Senior Tech Editor John Harrington

Fighting Cybercrime 2023? Sector Says 'Buy More Security Stuff'

Companies: AMZN, CRWD, CSCO, CYBR, FTNT, GOOG/GOOGL, MSFT, OKTA, PANW, RPD, S, ZS

December 14, 2022

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

Research Question:

How have evolving threats and successful hacking attacks reshaped the data security industry across 2022, and will there be new breakthroughs in 2023 that can slow the rate of cybercrime?

Key Findings

- Spending on cybersecurity continues to rise, but sources warn that many companies are not going to be part of any windfall.
- Sources agree that Microsoft Corp. (MSFT) is pulling away from other vendors in the depth and breadth of its unified cybersecurity platforms. It is, they say, a matter of the sheer financial power and human capability of the company to innovate and integrate that poses the largest threat to other companies' businesses across the sector. "If you properly leverage what they are doing, you can get rid of a lot of what you have been paying for and get a much more secure data environment," said the CEO of a security consulting and integration firm with several Fortune 1000 clients. "Check out what they introduced at their big Ignite event."
- Several sources referred to a "same as usual" approach among the hundreds of companies selling cybersecurity products as a continuing failure to stem cybercrime. "By encouraging customers to keep spending more on the category, it is the most glaringly self-serving [nonsense] imaginable," said the CIO of a UK-based data security integration and services company. "Spending more to obtain less satisfactory outcomes across the digital landscape is hardly a prescription for success. Yet this is where we remain, and I am afraid it will not change next year so long as the key objective is for the various entities doing business in cyber defense to accrue revenue. … Generally, spending on the category continues to go up, and losses due to cybercrime continue to exceed the spending on the category. That is a damning statistic."
- Generally, sources forecast that cloud-delivered security is now the only way to cover customers. "Your readers have to understand that cloud-mounted security is delivered from a hosted platform, most likely at AWS [Amazon.com Inc./AMZN], Microsoft or Google [Alphabet Inc./GOOG/GOOGL], even if the vendors they [customers] use are outside parties like a Palo Alto Networks [Inc./PANW]," said the CEO of a managed-security company dealing with healthcare clients. "Dollars spent by customers are split in rapidly changing ways. Much more of the smart spend isn't on products, it is on services delivered from people like us who manage security for our clients using various vendor products as tools. I think this is where the cloud-native security filters gain a big advantage. We can say, 'OK, you have your clinic's workloads at Microsoft, and we are going to secure them for you, as well as your devices on the edge.' How we do that is not the concern it used to be when they were doing this themselves at their locations. The customer doesn't want to deal with data security anymore. We take it on as a service, and we decide how to deliver it. This is where we can manage data security—including records, compliance, and identity management—at the core in the cloud and at the edge endpoints. And we can use Microsoft for everything, or almost everything. … The same holds true for AWS or Google Cloud. This is what I'd be most worried about if I happened to be one of the many outside [security] vendors—feature overlap will hurt them, not the cloud guys."
- The in-house network still belongs to Cisco Systems Inc. (CSCO), sources said, and Cisco is out to supply security from a cloud platform across its customers' environments. "Their Umbrella push is Cisco's fightback against what Microsoft is doing," said a senior security engineer at a value-added reseller/integration firm. "The fact that Cisco is fully invested in this approach tells you where things are, because they have been the kings of on-premises networking. Now they are pushing security as a service that they will supply, not the customer deploying Cisco's software themselves."
- Sources said companies such as Sentinel One Inc. (S), Rapid7 Inc. (RPD), CyberArk Software Ltd. (CYBR), Okta Inc. (OKTA), and Zscaler Inc. (ZS) that have most if not all of what they do duplicated by the cloud companies face dwindling prospects. Crowdstrike Holdings Inc. (CRWD), Palo Alto Networks, and Fortinet Inc. (FTNT) will "hang in there" in 2023 but are unlikely to grow revenue unless they keep acquiring other companies.

Positive: AMZN (AWS), CSCO (security division), GOOG/GOOGL (cloud platform security), MSFT
Neutral: CRWD, FTNT, PANW
Negative: CYBR, OKTA, RPD, S, ZS

If You Can Avoid Being Hacked While Spending Less To Do It, You Will

"It is a matter of scaling your [cybersecurity] needs properly if you want to get better results for less," said the CEO of a UK IT services company. "The continuing debate revolves around how many trained cyber professionals should you employ, and where do you find them. Because, the argument goes, you need such people to operate the defenses you deploy from whichever firms that provide said defenses. In other words, if you follow that line of argument, you will hire more people to interact with a variety of many applications dealing with access management, permissions for various degrees of data access, and the operation of all things security-related. Therefore, if it is your intention to actually gain control of all of this and properly scale your needs to match the results you are seeking, our recommendation is to seek outside help. Otherwise, you are stuck with competing interests around job security amongst your staff and vendor billings pertaining to salespeople calling on your business—both seeking to color your judgment. You must abandon doing things that way if you are to break the cycle. This is not easy to do. However, it is where things are moving because most end customers—at least those executives footing the bills—do not want to deal with cyber defense any longer. They want a qualified organization to take it over for them. That being the case, use of the cloud becomes the launch point, and you work out from there. We manage it; the cloud delivers the capabilities."

