Q1 2024 Cyber Security Update

Cyber Security News/Insight

- Revenue in the cybersecurity market is expected to grow to $183.1 billion in 2024 at an annual growth rate of 10.2%[1]. The security services segment is expected to contribute $92.9 billion and the cyber solutions segment is expected to contribute the rest.[2] During the period 2024-2028, revenue is expected to grow at an annual rate of 10.6%, resulting in a total market size of $273.6 billion by 2028[3]. This growth is expected to be led by the cyber solutions segment with an estimated CAGR of 15.2% and a resultant market size of $158.8 billion[4] in 2028, followed by the security services segment at a lower rate of 5.4% and a resultant market size of $114.7 billion in 2028[5]. Region-wise, the U.S is the largest market for cybersecurity, with a market size of $78.3 billion in 2024. It is expected to grow at a CAGR of 9.8% during the period 2024-2028 to a market size of $113.8 billion by 2028.[6]
- According to Statista, cybercrimes are expected to cost about $9.2 trillion in 2024 with the global cost expected to grow to $13.8 trillion in 2028.[7] According to the World Economic Forum's global risks report 2024, cyber insecurity is a global risk over multiple time horizons, with risks including malware, deepfakes and misinformation. These risks threaten supply chains, financial stability, and democracy.[8]
- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and its international partners warned about active exploitation of multiple vulnerabilities within Ivanti Connect Secure and Ivanti Policy Secure gateways.[9] Furthermore, the U.S. and its partner international government agencies published a Joint Cybersecurity Advisory on malicious activity by People's Republic of China (PRC) state-sponsored cyber actor, known as Volt Typhoon, to compromise critical infrastructure and associated actions that should be urgently undertaken by all organizations.[10]
- The White House issued an executive order to strengthen maritime port cybersecurity. More than $20 billion will be invested in improving port infrastructure over the next five years as per administration officials. As part of that, Persico Corporation, a U.S.-based subsidiary of Japanese company Mitsui E&S, will produce ship-to-shore cranes intended to phase out Chinese-built infrastructure, said Anne Neuberger, national security adviser for cybersecurity and emerging technology.[11]
- The EU's Cybersecurity Regulations came into force in early 2024, giving all agencies until September 2024 to conform to it. The regulation was proposed by the European Commission in 2022, and it lays down uniform cyber compliance requirements for EU institutions, bodies, offices, and agencies.[12]
- A report from the Joint Committee on the National Security Strategy (JCNSS) warned that the U.K. government might be sleepwalking toward a catastrophic ransomware incident. The committee said that their ransomware report recommendations given at the end of last year were rejected by the U.K. government. "In this response to our ransomware report, it is ever clearer that government does not know the extent or costs of cyberattacks across the country, though we're the third most cyber-attacked country in the world, nor does it have any intention of commensurately upping the stakes or resources in response," said JCNSS chair Margaret Beckett.[13]

- According to Kazutaka Nakamizo, deputy director of Japan's National Center of Incident Readiness and Strategy for Cybersecurity, China-backed hackers are increasingly targeting telecom carriers, internet providers and other critical infrastructure in Japan.[14]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q1 2024

