Blueshift RESEARCH TECH TRENDS YOU NEED TO KNOW

John Harrington
jfh@blueshiftideas.com

CISO Exhaustion, Competition Hits Cyber Security Growth Targets

Companies: CRWD, CSCO, CHKP, DARK, FTNT, MIME, MSFT, OKTA, PANW, SPLK, ZS

October 27, 2021

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

Research Question:

Does the digital landscape change so fast that IT security vendors can't keep up? Do customers feel constantly set upon to buy more and more products and services?

Key Findings

The sheer number of cybersecurity businesses trying to make sales has overwhelmed IT security professionals, from the chief information security officer (CISO) on down through the ranks—to the point that sources report that end-customer security pros are actively hiding from vendors pushing them to buy more products and services.

"They delete their LinkedIn accounts," one source said, "because that's how all these established companies and startups get their contact info to cold-call them all the time. It's torture. That's what our [consulting] clients tell us. The focus isn't on network security. These startup companies are trying to sell themselves to acquisition guys like Palo Alto or Splunk so they can score a windfall. The big guys are trying to make sales quotas. It's a game that has nothing to do with data protection."

It is impossible to know how many cybersecurity companies are out there, but lists are floating around. This one has 1,750 active vendors in 2021. "That's insane, don't you think?" said a UK-based source. "Where do you imagine any customer is going to find budget to continually combat this madness? I think Gartner forecasts that there will be something like 150 billion pounds spent on cybersecurity in 2022. In the past four years, we estimate that cyber criminals extracted 5 trillion pounds or more from the global economy through financial theft, ransomware, data damage, identity theft and other forms of criminal activity linked to the use of digital networks. That is likely a conservative figure because so much of it is covered up and not reported. The odds seem tilted toward the criminals. Why is that? It is because the global cybersecurity landscape is based on firms making money in the sector—including us—as opposed to finding a method to harden the overall system? There must be rational consolidation."

The term "cloud security" has also become something of a joke among many security pros. "It means nothing anymore," one said. At a recent symposium conducted by an endpoint security vendor, even the company's own executives derided the overuse of the word "cloud," said one source who attended. "All the vendors are 'cloud' now," the source said. "What does that even mean? Does their service work? Then prove it."

In addition, the number of people it takes to engender a full commitment to well-run cybersecurity in customer organizations is larger than the number of people who are willing to put in the hours for the decreasing pay, said several longtime security consulting CEOs who are Blueshift Tech Tends sources. "You can't find enough people who give a damn for what companies are willing to pay. That's why our customers want to push the entire security sequence onto us. They really don't want to deal with it anymore."

Other sources blame what one called "the pure poison of Silicon Valley venture capital. That's created a field day for hackers." The sheer number of security startups that have been funded over the past five years exceeds 2,000, said two sources who closely track the cybersecurity sector. Those companies hope to get acquired or eventually go public as venture capitalists look for so-called "unicorns" they can exit with huge gains in their pockets. "Honestly, that's the culture," one source said. "The VC people don't give a [damn] if what they are funding actually works. It's push up the valuation and try to cash out."

The net result is that hackers have successfully stolen trillions of dollars over the past five years, and the situation will continue to get worse. Taken together, big growth numbers for public cybersecurity will decline in 2022 because the entire sector is a bloated, competitive mess.

Positive: CRWD, CSCO (Duo MFA product), DARK, FTNT, MSFT, OKTA
Negative: MIME, PANW, SPLK, ZS

Key Trend Points

- Companies that are likely to post respectable growth into 2022, but at a level lower than they have previously forecast, are Crowdstrike Holdings Inc. (CRWD), Darktrace PLC (DARK), Okta Inc. (OKTA), Fortinet Inc. (FTNT), and certain parts of Cisco Systems Inc.'s (CSCO) security portfolio simply because the company still has a very large installed enterprise network base.
- A slowdown will hurt companies that have been claiming they are going to grow significantly over the next few years. The cloud security company Zscaler (ZS) is reported to be falling prey to aggressive sales tactics by several competitors. Palo Alto Networks Inc.'s (PANW) Wildfire, Fortinet's Fortigate, Cisco's Umbrella and several others, including Check Point Software Technologies Ltd. (CHKP), have been taking aim at Zscaler, several sources said. Competitors have pointed to technical problems that Zscaler customers have reported as a reason to leave the platform. "It's down to everyone trying to steal everyone else's customers anyway," one source said. "That being the case, if you are claiming cloud superiority, as Palo Alto is, then you are targeting Zscaler because they were doing cloud filtering earlier. You target their customers by bad-mouthing them, something that Palo Alto is well-known to do with competitors." However, Palo Alto's Wildfire platform, which competes directly against Zscaler, is "ridiculously overpriced," as one source put it. The net effect, another source said, is that, "all of these guys are beating each other's brains in for sales, and customers are pulling back because they are the ones under seige."
- Even smaller companies that operate in areas such as email security are going to get, as one source put it, "lost in the ether [of too many companies] trying to sell the same things to everyone." One name that three sources said will likely be hurt by budget slowdowns is Mimecast Ltd. (MIME)—which is in a niche that is being swallowed up by Microsoft Corp. (MSFT), among others. "Mimecast is offering email security that you can get as part of broader security offerings," a source said. "You are seeing less and less of them in the places where we did see them popping up before. Small players like this are going to be cleared out by Microsoft because Microsoft must protect the assets it has running in its own cloud and in on-premise licensing for Outlook and other Office 365 software. That means little guys like Mimecast are on a limited timeline, I think." Other sources agreed that smaller players that have offerings that bigger players bundle into their security platforms are extremely vulnerable to losing share. "Next year is going to be very, very hard on a lot of these security companies that aren't willing or able to spend millions on aggressive marketing," said a source.
- "Buying business" was a focus of several sources' comments. Criticism of Palo Alto Networks and Splunk Inc. (SPLK) centered on those companies' supposed growth being based on serial acquisitions, as opposed to organic growth based on innovation from within. "Neither of them has anything notably better, or even as good, as the competition, but they cost more," one source said. "That's why they have been buying up other companies to make themselves look bigger and more diverse." In Palo Alto's case, it has been on a buying spree. Integrating all of that into a simplified, cohesive, affordable platform is proving to be difficult for the company. End customers have consistently cited Palo Alto as being among the most expensive, aggressive and "pushy" in trying to upsell additional products and services. "If you are a customer of theirs from any previous time, you are on the call list for sure," said one source. He went on to detail how a client of his from a large company took him to dinner to get the source's company to agree to field all the sales calls from security companies that have been calling the client. "I asked him: 'How bad can it be? How many calls do you get in a month?' He looked at me and said, 'More than 100.' And I said I'd have to hire someone at 80K a year just to answer the calls, and he said, 'Well, OK,' and he was serious. We took it on for a little bit less than that." Another said, "They [the cybersecurity companies] can't keep up with their own sales quotas. It's not feasible. Not in this climate with budgets contracting [note: see Blueshift's Oct. 15 Tech Trends report on budget slowdowns]. I think the companies that are honest about it, like Darktrace, are more about trying to emphasize performance of the platform instead of hyping themselves as world-beaters. That's how we became involved with them. It was all business, no hype."
- Splunk was also cited for buying up companies while not having what two sources said is a clear strategy why they are important for anything more than mundane logging analysis and compliance. Splunk is not a security company, despite the fact it is trying to claim it is. "Anyone messing with data can make some claim that they are a security-focused company," one source said. "Splunk's whole model was to rake in money off the volume of data being produced from things like firewalls. You got caught up paying exorbitant sums based on the sheer amount of traffic. It was very lucrative for a while, until customers found alternatives. And that forced Splunk to drop pricing, which was too late. That big data traffic logging analysis and tracking business began to fade, so, of course, they are now claiming they are a security firm." Competition was also cited as being robust and lower in price. Sources cited Dynatrace Inc. (DT), Datadog (DDOG), LogDNA Inc., and

