



Houlihan Lokey



Cybersecurity Quarterly Update

FOURTH 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



Joseph Miller
Associate
San Francisco



Patrick Wong
Financial Analyst
San Francisco

Capital Markets



Sean Fitzgerald
Managing Director
New York



Chris Hebble
Managing Director
Los Angeles



David Kelnar
Managing Director
London

Global Cyber Reach



Mark Smith
Director
Cyber Europe
United Kingdom



Malte Abrams
Managing Director
Cyber Europe
Frankfurt



Sara Napolitano
Managing Director
Cyber Europe
Paris



Ido Zakai
Managing Director
Head of Tech, Israel
Tel Aviv



Raymond Fröjd
Managing Director
Head of Nordic Tech
Stockholm



Sameer Jindal
Managing Director
Mumbai



Prashant Bali
Director
Sydney



Gabrielle Worrall
Vice President
United Kingdom



Christie Adams
Financial Analyst
Paris



Samuel Pattison
Financial Analyst
United Kingdom

Financial Sponsors

30

Senior Financial
Professionals
Covering

~1,300

Investors

Cybersecurity Technology Expertise



Joshua Holmes
Head of Cyber and Tech Due Diligence
Dallas



Edouard Viot
Cybersecurity Consultant
Paris

Executive Summary: Q4 2023 in Review

Executive Summary

- Q4 ended the year 2023 as **the best quarter for public cybersecurity companies**, with the Houlihan Lokey Cybersecurity Index⁽¹⁾ reaching a year-to-date increase of 83% and a quarterly increase of 29%.
- Despite a roaring public market rebound, Q4 M&A and financing deal volume and deal count experienced sustained declines compared to the same period in 2022 and 2021.
- The ascent of AI within cyber products, growing apprehension about a surge in cyber-attacks, and heightened government regulation may **catalyze strong M&A activity in 2024** following a lackluster performance in 2023.
- The diverse range of attack methods and pathways, combined with rising levels of sophistication, underscores the need for a swiftly adapting solution ecosystem to effectively implement proactive measures for prevention, detection, and response.

A Strong Quarter for Public Companies

HOULIHAN LOKEY CYBERSECURITY INDEX⁽¹⁾



Q4 2023 Report Themes



AI will continue to be top of mind, and usage will increase by both offenders and defenders.



Cybersecurity spend growth remains robust driven by embedded tailwinds.



Attacks are more prevalent than ever, but solutions are less complex than they seem; 2FA can prevent 99% of breaches.



Governments continue to expand regulation, and enforcement is expected to accelerate.



Growing European-focused ecosystem is creating investment opportunities across the cybersecurity industry.

M&A Volume Substantially Drops From 2022 Levels

	Q4 '23	VS. Q4 '22	VS. Q4 '21
Volume	\$1.8B	↓ (24%)	↓ (37%) ⁽²⁾
# of Deals	47	↓ (25%)	↓ (21%)

ISOVALENT
\$650M

Dig Security
\$400M

TESSIAN
\$300M

Financing Levels Continue to Decline

	Q4 '23	VS. Q4 '22	VS. Q4 '21
Volume	\$2.7B	↓ (44%)	↓ (71%)
# of Deals	189	↓ (3%)	↓ (33%)

Island
\$100M

BioCatch
\$70M

Prove
\$44M

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

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

(2) Deal volume excludes McAfee's public take-private.

Table of Contents

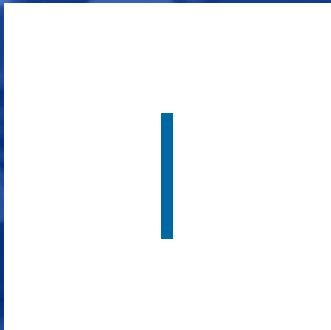
I Perspectives From the Front

II Capital Markets and Trends Update

III Conferences and Events

IV About Houlihan Lokey

V Appendix



Perspectives From the Front



Houlihan Lokey

Cybersecurity End Markets







2023 Year in Review

2024 Prediction Tracking

Cyber Research Summary

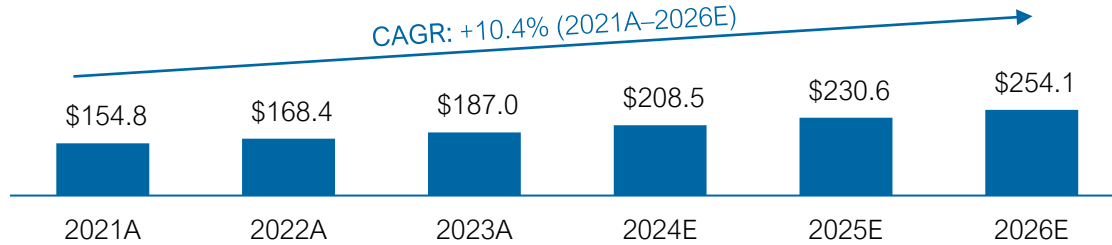
Data Breaches

Top-of-Mind Headlines in 2023

 <p>State Attacks</p>	<p>National Cyber Security Centre UK cyber experts warn of targeted phishing attacks from actors based in Russia and Iran Advisory highlights ongoing threat from spear-phishing by Russia-based group SEABORGIUM and Iran-based group TA453. GCHQ's National Cyber... Jan 26, 2023</p>	 <p>Generative AI</p>	<p>Forbes The Good, The Bad And The Reality: The Impact Of AI On Cybersecurity Danny Lopez, CEO of Glasswall, has had a successful international career to date in banking, marketing, diplomacy and technology. Nov 20, 2023</p>	 <p>Talent</p>	<p>Security Magazine 71% of organizations are impacted by cybersecurity skills shortage Most organizations (71%) report that they've been impacted by the cybersecurity skills shortage, leading to an increased workload for the... Sep 5, 2023</p>
 <p>Regulation</p>	<p>CyberScoop SEC disclosure rule for 'material' cybersecurity incidents goes into effect The controversial rule requires publicly traded companies to report such events to the agency within four business days. 1 month ago</p>	 <p>Dark Web Crackdown</p>	<p>Reuters 'Operation Cookie Monster': Dutch arrest their most-wanted suspect in cyber case Dutch police have arrested a man they described as their most wanted suspect in the investigation into the Genesis Market... Jul 25, 2023</p>	 <p>Mega Breaches</p>	<p>Cyber Security Hub Largest DDoS attacks ever reported by Google, Cloudflare and AWS Cyber Security Hub The DDoS attack was more than seven times larger than the previous recording breaking DDoS attack ... Internet infrastructure providers Google... Oct 13, 2023</p>


Market Growth Continues Driven by Embedded Tailwinds

Global Cybersecurity Spend (\$B)



- The constant evolution and sophistication of cyber threats, including malware, ransomware, and advanced persistent threats, drive the demand for cybersecurity solutions. As the frequency and severity of cyber-attacks rise, organizations invest in robust cybersecurity measures.
- The ongoing digital transformation across industries, coupled with the widespread adoption of cloud services, IoT, and interconnected technologies, creates an expanded attack surface. The growing interconnectivity of devices and systems necessitates heightened cybersecurity efforts.
- Organizations—challenged by the lack of cyber resources globally—are increasingly investing in advanced technologies such as AI-driven threat detection, automated response systems, and machine learning to augment their cybersecurity capabilities and bridge the talent gap.

Trends and Innovators We're Monitoring in 2024

 	<p>Artificial Intelligence Across Categories Adoption of AI in cybersecurity has been robust. From early threat detection to predictive analysis and adaptive security measures, category leaders in innovation are integrating AI into their tools and playing a pivotal role in fortifying digital landscapes.</p>
 	<p>Next-Generation of Cyber Training AI-driven adaptive learning, gamification, collaborative environments, and a commitment to continuous learning are driving a more effective set of cyber training tools where legacy solutions have historically fallen short.</p>
   	<p>Continuous Threat Exposure Management In 2022, Gartner introduced the CTEM framework, a program approach that takes a holistic view of threats and surfaces, actively prioritizing whatever most threatens business in the moment; vendors have adapted to support this approach.</p>
   	<p>Truly Unified Identity Orchestration The number of SaaS tools and cloud accounts in use at most businesses continues to increase, and not all of these are under the auspice of IT and security departments. Identity tools are adapting to provide a more precise overview and enable stronger oversight.</p>

Transaction Environment




2023 Year in Review

2024 Prediction Tracking











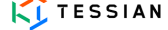



Cyber Research Summary

Data Breaches

2023 Transaction Environment Summary

 M&A	\$ Value: \$49.7B	Transactions: 252	YoY Transaction Growth: -3%
 Financing	Capital Raised: \$10.8B	Transactions: 624	YoY Transaction Growth: -38%
 Public	Index Return: 83%	Revenue Growth: 18%	Earnings Growth: 29%

Headline Transactions

<p>Deepwatch Raises \$180M Series B</p>  <p>Date: 2/15/2023 EV: N/A Rev: N/A EV/Rev: N/A</p>   <p>Target: Managed detection and response services.</p> <p>Rationale: Emerging market leader in managed detection and response security at the enterprise level.</p>	<p>Wiz Raises \$300M Series D</p>  <p>Date: 2/27/2023 EV: \$10.3B Rev: \$200M EV/Rev: 51.5x</p>   <p>Target: Cloud-native application protection platform built for security operations and development teams.</p> <p>Rationale: Rapid adoption of cloud networks and Wiz's position as the gold standard in cloud security position the business for continued success.</p>	<p>Cisco Acquires Armorblox</p>  <p>Date: 5/31/2023 EV: ND Rev: ND EV/Rev: ND</p>  <p>Target: AI-driven email security and data loss prevention SaaS.</p> <p>Rationale: Use of predictive and generative AI technology across Cisco's product portfolio.</p>
<p>Cisco Acquires Splunk</p>  <p>Date: 9/21/2023 EV: \$29.0B Rev: \$3.8B EV/Rev: 7.5x</p>  <p>Target: Machine-to-machine IT systems, cybersecurity, and application performance management SaaS.</p> <p>Rationale: Accelerate Cisco's connectivity security strategy.</p>	<p>Proofpoint Acquires Tessian</p>  <p>Date: 10/30/2023 EV: \$300M Rev: \$40M EV/Rev: 7.5x</p>  <p>Target: AI-enabled email security, defense, and data protection SaaS and APIs.</p> <p>Rationale: Expand advanced behavioral and dynamic detection platform functionality.</p>	<p>Palo Alto Acquires Talon Cyber</p>  <p>Date: 12/28/2023 EV: \$625M Rev: NM EV/Rev: NM</p>  <p>Target: Secure browser engineered to provide enterprise-grade security across all devices.</p> <p>Rationale: Better foothold in endpoint workstation security building on previous acquisition of Secdo.</p>

Takeaways in Dealmaking

Strategic Buyer Activity

Strategics are back, evident in the convergence of bid and ask prices and the sector's consolidation. The top eight most active strategics in cyber have made 35 acquisitions or investments in the past two years. The combination of the opportunity to bargain hunt in a compressed market and the rapid pace of innovation required to stay differentiated across categories of cyber has led to a contrarian trend among cyber strategics vs. the broader M&A market.

Premium Asset Valuations

Market-leading cybersecurity companies with compelling financial profiles continue to command premium valuations, even amid a broader M&A market experiencing depressed valuations. These innovative technologies, established market presence, and strong unit economics contribute to sustained investor confidence. The strategic nature of these assets to incumbents in the cybersecurity land grab has led to an increased willingness to pay.

Bilateral/Targeted Negotiations

Cyber transactions are being conducted via targeted and bespoke processes vs. broad auctions. A key driver behind this trend is the asymmetry in incentives, where sellers find themselves less motivated to go out to the market in an environment where cybersecurity assets are in high demand; buyers who recognize the scarcity of quality assets in this space are keenly interested and willing to engage in direct negotiation.

▲ Houlihan Lokey Transaction

Notable Highlights




- Led highly recognized Armorblox sale to Cisco.
- Advised leading financial sponsor Carlyle on cyber platform investment of NEVERHACK.
- Grew cyber team expertise through internal additions and the acquisition of 7 Mile Advisors.
- Hosted Former U.S. National Cyber Director as part of Houlihan Lokey tech conference cybersecurity panel.
- Cyber team featured in Yahoo! Finance.
- No. 1 technology M&A advisory team globally.
- Middle Market Growth: Investment Bank of the Year.

