Q1 2026 Cybersecurity Update

Cybersecurity News/Insight

- According to Statista, revenue in the cybersecurity market is expected to grow to $211.7 billion in 2026, with an annual growth rate of 7.7%[1]. The security services[2] segment is expected to contribute $106.1 billion to the total revenues, with the rest from cyber solutions.[3,4] During the period 2026-2030, revenue is expected to show an annual growth rate of 5.8% resulting in a total market size of $265.2 billion by 2030.[5] Region-wise, the largest market for cybersecurity, the U.S. is expected to have a market size of $93.0 billion in 2026.
- According to a U.S. intelligence assessment, Iran and its proxies pose a potential threat of targeted attacks on the United States. In the short term, this risk is expected to materialize primarily through low-level cyber-activity by Iran-aligned "hacktivists" against U.S. networks, including website defacements and distributed denial-of-service attacks.[6]
- According to Fitch Ratings, U.S. public finance issuers face elevated cyber risk because of the Iran conflict. Previous geopolitically motivated attacks on U.S. public finance entities primarily have targeted health care and utilities. Increased broad-based retaliatory cyber intrusions also are likely.[7]
- In February 2026, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive to secure Cisco SD-WAN systems, in response to a significant cyber threat targeting federal networks utilizing certain Cisco Systems and software.[8]
- In February 2026, OpenAI reached an agreement with the Defense Department to deploy its models in the agency's network.[9] The deal with OpenAI comes following President Donald Trump's announcement to all federal government agencies to cease using Anthropic's AI tools.[10]Following the deal, CEO Sam Altman said on X, "Two of our most important safety principles are prohibitions on domestic mass surveillance and human responsibility for the use of force, including for autonomous weapon systems. The DoW (Department of War) agrees with these principles, reflects them in law and policy, and we put them into our agreement." This suggests that the Pentagon agreed to Anthropic's suggested restrictions with OpenAI's models.[11]
- In February 2026, Anthropic has accused three Chinese AI firms (DeepSeek, Moonshot AI and MiniMax) of illicitly extracting capabilities from its Claude chatbot, in what was described as industrial-scale intellectual property theft.[12] OpenAI leveled similar charges in January 2026.
- According to Forrester (a global market research company), cybercrime operations from actors such as Russia, China, Iran, and North Korea is expected to expand in 2026.[13] This concern is echoed by Google's annual Cybersecurity Forecast for 2026.[14] One area that Google sees as particularly vulnerable to Chinese attacks is the semiconductor sector, due to competition from rivals such as TSMC and American export restrictions.[15]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q1 2026

- On March 12, Loblaw Companies Limited (TSE: L), the largest food and pharmacy retailer in Canada, announced that hackers breached a portion of its IT network and accessed basic customer information such as names, phone numbers, and email addresses.[16]

