Nasdaq Global Indexes
June 2025

Q2 2025 Cybersecurity Update

Cybersecurity News/Insight

- Revenue in the global cybersecurity market is expected to grow to $203.0 billion in 2025, with an annual growth rate of 9.3%[1]. The security services segment is expected to contribute $103.1 billion to the total revenues, with the rest driven from cyber solutions.[2] According to Statista, during the period 2025-2029, revenue is expected to show an annual growth rate of 7.6%, resulting in a total market size of $271.9 billion by 2029[3]. This growth is expected to be led by the cyber solution segment with an estimated CAGR of 10.4% and a resultant market size of $148.3 billion[4] by 2029, followed by the security services segment at a lower rate of 4.6% and a resultant market size of $123.6 billion by 2029[5]. Region-wise, the largest market for cybersecurity, the U.S. is expected to have a market size of $88.3 billion in 2025 and is expected to grow at a compound annual growth rate (CAGR) of 7.1% during the period 2025-2029 to a market size of $116.2 billion by 2029.[6]
- Globally IT budgets are forecast to reach $290 billion this year, according to the research body Celent. Banks are projected to spend $32 billion on cybersecurity by December 2025, and, according to EY, banks are expected to allocate 11% of their IT budgets to cybersecurity in 2025.[7]
- In April 2025, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) joined the National Security Agency (NSA) and other government and international partners to release a joint Cybersecurity Advisory (CSA) that warns organizations, internet service providers (ISPs), and cybersecurity service providers about fast flux enabled malicious activities that consistently evade detection. The CSA also provides recommended actions to defend against fast flux.[8]
- In June 2025, U.S. President Trump signed an executive order which modifies the previous administration’s cybersecurity directives. Some commenters believe this order signals a broader realignment of federal cybersecurity priorities, including a shift in focus away from federal digital identity initiatives and revision of compliance-heavy software security mandates.[9]
- In June 2025, European Union (EU) member states adopted a revised blueprint for cybersecurity crisis management recommended by the European Union Agency for Cybersecurity (ENISA).[10] The revised blueprint is expected to strengthen the response to large scale incidents and crisis in the EU.[11]
- In June 2025, Microsoft offered a cybersecurity program free of charge to European governments to bolster their defenses against cyber threats, including those enhanced by artificial intelligence (AI).[12] The program aims to boost intelligence-sharing on AI-based threats and helps to prevent and disrupt attacks. Recently, cyberattacks on EU have increased, with many linked to state-sponsored actors from China, Iran, North Korea and Russia.[13]
- In June 2025, Canada’s cybersecurity agency and the U.S. FBI have warned about Chinese hackers attacking telecom services in Canada.[14] The joint bulletin urged organizations to strengthen their networks against threats posed by Typhoon, a hacking group with links to China.

