New Chapter for Cybersecurity with AI Adoption, Driving New Threats & Growth

October 2023

- We continue to believe that the long-term investment thesis for cybersecurity is intact with the rise of generative AI as a potential new growth driver. While there have been areas of concern for cybersecurity in the recent past, they have primarily been outweighed by a robust demand environment, signs of strength emerging from recent government security deals with Zero Trust mandates, and an increasing regulatory push, including new executive orders and requirements outlined in the U.S. National Cybersecurity Strategy that are likely to further drive growth over the next two years[1].
- Companies are looking at cybersecurity operations much earlier in their lifecycle, suggesting that it continues to remain a high priority for IT spending[2].
- 2023 has seen changes in the demand and operating environment for cybersecurity, with an increase in insider threats and demand for security solutions leveraging AI/ML[3].
- The rise of generative AI and the ongoing migration into the cloud are reshaping the investment theme of cybersecurity.
- AI is expected to augment security analysts and help make traditional security operations tools easier to use. New risks are emerging from AI-enabled automation, however, including bots and symptoms like vast amounts of quickly spreading disinformation.

Growth Forecasts & Market Trends

- Growth in the cybersecurity market continues to compare favorably with other areas of IT spending, suggesting that CIOs continue to prioritize security spending.
- In its latest forecast, research firm Gartner predicted that enterprise information security spending will reach $186 billion in 2023 and grow to $278 billion in 2027, equating to an 11% compound annual growth rate. That's better than most information technology spending categories.[4]
- Statista forecasts similar growth rates for the cybersecurity market. Between 2023-2028, the market is estimated to grow at a compound annual growth rate (CAGR) of 9.6% to a market size of $256.6 billion in 2028. This growth is expected to be led by the cyber solution segment with an estimated CAGR of 14.2% and a resultant market size of $148.7 billion in 2028, followed by the security services segment at a lower rate of 4.8% and a resultant market size of $107.9 billion in 2028.[5]
- McKinsey estimates the total addressable market size for cybersecurity is $1.5-2.0T globally, implying at best only ~10% current penetration and a very long runway for growth.[6]

[1] https://www.insidegovernmentcontracts.com/2023/04/march-2023-developments-under-president-bidens-cybersecurity-executive-order
[2] https://www.idc.com/getdoc.jsp?containerId=prUS50498423
[3] https://www.cyberneticsearch.com/blog/top-5-cyber-security-trends-2023/
[4] https://www.investors.com/news/technology/cybersecurity-stocks
[5] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[6] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

- The new narrative for cybersecurity. The zero-trust model of security and AI-based security products is likely to dominate the new narrative for cybersecurity solutions. The zero-trust security model assumes that no user or device can be trusted without continuous verification. Research firm Markets and Markets projects that the global zero trust security market will grow from $19.6 billion in 2020 to $51.6 billion by 2026.[7] The global market for AI-based cybersecurity products is estimated to reach $133.8 billion by 2030, up from $14.9 billion last year.[8]

State of the Cybersecurity Market

- Cloud-based companies with cybersecurity offerings will likely have an edge over others. Companies with existing cloud-computing platforms will likely be best positioned to capture value. As per a report by Bank of America, cloud-based vendors like CrowdStrike (CRWD), Palo Alto Networks (PANW), and Zscaler (ZS) are likely to generate the highest value for investors. Smaller vendors offering differentiated solutions will likely still be competitive in certain parts of this market.[9]
- Wave of new cybersecurity startups. Analysts say a new wave of startups is taking share from industry incumbents[10]. They include Netskope, Wiz, Snyk, and Illumio. Other startups, including Venafi, Recorded Future, Noname Security, Obsidian Security, Deep Instinct, and Skyflow, have also been making waves. This new wave of startup activity suggests that demand for cybersecurity continues to be strong and will likely pressure incumbents into higher research and development spending.[11] Funding continues to go to cybersecurity startups. For example, cloud security firm Wiz recently raised $300 million at a $10 billion valuation. While the startup system is flooded, there remains a concern that the vast number of vendors will exacerbate tool sprawl and complicate customer decision-making.
- Threat environment becoming more complex. As evinced by recent statistics, organizations have become increasingly vulnerable to attacks. Attacks are now happening faster, with decreased time from compromise to exfiltration. According to the Identity Theft Resource Center report, 2022 saw supply chain attacks making headlines, with over 10 million people and more than 1,700 organizations affected.[12]
- AI set to transform the threat landscape. Bad actors have been able to develop new attack strategies with generative AI. They have been able to automate attacks, scan attack surfaces, and target a broader range of victims. These attacks are distinct, necessitating more sophisticated solutions.
- $10.5 trillion cybercrime market by 2025.[13] The dramatic increase in hostile nation-state-sponsored and organized crime-gang hacking activities will dramatically increase cybercrime costs. Cybercrime would be the third-largest economy after the U.S. and China if measured as a country.