Sources said it will be a matter of less than five years before losses resulting from cybercrime will have become so intolerable that some type of standards regarding data encryption and the artificially intelligent management of data and access to it will be mandated by stringent laws passed in places like the European Union and United States. "We have discussed it before—the insurance industry is not going to accept these kinds of losses anymore," said a senior executive at an East Coast security integrator. "That said, if there is no insurance to cover liability and loss, then any organization that fails to protect personal data, for example, will not be able to settle lawsuits or pay for things like loss of business continuity. I think it is pretty clear that will force a consolidation of the [cybersecurity] industry into a much more centralized configuration. Obviously, since we are now fully into cloud-delivered cyber defense by all the vendors already, we are going to see companies like Microsoft, Amazon, and Google forced into taking over many of the things that are currently sold by all these different vendors. I mean, who isn't claiming they have some form of IT security in their software product suites? It is simply too much. Standardizing a hardened approach to locking down data is only possible if it is built centrally, meaning on a cloud structure, and then it is managed by essentially specialists using AI and working inside that central design to deliver security uniformly from the core to the micro edge. By the micro edge, I mean embedded in IoT devices, in chips themselves, all the way through to application delivery at the server level, across databases, data warehousing, storage, and application development. Eliminate bad code before it goes into play. Cut off the vectors bad actors thrive on. Lock down endpoints so that users are forced into protocols of application and web use so that they aren't the targets they currently are. When that happens—and believe me, it will—most of these companies that are in this business will be gone. There is so much duplication, and much of it is last-generation thinking."

Sources said investors have an opportunity to, as one put it, "stop throwing money at these bad startups in the hope one of them will become a big growth opportunity." All the sources agreed that the day of taking a firewall company—as was the case with something like Palo Alto Networks—and turning it into a $50 billion company are essentially over. "Data security has to be run as an impregnable, standardized utility before things get any better," said the CEO of a data management company specializing in cloud migrations. "If people really understood how vulnerable the data we see all the time actually is—I mean their personal data—I'm not sure they'd be able to sleep at night. There is so much rampant negligence and general not caring by the organizations handling it—and I mean the people working for those organizations who do not have a vested interest in protecting any of it—that the loss of data will continue unchecked until it becomes a global security crisis. I already believe it is, and it continues to get worse.

"Investment has to be in creating a uniform system of data protection, from its creation to its end of life. Of course, this runs up against the entire [cybersecurity] industry, which is built on this idea that the marketplace should dictate how we deal with data protection. How is that working out? I think this is the grim realization that Microsoft has come to. The only thing that is a true threat to the cloud IT model is bad data security. That has forced them [the clouds] into taking matters into their own hands as far as development of next-generation data protection. Having a thousand or so companies all claiming they have the solution to data theft and other forms of cybercrime is absurd on its face. You have to carefully look at these companies, and you will see how much duplication of effort there is. They may claim they are all working toward a common good, but that is an outright lie, because they are in competition among themselves. They actually have an association that hands out achievement awards for excellence in cybersecurity. Seriously, look it up. They are handing out awards when there are more than a trillion dollars a year in losses and damages due to cybercrime—possibly a lot more. Think about that. They'd have an award for the 'Best Pilot On The Hindenburg' if they could, I'm sure."

Sources said the best rule of thumb for understanding the entire sector in 2023 is to look to see which functions the cloud is taking over from the independent cybersecurity companies. As one longtime source said: "You watch the smaller players fade out, and moving up the stack, you understand that something has to give. You can't keep having this increase in security spending if the losses keep getting bigger."

Background

Senior Technology Researcher John Harrington has been reporting on the data security industry for Blueshift Research since February 2014. Before that, he worked as the senior technology editor for another Wall Street-focused firm starting in 2001. John has also worked in the security, data center, and networking industries since 1995. For this report, he interviewed nine U.S.-based executive sources in cybersecurity, all repeats from previous Tech Trends reports, and three UK- and E.U.-based sources, also repeats from previous reports. Interviews were conducted in the last two weeks of November and first two weeks of December.

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.