Cybersecurity – Notable Ransomware Attacks and Breaches in Q2 2025

- On May 28, software maker MathWorks confirmed that a systems outage at the company on May 18 was the result of a ransomware attack that impacted IT systems. Services were slowly restored, starting with MATLAB Online and MATLAB Mobile. Many of their applications remained offline or were operating in a degraded state.[15]
- On May 28, data broker giant LexisNexis Risk Solutions (LNRS) notified more than 364,000 people that their personal information was stolen in a December 2024 data breach. The breach was discovered on April 1 after unknown third party claiming to have accessed certain information belonging to LNRS. Personal information stolen includes names, dates of birth, phone numbers, email addresses, Social Security numbers, and driver's license numbers.[16]
- On May 23, Canadian electric utility Nova Scotia Power admitted to a ransomware attack. The hackers gained access to personal information and important data such as driver's license numbers, Social Insurance numbers, and bank account numbers shared for pre-authorized payments. Other information such as power consumption, service requests, payment, billing, and credit history was compromised. The company highlighted that the incident did not cause any disruption to electricity generation, transmission and distribution facilities.[17]
- On May 21, Kettering Health canceled inpatient and outpatient procedures as it dealt with a system-wide outage caused by a ransomware attack. The Interlock ransomware gang was responsible for the incident and leaked 941 Gb of stolen data indicating the ransom was not paid.[18,19]
- On May 15, Coinbase Global (Nasdaq: COIN) disclosed a data breach after rogue contractors were bribed to leak customer data. According to a Securityweek report, management rejected a $20 million ransom demand from the hackers and instead set-up a $20 million reward fund for information leading to the hackers. The attackers had paid rogue contractors in non-U.S. support centers to copy information they were already authorized to view. The stolen data includes customer names, addresses, phone numbers, email addresses, the last four digits of Social Security numbers, and masked bank-account numbers and related identifiers. In its SEC filing the company pegged the preliminary cost of remediation and reimbursements at between $180 million and $400 million.[20]
- On May 14, Nucor (NYSE: NUE) disclosed that a cyberattack disrupted production at several locations. As of the date of this report, the identity of the attacker is not yet known, and the company has not revealed if any data was stolen.[21]
- On May 5, the DragonForce ransomware group claimed responsibility for the attack on three U.K.-based retailers namely Co-op, Harrods, and Marks & Spencer-M&S (LON: MKS) over a span of two weeks. M&S was the first to get hit as they suspended online purchases. Harrods notified users that its website and stores were operating normally. Co-op confirmed the attack affected its back office and call center services and customer data was stolen.[22]
- On April 26, Hitachi Vantara, a subsidiary of conglomerate Hitachi (TYO: 6501) was forced to take servers offline to contain an Akira ransomware attack that disrupted some of their systems. The attack has affected multiple projects owned by government entities.[23]
- On April 12, kidney dialysis services provider DaVita (NYSE: DVA) fell victim to a cyberattack which disrupted some of its operations. The company activated its containment measures but did not reveal the identity of the attacker and if any data was stolen.[24]

- On April 9, the Oregon Department of Environmental Quality (DEQ), the regulatory agency in charge of the quality of air, land and water in the state, revealed that a cyberattack forced them to shut down networks as prevention measures. The Rhysida ransomware group took credit for the attack and claimed to have stolen 2.5 Tb of data demanding $2.5 million. The DEQ refuses to confirm or deny if any data was stolen and has not engaged in any ransom discussions.[25,26]
- On April 9, Sensata Technologies (NYSE: ST) revealed that a ransomware attack on April 6 disrupted its operations including shipping, receiving and production. Files on some devices were encrypted while there is evidence that files were stolen.[27]

New Products

- In April 2025, Cloudflare (Nasdaq: NET) announced several new offerings to accelerate the development of AI agents.[28] This offering enables developers to easily build and deploy AI agents with the industry's first remote Model Context Protocol (MCP) server. It also enables developers to build agents in minutes, rather than months, simply, affordably, and at scale.[29] Furthermore, Cloudflare rolled out Workers VPC and Workers VPC Private Link, new solutions that enable developers to build secure, global cross-cloud applications on Cloudflare Workers.[30]
- In April 2025, Broadcom Inc. (Nasdaq: AVGO) announced Incident Prediction, an industry-first security capability that extends adaptive protection, a unique feature of Symantec Endpoint Security Complete (SES-C), by leveraging AI to identify and disrupt living-off-the land (LOTL) attacks and other cyberthreats.[31] In June 2025, the company announced general availability of the newest investment made to VMware Tanzu CloudHealth, a comprehensive new user experience that delivers a suite of feature enhancements and new AI-powered features like Intelligent Assist and Smart Summary.[32]
- In April 2025, CrowdStrike (Nasdaq: CRWD) introduced Falcon Adversary OverWatch Next-Gen SIEM, the first solution to bring managed threat hunting to third-party data. This extends the visibility of CrowdStrike's threat hunters into unmanaged attack surfaces adversaries have long exploited.[33] It also introduced new Falcon Data Protection innovations, enabling security teams to protect sensitive data across endpoints, cloud environments and GenAI and SaaS applications to prevent exfiltration by insiders and identity-based attackers.[34]
- In April 2025, Rubrik (Nasdaq: RBRK) introduced a new product, Identity Resilience, designed to secure the entire identity landscape alongside data. Identity Resilience aims to protect the most common entry points for attackers – human and non-human identities (NHIs) – to help organizations maintain operations with minimal downtime.[35]
- In April 2025, Palo Alto Networks (Nasdaq: PANW) released Cortex XSIAM 3.0, the next evolution of its SecOps platform, bolstered with proactive exposure management and advanced email security, enabling customers to further consolidate on Cortex for significantly better, faster and more cost-effective security operations.[36] It also introduced Prisma AIRS, an AI security platform that serves as the cornerstone for AI protection, designed to protect the entire enterprise AI ecosystem – AI apps, agents, models, and data at every step.[37]

