Blueshift RESEARCH TECH TRENDS YOU NEED TO KNOW

Senior Tech Editor John Harrington

Cloud-Fueled Spending Chaos Hits Security And Everything Else

Companies: ACN, AMZN, CHKP, CRWD, CSCO, FTNT, GOOG/GOOGL, IBM, MSFT, OKTA, PANW, S, ZS

Nov. 20, 2023

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

Research Question:

What is in store for the data security sector as cloud computing, especially Microsoft, continues to capture more of the security spend?

Key Findings

- Weaker than expected quarterly reports by security vendors Fortinet Inc. (FTNT) and Palo Alto Networks Inc. (PANW) are not a fluke, sources say, but a continuation of a shift in information technology spending that Blueshift Tech Trends has been extensively reporting on since early in 2023.
- Cisco Systems Inc. (CSCO) claimed that its recent report is not a reflection of deteriorating macroeconomic trends that caused the company to miss key results. Sources agree. Instead, they uniformly report that the problems striking spending across IT, including the usually robust data security segment, have their root in something "that is a lot worse for vendors than any cyclical economic issues," said one long-time source. "The cold, hard truth is that the cloud, especially Microsoft [Corp./MSFT], is taking increasing customer spend away from the outside vendors faster than they can make it up. That will only get worse moving into next year. It is totally changing the security spending landscape as well as the whole network equipment segment. Microsoft is probably going to wind up with as much as 30 to 40% of the overall global security spend by as early as the end of 2024."
- While estimates vary and are often not credited to the correct segments of IT, about $71 billion was spent on data-related security in 2022. Tech Trends' top security sources, who have been accurately reporting on spending trends since 2014, all agree that by the end of 2024, Microsoft's security-related revenue could top $30 billion, especially with its focus on the insertion of AI into platform applications like Copilot, which is being injected into every area of the company's cloud.
- "Next year is going to bring some mad consolidation," said the CEO of an East Coast IT security implementation and management company. "There is no way we will continue to see so many companies offering the same types of products and services across the data security landscape when Microsoft offers identical, often better, solutions at lower aggregate prices. As the whole [security] sector becomes a software-services play, Microsoft has such a tremendous advantage, it will be impossible for many of the other vendors to hold onto just what they have. The lucky ones will sell to Cisco or someone else that has the finances. Then we will never hear from them again."
- Sources agree that the way to look at the sector now is to match everything Microsoft currently offers, or what it is working on in security-related AI, against everything all other security vendors have that is the same or similar, and then "bet like hell on Microsoft," as one CEO of a cloud security management company said.
- Top names that repeatedly came up as being heavily exposed to what some sources are calling "cloud spending chaos" that will extend across 2024 are Zscaler Inc. (ZS), Okta Inc. (OKTA), Check Point Software Technologies Ltd. (CHKP), Fortinet, Palo Alto Networks, and SentinelOne Inc. (S). Sources were mixed on CrowdStrike Holdings Inc. (CRWD). "The way we look at it, it's Microsoft against the rest of the field," said the CEO of a security management and monitoring firm with major clients in healthcare and manufacturing. "All our clients have at least some resources over there [at Azure and 365], and every week they [Microsoft] keep adding to the security stack. With so much of it embedded for Copilot now, by the time you have the right number of seat licenses in place with the enhanced client pricing, and you determine actual costs vs. what you are running in-house, it is a no-brainer to make the shift, particularly if you preplan migrations to manage costs. What they [Microsoft] are doing is destructive to the way the security industry has been operating for 25 years."
- Said the CEO of an East Coast value-added reseller (VAR)/integration company: "You aren't going to hear [Cisco CEO Chuck] Robbins ever admit what the cloud is doing to them. But you are seeing it in real time, and it is bad news for them."

Positive: AMZN, GOOG/GOOGL, IBM, MSFT
Mixed: CRWD
Negative: ACN, CHKP, CSCO, FTNT, OKTA, PANW, S, ZS

If IT Security Spending Remains Flat Across 2024, Microsoft's Share Gains Will Smash Rivals

Spending in the data security sector could even rise above 2023 levels, sources said. But it will not rise enough to allow many companies in the sector to increase or even hang onto previous revenue levels.

"When a company like Fortinet says the demand for firewalls is dropping, what they actually mean is the demand for what they sell is dropping," said the CEO of a VAR/integration company that resells Fortinet. "Firewalls are still important. It's just that the way a firewall is deployed is drastically changing, and last-gen companies that have dominated the market—like Cisco, Palo Alto, Fortinet, Check Point, and a few others—are staring at a shift they can't stop. The virtual firewall inside Azure is a prime example. There isn't a damn thing Microsoft's competitors can do about how Microsoft protects clients within Azure. The more resources a customer has in Azure, the worse it is for these vendors. Because believe me, over the next few years, the product spend in security is going to drop because of the cloud. It is already happening, and it is accelerating. When you couple that with a softer overall IT spending climate, the math becomes simple.