Sumo Logic Inc. (SUMO) as better and cheaper logging analysis tools, while DataDog was cited as a better security platform. All the sources predicted that Splunk would increasingly become a background player as budgets continue to come under pressure. "There's not enough room for everyone," a source said.

- One area that will likely grow is multifactor authentication (MFA), with Microsoft, Okta and Cisco's Duo division cited as leaders in the field. Identity is the first key step in combating data theft because access permissions are the hackers' freeway on-ramp. "You have to force access protocols on employees who will not take the steps to protect even their own phones," one source said. Microsoft and Okta are not tied to specific enterprise network architectures. That gives them the cloud and on-premise flexibility that Duo may not enjoy because Duo's MFA maps back to existing Cisco customers in most cases, limiting what Duo might be able to do as an independent entity.
- Broad encryption of stored data and active application sessions is another key plank in basic security defense. "You encrypt it before some ransomware attacker does it for you," said one source. However, it's not that easy, said several other sources. "You have to have scale and uniformity," said another. "That's why Microsoft has such an edge, I think, going forward. They can put all the protocols inside their data centers and automate everything. MFA, encryption, containers—everything. That right there is bad news for everyone else trying to push their own 'we are cloud' stories. It will come down to Microsoft versus the field. It already is."
- The pressure on cybersecurity workers at end customers is at an all-time high and growing. This has been continually reported by Tech Trends since 2014. However, back then, hacking was not close to what it has become today—a multitrillion-dollar business. While varying statistics are being bandied about by any number of organizations documenting the cost of cybercrime, here's but one example. With those sorts of numbers out there, fewer individuals are willing to take on roles as chief information security officers in companies that place the entire responsibility for warding off data breaches on staff who are usually under-resourced in human terms, underpaid for the responsibility they shoulder and who have their time eaten up by the endless pressure to buy more security products constantly shoved at them by vendors.
- "If you were to ask me what the hardest job in the world is for what you are expected to do for the money you are paid, I'd say being a CISO at a company that handles critical databases loaded with personally identifiable information or that oversees a bunch of critical infrastructure would be right up there," said the CEO of a cybersecurity implementation firm doing business with Fortune 1,000 entities. "Another would be the insurance underwriter that sells cyber insurance to these unprepared and unprotected organizations that get hacked."

Additional Information

If budgets are tight—and they are, said sources across all our IT reporting—security spending will focus predominantly on trying to maintain systems in place into 2022, as opposed to adding more products and services, all 18 sources interviewed for this report agreed.

Areas deemed critical will continue to be funded as needed. These include endpoint security for the devices of remote and mobile workers, password security and access management, network internal and edge firewalls. and automated threat detection and updating.

The outsourcing of information security to companies that many Blueshift Tech Trends sources own will also grow as enterprises cut the number of in-house security workers they want to employ—or because they won't hire qualified people in their regions at salaries they are unwilling to pay.

As more work is based in the cloud, sources said, the pressure on information security companies to meet their own sales goals will continue to increase across 2022, because the cloud platforms are constantly chipping away at things that outside cybersecurity companies are also selling.

Background

Chief Technology Researcher John Harrington has been covering information technology for Blueshift Research since February of 2014. He has a deep background in information security and has developed sources around the world who work at the leading edge of the sector for clients across the business and organizational spectrum. For this report, he interviewed 18 repeat executive sources from previous Tech Trends IT security projects. Sixteen of the sources are based in the USA and two in the UK and doing business in both the UK and European Union. Interviews were conducted throughout October.

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, BABA, 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.
