Q3 2025 Cybersecurity Commentary

Executive Summary and Performance Commentary

Cybersecurity companies delivered marginally positive performance in Q3 2025, with the Nasdaq ISE Cyber Security Select™ Index (HXRXL™) up 0.7% for the quarter vs. the S&P 500 (+7.8%), which extended the post-April broad market rally. Of the index's 24 constituents, only 7 names experienced gains, with 10 down by more than 5%. 5 names were down more than 10% apiece, including overall worst performer Trend Micro (-20.6%), followed by Fortinet (-20.5%), Rapid7 (-18.9%), Tenable (-13.7%), and Radware (-10.0%). Overall, HXRXL is still outperforming the S&P 500 on a YTD basis, up 16.6% vs. 13.7%.
See pages 4-5 for more detailed commentary on the Top 3 / Bottom 3 performance contributors.

Investors continue to lack meaningful exposure to cybersecurity in their core portfolios. The S&P 500 currently tracks only 6 constituents that overlap with HXRXL, comprising <9% of its exposure. 18 of HXRXL's constituents (~65% of index weight) do not overlap with the S&P 500. With a volatility profile below what's typical for thematic indexes and one of the most stable, recession-proof growth trajectories across the entire IT spending arena, cybersecurity's dynamics more closely resemble 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 August 25, Nevada state officials publicly confirmed that a ransomware attack caused severe disruptions across state systems for several days and led to data theft. The attack forced the closure of all state offices for two days. U.S. cybersecurity agency CISA has been involved in the response operations.[1]

On August 11, the Pennsylvania Office of Attorney General confirmed that a ransomware attack caused a three-week outage that disrupted email, phones, and websites, forcing employees to use alternative communication channels to continue working. A file-encrypting ransomware was used to demand ransom, though no payment has been made. The identity of the attacker remains unknown.[2]
See page 6 for a full run-down of major ransomware attacks and data breaches.

According to the U.S., China used three private companies to hack global telecoms through an operation known as Salt Typhoon. The hacking operation included snooping on text messages from the campaigns of both Kamala Harris and Donald Trump, according to a coalition of U.S. agencies and 12 allied governments. Salt Typhoon hacked into telecommunication companies around the world, including AT&T and Verizon last year, allowing it to potentially access text and telephone communications between millions of people and track their locations.[3]

The Czech Republic banned the use of any products by the Chinese AI startup DeepSeek in state administration over cybersecurity concerns. Czech Prime Minister Petr Fiala said the government acted after receiving a warning from the national cybersecurity watchdog, which noted a threat of unauthorized access to user's data because the firm is obliged to cooperate with Chinese state authorities. The move aligns with similar actions taken by other countries, including Italy and Australia.[4]

See page 8 for a discussion of other noteworthy regulatory and policy developments globally.

Nasdaq Cybersecurity Thought Leadership

With the launch of highly impactful new tariff policies in Q2, our research team highlights the potential consequences of ratcheting geopolitical tensions and increased state-sponsored cyber threats.

In a separate note, we explore the growing importance of machine identity security in the digital age.

Quarterly Earnings Recap

Overall, HXRXL companies that beat revenue and earnings estimates in the most recent reported quarter did so by an average of 2.5% and 25.3% respectively, while the only company that missed did so by 5.8% and 44.4%, respectively. **96.5% of index weight beat on both top line and bottom-line estimates for EPS.** In aggregate, HXRXL companies grew revenues 12% YoY from $59.5B to $66.4B. **Aggregate net income surged by 176% from $3.6B to $10.1B, largely driven by Broadcom & Cisco.**

Q2 2025 Earnings	Beats		Misses	
	No. of Firms/ Index Weight	Average Beat (%)	No. of Firms/ Index Weight	Average Miss (%)
Q2 2025 Revenues	23/96.5%	2.5%	1/3.5%	-5.8%
Q2 2025 EPS	23/96.5%	25.3%	1/3.5%	-44.4%

Index Additions & Deletions (September 22, 2025)

Fastly – a leader in providing application security and delivery solutions for multi-cloud environments – was added back to the index at a weight of 2.7%. Fastly was previously deleted from the index at a weight of 2.2% after its market cap fell below the $1 billion minimum requirement as of the prior index reconstitution reference date of April 30, 2025.

