

Q2 2024 Cyber Security Update

Cyber Security News/Insight

- Revenue in the global cybersecurity market is expected to reach \$185.7 billion in 2024, with an annual growth rate of 11.0%¹. The security services segment is expected to contribute \$97.3 billion and cyber solutions is expected to contribute the rest.² During the period 2024-2029, revenue is expected to show an annual growth rate of 7.9%, resulting in a total market of \$271.9 billion by 2029³. This growth is expected to be led by the cyber solutions segment with an estimated CAGR of 10.9% and a resultant market size of \$148.3 billion⁴ by 2029, followed by the security services segment at a lower rate of 4.9% and a resultant market size of \$123.6 billion by 2029⁵. The largest market for cybersecurity is the U.S. with a market size of \$81.4 billion in 2024. It is expected to grow at a CAGR of 9.4% during the period 2024-2029 to a market size of \$116.2 billion by 2029.⁶
- According to Statista, cybercrimes are expected to cost about \$9.2 trillion in 2024 with the cost expected to grow to \$13.8 trillion in 2028.⁷ Based on a new report from the International Monetary Fund (IMF), global financial stability is threatened by the increasing frequency and sophistication of cyberattacks.⁸
- In April, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) publicly issued Emergency Directive 24-02 in response to a recent campaign by Russian state-sponsored cyber actor Midnight Blizzard targeting Microsoft corporate email accounts and potentially accessing correspondence with Federal Civilian Executive Branch (FCEB) agencies.⁹
- In May 2024, Germany announced that cybercrime by foreign actors rose 28% y/y in 2023. Furthermore, it has accused Russia of launching cyberattacks on German aerospace & defense firms, and the ruling party.¹⁰
- The 2024 Paris Olympic Games are facing an "unprecedented level" of cyber threats, according to the authorities. During the previous Olympic Games in Tokyo, it endured an estimated 450 million cyberattacks, according to technology giant Cisco. The company, which is an official partner for Paris 2024, says it expects eight times more attacks than the previous games in Tokyo.¹¹

Cybersecurity – Notable Ransomware Attacks and Breaches in Q2 2024

- On June 19, there were back-back cybersecurity attacks on a software company, CDK Global, that provides software for auto dealerships across the U.S. Nearly 15,000 car sellers that depend on CDK's dealer management software were affected. The company was forced to stop access to its core product, known as the dealer management system. Hackers demanded tens of millions of dollars in ransom. CDK issued a notice to customers that outside parties were reaching out to customers, while not naming the entity behind the intrusion.
- On June 4, Australian rare-earth metals producer Northern Minerals (ASX: NTU) announced that it was a victim of a cyberattack in March 2024 by the BianLian ransomware gang. The cybergang claimed to have exfiltrated project and mining research data, R&D and financial data, shareholder and investor information, the personal information of employees, and corporate email archives.¹²

- On May 9, Dell Technologies started informing millions of customers that data including full names and physical addresses – in addition to order service tags, item description, dates of orders and customer warranty information – was stolen during a security incident.¹³
- On May 8, Ascension, a non-profit that runs one of the largest healthcare systems in the U.S., was struggling to contain a cyberattack that caused disruption at hospitals throughout the country. Affected systems include electronic health records, the MyChart patient communication portal, certain phone systems, and systems used for ordering tests, procedures, and medications.¹⁴
- On May 5, the City of Wichita, Kansas shut down its computer network after becoming a victim of cyberattack by the Lockbit gang. The systems were encrypted with malware and it's unclear if any data was compromised, but the attack impacted water utility, municipal court, cultural, and public transportation payments.^{15,16}
- On April 16, the United Nations Development Programme (UNDP) announced it is investigating a ransomware attack that occurred on March 27 with hackers stealing sensitive data. While UNDP has not shared any additional information on the incident, it appears to be the handiwork of a group named 8base as they listed UNDP on their Tor-based website.¹⁷
- On April 16, hospitality chain Omni Hotels & Resorts confirmed that a cyberattack on March 29 resulted in customer information being stolen and disruptions across all properties. The attack by the Daixin Team ransomware group claimed to have stolen records from 2017 belonging to 3.5 million visitors. The gang demanded \$2 million in ransom money.¹⁸ On March 30, Japan-based optics giant Hoya, one of the largest global manufacturers of optical products, suffered a cyberattack that caused some of its production plants and business divisions to go offline. The company received a \$10 million ransomware demand from the Hunters International ransomware gang who claimed to have stolen 2TB of data.^{19,20}
- On March 30, AT&T (NYSE: T) disclosed that the data including social security numbers and other personal information of approximately 73 million current and former customers were exposed on the dark web. The company revealed the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders. AT&T is yet to determine if the source of data was AT&T or one of its vendors.²¹

