Cybersecurity

Challenges and promise of AI in cybersecurity

FIRST ANALYSIS QUARTERLY INSIGHTS

Integrative insights on emerging opportunities

January 28, 2025

First Analysis

Howard Smith

Direct: 312-258-7117
hsmith@firstanalysis.com

Main: 312-258-1400
www.firstanalysis.com

Liam Moran

Direct: 312-258-7197
lmoran@firstanalysis.com

First Analysis Cybersecurity Team

Howard Smith

Managing Director
hsmith@firstanalysis.com
312-258-7117

Matthew Nicklin

Managing Director
mnicklin@firstanalysis.com
312-258-7181

Liam Moran

Associate
lmoran@firstanalysis.com
312-258-7197

About the Authors

Howard Smith

Howard Smith is a managing director at First Analysis and is a managing partner of the firm's venture funds. He has over three decades of experience at First Analysis and works with entrepreneurs as an investor and as an advisor on growth transactions to help build leading technology businesses. Howard leads the firm's work in the cybersecurity, internet infrastructure and Internet of Things sectors. He also built the firm's historical franchises in call centers and computer telephony. His thought-leading research in these areas has been cited for excellence by the Wall Street Journal and other publications. He supports First Analysis' investments in EdgeIQ, Fortress Information Security, ObservIQ, Stamus Networks and Tracer. Prior to joining First Analysis in 1994, he was a senior tax consultant with Arthur Andersen & Co. He earned an MBA with honors from the University of Chicago and a bachelor's degree in accounting with highest honors from the University of Illinois at Urbana-Champaign. He is a certified public accountant.

Liam Moran

Liam Moran is an associate with First Analysis. Prior to joining First Analysis in 2020, he was in the executive development program with Macy's, where he was responsible for managing the financial modeling surrounding Macy's $3 billion asset-based loan, capital project valuations, and corporate forecasting. Liam graduated from Kenyon College with a bachelor's degree in economics and a concentration in integrated program in humane studies. He was a four-year member of the Kenyon varsity swimming team.

About First Analysis

First Analysis has a four-decade record of serving emerging growth companies, established industry leaders, and institutional investors in emerging high-growth tech-driven sectors, both through its venture capital investments and through First Analysis Securities Corp. (FASC), which provides investment banking and related services. FASC is a FINRA-registered broker-dealer and member SIPC. First Analysis's integrative research process underpins all its efforts, combining 1) dynamic investment research on thousands of companies with 2) thousands of relationships among executives, investors, and other key participants in our focus areas, yielding a deep, comprehensive understanding of each sector's near-term and long-term potential.

First Analysis

1 S. Wacker Dr., Suite 3900
Chicago, IL 60606
312-258-1400
www.firstanalysis.com

CYBERSECURITY

Challenges and promise of AI in cybersecurity

- We reflect on both the frustrations and successes we've heard about AI in cybersecurity.
- The biggest hope for AI in cybersecurity is that it can prevent attacks, detecting and potentially blocking novel attacks before they can cause damage; however, such solutions have not been the silver bullet they were hoped to be.
- In the near-term, we believe it will be challenging to implement AI to detect zero-day and novel threats due to the unpredictable nature of these attacks and the difficulty AI has in distinguishing harmless anomalies from true threats. Efforts to address these shortcomings with information transparency also face challenges.
- We're seeing the most success among solutions that use AI to improve cybersecurity teams' ability to interact with traditional cybersecurity approaches. By bridging the gap between technical complexity and human understanding, these AI solutions streamline security operations centers, enabling teams to be more efficient and effective.

FRUSTRATIONS ALONG WITH SOME SUCCESSES

AI has had a dramatic effect on the cybersecurity industry in the past year. In this report, we reflect on both the frustrations and successes we've heard about in the market. In terms of frustrations, the biggest hope for AI in cybersecurity is that it can prevent attacks, detecting and potentially blocking novel attacks before they can cause damage; however, such solutions have not been the silver bullet they were hoped to be. Among the successes are more mundane AI capabilities – such as using large language models (LLMs) to query data and enhance explanations. These solutions have received less hype compared to AI detection capabilities, but they are the most impactful use of AI we've seen to date. We believe they have the potential to transform how security operations operate in relatively short order.

DETECTING AND BLOCKING NOVEL ATTACKS – THE CHALLENGE OF FALSE ALERTS

One of the most challenging aspects of defending organizations against cyberattacks is identifying and stopping attacks quickly to prevent or minimize damage. This is difficult for known vulnerabilities and attack vectors; it is even more difficult for zero-day vulnerabilities and novel attack vectors, which, by definition, have not been seen before so cannot be identified or stopped with widely available signatures and rule updates. But with AI, organizations are successfully detecting and blocking even novel attacks because AI excels at quickly identifying anomalous behavior and data traffic patterns and other suspicious activity and conditions. We have heard of numerous examples of zero-day threats found and mitigated with AI.

However, there are two related drawbacks. The first is false positives. AI detects threats that legacy methods would have missed, but it also perceives many harmless activities and patterns as threats. False positives are not a new problem in cybersecurity solutions. And some AI enthusiasts contend false positive alerts (alerting cybersecurity personnel to harmless actions) is valuable because unusual activity is noteworthy, regardless of whether the cause is malicious. However, our conversations indicate this a minority view.

What makes AI false positives particularly problematic is a related shortcoming of AI: Unlike traditional solutions that provide information trails that cybersecurity personnel can follow to determine whether or not alerts are truly threats, AI detection solutions are too often black boxes that provide little or no forensic and other background data to help security operations center teams determine the basis the solutions use for generating their alerts. As a result, figuring out whether AI alerts warrant attention can be much more difficult than doing the same for traditional alerts.

The drawbacks of this lack of forensic and other background data extends to leaving organizations using AI detection solutions less able to improve their security postures overall. Security organizations like to learn from threats and breaches to help harden their organizations against future attacks. If they're unable to do this because they use an AI detection solution, they're inherently depending on their AI solution to detect and block nearly every attack because their traditional cyber defenses cease to evolve. If an AI solution can't block nearly every attack, then the organization is probably better off using a more traditional approach that catches most attacks and also enables its cybersecurity team to use the findings from those attacks to block numerous similar attacks in the future.

