Q4 2025 Cybersecurity Commentary

Executive Summary and Performance Commentary

Cybersecurity companies delivered negative price performance in Q4 2025, with the Nasdaq ISE Cyber Security Select™ Index (HXRXL™) down 7.5% for the quarter, underperforming the S&P 500 (+2.4%). Of the 23 constituents, only 4 names had gains, with 2 names experiencing double-digit gains including top performers Fastly (+19.1%) and Cisco Systems (+12.6%). 19 names experienced losses, with 8 names down more than 10% apiece, including the worst performer, Varonis Systems (-42.9%), followed by Zscaler (-24.9%), Trend Micro (-24.2%) and F5 (-21%)[1].

Investors continue to lack meaningful exposure to cybersecurity in their core portfolios. The S&P 500 currently tracks only 9 constituents that overlap with HXRXL, comprising <5% of its exposure. 14 of HXRXL's constituents (~48.3% of index weight) do not overlap with the S&P 500. The sector's relatively stable demand profile and lower-than-average thematic index volatility contribute to dynamics more closely resembling that of a "digital utility". It has not only evolved into an evergreen, defensive thematic strategy in recent years, but has also become strongly associated with the broader AI trade, increasingly impacted on both the demand and supply side.

Key Cybersecurity News Items

On November 5, the University of Pennsylvania confirmed that data had been stolen in a cyberattack. The attacker hacked an employee's PennKey SSO account that provided access to the university's Salesforce instance, Qlik analytics platform, SAP business intelligence system, and SharePoint files. In a post on a hacking forum, the attackers stated they are not currently leaking the data records but may do so within a month or two.

On October 27, Swedish state-owned power grid operator Svenska kraftnät confirmed that a data breach occurred following a cyberattack. The attack did not affect the country's power supply. The data breach was disclosed after the Everest ransomware group added Svenska to its Tor-based leak site and claimed to have stolen 280 GB of data.
See pages 5-7 for a full run down of major ransomware attacks and data breaches

Following a government shutdown in November, Congress extended the critical cyber threat info-sharing laws through the end of the 2026 fiscal year.

In September 2025, the Department of Defense (DOD) finalized rules for the Cybersecurity Maturity Model Certification (CMMC) program, moving it into the Defense Federal Acquisition Regulation Supplement (DFARS). This requires contractors to demonstrate compliance with specific cybersecurity standards to win DOD contracts.
See page 8 for a discussion of the industry outlook and other noteworthy regulatory/policy developments globally

Nasdaq Cybersecurity Thought Leadership

With the focus on continued trade negotiations and retaliatory measures in the fourth quarter, our research highlights how cybersecurity companies are navigating supply chain and trade policy risks.

Quarterly Earnings Recap

Overall, HXRXL companies that beat revenue and earnings estimates in the most recent quarter did so by an average of 2.3% and 12.3% respectively, while those that missed did so by 2.8% and 17.4% respectively. 91.1% of the index weight beat top-line estimates while 96.4% beat bottom-line estimates. In aggregate, HXRXL companies grew revenues 3.0% year-over-year. Aggregate net income surged by 26.3% year-over-year.

	Beats		Misses	
	No. of Firms/Index Weight	Average Beat (%)	No. of Firms/Index Weight	Average Miss (%)
Q4 2025 Revenues	21/91.1%	2.3%	2/8.9%	-2.8%
Q4 2025 Earnings	22/96.4%	12.3%	1/3.6%	-17.4%

Source: Nasdaq Global Indexes, FactSet data as of December, 2025

Index Additions & Deletions (December 22, 2025)

CyberArk Software, a leader in Privileged Access Management solutions (PAM), was deleted from the index at a weight of 4.4%, due to its pending acquisition by Palo Alto Networks.

