

Q3 2026 HXRXL™ Cybersecurity Commentary

October 2026

Sanjana Prabhakar, *Index Insights Senior Specialist*

Executive Summary and Performance Commentary

Cybersecurity companies delivered positive price performance in Q3 2026, with the Nasdaq ISE Cyber Security Select™ Index (HXRXL™) up 15.3% for the quarter, outperforming the S&P 500 (2.03%). Of the 23 constituents, 14 names had gains, with 13 names experiencing double-digit gains. 9 names experienced losses, with 2 names namely A10 Networks and Gen Digital down 10% apiece, and the rest experiencing single-digit losses.

The S&P 500 currently includes 9 constituents that overlap with HXRXL, comprising ~5% of its exposure. 9 of HXRXL's constituents (~45.5% of index weight) do not overlap with the S&P 500. The cybersecurity sector moved from being a sentiment-driven, AI-narrative-dependent trade in Q1 and Q3 2026 to a sector whose Q3 performance was supported by reported earnings, cybersecurity budgets, and geopolitical developments. The +15.3% return was lower in magnitude than Q3's +43.7%, with Q3 performance coinciding with reported earnings results, cybersecurity budget data, and continuing geopolitical cybersecurity developments. The rally in Q3 2026 was structurally broader with return dispersion halving. Q2 gains were driven by large caps, with market breadth remaining weak across cybersecurity firms. By Q3, participation broadened well beyond mega-caps with laggards Zscaler and Sentinel One catching up. Q3 2026 was defined by a persistent, multi-month geopolitical demand signal that proved difficult to model away. Iranian-linked cyberattacks on over 30 US municipal water systems triggered an FBI investigation in July and elevated the sector's non-discretionary, defense-oriented profile¹. A joint Five Eyes advisory warned of Russian-linked hacking attempts across financial services, energy, and healthcare reinforced the geopolitical demand case². In September, the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory warning that Chinese AI companies — including DeepSeek and Alibaba — were conducting aggressive campaigns to steal from American AI models³. Together, these reported developments highlighted continuing cybersecurity risks associated with state-sponsored actors. CrowdStrike reported what it described as its best quarter in company history in August, with revenue of \$1.47 billion beating the \$1.44 billion consensus estimate, and issued above-consensus Q3 guidance^{4,5}. Palo Alto Networks projected 23–24% revenue growth to \$14.1–\$14.2 billion in fiscal 2027⁶. These prints prevented the sector from being dismissed as a purely sentiment-driven trade —

¹<https://www.washingtonpost.com/national-security/2026/07/30/us-spy-agencies-suspect-iran-launched-cyberattack-minnesota-water-facilities/>

²<https://www.afr.com/politics/federal/asd-warns-of-russian-beserk-bear-cyber-attacks-20260714-p60f4e>

³<https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-251a>

⁴<https://finance.yahoo.com/markets/stocks/articles/crowdstrike-shares-jump-earnings-beat-204330304.html>

⁵<https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-second-quarter-fiscal-year-2027-financial/>

⁶<https://qz.com/palo-alto-networks-revenue-growth-forecast-fiscal-2027-090126>

a key distinction from Q2 2026, where the rally was driven primarily by multiple expansion rather than earnings delivery. The AI narrative flipped from headwind to tailwind relative to Q1 2026. Roughly 7 in 10 CISOs surveyed by IANS and Artico Search cited AI as their top priority for new security spending, with overall security budgets rising 5%⁷. Anthropic's unveiling of Claude Mythos — capable of autonomously discovering and exploiting software vulnerabilities — strengthened the structural demand case rather than threatening it⁸. HXRXL declined 6.7% in Q1 2026. During that period, some market commentary raised concerns that AI security tools could compete with existing cybersecurity offerings. By Q3, cited survey and company commentary increasingly emphasized AI-related demand for cybersecurity products. Rather than serving as a headwind for the cybersecurity sector, the recent slowdown in AI adoption rhetoric is underscoring the risks associated with uncontrolled AI deployment and reinforcing demand for cybersecurity solutions. As organizations implement stricter guardrails and governance frameworks, security spending is likely to increase^{9,10}.

