Nasdaq

Q3 2025 Cyber Security Update

Cyber Security News/Insight

- Revenue in the cybersecurity market is expected to grow to $196.5 billion in 2025, with an annual growth rate of 8.0%[1] (dialed down from previous estimate of $203.0 billion and 9.3%). The security services[2] segment is expected to contribute $100.4 billion to the total revenues, with the rest driven from cyber solutions.[3,4] 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[5]. This growth is expected to be led by the cyber solution segment with an estimated CAGR of 8.2% and a resultant market size of $142.4 billion[6] 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[7]. 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.[8]
- 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.[9] 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are known to conduct a range of targeted cyber activity to include exploiting known vulnerabilities in unpatched or outdated software, compromising internet-connected accounts and devices that use default or weak passwords and working with ransomware affiliates to encrypt, steal and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.[10] 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.
- 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.[11]
- The Czech Republic has 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.[12]
- 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.[13]

Cybersecurity – 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.[14]
- 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.[15]
- 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.[16]
- 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.[17]
- 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.[18]
- 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.[19,20]
- 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.[21,22,23]

New Products

- 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.[24]
- 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.[25]

- 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 10 times faster, more efficient, and cost effective.[26] 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.[27]
- In September 2025, Gen Digital Inc. (NASDAQ: GEN) teamed up with Intel to provide detection against AI-powered scams on 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.[28]
- In August 2025, Qualys Inc. (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.[29]

Cybersecurity – M&A and IPO Activity in Q3 2025

- 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.[30]
- 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 bring 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 raised $40 million in funding.[31]
- 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.[32]
- On September 12, Security and application delivery solutions provider F5 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).[33]
- 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 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.[34]

- 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 provide innovative category leading supply chain risk monitoring and vendor risk automation solutions in the cybersecurity and sustainability regulatory domains. Diginex's intends to expand in the cybersecurity space and be a global leader in compliance data verification and regulatory compliance automation.[35]
- On July 30, attack surface management solutions provider Axonius acquired medical device security company Cynerio for more than $100 million in 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.[36]

Venture Capital and Other Private Equity Activity:

- On September 17, Israel-based Irregular, previously known as Pattern Labs, announced it raised $80 million for its AI security lab. Irregular can evaluate AI models to determine their potential for misuse by threat actors, as well as the models' resilience to attacks aimed at them. Irregular claims it already has millions of dollars in annual revenue.[37]
- On September 16, endpoint security company Remedio announced it raised $65 million in first round funding that was led by Bessemer Venture Partners, with additional support from Picture Capital and TLV Partners. Remedio provides continuous, real-time device security posture management, hunting for misconfigurations and autonomously addressing them. Its platform leverages AI to resolve identified issues instantly across both SaaS and on-premise deployments.[38]
- On September 16, fraud prevention and AML compliance firm SEON announced it raised $80 million in Series C funding. With this new funding the total amount raised by the company stands at $187 million. The new investment round was led by Sixth Street Growth, with additional support from Hearst and previous investors Creandum, Firebolt, and IVP. SEON leverages AI to analyze tens of millions of customer interactions each day to detect and block fraud attempts in real time.[39]
- On September 16, Israeli cybersecurity company Vega, providing security analytics and operations solutions, announced it raised $65 million across seed and Series A funding. Accel, Cyberstarts, Redpoint, and CRV were investors. Vega's platform is advertised as a more efficient alternative to traditional SIEM solutions.[40]
- On August 12, 1Kosmos announced it raised $57 million in Series B funding from Forgepoint Capital, Oquirrh Ventures, and Origami Capital. The total funds raised stand at $72 million. The funds will be utilized to enhance its product, accelerate global expansion, and expand technology integrations with third-party identity and zero trust platforms. 1Kosmos provides remote identity verification and password less multi-factor authentication solutions for workers, customers, and residents.[41]
- On July 31, Israeli cybersecurity firm Noma Security announced it raised $100 million in Series B funding that was led by Evolution Equity Partners, with participation from Ballistic Ventures and Glilot Capital. It

had previously secured $32 million in Series A funding. Noma has developed a platform that enables organizations to securely adopt AI with the aid of security posture management, application security, governance and compliance, and dedicated AI agent security capabilities.[42]