New Cybersecurity Products Announced in Q4 2025 (AI-related in Bold)

- In November 2025, Cisco (NASDAQ: CSCO) introduced foundational multi-customer management capabilities within Cisco security cloud control, purpose-built for managed service providers (MSPs). The innovation streamlines operations, reduces costs, and accelerates time-to-value for MSPs to deliver advanced managed security services.[2]
- In November 2025, Broadcom (NASDAQ: AVGO) introduced Brocade X8 Directors and Brocade G820 56-port switch, the industry's first 128G Fiber Channel platforms designed for mission-critical workloads and enterprise AI applications. Brocade Gen 8 Fiber Channel safeguards storage for the quantum era and automates infrastructure management through embedded SAN AI technology.[3]
- In November 2025, Fortinet (NASDAQ: FTNT) rolled out a secure AI data center solution, an end-to-end framework purpose-built to protect AI infrastructures. It is designed to secure the full AI stack from data center infrastructure to applications and large language models. The solution claims to deliver advanced AI threat defenses with ultra-low latency and reduce power consumption on average by 69% compared to traditional approaches.[4]
- In October 2025, Palo Alto Networks (NASDAQ: PANW) launched Cortex AgentiX, a secure platform to build, deploy and govern the AI agent workforce. The product claims to deliver up to a 98% reduction in mean time to repair with 75% less manual work.[5]

- In November 2025, Gen Digital (NASDAQ: GEN) launched Scam Guardian and Scam Guardian Pro for mobile devices. Building on the desktop product, this mobile expansion brings AI-powered scam protection directly to people's smartphones and tablets.[6]

Cybersecurity M&A and IPO Activity in Q4 2025

Inside HXRXL Index Activity

- On November 19, Palo Alto Networks (Nasdaq: PANW) announced that it agreed to acquire observability platform provider Chronosphere in a deal valued at $3.35 billion, to be paid in cash and replacement equity awards. Chronosphere's platform enables teams to "zero in on the data that's most useful" and provides insights into every layer of their stack - infrastructure, applications and business. Chronosphere reported annual recurring revenue (ARR) of more than $160 million as of the end of September 2025.[7]

Outside HXRXL Index Activity

- On December 2, ServiceNow (NYSE: NOW) announced an agreement to acquire identity security company Veza Security. The terms of the deal are undisclosed, though reports indicated negotiations valued the company at over $1 billion. Veza has developed an identity security platform that provides non-human identity management, SaaS access security, identity security posture management, privileged access monitoring, data system access, governance and administration, and cloud access management capabilities.[8]
- On October 21, real-time event and risk detection solutions provider Dataminr announced plans to acquire threat intelligence firm ThreatConnect for $290 million in cash and equity. ThreatConnect provides a platform designed to help security teams aggregate, analyze and act on cyber threat intelligence. The acquisition will help combine Dataminr's data signals platform with ThreatConnect's deep internal data capabilities to create agentic AI-powered intelligence that is tailored to the needs of each customer.[9]
- On October 21, data portability and resilience solutions provider Veeam Software announced plans to acquire data security posture management (DSPM) company Securiti AI for $1.725 billion in cash and stock. Securiti AI provides data security and governance solutions, helping organizations comply with global privacy regulations, automate data security, and manage risks across multi-cloud and decentralized data environments. The acquisition will enable Veeam to eliminate the challenge of managing fragmented data across apps, clouds, SaaS, endpoints, and backups.[10]

Top 3 Index Performance Contributors in Q4 2025

Fastly[11,12,13,14]

- The stock was up 19% from September 30, 2025 - December 31, 2025.
- The stock rose on the heels of a good quarter with top-line and bottom-line beating analyst consensus estimates. The company provided positive Q4 guidance which lifted investor sentiment.

- Fiscal Q3 2025 revenue increased by 15.3% y/y to $158.2 million driven by cross-selling, new customer acquisition and upselling with existing network services customers. Net loss was $29.5 million vs. a loss of $38.0 million in Q3 2024. On a q-o-q basis, revenue increased by 6.4%.
- Q4 2025 revenue guidance is in the range of $159-$163 million. Non-GAAP EBIT is expected to be in the range of $8-$12 million. Non-GAAP EPS is expected to be in the range of $0.04-$0.08.

Cisco Systems[15,16,17]

- The stock price was up 13% from September 30, 2025 - December 31, 2025.
- The company reported strong Q1 results driven by AI demand.
- AI infrastructure orders from hyperscaler customers totaled $1.3 billion in Q1, with the business expected to contribute ~$3 billion to the topline in FY 2026. Cisco had $200 million of AI orders from neocloud, sovereign and enterprise customers in Q1 2026, with this category of customers expected to add upwards of $2 billion to FY 2026 revenue.
- Fiscal Q1 2026 revenue grew by 7.5% y/y to $14.9 billion. Net income increased by 5.5% y/y to $2.9 billion while net margins decreased to 19.2% vs. 19.6% in Q1 2025. On a q-o-q basis, revenue increased by 1.4%.
- Fiscal Q2 2026 total revenues are expected to be in the range of $15.0-$15.2 billion. GAAP EPS is expected to be in the range of $0.69-$0.74.