Cyber Engagements

6
2023
Engagements

90+
Closed Cyber Deals*
(All-Time)

Cyber Team Highlights

Transactions	Conferences	Insights	Team
<p>Completed 6 Engagements</p>  <p>Exceeding \$1B+ Aggregate Valuation</p> <p>▼</p> <p>30+ Houlihan Lokey Deal Team Members</p>	<p>600+ Houlihan Lokey Tech Conference Attendees</p>  <p>70 Participating Companies</p> <p>▼</p> <p>4 Cybersecurity Presenters</p> <p>30+ One-on-One Meeting Requests From Top Financial Sponsors</p>	<p>6 Houlihan Lokey Reports Published</p>  <p>Collectively 500+ Research Hours</p> <p>▼</p> <p>10,000+ Transaction Database</p> <p>12,000+ Company Universe</p>	<p>Welcomed 3 New Members to the Cyber Coverage Team</p>  <p>Currently 15+ Financial Professionals</p> <p>▼</p> <p>7 Countries</p> <p>100+ Years of Experience</p>

Cybersecurity Predictions for 2024

2023 Year in Review

2024 Prediction Tracking

Cyber Research Summary

Data Breaches

Shortage of Professionals



- 54% of cybersecurity professionals believe that the impact of the skills shortage on their organization has worsened over the past two years.
- Cybersecurity professionals will increasingly be expected to take on more complex workloads during 2024 as the threat landscape grows ever more sophisticated.

Generative AI



- As 2023 was dubbed “The Year of AI,” we expect to see more sophisticated and smarter AI-powered attacks in 2024.
- The winner of cyberwarfare will go to the party that can successfully utilize AI effectively against their respective advisories.

Governance and Regulation



- Governments and organizations are becoming increasingly aware of the risks to national security and to economic growth posed by cyber threats.
- Gartner has predicted that by 2026, 70% of company boards will include at least one member with expertise in cybersecurity.

Sophisticated Attacks



- From ransomware to phishing, we expect threat actors to continue to carry out more sophisticated attacks, especially on enterprises, as the payouts increase YoY.
- As businesses continue to grow their IT environment, hackers have more intrusion points into the supply chain than ever before.

Cybersecurity Insurance



- As cyber threats grow in complexity and frequency, organizations are increasingly turning to cybersecurity insurance to mitigate financial risks associated with data breaches and cyber-attacks.
- More insurers are entering the market, increasing competition, which is expected to lower premiums.

IoT Security Is Crucial



- The exponential growth of IoT devices, interconnecting an ever-increasing number of diverse and ubiquitous devices, poses significant security challenges, as their attractiveness to cyber-attacks and interconnected nature can lead to widespread vulnerabilities.

33N: There Is a Large Opportunity for Investors Within European Cybersecurity

2023 Year in Review

2024 Prediction Tracking

Cyber Research Summary

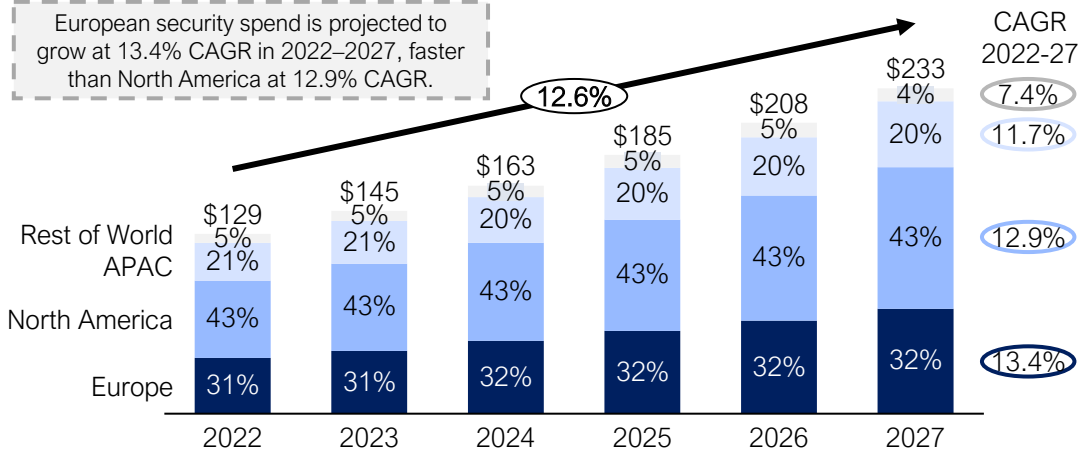
Data Breaches



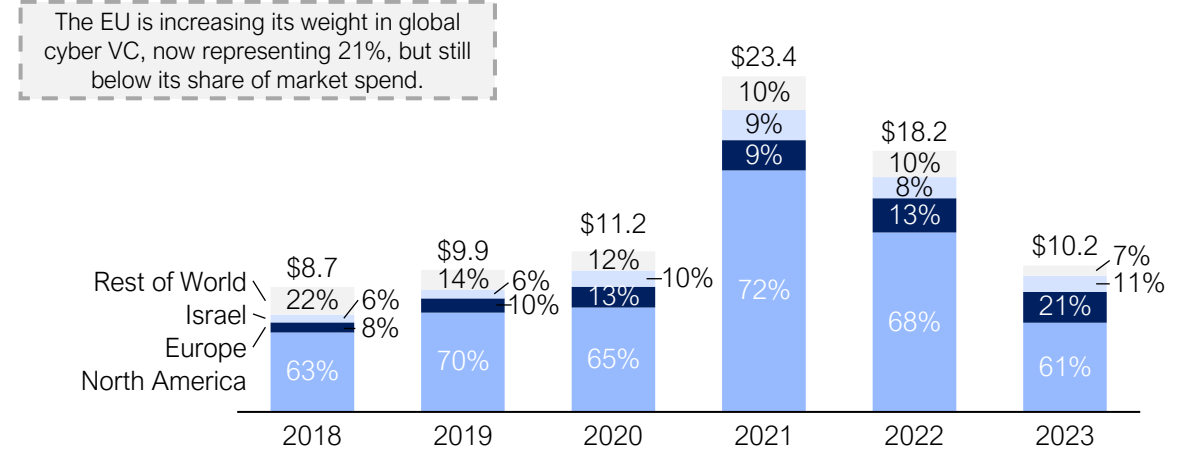
33N is a European cybersecurity and infrastructure software specialized VC investing globally. 20+ VC investments plus a pan-European MSSP buy-and-build, in the past 10 years. Here, they share key insights on the European cybersecurity market.

Market Size

Projected Security Spend (\$B) by Geography⁽¹⁾



Cybersecurity VC Investment (\$B) by Geography⁽²⁾



EU Market Drivers



The EU employs more software developers than the U.S., thanks to its top universities and research institutions, representing a huge addressable market and breeding ground for cybersecurity startups.



Public defense and security spending has hit all-time highs and is expected to continue accelerating.



The EU has historically been among the fastest-enforcing public strategies (e.g., Cyber Resilience Act, AI Act, GDPR), driving demand for cybersecurity solutions.



The EU-wide and nationwide funding incentives and incubators/accelerators are in place, providing supportive ecosystems for the early stages of a startup.



Security is increasingly managed; European MSSPs are looking to enrich their managed security and taking a leading role in driving enterprise adoption of cybersecurity solutions and services (either via M&A or partnerships).



Europe holds an immense growing opportunity, but a complex one.

- Europe can be both a breeding ground for global players as well as a sizeable addressable market for foreign providers but...
- Europe is composed of different regional/national markets that require specialized access and time to navigate.

Cybersecurity-specialized investors are at a unique advantage.

- Domain expertise and specialized network are key to successfully investing in this expansive ecosystem and adding distinctive value to portfolio companies.
- Having visibility into the global cyber ecosystem, including into advanced markets such as the U.S. and Israel, is key to identifying unique opportunities and adding value.

Service partners are key to scale across Europe.

- Service providers are the prescribers of cybersecurity technologies for the enterprise.
- A network of service partnerships may provide accelerated pan-European access.

Source: 33N Ventures.

(1) Gartner, IDC, McKinsey.

(2) PitchBook as of January 9, 2024.

Scythe.io: Continuous Threat Exposure Management Is a Must in 2024

2023 Year in Review

2024 Prediction Tracking

Cyber Research Summary

Data Breaches



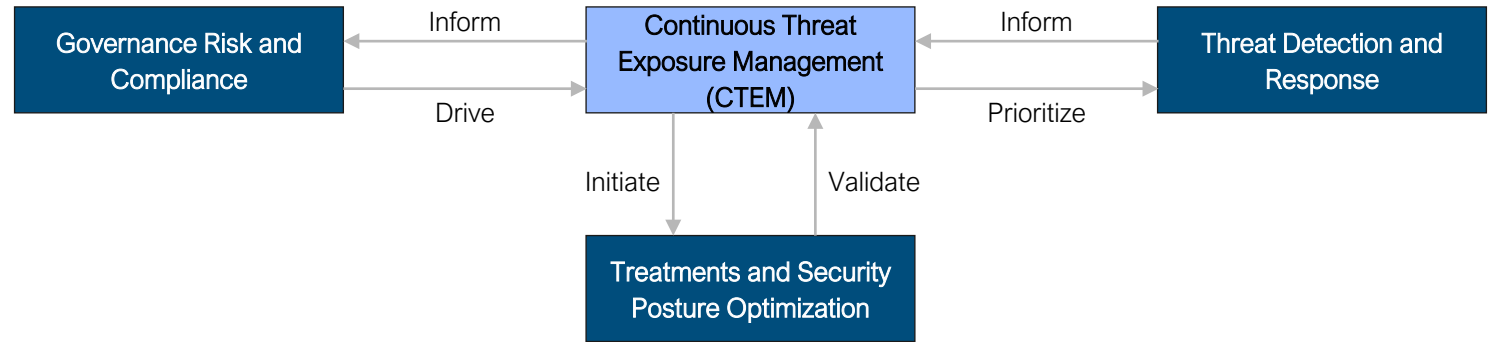
Organizations with vulnerability management programs face challenges as **traditional approaches struggle to keep up with evolving business needs and expanding attack surfaces**. The operational impracticality of fixing every known vulnerability has increased with digital transformation, leading to a complex technological environment. The **continuous threat exposure management (CTEM) program** is proposed as a pragmatic approach to prioritize treatments and refine security postures continuously. CTEM aims to provide **a consistent, actionable security remediation plan, emphasizing the importance of business risk appetite** in selecting remediation strategies. Unlike real-time constraints in security operations centers, CTEM **informs long-term strategy shifts without such limitations**.



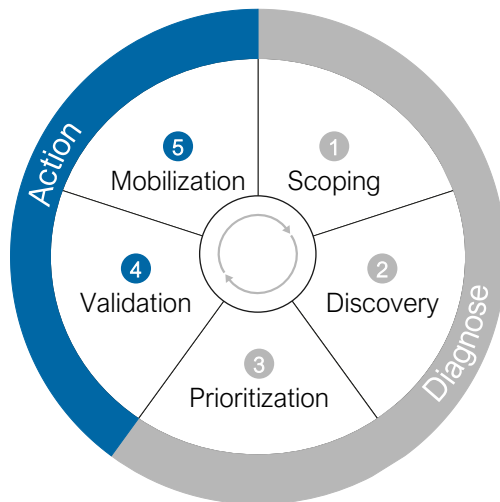
Scythe's innovative approach to CTEM redefines cyber resilience, enabling dynamic adaptation to emerging threats beyond the reach of traditional vulnerability management programs.



– Bryson Bort, Founder and CEO, Scythe



CTEM Program



The Scythe Approach

- 3 By emulating attacks, the SCYTHE platform allows organizations to assess their security control efficacy and incident response capabilities through a more comprehensive and continuous improvement approach.
- 4 The platform provides data that inform strategic decisions on cybersecurity, helping prioritize actions based on the organization's specific threat landscape and risk tolerance.
- 5 Finally, the SCYTHE platform confirms and communicates the actionable steps to all stakeholders, focusing on remediation efforts and measurable outcomes.

UC Berkeley, CNA, and World Economic Forum: Cybersecurity Futures 2030

2023 Year in Review

2024 Prediction Tracking

Cyber Research Summary

Data Breaches

The UC Berkeley Center for Long-Term Cybersecurity (CLTC), the World Economic Forum Centre for Cybersecurity, and CNA's Institute for Public Research have collaborated to explore how digital security could evolve over the next five to seven years through various workshops with key cybersecurity decision-makers.







Key Observations

-  Trust Matters
-  Digitization vs. Next Generation Technology
-  Public-Private Partnerships
-  U.S.-China Relations

- 1 Strengthening trust** has become a pivotal objective in cybersecurity endeavors for the upcoming decade. At a strategic level, governments with stability and commitment to long-term technology and cybersecurity strategies can **evolve into trusted entities**, enjoying benefits such as talent attraction, leadership roles in international standard-setting processes, and effective counteraction of disinformation campaigns.
- While there has been significant media attention on AI, automation, quantum computing, and other next-generation technologies, thought to be the main drivers of global security, **it is the pace and scale of digitalization that will drive changes in global security**, particularly in developing countries with large populations.
- Public-private partnerships will be imperative** to move the needle on combating sovereign and criminal cyber-attacks and information operations, but new incentive structures will be needed to achieve such partnerships.
- Global concerns about technological colonialism, particularly in relations with China and the U.S., persist regardless of the future U.S.-China relationship strength. **Leaders foresee a reshuffling of global alliances in the coming years** to align with their technology and security goals.