POTENTIAL FOR TRANSPARENT AI DETECTION SOLUTIONS

Because of AI detection's drawbacks, we are seeing demand for transparent AI detection solutions. These systems explain the reasons for their alerts. However, the nature of AI makes it very hard for these solutions to provide the logic behind alerts and even harder to explain the logic in terms that can be understood by human security teams. This challenge presented by the inherent opacity of AI logic is compounded by the nature of rapidly evolving cybersecurity threats.

We highlight two aspects of this issue. First, the very nature of detecting threats in complex environments with AI solutions is at odds with creating easily transparent AI solutions. Making AI models more transparent often comes at the expense of accuracy and effectiveness – a tradeoff acceptable in some industries but not in cybersecurity. Further, one of the primary reasons for using AI is its speed of detecting new threats. Anything that slows detection responses detracts from the value of using AI detection solutions, and providing transparency can slow AI responses. Lastly, cybersecurity threats can be extremely complex and involve analyzing interdependencies among many systems. This complexity combined with the dynamic nature of threat detection makes explanations of logic behind detections just as dynamic and complicated.

Second, efforts to explain the logic behind alerts help adversaries create attacks to evade detection. Attackers could systematically reverse engineer AI solutions' detection methods to counteract the solutions' effectiveness over time. By contrast, opaque AI detection alerts force adversaries to operate with incomplete information, increasing their likelihood of failure. We caveat that we have not seen high levels of transparency in cybersecurity solutions, so we have not seen much pushback on its benefit.

THE BOTTOM LINE FOR AI DETECTION: HYBRID APPROACHES FIRST

Near term, we believe it will be challenging to implement AI to detect zero-day and novel threats due to the unpredictable nature of these attacks and the difficulty AI has in distinguishing harmless anomalies from true threats. This is particularly true in high-stakes organizations such as critical infrastructure businesses, finance, and healthcare, where operational disruptions caused by false positives – or overreliance on advanced AI solutions – can have significant consequences. However, as AI models improve and training data becomes more robust, we believe AI's precision and reliability will increase, enabling broader adoption across industries with lower tolerance for cybersecurity and operational risk.

In the immediate term, we see potential in the hybrid approach that combines advanced AI models with more traditional detection methods. This could balance the benefit of quickly detecting sophisticated threats with enhanced visibility into the decision-making processes behind alerts. With clear explanations, cybersecurity professionals can refine defenses, build trust in their AI systems, and better understand how they can improve overall security posture. Over time, this unified approach could harmonize cutting-edge detection capabilities with greater transparency, offering organizations a more comprehensive and reliable defense strategy. We continue to monitor the market for solutions that aim to combine these approaches.

AI SUCCESS IN CYBERSECURITY: ENHANCING TRADITIONAL CYBERSECURITY SOLUTIONS

We have discovered the most common use of AI in both solutions and customer implementations is to improve cybersecurity

Responding to a critical attack: Where AI is involved and where it isn't

DETECT

AI prioritizes alerts from either AI-based or traditional detection methods through data analysis and event correlation

Active alerts feed

Critical priority

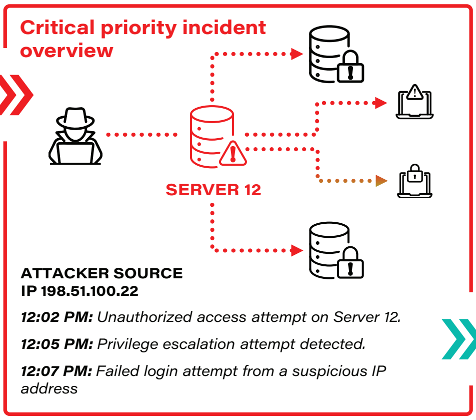
Privilege escalation attempt detected on Server 12 originating from IP 198.51.100.22

High priority

Suspicious software execution on Node C potentially linked to ransomware

Medium priority

Unusual file transfer detected from User X to external storage device



Critical priority incident overview

ATTACKER SOURCE
IP 198.51.100.22

12:02 PM: *Unauthorized access attempt on Server 12.*

12:05 PM: *Privilege escalation attempt detected.*

12:07 PM: *Failed login attempt from a suspicious IP address*

RESPOND

AI provides role-based explanations of complex threats in common language with **recommended remediation steps**

Threat explanations and recommended actions help speed the time to response

Executive role

A critical security threat has been identified: an unauthorized attempt to gain administrative access to Server 12 from external IP 198.51.100.22. This could be a sophisticated cyberattack. Immediate actions are underway to contain the threat and protect system integrity. Updates will follow as the situation progresses.

Technical cybersecurity analyst role

An alert was triggered due to an unauthorized privilege escalation attempt on Server 12 from IP 198.51.100.22, suggesting a targeted advanced persistent threat. Immediate containment and mitigation is needed.

Recommended Actions:

1. ***Block IP:*** *Immediately block traffic to/from IP 198.51.100.22*
2. ***Quarantine server:*** *Isolate Server 12 to prevent further compliance*
3. ***Forensic analysis:*** *Investigate the breach's extent and exploited vulnerabilities*
4. ***Credential reset:*** *Reset all privileged credentials on Server 12*

Source: First Analysis.

teams' ability to interact with traditional cybersecurity software. Cybersecurity alerts, whether AI-generated or not, are often highly technical and accompanied by raw data that has little meaning for a human reader. Exceptionally experienced cybersecurity personnel operating in well-known environments might be able to quickly interpret this and know what actions are required. However, most personnel need to spend substantial time researching the alerts they receive and determining responses, often drawing on colleagues for help.

AI addresses this challenge. With AI-powered chat bots and similar features built into cybersecurity solutions, users can use prompts like "provide more detail," "suggest appropriate mitigation measures," and "is there a mitigation solution that is less disruptive to the end user," and well-trained LLM-based solutions will respond with valuable answers. AI tools can also help cybersecurity personnel dig deeper into issues, such as by easily querying vast amounts of log data and tracing connections between seemingly unrelated events to identify root causes.