New Products

- In June 2024, Darktrace (NASDAQ: DARK) launched its new service offering, Darktrace Managed Detection & Response (MDR), which combines its detection and response capabilities with expertise of its global analyst team.²²
- In May 2024, CrowdStrike Holdings (NASDAQ: CRWD) announced new CrowdStrike Falcon Next-Gen SIEM innovations, which modernize SOC operations with a single, unified platform to deliver full visibility and protection across all workloads.²³
- In May 2024, Palo Alto Networks (NASDAQ: PANW) introduced new security solutions infused with Precision AI to help enterprises tackle AI-generated attacks and effectively secure AI-by-design.²⁴

Cybersecurity – M&A and IPO Activity in Q2 2024

Inside NQCYBR Index Activity:

- On June 10, Fortinet (NASDAQ: FTNT) announced plans to acquire Lacework, a late-stage cloud security startup. Fortinet said the plan is to integrate Lacework's CNAPP product into the Fortinet Unified SASE offering.²⁵
- On May 7, cloud and security giant Akamai (NASDAQ: AKAM) announced plans to acquire U.S.-based application programming interface (API) protection company Noname Security for \$450 million. The deal is expected to close in the second quarter of 2024 and Akamai expects the transaction to deliver roughly \$20 million in revenue for the fiscal year 2024.²⁶
- On April 26, PE firm Thoma Bravo agreed to acquire UK-based cybersecurity firm Darktrace (NASDAQ: DARK) for ~\$5.32 billion in cash, representing a 44% premium to the volume-weighted average price per share for the three-month period ended April 25, 2024. The acquisition represents an EV / Revenue multiple of 8.1 times, and EV / Adjusted EBITDA multiple of 34.2 times.²⁷

Top 3 Contributors to NQCYBR Index Performance in Q2 2024

Broadcom^{28, 29, 30}

- Stock price was up 21.1% from March 28, 2024 - June 28, 2024.
- Broadcom's performance was driven by strong results across its growing AI product portfolio and legacy VMware businesses with strong cybersecurity exposure. Q2 2024 revenue increased by 43% y/y to \$12.5 bn. Excluding VMware, revenue was up 12% y/y. Adjusted EBITDA increased by 31% y/y to \$7.4 bn. However, GAAP net profit was down to \$2.1 bn from \$3.5 bn in Q2 2023. Non-GAAP net profit increased to \$5.4 bn from \$4.5 bn in Q2 2023. Q2 Free Cash Flow (FCF) increased by 1.6% y/y to \$4.4 bn. Excluding restructuring and integration costs, FCF was up 18% y/y to \$5.3 bn.
- Raised FY 2024 guidance for consolidated revenue to \$51 bn and adjusted EBITDA to 61% of revenue.

CrowdStrike^{31, 32}

- Stock price was up 19.5% from March 28, 2024 - June 28, 2024.
- CrowdStrike's stock rose due to a strong start to their fiscal year 2025 and strong guidance. Additionally, it is largely viewed as a GenAI beneficiary. Fiscal Q1 2025 ended with an ARR of \$3.65 bn and new net ARR of \$212 mn (+22% y/y growth). Operating income was \$199 mn and operating margin of 22% was 5% above the corresponding period last year. FCF was \$322 mn and up 42% y/y.
- Subscription revenue was \$872 mn and was up 34% y/y while total revenue grew 33% to \$921 mn. Non-GAAP subscription gross margin was >80%.
- Guided FCF margin of 31%-33% of revenue for FY 2025 and non-GAAP operating margin of 28%-32%.

Palo Alto Networks³³

- Stock price was up 19.3% from March 28, 2024 - June 28, 2024.

- Palo Alto's stock rose due to strong quarterly results and acceleration in bookings growth. The company's ARR came in ahead of consensus. Operating margins expanded to 25.6%, ahead of Street's 25%. FCF also beat Street's estimates.
- Revenue grew 15% year-over-year and beat high-end of guidance, while ARR and Bookings also beat consensus.
- Over the last three years, PANW generated a FCF CAGR of greater than 25%.
- Additionally, long-term operating margins have been revised upward to 28%-29% in FY 2026 and low 30% long-term.

Bottom 3 Contributors in Q2 2024

Open Text Corp³⁴

- Stock price was down 22.6% from March 28, 2024 - June 28, 2024. Stock came under pressure due to preliminary FY 2025 guidance and cloud growth coming in weaker than expected.
- Revenue came in at \$1.45 bn for Q3 2024, up 16.3% y/y, with annual recurring revenue coming at \$1.2 billion, up 13.3% y/y. Cloud revenue grew 4% y/y. Enterprise cloud bookings grew 53% y/y, driven by greater deal duration and customer contract size. EBITDA margin of 32%, was down q/q, with cost savings post Micro Focus acquisition.

Trend Micro³⁵

- Stock price was down 19.8% from March 28, 2024 - June 28, 2024.
- Trend Micro's stock came under pressure due to headwinds from heightened competition and sluggish sales growth in the US. Additionally, certain businesses came under pressure including the IT infrastructure business in Japan, cloud operations in United States and IT infrastructure security in Europe.
- There was also a lack of positive catalysts on the horizon.