Nasdaq Cybersecurity Thought Leadership

With early reactions pricing in broad disruption risk, [our research highlights the market implications for the Mythos episode including how AI is reshaping the tempo of cybersecurity, rather than eliminating its economic relevance - with implications that are unevenly distributed across the security stack.](#)

Cybersecurity Industry Outlook and Top Headlines from Q3 2026

- As per a 2026 Cybersecurity Market Report, Forrester forecasts that worldwide information security spending will reach \$200 billion in 2026, while Gartner projects \$240 billion for 2026. Cybersecurity Ventures predicts the figure will be \$522 billion in 2026. Forrester forecasts cybersecurity spending to grow at a CAGR of 14.4% between 2024 through 2029 to \$302.5 billion by 2029¹¹. The cost of cybercrimes for the world economy may reach approximately \$10.5-\$10.8 trillion in 2026, according to Cybersecurity Ventures and is expected to cost \$12.2 trillion annually in 2031¹². The average cost of a data breach reached \$11.5 million in 2026 with the global average reaching \$4.99 million in 2026, according to IBM's annual cost of a Data Breach report conducted with the Ponemon Institute. AI-enabled breaches accounted for 1 in 4 malicious attacks, averaging \$6 million¹³.
- A joint advisory from NSA and CISA warned that Chinese AI companies — including DeepSeek, Moonshot AI, and Alibaba — have been conducting "aggressive, malicious, and targeted" campaigns to steal from American AI models, extracting billions of tokens from variants of Anthropic's Claude, Google's Gemini, and OpenAI's GPT since 2024¹⁴.
- President Trump signed an emergency order barring certain foreign-made transformers and critical energy equipment from the US power grid on national security grounds. The directive came amid bipartisan

⁷ <https://www.securityinfowatch.com/cybersecurity/news/55406256/ai-drives-cybersecurity-investment-as-security-budgets-remain-nearly-flat>

⁸ <https://www.armorcode.com/blog/anthropics-claude-mythos-and-what-it-means-for-security>

⁹ <https://www.ibm.com/think/news/ai-slowdown-calls-put-software-flaws-focus>

¹⁰ <https://www.cybersecuritydive.com/news/ai-leading-driver-cybersecurity-spending/830418/>

¹¹ <https://www.forrester.com/report/global-cybersecurity-market-forecast-2024-to-2029/RES186163>

¹² <https://cybersecurityventures.com/cybercrime-statistics-worldwide-the-2026-global-picture/>

¹³ <https://www.ibm.com/reports/data-breach>

¹⁴ <https://tech.yahoo.com/ai/articles/fbi-nsa-warn-chinese-ai-150500475.html>

concern that Chinese-manufactured components could contain exploitable vulnerabilities and followed a series of cyberattacks on US water facilities¹⁵.

- The White House's Office of the National Cyber Director has been drafting an executive order that would establish a government-led incubator to invest in cybersecurity research and spin out startups developing tools for government use, according to people familiar with the situation¹⁶.
- US intelligence agencies assessed that Iran was likely behind a coordinated cyberattack on more than 30 municipal water systems in Minnesota. The FBI launched an investigation into the attack, which came amid an ongoing US-Iran military conflict¹⁷.
- Cybersecurity experts are faulting Anthropic PBC and OpenAI for sloppy safeguards after their models broke into outside organizations — breaches they warned represent looming threats to national security. The breaches occurred as far back as April but weren't discovered until late July 2026, when Anthropic audited its cybersecurity testing after OpenAI disclosed that its own AI agents had escaped a testing environment and infiltrated Hugging Face, a repository for open-source AI models and documentation¹⁸.
- OpenAI launched the Daybreak for Frontline Defenders initiative on September 3, 2026, committing \$1 billion in subsidized artificial intelligence access, training, and tools to protect critical infrastructure from advanced cyberattacks. The program helps defenders review legacy code, spot suspicious activity, find software flaws, and test security patches before hackers strike¹⁹.
- The CISA submitted its final CIRCIA Cyber Incident Reporting Rule to the White House Office of Management and Budget (OMB) for interagency review on October 1, 2026. Covered critical infrastructure entities must report substantial cyber incidents within 72 hours and ransom payments within 24 hours²⁰.
- On August 25 2026, Boston Scientific announced that a cyberattack caused material disruptions to its IT network and global operations. Although manufacturing, order fulfillment, and shipping operations are now fully restored as of September 9, 2026, the two-week backlog has forced the medical device manufacturer to warn investors it will likely miss its Q3 and full-year 2026 net sales growth and adjusted EPS estimates²¹.
- On August 21 2026, hackers used social engineering techniques to breach Apollo's cloud systems in July, accessing personal information — part of a broader wave of attempted cyberattacks targeting major hedge funds including Two Sigma, Citadel, and Point72. The incident was part of a highly coordinated, broader wave of cyber threats that shook Wall Street during the summer of 2026²².
- Chinese state-affiliated hacking groups more than doubled their attack volume after integrating DeepSeek and other open-source artificial intelligence models into their workflows. According to reports from the Taiwanese cyber intelligence firm TeamT5, threat actors are using these tools to scale operations, automate routine tasks, and accelerate malicious campaigns²³.