- On March 11, medical technology company Stryker (NYSE: SYK) was hit by a wiper malware attack claimed by Handala, an Iranian-linked and pro-Palestinian hacktivist group. Handala claimed to have stolen 50 terabytes (TB) of data before wiping tens of thousands of systems and servers across the company's network. Stryker was forced to shut down offices in 79 countries.[17]
- On March 11, Telus Digital, the Canadian digital services and business process outsourcing (BPO) arm of Canadian telecommunications provider Telus, confirmed that it was impacted by a security incident after threat actors ShinyHunters claimed to have stolen nearly 1 petabyte of data from the company in a multi-month breach. ShinyHunters demanded $65 million in exchange for not leaking the company's data.[18]
- On March 3, data analytics company LexisNexis Legal & Professional confirmed that hackers breached its servers and accessed some customer and business information. A threat actor named FulcrumSec leaked 2GB of files on various underground forums and sites. The company noted that the stolen information was old and consisted mostly of non-critical details.[19]
- On March 3, Dutch paint company AkzoNobel (AMS: AKZA) confirmed that hackers breached the network of one of its U.S. sites. After a data leak from the Anubis ransomware gang, a company spokesperson said that the intrusion was contained and the impact was limited. The published data contained confidential agreements with high-profile clients and other valuable information.[20]
- On February 24, Wynn Resorts (Nasdaq: WYNN) confirmed that a hacker stole employee data from its systems after the company was listed on the ShinyHunters extortion gang's data leak site. Wynn did not confirm if any ransom was paid but mentioned that the attackers deleted the stolen data, which indicated that a ransom may have been paid.[21]
- On February 24, the ShinyHunters extortion group published personal information that contained 12 million records allegedly stolen from CarGurus (Nasdaq: CARG). CarGurus is a publicly traded automotive research and shopping company that operates in the U.S., Canada, and the U.K. While the company did not release any official statement, a day after the breach, HaveIBeenPwned (HIBP), the data breach monitoring and alerting platform, added that the dataset was compromised. HIBP attempted to confirm the validity/authenticity of the leaked records before adding them.[22]
- On February 23, U.S.-based healthcare diagnostic company Vikor Scientific (Vanta Diagnostics) disclosed a data breach that compromised the personal information of 140,000 people. The Everest ransomware group took credit for the cyberattack and claimed to have stolen roughly 12GB of data.[23]
- On February 23, a ransomware attack forced the University of Mississippi Medical Center to close all of its roughly three dozen clinics around the state and cancel elective procedures for a second day. Hospital authorities were trying to gauge the extent of the infiltration, while university officials warned that the shutdown could continue for days. The attackers had communicated with the university, but their demands were not disclosed.[24]
- On February 20, Japanese chip testing company Advantest Corporation (TSE: 6857) was targeted in a ransomware attack. The company investigated into any customer or employee data theft by the hackers. Advantest makes automatic test equipment for the semiconductor industry. It serves major chipmakers such as Intel, Samsung, and TSMC.[25]
- On February 20, medical device manufacturer UFP Technologies (Nasdaq: UFPT) disclosed a cybersecurity incident that involved the theft of files and the disruption of some of its IT systems. The

company investigated to determine what types of information was compromised and if it includes personal information. The identity of the attacker was not known.[26]

- On February 20, the French Ministry of Finance disclosed a cybersecurity incident that impacted data associated with 1.2 million user accounts. Hackers gained access to the national bank account registry (FICOBA) in January and stole a database containing sensitive information.[27]
- On February 18, a data breach at fintech firm Figure Technology Solutions (Nasdaq: FIGR), a self-described blockchain-native financial technology company, affected nearly 1 million accounts. In February 2026, data obtained from the fintech firm that contained over 900,000 unique email addresses along with names, phone numbers, physical addresses and dates of birth was published online. The ShinyHunters extortion group claimed credit for the attack and added the company to its dark web leak site.[28]
- On February 15, Japanese chip testing company Advantest Corporation (TSE: 6857) detected that it was targeted in a ransomware attack. The company was yet to determine if the attackers exfiltrated any sensitive information from the company. The identity of the attacker was not known.[29]
- On February 13, Louis Vuitton, Christian Dior Couture, and Tiffany, all three brands part of the Louis Vuitton Moët Hennessy (LVMH), (EPA: MC) were fined $25 million by the Personal Information Protection Commission (PIPC) of South Korea. The luxury brands failed to implement adequate security measures, which facilitated unauthorized access and the exposure of data belonging to more than 5.5 million customers.[30]
- On February 6, a major U.S.-based payment gateway and solutions provider, BridgePay, was a victim of a ransomware attack that disrupted key systems offline, triggering a widespread outage affecting multiple services. The company engaged the services of federal law enforcement, including the FBI and U.S. Secret Service, along with external forensic and recovery teams. Initial findings indicated that no payment card data was compromised.[31]
- On February 6, Starbucks (Nasdaq: SBUX) detected a data breach affecting hundreds of employees after threat actors gained access to their Starbucks Partner Central accounts. The personal information exposed in the incident includes employees' names, Social Security numbers, dates of birth, and financial account and routing numbers.[32]
- On February 4, Romanian national oil pipeline operator Conpet disclosed a cyberattack that disrupted its business systems and took down the company's website. However, the attack did not disrupt its core business operations. The Qilin ransomware gang claimed to have stolen 1TB of data and added Conpet to their dark web leak site.[33]
- On February 3, Panera Bread fell victim to cyberattack after data allegedly pertaining to over 5 million customers surfaced online, following hackers' failed extortion attempt against the U.S.-based bakery-cafe chain. The ShinyHunters extortion group claimed to have stolen roughly 14 million records, after compromising a Microsoft Entra single-sign-on (SSO) code. Later, the group published 760GB archive allegedly containing sensitive information of 5.1 million customers on its Tor-based leak site.[34,35]
- On January 29, the French data protection authority fined France Travail, the national employment agency, nearly €6 million for failing to secure job seekers' data. Hackers in March 2024 used social engineering and stole the personal information of 43 million people spanning 20 years.[36]
- On January 24, cyber attackers targeted the power grid system of Poland on December 29 & 30, 2025. The coordinated attack targeted multiple distributed energy resource (DER) sites across the country,