IPO & Private Market Activity

- While there has been a cooling in the IPO market for cybersecurity along with almost every other sector, it remains a ~$200B industry with no signs of demand slowing. The recent dry spell for the IPO market is likely to be broken by Rubrik, a data protection startup. According to Reuters, Rubrik has hired several banks to assist with its IPO. It is looking to raise about $750 million in its IPO, though the amount may change based on market conditions nearer the time, as preparations are still at an early stage.[14]

[7] https://www.cnbc.com/2022/03/01/why-companies-are-moving-to-a-zero-trust-model-of-cyber-security-.html
[8] https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html
[9] https://www.investors.com/news/technology/cybersecurity-stocks/
[10] https://www.investors.com/news/technology/cybersecurity-stocks/
[11] https://www.investors.com/news/technology/how-cloud-computing-giant-microsoft-is-changing-the-cybersecurity-market/
[12] https://www.axios.com/2023/06/23/software-supply-chain-attacks
[13] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[14] https://www.bankinfosecurity.com/blogs/rubrik-looking-to-break-cybersecuritys-ipo-dry-spell-p-3456

- Experts expect a recovery in the IPO market as early as 4Q 2023.[15]
- In the private markets, venture capital activity for cybersecurity startups has also been subdued in 2023 with $5.8B in funding across Early Stage, Later Stage, and Seed Round VC across 212 transactions (min size: $5MM) as of August 25, per Pitchbook. This compares to $17.2B in funding for full-year 2022 across 442 transactions.

M&A Activity

- M&A activity will likely rebound after a slowdown in the first half of 2023. There has been a slowdown in M&A activity regarding deal count and dollar value compared to 2022 as participants continue to deal with uncertain markets and higher financing costs. Additionally, M&A valuations in the sector have fallen on a YTD basis compared to 2022. The remainder of 2023 and 2024 is likely to see a pickup in M&A activity, driven by an uptick in exit activity by VC firms.[16]
- Exits in the form of M&A, which fell in H1 2023 to 26, the lowest level since 2020, are expected to rise as valuations of cybersecurity companies remain suppressed.[17]
- Google's acquisition of cybersecurity firm Mandiant in 2022 signaled to the markets that cybersecurity is critical in a cloud-first world. This sentiment was further strengthened by Microsoft's acquisition of Miburo, a vendor that counters disinformation. This followed a string of cybersecurity acquisitions by Microsoft in 2021, including RiskIQ, ReFirm Labs, and CyberX.
- While seemingly all "big Tech" companies have pledged to ramp up investments in cybersecurity, Google and Microsoft have made the largest investments to date. In 2021, they pledged to invest a combined $30 billion over five years. By expanding their presence in the cybersecurity domain, big Tech companies are adding another stabilizing force to the revenue growth trajectory.
- On September 21, 2023, Cisco (CSCO) and Splunk (SPLK) announced a definitive agreement under which Cisco intends to acquire Splunk for $157 per share in cash, representing approximately $28 billion in equity value. It is expected to close by the end of the third quarter of calendar year 2024.[18]
- Below is the list of NQCYBR™ constituents acquired since January 2022; despite an awful 2022 with global M&A volume down 37%, an additional seven NQCYBR companies were acquired at an average premium of 47% above their pre-announcement closing price:

Target	Acquirer	Deal Value	Announcement Date	Premium
KnowBe4	Vista Equity Partners	$4.6 billion	October 12, 2022	44%
Ping Identity	Thoma Bravo	$2.4 billion	August 3, 2022	63%
VMware	Broadcom	$61 billion	May 26, 2022	44%
ManTech	Carlyle	$4.2 billion	May 16, 2022	32%
SailPoint Technologies	Thoma Bravo	$6.9 billion	April 11, 2022	48%
Tufin Software	Turn/River Capital	$570 million	April 6, 2022	44%

[15] https://www.calcalistech.com/ctechnews/article/s1hlddrm2
[16] https://www.capstonepartners.com/insights/article-cybersecurity-ma-update/
[17] https://www.calcalistech.com/ctechnews/article/s1hlddrm2
[18] https://www.prnewswire.com/news-releases/cisco-to-acquire-splunk-to-help-make-organizations-more-secure-and-resilient-in-an-ai-powered-world-301934777.html