Recommendations

-  Strengthen the Supply Chain
-  Develop a Digital Savvy Population
-  Create Effective Policies
-  Thoughtfully Evaluate Technology

- Organizations will need to ensure they **have a stable and secure supply chain of resources**, including technology components, raw materials, and skilled, affordable workers.
- Having a digitally literate public and customer base that is media savvy and inoculated against mis-, dis- and mal-information will be a source of strength for organizations that wish to succeed in an era of degrading trust. **This can be achieved from investments from the public and private sectors.**
- Effective digital policies and regulations should demonstrate clear and stable priorities** of companies, governments, and other organizations. The inability to overcome social engineering—whether from internal or external sources—will increase polarization, erode trust in digital products and platforms, and leave organizations in a weakened position to solve other challenges.
- Excessive “digital consumerism” becomes a vulnerability** when it leads to dependency on major tech firms or technology products and services from other countries. Both organizations and nations should thoughtfully assess the benefits of investing in innovation rather than solely relying on readily available market solutions.


Houlihan Lokey Cyber FVA: Significant Recent Developments in the Cybersecurity Regulatory and Compliance Area

2023 Year in Review

2024 Prediction Tracking

Cyber Research Summary

Data Breaches

 Regulatory bodies are preparing to audit and enforce these regulations. Unlike the self-certification processes of yesteryear, impacts will be felt across company third-party service providers (e.g., business process outsourcing providers, IT and software providers).

December 2023

SEC
Cybersecurity
Rule

SUMMARY

Public companies must publicly disclose their cyber practices, maintain strong governance, and quickly report cyber breaches.

IMPACTED BUSINESSES

All publicly traded companies under the SEC, across all industries.

SUMMARY

Requires regulated entities to adopt detailed cyber practices and quickly report cyber breaches.

IMPACTED BUSINESSES

Financial services: From small brokers to international banking entities, including insurance companies; banks, trusts, and foreign bank branches; mortgage banks, brokers, and lenders; and money transmitters, check cashers, and other nondepository financial institutions.

NYDFS
Cybersecurity
Regulation

December 2023

March 2023

PCI Version 4



SUMMARY

Version 4 modernizes expected security controls for payment info handling; also forces companies to reconsider their business processes to save costs.

IMPACTED BUSINESSES

Direct-to-consumer (D2C) e-commerce and brick-and-mortar (from Target.com to car washes), B2B bill payment vendors, merchant banks, and financial institutions.

SUMMARY

Long-standing healthcare privacy and security law.

Major rewrite coming in 2024.

IMPACTED BUSINESSES

U.S.-based healthcare: healthcare providers (traditional physician offices, ER, and virtual care), healthcare clearinghouses (e.g., medical claim and invoice processing), and any business with access to protected health information (PHI).

HIPAA, by
Extension,
HITRUST,
and HITECH



August 1996

Late CY 2024

DoD's CMMC



SUMMARY

Transforming the Department of Defense's (DoD) supply chain through cybersecurity with material impacts on company revenue streams.

IMPACTED BUSINESSES

Businesses in the DoD supply chain, including defense contractors, manufacturers, fabricators, IT solution providers, and companies subject to ITAR and DFARS.

SUMMARY

Bringing EU GDPR-like consumer privacy protections to California residents.

Used as a model for other U.S. states (Virginia, Colorado, etc.).

IMPACTED BUSINESSES

CA-registered or operating companies processing customer data, across all industries.

Limited exclusions for startups.

California
CCPA/CPRA



January 2020

Critical Takeaways

- Microsoft has leveraged its unique vantage point via its ecosystem of more than 10,000 security experts, AI-powered analysis of more than **65 trillion data points**, and **15,000 security partners** to identify the most thematic cybersecurity challenges for corporations and the most effective way to combat them.
- Ransomware, DDoS attacks, Nation State Threats, and IoT-OT security practices** command the attention of businesses with dramatic growth of malicious acts and nuanced evolutions that require well-coordinated defenses.
- In reality, the **vast majority** of successful cyber-attacks could be thwarted by implementing a few fundamental security hygiene practices.
- The use of advanced AI techniques and greater **global collaboration against cybercrime and initiatives** like the *Cybercrime Atlas* trends will begin to reverse and cyber activity will be cut off at the source.

The Scale of Attacks Are Multiplying Rapidly



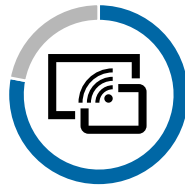
10x increase in the number of attempted password attacks in 2023; 4K password attacks per second targeting Microsoft cloud identities.

Stakes Are Higher Driven by Nation State Attackers



41% of threat notifications Microsoft sent to online services went to critical infrastructure organizations—Russia, China, Iran, North Korea, and now Palestine are the most active Nation State cyber-attackers.

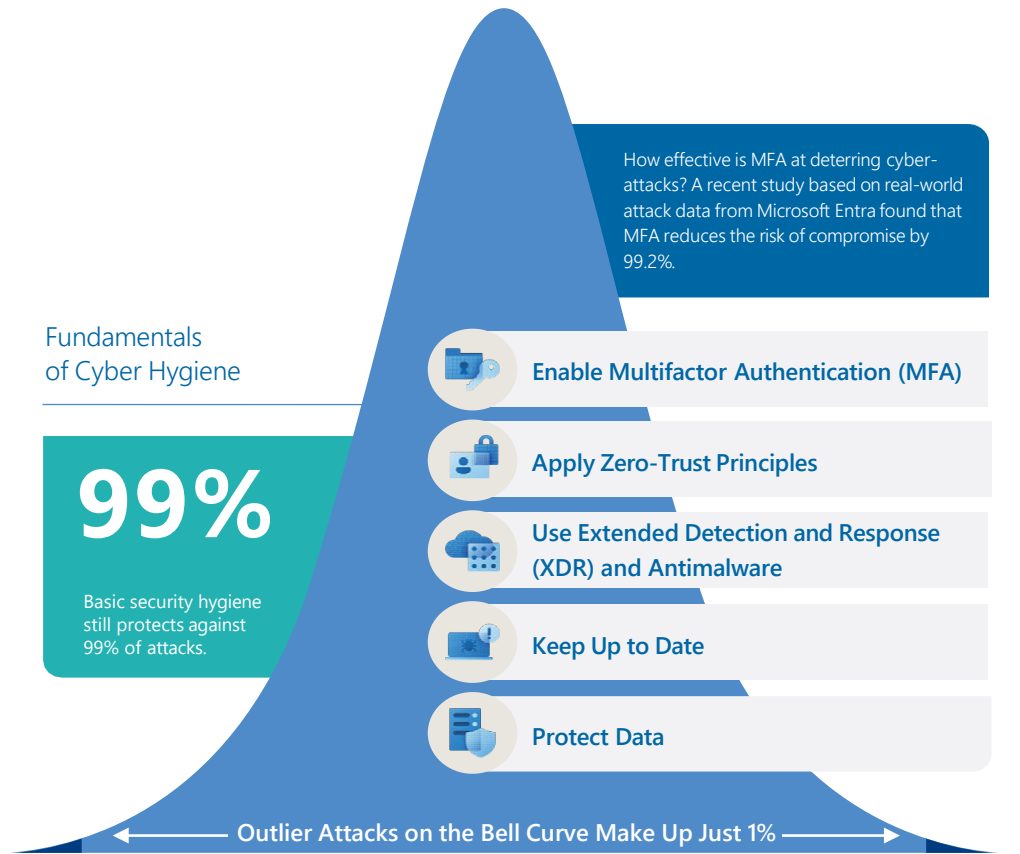
Attackers Are Honing In on the Most Vulnerable Vectors



78% of connected devices on the Microsoft Defender customer networks have known vulnerabilities—IoT defense strategy remains critical to protecting the business ecosystem.

Basic Security Hygiene Remains Highly Effective in Combating the Vast Majority of Cyber Threats

Even with the rapidly evolving cybersecurity technology ecosystem, the vast majority of successful **cyber-attacks could be thwarted by simply implementing a few fundamental security hygiene practices.**



How effective is MFA at deterring cyber-attacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2%.

Fundamentals of Cyber Hygiene

99%

Basic security hygiene still protects against 99% of attacks.

- Enable Multifactor Authentication (MFA)
- Apply Zero-Trust Principles
- Use Extended Detection and Response (XDR) and Antimalware
- Keep Up to Date
- Protect Data

Outlier Attacks on the Bell Curve Make Up Just 1%

Apple: The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase

2023 Year in Review

2024 Prediction Tracking

Cyber Research Summary

Data Breaches

Critical Takeaways

Global Increase in Cyber-Attacks

- Cybercriminals globally target readable personal data, **leading to a surge in cyber-attacks and data breaches**, especially in cloud storage.
- A recent study indicates historically high levels of threats to consumer data in the cloud, with indicators suggesting a worsening situation.

Record Data Breaches in the U.S.

- Data breaches in the U.S. have hit an all-time high, with a **nearly 20% increase** in the first nine months of 2023 compared to the entire 2022.
- The rise is attributed to the growing trend of individuals living more of their lives online, resulting in organizations collecting significant amounts of personal data, making them prime targets for cybercriminals.

Factors Driving Increased Threats

- Ransomware attacks have become **more numerous, sophisticated, and aggressive** in 2023, with hackers organized into ransomware gangs targeting organizations with sensitive data.
- Exploitation of vulnerabilities in vendors' systems is on the rise, spreading consequences to numerous organizations that depend on those vendors. Recommendations include limiting readable personal data storage and adopting advanced encryption solutions.

Expert Commentary



"We assess that ransomware attacks targeting U.S. networks will increase in the near and long terms. Cybercriminals have developed effective business models to increase their financial gain, likelihood of success, and anonymity."

—Alejandro Mayorkas, U.S. Secretary of Homeland Security



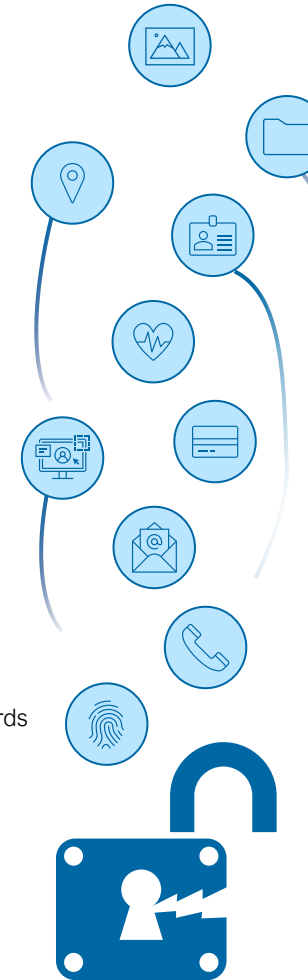
"In cyberspace, the threats only seem to evolve, and the stakes have never been higher... And over the past few years, we've increasingly seen cybercriminals using ransomware against U.S. critical infrastructure sectors."

—Christopher Wray, Director of the FBI



"In recent years, we have seen an unprecedented increase in both the number of cyber threats and their sophistication, with attacks becoming more tailored as criminals aim for maximum impact, and maximum profit."

—Bernardo Pillot, INTERPOL's Assistant Director of Cybercrime Operations



1 of 4

In the first three quarters of 2023, one in four people in the U.S. had their health data exposed in a data breach.

360 Million

In the first eight months of 2023 alone, more than 360 million people were victims of corporate and institutional data breaches.

+70%

In the first three quarters of 2023, the number of ransomware attacks increased by almost 70% compared to the first three quarters of 2022.

98%

98% of organizations have a relationship with a vendor that experienced a data breach within the past two years.

95%

In the 2023 IBM Cost of a Data Breach Report, 95% of breached organizations surveyed experienced more than one data breach. According to a 2022 study by Forrester, nearly 75% of surveyed organizations were victims of a data breach in the prior 12 months.

3x

The number of data breaches more than tripled between 2013 and 2022.

2.6 Billion

More than 2.6 billion personal records were breached in 2021 and 2022 (1.1 billion in 2021 and 1.5 billion in 2022).

80%

According to a 2023 report, more than 80% of data breaches involved data stored in the cloud.

Automation Remains a Top Focus for Security Budgets

Almost all saw a surge in their cybersecurity automation budgets from last year. However, **only 18.5% experienced a net new budget this year, a decrease from 34% in the previous year.** Budgets are now often reallocated from external sources or other tools, with a slight decline in funds from headcount compared to last year. Despite economic challenges, **there's a global consensus on the pivotal role of cybersecurity automation in business strategies.**

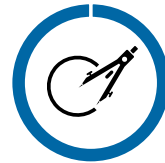
Processes/Use Cases Automated in Organizations

Processes	2022	2023
Phishing Analysis	26%	31%
Incident Response	26.5%	30%
Vulnerability Mgmt./ Prioritization	25%	30%
Alert Triage	18%	30%
Threat Intelligence Mgmt.	26.5%	29%
Password Reset	21%	28%
Threat Hunting	25%	27%

Increasing efficiency remains the top reason why organizations are adopting cyber automation. Notably, **the importance of maintaining cybersecurity standards has declined in priority.** This shift may indicate a heightened emphasis on efficiency and productivity amid a more challenging economic environment, rather than a diminishing interest in cybersecurity performance.

