Q2 2026 HXRXL™ Cybersecurity Commentary

July 2026

Sanjana Prabhakar, *Index Insights Senior Specialist*

Executive Summary and Performance Commentary

Cybersecurity companies delivered positive price performance in Q2 2026, with the Nasdaq ISE Cyber Security Select™ Index (HXRXL™) up 40.1% for the quarter, outperforming the S&P 500 (14.9%). Of the 23 constituents, 20 names had gains, with 2 names (Tenable Holdings and Palo Alto Networks) experiencing triple digit gains and 16 names experiencing double-digit gains. 3 names experienced losses, with 2 names down more than 10% apiece, including, Fastly (36.8%), which recorded the largest decrease among index constituents, followed by Northrop Grumman (-25.3%).

The S&P 500 currently tracks only 9 constituents that overlap with HXRXL, comprising 5% of its exposure. 14 of HXRXL's constituents (~53.3% of index weight) do not overlap with the S&P 500. The Q2 2026 performance pattern reinforced the divergence described in the prior quarter update: semiconductors remained the most direct and highest-conviction AI beneficiary, cybersecurity continued to trade as a defensive, geopolitically-driven compounder, and software remained under pressure from structural AI-disruption fears — recovering only partially on sentiment shifts rather than fundamental re-rating. Semiconductors were the standout performers of Q2 2026 by a wide margin, with the SOX gaining **+87.8%** — its best quarter on record[1]. The rally appears to be driven by an AI-fueled memory chip boom, as capital expenditures increasingly shifted toward high-bandwidth memory (HBM) and massive supply chain agreements. Software was the clear laggard, posting a modest **+13.2%** gain — a stark contrast to the other two segments. The quarter began with continued selling pressure, as AI-disruption fears weighed heavily on the group. A meaningful intra-quarter recovery began in late May; however, the recovery was uneven and the sector gave back some gains into quarter-end, finishing well below its semiconductor and cybersecurity peers. Cybersecurity was the second-best performing segment of all three technology sectors, with HXRXL gaining **+40.1%** over the quarter. The sector continued to benefit from its non-discretionary, defensive characteristics and geopolitical tailwinds stemming from the US-Iran conflict, which elevated demand for digital resilience and defense-oriented infrastructure. Anthropic's unveiling of its Claude Mythos model — capable of discovering and exploiting software vulnerabilities — may strengthen the structural demand case for cybersecurity. The relative performance of these three segments helps explain HXRXL's Q2 return. HXRXL effectively occupied the middle ground between semiconductors and software during Q2 2026. The index participated in the market's enthusiasm surrounding AI while avoiding many of the business-model risks facing software vendors, resulting in strong relative performance despite remaining well below the gains posted by semiconductor stocks. In a quarter where the dispersion between semis and software was extreme (~75 percentage points between SOX and IGV), HXRXL's exposure produced a return that came in between the two, reflecting its hybrid exposure.

[1] https://www.marketwatch.com/story/why-highflying-chip-stocks-are-suddenly-losing-their-luster-f0659145

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.

Quarterly Earnings Recap

Overall, HXRXL companies that beat revenue and earnings estimates in the most recent quarter did so by an average of 2.7% and 13.5% respectively, while those that missed revenues did so by 0.4%. 92.7% of the index weight beat top-line estimates while **100% beat bottom-line estimates**. In aggregate, HXRXL companies grew quarterly revenues 7.1% year-over-year. **Aggregate quarterly net income surged by 36.2% year-over-year.**

	Beats		Misses	
	No. of Firms/Index Weight	Average Beat (%)	No. of Firms/Index Weight	Average Miss (%)
Q2 2026 Revenues	21/92.7%	2.7%	2/7.3%	-0.4%
Q2 2026 Earnings	23/100%	13.5%	0	0

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

Index Deletions (June 22, 2026)

Netskope (NTSK), a cloud security platform provider which offers network transformation, security modernization and framework solutions was added to the index at a weight of 2.6 %.