Mandiant	Google	$5.4 billion	March 8, 2022	57%

Further Consolidation in the Market

- The cybersecurity market is unlikely to consolidate in the near future, but potentially will over time. The market is relatively nascent and fragmented compared to other technology areas like cloud computing. While cybersecurity, as a software category, is comparatively more difficult to scale, demand for a "single pane of glass" (e.g., single holistic solution) from the client side will likely encourage industry participants to consolidate over time.
- Economies of scale will likely accrue for companies that consolidate their offerings. Additionally, certain customers may prefer "large" security vendors over mid or small-sized security vendors, given the criticality of cyber defense, which is also likely to encourage consolidation.[19]
- Customers looking to simplify their operations will likely encourage cybersecurity companies to consolidate. For example, vendors will likely consolidate platforms around one or more major cybersecurity domains. Identity security services may be offered through a common platform that combines governance, privileged access, and access management features.[20]

Security for a Multi-Cloud Environment

- Increased demand for cybersecurity solutions tailored for a multi-cloud environment. Making a secure transition to the cloud has been a top priority for CIOs of leading companies. Many organizations begin their cloud journey with a single central cloud platform, such as AWS, Microsoft Azure, or Google Cloud Platform. Eventually, many larger organizations realize numerous potential limitations in a single-cloud model, including downtime concerns, security and privacy, vulnerability to attacks, and vendor lock-in.[21] This has led to an interest in transitioning to a multi-cloud model.

- Widespread adoption of multi-cloud strategies. According to a 2022 report, 89% of organizations have a multi-cloud strategy to distribute applications and services, with 80% taking a hybrid approach combining private and public clouds. But, the number one challenge for enterprises using the cloud – and increasingly organizations choosing to work with multiple cloud vendors – is securing a multi-cloud environment.[22]
- The transition to multi-cloud is a fundamental shift on par with when the internet was born, according to the COO-Digital at Entrust, the global leader in security protection for identities, payments, and digital infrastructure. While this transition unlocks innovation, it dramatically increases the surface area for attacks, making it critical to secure sensitive data.[23]
- Security issues abound with the rise in multi-cloud adoption. The topmost concern for security providers is the lack of standardization across different cloud providers. Each cloud provider has its own security protocols and standards, which can make it challenging to ensure consistent security across multiple clouds. Additionally, multi-cloud environments can be more complex and challenging to manage than single-cloud environments, increasing the risk of security breaches.[24]

[19] https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cybersecurity-thought-leadership-2021.pdf
[20] https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cybersecurity-thought-leadership-2021.pdf
[21] https://www.techtarget.com/searchsecurity/feature/The-risks-of-multi-cloud-security-compared-to-single-cloud
[22] https://www.wired.com/sponsored/story/the-future-of-multi-cloud-security/
[23] https://www.wired.com/sponsored/story/the-future-of-multi-cloud-security/
[24] https://www.linkedin.com/pulse/cloud-security-multi-cloud-environments-best-practices-raj-pathak/

- Among the vulnerabilities that are unique to multi-cloud, the most common ones include lack of consistency across platforms, exponentially higher data and application volumes that limit the speed of threat mitigation, data unpredictability, and reduced visibility into cross-platform attacks.[25]

Nasdaq CTA Cybersecurity™ Index (NQCYBR)
Company-Specific AI Highlights
Weightings as of EOD 9/29/2023

