HAROLD BYUN

CHIEF PRODUCT OFFICER
APPOMNI

AppOmni

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 173

REVENUE: Private Company

K LOGIX PARTNER PROFILES

DESCRIBE YOUR ROLE AT APPOMNI.

I'm the Chief Product Officer for AppOmni, the leader in SaaS security. I've worked on both the practitioner and on the vendor side, and I have over 25 years in the security industry.

I came to AppOmni through my relationship with our Co-Founder and CEO Brendan O'Connor. We previously worked together at ServiceNow, and he was interested in bringing me on board. So far it's been incredibly rewarding in terms of the execution that we've already had.

My role here is to work with the engineering team to continue to deliver on product enhancements to our product, roadmap and strategy, and deliver what our customers need.

HOW ARE YOU PROTECTING CUSTOMER DATA?

We've done a number of things from a security perspective to ensure we are protecting customer data. First and foremost, this company is really built by security practitioners. Brendan, our CEO, was the previous Chief Trust Officer of Salesforce. Our Co-Founder Brian Soby was also a top security practitioner at Salesforce. Our Chief Development Officer has been in cybersecurity leadership for Cisco and Exabeam, and our Sr. VP of Engineering was a security lead at Apple. Many of our employees have been working on the SaaS threat and SaaS security side for the better part of 10 to 15 years, looking at advanced attackers and how those organizations try to tear apart these SaaS applications.

That practitioner mindset informs how we've built and continue to expand our product. In addition, we choose to have our own security implementation and operations in terms of how we function as an organization.

Also, we are SOC 2 Type 2 certified, which involves a fairly lengthy audit to ensure our operational controls from a security and SDLC perspective are actually in place and effective. We are currently undergoing initial FedRAMP certification to ensure we're able to best serve governmental organizations and agencies.

Then there are a number of things we do from a continuous deployment and monitoring perspective in terms of our SDLC and what we have wired up from a CI/CD deployment model from a code review, code check, and code analysis viewpoint. There's also full-blown vulnerability management and active threat intelligence. And on top of that, our solution doesn't retain much PII from our customer basis. Our solution is around the metadata of security configurations, and we've made an intentional effort to avoid collecting customer data wherever and whenever we can.

WHAT ABOUT YOUR APPROACH TO 3RD PARTY RISK?

We currently serve 20% of the Fortune 100, so we represent a certain level of risk as a third-party vendor to our customer base. We engage in standard supplier risk responses as well as formal interviews, which can be very in-depth. We've had three-day review sessions with clients, going through every single response in their supplier risk assessment.

We facilitate a mode where we can operate in a hybrid model. And that's been based on customer concerns and customer feedback where they've informed us that they want more control over the permission set and permission scopes that are used to interact with some of their applications, as well as some of their environments. The customer can deploy this code base locally in their own infrastructure to vet any of the data being retrieved before it is sent back to us. It can run with the privilege scope they're comfortable with in their own environment so we're not an external entity communicating or reaching into their environment. In the event customers want us to run the code from our own environment connecting into their SaaS apps, we have a credential vaulting mechanism. We always try to take a least privilege approach from a scoping mechanism whenever we interact with those environments.

In terms of our own third parties, we have a security program that requires reviews of different applications or third parties that we're using in our environment. Everything is integrated into an identity provider solution with a hardware key requirement for all the employees in the organization. And anybody who cannot support that requirement is not used as a third-party vendor.

We also have our own third-party vendor review process. Depending again on permission scopes and how these vendors would connect into our organization or the information-sharing that's required, we may choose to not engage with some of those vendors.

WHAT IS TRENDING WITH CUSTOMERS?

I have observed many customers discussing the friction that CISOs and security teams encounter with their business and application counterparts. Often, these parties might not be aligned. Security is trying to accomplish what is best for the company from an implementation perspective, but the business goals might not be aligned. These situations require navigation. In some cases, an organization has significant success streamlining and operationalizing a program around SaaS security. And in other cases, there is resistance from the business. But once they bring in our solution, we may find hundreds of thousands or millions of data records exposed to the Internet, to the public, which then provides a shining light into the risks present. There's important dialogue to have with the business, and for security and IT to collaborate with them to find a secure solution.

Another trending topic is SaaS connectivity around third-party risk. There are many SaaS-to-SaaS connections established with the core SaaS platform that don't go through security, procurement or legal reviews. An end-user might install a plugin for something they want to try out, then decide they don't want to use it. However, once that plugin is installed in the SaaS application, it ends up creating a long-lived connection in the environment. It could be there for one, two years or longer. I think there's a huge lack of visibility in that area.

HOW DOES YOUR SECURITY BUDGET SPEND COMPARE TO END USER ORGANIZATIONS?

I would definitively say we spend more. We recognize that as a security vendor, there is a very low tolerance for getting breached or being the source of an attack for customers. We invest in making sure that doesn't happen.

When it comes to budget spending, our in-house security practitioner base has extensive experience doing security reviews for SaaS platforms they've previously worked at. As a result, we have exceptional hygiene around those types of things we do internally, and we tend to gravitate to building a lot in-house. When we need external validation, we will look to outside organizations to help us from an assurance and validation perspective. From a tooling perspective, we certainly use modern third-party solutions for additional analysis and code analysis.