including combined heat and power (CHP) facilities and wind and solar dispatch systems. The attacker managed to compromise operational technology systems damaging key equipment beyond repair but failed to disrupt the power. Russian state-sponsored hacking group Sandworm, attempted to deploy a new destructive data-wiping malware dubbed DynoWiper during the attack.[37,38]

- On January 24, Nike (NYSE: NKE) revealed that it launched an investigation after a cybercrime group claimed to have stolen data from its systems. Nike was listed as a victim on the Tor-based leak website operated by the WorldLeaks gang on January 22. The hackers later leaked 1.4TB of stolen data containing corporate data providing information on Nike's business operations.[39,40]
- On January 10, automated investment platform Betterment's systems were breached under a distributed denial-of-service (DDoS) attack. Hackers stole email addresses and other personal information from 1.4 million accounts. Threat actors sent fraudulent emails disguised as a company promotion after gaining access to some of its systems in a social engineering attack. In a follow-up forensic investigation, conducted in collaboration with the cybersecurity firm CrowdStrike, it was found that no customer accounts were compromised in the breach. [41]
- On January 5, third-party claims and benefits administrator Sedgwick confirmed that a ransomware group claimed it hacked Sedgwick Government Solutions. Sedgwick Government Solutions provides claims and risk management services to the U.S. government agencies, including the DHS, CISA, and municipalities across the country.[42]

New Products

- In February 2026, Cisco (NASDAQ: CSCO) introduced suite of capabilities to help enterprises securely adopt AI technology while maintaining agent integrity and control of agentic interactions.[43] Furthermore, Cisco in partnership with SharonAI Holdings Inc. (NASDAQ: SHAZ) announced the launch of Australia's first Cisco Secure AI Factory in partnership with NVIDIA.[44]
- In February 2026, Broadcom (NASDAQ: AVGO) introduced Wi-Fi 8 Access Point (AP) and switch solution purpose-built with a unified architecture for AI-ready enterprise networks. According to the company's press release, the new capabilities are intended to address rising demand for hybrid work and support performance, efficiency and security needed for next-generation enterprise networking.[45]
- In March 2026, CrowdStrike (NASDAQ: CRWD) and Perplexity announced a strategic partnership to integrate the CrowdStrike Falcon platform with Comet Enterprise, giving enterprise administrators an additional layer of security and monitoring in Perplexity's AI-native browser.[46]
- In March 2026, Fortinet (NASDAQ: FTNT) rolled out FortiOS 8.0, an operating system as part of Fortinet's Secure. It delivers new AI-driven security, next-generation SASE, and quantum-safe capabilities to help organizations simplify their security architecture while delivering consistent protection and performance across the entire digital infrastructure.[47]
- In March 2026, Check Point Software Technologies Ltd. (NASDAQ: CHKP) introduced Secure AI Advisory Service, a new service designed to help enterprises accelerate AI adoption, while integrating governance, risk oversight, and regulatory considerations throughout the AI lifecycle.[48] Furthermore, in January 2026, the company rolled out Check Point Exposure Management, a new approach designed to help organizations defend against AI-era attacks by turning fragmented exposure data into prioritized, actionable, and safe remediation.[49]This helps security teams which are flooded with intelligence, but fragmented exposure data spread across multiple tools limits their ability to prioritize risks and turn insight into effective, safe remediation using their existing security investments.