- On July 31, U.S.-based API security firm Wallarm raised $55 million in Series C funding from Toba Capital. This brings the total funds raised to $70 million. Wallarm has developed a unified platform for API and agentic AI security, designed to help organizations stop attacks.[43]
- On July 30, U.S.-based BlinkOps announced it raised $50 million in Series B funding that was led by O.G. Venture Partners, with participation from Lightspeed Venture Partners, Hetz Ventures and Vertex Growth. The total funds raised stands at $90 million. BlinkOps has developed an agentic security automation platform that enables organizations to generate automation workflows for several types of tasks which enables the creation of custom security micro-agents for SOC and incident response, vulnerability management, cloud security, governance, risk and compliance (GRC), and identity and access management (IAM).[44]
- On July 24, Application security and compliance solutions provider HeroDevs announced that it raised $125 million in growth funding from PSG, adding to the $8 million funds it raised earlier. The U.S.-based firm provides security support for deprecated open-source software (OSS), to help organizations keep their critical applications protected and compliant long after they reach their official end-of-life (EoL) status. The firm counts Google, Microsoft, GE, and Capital One as their customers.[45]
- On July 23, U.S.-based risk management and compliance solutions provider firm Vanta announced that it raised $150 million in Series D funding which was led by Wellington Management, with participation from Growth Equity at Goldman Sachs Alternatives, Sequoia, J.P. Morgan, Craft Ventures, Y Combinator, Atlassian Ventures and CrowdStrike Ventures. With this new funding, the total funds raised stands at $504 million and values the firm at $4.15 billion. Vanta has developed a platform designed to simplify and centralize security and compliance for organizations that integrate with hundreds of third-party tools for cloud infrastructure, version control, productivity, and identity services.[46]
- On July 22, Darktrace, owned by PE firm Thoma Bravo, announced that it acquired network traffic visibility provider Mira Security to strengthen its position in the network security space. Mira Security provides visibility into network traffic, helping organizations detect and mitigate threats, and ensure they meet privacy and compliance requirements. Darktrace will integrate it with its existing encrypted traffic analysis capabilities.[47]
- On July 16, Italian IoT-embedded cybersecurity firm Exein announced that it raised $81 million in Series C funding and was led by Balderton, with additional support from Supernova, Lakestar, and previous investors 33N, United Ventures, and Partech. The firm in total has raised $106 million in funds. Exein focuses on securing individual devices that provide AI-enabled, real-time threat detection capabilities embedded into IoT devices used across critical infrastructure, automotive, energy, healthcare, robotics, and semiconductor industries. The new funds will help the firm to expand across the U.S. and Asia and strengthen its presence in Europe.[48]

[1] https://www.statista.com/outlook/tmo/cybersecurity/worldwide

[2] *Security Services: Security services refer a wide range of services that enhance an organization's protection and security strategy against common cybercrimes.*

[3] *Cyber Solutions: refer to automated security technologies that help monitor and secure IT systems, data, networks, and digital assets, protecting against cyberattacks*

[4] https://www.statista.com/outlook/tmo/cybersecurity/worldwide

[5] https://www.statista.com/outlook/tmo/cybersecurity/worldwide

[6] https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/worldwide

[7] https://www.statista.com/outlook/tmo/cybersecurity/security-services/worldwide

[8] https://www.statista.com/outlook/tmo/cybersecurity/united-states

[9] https://www.cisa.gov/news-events/news/joint-statement-cisa-fbi-dc3-and-nsa-potential-targeted-cyber-activity-against-us-critical

[10] https://www.bloomberg.com/news/articles/2025-09-08/trump-targets-asian-cyber-scam-centers-that-bilked-billions

[11] https://www.nbcnews.com/tech/security/china-used-three-private-companies-hack-global-telecoms-us-says-rcna227543

[12] https://apnews.com/article/czech-china-deepseek-ban-104f58035294f9f6ca988119732b8620