- On Mar 16, the International Monetary Fund (IMF) detected a security breach where 11 email accounts were hacked. The email accounts were later re-secured, and the ongoing probe does not reveal that the attacker gained access to any other data. It is unclear what type of data may have been obtained from the IMF email accounts. The email accounts that were hacked into did not belong to the Managing Director or other top officials of IMF.[15]
- On Mar 15, a data breach at the French government unemployment agency France Travail, formerly known as Pole Emploi, may have affected 43 million people. The compromised database stores the information of individuals who are registered with the agency currently and over the past 20 years, as well as people who only created an account on its website. The attacker's identity is yet to be known.[16]
- On Feb 26, Thyssenkrupp (ETR: TKA) confirmed a ransomware attack disrupted one of its automotive divisions, forcing the company to shut its IT systems which halted factory production. The company stated that an attack was detected at an early stage and was able to contain the threat.[17,18]
- On Feb 21, UnitedHealth Group (NYSE: UNH) subsidiary Change Healthcare was hit by a cyberattack perpetrated by the Alphv/ BlackCat ransomware gang which disrupted claims and payments infrastructure. An investigation was launched to focus on whether there was a breach of protected health information. Change Healthcare is a vital lynchpin in the system for making and clearing insurance claims as it processes about 50% of medical claims in the U.S. for around 900,000 physicians, 33,000 pharmacies, 5,500 hospitals and 600 laboratories. UnitedHealth paid out more than $2 billion to help affected health-care providers. More than 60% of the 1,000 hospitals surveyed estimated the revenue hit to be around $1 million per day. Change Healthcare reportedly paid a $22 million ransom to the BlackCat cybercrime group.[19,20,21,22]
- On Feb 15, PSI Software (ETR: PSAN), a Germany-based control systems provider to major European energy suppliers, announced that a ransomware attack forced the company to disconnect their IT systems to prevent data infiltration. The intruder's identity was not determined.[23]
- On Feb 12, Germany-based automotive, consumer, and industrial battery manufacturer Varta, (ETR: VAR1) operating in 45 countries with production facilities in Germany, China, Romania, and Indonesia, became a victim of a cyberattack. It disrupted production at five of its plants on Feb 14 as a result of shutting down its IT systems. The extent of damage was not known at the time of reporting.[24]
- On Feb 12, computer systems at 100 hospitals across Romania went offline after a ransomware attack hit their healthcare management system. The Hipocrate Information System (HIS) used by hospitals to manage medical activity and patient data was targeted and was offline after its database was encrypted.[25]
- On Feb 5, Prudential Financial (NYSE: PRU) identified a security breach where the attacker accessed the company's administrative and user data. The company was yet to identify the number of its employees affected but mentioned that a ransomware group may be behind the intrusion.[26]
- On Jan 31, aircraft parts dealer Willis Lease Finance Corporation (NASDAQ: WLFC) detected unauthorized access to its IT systems, which was contained by Feb 2. The Black Basta ransomware

gang claimed responsibility for the attack and is said to have exfiltrated over 900 gigabytes (GB) of data from WLFC, including sensitive company data, employee and customer information, shared folders, and confidential documents.[27]

- On Jan 21, Lockbit ransomware group claimed to have hacked into U.S. sandwich chain Subway and exfiltrated their SUBS internal system, which includes hundreds of gigabytes of financial and other data such as employee salaries, franchise royalty payments, master franchise commission payments, restaurant turnovers, etc.[28] On Feb 20, the U.S. Department of Justice announced it had finally disrupted the LockBit ransomware group by seizing infrastructure including their public-facing websites and critical servers. The announcement was made along with the U.K.'s National Crime Agency Cyber Division, and the global operation was aided by multiple international partners including France, Germany, Switzerland, Japan, Australia, Sweden, Canada, Netherlands, Finland, and other European police and criminal enforcement agencies. [29]
- On Jan 21, Finnish IT services company Tietoevry (HEL: TIETO), which offers managed services and enterprise cloud hosting, revealed a ransomware attack from Akira. This attack impacted its cloud hosting customers in one of its data centers in Sweden.[30]
- On Jan 19, American global apparel, and footwear company VF Corporation (NYSE: VFC) in an 8-K filing disclosed that a ransomware attack in Dec 2023 resulted in stolen personal information impacting 35.5 million customers. However, the company mentioned that customers' social security numbers, bank account information, and payment card information was not impacted.[31]
- On Jan 19, the North America subsidiary of Veolia (EPA: VIE) disclosed a ransomware attack impacted part of their Municipal Water division and disrupted its bill payment systems. The attack did not disrupt the company's water treatment operations or wastewater services, and the company was assessing the level of damage from the attack.[32]
- On Jan 19, Schneider Electric (EPA: SU) disclosed that their Sustainability Business division was affected after a cyberattack impacted Resource Advisor and other division specific systems. The Cactus ransomware group claimed responsibility and has said to have accessed 1.5 TB of data, including customer information. The group published a small set of stolen data on its leak website and threatened to publish the full data if the ransom was not paid.[33,34,35]
- On Jan 18, the website of Foxsemicon Integrated Technology (TPE: 3413), a subsidiary of Taiwanese electronics giant Foxconn, was hijacked. The Lockbit ransomware gang posted a message on the company website and claimed to have stolen 5 terabytes (TB) of data belonging to customers and employees. Foxsemicon informed the Taiwan Stock Exchange that their initial assessment indicated the incident should not have a significant impact on its operations.[36]
- On Jan 17, the largest aviation leasing company in the world AerCap (NYSE: AER) was targeted by cyber attackers. The company in its 6-K filing stated that they have regained control of their IT systems and suffered no financial loss from the incident. An emerging ransomware group named 'Slug' has taken responsibility for stealing one TB of data and listed it on their leak site.[37]
- On Jan 16, the city of Calvià on the Spanish island of Majorca announced a ransomware attack impacted its municipal services. A local media outlet learned that cybercriminals set a ransom of $11 million. The mayor told the local press that the municipality would not be paying the ransom under any circumstances.[38]

