,889	10,374	11,893	3,184	5,589	6,587	15.9%	14.2%	12.2%	26.0%	28.3%	30.1%
Median		12,387	11,490	2,263	2,564	2,837	22	553	628	16.9%	11.8%	11.3%	19.3%	25.5%	26.6%
First Quartile		2,805	2,588	548	607	675	(42)	113	128	13.4%	9.3%	10.8%	13.1%	21.0%	22.3%

Source: Trading multiples are based on share price, other market data, and broker consensus future-earnings estimates from S&P Capital IQ as of September 30, 2024.
Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >50x or <0x. Sorted by enterprise value. Growth categorizations are based on 2024E–2025E revenue growth breakpoints; high-growth ≥ 20%, medium-growth >10% and <20%, low-growth ≤ 10%.

Low-Growth Cybersecurity Operating Metrics

($ in Millions, Except Price per Share)

Company	Stock Price	Equity Mkt Cap	Enterprise Value	Revenue			EBITDA			Revenue Growth			EBITDA Margin		
				CY 2023A	CY 2024E	CY 2025E	CY 2023A	CY 2024E	CY 2025E	2022A–2023A	2023–2024E	2024–2025E	CY 2023A	CY 2024E	CY 2025E
Gen	$27.43	$17,336	$24,816	$3,789	$3,883	$4,021	$1,668	$2,312	$2,416	22.0%	2.5%	3.5%	44.0%	59.5%	60.1%
CHECK POINT	192.81	22,081	18,184	2,415	2,564	2,704	933	1,135	1,198	3.6%	6.2%	5.5%	38.6%	44.3%	44.3%
opentext	33.28	9,039	14,192	5,696	5,467	5,405	1,435	1,795	1,834	61.2%	(4.0%)	(1.1%)	25.2%	32.8%	33.9%
f5	220.20	13,071	12,159	2,805	2,818	2,934	725	1,053	1,143	3.6%	0.4%	4.1%	25.9%	37.4%	39.0%
TREND	59.23	7,771	6,314	1,764	1,890	2,007	432	492	558	4.0%	7.1%	6.2%	24.5%	26.0%	27.8%
Qualys.	128.46	4,823	4,224	554	600	647	190	262	275	13.2%	8.2%	7.9%	34.3%	43.7%	42.5%
solarwinds	13.05	2,236	3,306	759	783	818	227	371	379	5.5%	3.2%	4.5%	29.9%	47.3%	46.3%
RAPID7	39.89	2,834	3,081	778	835	904	19	180	196	13.5%	7.4%	8.2%	2.4%	21.5%	21.6%
Secureworks	8.85	771	744	366	330	344	(63)	23	35	(21.1%)	(9.7%)	4.0%	NM	7.0%	10.2%
F-Secure	2.41	409	611	144	164	171	38	60	65	21.5%	14.0%	3.8%	26.4%	36.6%	38.1%
OneSpan	16.67	649	577	235	243	254	(5)	59	63	7.4%	3.3%	4.5%	NM	24.2%	24.9%
Cognyte	6.79	502	445	313	345	370	(8)	25	33	0.4%	10.1%	7.3%	NM	7.4%	8.9%
WITH secure	1.17	205	193	158	168	180	(29)	4	11	9.7%	6.4%	7.1%	NM	2.4%	6.3%
Telos	3.59	256	190	145	106	126	(35)	(19)	(0)	(33.0%)	(27.2%)	1.5%	NM	NM	NM
Top Quartile	$8,722	$10,698	$2,252	$2,395	$2,530	$652	$913	$997	13.4%	7.3%	6.8%	34.3%	43.7%	42.5%	
Mean	5,856	6,360	1,423	1,443	1,492	395	554	586	8.0%	2.0%	4.8%	27.9%	30.0%	31.1%	
Median	2,535	3,193	657	692	733	114	221	236	6.4%	4.7%	4.5%	26.4%	32.8%	33.9%	
First Quartile	539	585	255	265	276	(7)	34	42	3.6%	1.0%	3.9%	25.2%	21.5%	21.6%	

Source: Trading multiples are based on share price, other market data, and broker consensus future-earnings estimates from S&P Capital IQ as of September 30, 2024.
Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >50x or <0x. Sorted by enterprise value. Growth categorizations are based on 2024E–2025E revenue growth breakpoints; high-growth ≥ 20%, medium-growth >10% and <20%, low-growth ≤ 10%.

Disclaimer

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., Houlihan Lokey Advisory, Inc., and Waller Helms Securities, LLC, each an SEC-registered broker-dealer and members of FINRA (www.finra.org) and SIPC (www.sipc.org) (investment banking services); (ii) Europe: Houlihan Lokey UK Limited (FRN 792919), Houlihan Lokey Advisory Limited (FRN 116310), and Houlihan Lokey PFG Advisory Limited (FRN 725267), 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); Houlihan Lokey Private Funds Advisory S.A., a member of CNCEF Patrimoine and registered with the ORIAS (#14002730); (iii) the United Arab Emirates, Dubai International Financial Centre (Dubai): Houlihan Lokey (MEA Financial Advisory) Ltd., regulated by the Dubai Financial Services Authority; (iv) Singapore: Houlihan Lokey (Singapore) Private Limited 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 (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. No entity affiliated with Houlihan Lokey, Inc., provides banking or securities brokerage services, nor is any such affiliate subject to FINMA supervision in Switzerland or similar regulatory authorities regarding such activities in other jurisdictions. 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 financial 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