New Cybersecurity Products Announced in Q3 2025 (AI-Related in Bold)

- In September 2025, Gen Digital (NASDAQ: GEN) teamed up with Intel to provide detection against AI-powered scams in the newest generation of Intel Core Ultra processors. Norton 360 customers with Norton Genie Scam Protection now have advanced deepfake protection on AI PCs with the latest Intel processors, enabling faster, always-on detection that proactively protects against today's most sophisticated scams.[5]
- In August 2025, Qualys (NASDAQ: QLYS) introduced several new agentic AI capabilities on the Qualys platform. The new AI fabric introduces a marketplace of cyber risk AI agents delivering real-time risk insights across all attack surfaces, prioritized by business impact. Additionally, it reduces risk and operational costs by autonomously remediating with speed, scale, and accuracy, all while powering a smarter, more efficient risk operations center.[6]
- In August 2025, Cloudflare (NASDAQ: NET) announced new capabilities for Cloudflare One, its Zero Trust platform, designed to help organizations securely adopt, build and deploy emerging generative AI

applications. With these new features users can automatically understand, analyze and set controls on how generative AI is used throughout their organization – enhancing the productivity and innovation of their teams without sacrificing security or privacy standards.[7]

- In August 2025, Palo Alto Networks (NASDAQ: PANW) announced Cortex Cloud Application Security Posture Management (ASPM), a prevention-first application security module that blocks security issues from reaching production. It enables customers to fix security risks before cloud and AI applications have been deployed, which is up to 10 times faster, more efficient, and cost effective.[8] In addition, Cortex Cloud ASPM includes an open AppSec partner ecosystem, enabling organizations to consolidate data from their preferred third-party code scanners into one centralized platform for comprehensive visibility.[9]
- In July 2025, CyberArk (NASDAQ: CYBR) announced that CyberArk Secure Cloud Access (SCA) MCP Server and CyberArk Agent Guard are available in the new AWS Marketplace AI Agents and Tools category. Customers can use AWS Marketplace to easily discover, buy, and deploy AI agent solutions using their AWS accounts, accelerating agent and agentic workflow development.[10]

Cybersecurity M&A and IPO Activity in Q3 2025

Inside HXRXL Index Activity:

- On September 9, SentinelOne (NYSE: S) announced its acquisition of U.S.-based Observo AI in a cash and stock deal valued at $225 million. Observo AI has developed an AI-native data pipeline platform for DevOps and security designed to help enterprises manage the significant amount of data generated by IT infrastructure and security tools. SentinelOne expects Observo AI to enable it to boost its SIEM and data offerings. The deal is expected to close in Q3 of FY 2026.[11]
- On August 27, CrowdStrike (NASDAQ: CRWD) announced its acquisition of Spanish startup Onum in a deal that is reportedly valued at $290 million, though specific terms of the deal were not disclosed. The acquisition will add valuable technology to enhance its Falcon Next-Gen SIEM. Onum is built on a stateless, in-memory architecture, which CrowdStrike says will complement its SIEM and bring speed, scale, and efficiency in onboarding while giving customers control of their security and observability data. Launched in 2023, Onum provides real-time telemetry pipeline technology and had raised $40 million in funding.[12]
- On July 30, Palo Alto Networks (NASDAQ: PANW) agreed to acquire identity security company CyberArk (NASDAQ: CYBR) in a deal valued at ~$25 billion. The integration of CyberArk's Identity Security Platform with Palo Alto Networks offers a unified solution that eliminates security gaps and simplifies operations. As autonomous agentic AI becomes more prevalent, Identity Security will serve as a critical framework. The deal is expected to close in H2 of FY 2026.[13]
- On September 12, security and application delivery solutions provider F5 (NASDAQ: FFIV) announced its acquisition of AI security firm CalypsoAI for $180 million, mainly in cash. CalypsoAI has developed a platform designed to use agentic red teaming, real-time defenses, and automated security enforcement to secure AI at inference (i.e., while the AI is in a live, operational state). F5 plans to integrate these capabilities into its Application Delivery and Security Platform (ADSP).[14]

Outside HXRXL Index Activity:

- On September 9, Mitsubishi Electric (TYO: 6503) signed an agreement to acquire OT and IoT cybersecurity company Nozomi Networks for $1 billion. Nozomi has developed a platform designed to

give organizations visibility and control over OT and IoT systems. Mitsubishi already owns a 7% stake in the company and will pay $883 million in cash to acquire the remaining stake. Nozomi had revenues of $75 million and $62 million in 2024 and 2023, respectively. The transaction is expected to close in Q4 2025.[15]

- On August 12, Diginex (NASDAQ: DGNX) announced that it signed a non-binding Memorandum of Understanding to acquire 100% of the equity interests of IDRRA Cyber Security Ltd., which operates under the trade name Findings. The deal consideration amount is $305 million, with $270 million in Diginex shares, and up to $35 million in cash, of which $20 million is financial target achievement-based payment. Findings provides innovative category-leading supply chain risk monitoring and vendor risk automation solutions in the cybersecurity and sustainability regulatory domains. Diginex intends to expand in the cybersecurity space and be a global leader in compliance data verification and regulatory compliance automation.[16]
- On July 30, attack surface management solutions provider Axonius acquired medical device security company Cynerio for more than $100 million in a cash-and-stock deal. Cynerio specializes in securing medical devices in healthcare environments and its solutions enable organizations to implement micro segmentation, protect sensitive information, and block ransomware attacks. The acquisition will enable Axonius to accelerate its expansion into the healthcare market.[17]

Top 3 Index Performance Contributors in Q3 2025

Broadcom[18]

- Stock price was up 19.9% from June 30, 2025 – Sept 30, 2025
- The stock rose on the heels of a strong quarter and improved fiscal 2026 AI revenue outlook. Specifically, the company indicated that its AI revenue (~30-35% of its mix) should grow 20% q/q next quarter and further accelerate into 2026. In combination with a slowly improving non-AI semi segment and software segment, it expects to deliver an impressive 40% y/y revenue growth in FY 2026.
- The company also announced that it is ramping a 4th XPU customer that should yield $10 billion in incremental revenue in FY 2026. It announced a record backlog of $110 billion with orders in the non-AI semis segment rising 23% year-over-year, despite a slower than typical recovery in non-AI semis.
- Fiscal Q3 2025 revenue was $15.9 billion, a 22.0% increase y/y. AI related revenue increased by 63% year-over-year to $5.2 billion, driven by strong demand for the company's custom AI accelerators and networking solutions. It is now guiding 4Q revenue of approximately $17.4 billion. It reported net income of $4.2 billion, with gross margin of 78.4%, operating margin of 65.5% and adjusted EBITDA margin of 67.1%.

Northrop Grumman[19]

- Stock price was up 22.4% from June 30, 2025 – Sept 30, 2025
- The stock rose on the heels of a strong quarter, improved guidance, and positive sentiment from analysts covering the stock. Additionally, the company benefitted from the signing of new contracts, including one for the B-21 bomber program and other defense work, as well as strong performance across its various divisions, particularly its Aeronautics Segment.

- In Q2 2025, the company reported $10.4 billion in revenue and $8.2 per share in adjusted earnings, beating expectations by 2.6% and 19%, respectively. The outperformance was driven by robust demand across its portfolio, strong international growth and improved execution across its segments. The company raised its full-year adjusted EPS guidance, suggesting positive sentiment.

General Dynamics[20]

- Stock price was up 17.5% from June 30, 2025 – Sept 30, 2025
- The stock rose on the heels of a strong quarter, which beat expectations for revenue and earnings. Growth was higher across all segments, particularly due to strong order activity and revenue growth in its Marine and Aerospace divisions. Additionally, its book-to-bill ratio of 2.2:1 for the quarter showed that orders exceeded revenue, pointing to a strong pipeline. The company's backlog increased to $103.7 billion, suggesting strong future growth prospects.
- In Q2 2025, the company reported revenue of $13 billion and diluted EPS of $3.74, which represented increases of 8.9% and 14.7% year-over-year respectively, compared to the same quarter the previous year.