Top 3 Index Performance Contributors in Q2 2026

Palo Alto Networks[1,2,3,4]

- The stock was up 113% from March 31, 2026 - June 30, 2026.
- The company reported strong, sustained growth in network security driven by rising AI traffic and expanding data center demand. Q3 added 110 net new platformized customers, including ~20 new net in Identity and Observability. Remaining performance obligation grew 36% y/y to $18.4 billion, including $1.8 billion from CyberArk and Chronosphere. Q3 ARR reached $600 million, up 100% y/y.
- Product segment revenue was $594 million, up 31.1% y/y. Subscription and support segment revenue was $2.4 billion, up 31.2% y/y.
- Fiscal Q3 2026 revenue increased by 31.1% year-over-year (y/y) to $3.0 billion driven by strong platformization momentum. Q3 total revenue includes $388 million from CyberArk and Chronosphere acquisitions. EBIT was -$252 million while EBIT margins declined to -8.4% vs. +9.6% in Q3 2025. Net loss was -$177.0 million, while net margins were -5.9% vs +11.5% in Q3 2025. On a quarter-on-quarter basis, revenue increased by 15.7%. Fiscal Q4 2026 revenue is expected to be in the range of $3.34-$3.36 billion. Non-GAAP diluted EPS is expected to be in the range of $0.96-$0.98 per share.

CrowdStrike Holdings[5,6]

- The stock was up 96% from March 31, 2026 - June 30, 2026.
- The stock rose on strong earnings beat, accelerating growth, rapid growth of AI and resulting increase in cybersecurity spending. CrowdStrike announced a 4:1 stock split, which officially took effect when markets opened on July 2, 2026.
- CrowdStrike delivered strong Q1 2027 results as Annual Recurring Revenue (ARR) grew 24% y/y to $5.51 billion and net new ARR grew 32% y/y to $256 million. The company raised its FY 2027 ARR growth guidance by 520 basis points to 27.7% y/y. CrowdStrike also expanded its strategic position in AI security through Project QuiltWorks, a cybersecurity coalition that includes OpenAI and Anthropic, and announced new collaborations with Intel and IBM.
- Subscription segment revenue was $1.3 billion, up 25.7% y/y. Professional Services segment revenue was $64.8 million, up 23.0% y/y.
- Fiscal Q1 2027 revenue grew by 25.6% y/y to $1.4 billion. Net income came in at $27.8 million vs. a net loss of $104.3 million the previous year. On a q-o-q basis, revenue increased by 6.1%. Fiscal Q2 2027 revenue is expected to be in the range of $1.44-$1.44 billion. Non-GAAP EPS is expected to be in the range of $1.16-$1.17.

Fortinet[7,8]

- The stock was up 88% from March 31, 2026 - June 30, 2026.
- The stock surge was driven by strong earnings and raised full-year guidance, with net income beating estimates by $0.201 (33%) and management forecasting 2026 revenue between $7.7 billion and $7.9 billion.
- The company delivered strong growth, with total billings increasing 31% year-over-year to $2.09 billion, driven by the ongoing convergence of networking and cybersecurity. Unified SASE billings grew 31%, supported by strong demand for SD-WAN and FortiSASE, while AI-driven security operations billings rose 23%. Despite a modest impact from recent pricing changes, the company sees long-term growth supported by AI adoption, vendor consolidation, and technology refresh cycles.
- Product segment revenue was $645.1 million, up 40.5% y/y. Service segment revenue was $1.2 billion, up 11.5% y/y.
- Fiscal Q1 2026 revenue grew by 20.1% y/y to $1.8 billion. On a q-o-q basis, revenue decreased by 2.9%. Net Income increased by 23.3% y/y to $534.5 million while net margins increased by 70 basis points y/y to 28.9%. Fiscal Q2 2026 total revenues are expected to be in the range of $1.83-$1.93 billion. Non-GAAP diluted EPS is expected to be in the range of $0.72-$0.76.

Bottom 3 Contributors in Q2 2026

Fastly[9,10]

- The stock was down 37% from March 31, 2026 - June 30, 2026.
- The stock came under pressure from earnings expectations, future growth prospects, and AI's impact on the software and infrastructure companies.