- On Jan 4, lending giant LoanDepot (NYSE: LDI) disclosed in an 8-K filing that the company had detected unauthorized access to its systems. At a later date, on Jan 22, the company revealed that the attack affected approximately 16.6 million individuals. The Alphv/Blackcat ransomware gang claimed responsibility for the attack.[39,40]
- On Jan 2, Xerox Corporation (NASDAQ: XRX) revealed that the U.S. division of Xerox Business Solutions (XBS) was compromised by hackers with a limited amount of personal information exposed. The gang known as INC Ransom added the corporation to its extortion portal on Dec 29, and claimed to have stolen sensitive data and confidential documents.[41]
- In early Jan, Hyundai Motors' Europe division suffered a cyberattack by the Black Basta ransomware gang, which claimed to have stolen 3 TB of data. While the company has not confirmed, the stolen data may contain legal, sales, human resources, accounting, IT, and management related information.[42]

New Products

- In February 2024, CrowdStrike (NASDAQ: CRWD) announced the general availability of Charlotte AI and Falcon for IT, as well as new innovations to Falcon Data Protection, to unify Security and IT. These new products use GenAI, minimize the data exposure risks associated with commercial GenAI tools, and deliver AI-native innovation.[43]
- In March 2024, Darktrace (NASDAQ: DARK) and Xage Security (a zero-trust cybersecurity solutions provider) announced a new partnership to help businesses prevent cyberattacks and insider threats in critical environments. This collaboration brings together Xage Security's leading zero trust protection with Darktrace's AI-powered anomaly-based threat detection. In the company's own words, the integration between Darktrace/OT™ and Xage Fabric makes it easy to identify and respond to breaches in progress at any stage in operational technology (OT) and information technology (IT) environments.[44]
- In January 2024, Juniper Networks (NASDAQ: JNPR) launched the industry's first AI-Native Networking Platform. The new product leverages AI to assure the best end-to-end operator and end-user experiences. Trained on seven years of insights and data science development, Juniper's AI-Native Networking Platform was designed from the ground up to assure that every connection is reliable, measurable and secure for every device, user, application and asset."[45]
- In January 2024, Fortinet Inc. (NASDAQ: FTNT) announced the industry's only comprehensive secure networking solution integrated with Wi-Fi 7. These solutions deliver cutting-edge wireless performance and, as a part of the Fortinet Secure Networking solution, seamlessly integrate with AIOps and FortiGuard AI-Powered security services for unmatched security, visibility, and control.[46] In February, the company introduced its new product, FortiGate Rugged 70G. It incorporates 5G Dual Modem secure networking features in a ruggedized, compact form factor ideal for industrial environments and remote ATMs.[47]
- In March 2024, Cloudflare Inc. (NASDAQ: NET) launched Magic Cloud Networking, a secure and scalable way for businesses to connect and secure their public cloud environments.[48] Furthermore, it has introduced Defensive AI, which helps organizations to implement a personalized approach to protect their workforce and data, tackling the threat landscape of the future.[49]

Cybersecurity – M&A and IPO Activity in Q1 2024

Inside NQCYBR™ Index Activity:

- On Jan 11, Infosys (NYSE: INFY), a global leader in next-generation digital services and consulting, today announced a definitive agreement to acquire InSemi, a leading semiconductor design and embedded services provider. This strategic investment further strengthens Infosys' Engineering R&D capabilities and demonstrates continued commitment to co-create with global clients to help them navigate their transformational journey. [50]
- On Jan 9, 2024, Hewlett Packard Enterprise (NYSE: HPE) and Juniper Networks, Inc. (Nasdaq: JNPR) jointly announced a definitive agreement under which HPE will acquire Juniper in an all-cash transaction for $40.00 per share, a premium of 32% to Juniper's closing price on January 8, 2024, representing an equity value of approximately $14 billion. The transaction is expected to close by June 30, 2025, and be accretive to non-GAAP EPS and free cash flow in the first year post close.

