Senior Tech Editor John Harrington

Advanced AI: Sink Or Swim Time For Cybersecurity Vendors

Companies: AMZN, CRWD, CSCO, CYBR, DELL, FTNT, GOOG/GOOGL, IBM, MSFT, OKTA, PANW, ZS

March 30, 2023

"Heard, tracked, understood, witnessed, confirmed, and you should really think about paying attention to this stuff."

Research Question:

How are AI advancements and hype affecting the cybersecurity industry? What are data security vendors doing with AI/ML and cybersecurity automation, and can they protect their market from the major cloud operators with their investments in AI-driven security for their own platforms?

Key Findings

- Claims by cybersecurity vendors that artificial intelligence and machine learning (ML) are set to spark a new dawn and increase revenues for every player in the sector might push up valuations in the near term for some companies—but sources warn that AI and ML are going to disrupt the industry in "unsustainable" ways. What looks good today might be gone in a relatively short time.
- "The development of AI in cybersecurity puts the big clouds at the center of the industry more than ever," said the CEO of a managed-security monitoring company doing business in the United States. "The clouds increasingly pull vendors into their partnership orbits because there is no other way to play now. A stand-alone company has to have compatibility with the big clouds. The most advanced machine-learning development is done on those platforms. On the margins, you have a mind-blowing array of claims regarding AI coming from virtually every company in the sector. In the short term, it all seems as if everyone is going to benefit. Not true. There will be an AI hype dead-cat bounce that will lift some companies' valuations—but what you have to understand is automation will only increase an already brutally competitive landscape. Look for some upside now after the sector has taken a beating. But watch it, because for a lot of companies out there, it's going to be a short spring."
- Every company discussed in this report is immersed in machine automation through some form of AI. Topping the list are Microsoft Corp. (MSFT), Amazon.com Inc.'s (AMZN) Amazon Web Services, and Alphabet Inc.'s (GOOG/GOOGL) Google Cloud Platform—which has gobbled up Mandiant and turned it into a platform called Chronicle that is part of a sweeping Google effort to incorporate AI into its cloud security offerings. "The clouds have unlimited development funds to push AI automation in cyber [security]," said an executive at a West Coast security integrator. "Because they do, every company in the sector has to partner with them. That's exactly what is happening. All of them boast about their cloud interoperability, and I think [investors] will buy this as a positive near term. Over time, though, it's going to push sector consolidation. That wheel is already turning. It's not so much that somebody like Cisco [Systems Inc./CSCO] is competing with the cloud as much as it is that, over time, they will more and more be an extension of the cloud."
- "In this game, it pays to be big because you either set the agenda, or you have enough money that you can slot into the agenda," said the CEO of a security value-added-reseller (VAR)/integration firm in the Northeast. "Things we look out for include negative stories in the industry media regarding any of the security companies. Something that is circulating right now regarding Okta [Inc./OKTA] is an example of how the pressure on vendors to compete can lead to mistakes that can undo a ton of hard work."
- "It can get very confusing for customers because you have partnerships, alliances, and varying levels of cooperation among security companies; when actually they are, for the most part, competing against each other at the product level," said a senior sales executive at a UK security consulting firm. "Yet at the same time, they are behooved to maintain they are integrated at the operational level with their competition so as to not appear they are an outlier in the business. Of course, the new (exciting thing) getting all the publicity at the moment revolves around AI."
- That being the case—and it is—we asked the sources for this report how they would play the sector near to midterm and out over time. See below.

How Is AI Awareness And Hype Likely To Affect The Value of Cybersecurity Companies?

For this report, sources commented on the following companies and how they see AI automation and machine learning playing on individual names in the near, mid-, and—for some—long term.

AMZN (AWS): Positive near, mid- and long term. Comments that typified the consensus included "You never bet against their size, scope, cash, and ability to develop anything on the AI front," said the CEO of a security consulting company that provisions clients in AWS. Said a senior security solutions engineer with a cloud migration company: "Pretty much every company in the sector has been forced into the AWS Marketplace. It's unavoidable. You have to integrate with them."