Automation Adoption Faces Some Challenges

The widespread adoption of cybersecurity automation has brought forth significant challenges, with a prevalent issue being a **lack of trust** in the outcomes delivered by automated processes. Slow user adoption closely follows, indicating a connection between trust issues and adoption rates, particularly in environments with high team member churn.



100%

of security professionals have experienced problems when trying to automate cybersecurity.



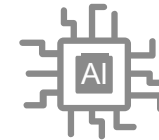
27%

of CISOs have expressed that the availability of training is an important feature when they are selecting automation solutions.

Top Issues When Implementing Cybersecurity Automation by Rank

- 1st Lack of Trust of Outcomes
- 2nd Slow User Adoption
- 3rd Bad Decisions
- 4th Lack of Skill

Actionable Recommendations



Invest in Smart Tools to Manage Mounting Security Team Stress

Companies can boost threat intelligence analyst well-being and retain employees by **investing in intelligent tools with AI capabilities.** These tools streamline work processes, enabling quicker and more accurate decision-making. Additionally, offering flexible working hours and locations promotes a healthier work-life balance, contributing to a positive work environment and increased job satisfaction.



Focus on Proven Use Cases and Data Drive Decisions

Companies should prioritize proven automation use cases in cybersecurity, including **threat intelligence management, incident response, phishing analysis, and vulnerability management.** These cases have shown value by saving time and improving security procedures, forming a strong basis for a successful automation strategy. Moreover, companies should emphasize the integration of multiple data sources to enhance contextual insights, allowing automation to focus on relevant and high-priority events aligned with the real-time threat landscape for continuous improvement.

Training the Future

Training is the strongest tool in any company's toolbox to combat issues like "lack of trust in outcomes" and "slow user adoption."

Breach Overview

Company Description: Cloud-native security company that focuses on identity and access management.

Date of Breach: September 2023.

What Happened: A threat actor gained unauthorized access to files inside Okta's customer support system (Okta Help Center), which contained information such as company name, employee description/role, address, phone numbers, emails, and date of last password changes.

Outcome of Breach: Shares of Okta fell 2% on the day of the announcement, with an additional 12% after the announcement that all customers were affected.

Key Stats

134

Okta customers initially thought to be impacted, roughly less than 1%.

99.6%

of customers were impacted by the breach after further investigations.

~\$2B

Okta market capitalization lost after the announcement.

Attack Methodology and Rationale



While it is still unclear who the threat actor is, the European and U.S. group of hackers called Scattered Spider is suspected of being tied to this breach. This group has previously leveraged various social engineering tactics to target accounts of Okta customers, including Caesars Entertainment and MGM resorts.



After investigations, the unauthorized access to Okta's customer support system occurred through a service account stored within the system, with permission to manage support cases. Okta Security found an employee signed into their personal Google profile on the Okta-managed laptop, where the service account credentials were saved, which likely was the point of exposure.

Expert Opinions and Commentary



"It's like the fog of war, and you may not actually have all the answers. So, companies are in a difficult position—your duty to disclose versus the fact that you might not have all the information available. That's kind of an unfortunate reality of the cyber world we live in and for companies like Okta to rebuild trust, it's probably going to be a longer road to do that."

—Merritt Maxim, VP and Research Director at Forrester

The Outcome

- After more than five weeks after Okta first told customers of the September breach, the company's Chief Security Officer, David Bradbury, announced that hackers had stolen information on essentially all users of its customer support system.
- Many of the compromised accounts are those of Okta administrators and IT personnel tasked with implementing Okta's authentication technology in customer environments. These individuals need to remain vigilant against targeted phishing attacks.
- Okta discovered additional reports and support cases the threat actor accessed, which further broadened the exposure to all Okta Workforce Identity Cloud and Customer Identity Solution customers. Fortunately, Government agency customers using Okta's FedRamp High and Department of Defense IL4 environments were not impacted.

Key Takeaway

Access Controls to Service Accounts

Unlike standard user accounts, which are accessed by humans, service accounts are mostly reserved for automating machine-to-machine functions, such as performing data backups or antivirus scans every night at a particular time. For this reason, they can't be locked down with multifactor authentication the way user accounts can.



Companies can secure their service accounts either by limiting or conditioning the IP addresses that can connect to the account or by regularly rotating access tokens used to authenticate access.

Breach Overview

Company Description:	American discount variety store chain.
Date of Breach:	August 2023.
What Happened:	Dollar Tree shared the private, unencrypted information of its employees and customers with a human-resources software vendor, Zeroed-In Technologies, LLC, which then stored that private information in an unencrypted, internet-accessible environment on its public network.
Outcome of Breach:	Dollar Tree is now facing a class action lawsuit filed by employees.

Key Stats⁽¹⁾

~1.9M+

Dollar Tree and Family Dollar employees affected.

\$16.6K+

Dollar Tree and Family Dollar retail locations across the U.S. and Canada.

\$1

is all it takes to buy a Social Security number on the dark web.⁽¹⁾

Attack Methodology and Rationale



While the Zeroed-In investigation was able to determine that these systems were accessed, it was not able to confirm all of the specific files that were accessed or taken by the unauthorized actor.



Dollar Tree has remained largely silent on the issue, pushing the blame onto Zeroed-In as its third-party HR software provider.

Expert Opinions and Commentary



“On one hand, organizations are forced to work closely with third-party providers to be competitive, while on the other hand, if these third parties are not secure, which is out of their control, it inherently puts organizations at risk and challenges their ability to remain secure. Determined cyber-attackers will keep probing an organization’s defenses until they find the weakest chain in the supply chain, which in some cases may be your service provider.”

—Etay Maor, Senior Director of Security Strategy at Cato Networks

The Outcome



Dollar Tree and Zeroed-In are facing class-action litigation filed in the U.S. District Court in Florida, alleging that the companies were negligent in notifying employees about the data breach. Employees were notified four months later (in late November via mail), despite the breach occurring in August.



Zeroed-In promised a year of identity fraud services to impacted individuals, but the lawsuit claims this is a wholly inadequate solution.



It remains unclear if Dollar Tree is supporting the third-party data breach victims in any way.

Key Takeaway



Zero-Trust and Supply Chain Defense

This breach underscores the importance of a zero-trust approach to supplier risk management, involving comprehensive mapping, data classification, and the adoption of next-gen data loss prevention (DLP) tools.

Companies can conduct comprehensive mapping utilizing identity and access management tools to ensure a clear understanding of who has access to their data.

Many third-party software providers such as Slack, Teams, and Zoom are offering next-gen DLP tools native to their solutions.

Breach Overview

Company Description: Global software company that provides a wide range of products and services to help organizations develop, deploy, and manage business applications.

Date of Breach: May 2023.

What Happened: Progress Software's managed file transfer (MFT) solution, known as MOVEit Transfer, which allows organizations to share large files and datasets over the internet, was targeted by the CL0P Ransomware Gang.

Outcome of Breach: Progress Software has received a subpoena from the SEC, incurred \$1 million in cost after insurance recoveries, and 58 class action lawsuits related to the breach.

Key Stats⁽¹⁾

2,500+
Organizations at risk.

64M+
Individuals affected.

Selected Organizations Affected

BRITISH AIRWAYS

BBC

blue
california

NOVA SCOTIA

SONY

zellis

Attack Methodology and Rationale

CL0P Ransomware Gang, also known as TA505, began exploiting a previously unknown SQL injection vulnerability in Progress Software's MOVEit Transfer. The first attack occurred in May with a second occurring right after in June.



The Cl0p gang is generally considered to be a Russian cybercriminal group (ostensibly not operating at the behest of the Kremlin) and it operates with impunity inside Russia's border. This has caused the U.S. State Department to reward up to \$10 million for information conclusively linking the Cl0p ransomware group to foreign governments.

While the initial breach only directly compromised at least 100 customers, the actual number of victims swells when the downstream repercussions are considered. More than 84% of known victim organizations impacted were via their third-party vendors.⁽¹⁾

Expert Opinions and Commentary



"Software is now integral to so many physical products that the software industry can't claim special immunity because their products are complex or hard to debug. It is critical to address the lack of accountability to drive the market to produce safer products and services while preserving innovation"

—Willy Leichter, Vice President at Cyware

Cybersecurity experts reemphasize the issue of a small number of technology companies producing software with massive and far-reaching effects.

The Outcome

- In a recent filing with the U.S. Securities and Exchange Commission (SEC), the company reported \$2.9 million in losses due to the attack up to the end of August 2023; however, it held \$15 million in cyber insurance policies at the time of the attack and still has \$10.1 million available. \$1.9 million of the costs associated with the attack are being covered by its insurance policies, and it has only incurred direct costs of \$1 million.
- Progress Software has also confirmed that it received an SEC subpoena on October 2, 2023, seeking documents related to the incident and information on the vulnerability that was exploited. The company intends to fully cooperate with the investigation.
- The education sector was the worst affected, accounting for around 41% of victims, followed by healthcare (19%), and finance/professional services (12%).⁽²⁾

Key Takeaways



Limiting the Damage: End-to-End Encryption

Limiting the amount of readable consumer data retained by organizations is one of the most effective ways to protect consumers. End-to-end encryption, a type of encryption that ensures only the sender and receiver of the data can access and modify data, is one method companies use to protect their data.



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.

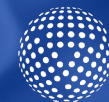
Sources: Tech Crunch, "Microsoft says Cl0p ransomware gang is behind MOVEit mass-hacks, as first victims come forward"; Tech Crunch, "SEC is investigating MOVEit mass-hack, says Progress Software"; CSO, "US feds stress urgent MOVEit platform patching after attacks hit agencies."

(1) Cybersecurity Dive, "Progress Software's MOVEit meltdown: uncovering the fallout."

(2) The HIPPA Journal, "SEC Launches Investigation into Progress Software's MOVEit Hack."



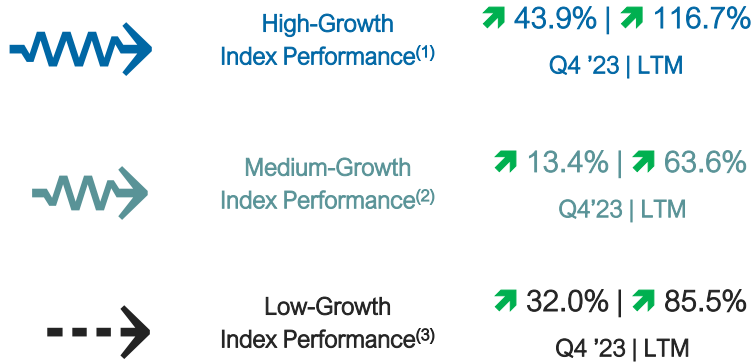
Capital Markets and Trends Update



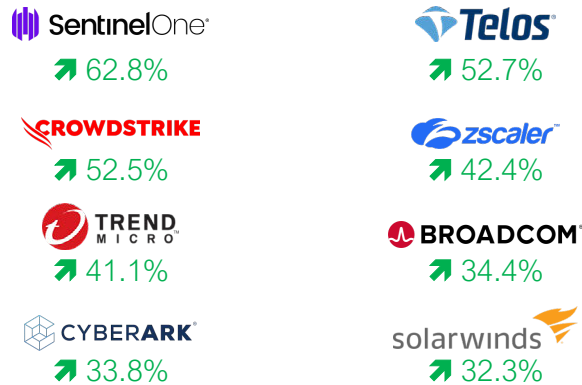
Cybersecurity Dashboard

Public Market Environment

Public cybersecurity companies experienced solid growth and closed out 2023 with their best quarter performance.

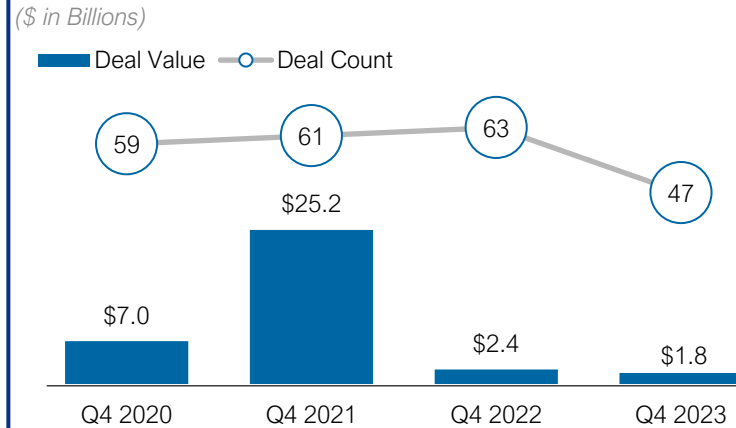


Selected Cybersecurity Performance Q4 2023



M&A Environment

Despite positive public market activity, M&A activity was depressed.