Cybersecurity – M&A and IPO Activity in Q2 2025

- On May 27, Zscaler (Nasdaq: ZS) announced plans to buy managed detection and response (MDR) specialist Red Canary for $675 million, valuing Red Canary at ~5.7x of its $140 million ARR. Red Canary has raised total funds of $135 million including $81 million in Series C funding in 2021. Zscaler plans to add Red Canary's capabilities to triage that telemetry, chase down alerts and, when necessary, put hands on keyboards to remediate live incidents. Red Canary acts as a natural expansion for Zscaler's entry into managed detection and response and threat intelligence. The deal is reportedly expected to close in August 2025 subject to regulatory approvals.[38,39]
- On April 28, Palo Alto (Nasdaq: PANW) confirmed its intention to acquire U.S.-based AI security company Protect AI. Protect AI has developed a platform that enables organizations to secure AI models, to conduct AI red teaming, and to ensure AI runtime security. Palo Alto said the acquisition will enhance its Prisma AIRS AI security platform. Israeli news website Globes previously reported that its sources had estimated the deal at $650-700 million though Palo Alto has not shared any financial information. In August 2024, Protect AI had raised $60 million in Series B funding. The deal is reportedly expected to close in Q1 2026.[40]
- On May 28, Leidos Holdings (NYSE: LDOS) announced that it acquired Kudu Dynamics for $300 million in cash. Kudo will accelerate Leidos' strategy for AI-enabled offensive cyber, electromagnetic spectrum operations and vulnerability research. Kudu Dynamics has rapidly grown its work across the Department of Defense, leading the industry in automated targeting, scalable hardware reverse engineering and the generation of other non-kinetic effects.[41]
- On May 15, Proofpoint announced that it is buying Germany-based Microsoft 365 security solutions provider Hornetsecurity. The company provides email security, user protection, impersonation protection, enterprise data loss prevention, insider threat management, data security posture management (DSPM), and security awareness products. Financial terms were not disclosed but CNBC reported the deal value at $1 billion.[42]
- On March 18, Google (Nasdaq: GOOG) announced to acquire cloud security Wiz in a $32 billion all-cash deal. Wiz will be part of Google Cloud and help to accelerate two large and growing trends in the AI era: improved cloud security and the ability to use multiple clouds (multicloud). Wiz has developed solutions designed to scan enterprise cloud deployments to find and proactively fix security flaws that could pose a risk to organizations.[43]

Venture Capital and Private Equity Activity:

- On June 11, U.S.-based autonomous security provider Horizon3.ai announced that it raised $100 million in Series D finding and was led by NEA, with additional support from 9Yards Capital, Craft Ventures, and SignalFire. The total funds raised by the company stands at $178.5 million. Their NodeZero platform harvests information on exploitable CVEs, misconfigurations, product defaults, ineffective security controls, and exposed credentials, and provides security teams with proof of exploit, enabling them to visualize how attackers could compromise their systems.[44]
- On June 10, U.S.-based security automation firm Swimlane announced it raised $45 million from Energy Impact Partners and Activate Capital, with additional support from Trinity Capital. The total amount raised by the firm stood at $215 million. Swimlane has built a cybersecurity platform that leverages agentic AI and automation to resolve security, IT/OT operations, and compliance issues.[45]