Bottom 3 Index Performance Contributors in Q3 2025

Fortinet[21]

- Stock price was down 20.5% from June 30, 2025 – Sept 30, 2025
- The company reported revenues of $1.6 billion for the second quarter of 2025, a 14% year-over-year growth. Billings grew 15% year-over year to $1.8 billion. It reported GAAP operating margin of 28% and non-GAAP operating margin of 33%, raising its 2025 full year billings guidance midpoint by $100 million.
- While the company reported solid second quarter results beating Street estimates, investors were disappointed that product revenue growth and billings were not stronger, with 40%-50% of its accelerated firewall refresh cycle already complete. Future growth prospects appear limited, given that the refresh cycle is ending. Following its update on its refresh cycle and revenue forecast, several firms downgraded the stock.

Trend Micro[22]

- Stock price was down 20.6% from June 30, 2025 – Sept 30, 2025
- The stock came under pressure due to increased competition from other industry players, including Palo Alto, Microsoft, CrowdStrike and other companies competing for the same budget. Additionally, concerns over slowing corporate spending, especially among midsize companies, dampened investor sentiment. These factors outweighed solid operational performance and growth in its core products.
- Sales came in weaker than expected, largely due to ongoing economic uncertainty, which caused a delay in deals. The company reported confidence in closing deals in the second half of the year.
- In the most recent quarter, Trend Micro reported sales of $459 million, a decrease of 3.2% year-over-year, and EPS of $0.29, which missed consensus estimates of $0.52. Despite a 94% increase in its flagship Trend Vision One™ platform's recurring revenue, overall results were disappointing.

Rapid7[23]

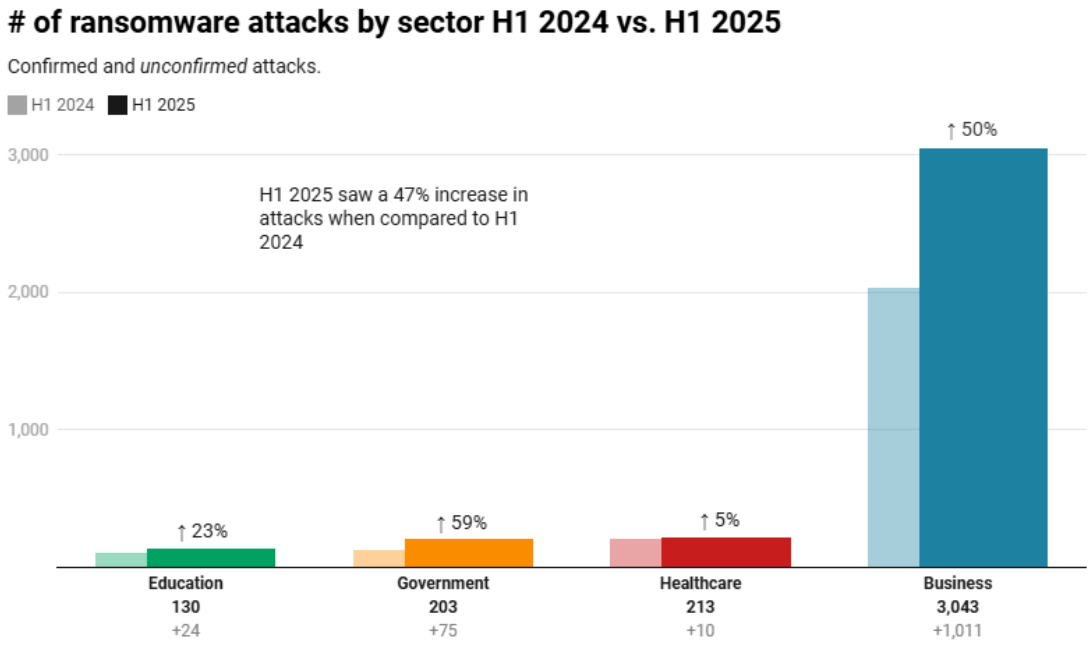
- Stock price was down 18.9% from June 30, 2025 – Sept 30, 2025
- The stock was down due to slowdown in revenue growth, especially in its legacy business, demand weakness in U.S. mid-market segment and decline in investor sentiment among analysts. The company is implementing new strategies such as integrating AI into its tools and expanding internationally, which have yet to materialize in terms of improving fundamentals or impacting stock performance.
- In Q2 2025, the company reported revenues of $214 million, a 3% increase year-over-year with Annual Recurring Revenue growing 3% year-over-year to $841 million. Its EPS of $0.58 beat analyst forecasts. Other highlights include positive free cash flow of $42 million.