Additionally, AI systems can dynamically adjust reporting and dashboards to suit users' expertise, offering in-depth technical insights to seasoned security professionals while presenting simplified explanations to less technical executives. This capability not only enhances collaboration across teams but also ensures critical information is accessible to everyone involved. By bridging the gap between technical complexity and human understanding, AI streamlines security operations centers, enabling teams to be more efficient and effective in adjusting cybersecurity posture to keep up with today's rapidly evolving threat landscape.

AI CAN BE A KEY PARTNER IN CYBERSECURITY EFFORTS

To capture the full value of AI in cybersecurity, cybersecurity personnel must expand their skills to include proficiently writing appropriate and relevant AI prompts and queries. Nonetheless, AI's ability to both explain and investigate alerts enables less technically experienced personnel to be involved in security operations, potentially helping alleviate the shortage of skilled cybersecurity professionals, and makes it a strong partner for everyday cybersecurity operations.

Cybersecurity index: Volatile summer, but gains since September

The First Analysis Cybersecurity Index gained 17% over the one-year period ended Jan. 16 but trailed the Nasdaq by 12.4 points and the S&P 500 by 7.6 points. The cybersecurity index's gain over the period peaked at 25% in mid-December, and it subsequently declined during the Dec. 18 market sell-off along with the other indexes and has remained rangebound since then.

Of the 17 cybersecurity stocks, eight appreciated by more than 15%, led by OneSpan (OSPN), up 86%, and CyberArk (CYBR), up 56%. Fortinet (FTNT), the third-largest-capitalization company in the space accounted for 7 points the index's total gain. CrowdStrike (CRWD), the second-largest-capitalization company, accounted for another 5 points. Of the nine other stocks,