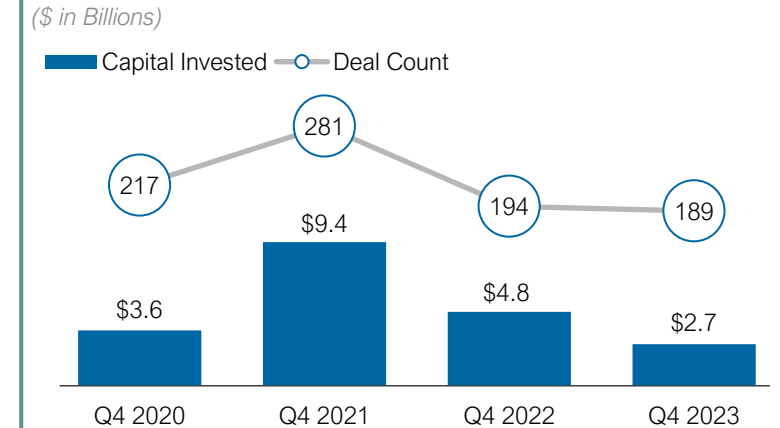


Selected Q4 Transactions

Ann. Date	Acquirer	Target	EV	EV/Rev
Dec-26	SONICWALL	BANYAN SECURITY	NA	NA
Dec-21	CISCO	ISOVALENT	\$650	NA
Oct-31	paloalto	Dig Security	\$400	NA
Oct-30	proofpoint	TESSIAN	\$300	7.5x
Oct-23	Rockwell Automation	VERVE	\$185	5.8x

Private Funding Environment

Investors continue to show restraint in their capital deployments, showcasing their desire for quality, sound, and strategic assets.



Selected Q4 Financings

Ann. Date	Investor	Target	Amount	Val.
Dec-19	L2Point	SIMSPACE	\$45	\$150
Dec-18	BainCapital VENTURES	halcyon	\$40	\$236
Nov-20	SAPPHIRE VENTURES	BioCatch	\$70	\$1,070
Oct-23	CANAPI PRYSM CAPITAL	Island	\$100	\$1,500
Oct-17	Capital One VENTURES MassMutual Ventures	Prove	\$44	\$1,334

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

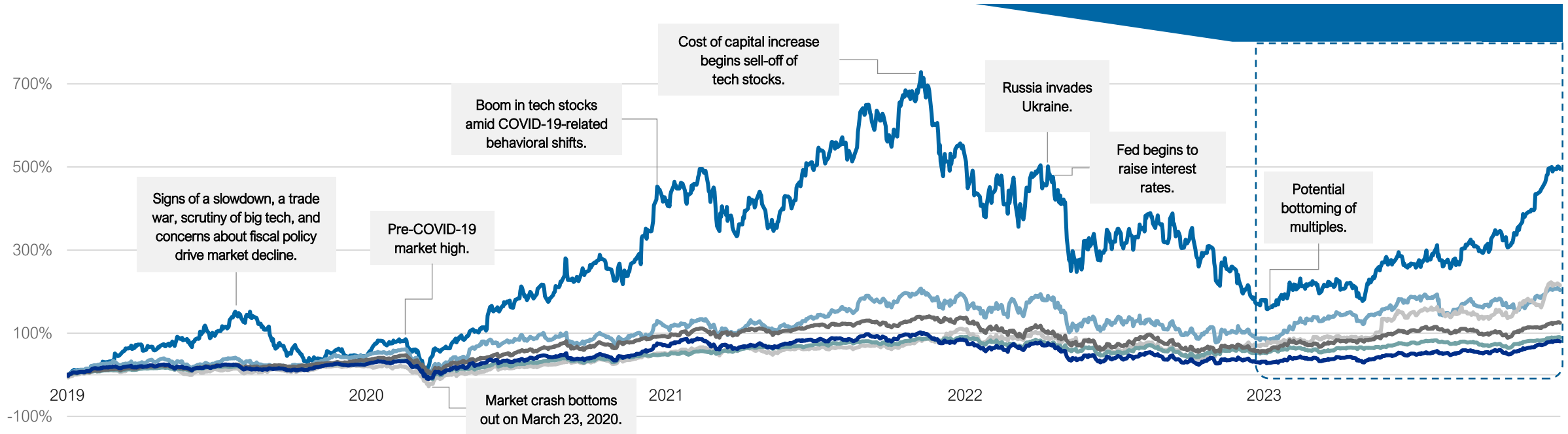
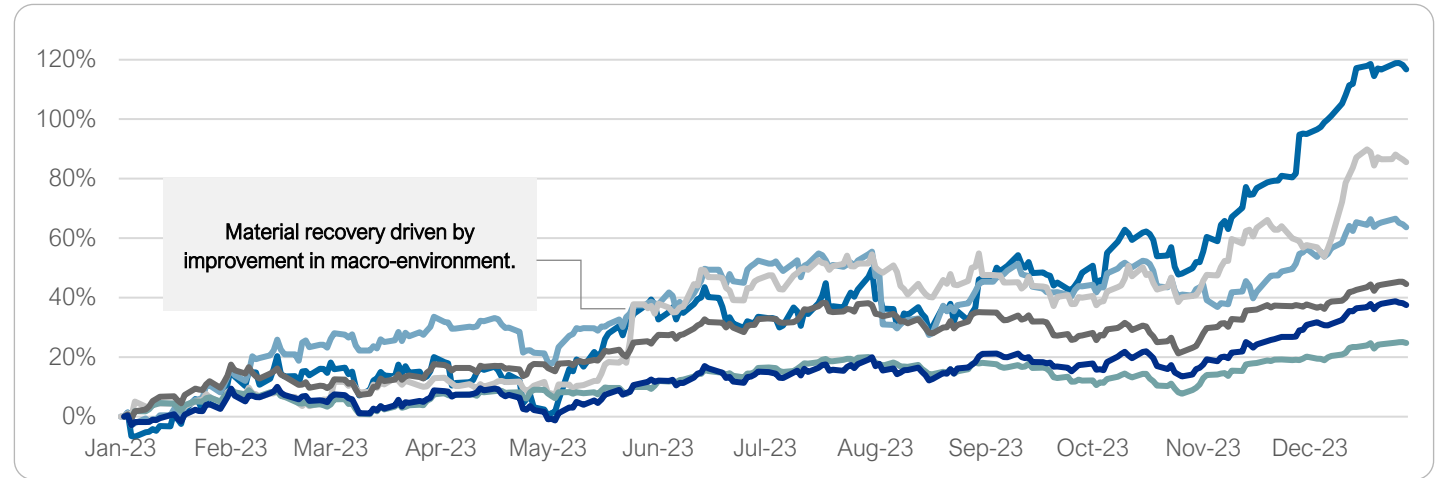
(1) High-growth cybersecurity includes CRWD, ZS, CYBR, DARK, and S.

(2) Medium-growth cybersecurity includes PANW, FTNT, SPLK, OKTA, QYLS, TENB, RPD, MITK, FSECURE, and RSKD.

(3) Low-growth cybersecurity includes AVGO, GEN, OTEX, CHKP, FFIV, 4704, SWI, SCWX, CGNT, OPSN, WITH, and TLS.

Segments of Cybersecurity Posted Strong Quarter and Outpaced Broader Indexes

Index	Q4 '23	LTM
High-Growth Cyber ⁽¹⁾	↗ 43.9%	↗ 116.7%
Medium-Growth Cyber ⁽²⁾	↗ 13.4%	↗ 63.6%
Low-Growth Cyber ⁽³⁾	↗ 32.0%	↗ 85.5%
HACK	↗ 10.6%	↗ 39.2%
S&P 500	↗ 11.2%	↗ 24.7%
Nasdaq	↗ 12.8%	↗ 44.5%



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

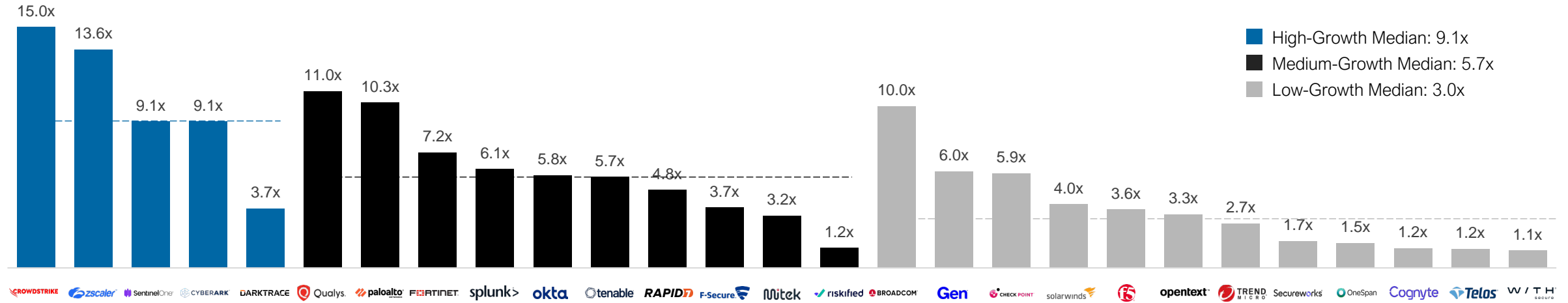
(1) High-growth cybersecurity includes CRWD, ZS, CYBR, DARK, and S.

(2) Medium-growth cybersecurity includes PANW, FTNT, SPLK, OKTA, QYLS, TENB, RPD, MITK, FSECURE, and RSKD.

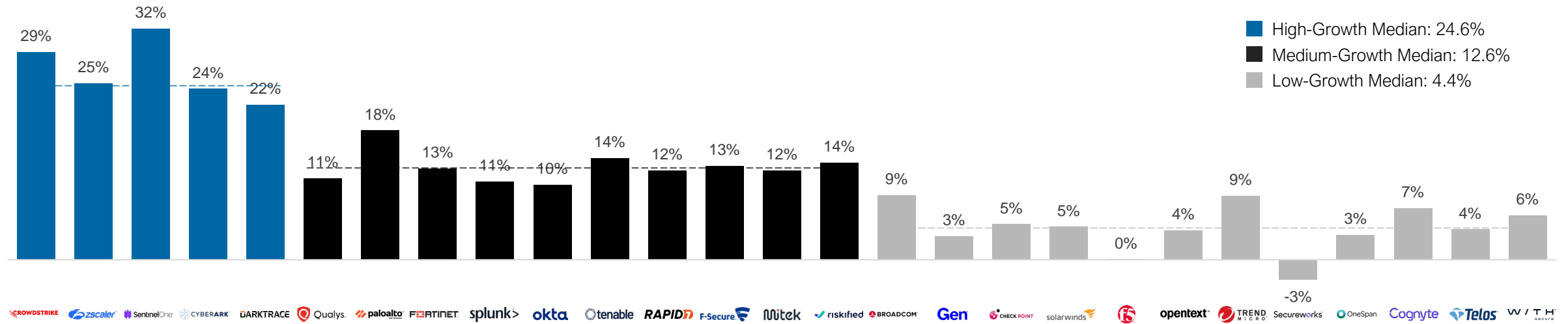
(3) Low-growth cybersecurity includes AVGO, GEN, OTEX, CHKP, FFIV, 4704, SWI, SCWX, CGNT, OPSN, WITH, and TLS.

Public Company Benchmarking: Cybersecurity Software

EV/2024E Revenue



CY 2023A–2024E 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 December 31, 2023. Notes: All financials are calendarized to a December year-end. Sorted by EV/2024E revenue. Broadcom figures has been pro forma adjusted for its acquisition of VMware.