Cybersecurity – M&A and IPO Activity in Q1 2026

- On March 4, Swiss insurance company Zurich Insurance Group (SWX: ZURN) agreed to acquire UK-based Beazley for approximately £8.1 billion ($11 billion). The merger is driven by Beazley's leadership in cyber insurance and its strategic positioning within the Lloyd's of London presence. Zurich estimates that the combined entity will generate roughly $15 billion in specialty gross written premiums annually. Zurich also expects the transaction to unlock $150 million in annual cost savings by 2029 and over $1 billion in incremental revenue opportunities in the medium term. Beazley shareholders will receive 1,335 pence per share, which represents a nearly 60% premium over the company's closing price in mid-January. The deal still requires final shareholder and regulatory approvals. Completion is currently anticipated in H2 2026.[50]
- On February 17, Palo Alto Networks (NDX: PANW) announced its intent to acquire endpoint security company Koi in a deal that is reported to be valued at $400 million. Koi which had raised $48 million in funding, offers an endpoint security platform that focuses on protecting various types of software, including applications, code, operating system packages, extensions, AI models, AI agents, and containers. The acquisition aims to enhance Palo Alto's Prisma AIRS AI security platform and Cortex XDR endpoint security solution to provide "significant visibility into the AI attack surface to improve security policy and malware prevention."[51]
- On February 13, Israeli cybersecurity firm Check Point (Nasdaq: CHKP) acquired Israeli cybersecurity companies Cyata, Cyclops, and Rotate. Financial details were not available though Check Point is believed to have paid $150 million to acquire all three firms. Cyata will help Check Point enhance its end-to-end AI security platform by enabling discovery, governance, and control of autonomous AI agents. Cyclops helps the company strengthen exposure management with AI-driven asset discovery and continuous monitoring across cloud, on-premises, OT, and SaaS environments to deliver a complete CTEM (Continuous Threat Exposure Management) solution. Rotate brings talent and capabilities to accelerate workspace momentum specifically in the managed service provider (MSP) market, providing an all-in-one platform tailored for MSPs.[52]
- On February 3, data security company Varonis Systems (Nasdaq: VRNS) announced that it has acquired AllTrue.ai. The purchase price was not disclosed; however the Wall Street Journal report valued the deal at $150 million. AllTrue.ai's platform gives organizations visibility into where AI is being used, the models and agents that are running, and the data they can access. By integrating AllTrue.ai's capabilities into its own platform, Varonis will enable customers to monitor and control AI behavior, reduce risks, and maintain and demonstrate compliance.[53]
- On January 13, CrowdStrike (Nasdaq: CRWD) announced plans to acquire browser security startup Seraphic Security for approximately $420 million to be paid predominantly in cash. Seraphic's technology promises protection from zero-day browser exploits, phishing, and other browser-based attacks, all without requiring separate secure browsers or rerouting traffic. CRWD believes the acquisition will allow it to extend zero-trust protection to the browser and fuse Seraphic's continuous in-session browser protection with SGNL's continuous identity to secure every interaction from the endpoint to the browser to the cloud. The acquisition is expected to close during Q1 2027.[54]
- On January 8, CrowdStrike (Nasdaq: CRWD) announced plans to acquire identity security startup SGNL in a deal valued at $740 million, to be paid predominantly in cash. U.S.-based SGNL has built an "identity-first" security solution that protects organizations' assets by eliminating static credentials and providing real-time automated access decisions. The deal aims to strengthen CrowdStrike's Falcon

platform with “continuous identity” protection to secure human and AI-driven access in real-time. SGNL has raised $42 million in funding, including a $30 million Series A round in February 2025. The deal is expected to close during CrowdStrike’s Q1 2027, subject to customary closing conditions and regulatory clearances.[55]

