Blueshift RESEARCH TECH TRENDS YOU NEED TO KNOW

John Harrington
jfh@blueshiftideas.com

# Hackers Training Security AI to Think They Are Good Guys

Companies: AMZN, CHKP, CRWD, CSCO, FTNT, GOOG/GOOGL, MSFT, PANW, PFPT, ZS

June 5, 2020

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

**Research Question:**

**With spending on IT security products at an all-time high, why are the numbers of successful hacks increasing at such an alarming rate?**

## Key Findings

**Organized hacking groups of criminal gangs and state-sponsored actors are dissecting the software of firewalls and other IT security products that are utilizing software-based AI/machine learning so they can "teach" machines they are legitimate traffic—when they are anything but. This spoofing of what a long-time security source calls "the endless avalanche of bad software in the IT security market" has created a new frontier for hackers who are "feasting" on so-called AI/machine learning IT security products sold by a dizzying array of companies. Sources said IT security firms selling products and subscriptions to customers will have to engage in a relentless real-time fight against the subversion of their automated platforms or they will lose, taking customers down with them. The more customers spend on security, the worse the problem is getting, as endless software updates and new releases by security companies are actually what a source called "fresh food for the sharks."**

- Cloud-based solutions are not foolproof unless humans are constantly monitoring what is happening with data traffic. The reliance on machine learning to ferret out malefactors is being deemed a step toward data security failure precisely because hackers are "hell bent," as one key source put it, "to play with the minds of the machines in order to create a false sense of security" among end users protecting data.
- Another source said U.S., UK, and European governments are "well aware" of the activity and that all security companies have been put on notice that the battle has deeply intensified since the outbreak of COVID-19 and the subsequent global lockdowns that have sent workers into remote communications mode.
- Amazon.com Inc. (AMZN) Web Services (AWS), Microsoft Corp. (MSFT) Azure, and Alphabet Inc.'s (GOOG/GOOGL) Google Cloud Platform host a myriad of their own security tools backed by large workforces fending off attempted attacks around the clock. However, there is a human resources gap of qualified people in even the most ardent of human security monitoring by large organizations that leaves their in-house and endpoint security often open to breach. While the big clouds may be able to maintain their levels of dedicated security personnel, the clouds are also hosting third-party software for virtual firewall and security companies. Cloud sources report those companies—like Zscaler Inc. (ZS), Proofpoint Inc. (PFPT), Crowdstrike Holdings Inc. (CRWD), and others—have to interact with what has become a chronically understaffed customer universe during the pandemic. This worsening comes on top of what has already been a very hit and miss IT security industry when it comes to successfully battling the relentless attacks.
- Sources called the current level and frequency of attempted breaches the worst they have ever seen. As hackers spend more time cracking machine learning software, leading security firms Cisco Systems Inc. (CSCO), Check Point Software Technologies Ltd. (CHKP), Fortinet Inc. (FTNT), and Palo Alto Networks Inc. (PANW) find themselves in a position where their customers lack qualified people to monitor the systems they are running, with scores leaving it to the "artificial intelligence" vendors claim they are deploying to stop attacks. Sources are calling this an expanding information security "crisis."
- Sources said Fortinet's early experience in integrated cloud-assisted "fabric" defense has helped the company bolster customer defenses. The actively human-monitored Crowdstrike detection system received high marks as a key tool that has to be backed by other layers of security. Cisco is seen as being so rooted in the on-premise networking world that there is a hole in the company's program in how its systems are monitored. Check Point and Palo Alto Networks have been heavily criticized for contributing to marketplace complexity and confusion. Cloud firms Zscaler and Proofpoint were also cited for claiming they have intelligent systems that customers think can catch all threats when, in fact, claims of AI and machine learning capabilities are the precise targets hackers are now going after.

**Positive: AMZN, CRWD, FTNT, GOOG/GOOGL, MSFT**
**Negative: CHKP, CSCO, PANW, PFPT, ZS**

## Additional Information

Artificial machine intelligence has to be built up incrementally over time—just as humans learn on a timeline. AI is 100% dependent on your sample size—data inputs—and a key AI development source reports that "nobody is talking about this." Individual security vendors are limited in their baselines of data to build AI because they have just thousands of endpoints feeding data into their AI models at any given time. In stark contrast, the big clouds have billions of inputs coming in from all over the world constantly moving data into their collective AI learning efforts. The clouds also have millions of code developers worldwide working on internal data security defenses for those companies around the clock. The outside security vendors do not. Standalone vendors are, therefore, "extremely vulnerable" to having hackers "grab an endpoint device" and figure out what kind of data flows into a targeted network so they can fool the AI interface into seeing them as belonging. If any of the companies outside of Microsoft, Amazon, and Google are trying to sell AI as a magic bullet, a source said, it is destined to blow up on them in a major way because their data inputs are too scrawny to create a truly intelligent security platform. Therefore, the successful hacking grows right along with the amount of money being spent to combat it.

Sources that run constant security as a service for customers using layered tools report the "go-to" firewall company now is Fortinet. Crowdstrike provides real-time threat and virus detection that pairs perfectly with Fortinet's FortiGate fabric defense platform to create a basis for other tools to be added in around access identity and packet inspection at the layer two switch level. However, they emphasized, these security as a service bundles must be staffed by humans deeply trained at a near-military level to sort out anomalies in real time to thwart attacks coming at their customer networks from virtually every time zone on Earth around the clock.