Public Investors Have Begun to Slightly Favor Growth

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

Mean: 4% | 3.9x
Median: 4% | 3.2x

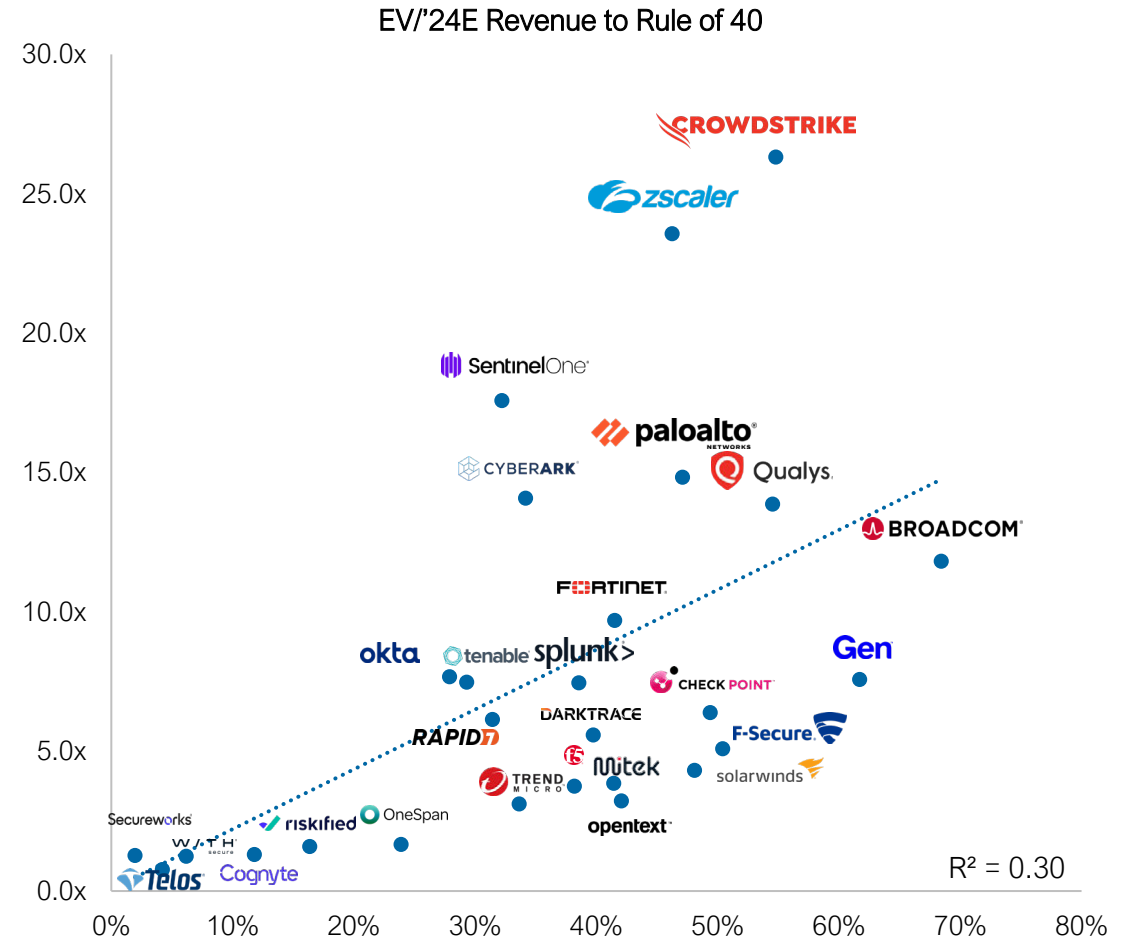
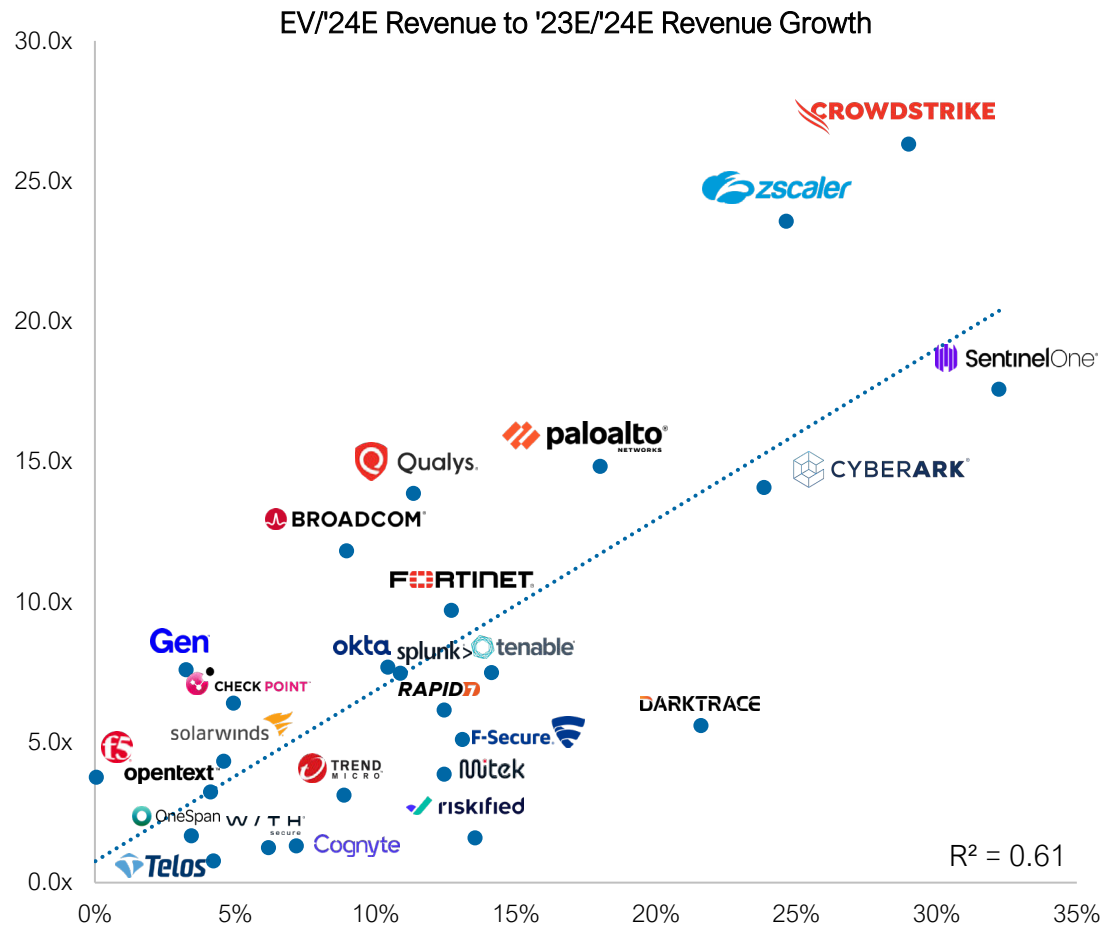
Mean: 13% | 7.8x
Median: 13% | 6.2x

Mean: 26% | 17.4x
Median: 25% | 17.6x

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

Mean: 11% | 5.4x
Median: 10% | 3.8x

Mean: 13% | 10.9x
Median: 12% | 8.6x



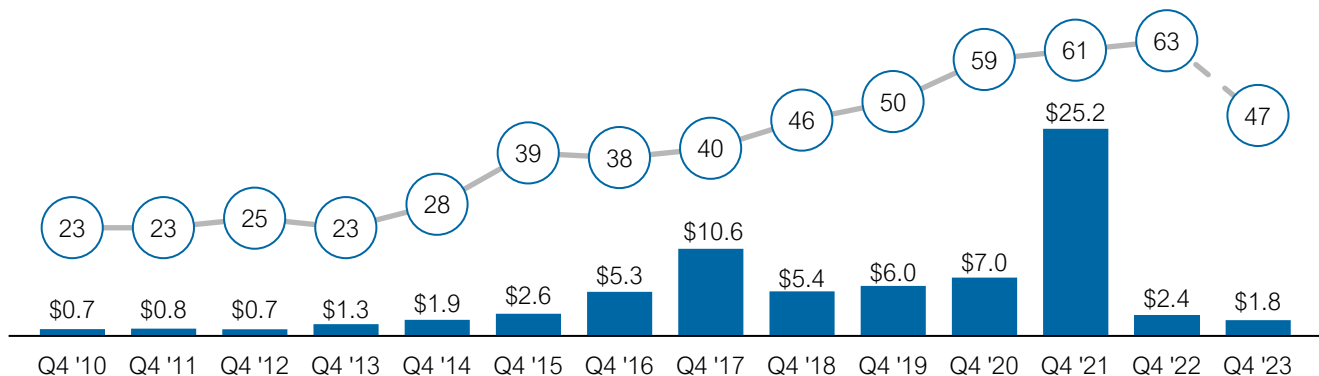
Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of December 31, 2023.
Notes: All financials are calendarized to a December year-end. Companies with negative values for revenue growth are included in the calculation for R² but is not included in the charts.
Broadcom figures has been pro forma adjusted for its acquisition of VMware.

Cybersecurity M&A Activity

Historical Q4 M&A Summary

(\$ in Billions)

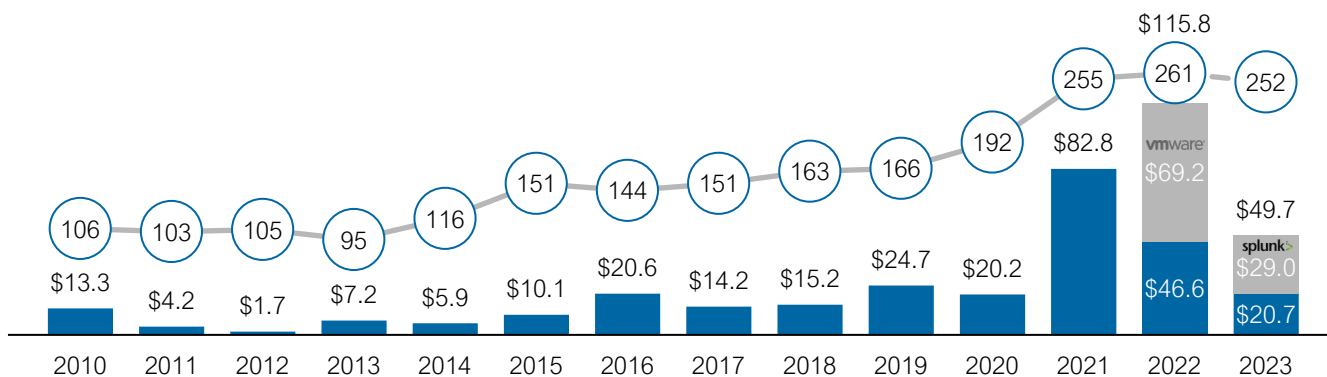
■ Deal Value ○ Deal Count



Annual M&A Summary

(\$ in Billions)

■ Deal Value ○ Deal Count



Selected M&A Transactions

(\$ in Millions)

Ann. Date	Acquirer	Target	EV	EV/Rev
Dec-26	SONICWALL	BANYAN SECURITY	N/A	NA
Dec-21	CISCO	ISOVALENT	\$650	NA
Dec-19	OKTA	Spera	NA	NA
Dec-4	WIZ	raftt	NA	NA
Nov-30	H.I.G. CAPITAL	Mainline INFORMATION SYSTEMS	NA	NA
Nov-9	THRIVE	4it	NA	NA
Nov-6	paloalto NETWORKS	TALON	\$625	NM
Oct-31	paloalto NETWORKS	DIG Security	\$400	NA
Oct-30	proofpoint	TESSIAN	\$300	7.5x
Oct-23	Rockwell Automation	VERVE	\$185	5.8x
Oct-10	ARCTIC WOLF	revelstoke	NA	NA
Oct-2	TheChertoffGroup	Trustwave	\$205	NA

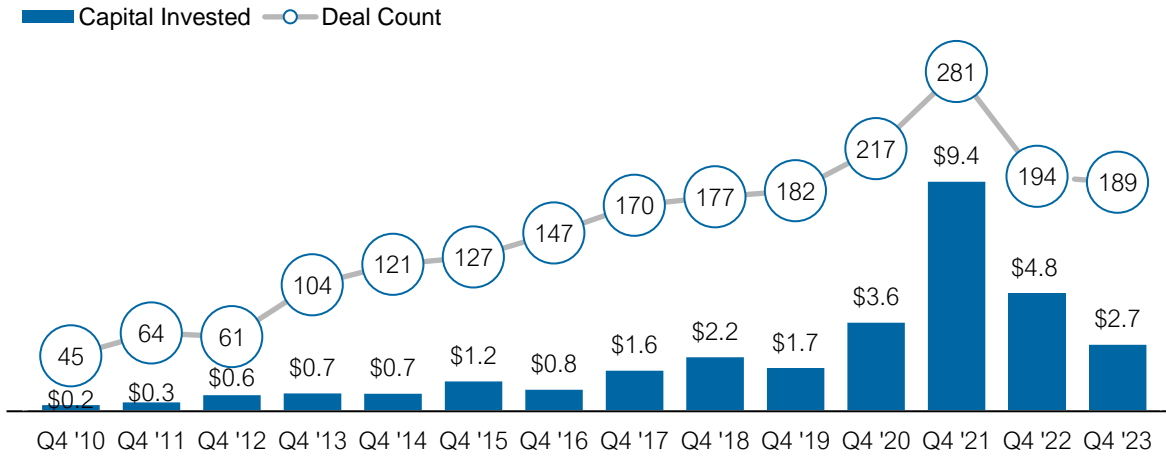
Sources: S&P Capital IQ, PitchBook, 451 Research as of December 31, 2023.

Notes: NA indicates not available; NM indicates not meaningful. 2022 M&A deal volume includes Broadcom's acquisition of VMware. 2023 M&A deal volume includes Cisco's acquisition of Splunk.