CRWD: Positive near and midterm. "They are partnering with everyone they can to extend their reach," said the CEO of an East Coast security VAR/integrator who was typical of several comments that reflected positively on CrowdStrike Holdings Inc. (CRWD). "The fact they were pushing hard on machine learning ahead of most of the others gives them street cred because the entire Falcon platform is an AI play. I think companies like Dell [Technologies Inc./DELL] need them because Dell's security reputation sucks."

CSCO: Positive near and midterm. Sources said Cisco's sheer size and the approach it has taken through the Umbrella security platform and its compatibility with the three major clouds will likely boost the company's enterprise security business through the year. "They have the lead in installed-base hybrid networking. Nobody else is close," said a longtime executive source at a networking and security VAR doing business with the Fortune 1000. "The expansion of their machine learning in setting up their cloud access security broker stack is not going to be a hard sell for their biggest customers." Other sources cautioned, however, that over a period of years, the cloud will continue to winnow away at Cisco's installed enterprise networking base.

CYBR: Positive near term, mixed midterm. "AI hype is helping them," said an IT networking source in the Northeast. Other sources agreed, with several saying a push by CyberArk Software Ltd. (CYBR) to create alliances, even with competitors, "looks good to customers," as one source put it.

FTNT: Positive near and midterm. All the sources commenting on Fortinet Inc. (FTNT) said they strongly believe that the focus on AI and ML will boost Fortinet for the foreseeable future, as the company has the technology and pricing that appeals to the midmarket customer base that is operating on a dispersed hybrid working model now more than ever. "It is a perfect design for what they have been doing for a long time," said the CEO of a security integration firm doing business in the Northeast and mid-Atlantic. Said another security integration executive: "Automated security operations is their mantra. AI hype plays directly into their message."

GOOG/GOOGL: Positive near, mid- and long term. All sources pointed to Google's leading position in AI over the past several years and how the company is incorporating its expertise in native security applications for its cloud platform as well as building an ecosystem with other outside security and networking companies.

IBM: Positive near term, mixed midterm. Sources pointed to International Business Machines Corp.'s (IBM) long-running Watson AI efforts on many fronts getting some traction around cybersecurity where large-scale machine learning can catalog massive amounts of data to help manage thousands of cyber threats. "All the AI publicity plays in their favor for now," said a UK source, "especially in the financial sector, where people are quite skittish at the moment. Any sort of cyber threats against large institutions cannot be allowed to succeed. In that vein, we are seeing a money-is-not-an-object-to-protect-us mentality. This is a global phenomenon."

MSFT: Positive near, mid- and long term. Every source said that they see Microsoft's taking the lead in the development of AI and ML and that the company is constantly applying its capabilities to security within its cloud platforms and across areas that extend outside, such as endpoint protection and comprehensive identity management.

OKTA: Negative near, mid- and long term. Every source said they believe that Okta has missed the market in access management and digital identification in the face of competition, especially from the major clouds and myriad other security companies that offer access and ID management as part of their own platforms.

PANW: Positive near and midterm. Sources have a complex view of Palo Alto Networks Inc. (PANW). While all the commenting sources said the hype around AI automation will be good for the company, especially near term, several also said Palo Alto is more about marketing than it is real innovation. "Look at Cortex—it is a lot for a customer to ingest," said the CEO of a Midwestern security-focused network and cloud integration company. "It's complex and expensive. I think AI hype is something they [Palo Alto] have been pushing themselves for some time. In that regard, all the AI hysteria at the moment seems made to

order for them, and I am sure investors are buying it. There is an equation here that I do not think analysts are appreciating or recognizing: The more automation you pack into what you are offering, the cheaper things must become over time in order to remain competitive. In that case, the most AI-automated security platforms should become the most secure *and* cheapest to run over the long term. In other words: Cash in now on the hype cycle and be careful, because if you really are building cybersecurity robots, your software sales base must naturally dwindle over time as the clouds themselves automate you out of business. Something like that."