- On December 23, IT services company ServiceNow (NYSE: NOW) has agreed to acquire cybersecurity company Armis in an all-cash deal for $7.75 billion. Armis had raised $435 million in December 2025 in a pre-IPO round. However, Armis abandoned its IPO plans in favor of an acquisition. Armis has developed solutions that enable enterprises to discover IT, OT and IoT assets in their environments. In addition to asset intelligence and visibility, the company’s platform provides protection, risk assessment, vulnerability prioritization, and remediation and compliance capabilities.[56]

Venture Capital and Private Equity Activity:

- On March 10, U.S.-based Armadin announced a massive Seed and Series A Funding round of $189.9 million. The funding was led by Accel, with participation from Google Ventures, Kleiner Perkins, Menlo Ventures, In-Q-Tel, and follow-on investment from 8VC and Ballistic Ventures. Armadin uses AI-powered red teaming to find and exploit weaknesses in the same way that attackers attack them.[57]
- On March 10, Kai received $125 million in a seed and Series A funding from Evolution Equity Partners, N47, and other investors. The funds will be utilized for an AI-powered platform that aims to bridge IT and OT cybersecurity.[58]
- On February 10, Israeli cybersecurity startup Vega raised $120 million in a Series B funding round that was led by existing investor Accel, with participation from Cyberstarts, Redpoint, and CRV. This brings the total amount raised by the company to $185 million in under two years. Vega’s platform is advertised as a more efficient alternative to traditional SIEM solutions. The platform leverages AI to enable SOC teams to create new detections or use ones from a continuously updated list provided by Vega and help organizations detect and respond to threats.[59]
- On January 11, agentic AI security operations company Torq announced that it raised $140 million in a Series D funding at a valuation to $1.2 billion. This brings the total funds raised by the company to $332 million. The latest investment round was led by Merlin Ventures, with additional support from all previous investors. Torq has built an AI-powered ‘hyperautomation’ security operations center (SOC) platform that enables organizations to instantly detect and respond to security events at scale, eliminating alert fatigue, false positives, and burnout.[60]
- On January 26, cloud security company Upwind announced it raised $250 million in a Series B funding round at valuation of $1.5 billion. This brings the total funds raised by the company to $430 million. The new investment round was led by Bessemer Venture Partners, with additional support from Salesforce Ventures and Picture Capital. Upwind offers a runtime-native cloud security platform that provides organizations with increased visibility into networks, APIs, and data flows.[61]
- On January 22, cyber-physical systems security company Claroty announced that it raised $150 million in a Series F funding round. This brings the total funds raised to approximately $900 million. Golub Growth led the latest funding. Existing investors have confirmed an additional participation of up to $50 million. The company was reportedly valued at $2.5 billion following its $100 million strategic growth funding round in March 2024. Claroty has developed a platform that provides asset visibility, exposure management, network protection, secure access, and threat detection capabilities for xIoT systems, a term that encompasses operational technology such as ICS, IoT, and IIoT.[62]

- On January 8, data security firm Cyera announced a $400 million Series F funding round at a valuation of $9 billion. The funding was led by Blackstone, with participation from Accel, Coatue, Cyberstarts, Georgian, Greenoaks, Lightspeed Venture Partners, Redpoint, Sapphire, Sequoia Capital, and Spark. The latest funding brings the total funds raised by the firm to $1.7 billion. In June 2025, the company raised $540 million in Series D funding, which brought its valuation to $6 billion. Cyera has developed solutions designed to give organizations a complete view of data use, storage, and security. Its platform provides data security posture management (DSPM) and data loss prevention (DLP) capabilities, with AI-focused features being added recently.[63]
- On December 9, identity security firm Saviynt in a Series B growth equity funding raised $700 Million at a valuation of $3 billion. The funding round was led by KKR, with participation from Sixth Street Growth, TenEleven, and Carrick Capital Partners. Saviynt has developed an AI-powered platform designed for managing and securing human, non-human, and AI agent identities across applications, data, and infrastructure.[64]