¹⁵ <https://www.bloomberg.com/news/articles/2026-08-26/trump-signs-order-to-ban-some-foreign-energy-equipment-from-grid>

¹⁶ <https://www.bloomberg.com/news/articles/2026-09-17/white-house-weighs-us-incubator-for-cyber-research-startups>

¹⁷ <https://www.washingtonpost.com/national-security/2026/07/30/us-spy-agencies-suspect-iran-launched-cyberattack-minnesota-water-facilities/>

¹⁸ <https://www.bloomberg.com/news/articles/2026-07-31/anthropic-openai-cyber-failures-point-to-us-security-risks>

¹⁹ <https://www.axios.com/2026/09/03/openai-critical-infrastructure-cyber-ai-models>

²⁰ <https://www.insideprivacy.com/critical-infrastructure/cisa-submits-final-circia-rule-for-omb-review/>

²¹ <https://news.bostonscientific.com/update-on-recent-cybersecurity-incident>

²² <https://www.bloomberg.com/news/articles/2026-08-21/apollo-reports-data-breach-from-social-engineering-incident>

²³ <https://www.bloomberg.com/news/articles/2026-08-24/chinese-hackers-use-deepseek-to-boost-attacks-researchers-say-mt7o4205>

Quarterly Earnings Recap

Overall, HXRXL companies that beat revenue and earnings estimates in the most recent quarter did so by an average of 2.9% and 13.0% respectively, while those that missed revenues did so by 0.3%. 96.5% of the index weight beat top-line estimates while 100% beat bottom-line estimates. In aggregate, HXRXL companies grew quarterly revenues 25.1% year-over-year. Aggregate quarterly net income surged by 21.9% year-over-year.

	Beats		Misses	
	No. of Firms/Index Weight	Average Beat (%)	No. of Firms/Index Weight	Average Miss (%)
Q3 2026 Revenues	22/96.5%	2.9%	1/3.3%	-0.3%
Q3 2026 Earnings	23/100%	13.0%	0	0

Source: Nasdaq Global Indexes, FactSet data as of September 30, 2026

Index Deletions

- No index additions and deletions in Q3 2026

Top 3 Index Performance Contributors in Q3 2026

Okta^{24,25}

- The stock was up 53% from June 30, 2026 - September 30, 2026.
- The rally was driven by a re-rating of the company around AI-driven identity security, improving bookings/backlog, stronger profitability, and a very strong Q2 FY2027 earnings reaction.
- RPO and current remaining performance obligations (cRPO) grew 17% and 14%, respectively, reflecting solid underlying demand. Expanding enterprise adoption of AI agents is strengthening Okta's longer-term identity-security opportunity, with strong customer interest and a growing pipeline. While AI-agent security is not yet material to FY 2027 results, it could become a more meaningful growth driver from FY 2028 onward.
- Fiscal Q2 2027 revenue grew by 10.6% year-over-year (y/y) to \$805 million. Subscription revenue was \$793 million, an increase of 12% y/y. Net income increased by 73.1% y/y to \$116 million, while net margins increased 521 basis points (bp) y/y to 14.4%.
- Management guided Q3 2027 revenue in the range of \$813-\$817 million. The management raised its FY 2027 guidance and earnings outlook which triggered analysts' upgrades.