ZS: Negative near, mid- and long term. Sources remain negative on the prospects for Zscaler Inc. (ZS), as they have over the past three years. In the past 12 months, the company has lost 57% of its market cap as competition in so-called "zero trust" models of intelligent/secure wide area network access continues to expand with customers using the cloud, especially Microsoft's platforms. Zscaler recently struck up a partnership with CrowdStrike that sources see as more beneficial for CrowdStrike. No sources saw AI development as having any beneficial effect on Zscaler. "I can see Zscaler's customers adopting Falcon [CrowdStrike's comprehensive security platform], but I don't see CrowdStrike's base migrating over to Zscaler," said a senior sales engineer executive at a West Coast network integration and security firm. "[Zscaler] doesn't fit where we are anymore when you stack it up against a native cloud pathway, like Google's private VPNs. It's an old approach in new times. There are still problems we see with it accessing cloud applications. It's not suitable for where we are going, and I do not see how it will last through the current automation push we are seeing unleashed on the world."

AI claims by cybersecurity vendors are having near-term positive effects with customers. However, sources agreed almost unanimously—12 of 14—that increased spending on AI-augmented cybersecurity will not be a long-term trend. It will likely flatten out by the end of 2023, they agreed. Instead, sources said they believe that automation of threat detection, identity management, access controls, and bulk data protection via automatic encryption of data at rest will create a type of inadvertent standardization in IT security. "It is already becoming expected," one source said. "Your problem will be if you claim you have it, but you really do not on a broad footing, flashy AI claims will backfire." Sources said more emphasis will be placed on proven central solutions provided as built-in features inside the major clouds, as opposed to adding more complex layers of defense sold by hundreds of competing companies.

"There is a current buzz around the idea that machine training can keep up with the bad guys," said the CEO of a security monitoring and management company based in the Midwest but doing business nationally in healthcare, manufacturing, and state and local government. "What you have to understand is that the bad guys are taking the same approach to automation. The use of bots to attack weaknesses has been around for a long time. It will continue to get more sophisticated as the defenses get more sophisticated. Bad actors have dramatically reduced the lag time between when an exploit [code vulnerability or other weakness] is detected and when they actually launch a successful attack based on a newly discovered vulnerability. So, a trained good machine is already pitted against a trained bad machine. That means successful attacks will continue to increase in the scatter-gun competitive world of the security companies. The only way to beat that is to centralize on serious AI engines with very strict policy rules and internal controls that define access permissions; user behaviors; and, above all, grades and encrypts data in real time. Microsoft, Google, and AWS have the resources and scale to do that. Everyone else, over time, falls down the line behind them."

Background

John Harrington has been the senior technology researcher for Blueshift Research since February 2014. He has an extensive background in reporting on technology trends for more than 20 years across all areas of information technology. He has a deep understand of and experience in cybersecurity processes and implementation dating back more than 20 years. For this report, John interviewed 12 key executive sources in the U.S. and two in the UK, all repeats from previous Tech Trends reports. Interviews were conducted in the last two weeks of February and the first three weeks of March.

About the Author

John Harrington is an award-winning investigative reporter and veteran Wall Street researcher. John previously served as senior editor and senior researcher at OTR Global and was a three-time Emmy Award-winning TV journalist.

John brings expertise and relationships in internet networking, network security, fiber-optic communications, and data center computing to Blueshift Research. He will contribute regularly, sharing deep insight into tech and communications trends, often before they are recognized by Wall Street.

Report Coverage Areas and Companies

Blueshift Research has been reporting on the following technology areas since Feb. 14, 2014, covering these public companies:

- Cloud Computing/On-Demand Hosted IT (AMZN, CRM, GOOG/GOOGL, IBM, MSFT, ORCL, WDAY)
- Enterprise IT Networking (ANET, CSCO, CTXS, DELL, FFIV, HPE, IBM, JNPR, MSFT, ORCL, RHT)
- Data Security (CHKP, FEYE, FTNT, INTC, JNPR, MSFT, PANW, SYMC)
- Data Storage/Management/Analysis (AMZN, BRCD, CSCO, GOOG/GOOGL, HPE, IBM, INTC, MSFT, NTAP, ORCL, PSTG, RHT, TDC, WDC)
- Data Centers and Fiber Optic Networking (AMZN, CONE, DFT, DLR, EQIX, GOOG/GOOGL, IBM, INTC, MSFT, NVDA, QTS, ZAYO)
- Fiber Network Construction and Implementation (ALU, CIEN, CSCO, DY, GLW, IESC, JNPR, NOK)

To access these reports, please contact your Blueshift Research sales representative or John Harrington.