Broadcom[18,19,20]

- The stock was up 5% from September 30, 2025 - December 31, 2025.
- The custom accelerator (XPUs) business more than doubled year-over-year as customers increased adoption of XPUs in training their LLMs and monetizing their platforms through inferencing APIs and applications. In October, OpenAI and Broadcom announced a collaboration for 10 gigawatts of custom AI accelerators. Of Broadcom's consolidated backlog of $162 billion, the company expects $73 billion in AI data centers to be delivered over the next 18 months.
- The Q4 revenue growth momentum is expected to continue in Q1 2026 and AI semiconductor revenue is expected to double y/y to $8.2 billion, driven by custom AI accelerators and Ethernet AI switches.
- Fiscal Q4 2025 revenue grew by 28.2% y/y to $18.0 billion driven primarily by AI semiconductor revenue. An income tax benefit of $1.6 billion boosted net income by 102.6% y/y to $8.5 billion while net margins increased to 47.3% vs. 29.9% in Q4 2024.
- Fiscal Q1 2026 total revenues are expected to be $19.1 billion. Adjusted EBITDA is expected to be 67% of guided revenue. Non-AI semiconductor revenue is expected to be approximately $4.1 billion, flat y/y.

Bottom 3 Index Performance Contributors in Q4 2025

Varonis Systems[21,22,23,24]

- The stock was down 43% from September 30, 2025 - December 31, 2025.
- Investors were disappointed with Q3 results with top-line and bottom-line missing consensus estimates and Q4 2025 guidance coming in below expectations. FY 2025 ARR guidance of $730.0-$738.0 million was reduced to account for the underperformance and weaker than expected renewals in the Federal and non-Federal on-prem subscription business.
- Fiscal Q3 2025 revenue grew by 9.1% y/y to $161.6 million. Net loss was $30.0 million vs. a loss of $18.3 million in Q3 2024. On a q-o-q basis, revenue increased by 6.2%.
- The majority of the decline in revenue was driven by customers converting to SaaS platform. SaaS revenues were $125.8 million vs. $57.8 million in Q3 2024.
- Q4 2025 revenue is expected to be in the range of $165-$171 million. Non-GAAP diluted EPS is expected to be in the range of $0.02-$0.04.

Zscaler[25,26]

- The stock was down 25% from September 30, 2025 - December 31, 2025.
- The stock has been down since the beginning of November and fell further as Q1 results disappointed investor expectations.
- The three growth pillars, Zero Trust Everywhere, AI security, and data security, are accelerating and exceeding internal expectations. The competitive landscape remains stable; brand strength has increased, with minimal impact from new firewall entrants.
- Fiscal Q1 2026 revenue grew by 25.5% y/y to $788.1 million. Net loss was $11.6 million vs. a loss of $12.1 million in Q1 2025. On a q-o-q basis, revenue increased by 9.6%.
- Fiscal Q2 2026 revenue is expected to be in the range of $797-$799 million. Guided non-GAAP diluted EPS is expected to be in the range of $0.89-$0.90.

Trend Micro[27,28, 29]

- The stock was down 24.3% from September 30, 2025 - December 31, 2025.
- The stock came under pressure due to investor concerns regarding modest revenue growth and macroeconomic factors. Specifically, net sales increased only by 1% year-over-year in Q3 2025, although profitability was strong.
- Ongoing economic uncertainty, currency headwinds and challenges in government procurement in certain regions weakened sales.
- The company's shift from a traditional perpetual license model to its "Vision One" platform has created some uncertainty with revenue recognition.