- BlackBerry (BB): 1.59% weighting
    - AI-driven BlackBerry security protects the complete attack surface with automated threat prevention, detection, and response capabilities. CylancePROTECT delivers industry-leading threat prevention powered by AI, combined with application and script control, memory protection, and device policy enforcement, to identify and block threats before they can cause harm. Earlier this month, BlackBerry announced a major update to its patented Cylance AI engine, which can now enhance cybersecurity threat prediction capabilities for organizations by 40% versus earlier versions.[26]
- Cisco (CSCO): 5.82% weighting
    - Leverages Zero Trust security and acquired Duo Security for $2.35 billion in 2018. In June, Cisco announced that it is previewing and investing in the first generative AI capabilities in the Security Cloud to simplify security operations and increase efficiency.[27]
- CrowdStrike (CRWD): 3.19% weighting
    - CrowdStrike announced a new AI-powered generative assistant called Charlotte AI in May 2023. The assistant is designed to help users, from novices to experts, operate like a seasoned security professional. Charlotte AI is trained on CrowdStrike's security event data, threat intelligence, and telemetry from users, devices, and cloud workloads. Users can ask Charlotte AI questions like how susceptible their system is to the latest vulnerability. Charlotte AI will return real-time answers. CrowdStrike also announced new AI-powered indicators of attack (IoA) models. These models use machine intelligence to stop breaches by detecting and predicting malicious behavior in real-time.[28]
- Fortinet (FTNT): 6.06% weighting
    - Fortinet offers AI-powered cybersecurity solutions to protect organizations against known and emerging cyber threats. FortiAI, a deep learning solution designed specifically to remove the need for time-consuming manual investigation of cyberattacks, enables organizations to accelerate their responses to advanced threats by identifying and classifying attack vectors in real-time and instantaneously blocking them from reaching corporate networks.[29]
- Netscout Systems (NTCT): 1.27% weighting
    - In July, Netscout announced the release of its next-generation Omnis Cyber Intelligence (OCI) solution. OCI is an advanced network detection and response (NDR) solution that uses highly scalable deep packet inspection (DPI) and multiple threat detection methods at the source of packet capture to detect threats in real-time and allows historical investigation of

[25] https://www.bmc.com/blogs/security-threats-multi-cloud/
[26] https://www.blackberry.com/us/en/solutions/artificial-intelligence-predictive-security#top
[27] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m06/cisco-shows-breakthrough-innovation-towards-ai-first-security-cloud.html
[28] https://www.crowdstrike.com/blog/crowdstrike-introduces-charlotte-ai-to-deliver-generative-ai-powered-cybersecurity/
[29] https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

high-fidelity network metadata and packets. The next-gen OCI features threat detection that combines ML-based behavioral analysis, threat intelligence, intrusion detection signatures, and continuous attack surface monitoring to detect threats at scale with higher confidence.[30]

- Okta (OKTA): 3.03% weighting
    - In June, Okta's CEO announced plans to allocate $40 million of its annual research and development budget to new artificial intelligence projects. The investment represents about 10% of the total R&D budget for the 14-year-old software maker, known for providing user identification services. One of its first projects is a bot that guides customers on how to use the firm's products.[31]
- Palo Alto Networks (PANW): 5.99% weighting
    - Uses analytics to automate routine tasks and enforcement. In May, PANW announced plans to release a proprietary large language model for security on an earnings call (AI was mentioned 32 times during this call). The company uses other forms of AI, like machine learning, across its services but is looking to incorporate generative AI to improve its processes and operations. See Q2'23 cyber quarterly update (New Products section) for more details on PANW's AI/ML-powered cloud next-generation firewall product.
- Qualys Inc. (QYLS): 3.05% weighting
    - Qualys TotalCloud manages and reduces cloud security risk using deep learning artificial intelligence for advanced threat detection. Using deep learning AI techniques, TotalCloud can detect unknown malware in less than one second with more than 99% accuracy. As a result, it helps organizations detect and reduce the impact of malware infiltration. Better still, it reduces threat meantime-to-detect (MTTD) to less than a second, radically improving the risk profile for any organization.[32]
- Rapid7 Inc (RPD): 1.88% weighting
    - Rapid7's security solutions help customers unite cloud risk management and detection to reduce attack surfaces and eliminate threats quickly and precisely. Rapid7 is a cybersecurity company that uses AI to help security, IT, and DevOps teams manage risk, detect attackers, and optimize operations. Rapid7's InsightIDR feature uses AI to detect the use of stolen credentials and flag risky users and behaviors. InsightIDR also uses automation to surface notable user and asset behavior on a visual timeline.[33]
- Tenable Holdings (TENB): 3.07% weighting
    - In 2021, it acquired France-based Alsid, focusing on identity access management. Earlier this month, Tenable announced the launch of ExposureAI, new generative AI capabilities, and services across the Tenable One Exposure Management Platform. Tenable has also introduced Tenable Exposure Graph, a scalable data lake powered by Snowflake that fuels the ExposureAI engine. This unified data platform - representing over 1 trillion unique exposures, IT assets, and security findings (vulnerabilities, misconfigurations, and identities)