Akamai Technologies³⁶

- Stock price was down 17.2% from March 28, 2024 - June 28, 2024.
- Akamai's stock came under pressure as its first quarter EPS missed analyst estimates. Additionally, there was weakness in its content-delivery network business. Revenues from delivery solutions slid 11% year-over-year to \$351.8 million while security solutions and compute sales reported an increase of 21% and 25% respectively.
- Additionally, its second quarter revenue and adjusted EPS revenue came below estimates. For full year 2024, revenue is expected to grow 6%-8% year-over-year and adjusted EPS expected to rise 7% to 11%.

Disclaimer:

Nasdaq® is a registered trademark 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.

© 2024. Nasdaq, Inc. All Rights Reserved.

-
- ¹ <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>
 - ² <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>
 - ³ <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>
 - ⁴ <https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/worldwide>
 - ⁵ <https://www.statista.com/outlook/tmo/cybersecurity/security-services/worldwide>
 - ⁶ <https://www.statista.com/outlook/tmo/cybersecurity/united-states>
 - ⁷ <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>
 - ⁸ <https://es.weforum.org/agenda/2024/06/la-estabilidad-financiera-mundial-en-peligro-debido-a-las-ciberamenazas-advierde-el-fmi-lo-que-hay-que-saber/>
 - ⁹ <https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-immediately-mitigate-significant-risk-russian-state-sponsored-cyber>
 - ¹⁰ <https://www.usnews.com/news/world/articles/2024-05-13/germany-says-cybercrime-by-foreign-actors-rose-by-28-in-2023>
 - ¹¹ <https://www.weforum.org/agenda/2024/06/paris-olympics-2024-cybersecurity-experts-cyber-threats/>
 - ¹² <https://www.securityweek.com/ransomware-gang-leaks-data-from-australian-mining-company/>
 - ¹³ <https://www.securityweek.com/dell-says-customer-names-addresses-stolen-in-database-breach/>
 - ¹⁴ <https://www.securityweek.com/healthcare-giant-ascension-hacked-hospitals-diverting-emergency-service/>
 - ¹⁵ <https://www.securityweek.com/city-of-wichita-shuts-down-network-following-ransomware-attack/>
 - ¹⁶ <https://www.securityweek.com/lockbit-takes-credit-for-city-of-wichita-ransomware-attack/>
 - ¹⁷ <https://www.securityweek.com/united-nations-agency-investigating-ransomware-attack-involving-data-theft/>
 - ¹⁸ <https://www.securityweek.com/omni-hotels-says-personal-information-stolen-in-ransomware-attack/>
 - ¹⁹ <https://www.bleepingcomputer.com/news/security/hoyas-optics-production-and-orders-disrupted-by-cyberattack/>
 - ²⁰ <https://www.bleepingcomputer.com/news/security/optics-giant-hoya-hit-with-10-million-ransomware-demand/>
 - ²¹ <https://www.securityweek.com/att-says-data-on-73-million-customers-leaked-on-dark-web/>
 - ²² <https://darktrace.com/news/darktrace-launches-managed-detection-response-service-to-bolster-security-operations>
 - ²³ <https://www.crowdstrike.com/press-releases/crowdstrike-delivers-falcon-next-gen-siem-innovations/>
 - ²⁴ <https://investors.paloaltonetworks.com/news-releases/news-release-details/palo-alto-networks-launches-new-security-solutions-infused>
 - ²⁵ <https://www.securityweek.com/fortinet-expands-cloud-security-portfolio-with-lacework-acquisition/>
 - ²⁶ <https://www.securityweek.com/akamai-to-acquire-api-protection-startup-noname-security-for-450-million/>
 - ²⁷ <https://www.securityweek.com/darktrace-to-be-taken-private-in-5-3-billion-sale-to-thoma-bravo/>
 - ²⁸ <https://investors.broadcom.com/financial-information/quarterly-results>

-
- ²⁹ <https://investors.broadcom.com/news-releases/news-release-details/broadcom-inc-announces-second-quarter-fiscal-year-2024-financial>
- ³⁰ <https://investors.broadcom.com/static-files/602c2fd3-89a0-436f-b638-4890f20feda7>
- ³¹ <https://ir.crowdstrike.com/financial-information/quarterly-results>
- ³² <https://ir.crowdstrike.com/static-files/8ae4af6f-8d70-4c59-822d-c78b2bd43327>
- ³³ <https://ir.darktrace.com/financial-results>
- ³⁴ https://s23.q4cdn.com/197378439/files/doc_financials/2024/q1/OpenText-Reports-First-Quarter-Fiscal-Year-2024-Financial-Results.pdf
- ³⁵ https://www.trendmicro.com/en_us/about/investor-relations.html
- ³⁶ <https://www.ir.akamai.com/static-files/510a13eb-3a40-48cc-8cc9-12b8817f5e64>