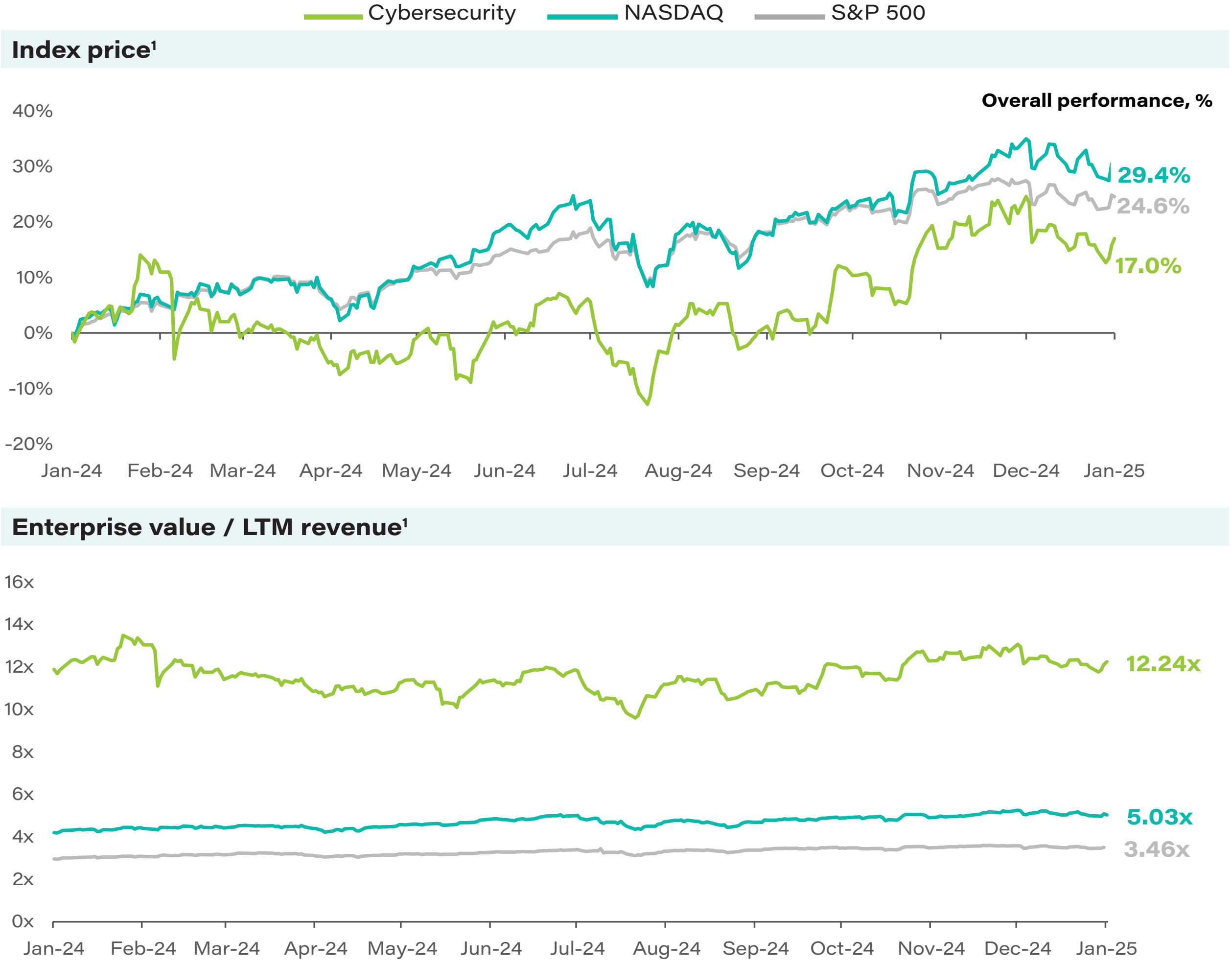
Cybersecurity public comparables*

($ in millions)		Revenue growth				Enterprise value /			
						Revenue		EBITDA[1]	
Company	**LTM revenue**	**2023A - 2024E**	**2024E - 2025E**	**LTM gross margin**	**LTM EBITDA margin**	**2024E**	**2025E**	**2024E**	**2025E**
Check Point Software Tech. (CHKP)	$2,524.8	6.0%	5.7%	88.6%	36.7%	6.92x	6.54x	15.7x	15.7x
Cloudflare (NET)	1,572.2	28.2%	26.1%	77.5%	(2.8%)	23.49x	18.63x	NMF	NMF
CrowdStrike (CRWD)	3,740.4	28.6%	21.5%	75.2%	3.7%	21.90x	18.03x	NMF	NMF
CyberArk Software (CYBR)	909.5	31.3%	32.0%	81.1%	(3.6%)	16.77x	12.70x	NMF	NMF
Fortinet (FTNT)	5,710.8	11.1%	12.6%	79.7%	30.3%	11.79x	10.47x	33.1x	33.1x
Okta (OKTA)	2,533.0	14.8%	7.9%	76.1%	(2.1%)	5.16x	4.78x	22.9x	22.9x
OneSpan (VDSI)	244.9	2.2%	3.4%	71.1%	21.4%	2.73x	2.64x	9.9x	9.9x
Palo Alto Networks (PANW)	8,288.2	13.6%	14.6%	74.2%	13.8%	13.33x	11.63x	43.1x	43.1x
Qualys (QLYS)	593.0	9.0%	7.7%	81.5%	33.6%	7.39x	6.87x	16.4x	16.4x
Radware (RDWR)	266.9	4.6%	6.4%	80.5%	(2.6%)	2.26x	2.13x	18.6x	18.6x
Rapid7 (RPD)	833.0	8.0%	5.5%	70.6%	10.8%	3.68x	3.49x	16.5x	16.5x
SecureWorks (SCWX)	339.7	(9.8%)	4.2%	66.8%	(8.1%)	2.13x	2.04x	19.1x	19.1x
SentinelOne (S)	770.1	31.7%	25.7%	73.6%	(37.8%)	7.94x	6.31x	NMF	NMF
Tenable Holdings (TENB)	877.6	12.2%	9.7%	77.5%	1.7%	5.56x	5.07x	26.5x	26.5x
Trend Micro (TSE: 4704)	1,723.4	9.0%	5.6%	76.1%	27.0%	3.37x	3.19x	12.5x	12.5x
Varonis Systems (VRNS)	546.5	11.8%	12.4%	84.1%	(17.2%)	8.43x	7.50x	NMF	NMF
Zscaler (ZS)	2,299.0	27.1%	20.0%	78.0%	(3.0%)	11.33x	9.45x	45.9x	45.9x
Average	***$1,986.6***	***14.1%***	***13.0%***	***77.2%***	***6.0%***	***9.07x***	***7.73x***	***23.4x***	***23.4x***
Median	***$909.5***	***11.8%***	***9.7%***	***77.5%***	***1.7%***	***7.39x***	***6.54x***	***18.8x***	***18.8x***

Source: Capital IQ, First Analysis.

Notes: * Public comparable company data shown above is as of Jan. 16, 2025.
(1) EBITDA multiples less than 0 and greater than 50 labeled "not meaningful" (NMF). LTM = last 12 months. EBITDA = earnings before interest, taxes, depreciation and amortization.

First Analysis Cybersecurity Index 1-year performance


Index price[1]

Enterprise value / LTM revenue[1]

Source: Capital IQ.

Notes: (1) Index performance is weighted by market cap. For the period from Jan. 16, 2024, through Jan. 16, 2025.

seven were down over the period, including Rapid7 (RDP) and Qualys (QLYS), which were each down by more than 25%.

The index's enterprise value multiple of trailing-12-month revenue as of Jan. 16 was 12.2, up slightly from 11.9 at the beginning of the one-year period and only modestly below its peak of 13.5 on Feb. 9. It is still well above the Nasdaq's 5.0. The average enterprise value multiple of estimated revenue is 9.1 for 2024 and 7.7 for 2025. Cloudflare (NET) trades at the highest multiple for estimated 2024 revenue (23.5) and estimated 2025 revenue (18.6), narrowly ahead of CrowdStrike with a 21.9 multiple for 2024 and 18.0 for 2025. Revenue growth on average is expected to be 13.0% in 2025, down from 14.3% in our July 2024 report.

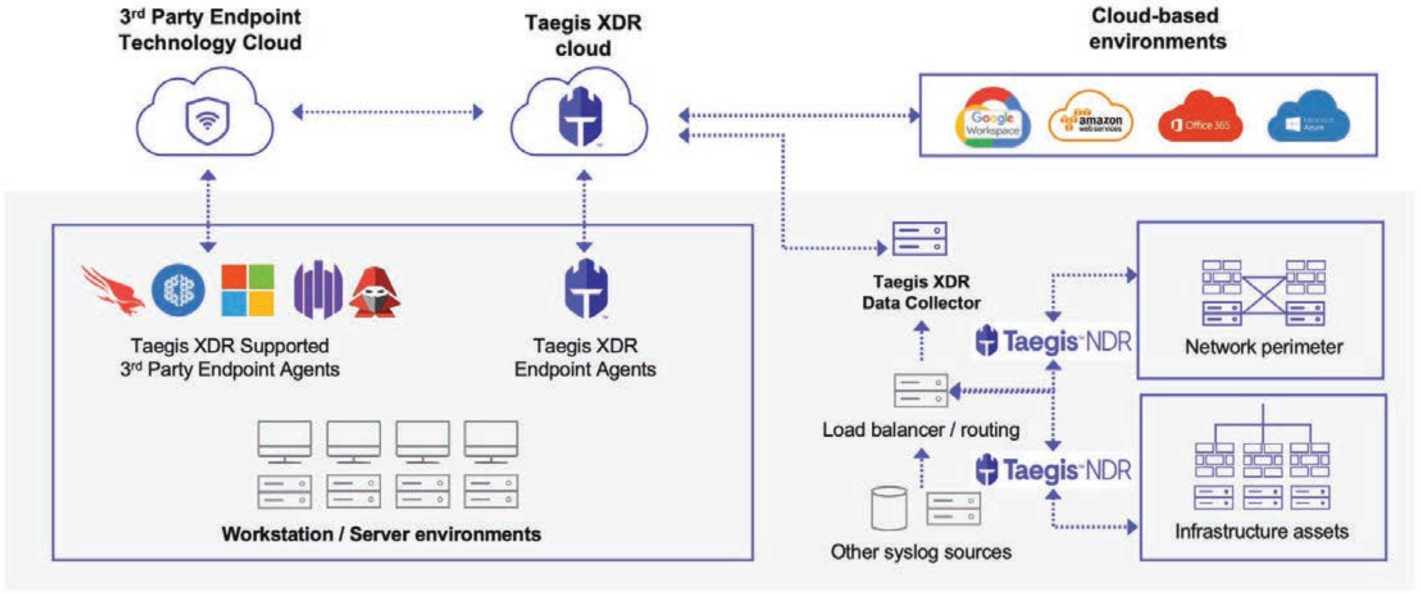
Since our last publication, we have removed one constituent from the First Analysis Cybersecurity Index: Darktrace, following its acquisition by Thoma Bravo. The metrics above reflect this change for the current period.