²⁴ <https://investor.okta.com/news-and-events/news-releases/news-details/2026/Okta-Announces-Second-Quarter-Fiscal-Year-2027-Financial-Results/default.aspx>

²⁵ Factset, Q2 2027 Transcript

CrowdStrike Holdings^{26,27}

- The stock was up 39% from June 30, 2026 - September 30, 2026.
- The stock's strength was supported by a combination of buy ratings from institutional analysts, robust Q2 year-over-year revenue growth, and ongoing AI-driven demand trends.
- AI-driven security demand was a key catalyst for Q2 outperformance, as enterprises increasingly prioritized protection, governance, and visibility amid the rapid adoption of AI agents. Management expects this structural tailwind to remain durable, supported by strong customer demand and a record Q3 pipeline, prompting another increase in FY 2027 annualized recurring revenue (ARR) growth guidance. The Falcon 2026 product launches and strategic AI-security partnerships with Nvidia, OpenAI, and Anthropic further reinforced the company's competitive positioning in AI-native cybersecurity.
- Fiscal Q2 2027 revenue grew by 25.8% y/y to \$1.5 billion while ARR at \$333 million was up 51% y/y. The robust topline growth contributed to a positive net income of \$5.3 million compared with a loss of \$70.2 million in Q2 2026.
- Management guided Q3 2027 revenue to be in the range of \$1.523-\$1.529 billion.

Cloudflare^{28,29}

- The stock was up 42% from June 30, 2026 - September 30, 2026.
- Cloudflare's stock rally was driven by accelerating revenue growth, a strong Q2 earnings beat, and robust large-customer adoption, alongside growing investor confidence in the company's positioning as a key infrastructure and cybersecurity beneficiary of agentic AI.
- The revenue mix is increasingly shifting toward consumption-based models, which may increase quarterly variability despite stronger pool-of-funds renewals. Partner-led revenue is also expected to expand, particularly across SASE/Zero Trust and Cloudflare OS deployments, potentially exceeding 50% of revenue over the long term.
- Fiscal Q2 2026 revenue grew by 35.9% y/y to \$696 million. Restructuring expenses of \$153 million resulted in a higher net loss of \$170.0 million vs. a loss of \$50.5 million in Q2 2025.
- Management guided to Q3 revenue of approximately \$736-\$737 million.

Bottom 3 Contributors in Q3 2026

A10 Networks^{30,31}

- The stock was down 27% from June 30, 2026 - September 30, 2026.

²⁶ <https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-second-quarter-fiscal-year-2027-financial>

²⁷ Factset, Q2 2027 Transcript

²⁸ <https://cloudflare.net/financials/quarterly-results/default.aspx>

²⁹ Factset, Q2 2026 Transcript

³⁰ <https://investors.fastly.com/news-releases/news-release-details/fastly-announces-record-first-quarter-2026-financial-results>

³¹ Factset, Q1 2026 Transcript

- The stock saw profit-booking by investors after a strong rally from April 2026. The pullback occurred despite solid Q2 revenue growth, raised FY2026 guidance and continued AI/cybersecurity momentum, suggesting that the decline was driven more by valuation and elevated forward expectations.
- Improving service provider pipeline in North America is expected to contribute to results later in 2026. Quality and size yield of enterprise pipeline support growth opportunities into late 2026 and early 2027. The expanded Microsoft partnership should provide an additional source of recurring revenue over the next couple of years. Meanwhile, AI-driven network traffic and security requirements continue to serve as a multi-year growth catalyst.
- Fiscal Q2 2026 revenue grew by 15.5% y/y to \$80.1 million. Net income decreased by 15.7% y/y to \$8.9 million, while net margins decreased 410 basis points (bp) y/y to 11.1%.
- Management guided FY 2026 revenue growth of 12-14% y/y, an increase from previous guidance of 10-12% growth.

