John Harrington
jfh@blueshiftideas.com

Privacy Will Be The Next Big Battleground In Data Security

Companies: AAPL, AMZN, CHKP, CRWD, FTNT, GOOG/GOOGL, META, MSFT, PANW, ZM

Sept. 16, 2022

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

Research Question:

With successful hacking incidents at an all-time high, what new areas are being developed by data security vendors to strike back? What will work? What won't? Which vendors offer the best opportunity for growth as new methods evolve?

Key Findings

- Malware and ransomware fears are providing some revenue cover for the data security sector. But not all companies will benefit, and new approaches to digital security are brewing. Microsoft Corp. (MSFT) has the edge, sources report.
- The collection of personal data by companies such as Meta Platforms Inc. (META) via Facebook and Instagram; Twitter Inc. (TWTR); Alphabet Inc.'s (GOOG/GOOGL) Google via search, Gmail, and YouTube; LinkedIn Corp. (LNKD); credit reporting agencies; insurance carriers; streaming-television subscriptions; and myriad other collection points in finance, healthcare, online shopping, and more has placed organizations and individuals at an all-time high risk of falling victim to digital crime. Security spending appears generally steady into Q4, sources report, even as other areas of IT networking are slowing. "The [data security] sector provides a limited safe haven, that's right. You have to keep trying to protect the data," said a senior systems engineer at an East Coast IT security monitoring company. "People are scared by what they are seeing, and a ton of what they are seeing as far as successful ransomware attacks are really their own damn fault. … I think a very prolonged, nasty storm is just over the horizon for these social platforms as far as being viable, long-term businesses. The entire ad-based concept of revenue generation is at the root of so much data compromise."
- Every source interviewed for this update agrees that the next meaningful frontier in IT security growth, if it is to happen, must focus on information privacy. "Every single data security product on the market will continue to be bypassed by cyber criminals," a long-term cybersecurity CEO source said, "unless we can get our collective arms around the crazy amount of data that makes it so simple to target people and their organizations."
- The criminals are constantly able to break into networks because unwitting users import malware through a dizzying array of phishing scams and through hackers' use of stolen, personally identifiable information. The numbers that are tossed around are staggering, and they only represent the *reported* data breaches.
- The vendors to bet on, sources said, have the most money to create layers of defense against the use of personal information. The operators with the most cash are the big three public clouds, and all have divisions that together generate billions in revenue by collecting personal and organizational information. That sets up what several called a "crazy" battle where, for example, Microsoft will be pitted against its own LinkedIn platform. "What do you think those meetings are like at Microsoft when the LinkedIn people are pushing for more and more users to post more and more personal information so the platform can make money, while the security developers are looking at the platform as a rampant threat generator?" asked a senior IT security consultant at an East Coast network integration firm. "They certainly can't deny it's happening."
- In this environment, endpoint protection and a solid data backup and recovery plan are essentials for organizations and individuals, sources said. Tied to that has to be a far more comprehensive push to get every digital user to understand that there is a correct way to leverage digital communications and a whole lot of wrong ways. "Stop using the Internet to invite criminals into your lives," said the CEO of a large UK IT security management firm. "Some of the loose and careless conduct, especially by people calling themselves infosec professionals, is, frankly, disgraceful. They can't contain the recklessness of their own people. That said, it is also a key reason why the big security vendors like Palo Alto [Networks Inc./PANW] are able to keep bringing in revenue, despite the level of successful data breaches. All of them benefit. Cisco [Systems Inc./CSCO], Fortinet [Inc./FTNT], Check Point [Software Technologies Ltd./CHKP], the lot. The entire sector represents a symbiotic relationship amongst three sets of actors: careless endpoint users; enterprise and internet-based operators, including the Metas, Googles and [Amazon.com Inc./AMZN] AWSes of the world; and the global cybercrime and state-sponsored data theft gangs. That troika has to be broken apart if this madness is to abate."

Positive: AAPL, AMZN, CRWD, FTNT, MSFT, PANW
Negative: CHKP, GOOG/GOOGL, META, ZM

Tech Sector War Looms Where Security Applications Will Begin Thwarting Info Aggregators

The sustainability of targeted-advertising online business models that suck up user data in order to monetize it with advertisers was heavily called into question by sources. Twitter, Meta, and Google are all seen as having problems with their data practices. Zoom Video Communications Inc. (ZM) and privately held ByteDance (TikTok) were also seen as facing serious data security problems. Sources were positive on steps that Apple Inc. (AAPL) is taking to improve both data security across its iCloud and for its customers' online privacy.

The Amazon Web Services cloud business continues to receive positive feedback because that division of the company is taking steps to block customer data compromises—even if other divisions of the company, such as Twitch, have been breached, and Amazon.com has billions of transactional records from online shopping and Prime video services that are potentially vulnerable. "It is so critical for them to protect that data inside AWS because AWS is where all of Amazon's other businesses do their internal IT, along with all the customers they also host in their cloud," said the CEO of a cloud-focused network integration company in the Pacific Northwest. "They can't afford a big breach. The Twitch breach was a bad one. They can't have another. I think that is why they are spending so much to make sure they have fortified their operations." Several other sources agreed that AWS has everything to lose and, therefore, is taking proactive steps to combat hackers at a high level. "They have the CIA as a customer," said another source. "So, what do you think the internal security discussions are like?"

Google also received solid feedback for its Google Cloud Platform security initiatives. But sources were harsh when discussing other aspects of Google's business that are open to exploit, and they were very critical of Google's data gathering and tracking processes that span across divisions such as YouTube.