Cybersecurity M&A: Notable transactions include SecureWorks, Dazz, and Fend

We highlight three noteworthy cybersecurity merger and acquisition announcements from the fourth quarter.

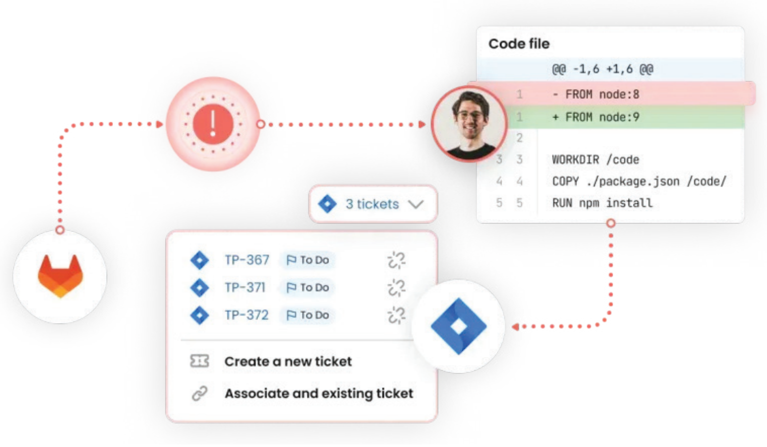
On Oct. 21, SecureWorks (SCWX), a First Analysis Cybersecurity Index constituent, announced it would be acquired by Sophos in an all-cash transaction that valued the company at $859 million, or 2.4 times trailing 12-month (August) revenue. The price of $8.50 per share was a 28% premium to SecureWorks' volume-weighted average price over the prior three months. Sophos, backed by private equity firm Thoma Bravo, is a leading provider of managed security services and end-to-end security products. It plans to integrate SecureWorks' Taegis platform to deliver complementary advanced managed detection and response (MDR) and extended detection and response (XDR) capabilities. Sophos plans to use SecureWorks to broaden the Sophos solution and enhance its strengths in identity threat detection and response (ITDR), next-gen security information and event management (SIEM) capabilities, operational technology security, and enhanced vulnerability risk prioritization. The combined company hopes to achieve greater market presence broadly across small, mid-size, and enterprise customers. The acquisition is expected to be completed in early 2025.

Taegis, SecureWorks' extended detection and response platform, integration overview



Source: SecureWorks.

Dazz helps prioritize time and cybersecurity professional resources with simple remediation workflows



Code file

```
@@ -1,6 +1,6 @@
- FROM node:8
+ FROM node:9

WORKDIR /code
COPY ./package.json /code/
RUN npm install
```

Source: Dazz.

In late November, Wiz announced it would acquire Dazz for $450 million. Dazz provides a remediation engine that enables security teams to correlate data from multiple sources and manage application risks in a unified platform. The company's mapping capabilities help pinpoint root issues, enabling engineers to address vulnerabilities directly in code while integrating important context from the cloud environment into security workflows. Wiz's platform scans applications, data and network flows for security risks and offers detailed views to help users understand where those risks exist. Wiz's co-founder Ami Luttwak expects with Dazz's application security posture management capabilities and remediation expertise, the combined company will provide "a 360-degree view of risk, covering infrastructure and application." This marks Wiz's third acquisition, following Raftt Systems in late 2023 and Gem Security in early 2024, after having raised over $1 billion in February 2023.

On Dec. 18, Fend, a company we featured in our December 2021 quarterly report on data diodes security, was acquired by Opswat, a global leader in information technology, operational technology, and industrial control system critical infrastructure cybersecurity. Fend helps secure operational technology against threats with the company's data diode, or unidirectional gateway, solution. This hardware-based solution secures one-way communication channels, allowing data to flow from one network to another while physically blocking the reverse direction. The company has expertise in protecting U.S. government agencies, utilities, and oil and gas, manufacturing and other critical industries where air-gapped environments are necessary to prevent threats. Fend's capabilities broaden Opswat's end-to-end solution platform for protecting complex networks and ensuring compliance.

Fend's XE15 data diode brings industrial equipment online with total security of full optical isolation

Source: Fend.

Select recent M&A transactions *(sorted by date of announcement)*

($ in millions)

