AVISHAI AVIVI

CISO
SAFE BREACH

SafeBreach

HEADQUARTERS: Sunnyvale, CA

EMPLOYEES: 140

REVENUE: Private Company

K LOGIX PARTNER PROFILES

HOW DOES SAFEBREACH PROTECT CUSTOMER DATA?

First and foremost, being a security vendor, we have to realize that customers rely on us for their own security. And if we get breached or compromised, that can spell doom for our customers. We take that responsibility very, very seriously.

The idea is to look at multiple layers of security, but also really separating the environments out so that our customer data cannot in any way, shape, or form be impacted. Let's say someone attacks SafeBreach through a phishing e-mail or something like that. The reality of it is the environments are so separated and isolated that even if something happens and all of SafeBreach enterprise goes down, our customers are still safe because they're in a completely separate space. It's not just air gapping or all the typical security mechanisms you're aware of, it's just treating it almost like a separate company and that separate company actually has no outside interfaces other than serving our customers. There are no e-mails that go in, no web browsing that can go out. Nothing of that nature can introduce risk to our customers. That's really the philosophy behind our security posture.

WHAT IS YOUR APPROACH TO SHIFTING LEFT AND THE SDLC?

There's been this movement that security needs to enable the business and not be the department of no. And to me, enabling is too much of a passive action. The way I look at it, my role is to facilitate. I like to partner with the business, partner with the development team so they see me as an active partner in their efforts. And then they actually bring me in from the get-go, so once we are involved in the design phase, we are able to better inform them on how to be more secure. The idea is that I'm never going to be able to prevent them from taking on risk, but I can help them take on risk in a way that is more controlled. It's like telling your kids – 'I'm not going to tell you not to use TikTok, let me just give you advice how to use TikTok in a way that you're going to stay safe'.

So in a sense, if you come to the discussion with the need to shift left, it tells me that there's already a problem. The fact that we need to shift left means that you're not in the right place to begin with. And that's something to be aware of.

HOW DOES SAFEBREACH APPROACH THIRD PARTY RISK?

Let's assume you're breached. How do you isolate the damage? How do you compartmentalize the environment in a way that even if something gets breached, it can't make an impact to the surrounding elements? Or can't cause harm to the next area? Let's look at submarines as an example. Submarines are designed in a way that even if there's a rupture to the hull in one department it all automatically seals or will seal in a way that the rest of the submarine doesn't go down because it's flooded. This idea is the same as how it should be designed in security. Design your environment in a way that prevents your organization from becoming a supply chain to your customer.

Now obviously there are some exceptions that exist because you have to incorporate third party libraries into the code that you develop and deliver. Well, how do you isolate those components in the sense that even if the supply chain vulnerability is exposed in those libraries, your system does a good job of isolating the interaction

points between that library and the rest of the system? It's all about creating that safe compartment, that safe shell that will protect it from expanding to the next area, or expand that blast radius.

HOW DO YOU INTERACT WITH CUSTOMERS?

I'm not just the SafeBreach CISO. I'm also a SafeBreach customer. I use SafeBreach internally and so I like to interact with customers because I want to understand how they use the product. And then also give them my point of view as a practitioner and how they can better utilize our product and get the most benefit. I'm very customer facing in the sense that I love the product and I love to see it being used correctly.

There's a couple of trends that I see. I see a lot of customers using our product in their environment and they might not think about how it helps other parts of their organization. Mainly with other teams, even teams within the same group. For example, purple teams and red teams love our product. But our product can also be used by the intel team, by the detection team, by the SOC, and even the M&A group. People are sometimes only focused on their piece of the pie, without thinking about how they can expand a product's use.

The other thing I see is that customers don't necessarily understand how they can prove or show the value of what they're doing in security. They might struggle to quantify or understand exactly how secure they are. And in a lot of cases, they might think they configured a file correctly, they're SOC2 compliant, or they think they have the best antivirus in the market, so they should be fine. More often than not, they aren't as secure as they think they are. SafeBreach helps them actually know they are secure.

For example, Log4j comes out on a weekend or a holiday weekend. Half of your technology team is already out of the office, and you have questions starting to come in from the board or from your customers, if you exposed to Log4j. How can you leverage SafeBreach to show that you're not exposed? It has a 24-hour SLA, so it can weaponize Log4j attacks. And you can then run them across your infrastructure. This gives you the ability to know, and not just hope, that you're secure because your security controls reacted or behaved the way you expected them to.

HOW DOES SAFEBREACH HELP CISOS COMMUNICATE VALUE WITH THEIR EXECUTIVES?

Part of the art of what CISOs do is being able to translate those technical and acronym laden concepts into business terms. It's not to say that boards need to have things spoon fed to them, it's just that they think in business terms and so you need to be able to make it understandable and palatable to them. Boards often say they hear all this chatter in the news about Log4j. And they might ask if it's the next biggest thing to look out for. They mainly care if they need to worry about the business. And the quick answer from CISOs is that they are there to help give them that data. SafeBreach gives CISOs that data and then the art of converting it into a story is up to the customer.

Another point is that CISOs have GAS. And what I mean by that is something I borrow from the photography world. It's an acronym for Gear Acquisition Syndrome.

A new photographer will almost always start buying a lot of gear. Whether or not they're going to use it. They buy the most expensive lens and this flash and this bag, and at the end of the day, it's all about composing the right picture. And exposing the film or the digital sensor for the right amount of time. And you get great pictures. You don't have to have the most advanced camera. You don't have to have the best lens. Yes, it makes things a little bit easier, but at the end of the day, they're not going to change the end product, the end picture. The same goes for security. Having the latest security tool and the best security tool doesn't mean you're going to use 80% of the functions to get more security.

It might make it a little bit easier, right? Maybe in the hands of a pro, they'll be able to do more. But at the end of the day, it boils down to very basic factors.