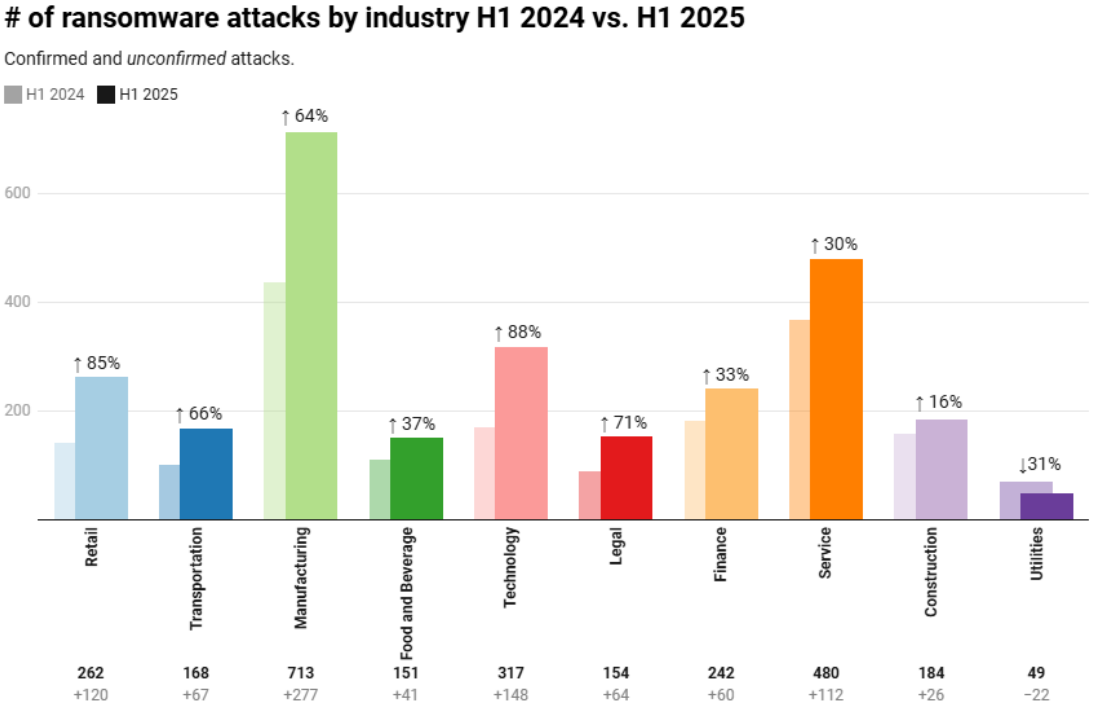
Notable Ransomware Attacks and Breaches in Q3 2025

- On August 25, Nevada state officials publicly confirmed that a ransomware attack caused severe disruptions across state systems for several days and led to data theft. The attack forced the closure of all state offices for two days. The U.S. cybersecurity agency CISA has been involved in the response operations.[24]
- On August 21, UK-based telecom firm Colt Technology Services confirmed a data breach of its internal systems after a ransomware attack, clarifying that customer infrastructure remained unaffected. WarLock ransomware group took credit for the attack and are in the process of auctioning the stolen files.[25]
- On August 20, Inotiv (NASDAQ: NOTV) confirmed a ransomware attack disrupted business operations and that certain internal systems were encrypted. The Qilin ransomware group added Inotiv to its Tor-based leak site and claimed to have stolen 176 Gb of business-related data.[26]
- On August 16, chip programming solutions provider Data I/O (NASDAQ: DAIO) was the target of a ransomware attack that caused significant disruptions to communications, shipping, manufacturing, and other functions. The 8-K SEC filing suggests some data may have been stolen. The company has engaged cybersecurity experts and expects the incident to have a material impact on its financials.[27]
- On August 11, the Pennsylvania Office of Attorney General confirmed that a ransomware attack caused a three-week outage that disrupted email, phones, and websites, forcing employees to use alternative communication channels to continue working. A file-encrypting ransomware was used to demand ransom, though no payment has been made. The identity of the attacker remains unknown.[28]
- On July 28, a subsidiary of Allianz (ETR: ALV), Allianz Life Insurance Company, North America was a victim of a cyberattack which resulted in personal information being compromised. Attackers gained access to a cloud-based CRM on July 16 and gained access to personally identifiable information of 1.1 million customers, financial professionals, and some employees.[29,30]
- On July 10, Ingram Micro (NYSE: INGM) restored all services following a ransomware attack on July 3, that halted order processing and shipping for several days. The SafePlay ransomware group accessed the company's system through GlobalProtect VPN platform and alleged to have stolen 3.5 TB of data, threatening to release it if the ransom demands were unmet. The identity of the attacker remains unknown.[31,32,33]