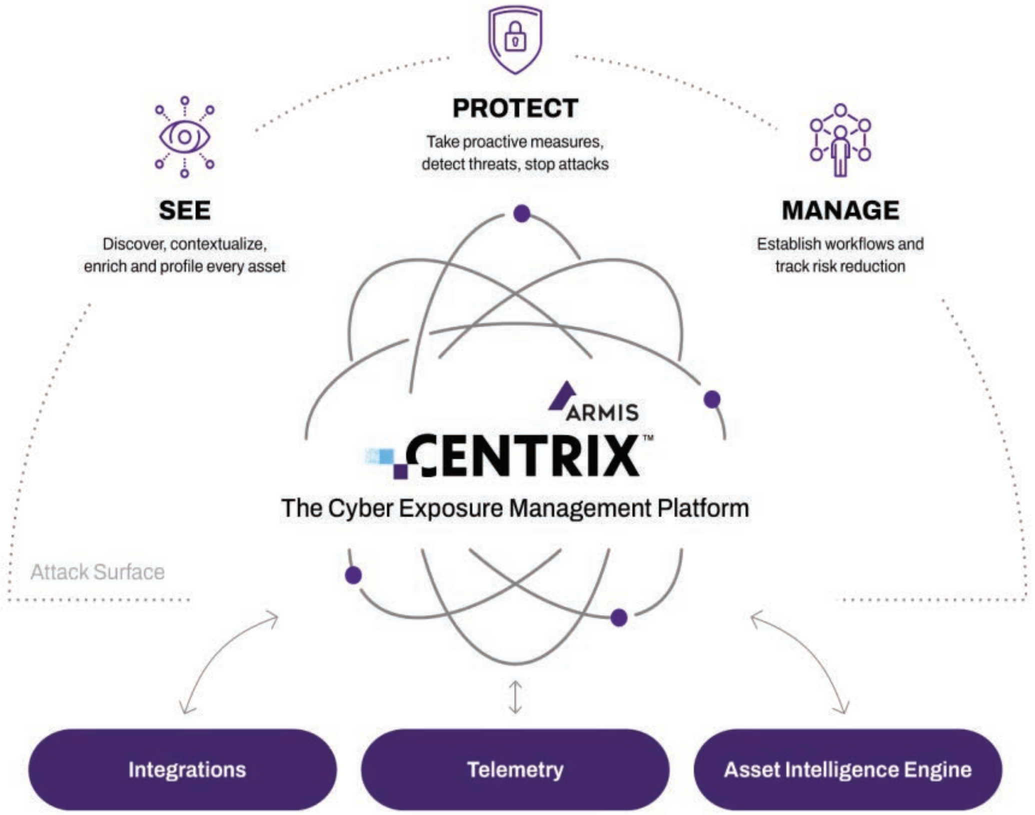
Date	Target	Target business description	Buyer	Enterprise value	Enterprise value/rev
1/9/2025	Cado Security	Forensic analysis platform that automates threat detection across multiple environments	Darktrace	Undisclosed	Undisclosed
12/18/2024	Fend	Hardware cybersecurity solutions that use network segmentation and data diodes to protect critical infrastructure from cyberattacks and ransomware	Opswat	Undisclosed	Undisclosed
12/11/2024	Perception Point	AI-powered threat prevention solutions that protect email, web browsers, and cloud apps from advanced cyber threats	Fortinet (FTNT)	Undisclosed	Undisclosed
11/21/2024	Dazz	Unified platform that streamlines the remediation process of security issues across cloud environments, code, applications, and infrastructure	Wiz	$450.0	Undisclosed
11/20/2024	Adlumin	End-to-end security operations platform that provides monitoring, incident response, and proactive threat management solutions	N-able (NABL)	$265.9	12.1x
11/6/2024	Mission Secure	Cyber defense solutions for industrial control systems to protect against cyber threats, internal threats, and supply chain disruptions	ServiceNow (NOW)	Undisclosed	Undisclosed
11/6/2024	Adaptive Shield	SaaS security posture management provider that helps organizations monitor and improve the security of their applications	CrowdStrike (CRWD)	$200.7	Undisclosed
10/21/2024	SecureWorks (SCWX)	Intelligence-driven information security solutions provider that helps organizations prevent, detect and respond to cyber threats	Sophos	$859.0	2.5x
10/8/2024	Kivera	Solutions designed to safeguard cloud usage for highly regulated organizations	Cloudfare (NET)	$29.4	Undisclosed
10/2/2024	Prevalent	Third-party risk management and compliance solutions provider that helps organizations assess, monitor and mitigate vendor risks	Mitratech Holdings	Undisclosed	Undisclosed

Source: Capital IQ, First Analysis.

Cybersecurity private placements: Notable transactions include Armis and Upwind

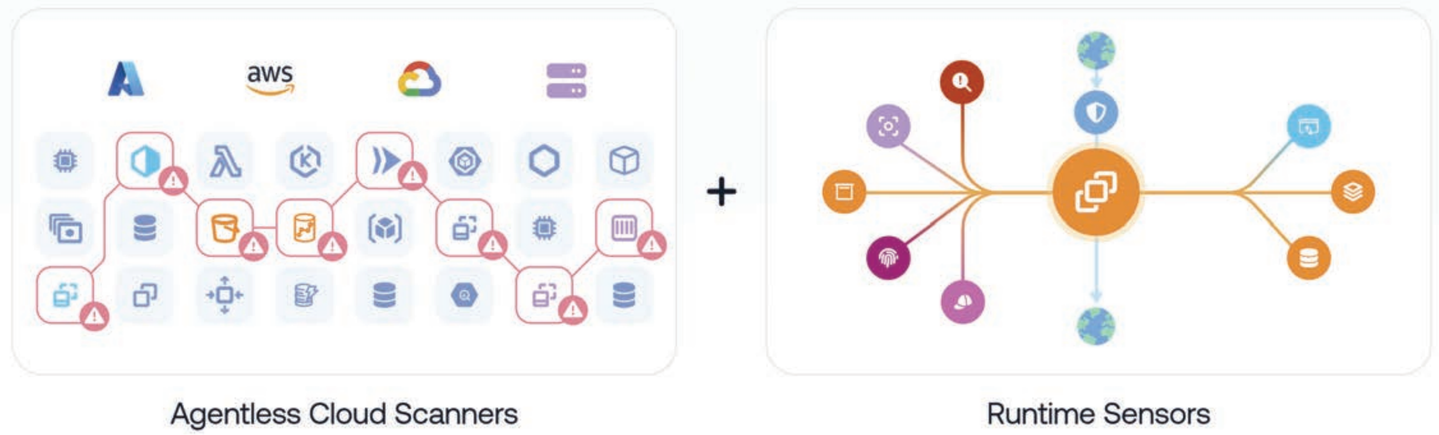
In late October, Armis announced it received $200 million in a Series D funding co-led by new investors General Catalyst and Alkeon Capital and including participation from returning investors Brookfield Growth, Georgian, Insight Ventures, Capital G and OEP Capital. Armis provides a comprehensive cyber-exposure management platform for asset management and physical systems, remediation of vulnerabilities, onsite and cloud infrastructure, and continuous integration and continuous delivery pipelines. The company plans to use the capital to fuel product innovation, go-to-market programs and, potentially, acquisitions. The company earlier announced it had surpassed $200 million annualized recurring revenue (ARR). The round was raised at a post-money valuation of $4.3 billion, or about 21.5 times ARR. The company plans to pursue an initial public offering after reaching $1 billion in ARR.