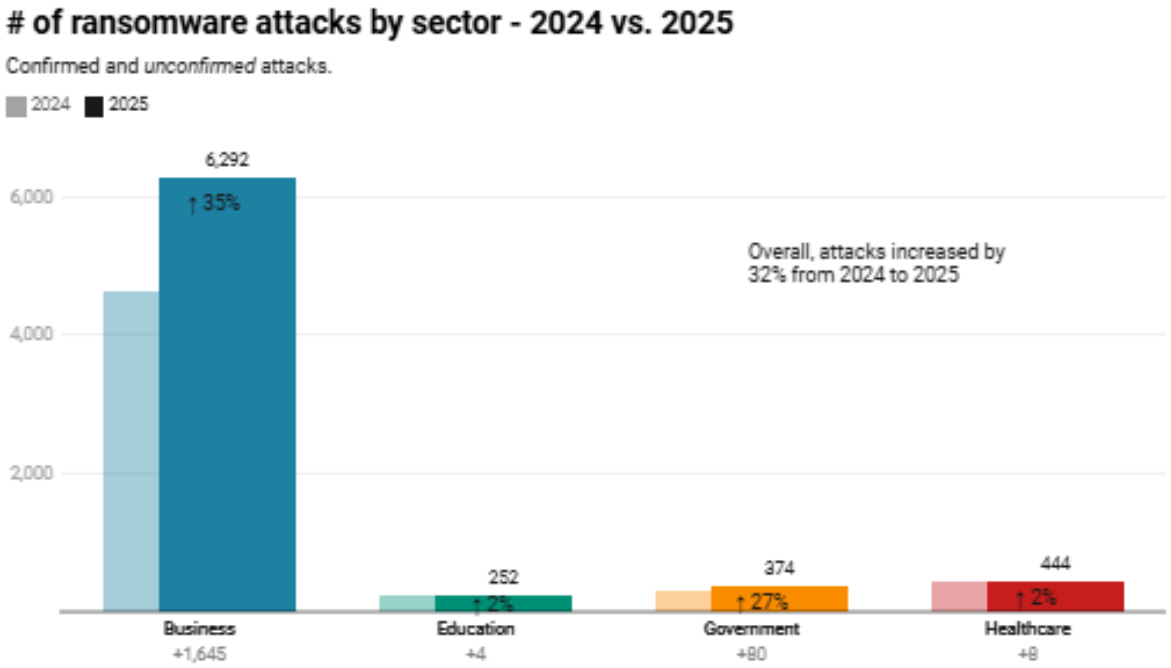
- Fiscal Q3 2025 revenue came in at ¥68.84 billion (approx. $466M), slightly above consensus of ¥68.47B expected) and net income came in at ¥12.61 billion (approx. $85M) significantly higher than the estimated ¥10.7 billion.
- The company guided revenue for the full year to be ¥274 billion (approx. $1.86B USD) and net income to be ¥30.2 billion (approx. $205M USD).

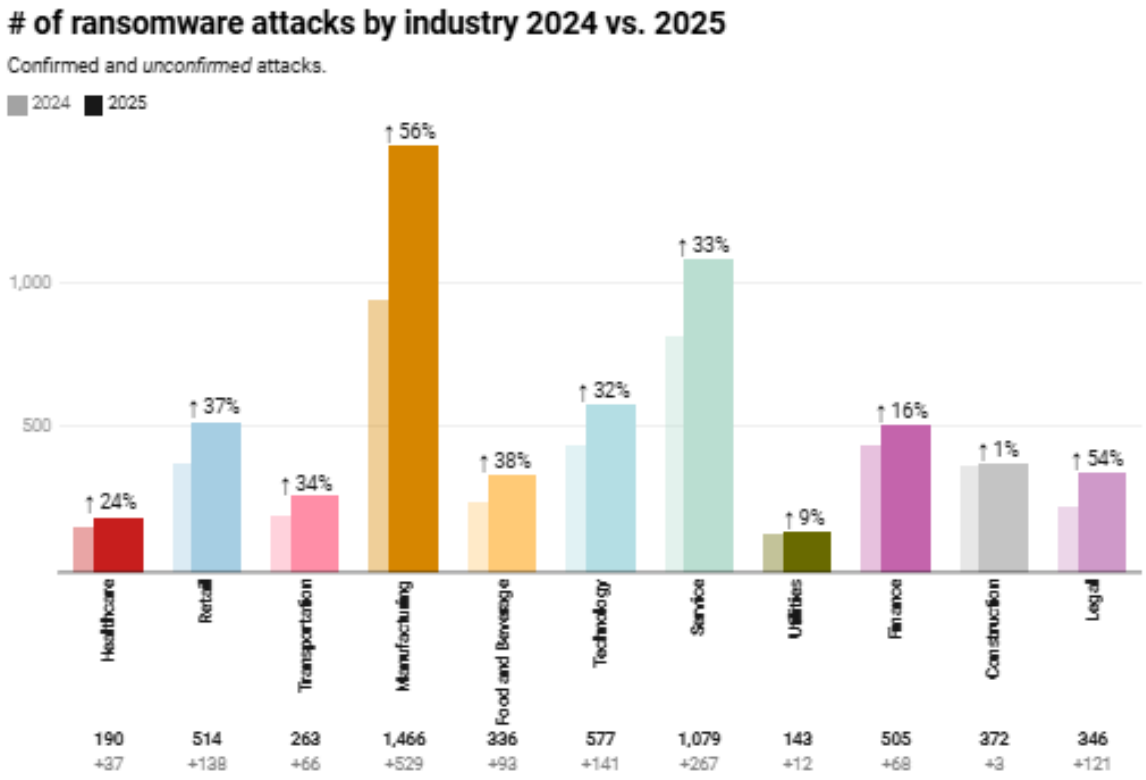
Notable Ransomware Attacks and Breaches in Q4 2025