- The company reported strong momentum, with Remaining Performance Obligations (RPO) increasing 63% y/y to $369 million, including $275 million scheduled for the next 12 months, highlighting strong future revenue visibility. The company's Security suite continues to gain traction among both existing and new customers and is expected to surpass a $200 million annual revenue run rate in FY 2026.
- Fiscal Q1 2026 revenue increased by 19.8% y/y to $173.0 million driven by continued success in go-to market upsell and cross-sell motions within expanded product platform. Net loss was lower at $20.5 million vs. a loss of $39.1 million in Q1 2025. On a q-o-q basis, revenue increased by 1.1%. Fiscal Q2 2026 revenue is expected to be in the range of $170-$176 million. Non-GAAP EPS is expected to be in the range of $0.05-$0.08.

Northrop Grumman Corporation[11,12]

- The stock was down 25% from March 31, 2026 - June 30, 2026.
- Investors reconsidered their defense stock holdings as Middle East tensions eased. Sentiment was further weakened in June by reports that U.S. policymakers were exploring measures to limit defense contractors' ability to conduct stock buybacks and pay dividends.
- The company reported strong Q1 performance, securing $9.8 billion in net awards and growing its backlog to $96 billion, driven by demand for U.S. nuclear triad modernization programs. Its portfolio remains closely aligned with priorities in the proposed FY 2027 U.S. defense budget, which includes a $1.5 trillion funding request, significantly above current levels.
- Fiscal Q1 2026 revenue grew by 4.4% y/y to $9.9 billion. Net income increased by 81.9% to $875 million while net margins improved by 380 basis points y/y to 8.9% in Q1 2026. On a q-o-q basis, revenue decreased by 15.6%.

Checkpoint Software Technologies[13,14]

- The stock was down 8% from March 31, 2026 - June 30, 2026.
- The stock came under pressure after the company reported a Q1 revenue miss and lowered its FY 2026 revenue guidance to $2.77–$2.85 billion, down from the previous $2.83–$2.95 billion range. Investor concerns were amplified by ongoing pressure in its firewall business, weaker growth prospects highlighted by analysts, and Bank of America's downgrade in May 2026.
- Fiscal Q1 2026 revenue grew by 4.8% y/y to $668.4 million. Net income grew by 0.4% to $191.6 million while net margins declined by 130 basis points y/y to 28.7% in Q1 2026. On a q-o-q basis, revenue decreased by 10.3%. Fiscal Q2 2026 revenue is expected to be in the range of $660-$690 million. Non-GAAP EPS is expected to be in the range of $2.40-$2.50, GAAP EPS is expected to be $0.7 less.

Cybersecurity Industry Outlook and Top Headlines from Q2 2026

- Forrester forecasts cybersecurity spending to grow at a CAGR of 14.4% between 2024 through 2029 to $302.5 billion by 2029[2]. The cost of cybercrimes for the world economy was about $10.5 trillion in 2025, with current projections indicating that it could exceed $11-$12 trillion per year in 2026 as ransomware, data

[2] https://www.forrester.com/report/global-cybersecurity-market-forecast-2024-to-2029/RES186163

theft and AI-driven attacks continue to scale. The average cost of a data breach was $4.44 million in 2026, with the cost remaining the highest in the U.S. at about $10.2 million[3].