[13] https://www.ft.com/content/3e7c7a96-09e7-407f-98d7-a29310743d28

[14] https://www.securityweek.com/nevada-confirms-ransomware-attack-behind-statewide-service-disruptions/

[15] https://www.securityweek.com/telecom-firm-colt-confirms-data-breach-as-ransomware-group-auctions-files/

[16] https://www.securityweek.com/pharmaceutical-company-inotiv-confirms-ransomware-attack/

[17] https://www.securityweek.com/chip-programming-firm-data-i-o-hit-by-ransomware/

[18] https://www.securityweek.com/pennsylvania-attorney-general-confirms-ransomware-behind-weeks-long-outage/

[19] https://www.securityweek.com/allianz-life-data-breach-impacts-most-of-1-4-million-us-customers/

[20] https://www.reuters.com/legal/government/hack-allianz-life-impacts-11-million-customers-breach-notification-site-says-2025-08-18/

[21] https://www.securityweek.com/ingram-micro-restores-systems-impacted-by-ransomware/

[22] https://www.blackfog.com/how-ingram-micro-overcame-a-major-ransomware-attack/

[23] https://www.csoonline.com/article/4031695/ransomware-gang-tells-ingram-micro-pay-up-by-august-1.html

[24] https://www.cyberark.com/press/cyberark-announces-availability-of-tools-to-secure-ai-agents-in-the-new-aws-marketplace-ai-agents-and-tools-category/

[25] https://www.cloudflare.com/press-releases/2025/cloudflare-launches-new-zero-trust-tools-for-secure-ai-adoption-at-scale/

[26] https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-redefines-application-security-with-the-industry-s-most-comprehensive-prevention-first-aspm

[27] https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-redefines-application-security-with-the-industry-s-most-comprehensive-prevention-first-aspm

[28] https://newsroom.gendigital.com/2025-09-16-Norton-Unveils-Advanced-Deepfake-Protection-Powered-by-Intel-R-Core-TM-Ultra-Processors

[29] https://www.qualys.com/company/newsroom/news-releases/usa/qualys-unveils-industrys-first-agentic-ai-powered-risk-operations-center/

[30] https://www.securityweek.com/sentinelone-to-acquire-observo-ai-in-225-million-deal/

[31] https://www.securityweek.com/crowdstrike-to-acquire-onum-to-fuel-falcon-next-gen-siem-with-real-time-telemetry/

[32] https://www.securityweek.com/palo-alto-networks-to-acquire-cyberark-for-25-billion/

[33] https://www.securityweek.com/f5-to-acquire-calypsoai-for-180-million/

[34] https://www.securityweek.com/mitsubishi-electric-to-acquire-nozomi-networks-for-nearly-1-billion/

[35] 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

[36] https://www.securityweek.com/axonius-acquires-medical-device-security-firm-cynerio-in-100-million-deal/

[37] https://www.securityweek.com/irregular-raises-80-million-for-ai-security-testing-lab/

[38] https://www.securityweek.com/endpoint-security-firm-remedio-raises-65-million-in-first-funding-round/

[39] https://www.securityweek.com/fraud-prevention-company-seon-raises-80-million-in-series-c-funding/
[40] https://www.securityweek.com/security-analytics-firm-vega-emerges-from-stealth-with-65m-in-funding/
[41] https://www.securityweek.com/1kosmos-raises-57-million-for-identity-verification-and-authentication-platform/
[42] https://www.securityweek.com/noma-security-raises-100-million-for-ai-security-platform/
[43] https://www.securityweek.com/api-security-firm-wallarm-raises-55-million/
[44] https://www.securityweek.com/blinkops-raises-50-million-for-agentic-security-automation-platform/
[45] https://www.securityweek.com/herodevs-raises-125-million-to-secure-deprecated-oss/
[46] https://www.securityweek.com/grc-firm-vanta-raises-150-million-at-4-15-billion-valuation/
[47] https://www.securityweek.com/darktrace-acquires-mira-security/
[48] https://www.securityweek.com/iot-security-firm-exein-raises-81-million/