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

[5] https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue
[6] https://www.reuters.com/world/middle-east/intelligence-assessment-warns-iranian-attacks-us-following-khameneis-death-2026-03-02/
[7] https://www.fitchratings.com/research/us-public-finance/us-public-finance-cyber-risk-elevated-due-to-iran-conflict-09-03-2026
[8] https://www.cisa.gov/news-events/news/immediate-action-required-cisa-issues-emergency-directive-secure-cisco-sd-wan-systems
[9] https://edition.cnn.com/2026/02/27/tech/openai-pentagon-deal-ai-systems
[10] https://edition.cnn.com/2026/02/27/tech/openai-pentagon-deal-ai-systems
[11] https://edition.cnn.com/2026/02/27/tech/openai-pentagon-deal-ai-systems
[12] https://www.theguardian.com/technology/2026/feb/23/us-ai-anthropic-china
[13] https://www.euronews.com/next/2026/01/12/from-ai-breaches-to-rising-geopolitical-threats-heres-what-to-expect-from-cybersecurity-in
[14] https://services.google.com/fh/files/misc/cybersecurity-forecast-2026-en.pdf
[15] https://services.google.com/fh/files/misc/cybersecurity-forecast-2026-en.pdf
[16] https://www.bleepingcomputer.com/news/security/canadian-retail-giant-loblaw-notifies-customers-of-data-breach/
[17] https://www.bleepingcomputer.com/news/security/stryker-attack-wiped-tens-of-thousands-of-devices-no-malware-needed/
[18] https://www.bleepingcomputer.com/news/security/telus-digital-confirms-breach-after-hacker-claims-1-petabyte-data-theft/
[19] https://www.bleepingcomputer.com/news/security/lexisnexis-confirms-data-breach-as-hackers-leak-stolen-files/
[20] https://www.bleepingcomputer.com/news/security/paint-maker-giant-akzonobel-confirms-cyberattack-on-us-site/
[21] https://www.bleepingcomputer.com/news/security/wynn-resorts-confirms-employee-data-breach-after-extortion-threat/
[22] https://www.bleepingcomputer.com/news/security/cargurus-data-breach-exposes-information-of-124-million-accounts/
[23] https://www.securityweek.com/us-healthcare-diagnostic-firm-says-140000-affected-by-data-breach/
[24] https://www.securityweek.com/mississippi-hospital-system-closes-all-clinics-after-ransomware-attack/ https://www.securityweek.com/mississippi-hospital-system-closes-all-clinics-after-ransomware-attack/
[25] https://www.securityweek.com/chip-testing-giant-advantest-hit-by-ransomware/
[26] https://www.securityweek.com/medical-device-maker-ufp-technologies-hit-by-cyberattack/
[27] https://www.bleepingcomputer.com/news/security/data-breach-at-french-bank-registry-impacts-12-million-accounts/
[28] https://www.bleepingcomputer.com/news/security/data-breach-at-fintech-firm-figure-affects-nearly-1-million-accounts/
[29] https://www.securityweek.com/chip-testing-giant-advantest-hit-by-ransomware/
[30] https://www.bleepingcomputer.com/news/security/louis-vuitton-dior-and-tiffany-fined-25-million-over-data-breaches/
[31] https://www.bleepingcomputer.com/news/security/payments-platform-bridgepay-confirms-ransomware-attack-behind-outage/
[32] https://www.bleepingcomputer.com/news/security/starbucks-discloses-data-breach-affecting-hundreds-of-employees/
[33] https://www.bleepingcomputer.com/news/security/romanian-oil-pipeline-operator-conpet-discloses-cyberattack-qilin-ransomware/
[34] https://www.securityweek.com/hackers-leak-5-1-million-panera-bread-accounts/
[35] https://www.bleepingcomputer.com/news/security/panera-bread-data-breach-impacts-51-million-accounts-not-14-million-customers/
[36] https://www.bleepingcomputer.com/news/security/france-fines-unemployment-agency-5-million-over-data-breach/
[37] https://www.bleepingcomputer.com/news/security/sandworm-hackers-linked-to-failed-wiper-attack-on-polands-energy-systems/
[38] https://www.bleepingcomputer.com/news/security/cyberattack-on-polish-energy-grid-impacted-around-30-facilities/
[39] https://www.securityweek.com/nike-probing-potential-security-incident-as-hackers-threaten-to-leak-data/
[40] https://www.bleepingcomputer.com/news/security/nike-investigates-data-breach-after-extortion-gang-leaks-files/