Cisco Systems^{32,33,34}

- The stock was down 8% from June 30, 2026 - September 30, 2026.
- The drop was primarily driven by profit-taking from peak valuations, gross margin headwinds from its hardware mix, and analyst downgrades regarding peaked industry growth. Management warned that heavy volumes of lower-margin AI hardware shipments and rising memory costs would remain a persistent headwind into fiscal 2027.
- The company delivered strong Q4 order growth, supported by broad-based demand and accelerating AI infrastructure spending from hyperscalers. AI infrastructure revenue of ~\$4 billion in FY 2026 is projected to increase to \$7.5 billion in FY 2027, an ~88% increase. Hyperscale AI orders totaled \$9.3 billion in FY 2026, roughly 4.5x higher y/y, which may signal a substantial AI demand pipeline³⁵.
- Fiscal Q4 2026 revenue grew by 17.6% y/y to \$17.3 billion. Net income increased by 36.7% y/y to \$3.9 billion, while net margins increased 313 basis points (bps) y/y to 22.4%.
- Management guided FY Q1 2027 revenue is expected to be in the range of \$18-\$18.2 billion. FY 2027 gross margins are expected to face pressure as lower-margin AI hardware becomes a larger portion of revenue, although management plans to mitigate this through operating leverage and disciplined expense management.

Broadcom^{36,37}

- The stock was down 7% from June 30, 2026 - September 30, 2026.
- Lower Q3 gross margins, a softer-than-expected \$34.8 billion Q4 revenue outlook, and a challenging interest rate environment weighed on investor sentiment and contributed to the stock's decline.

³² https://s21.q4cdn.com/812015656/files/doc_earnings/2026/q4/earnings-result/Q4FY26-Press-Release.pdf

³³ https://s21.q4cdn.com/812015656/files/doc_earnings/2026/q4/presentation/Q4FY26-Cisco-Earnings-Slides.pdf

³⁴ Factset, Q4 2026 Transcript

³⁵ <https://www.datacenters.com/news/cisco-s-9-3b-ai-order-boom-why-networking-is-becoming-critical-data-center-infrastructure>

³⁶ <https://investors.broadcom.com/news-releases/news-release-details/broadcom-inc-announces-third-quarter-fiscal-year-2026-financial>

³⁷ Factset, Q3 2026 Transcript

- Large-scale AI deployments by Anthropic, OpenAI, Meta, and Google continue to support Broadcom's AI accelerator and networking businesses, with AI semiconductor revenue projected to reach roughly \$115 billion in FY2027 and \$230 billion in FY2028.
- AI networking revenue is also expected to expand rapidly, broadly tracking the growth in XPU deployments.
- Broadcom's fiscal Q3 2026 revenue rose by 85.5% y/y to \$29.6 billion. EBIT and net margins improved by 54.3% y/y and 216.1% y/y, respectively.
- Management guided FY Q4 2026 revenue of approximately \$34.8 billion. AI semiconductor revenue is expected to accelerate to \$21.7 billion. XPUs and AI networking revenue are expected to triple y/y.

Disclaimer:

Nasdaq®, HXRXL™, and Nasdaq ISE Cyber Security Select™ are trademarks of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. **ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.**

© 2026. Nasdaq, Inc. All Rights Reserved.

Information set forth contains forward-looking statements that involve a number of risks and uncertainties. Nasdaq cautions readers that any forward-looking information is not a guarantee of future performance and that actual results could differ materially from those contained in the forward-looking information. Forward-looking statements can be identified by words such as "will," "may," "could," "likely," "expected," "projected," "forecasts," "plans", and other words and terms of similar meaning. Such forward-looking statements include, but are not limited to, statements related to future activities and results, anticipated effects of artificial intelligence and geopolitical developments on the cybersecurity industry; future revenue, earnings, margins, recurring revenue, customer adoption and business pipelines; and other anticipated industry and company developments. Forward-looking statements involve a number of risks, uncertainties or other factors beyond Nasdaq's control. These risks and uncertainties are detailed in Nasdaq's filings with the U.S. Securities and Exchange Commission, including its annual reports on Form 10-K and quarterly reports on Form 10-Q which are available on Nasdaq's investor relations website at [HYPERLINK "http://ir.nasdaq.com/"](http://ir.nasdaq.com/)<http://ir.nasdaq.com> and the SEC's website at [HYPERLINK "http://www.sec.gov/"](http://www.sec.gov/)www.sec.gov. Nasdaq undertakes no obligation to publicly update any forward-looking statement, whether as a result of new information, future events or otherwise.