[30] https://www.netscout.com/press-releases/netscout-releases-next-generation-omnis-cyber-intelligence
[31] https://news.bloomberglaw.com/artificial-intelligence/okta-invests-in-ai-as-ceo-warns-its-too-soon-for-regulation
[33] https://www.rapid7.com/products/insightidr/features/user-behavior-analytics/#:~:text=You'll%20detect%20this%20movement%20and%20the%20use,visual%20timeline%20so%20you%20can%20decide%20how
[33] https://www.rapid7.com/products/insightidr/features/user-behavior-analytics/#:~:text=You'll%20detect%20this%20movement%20and%20the%20use,visual%20timeline%20so%20you%20can%20decide%20how

across IT, public cloud and OT environments - is the largest repository of contextual exposure data worldwide and feeds all of Tenable's Exposure Management products.[34]

- Zscaler Inc (ZS): 3.10% weighting
    - Zscaler's AI-powered controls use generative AI to improve threat detection, prevention, and response. The controls are designed to detect millions of new attacks while safeguarding sensitive data and include AI-powered phishing detection, command-and-control detection, and cloud browser isolation.[35]
- Cloudflare (NET): 3.01% weighting
    - In May, Cloudflare extended its single-vendor SASE platform, Cloudflare One, to generative artificial intelligence (AI) services. Cloudflare One for AI, a suite of Zero Trust security controls, enables enterprises to safely and securely use the latest generative AI tools without putting intellectual property and customer data at risk.[36]
- Darktrace (DARK): 1.70% weighting
    - Darktrace is a leading company in the global AI-based cybersecurity domain. Darktrace's strength is linked to its AI research center with 200+ employees and 125+ patents and pending applications. It developed the first at-scale deployment of AI in cyber security, and is a pioneer in autonomous response technology. Most AI-based cybersecurity products typically rely on identifying threats based on historical attack data and reported techniques. However, Darktrace's self-learning AI is the only solution that learns from the organization's data and detects cyber-threats, even without reference to historic events. The company is unique in terms of its emphasis on scalable AI-based products, such as its automated Cyber AI Analyst, which sets it apart from its competitors. See 2Q'23 company spotlight and 1Q'23 cyber quarterly update (New Products section) for more details.
- F5 (FFIV): 3.06% weighting
    - Network trafficking manager with a focus on security and policy management in both on-premise data center and cloud environments. From an April 2023 press release:

> "In addition to AI-based enhancements for Distributed Cloud API Security, F5 is introducing AI-driven web application firewall (WAF) capabilities, including unique malicious user detection and mitigation capabilities that create a per-user threat score based on behavioral analysis that determines intent. This enables security operations to choose between alerting or automatic blocking to mitigate an attack that would otherwise go undetected by static signatures. With F5, all traffic is monitored and proactive defenses are applied based on malicious user behavior that can be correlated across Distributed Cloud WAAP deployments. New functionality also provides false positive suppression, making it easier to block bad traffic without accidentally blocking legitimate users, and streamlines operations by reducing the time necessary to enable specific app protections."[37]

- Gen Digital (GEN): 2.71% weighting
    - (Formerly NortonLifeLock): Gen Digital has a family of trusted Cyber Safety brands, Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner with a long track record of

[34] https://investors.tenable.com/news-releases/news-release-details/tenable-integrates-generative-ai-capabilities-across/#:~:text=%E2%80%9CFor%20years%2C%20Tenable%20has%20used,%2C%20Chief%20Technology%20Officer%2C%20Tenable
[35] https://www.zscaler.com/resources/zscaler-for-users
[36] https://www.cloudflare.com/press-releases/2023/zero-trust-security-to-safely-use-generative-ai/
[37] https://www.f5.com/company/news/press-releases/f5-safeguards-digital-services-new-ai-powered-app-api-security

providing security solutions to millions of users. In 2023, it offered access to Norton Genie, a real-time AI-powered scam detector, to provide an easy, fast, and free way to check if texts, emails, websites, and social media posts are a scam. LifeLock, Norton, Avast are industry leaders. LifeLock is the #1 most recognized brand in identity theft protection. Norton is the #1 Cyber Safety brand globally, empowering individuals and families with award-winning protection for their devices, online privacy, and identity. Avast is a global leader in digital security and privacy, using machine learning and artificial intelligence technologies to detect and stop threats in real time.[38]