Outside NQCYBR Index Activity:

- On Feb 6, cybersecurity firm ZeroFox (NASDAQ: ZFOX), which markets itself as a provider of "external cybersecurity solutions", entered into a definitive agreement to be acquired by Haveli Investments, a tech-focused private equity firm, in an all-cash transaction with an enterprise value of roughly $350 million. ZeroFox shareholders will receive $1.14 per share in cash upon completion of the transaction, well below its 52-week high of $3.49 per share. The transaction is expected to close in the first half of 2024 and is not subject to a financing condition.[51]
- On Jan 8, data security firm Cohesity and Veritas jointly announced that Cohesity will buy Veritas' data protection business, creating a data security and management giant valued at roughly $7 billion. The new company will continue to invest in and advance the strategy of all Cohesity products and services, as well as Veritas' NetBackup, NetBackup appliances, and Alta data protection offerings. The transaction is expected to close by the end of 2024, and Cohesity said the transaction would be financed through a combination of equity and debt.[52]
- On Jan 4, Atos (EPA: ATO) announced that Airbus (EPA: AIR) could acquire Atos' cybersecurity unit for up to $2 billion. The possible sale of its Big Data and Security (BDS) business was announced by Atos in a market update outlining its strategy for repaying and refinancing financial debts. The potential deal is at a preliminary stage, but Atos said it will initiate a due diligence phase after receiving an offer valuing BDS between €1.5 billion ($1.64 billion) and €1.8 billion ($1.97 billion). In 2023, Airbus made a bid for a 30% stake in Atos' Evidian security business, which would later become Eviden. Some shareholders expressed opposition and the plan was dropped.

Venture Capital and Other Private Equity Activity:

- On Mar 13, Industrial and Internet of Things (IoT) cybersecurity firm Nozomi Networks announced that it raised $100 million in a Series E funding from Mitsubishi Electric and Schneider Electric, which brings the total amount raised to $250 million. Nozomi boasts that its technology protects more than 105 million OT, IoT and IT devices worldwide, across 12,000+ installations. The funds will be used to expand its industrial cybersecurity business.[53]
- On Mar 6, extended IoT (XIoT) cybersecurity company Claroty raised another $100 million at a reported valuation of $2.5 billion, bringing the total amount secured to $735 million. Delta-v Capital, AB Private

Credit Investors at AllianceBernstein, Standard Investments, Toshiba Digital Solutions, SE Ventures, Rockwell Automation, and Silicon Valley Bank took part in the latest funding round. The company provides solutions for protecting what it calls XIoT, which includes OT, IoT, Internet of Medical Things (IoMT), and building management systems (BMS), and boasts more than $100 million in ARR (annual recurring revenue) in 2023.[54]

- On Mar 5, U.S.-based Dtex Systems, working on technology to automate the detection of insider threats, raised $50 million in a Series E funding led by CapitalG, the investment arm of Google's parent company Alphabet. Dtex uses a combination of machine learning and network monitoring technologies to spot unusual patterns or activities to minimize data loss from insider threats. It positioned its flagship product as a platform with tooling for Data Loss Prevention (DLP), User Behavior Analytics (UBA) and User Activity Monitoring. [55]
- On Mar 5, Israel-based Axonius, a player in the attack surface management space with $100 million in ARR, banked $200 million in late-stage funding (Series E) led by existing investors Accel and Lightspeed Venture Partners. Growth equity firm Stripes also took an equity position. Axonius has raised approximately $600 million since 2017 and is considered one of cybersecurity's so-called unicorns with a valuation of $2.6 billion. Axonius' product touches multiple pain points – Cyber Asset Attack Surface Management (CAASM), SaaS Security Posture Management (SSPM), and SaaS Management Platforms (SMP) – with more than 1,000 platform integrations to help identify security gaps, risk, misconfigurations, and cost inefficiencies.[56]
- On Feb 12, bug bounty platform provider Bugcrowd announced they raised $102 million from General Catalyst, Rally Ventures, and Costanoa Ventures in a strategic growth funding round. The funds will be used to accelerate growth, enhance its crowdsourced security platform, and for strategic M&A opportunities. Bugcrowd enables organizations to run crowdsourced bug bounty and vulnerability disclosure programs, helping them find vulnerabilities in their products and systems with the aid of hundreds of thousands of white hat hackers who have signed up on their platform.[57]
- On Jan 29, wireless threat intelligence firm Bastille Networks announced that they raised $44 million in Series C funding. The investment round was led by Goldman Sachs, with additional funding from existing investor Bessemer Venture Partners, bringing the total amount raised to $80 million. Founded in 2014, Bastille Networks helps organizations identify all covert, rogue, and vulnerable wireless devices in their environments and secure them.[58]
- On Jan 23, Israeli late-stage startup Silverfort disclosed that they raised $116 million in new financing to scale their ambitions in the identity security space. The Series D funding was led by Brighton Capital and existing investors Acrew Capital, Greenfield Partners, Citi Ventures, General Motors Ventures, Maor Investments, Vintage Investment Partners and Singtel Innov8. The total amount raised by the firm now stands at $222 million. The company's technology helps businesses to manage Multi-Factor Authentication (MFA), Identity Threat Detection and Response (ITDR), Identity Security Posture Management (ISPM), and real-time protection for privileged users and service accounts.[59]
- On Jan 18, identity and authentication startup Oleria, founded by former Salesforce CISO Jim Alkove, raised $33 million in a Series A round from Evolution Equity Partners. Previous investors Salesforce Ventures, Tapestry VC, and Zscaler also expanded their equity stakes. The firm has raised a total of $40 million in venture capital funding to continue work on technology in the adaptive and autonomous identity security space. The company's approach is meant to keep digital assets secure through