- On June 3, Israel-based microsegmentation firm Zero Networks announced it raised $55 million in Series C funding which was led by Highland Europe, with additional support from previous investors F2 Venture Capital, PICO Venture Partners, Venrock, and U.S. Venture Partners (USVP). That brings the total amount raised to over $100 million. Zero Networks helps organizations secure their networks through microsegmentation, preventing threat actors from moving laterally after initial compromise.[46]
- On April 23, software supply chain security solutions provider Endor Labs announced that it raised $93 million in Series B funding led by DFJ Growth, with participation from Salesforce Ventures, Lightspeed Venture Partners, Coatue, Dell Technologies Capital, Section 32, and Citi Ventures. Endor Labs previously raised $70 million in a Series A funding round and more than $25 million in seed funding. The investment will support the expanded AppSec platform.[47]
- On April 21, Exaforce raised $75 million in a Series A funding led by Khosla Ventures and Mayfield apart from other investors like Thomvest and Touring Capital. Exaforce's product blends large language models with semantic, statistical, and behavioral models to sift through vast amounts of logs, cloud telemetry, and threat data to deliver enhanced accuracy and repeatability in threat detection and response and is designed to cut down manual SOC tasks by a factor of ten.[48]
- On March 31, ReliaQuest announced that it raised $500 million in a new growth funding round led by EQT, KKR and FTV Capital, with participation from Ten Eleven Ventures and Finback Investment Partners. This takes the total funding to over $830 million and values ReliaQuest at $3.4 billion. ReliaQuest has developed an AI-powered platform that integrates with more than 200 third-party cybersecurity tools, enabling security teams to quickly detect, contain, investigate, and respond to cyber threats and leverages agentic AI to operate and learn autonomously. ReliaQuest claims to have more than 1,000 customers with an annual recurring revenue that surpasses $300 million.[49]
- On March 19, Real-time information discovery platform Dataminr announced that it raised $85 million, bringing the total funds raised to over $1 billion. The new investment, a combination of convertible financing and credit, coming from NightDragon and HSBC, will allow the firm to advance its generative AI and agentic AI capabilities. Powered by AI, Dataminr has built a platform that monitors events, risks, and threats to provide real-time information to customers.[50]

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.