- Juniper Networks (JNPR): 2.97% weighting
    - Its Connected Security products safeguards users, applications, and infrastructure by extending security to every point of connection, from client to cloud, across the entire network. It differentiates itself from competitors by providing security solutions for the network with one platform. It has tailored solutions for the following verticals: Healthcare, Higher Education, K-12 Education and Retail. Its security solutions span the following: next-generation firewalls, public cloud security, threat detection and mitigation, SD-WAN, Zero Trust Data Center, Service Provider Security. Its enterprise solutions are leveraging AI to optimize wireless and wired access, to optimize network performance and reliability. Its services now include a Mist AI engine which makes wireless networks more predictable.[39]
- Open Text (OTEX): 2.72% weighting
    - It provides a suite of products to power digital businesses, including Business Network (BN), Content Cloud, Experience Cloud, Security and Protection Cloud, and Developer Cloud with advanced technologies such as AI, automation, and analytics. Its OpenText™ Cybersecurity implements Zero Trust access across attack surfaces and leverages real-time threat intelligence. Its OpenText™ BrightCloud™ Threat Intelligence leverages AI for threat detection with comprehensive monitoring of attacks. Its Webroot™ Business Endpoint Protection utilizes advanced machine learning and offers cloud-based protection while other products help customers stay compliant with regulatory and industry standards, close cases quickly with reliable forensic investigation results, and provide backup.[40]
- Splunk (SPLK): 3.75% weighting
    - Its security solutions are designed for the modern SOC and include various security tools for several end-user industries. In addition to providing security solutions, it also provides solutions for cloud transformation, IT modernization, and digital resilience. Its security solutions include the Splunk Attack Analyzer, Splunk Enterprise Security, Splunk Mission Control, Splunk Security Essentials, and Splunk SOAR. These solutions provide real-time security visibility and threat detection, automating repetitive security tasks and securing against unknown threats. The company serves several industries, including aerospace and defense, communications, energy and utilities, financial services, healthcare, higher education, manufacturing, nonprofits, online services, public sector, and retail. It recently announced a new suite of AI offerings leveraging Generative AI to enhance the company's unified security and observability platforms. Splunk AI represents a series of AI solutions and capabilities that enable IT and security professionals to detect anomalies better and sift through large volumes of data. It launched a new AI assistant, AIOps capabilities, and AI-based machine learning models into Splunk.[41]

[38] https://newsroom.gendigital.com
[39] https://www.juniper.net/us/en/security.html
[40] https://www.opentext.com/solutions/line-of-business/security
[41] https://www.splunk.com/en_us/products/enterprise-security.html

- Trend Micro (4704): 2.78% weighting
    - Using advanced AI learning, Trend Micro stops ransomware. It also protects against malware, online banking and shopping threats. Trend Micro also uses machine learning to detect emerging security risks. Trend Micro Predictive Machine Learning (PML) uses digital DNA fingerprinting, API mapping, and other file features to correlate threat information and perform in-depth file analysis.[43]
- Akamai (AKAM): 3.15% weighting
    - Akamai is a content delivery network (CDN) and cloud services provider. They use artificial intelligence (AI) and machine learning (ML) to detect and defend against new attacks. For example, Akamai Brand Protect uses AI detectors to detect and disrupt phishing sites. Akamai also uses AI to detect bot traffic, mitigate malicious bots, manage good bots, and recognize trusted users.[44]
- SentinelOne (S): 2.99% weighting
    - In April, SentinelOne announced a new threat-hunting platform, which uses generative AI to identify and stop attacks and combines real-time neural networks and a large language model (LLM)-based natural language interface. The platform is designed to help users monitor and operate security data and increase productivity. It uses multiple layers of AI technology to provide security capabilities and real-time, autonomous responses to attacks. Additionally, the platform uses generative ChatGPT-4 and neural networks to identify and thwart attacks. SentinelOne also offers SentinelOne Singularity, an enterprise cybersecurity platform that provides prevention, detection, and response.[45]

Sources: Nasdaq Global Indexes, Bloomberg, Pitchbook.

[43] https://success.trendmicro.com/dcx/s/solution/1122594-configuring-predictive-machine-learning-settings-in-apex-one?language=en_US&sfdcIFrameOrigin=null#:~:text=Trend%20Micro%20Predictive%20Machine%20Learning,mapping%2C%20and%20other%20file%20features.
[44] https://www.akamai.com/blog/security/akamai-announces-advanced-bot-detections#:~:text=In%20fact%2C%20we're%20announcing%20enhancements%20today%20that,Akamai%20customers%20benefit%20from%20a%20network%20effect%2C
[45] https://ciosea.economictimes.indiatimes.com/news/security/sentinelone-unveils-new-ai-platform-for-cybersecurity/99748726#:~:text=The%20SentinelOne%20threat%2Dhunting%20platform%20seamlessly%20fuses%20real%2Dtime%2C,boost%20their%20productivity%20and%20scale%20their%20operations.