continuous access reviews and remediation, while removing static and inflexible identity and access management that can slow down business operations.[60]

- On Jan 17, Israel-based vulnerability management firm Vicarius raised $30 million in a Series B funding round led by Bright Pixel (formerly Sonae IM). AllegisCyber Capital, AlleyCorp, and Strait Capital also participated in the funding round. Total funding for the company has now reached $59.2 million. Vicarius provides automated vulnerability management through its vRx product, which uses a PLG (product-led growth) model.[61]
- On Jan 10, ExtraHop announced that they had secured $100 million in growth funding from existing investors. ExtraHop, acquired by a pair of private equity firms in 2021, had ARR (annual recurring revenue) of $200 million in 2023. The company sells a range of software products for organizations to manage network detection and response, and AI-powered IT analytics tasks.[62]
- On Jan 3, Israel-based Aqua Security, a late-stage player in the cloud native security platform (CNAPP) space, banked $60 million in an extended Series E funding round from new investor Evolution Equity Partners, at a valuation upwards of $1 billion. Previous backers Insight Partners, Lightspeed Venture Partners and StepStone Group also increased their equity stakes. Aqua Security, which has raised $325 million since its founding in 2015, provides technology to help organizations improve security for containerized and cloud-native applications. The company claims its software provides full visibility and security automation across an application's entire lifecycle.[63]

[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/chart/28878/expected-cost-of-cybercrime-until-2027/
[8] https://www.weforum.org/agenda/2024/01/reflections-on-davos-2024-the-state-of-cybersecurity/
[9] https://www.cisa.gov/news-events/news/cisa-us-and-international-partners-warn-ongoing-exploitation-multiple-ivanti-vulnerabilities
[10] https://www.cisa.gov/news-events/news/us-and-international-partners-publish-cybersecurity-advisory-peoples-republic-china-state-sponsored
[11] https://therecord.media/port-cybersecurity-china-cranes-biden-executive-order?&web_view=true
[12] https://www.bankinfosecurity.com/eu-enhances-cybersecurity-requirements-for-agencies-a-24076?&web_view=true
[13] https://www.forbes.com/sites/emmawoollacott/2024/03/12/uk-government-accused-of-ostrich-strategy-on-ransomware/?sh=4c514b4210a8
[14] https://therecord.media/japan-critical-infrastructure-cyberthreats?&web_view=true
[15] https://www.securityweek.com/imf-emails-hacked/
[16] https://www.securityweek.com/43-million-possibly-impacted-by-french-government-agency-data-breach/
[17] https://www.securityweek.com/german-steelmaker-thyssenkrupp-confirms-ransomware-attack/
[18] https://www.bleepingcomputer.com/news/security/steel-giant-thyssenkrupp-confirms-cyberattack-on-automotive-division/
[19] https://www.securityweek.com/hhs-aiding-organizations-hit-by-change-healthcare-cyberattack/
[20] https://www.securityweek.com/government-launches-probe-into-change-healthcare-data-breach/
[21] https://www.cnbc.com/2024/03/18/unitedhealth-group-paid-more-than-2-billion-to-providers-after-attack.html
[22] https://www.reuters.com/business/healthcare-pharmaceuticals/unitedhealth-says-advanced-over-2-bln-payments-providers-2024-03-18/
[23] https://www.securityweek.com/control-systems-firm-psi-struggles-to-recover-from-ransomware-attack/
[24] https://www.securityweek.com/cyberattack-disrupts-production-in-varta-battery-factories/
[25] https://www.bleepingcomputer.com/news/security/ransomware-attack-forces-100-romanian-hospitals-to-go-offline/
[26] https://www.securityweek.com/prudential-financial-discloses-data-breach/
[27] https://www.securityweek.com/willis-lease-finance-corp-discloses-cyberattack/
[28] https://www.securityweek.com/sandwich-chain-subway-investigating-ransomware-groups-claims/
[29] https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant

[30] https://www.bleepingcomputer.com/news/security/tietoevry-ransomware-attack-causes-outages-for-swedish-firms-cities/
[31] https://www.bleepingcomputer.com/news/security/vans-north-face-owner-says-ransomware-breach-affects-35-million-people/
[32] https://www.bleepingcomputer.com/news/security/water-services-giant-veolia-north-america-hit-by-ransomware-attack/
[33] https://www.se.com/ww/en/about-us/newsroom/news/press-releases/sustainability-business-division-of-schneider-electric-responds-to-cybersecurity-incident-65b8035eb11dced626091019
[34] https://www.securityweek.com/schneider-electric-division-responding-to-ransomware-attack-data-breach/
[35] https://www.securityweek.com/cactus-ransomware-group-confirms-hacking-schneider-electric/
[36] https://www.securityweek.com/ransomware-group-targets-foxconn-subsidiary-foxsemicon/
[37] https://www.securityweek.com/aircraft-lessor-aercap-confirms-ransomware-attack/
[38] https://www.bleepingcomputer.com/news/security/majorca-city-calvi-extorted-for-11m-in-ransomware-attack/
[39] https://www.securityweek.com/loandepot-breach-16-6-million-people-impacted/
[40] https://www.bleepingcomputer.com/news/security/alphv-ransomware-claims-loandepot-prudential-financial-breaches/
[41] https://www.bleepingcomputer.com/news/security/xerox-says-subsidiary-xbs-us-breached-after-ransomware-gang-leaks-data/
[42] https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/
[43] https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-unifies-security-it-unleashes-transformative-power
[44] https://ir.darktrace.com/press-releases/2024/3/4/4bb40e76715d97cc702e1e409eb71fd32300a83ce52facfbe33c320b25a54f35
[45] https://investor.juniper.net/investor-relations/press-releases/press-release-details/2024/Juniper-Networks-Unveils-Industrys-First-AI-Native-Networking-Platform-to-Deliver-Exceptional-User-Experiences-and-Lower-Operational-Costs/default.aspx
[46] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-announces-industry-first-wi-fi-7-enabled-secure-networking-solution
[47] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-converges-dual-5g-modem-ai-powered-security-zero-trust-to-securely-connect-and-protect-operational-technology
[48] https://www.cloudflare.com/en-in/press-releases/2024/cloudflare-enters-multicloud-networking-market-unlocks-simple-secure/
[49] https://www.cloudflare.com/en-in/press-releases/2024/cloudflare-expands-capabilities-to-protect-organizations-against-emerging/
[50]https://www.infosys.com/newsroom/press-releases/2024/acquire-semiconductor-design-services.html
[51] https://www.securityweek.com/zerofox-to-be-taken-private-in-350-million-deal/
[52]https://www.securityweek.com/zerofox-to-be-taken-private-in-350-million-deal/
[53] https://www.securityweek.com/cohesity-to-buy-veritas-data-protection-businesses/
[54] https://www.securityweek.com/nozomi-networks-raises-100-million-to-expand-industrial-cybersecurity-business/
[55] https://www.securityweek.com/fresh-100-million-claroty-funding-brings-total-to-735-million/
[56] https://www.securityweek.com/dtex-systems-snags-50m-from-alphabets-capitalg/
[57] https://www.securityweek.com/axonius-banks-200-million-in-late-stage-funding/
[58] https://www.securityweek.com/bugcrowd-raises-102-million/
[59] https://www.securityweek.com/bastille-networks-raises-44-million-to-secure-wireless-devices/
[60] https://www.securityweek.com/identity-security-firm-silverfort-lands-116-million-investment/
[61] https://www.securityweek.com/oleria-secures-33m-investment-to-grow-id-authentication-business/
[62] https://www.securityweek.com/vulnerability-management-firm-vicarius-raises-30-million/
[63] https://www.securityweek.com/extrahop-banks-100m-in-growth-funding-adds-new-execs/
[64] https://www.securityweek.com/aqua-security-scores-60m-series-e-funding/