Cybersecurity Financing Activity

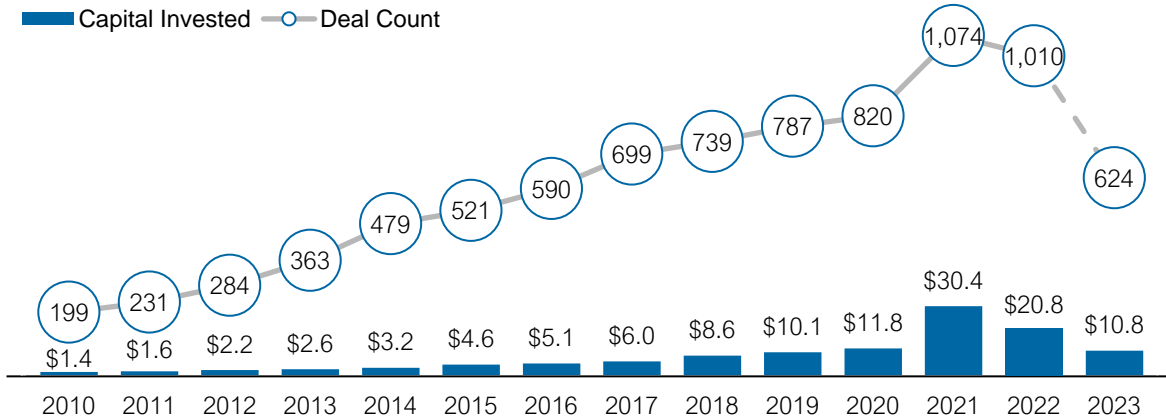
Historical Q4 Financing Summary

(\$ in Billions)



Annual Financing Summary

(\$ in Billions)



Selected Minority Transactions

(\$ in Millions)

Ann. Date	Lead Investor	Target	Amount	Valuation	Total Raised
Dec-19	L2Point	SIMSPACE	\$45	\$150	\$55
Dec-18	BainCapital VENTURES	halcyon	\$40	\$236	\$109
Dec-04	HIGHLAND CAPITAL PARTNERS	ArmorCode	\$40	N/A	\$50
Dec-01	GREENFIELD PARTNERS	torq	\$40	\$172	\$118
Nov-29	ISTARI	BlueVoyant	\$140	N/A	\$726
Nov-21	NEA	SECOND FRONT SYSTEMS	\$40	\$275	\$80
Nov-20	SAPPHIRE VENTURES	BioCatch	\$70	\$1,070	\$302
Nov-01	Amplify SEQUOIA	Chainguard	\$61	\$411	\$116
Oct-24	Decibel	Censys	\$75	\$325	\$131
Oct-23	CANAPI PRYSM CAPITAL	Island	\$100	\$1,500	\$375
Oct-18	INSIGHT PARTNERS	secure W2	\$80	N/A	\$80
Oct-17	CAPITAL ONE VENTURES MassMutual Ventures	Prove	\$44	\$1,334	\$275



Conferences and Events



Houlihan Lokey

Recent Conferences and Events

Conference Highlights



600+

Conference Attendees



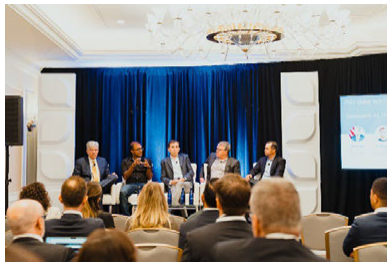
70+

Participating Companies



Targeted

One-on-One Meetings With High-Profile
Capital Providers



Upcoming Conferences and Events

Cybersecurity Focus: Panel Discussions and 1x1 Meetings
GenAI: The Next Frontier in Cybersecurity



Chris Inglis
Former U.S. National Cyber Director



DJ Sampath
Vice President of Product,
AI Cisco Secure



Brendan Hannigan
Co-Founder and CEO



J. Paul Haynes
President and COO

ESENTIRE

Participating Cybersecurity Companies



Selected Conference Attendees





Recent Conferences and Events

WHAT TO EXPECT AT THE EVENT

- **Panel Discussions From CEOs at High-Growth Companies:** A wide range of speakers will share their insights about navigating current market conditions and positioning their companies for future success across a variety of technology sectors.
- **Featured Speakers:** The conference will feature 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 will arrange 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:** Join an audience of strategic, financial, and institutional investors as well as other capital providers for lunch and end-of-day cocktails.

14 March
2024

London | London Hilton on Park Lane

Upcoming Conferences and Events

AGENDA

MARCH 13

Evening Pre-Conference VIP Reception

MARCH 14

CONFERENCE:
Panels and 1x1s



Interested in presenting your company at GTC 2024 in London?
Email GTConference@HL.com.

Recent Conferences and Events

SINET Overview

- The Security Innovation Network (SINET) is dedicated to advancing cybersecurity innovation by fostering collaboration among government, industry, and academia. Its mission is to address cybersecurity challenges through collective efforts.
- SINET organizes networking events, conferences, and workshops to connect cybersecurity professionals, entrepreneurs, and government officials. These platforms serve as opportunities for showcasing and discussing cutting-edge cybersecurity solutions and technologies.
- While originating in the U.S., SINET has a global reach, collaborating with international partners to address cybersecurity challenges worldwide. With an advisory board comprising experts and leaders, SINET guides its activities strategically to promote innovation in the field.

2024 Panel Topics:

Approaches to Building a Secure GenAI Environment

New Naval Strategy

Hidden Supply Chain Risks

SEC Cyber Disclosure

Data Extortion: Ransomware

Innovating Budgets During Austere Times

Enhancing Governance of Risk

How to Achieve the Greatest ROI When Implementing Cybersecurity Technologies

Upcoming Conferences and Events

Selected Keynote Speakers



Antony Abraham
Deputy CSIO
HPE



Abhi Agarwal
Global Head of Cyber
BioMarin Pharmaceutical



Nima Baiati
Executive Director
Lenovo



Rich Baich
CISO
AT&T



Deepali Bhoite
CISO
Anaplan



Tim Brown
CISO
SolarWinds



Cassio Goldschmidt
CISO
ServiceTitan



Swathi Joshi Bhat
VP, Cloud Security
Oracle



Anmol Misra
Director
Autodesk



Rick Patterson
EVP, CISO
CLEAR



Robert Silvers
Head of Security
ChargePoint



Kevin Walker
CSO
Procure

SINET Webinars

January 30

Cyber Enforcement Trends: What They Mean for CISOs and Other Executives in the New Line of Fire

February 6

What the Ransomware Landscape Looks Like for 2024

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.
- The 2024 conference is centered around the theme “The Art of Possible,” underscoring the notion that cybersecurity professionals are akin to artists who rely on their intuition and collaborative efforts to craft solutions that unite us all in the pursuit of a more secure world.

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.



Sandbox

Offers immersive experiences featuring several interactive villages, the RSAC Cybrew Café, and cutting-edge research talks.



Early-Stage Expo

Exhibit space to discover and connect with 50+ rising stars in cybersecurity innovation.



Security Scholar

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



Inclusive Security

Discuss how focus on inclusion has helped organizations improve their security posture.

Upcoming Conferences and Events

Interesting in Meeting Us at RSA?



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



Mark Smith
Director
Cyber Europe
United Kingdom
Mark.Smith@HL.com



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



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

Recent Conferences and Events

- 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.

Black Hat USA 2024



The event includes four days of training and a two-day main conference featuring more than 100 selected Briefings, dozens of open-source tool demos in 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



Carbon Black.



KnowBe4



Upcoming Conferences and Events



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 Certified Pentester.



Black Hat Business Hall

Solution providers and startups showcase the latest technologies and security services.

A hand holding a glowing digital globe with a network of nodes and lines.

IV

About Houlihan Lokey



Houlihan Lokey



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

2,660 Global Employees ⁽¹⁾	36 Locations	\$8.3 Billion Market Cap ⁽¹⁾		\$1.8 Billion Revenue ⁽²⁾	~25% Employee-Owned	No Debt
---	------------------------	---	--	--	-------------------------------	-------------------

Corporate Finance

- No. 1 Global M&A Advisor
- Leading Capital Markets Advisor Raising More Than ~\$14 Billion in the Past Year

Rank	Advisor	Deals
1	Houlihan Lokey	352
2	Rothschild	349
3	Goldman Sachs	300

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

Financial Restructuring

- No. 1 Global Restructuring Advisor
- \$3.5 Trillion of Aggregate Transaction Value Completed

Rank	Advisor	Deals
1	Houlihan Lokey	73
2	PJT Partners	64
3	Rothschild	51

Source: LSEG (formerly Refinitiv).

Financial and Valuation Advisory

- No. 1 Global M&A Fairness Opinion Advisor Over the Past 25 Years
- 2,000+ Annual Valuation Engagements

Rank	Advisor	Deals
1	Houlihan Lokey	1,247
2	JP Morgan	1,035
3	Duff & Phelps, A Kroll Business	977

Source: LSEG (formerly 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	217
2	Lincoln International	156
3	William Blair & Co	112

Source: PitchBook. Excludes accounting firms and brokers.

(1) As of January 31, 2024.
(2) LTM ended December 31, 2023.

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

2023 M&A Advisory Rankings
All Global Technology Transactions

Advisor	Deals
1 Houlihan Lokey	89
2 Rothschild & Co	76
3 JP Morgan	68
4 Goldman Sachs & Co	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 Inc	31
3 Lincoln International	25
4 Raymond James Financial Inc	24
5 Generational Equity	20

Source: LSEG (formerly Refinitiv).

No. 1
TECH M&A
ADVISOR*

15
LOCATIONS
WORLDWIDE

235+
TECHNOLOGY
FINANCIAL
PROFESSIONALS

40+
MANAGING
DIRECTORS
















































116
TECHNOLOGY
DEALS IN CY23



<p>AMERICAS</p> <ul style="list-style-type: none"> Atlanta Baltimore Boston Charlotte Chicago Dallas Houston 	<ul style="list-style-type: none"> Los Angeles Miami Minneapolis New York San Francisco São Paulo Washington, D.C. 	<p>EUROPE AND MIDDLE EAST</p> <ul style="list-style-type: none"> Amsterdam Antwerp Dubai Frankfurt London Madrid Manchester Milan Munich Paris Stockholm Tel Aviv Zurich 	<p>ASIA-PACIFIC</p> <ul style="list-style-type: none"> Beijing Fukuoka Gurugram Hong Kong SAR Mumbai Shanghai Singapore Sydney Tokyo
---	---	---	---

Local Technology Team

Deep Cybersecurity Experience Across the Ecosystem

 <p>has been acquired by</p>  <p>Sellside Advisor</p>	 <p>has been acquired by</p>  <p>Sellside Advisor</p>	<p>CARLYLE</p> <p>has acquired a majority stake in</p> <p>NEVERHACK</p> <p>formerly known as</p>  <p>a portfolio company of</p> <p>IK Partners</p> <p>Buyside Advisor</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 acquired a majority stake in</p>  <p>Buyside Advisor*</p>	 <p>has been acquired by</p>  <p>Sellside Advisor*</p>	 <p>has invested in</p>  <p>Financing 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>Threema.</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>

Tombstones included herein represent transactions closed from 2010 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

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 1,700 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.

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 Global and U.S. Under \$1B 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: LSEG (formerly Refinitiv).
*Excludes accounting firms and brokers.

Other Houlihan Lokey Cyber Sector Reports

Generative AI in Cybersecurity Report



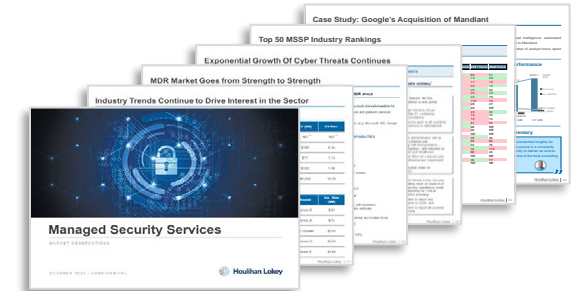
European Cybersecurity Ideabook



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
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



Joseph Miller
Associate
San Francisco
JJMiller@HL.com



Patrick Wong
Financial Analyst
San Francisco
Patrick.Wong@HL.com

Global Cyber Reach



Mark Smith
Director
Cyber Europe
United Kingdom
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
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

Cybersecurity Technology Expertise



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



Edouard Viot
Cybersecurity Consultant
Paris

Yearly Conferences










V

Appendix



High-Growth Cybersecurity Trading Metrics



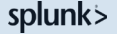







(\$ in Millions, Except Price per Share)

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 2023E	CY 2024E	CY 2025E	CY 2023E	CY 2024E	CY 2025E
 CROWDSTRIKE	\$255.32	\$261.81	97.5%	147.2%	\$3,166	\$60,589	\$58,974	19.3x	15.0x	11.9x	NM	NM	43.5x
 ZSCALER	221.56	227.29	97.5%	101.1%	2,324	32,588	31,765	16.9x	13.6x	10.9x	NM	NM	47.1x
 CYBERARK	219.05	222.51	98.4%	73.4%	993	9,125	8,331	11.3x	9.1x	7.4x	NM	NM	43.7x
 DARKTRACE	4.67	5.45	85.7%	46.5%	359	3,166	2,705	4.5x	3.7x	3.1x	20.5x	20.3x	14.9x
 SENTINELONE	27.44	27.97	98.1%	88.3%	798	7,970	7,421	12.0x	9.1x	7.0x	NM	NM	NM

Top Quartile	\$32,588	\$31,765	16.9x	13.6x	10.9x	20.5x	20.3x	44.5x
Mean	\$22,688	\$21,839	12.8x	10.1x	8.1x	20.5x	20.3x	37.3x
Median	\$9,125	\$8,331	12.0x	9.1x	7.4x	20.5x	20.3x	43.6x
First Quartile	\$7,970	\$7,421	11.3x	9.1x	7.0x	20.5x	20.3x	36.4x

Medium-Growth Cybersecurity Trading Metrics







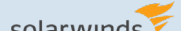





(\$ in Millions, Except Price per Share)