Even though it clearly has what one source termed "their embarrassing LinkedIn problem," Microsoft was consistently cited as being the best-positioned of all vendors to seriously combat cyber criminals—both inside and outside their cloud. "They have the cash and the big infrastructure to take over the sector. I believe that more now than I did the last time we talked about it," said a senior information security engineer at an integration company that provides hybrid networks for large clients. "They are making advances on several fronts that the competition will be hard-pressed to match. They are not just developing for their cloud; they are pushing out services like the Endpoint Defender platform, no matter if your users are in the cloud or on a local office network."

Sources cited Palo Alto Networks' relentless sales and marketing machine as a reason the company continues to create revenue, despite the fact it continues to struggle to break even in GAAP terms. Fortinet is also seen as a steady presence in unsteady times. "They have a very loyal base, and hybrid network security is a heavy focus for them," said the CEO of a value-added-reseller/integration company that deals with all the major cybersecurity companies. Sources said Check Point continues to lag behind its major competition.

Of course, it is the end users who make it much easier for hackers to target them, simply based on their own digital behavior, sources said. That's why all the sources interviewed for this report remain positive regarding Crowdstrike Holdings Inc. (CRWD) and its expanding Falcon platform for endpoint and threat detection and countermeasures. Several sources pointed to the expansion of Crowdstrike's corporate threat platform to offer a home version for remote workers as another step to combat lax end-user practices that can help hackers inject malware into a work environment.

"Social-engineered hacking is moving up the threat assessment ladder right to the top," said the CEO of a security consulting firm with large healthcare clients. "If I know from a LinkedIn profile that you are a C-suite executive at a large healthcare operation, and I start a search to find out other things about you, I'm going to find things. That's a targeted attack, and those are running rampant. Let's say I find a newspaper article where your company has sponsored a golf tournament, and I see you golf. I can spoof you with a phishing email related to those interests, and you might open it up. I've got you at step one of a malware injection. This gets directly to the data privacy issues we have discussed. Do you actually think having your LinkedIn profile replete with so much of your information is truly necessary for you to conduct your business as a top executive? We pose that question to our clients all the time, particularly after we have run a successful pen test (penetration test) on one of them, and it was a successful social hack. In one case, the executive was so agitated that we got him, he tried to have us fired. It is very embarrassing when the CEO or the CFO falls for it, but it is much more common than you think because of a type of arrogance that they can't do anything wrong."

After Apple fired the first data-privacy-as-a-security-issue shot at Meta, Meta fired back that Apple was out to destroy small business by letting its customers decide whether they want to be tracked. What one source called Meta's "continual

belligerence" regarding its data-gathering practices is lining up the security community against the company. "That's bad news for them," said a senior IT security source based in Silicon Valley. "They think they are entitled to use personal information any way they want in order to fund their business model. That is not sustainable because the entire model is broken wide open. It is too easy to target and exploit people who use these platforms. It is a collision course between privacy and security and tracking and data insecurity. Both can't exist side by side. It has to either change, or it will implode, and the digital economy will be severely damaged at a time when we can least afford for that to happen."

According to several Tech Trends security sources, the row between Apple and Meta was like a lightbulb turning on for the big security vendors. "It got them thinking: Is data privacy a new area for IT security development? Can we move into that and reignite big growth? Take a look at Palo's Unit 42. What do you think is going to happen when their crack threat assessment team keeps telling customers that attacks are happening at such a high rate because they have too many of their employees on Facebook, Instagram, and LinkedIn?" said the CEO of a Midwest security monitoring company with large healthcare and manufacturing clients. "That's already a big conversation with all of our clients, and we have several running Palo Alto, Crowdstrike, Fortinet, and Check Point. We are now making money by getting our clients to limit where their key people are exposing themselves to scrutiny on social media. We have a digital education program, and our clients have to enforce policies we develop in order to use our service. You will be seeing the return of blockers keeping things like Twitter and Instagram from intermingling with internal and cloud application networking. Fortinet was already positioning for an antisocial hacking approach during the pandemic two years ago. It's coming, the whole war between social networking and business networking."

"There are divisions at Google, Amazon, and Microsoft that are going to be pitted against each other because they operate at cross purposes in many cases," said a senior IT security consultant and longtime Tech Trends source. "Look at YouTube. You can click on millions of videos and see what people are doing in their own homes. You can see what they cook, what they read, what they drive, how they recreate. China has legions of hackers who work for the military that do nothing but capture this kind of information. That is part of the whole TikTok paranoia regarding what happens to the data on that platform. Zoom is the same thing. The Chinese do not have to steal it. It is being voluntarily given away for free. Facebook (Meta) is the same thing. Instagram. If it is posted and available for public consumption, whatever is in there is up for grabs. Ditto LinkedIn. You can join platforms like Glassdoor, Indeed—it really is endless. Once you are a subscriber, there is more personal information to be gleaned about people and companies than you can possibly imagine. It makes social hacks a recreational sport for professional hackers."

Background

Senior Technology Researcher John Harrington has been reporting on data security trends for Blueshift Research since the beginning of 2014. John has a professional background in network security as well as a lengthy investigative journalism and investigative research background. For this report, he interviewed 10 executive sources in all areas of data security, all of whom are repeat Tech Trends sources dating back several years. Eight sources are based in the United States and two in the UK. All have a view across the entire spectrum of cloud and on-premise data security, including providing managed security services for large clients in sectors such as healthcare, manufacturing, supply chain logistics, transport, education, and government. Interviews were conducted in the final week of August and the first two weeks of September.

About the Author

John Harrington is an award-winning investigative reporter and veteran Wall Street researcher who has also worked in the information technology industry in data security and data center networking roles. 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 contributes 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.