[41] https://www.bleepingcomputer.com/news/security/data-breach-at-fintech-firm-betterment-exposes-14-million-accounts/
[42] https://www.securityweek.com/sedgwick-confirms-cyberattack-on-government-subsidiary/
[43] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2026/m02/cisco-redefines-security-for-the-agentic-era.html
[44] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2026/m02/sharon-ai-cisco-launch-australia-first-cisco-secure-ai-factory-with-nvidia.html
[45] https://www.broadcom.com/company/news/product-releases/63936
[46] https://www.crowdstrike.com/en-us/press-releases/crowdstrike-perplexity-extend-enterprise-grade-security-to-comet-enterprise/
[47] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2026/fortinet-introduces-fortios-8-expand-secure-networking-with-secure-ai-controls-fabric-based-ai-agents-flexible-sase-and-simplified-sdwan
[48] https://www.checkpoint.com/press-releases/check-point-launches-a-secure-ai-advisory-service-to-help-enterprises-govern-and-scale-ai-transformation/
[49] https://www.checkpoint.com/press-releases/check-point-introduces-ai-driven-exposure-management-to-close-the-cyber-security-remediation-gap/
[50] https://www.securityweek.com/zurich-acquires-beazley-in-11-billion-deal-to-lead-cyberinsurance/
[51] https://www.securityweek.com/palo-alto-networks-to-acquire-koi-in-reported-400-million-transaction/
[52] https://www.securityweek.com/check-point-announces-trio-of-acquisitions-amid-solid-2025-earnings-beat/
[53] https://www.securityweek.com/varonis-acquisition-of-alltrue-ai-valued-at-150-million/
[54] https://www.securityweek.com/crowdstrike-to-acquire-browser-security-firm-seraphic-for-420-million/
[55] https://www.securityweek.com/crowdstrike-to-buy-identity-security-firm-sgnl-for-740-million-in-cash/
[56] https://www.securityweek.com/servicenow-to-acquire-armis-for-7-75-billion-in-cash/
[57] https://www.securityweek.com/kevin-mandias-armadin-launches-with-189-9-million-in-funding/
[58] https://www.securityweek.com/kai-emerges-from-stealth-with-125m-in-funding-for-ai-platform-bridging-it-and-ot-security/
[59] https://www.securityweek.com/vega-raises-120m-in-series-b-funding-to-grow-security-analytics-platform/
[60] https://www.securityweek.com/torq-raises-140-million-at-1-2-billion-valuation/
[61] https://www.securityweek.com/upwind-raises-250-million-at-1-5-billion-valuation/
[62] https://www.securityweek.com/claroty-raises-150-million-in-series-f-funding/
[63] https://www.securityweek.com/cyera-raises-400-million-at-9-billion-valuation/
[64] https://www.securityweek.com/identity-security-firm-saviynt-raises-700-million-at-3-billion-valuation/