- On November 22, the OnSolve CodeRED emergency alert system, provided by Crisis24 in the U.S., was disrupted due to a cyberattack, preventing it from sending emergency notifications. Crisis24 did not issue a statement, but customers reported that cybercriminals had obtained personal data of OnSolve CodeRED users. The attackers claimed negotiations failed because the vendor was only willing to pay a $100,000 ransom.[30]
- On November 20, Italy's national railway operator, the FS Italiane Group fell victim to a cyberattack after a threat actor breached Almaviva, the organization's IT services provider. The hacker claimed to have stolen 2.3 terabytes (TB) of data that include confidential documents and sensitive company information, and later leaked it on a dark web forum.[31]
- On November 14, Pajemploi, the French social security service for parents and home-based childcare providers, detected a data breach potentially exposing the personal information of 1.2 million individuals. The incident impacted registered professional caregivers working for private employers, typically parents using the Pajemploi service. No ransomware group has claimed credit for the attack.[32]
- On November 5, the University of Pennsylvania confirmed that data had been stolen in a cyberattack. The attacker hacked an employee's PennKey SSO account that provided access to the university's Salesforce instance, Qlik analytics platform, SAP business intelligence system, and SharePoint files. In a post on a hacking forum, the attackers stated they are not currently leaking the data records but may do so within a month or two.[33]
- On October 27, Swedish state-owned power grid operator Svenska kraftnät confirmed that a data breach occurred following a cyberattack. The attack did not affect the country's power supply. The data breach was disclosed after the Everest ransomware group added Svenska to its Tor-based leak site and claimed to have stolen 280 GB of data.[34]
- On October 19, Japanese retail company Muji suspended online sales in Japan due to a logistic outage caused by a ransomware attack on its delivery partner, Askul. Askul later confirmed that the attack caused significant disruptions to orders and shipping and resulted in 700,00 customer records being compromised. The RansomHouse ransomware group took credit for the attack and claimed to have stolen 1 TB of data which was leaked on November 10 and December 2, indicating the ransom was not paid.[35,36]
- On October 15, U.S.-based fencing and pet solutions provider Jewett-Cameron Company (Nasdaq: JCTC) reported a cyberattack. Following the attack, the company was unable to access several business applications related to operations and corporate functions. The identity of the attackers was not known, but they threatened to leak the stolen information if the ransom was not paid.[37]
- On October 14, Spanish fashion retailer MANGO notified customers of a data breach after its marketing vendor was compromised, exposing their personal data. MANGO specified that last names, banking information, credit card data, IDs, passports, or account credentials were not compromised in the incident.[38]

- On October 3, a hacking group believed to be a splinter of the ShinyHunters/Scattered Spider/LAPSUS$ collective released millions of records allegedly stolen from Salesforce customers. They claimed to have stolen 1 billion records from 39 Salesforce customers and demanded ransom from both Salesforce and the affected companies. The group started leaking personal data on their Tor-based site for six of the named victims: Albertsons, Engie Resources, Fujifilm, GAP, Qantas, and Vietnam Airlines.[39,40]
- On October 2, sports betting company DraftKings (Nasdaq: DKNG), notified an undisclosed number of customers that their accounts had been hacked in a recent wave of credential stuffing attacks. The company said the attackers did not access sensitive data like government-issued identification numbers, full financial account numbers, or bank account details.[41]

In 2025, ransomware attacks surged with 7,419 logged globally. This represents a 35% increase when compared to 2024. Businesses saw the sharpest rise in attacks, up 35% from 2024, followed by government entitles (up 27%), while healthcare companies and educational institutions saw the smallest rise in attacks (up 2%). Over 59.2 million records were compromised, and the average ransom demanded exceeded $1.04 million. Government entities faced the highest ransom demand of $1.56 million, followed by businesses with an average ransomware demand of $1.1 million[42].