Armis Centrix platform operationalizes the remediation life cycle by prioritizing risk and recommendation workflows


PROTECT
Take proactive measures, detect threats, stop attacks
SEE
Discover, contextualize, enrich and profile every asset
MANAGE
Establish workflows and track risk reduction
ARMIS
CENTRIX™
The Cyber Exposure Management Platform
Attack Surface
Integrations
Telemetry
Asset Intelligence Engine

Source: Armis.

Upwind Security's cloud scanners discover inventory and security posture while runtime sensors prioritize real risks and protect in real time



Source: Upwind Security.

On Dec. 2, Upwind Security announced a $100 million series A funding led by Craft Ventures and joined by TCV and Alta Park along with existing investors Greylock, Cyberstarts, Leaders Fund, Cerca and Sheva. The post-money valuation was $900 million. Upwind Security develops a runtime detection and response platform to secure cloud-native infrastructure. The company helps streamline the overwhelming quantity of alerts generated from threat detection tools, enabling teams to concentrate on the most actionable genuine threats and thereby shrinking response times. With the proceeds, the company plans primarily to fuel research and development efforts for threat intelligence and cloud security automation. In addition, the company plans to expand its market presence across its three locations in Israel, San Francisco and Iceland. This was the company's third institutional round and brings the total funding to date to $180 million.

Select recent private placements *(sorted by date of announcement)*

($ in millions) Date	Company	Business description	Investors	Raise type	Amount raised	Total amount raised
1/7/2025	360 Advanced	Cybersecurity and compliance solutions designed to improve security, streamline regulatory compliance, and support business growth	Bregal Sagemount	Growth	Undisclosed	Undisclosed
12/16/2024	CISO Global (CISO)	End-to-end cybersecurity and compliance solutions that manage security operations, streamline risk management, and strengthen organizations' cybersecurity resilience	Target Capital	PIPE	$6.5	NA
12/16/2024	Keepit	Cloud-based backup and recovery solutions to protect and secure data from SaaS platforms like Microsoft 365, Google Workspace and Salesforce	One Peak Partners and Investment Fund of Denmark	Growth	$50.0	$90.0
12/12/2024	Sublime Security	Cloud email security platform that provides advanced threat detection, visibility and customization for security teams	IVP; Citi Ventures; Index Ventures; Decibel Partners; Slow Ventures	Series B	$60.0	$93.8
12/10/2024	Astrix Security	Security solutions to protect organizations from risks associated with third-party integrations, focusing on managing and securing access between external apps and SaaS platforms	Menlo Ventures Management; Anthropic; Charles River Ventures; Deer Management; F2 Capital; Workday Ventures	Series B	$45.0	$95.0
12/4/2024	Tuskira	AI-powered security platform that integrates and optimizes multiple tools to preemptively defend against cyber threats, reduce vulnerabilities and improve defense posture	Intel Capital; SYN Ventures; Sorenson Capital, Rain Capital; Wipro Venture	Series A	$28.5	$28.5
11/21/2024	Silent Push	Advanced threat intelligence solutions, focusing on detecting and analyzing malicious infrastructure to protect organizations from cyber threats	StepStone (STEP); Ten Eleven Ventures	Series A	$10.0	$20.0
11/19/2024	ThreatMon	Cybersecurity company providing tailored solutions for businesses of various scale to safeguard their digital assets	Pragma Capital Partners	Growth	Undisclosed	Undisclosed
11/8/2024	Upwind Security	Cloud security provider securing cloud infrastructure by leveraging runtime data to identify, mitigate and automate responses to critical security threats	Alta Park Capital; Cerca Partners; Craft Ventures; Cyberstarts; Greylock Partners; Leaders Fund; Sheva Fund; Technology Crossover Ventures	Series A	$100.0	$177.4
10/31/2024	Halcyon	Protects enterprises from ransomware by providing advanced prevention, detection and mitigation solutions tailored to combat sophisticated cyber threats	Bain; Corner Capital; Dropbox; Evolution Equity Partners; ServiceNow Ventures; SYN Ventures; The Harmony Group	Growth	$127.8	$190.0
10/30/2024	MIND	Data security platform that automates data loss prevention and insider risk management to protect sensitive information and mitigate risk	YL Ventures; Adobe (ADBE); ADT (ADT); Crowdstrike (CRWD); FireEye (FEYE)	Seed	$11.0	$11.0
10/28/2024	Filigran	Cybersecurity platform that provides threat intelligence and simulation solutions for crisis preparation and management	Accel; Insight Partners; Moonfire	Series B	$35.0	$56.6

Select recent private placements *(sorted by date of announcement)*

($ in millions) Date	Company	Business description	Investors	Raise type	Amount raised	Total amount raised
10/28/2024	Armis	Cyber exposure and security company that protects organizations' attack surface and manages cyber risk in real time	Alkeon Capital; General Catalyst; Brookfield Growth; Georgian	Series D	$200.0	$737.0
10/24/2024	Concentric AI	AI-powered data security solution that discovers, categorizes, and protects critical business data across on-premises, cloud, and communication platforms	Top Tier Capital Partners;HarbourVest Partners; CyberFuture; Ballistic Ventures; Engineering Capital; Clear Ventures; Citi Ventures	Series B	$45.0	$67.0
10/23/2024	Craftt	Decentralized platform providing access to benefits to create a seamless and connected workforce for independent workers	Digital Currency Group; Superscrypt	Seed	$2.0	$2.0

Source: Capital IQ, First Analysis.