in the first half of 2025, ransomware attacks surged with 3,627 incidents logged globally. This represents a 47% increase compared to H1 2024. Government and education sectors saw sharp rises in attacks, 60% and 23% respectively, while businesses experienced a 50% increase, especially in industries like technology (+88%), retail (+85%), and legal (+71%). Over 17 million records were compromised in confirmed attacks,

and the average ransom demand exceeded $1.6 million. Notably, government entities faced the highest ransom demands, with some reaching $12 million, while businesses and healthcare organizations saw lower averages. [34]





Cybersecurity Industry Outlook and Top Headlines from Q3 2025

- Revenue in the cybersecurity market is expected to grow to $196.5 billion in 2025, with an annual growth rate of 8.0%[35] (dialed down from previous estimate of $203.0 billion and 9.3%). The security services[36] segment is expected to contribute $100.4 billion to the total revenues, with the rest driven from cyber solutions.[37,38] During the period 2025-2030, revenue is expected to show an annual growth rate of 5.9% resulting in a total market size of $262.3 billion by 2030[39]. This growth is expected to be led by the cyber solutions segment with an estimated CAGR of 8.2% and a resultant market size of $142.4 billion[40] by 2030, followed by the security services segment at a lower rate of 3.6% and a resultant market size of $119.9 billion by 2030[41]. Region-wise, the U.S., which is the largest market for cybersecurity, is expected to have a market size of $86.4 billion in 2025 and is expected to grow at a CAGR of 5.7% (slightly lower than the global growth rate) during the period 2025-2030 to a market size of $114.1 billion by 2030.[42]
- The Cybersecurity and Infrastructure Security Agency (CISA) has issued a joint statement with FBI, DC3 and NSA on potential targeted cyber activity against U.S. critical infrastructure by Iran.[43] According to the joint statement, Iranian state-sponsored or affiliated threat actors are known to conduct a range of targeted cyber activity to include exploiting known vulnerabilities in unpatched or outdated software, compromising internet-connected accounts and devices that use default or weak passwords and working with ransomware affiliates to encrypt, steal and leak sensitive information. The agencies have urged critical infrastructure organizations to stay vigilant to Iranian-affiliated cyber actors that may target U.S. devices and networks.
- US imposed sanctions on a network of cyber scam centers operating in Southeast Asia (Myanmar and Cambodia) to heighten pressure on operations allegedly using forced labor to bilk billions from Americans annually.[44] According to the US Treasury Department, Americans lost more than $10 billion due to Southeast Asia-based scams last year. The scam operators coerce individuals to scam strangers online using messaging apps or text messages.
- Russian hackers have stepped up sabotage attempts against Polish critical infrastructure, with hospitals and city water systems among the targets. The Polish government is increasing its cyber security budget to a record €1 billion this year (from €600 million in 2024), after the Russian sabotage attempts.[45]

[1] https://www.securityweek.com/nevada-confirms-ransomware-attack-behind-statewide-service-disruptions/
[2] https://www.securityweek.com/pennsylvania-attorney-general-confirms-ransomware-behind-weeks-long-outage/
[3] https://www.nbcnews.com/tech/security/china-used-three-private-companies-hack-global-telecoms-us-says-rcna227543