Healthcare figures included here are for companies that don't offer direct care, e.g. pharmaceutical manufacturers or billing providers. Some utility companies are also classed as government entities in our overall sector figures.

Cybersecurity Industry Outlook and Top Headlines from Q4 2025

- The International Data Corporation projects cybersecurity spending to reach $377 billion by 2028.[43]The cost of cybercrimes for the world economy is expected to reach $10.5 trillion for the year 2025[44] with the average cost of a data breach at $4.4 million, a 9% y/y reduction driven by faster identification and containment.[45]
- In December 2025, the Cybersecurity and Infrastructure Security Agency (CISA) released its revised cross-sector cybersecurity performance goals, offering organizations a more robust framework for integrating cybersecurity into daily operations. It incorporates three years of operational insights, and addresses emerging threats through data-driven, actionable guidance.[46] The agency issued a joint advisory with the FBI and other U.S. and global partners urging immediate action to defend critical infrastructure from pro-Russia hacktivist threats.[47] The advisory warns of organized threat actors seeking targets of opportunity across all critical infrastructure sectors.[48]
- In December 2025, the United States halted plans to impose sanctions on China's ministry of state security over a massive cyber spying campaign (a wide-ranging and years-long cyberespionage campaign tracked as Salt Typhoon) to avoid derailing a trade truce struck by both countries this year.[49]
- In November 2025, the United States, Australia and Britain announced coordinated sanctions against Russia-based web company Media Land, accusing it of supporting ransomware operations. Britain has accused Media Land of being one of the most significant operators of so-called bulletproof hosting services, which provide infrastructure for ransomware and phishing attacks.[50]
- In November 2025, Google shutdown the group behind the E-ZPass, USPS text scam. Google said it has disrupted the foreign cybercriminal group behind a text scam operation within 24 hours of filing its lawsuit.[51]

- OpenAI has warned its upcoming AI models could pose a "high" cybersecurity risk, as their capabilities advance rapidly. The company further added it's investing in strengthening models for defensive cybersecurity tasks and creating tools that enable defenders to more easily perform workflows such as auditing code and patching vulnerabilities.[52]