"If one entity, in this case Microsoft, continues to gain revenue in the sector, those gains are coming against the revenue of everyone else. I don't even know what the counterargument to that is. There isn't a logical counterargument because the overall spend is not going to keep going up. These projections that suggest that are specious at best. The efficiency that an AI security stack can bring to customers at Azure or in 365, SharePoint—everything Microsoft has—is going to divert revenue away from other vendors on an accelerating basis. This is going to include the federal government. So these companies that are lined up trying to get as much of that as possible are still competing against Microsoft, [Alphabet Inc.'s] Google [GOOG/GOOGL], and [Amazon.com Inc./AMZN] AWS [Amazon Web Services] for the federal bucks. What will we see? Many more acquisitions by bigger companies—Cisco, Palo, Microsoft, Google, Amazon, IBM [International Business Machines Corp./IBM]—because they have the money. I think Cisco and Palo face mounting challenges. IBM has a big enough base, and they are deeper into AI security development than many others. Because of the size of their clients, they can sell into a captive audience. Smaller vendors will likely sell out cheap or just go away. It's not a zero-sum game. It is a lot more like a slow strangulation as we see realignment.

"The only certainty is that Microsoft will be the dominant security company out there. They already are.

"We have done CBAs [cost-benefit analyses] for several clients on like-for-like services in Azure and outside vendors, particularly Zscaler. It is interesting because Zscaler has a partnership with Azure for zero trust access into the Azure cloud, but the two compete on the cloud firewall front. This is where it gets interesting. Because the minute you find yourself using Zscaler in conjunction with Microsoft's cloud, over a period of time, there can only be one way this is going to work out. Microsoft will eventually take over Zscaler's customers because the two can operate without the other, or in tandem. The difference here being that Microsoft owns the cloud infrastructure, and Zscaler is charging its customers to use them to securely access Azure. All well and good. However, can you do the same thing by just working with Microsoft? The answer is yes. There are different ways to attack the issue. So, using Azure Virtual Desktop, you can work off existing licenses you already have. That is a big plus. In addition, there are so many new features being constantly introduced into the Azure platform, the main issue revolves around telling customers what if any outside vendors they need to manage or access their Microsoft resources. This is the killer question. Because the answer is—none, if you know what you are doing. That's our business. We know what we are doing, and we save our client significant amounts of money.

"We are at the [Microsoft] Ignite conference in Seattle, and it is an understatement to say how far ahead of the game they are. We have been in discussions about Purview because we are in data management, as you know This is one of those things that has profound implications. This is going to take all the data protection vendors outside Microsoft and turn them into dead men walking. That is not an exaggeration. First of all, it tackles the Holy Grail of data, which is classification. In other words, what data is important, what is kind of important, and what is not worth saving or managing? This is the eternal struggle of amassing data. What do you have? What is in it? Where is it? That's a huge issue because nobody really knows what they have and exactly where whatever it is sits. Instead of dancing around the problem, they [Microsoft] are attacking it head-on. Purview is going to blow up the data retention and management area. Compliance alone is a multibillion-dollar segment. We look at Accenture [PLC/ACN], for example, and they have been involved in the business of business as usual. And honestly, with the spending slowdown that has been getting worse across enterprise and the changes like Purview coming on, the days of these kinds of mega-consulting, software-pushing houses like Accenture are slipping away. We see it, and so do other smaller, more agile

shops like ours that are into direct action recommendations and deployments for clients without the dragged-out engagements that have been the bread and butter for the Accentures of the world forever. They have to be looking at this landscape and realizing they are in trouble.

"The AI insertion into everything they [Microsoft] have going on with OpenAI is so far past anything anyone else is doing on the enterprise side. You can't overestimate what is going on. When you apply this to data security and access, since they are integrating security into everything—everything—it breaks the model the industry has been operating on. It totally trashes it. We are talking about a completely different way of approaching security.

"There are guys from various security companies walking around here with a glazed look on their faces. We had drinks with some people last night from one company, and one of their guys said, 'We're trying to see what areas we can collaborate' with Microsoft. A couple of years ago, they wouldn't be at something like this. They'd be working on how they were going to beat Microsoft. Now they are trying to figure out how to tie in. If they don't, they know they'll be on the outside looking in."

Background

John Harrington has been the senior technology researcher for Blueshift Research since February 2014. He has an extensive background in reporting on trends for more than 20 years across all areas of information technology. He also has an industry background in network security and data protection. For this report, John talked with 12 key repeat sources, 11 in the United States and one in the UK, to determine what will be affecting the IT security sector moving into 2024. Interviews were conducted from the beginning of November through Nov. 16.

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)

For more information or to access prior reports, please contact your Blueshift Research sales representative.