The human/artificial interface is where the current breakdown is amplified by the pandemic. Sources were in total agreement that the number and types of attacks are far greater right now than they have ever previously experienced. And it is going to get worse as businesses are forced to lay off thousands of people around the world—including experienced IT security professionals. One source called the gulf between humans and AI in data security "the Grand Canyon of opportunity" for organized hackers and rogue opportunists to exploit faults in all the new security software flooding onto the market.

### The Upside

Global clouds: The three at Microsoft, AWS, and Google have billions to spend on development of real-time counter defenses against attackers without turning unprofitable. This nearly unlimited well of cash flow funds developer communities like Microsoft's GitHub, where hungry developers all over the world scramble to create software they can sell to the cloud operators. The cautionary tale here, though, is that developers unable to cash in from legitimate code work can turn to the hacker side of the fence and try to game the AI expansion to set up hard-to-detect holes in those artificial defenses. The big clouds are more prepared to deal with that—but outside vendors that are going it on their own are under tremendous stress.

Crowdstrike and Fortinet: In the case of Fortinet, the company has more experience and is priced right—well below Palo Alto Networks and Check Point—to grow in the current battlefield, not the least because it operates in the cloud world, in the on-premise networks, and out to all the individual devices that access data networks. Sources said the Fortinet platform meshes very well with certain other vendors, particularly relative newcomer Crowdstrike. Both these companies remain on the correct side of the Tech Trends trend line.

### The Downside

Check Point and Palo Alto Networks: Both keep buying up outside firms and trying to cobble them into cloud-based service platforms like Palo Alto's Prisma. Sources are sour on the two companies as being behind the curve, overpriced, and too complex for a cash-crunched customer base they now expect to adopt whatever the companies tell them to adopt. The constant dangling of AI as a big advantage by the companies is predicted to backfire as sophisticated attackers penetrate the AI learning curve to get through the defenses as if they always belonged there.

Cisco Systems: The shift to remote working has shown big network operators that they can keep going by using the cloud. Cisco's security sales are ultimately tied to the company's networking hardware and software and, as things continue to tighten up for on-premise network operators, a human resources pinch is already underway. Sources say Cisco is caught in a type of no man's land between the cloud and the old days of local area networking based in corporate data centers. They predict Cisco will have to eventually cut loose a large part of the company's product portfolio and thousands of workers.

Zscaler: Sources continue to be adamant that there are many underlying problems with Zscaler's offering on the execution and monitoring side. They stand by their comments from last August's Tech Trends report when they sent out a warning about issues

at the company. Sources say the platform is still prone to network errors and other problems.

Proofpoint: As the big clouds continue to bolster their own defenses, sources believe that early-innings cloud security filter firm Proofpoint could dwindle as exact services offered by the company are baked into platforms like Microsoft Azure.

## Background

For this report, Blueshift Research Tech Trends Senior Technology Researcher John Harrington interviewed seven long-time Blueshift Tech Trends executive sources in IT security systems integration and software development that have added to our security coverage since early 2014. Three are based in the EU and UK, with the other four operating across the United States, with one involved in major cloud network implementation for Fortune 500 companies. Interviews were conducted throughout May and into the first week of June.

## Key Quotes

- "You can buy the biggest, shiniest fire engines. If you don't have the right people to get it out of the station and operate it, the town will burn down. This is the entire problem with how this AI myth is being spread—the machine can't drive itself and fight the fires that are constantly igniting with all the attacks coming in from every direction. Critically, if you have likely millions of code developers and computer operating system guys out there organizing into hacker collectives, criminal gangs, and working for state funded efforts, they are going to work to exploit all of the machine learning that is being pushed by the various security vendors on their customers. If the machine is spoofed into thinking you are walking like a duck, quacking like a duck—the machine is going to think you are a duck. If ducks are supposed to be inside your data network, then everything looks great until sometime down the road, if ever, you find out some of the ducks are actually T-Rex." — CEO of a security platform as a service company doing business in big health care, manufacturing, higher education, and professional sports

- "Right now, hacking is at an all-time high. With the COVID situation, you have millions of people passing around data to and from their houses and they are the perfect welcome sign to be used as a conduit into all kinds of network systems for an unfathomable number of bad actors. In all the years I've been at this, things are by far the worst I have ever seen them in terms of the level of malicious activity we are detecting. The hacking is indiscriminate in that they are going after whatever they can find that is open or poorly protected. They are going after VoIP phone systems. They are after open endpoints. You have to lock everything down and have people monitoring the situation—not some artificially unintelligent machine. The entire AI marketing blitz is being exposed as [nonsense]. You deploy the tools, layer them, monitor them, and, still, things can get through. You will see a record number of successful breaches like the Easy Jet situation being revealed in the coming months. Change passwords frequently." — CEO of a large business network service provider doing business in the UK and EU

> In all the years I've been at this, things are by far the worst I have ever seen them in terms of the level of malicious activity we are detecting. The hacking is indiscriminate... You have to lock everything down and have people monitoring the situation—not some artificially unintelligent machine. The entire AI marketing blitz is being exposed as [nonsense].
>
> *CEO of a large business network service provider doing business in the UK and EU*

- "Here is the dark side of this machine learning: the machine learns what is put into it. Machine learning can be helpful for good but, inversely, it has as much capability for hackers to use legitimate customer accounts to teach the machine that their illicit traffic is just like all the good traffic. That is happening now and I will be damned if you are going to hear that from any of these firms selling machine learning as the end all of hacking. Quite the contrary—it is not, but don't expect any security firm to tell you that in a sales presentation. The way it works is they collect the sale and, when things go off, they blame firms like ours when their products were as easy to breach as the Maginot Line." — CEO of UK-based IT security integration company

## 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. John 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.**

---