[1] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[2] Id.
[3] Id.
[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.theguardian.com/business/2025/jun/15/uk-banks-hackers-attacks-cybersecurity
[8] https://www.cisa.gov/news-events/news/cisa-and-partners-issue-fast-flux-cybersecurity-advisory
[9] https://www.forbes.com/sites/emilsayegh/2025/06/07/trump-drops-a-cybersecurity-bombshell-with-biden-era-policy-reversal/
[10] https://enisa.europa.eu/news/new-cyber-blueprint-to-scale-up-the-eu-cybersecurity-crisis-management
[11] https://enisa.europa.eu/news/new-cyber-blueprint-to-scale-up-the-eu-cybersecurity-crisis-management
[12] https://www.reuters.com/sustainability/boards-policy-regulation/microsoft-offers-boost-european-governments-cybersecurity-free-2025-06-04/
[13] https://www.reuters.com/sustainability/boards-policy-regulation/microsoft-offers-boost-european-governments-cybersecurity-free-2025-06-04/
[14] https://timesofindia.indiatimes.com/technology/tech-news/fbi-and-canadian-cybersecurity-agency-warns-chinese-hackers-attacking-telecom-services-in-canada/articleshow/122008362.cms
[15] https://www.securityweek.com/matlab-maker-mathworks-recovering-from-ransomware-attack/
[16] https://www.securityweek.com/364000-impacted-by-data-breach-at-lexisnexis-risk-solutions/
[17] https://www.securityweek.com/nova-scotia-power-confirms-ransomware-attack-280k-notified-of-data-breach/
[18] https://www.securityweek.com/ransomware-attack-forces-kettering-health-to-cancel-procedures/
[19] https://www.securityweek.com/ransomware-gang-leaks-alleged-kettering-health-data/
[20] https://www.securityweek.com/coinbase-rejects-20m-ransom-after-rogue-contractors-bribed-to-leak-customer-data/
[21] https://www.securityweek.com/production-at-steelmaker-nucor-disrupted-by-cyberattack/
[22] https://www.securityweek.com/ransomware-group-claims-attacks-on-uk-retailers/
[23] https://www.bleepingcomputer.com/news/security/hitachi-vantara-takes-servers-offline-after-akira-ransomware-attack/
[24] https://www.securityweek.com/kidney-dialysis-services-provider-davita-hit-by-ransomware/
[25] https://www.securityweek.com/ransomware-group-claims-hacking-of-oregon-regulator-after-data-breach-denial/
[26] https://www.securityweek.com/oregon-agency-wont-say-if-hackers-stole-data-in-cyberattack/
[27] https://www.securityweek.com/operations-of-sensor-giant-sensata-disrupted-by-ransomware-attack/
[28] https://www.cloudflare.com/press-releases/2025/cloudflare-accelerates-ai-agent-development-remote-mcp/
[29] https://www.cloudflare.com/press-releases/2025/cloudflare-accelerates-ai-agent-development-remote-mcp/
[30] https://www.cloudflare.com/press-releases/2025/cloudflare-launches-workers-vpc-and-vpc-private-link-for-cross-cloud-apps/
[31] https://www.broadcom.com/company/news/product-releases/63051
[32] https://www.broadcom.com/company/news/product-releases/63161
[33] https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-delivers-industry-first-managed-threat-hunting
[34] https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-unveils-unified-data-protection-secure-data-across
[35] https://www.rubrik.com/company/newsroom/press-releases/25/new-rubrik-identity-resilience-designed-to-mitigate-the-most-targeted-point-of-cyber-attacks
[36] https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-cortex-xsiam-delivers-industry-s-first-ai-driven-secops-platform-to-span-proactive-and-reactive-security
[37] https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-introduces-prisma-airs--the-foundation-on-which-ai-security-thrives
[38] https://www.securityweek.com/zscaler-to-acquire-mdr-specialist-red-canary/
[39] https://www.forbes.com/sites/emilsayegh/2025/06/05/zscaler-buying-red-canary-a-canary-in-the-cybersecurity-coalmine/
[40] https://www.securityweek.com/palo-alto-networks-to-acquire-ai-security-firm-protect-ai/
[41] https://www.leidos.com/insights/leidos-acquires-kudu-dynamics-advancing-ai-capabilities-cyber-warfighters
[42] https://www.securityweek.com/proofpoint-to-acquire-hornetsecurity-in-reported-1-billion-deal/
[43] https://www.securityweek.com/google-to-acquire-cloud-security-giant-wiz-for-32-billion-in-cash/
[44] https://www.securityweek.com/horizon3-ai-raises-100-million-in-series-d-funding/
[45] https://www.securityweek.com/swimlane-raises-45-million-for-security-automation-platform/
[46] https://www.securityweek.com/zero-networks-raises-55-million-for-microsegmentation-solution/
[47] https://www.securityweek.com/endor-labs-raises-93-million-for-appsec-platform/
[48] https://www.securityweek.com/exaforce-banks-hefty-75-million-for-ai-powered-soc-remake/
[49] https://www.securityweek.com/security-operations-firm-reliaquest-raises-500m-at-3-4b-valuation/
[50] https://www.securityweek.com/dataminr-raises-85-million-for-ai-powered-information-platform/