Cybersecurity public comparables appendix*

($ in millions)				Revenue growth				Enterprise value /			
								Revenue		EBITDA[1]	
Company	**Market cap**	**Enterprise value**	**LTM revenue**	**2023A - 2024E**	**2024E - 2025E**	**LTM gross margin**	**LTM EBITDA margin**	**2024E**	**2025E**	**2024E**	**2025E**
Check Point Software Tech. (CHKP)	$20,541.4	$17,703.8	$2,524.8	6.0%	5.7%	88.6%	36.7%	6.92x	6.54x	15.7x	15.7x
Cloudflare (NET)	39,405.5	39,032.4	$1,572.2	28.2%	26.1%	77.5%	(2.8%)	23.49x	18.63x	NMF	NMF
CrowdStrike (CRWD)	89,504.6	86,073.9	$3,740.4	28.6%	21.5%	75.2%	3.7%	21.90x	18.03x	NMF	NMF
CyberArk Software (CYBR)	17,523.7	16,564.4	$909.5	31.3%	32.0%	81.1%	(3.6%)	16.77x	12.70x	NMF	NMF
Fortinet (FTNT)	72,084.9	69,461.1	$5,710.8	11.1%	12.6%	79.7%	30.3%	11.79x	10.47x	33.1x	33.1x
Okta (OKTA)	14,680.0	13,392.0	$2,533.0	14.8%	7.9%	76.1%	(2.1%)	5.16x	4.78x	22.9x	22.9x
OneSpan (VDSI)	724.5	656.6	$244.9	2.2%	3.4%	71.1%	21.4%	2.73x	2.64x	9.9x	9.9x
Palo Alto Networks (PANW)	116,259.0	113,966.3	$8,288.2	13.6%	14.6%	74.2%	13.8%	13.33x	11.63x	43.1x	43.1x
Qualys (QLYS)	4,995.3	4,469.9	$593.0	9.0%	7.7%	81.5%	33.6%	7.39x	6.87x	16.4x	16.4x
Radware (RDWR)	913.4	619.0	$266.9	4.6%	6.4%	80.5%	(2.6%)	2.26x	2.13x	18.6x	18.6x
Rapid7 (RPD)	2,515.0	3,092.9	$833.0	8.0%	5.5%	70.6%	10.8%	3.68x	3.49x	16.5x	16.5x
SecureWorks (SCWX)	750.2	702.0	$339.7	(9.8%)	4.2%	66.8%	(8.1%)	2.13x	2.04x	19.1x	19.1x
SentinelOne (S)	7,137.0	6,496.8	$770.1	31.7%	25.7%	73.6%	(37.8%)	7.94x	6.31x	NMF	NMF
Tenable Holdings (TENB)	5,116.6	4,977.9	$877.6	12.2%	9.7%	77.5%	1.7%	5.56x	5.07x	26.5x	26.5x
Trend Micro (TSE: 4704)	7,142.6	5,875.0	$1,723.4	9.0%	5.6%	76.1%	27.0%	3.37x	3.19x	12.5x	12.5x
Varonis Systems (VRNS)	5,160.2	4,704.3	$546.5	11.8%	12.4%	84.1%	(17.2%)	8.43x	7.50x	NMF	NMF
Zscaler (ZS)	28,777.4	27,308.3	$2,299.0	27.1%	20.0%	78.0%	(3.0%)	11.33x	9.45x	45.9x	45.9x
Average	***$25,484.2***	***$24,417.4***	***$1,986.6***	***14.1%***	***13.0%***	***77.2%***	***6.0%***	***9.07x***	***7.73x***	***23.4x***	***23.4x***
Median	***$7,142.6***	***$6,496.8***	***$909.5***	***11.8%***	***9.7%***	***77.5%***	***1.7%***	***7.39x***	***6.54x***	***18.8x***	***18.8x***

Source: Capital IQ.

Notes: * Public comparable company data shown above is as of Jan. 16, 2025.

[1] EBITDA multiples less than 0 and greater than 50 labeled "not meaningful" (NMF). LTM = last 12 months. EBITDA = earnings before interest, taxes, depreciation and amortization.

USE OF THIS DOCUMENT:

This communication is provided by First Analysis for informational purposes only. This communication is not intended to provide investment recommendations or investment analysis on any specific industry or company. Neither the information nor any opinion expressed herein constitutes a solicitation by us of the purchase or sale of any securities. This is not a complete analysis of every material fact regarding any company or industry. The content of this communication is solely our judgment as of this date and is subject to change. The information has been obtained from sources we consider to be reliable, but we cannot guarantee its accuracy. Past performance and any projections herein should not be taken as indications or guarantees of future events or performance. All investing involves risks, including loss of principal. Transaction advisory services and securities offered through First Analysis Securities Corp. (FASC), a registered broker dealer with FINRA and member SIPC. FASC may act as financial advisor and/or underwriter for companies mentioned in this communication. Venture capital investment advisory services offered through First Analysis Capital Management LLC, a registered investment adviser with the SEC. FASC and First Analysis Capital Management LLC, are subsidiaries of First Analysis Corp. Venture capital funds associated with First Analysis Corp., other First Analysis affiliates, and their employees may have interests in companies mentioned in this communication. More information is available on request by calling (312) 258-1400 or by writing to: First Analysis, One South Wacker Drive, Suite 3900, Chicago, IL 60606.

First Analysis

First Analysis has a four-decade record of serving emerging growth companies, established industry leaders, and institutional investors in emerging high-growth tech-driven sectors, both through its venture capital investments and through First Analysis Securities Corp. (FASC), which provides investment banking and related services. FASC is a FINRA-registered broker-dealer and member SIPC. First Analysis's integrative research process underpins all its efforts, combining 1) dynamic investment research on thousands of companies with 2) thousands of relationships among executives, investors, and other key participants in our focus areas, yielding a deep, comprehensive understanding of each sector's near-term and long-term potential.

One South Wacker Drive, Suite 3900 · Chicago, IL 60606 · 312-258-1400 · www.firstanalysis.com