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 2023E	CY 2024E	CY 2025E	CY 2023E	CY 2024E	CY 2025E
 paloalto	\$294.88	\$318.00	92.7%	113.0%	\$3,894	\$103,695	\$91,304	12.1x	10.3x	8.7x	40.3x	35.3x	29.6x
 FORTINET	58.53	81.24	72.0%	20.6%	2,440	46,133	42,833	8.1x	7.2x	6.2x	27.5x	24.9x	20.2x
 splunk>	152.35	152.77	99.7%	75.5%	1,690	26,717	27,249	6.8x	6.1x	5.4x	25.5x	22.2x	18.6x
 okta	90.53	92.38	98.0%	30.2%	2,130	14,814	14,260	6.4x	5.8x	5.1x	49.1x	33.0x	26.7x
 Qualys	196.28	206.35	95.1%	76.0%	426	7,381	6,791	12.2x	11.0x	9.9x	26.9x	25.5x	22.6x
 tenable	46.06	49.77	92.5%	21.5%	474	5,316	5,111	6.5x	5.7x	5.0x	43.0x	37.3x	29.0x
 RAPID7	57.10	60.15	94.9%	63.3%	383	3,469	4,209	5.4x	4.8x	4.3x	34.6x	25.5x	23.1x
 Mitek	13.04	13.98	93.3%	34.3%	128	601	606	3.6x	3.2x	NA	16.1x	11.2x	NA
 F-Secure	2.25	3.80	59.2%	(24.2%)	18	387	605	4.2x	3.7x	3.6x	13.0x	10.0x	9.2x
 riskified	4.68	6.73	69.5%	1.5%	450	816	415	1.4x	1.2x	1.1x	NM	43.6x	18.0x

Top Quartile	\$23,741	\$24,002	7.8x	6.9x	6.2x	40.3x	34.7x	26.7x
Mean	\$20,933	\$19,338	6.7x	5.9x	5.5x	30.7x	26.8x	21.9x
Median	\$6,348	\$5,951	6.4x	5.7x	5.1x	27.5x	25.5x	22.6x
First Quartile	\$1,480	\$1,507	4.5x	4.0x	4.3x	25.5x	22.8x	18.6x

Low-Growth Cybersecurity Trading Metrics



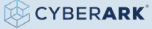


(\$ in Millions, Except Price per Share)

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 2023E	CY 2024E	CY 2025E	CY 2023E	CY 2024E	CY 2025E
 BROADCOM	\$1,116.25	\$1,151.82	96.9%	101.7%	\$14,189	\$476,639	\$548,021	10.9x	10.0x	9.2x	19.2x	16.9x	15.1x
 Gen	22.82	23.74	96.1%	5.6%	490	14,702	23,550	6.2x	6.0x	5.8x	10.6x	10.3x	9.5x
 opentext	42.02	43.25	97.2%	41.8%	1,103	11,408	19,599	3.5x	3.3x	3.4x	10.5x	8.8x	9.1x
 CHECK POINT	152.79	154.12	99.1%	20.5%	1,530	18,075	14,887	6.2x	5.9x	5.6x	13.6x	13.2x	12.5x
 TREND MICRO	178.98	180.70	99.0%	23.6%	826	10,754	10,164	3.6x	3.6x	3.5x	10.1x	9.5x	NA
 solarwinds	53.55	59.90	89.4%	14.1%	2,121	7,331	5,285	3.0x	2.7x	2.6x	12.6x	11.1x	9.9x
 Securworks	12.49	12.55	99.6%	32.6%	289	2,056	3,107	4.1x	4.0x	3.7x	9.6x	9.1x	8.8x
 Cognyte	7.38	10.06	73.4%	17.5%	58	632	588	1.6x	1.7x	1.6x	NM	35.1x	NA
 OneSpan	6.43	6.94	92.7%	101.6%	69	465	407	1.3x	1.2x	1.1x	49.0x	26.3x	9.9x
 W / T H secure	10.72	19.25	55.7%	(7.6%)	68	436	364	1.6x	1.5x	1.5x	NM	7.5x	5.6x
 Telos	1.15	1.92	59.7%	(21.6%)	40	201	178	1.1x	1.1x	1.0x	NM	NM	19.7x
 Telos	3.65	5.36	68.1%	(29.7%)	100	250	166	1.2x	1.2x	1.0x	NM	NM	27.3x
Top Quartile						\$12,231	\$16,065	4.6x	4.4x	4.2x	15.0x	16.0x	14.4x
Mean						\$45,246	\$52,193	3.7x	3.5x	3.3x	16.9x	14.8x	12.7x
Median						\$4,694	\$4,196	3.2x	3.0x	3.0x	11.6x	10.7x	9.9x
First Quartile						\$458	\$396	1.5x	1.5x	1.4x	10.4x	9.2x	9.2x

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of December 31, 2023. Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Sorted by Enterprise Value. Growth categorizations are based on 2023E-2024E revenue growth breakpoints; high-growth ≥ 20%, medium-growth >10% and <20%, low-growth ≤ 10%. Broadcom figures has been pro forma adjusted for its acquisition of VMware.

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 2023E	CY 2024E	CY 2025E	CY 2023E	CY 2024E	CY 2025E	2022A–2023E	2023–2024E	2024–2025E	CY 2023E	CY 2024E	CY 2025E
 CROWDSTRIKE	\$255.32	\$60,589	\$58,974	\$3,050	\$3,934	\$4,939	\$772	\$1,015	\$1,355	36.1%	29.0%	25.5%	25.3%	25.8%	27.4%
 ZSCALER	221.56	32,588	31,765	1,877	2,340	2,914	389	506	675	39.2%	24.6%	24.6%	20.7%	21.6%	23.1%
 CYBERARK	219.05	9,125	8,331	739	915	1,123	41	94	191	24.9%	23.9%	22.7%	5.6%	10.3%	17.0%
 DARKTRACE	4.67	3,166	2,705	605	736	878	132	134	181	25.1%	21.6%	19.3%	21.8%	18.1%	20.7%
 SENTINELONE	27.44	7,970	7,421	616	815	1,062	(124)	(7)	93	46.0%	32.2%	30.4%	NM	NM	8.8%

Top Quartile	\$32,588	\$31,765	\$1,877	\$2,340	\$2,914	\$389	\$506	\$675	39.2%	29.0%	25.5%	22.7%	22.7%	23.1%
Mean	\$22,688	\$21,839	\$1,377	\$1,748	\$2,183	\$242	\$348	\$499	34.3%	26.3%	24.5%	18.4%	19.0%	19.4%
Median	\$9,125	\$8,331	\$739	\$915	\$1,123	\$132	\$134	\$191	36.1%	24.6%	24.6%	21.3%	19.9%	20.7%
First Quartile	\$7,970	\$7,421	\$616	\$815	\$1,062	\$41	\$94	\$181	25.1%	23.9%	22.7%	16.9%	16.2%	17.0%

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 2023E	CY 2024E	CY 2025E	CY 2023E	CY 2024E	CY 2025E	2022A–2023E	2023–2024E	2024–2025E	CY 2023E	CY 2024E	CY 2025E
paloalto	\$294.88	\$103,695	\$91,304	\$7,523	\$8,879	\$10,462	\$2,268	\$2,584	\$3,087	22.2%	18.0%	17.8%	30.1%	29.1%	29.5%
FORTINET	58.53	46,133	42,833	5,301	5,974	6,934	1,558	1,721	2,122	20.0%	12.7%	16.1%	29.4%	28.8%	30.6%
splunk>	152.35	26,717	27,249	4,006	4,443	5,077	1,070	1,229	1,463	9.6%	10.9%	14.3%	26.7%	27.7%	28.8%
okta	90.53	14,814	14,260	2,244	2,479	2,818	290	433	534	20.8%	10.4%	13.7%	12.9%	17.5%	19.0%
Qualys	196.28	7,381	6,791	555	618	689	253	267	300	13.3%	11.4%	11.5%	45.6%	43.2%	43.6%
tenable	46.06	5,316	5,111	792	904	1,032	119	137	176	15.9%	14.1%	14.2%	15.0%	15.2%	17.1%
RAPID7	57.10	3,469	4,209	774	870	984	122	165	183	12.9%	12.5%	13.1%	15.7%	19.0%	18.5%
Nitek	13.04	601	606	167	188	NA	38	54	NA	6.1%	12.5%	NA	22.6%	29.0%	NA
F-Secure	2.25	387	605	143	162	168	47	60	66	20.6%	13.1%	4.1%	32.6%	37.3%	39.1%
riskified	4.68	816	415	298	338	391	(14)	10	23	14.0%	13.6%	15.6%	NM	2.8%	5.9%

Top Quartile	\$23,741	\$24,002	\$3,566	\$3,952	\$5,077	\$875	\$1,030	\$1,463	20.4%	13.4%	15.6%	30.1%	29.1%	30.6%
Mean	\$20,933	\$19,338	\$2,180	\$2,485	\$3,173	\$575	\$666	\$884	15.5%	12.9%	13.4%	25.6%	25.0%	25.8%
Median	\$6,348	\$5,951	\$783	\$887	\$1,032	\$187	\$216	\$300	15.0%	12.6%	14.2%	26.7%	28.2%	28.8%
First Quartile	\$1,480	\$1,507	\$362	\$408	\$689	\$65	\$80	\$176	13.0%	11.6%	13.1%	15.7%	17.8%	18.5%

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 2023E	CY 2024E	CY 2025E	CY 2023E	CY 2024E	CY 2025E	2022A–2023E	2023–2024E	2024–2025E	CY 2023E	CY 2024E	CY 2025E
BROADCOM	\$1,116.25	\$476,639	\$548,021	\$50,069	\$54,562	\$59,835	\$28,562	\$32,451	\$36,394	8.0%	9.0%	9.7%	57.0%	59.5%	60.8%
Gen	22.82	14,702	23,550	3,797	3,920	4,063	2,231	2,292	2,474	22.2%	3.3%	3.6%	58.8%	58.5%	60.9%
opentext	42.02	11,408	19,599	5,651	5,884	5,772	1,870	2,233	2,156	(7.0%)	4.1%	NM	33.1%	37.9%	37.4%
CHECK POINT	152.79	18,075	14,887	2,414	2,533	2,655	1,093	1,126	1,191	3.6%	4.9%	4.8%	45.3%	44.5%	44.9%
F5	178.98	10,754	10,164	2,798	2,800	2,934	1,006	1,068	0	3.3%	0.1%	4.8%	36.0%	38.1%	NM
TREND MICRO	53.55	7,331	5,285	1,770	1,927	2,068	420	477	532	4.3%	8.9%	7.4%	23.7%	24.8%	25.7%
solarwinds	12.49	2,056	3,107	751	785	833	323	342	353	4.4%	4.6%	6.1%	43.0%	43.5%	42.4%
Secureworks	7.38	632	588	364	354	365	(30)	17	0	(21.5%)	(2.8%)	3.1%	NM	4.7%	NM
Cognyte	6.43	465	407	311	333	362	8	15	41	(0.3%)	7.2%	8.7%	2.7%	4.6%	11.3%
OneSpan	10.72	436	364	230	238	250	3	49	66	4.9%	3.4%	5.2%	1.5%	20.5%	26.2%
W / T H secure	1.15	201	178	157	167	177	(24)	(0)	9	9.2%	6.2%	5.8%	NM	NM	5.1%
Telos	3.65	250	166	136	142	171	(8)	(6)	6	(37.1%)	4.2%	20.0%	NM	NM	3.6%

Top Quartile	\$12,231	\$16,065	\$3,048	\$3,080	\$3,216	\$1,287	\$1,403	\$1,433	5.7%	6.4%	8.0%	45.3%	44.2%	44.3%
Mean	\$45,246	\$52,193	\$5,704	\$6,137	\$6,624	\$2,955	\$3,339	\$3,602	(0.5%)	4.4%	7.2%	33.5%	33.7%	31.8%
Median	\$4,694	\$4,196	\$1,260	\$1,356	\$1,451	\$371	\$409	\$209	3.9%	4.4%	5.8%	36.0%	38.0%	31.8%
First Quartile	\$458	\$396	\$291	\$310	\$334	\$1	\$16	\$8	(2.0%)	3.4%	4.8%	23.7%	21.5%	14.9%

Source: Trading multiples are based on share price, other market data, and broker consensus future earnings estimates from S&P Capital IQ as of December 31, 2023. Notes: All financials are calendarized to a December year-end. NM indicates not meaningful, not disclosed, or EV/EBITDA >30x or <0x. Sorted by Enterprise Value. Growth categorizations are based on 2023E–2024E revenue growth breakpoints; high-growth ≥ 20%, medium-growth > 10% and < 20%, low-growth ≤ 10%. Broadcom revenue and EBITDA figures has been pro forma adjusted for its acquisition of VMware.

Disclaimer

© 2024 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 Advisors 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.asic.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. No entity affiliated with Houlihan Lokey, Inc., provides banking or securities brokerage services and is not subject to FINMA supervision in Switzerland or similar regulatory authorities 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