[4] https://apnews.com/article/czech-china-deepseek-ban-104f58035294f9f6ca988119732b8620
[5] https://newsroom.gendigital.com/2025-09-16-Norton-Unveils-Advanced-Deepfake-Protection-Powered-by-Intel-R-Core-TM-Ultra-Processors
[6] https://www.qualys.com/company/newsroom/news-releases/usa/qualys-unveils-industrys-first-agentic-ai-powered-risk-operations-center/
[7] https://www.cloudflare.com/press-releases/2025/cloudflare-launches-new-zero-trust-tools-for-secure-ai-adoption-at-scale/
[8] https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-redefines-application-security-with-the-industry-s-most-comprehensive-prevention-first-aspm
[9] https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-redefines-application-security-with-the-industry-s-most-comprehensive-prevention-first-aspm
[10] https://www.cyberark.com/press/cyberark-announces-availability-of-tools-to-secure-ai-agents-in-the-new-aws-marketplace-ai-agents-and-tools-category/
[11] https://www.securityweek.com/sentinelone-to-acquire-observo-ai-in-225-million-deal/
[12] https://www.securityweek.com/crowdstrike-to-acquire-onum-to-fuel-falcon-next-gen-siem-with-real-time-telemetry/
[13] https://www.securityweek.com/palo-alto-networks-to-acquire-cyberark-for-25-billion/
[14] https://www.securityweek.com/f5-to-acquire-calypsoai-for-180-million/
[15] https://www.securityweek.com/mitsubishi-electric-to-acquire-nozomi-networks-for-nearly-1-billion/
[16] https://www.globenewswire.com/news-release/2025/08/12/3132145/0/en/Diginex-Announces-MOU-for-US-305m-Acquisition-of-Findings-a-leading-cybersecurity-and-compliance-automation-company.html
[17] https://www.securityweek.com/axonius-acquires-medical-device-security-firm-cynerio-in-100-million-deal/
[18] https://investors.broadcom.com/news-releases/news-release-details/broadcom-inc-announces-third-quarter-fiscal-year-2025-financial
[19] https://investor.northropgrumman.com/static-files/
[20] https://s22.q4cdn.com/891946778/files/doc_financials/2025/q1/GD-2025-03-30-Exhibit-99-1.pdf
[21] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2025/fortinet-reports-second-quarter-2025-financial-results
[22] https://newsroom.trendmicro.com/2025-08-07-Trend-Micro-Reports-Earnings-Results-for-Q2-2025
[23] https://investors.rapid7.com/news/news-details/2025/Rapid7-Announces-Second-Quarter-2025-Financial-Results/
[24] https://www.securityweek.com/nevada-confirms-ransomware-attack-behind-statewide-service-disruptions/
[25] https://www.securityweek.com/telecom-firm-colt-confirms-data-breach-as-ransomware-group-auctions-files/
[26] https://www.securityweek.com/pharmaceutical-company-inotiv-confirms-ransomware-attack/
[27] https://www.securityweek.com/chip-programming-firm-data-i-o-hit-by-ransomware/
[28] https://www.securityweek.com/pennsylvania-attorney-general-confirms-ransomware-behind-weeks-long-outage/
[29] https://www.securityweek.com/allianz-life-data-breach-impacts-most-of-1-4-million-us-customers/
[30] https://www.reuters.com/legal/government/hack-allianz-life-impacts-11-million-customers-breach-notification-site-says-2025-08-18/
[31] https://www.securityweek.com/ingram-micro-restores-systems-impacted-by-ransomware/
[32] https://www.blackfog.com/how-ingram-micro-overcame-a-major-ransomware-attack/
[33] https://www.csoonline.com/article/4031695/ransomware-gang-tells-ingram-micro-pay-up-by-august-1.html
[34] https://www.comparitech.com/news/ransomware-roundup-h1-2025/
[35] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[36] *Security Services: Security services refer a wide range of services that enhance an organization's protection and security strategy against common cybercrimes.*
[37] *Cyber Solutions: refer to automated security technologies that help monitor and secure IT systems, data, networks, and digital assets, protecting against cyberattacks*
[38] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[39] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[40] https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/worldwide
[41] https://www.statista.com/outlook/tmo/cybersecurity/security-services/worldwide
[42] https://www.statista.com/outlook/tmo/cybersecurity/united-states
[43] https://www.cisa.gov/news-events/news/joint-statement-cisa-fbi-dc3-and-nsa-potential-targeted-cyber-activity-against-us-critical
[44] https://www.bloomberg.com/news/articles/2025-09-08/trump-targets-asian-cyber-scam-centers-that-bilked-billions
[45] https://www.ft.com/content/3e7c7a96-09e7-407f-98d7-a29310743d28