- In June 2026, the Cybersecurity and Infrastructure Security Agency (CISA) ordered federal agencies to prioritize security updates based on risk, with requirements to patch critical vulnerabilities in as little as 3 days[4].
- On June 2, 2026, the White House issued an executive order (EO), titled "Promoting Advanced Artificial Intelligence Innovation and Security," establishing a voluntary framework permitting developers of certain advanced artificial intelligence (AI) models to voluntarily provide the federal government with model access prior to public release for cybersecurity and national security assessments[5].
- Intelligence agencies warn that malicious hackers may actively deploying "agentic" (autonomous) AI. These systems conduct reconnaissance and execute attacks with reduced human oversight, speeding up the threat lifecycle and forcing federal agencies to shorten their vulnerability fix windows, in some cases to just three days[6].
- Major AI announcements from Anthropic (such as Claude Mythos) were caught in the crosshairs of national security directives. Cybersecurity executives are urging the US government to ease these restrictions so security professionals can leverage the models for defense[7].
- The FBI and Google announced the takedown of Outsider Enterprise, a large phishing-as-a-service (PhaaS) platform that caused billions of dollars in losses. The takedown action, part of the FBI's Operation Riptide, an effort to disrupt cybercriminal networks, led to the seizure of domains linked to Outsider Enterprise's administrative servers and of a Shopify e-commerce storefront and account employed for phishing kit testing[8].
- In June 2026, the Iran-linked threat actor Handala claimed to have hacked California Water Service (Cal Water) and published 5 gigabytes of data allegedly stolen from the US water utility. While the level of access Handala had has not been confirmed, threat intelligence company Dataminr says the threat actor likely hacked into Cal Water's RTKBase instance, a GNSS base station platform, and then moved laterally to a billing system[9].
- In June 2026, Novo Nordisk suffered a cybersecurity incident where unauthorized actors accessed internal systems and copied clinical trial and proprietary data. The company confirmed the breach, emphasizing that affected clinical trial data was pseudonymized—containing only patient IDs, birth years, sex, and health metrics, but no direct identifiers like names[10].
- Between May 27 and June 9, the data extortion group ShinyHunters infiltrated Oracle's PeopleSoft applications, which are used heavily by colleges, universities, and other enterprise clients for human capital

[3] https://app.stationx.net/articles/cyber-security-breach-statistics
[4] https://www.cisa.gov/news-events/news/cisa-issues-new-directive-improving-how-federal-agencies-prioritize-mitigation-cyber-vulnerabilities
[5] https://www.hklaw.com/en/insights/publications/2026/06/executive-order-on-artificial-intelligence-expands-cybersecurity
[6] https://www.govconwire.com/articles/chuck-brooks-govcon-expert-ai-cyber-threats-cisa-security-strategy
[7] https://www.reuters.com/legal/litigation/cyber-leaders-urge-us-lift-curbs-anthropics-security-models-2026-06-15/
[8] https://cyberscoop.com/outsider-cybercrime-network-takedown-china-fbi-google-lumen/
[9] https://industrialcyber.co/utilities-energy-power-water-waste/iran-linked-handala-group-targets-cal-water-exposing-potential-pathways-between-it-and-ot-environments/
[10] https://www.americanpharmaceuticalreview.com/1315-News/626142-Novo-Nordisk-Hit-By-Cyberattack-Non-Public-Data-Copied-But-Operations-Continue/

management. Google's Threat Intelligence Group (GTIG) and Mandiant issued alerts to affected higher-education institutions, as some were compromised and had their data leaked publicly following the attack[11].

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", 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. 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 and the SEC's website at HYPERLINK "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.

[1] https://investors.paloaltonetworks.com/news-releases/news-release-details/palo-alto-networks-reports-fiscal-third-quarter-2026-financial
[2] https://paloaltonetworks.gcs-web.com/static-files/601be8fb-414c-4fbe-be1b-daf0b8e8467d
[3] https://paloaltonetworks.gcs-web.com/static-files/67ce9226-4fe0-43cd-b83e-42efb035f38c
[4] Factset, Q3 2026 Transcript
[5] https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-first-quarter-fiscal-year-2027-financial
[6] Factset, Q1 2027 Transcript
[7] https://investor.fortinet.com/static-files/98008e24-af31-46aa-a962-375e653af2a3
[8] Factset, Q1 2026 Transcript
[9] https://investors.fastly.com/news-releases/news-release-details/fastly-announces-record-first-quarter-2026-financial-results
[10] Factset, Q1 2026 Transcript
[11] https://investor.northropgrumman.com/static-files/6791abf6-1899-405a-8f0a-4d8188a52d10
[12] Factset, Q1 2026 Transcript
[13] https://www.checkpoint.com/downloads/investor/check-point-q1-2026-presentation.pdf?v=1.0
[14] Factset, Q1 2026 Transcript

[11] https://www.govtech.com/education/higher-ed/cyber-attack-on-oracle-exposes-data-of-higher-ed-clients