[1] Bloomberg, Factset
[2] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m11/cisco-simplifies-security-for-managed-service-providers-accelerating-their-hybrid-mesh-firewall-deployments-and-business-growth.html
[3] https://www.broadcom.com/company/news/product-releases/63686
[4] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2025/fortinet-launches-secure-ai-data-center-solution-to-protect-models-data-and-infrastructure-at-scale
[5] https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-unveils-cortex-agentix-to-build--deploy-and-govern-the-agentic-workforce-of-the-future
[6] https://newsroom.gendigital.com/2025-11-12-Avast-Brings-AI-powered-Scam-Defense-to-Mobile
[7] https://www.securityweek.com/palo-alto-networks-to-acquire-observability-platform-chronosphere-in-3-35-billion-deal/
[8] https://www.securityweek.com/servicenow-to-acquire-identity-security-firm-veza-in-reported-1-billion-deal/
[9] https://www.securityweek.com/dataminr-to-acquire-threatconnect-for-290-million/
[10] https://www.securityweek.com/veeam-to-acquire-data-security-firm-securiti-ai-for-1-7-billion/
[11] https://investors.fastly.com/news/news-details/2025/Fastly-Announces-Listing-Transfer-to-Nasdaq/default.aspx
[12] https://investors.fastly.com/news/news-details/2025/Fastly-Inc--Announces-Proposed-Convertible-Senior-Notes-Offering/default.aspx
[13] https://investors.fastly.com/news/news-details/2025/Fastly-Announces-Record-Third-Quarter-2025-Financial-Results/default.aspx
[14] Factset, Q3 2025 Transcript
[15] https://s2.q4cdn.com/951347115/files/doc_earnings/2026/q1/earnings-result/Q1FY26-Press-Release.pdf
[16] https://s2.q4cdn.com/951347115/files/doc_earnings/2026/q1/presentation/Q1-26-Earnings-Slides.pdf
[17] Factset
[18] https://investors.broadcom.com/news-releases/news-release-details/broadcom-inc-announces-fourth-quarter-and-fiscal-year-2025
[19] https://investors.broadcom.com/news-releases/news-release-details/openai-and-broadcom-announce-strategic-collaboration-deploy-10
[20] Factset, Q4 2025 Transcript
[21] https://ir.varonis.com/news-and-events/press-releases/press-release-details/2025/Varonis-Announces-Third-Quarter-2025-Financial-Results/default.aspx
[22] https://ir.varonis.com/news-and-events/press-releases/press-release-details/2025/Varonis-Announces-Second-Quarter-2025-Financial-Results/default.aspx
[23] https://ir.varonis.com/news-and-events/press-releases/press-release-details/2025/Varonis-Announces-150-Million-Share-Repurchase-Authorization/default.aspx
[24] Factset
[25] https://ir.zscaler.com/static-files/52a8524c-6bc0-41bf-aa3b-a476ca1e8572
[26] Factset, Q1 2026 Transcript
[27] https://www.investing.com/news/analyst-ratings/jpmorgan-downgrades-trend-micro-stock-to-neutral-amid-it-spending-cuts-93CH-4266539
[28] https://www.trendmicro.com/en_us/about/investor-relations.html#financial-reports-tm-id
[29] Returns are in USD terms
[30] https://www.securityweek.com/ransomware-attack-disrupts-local-emergency-alert-system-across-us/

[31] https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-23tb-data-from-italian-rail-group-almaviva/
[32] https://www.bleepingcomputer.com/news/security/french-agency-pajemploi-reports-data-breach-affecting-12m-people/
[33] https://www.bleepingcomputer.com/news/security/university-of-pennsylvania-confirms-data-stolen-in-cyberattack/
[34] https://www.securityweek.com/hackers-target-swedish-power-grid-operator/
[35] https://www.bleepingcomputer.com/news/security/retail-giant-muji-halts-online-sales-after-ransomware-attack-on-supplier/
[36] https://www.securityweek.com/700000-records-compromised-in-askul-ransomware-attack/
[37] https://www.securityweek.com/fencing-and-pet-company-jewett-cameron-hit-by-ransomware/
[38] https://www.bleepingcomputer.com/news/security/clothing-giant-mango-discloses-data-breach-exposing-customer-info/
[39] https://www.salesforceben.com/hackers-leak-millions-of-salesforce-customer-records-after-failed-ransom-bid/
[40] https://www.crn.com/news/security/hacker-group-says-1-billion-records-stolen-from-salesforce-users?itc=refresh
[41] https://www.bleepingcomputer.com/news/security/draftkings-warns-of-account-breaches-in-credential-stuffing-attacks/
[42] https://www.comparitech.com/news/worldwide-ransomware-roundup-2025-end-of-year-report/
[43] https://www.ibm.com/think/topics/cybersecurity
[44] https://www.ibm.com/think/topics/cybersecurity
[45] https://www.ibm.com/reports/data-breach
[46] https://www.cisa.gov/news-events/news/cisa-unveils-enhanced-cross-sector-cybersecurity-performance-goals
[47] https://www.cisa.gov/news-events/news/cisa-fbi-and-us-and-global-partners-urge-immediate-action-defend-critical-infrastructure-pro-russia
[48] https://www.cisa.gov/news-events/news/cisa-fbi-and-us-and-global-partners-urge-immediate-action-defend-critical-infrastructure-pro-russia
[49] https://www.usnews.com/news/world/articles/2025-12-03/us-halted-plans-to-sanction-chinese-spy-agency-to-maintain-trade-truce-ft-says
[50] https://www.reuters.com/world/asia-pacific/us-uk-australia-announce-sanctions-against-russia-based-media-land-over-2025-11-19/
[51] https://www.cnbc.com/2025/11/13/google-text-scam-phishing-e-zpass-usps.html
[52] https://money.usnews.com/investing/news/articles/2025-12-10/openai-warns-new-models-pose-high-cybersecurity-risk