KARL MATTSON

CISO
NONAME

noname

HEADQUARTERS: San Jose, CA

EMPLOYEES: 260

REVENUE: Private Company

DESCRIBE YOUR ROLE AT NONAME?

I joined Noname about two years ago as CISO. I consider my job split into four different areas. First is to build an information security program. The second is corporate IT. The third is risk and compliance. And 4th is as a field CISO. I joined the company after having been one of its first customers. In the decade prior to joining Noname, most of my time was in financial services. Working here is my first job in a company that's not a publicly traded, large enterprise. I came to Noname to build out the structures of security, risk, compliance, and IT to help us grow and scale. My strategy is to build those programs the way our customers would want and expect to see them built, with the same elements of structure and capabilities. I apply that large enterprise lens to everything that we do.

HOW ARE YOU PROTECTING CUSTOMER DATA THAT RESIDES WITHIN YOUR ENVIRONMENT?

We do so with a three-pillar approach. The first pillar is architecture - we have a SaaS offering for customers, a single tenant SaaS solution. Every customer's environment is unique and separate. Single tenancy is an enormous positive impact in terms of protecting customer data, because there is no single point of shared data amongst customers. The second pillar is the ongoing identification and classification of data, as well as the monitoring data movement, which is really what Noname specializes in. We are using the Noname product internally, looking at movement of data in the environments as well as the hardening of data stores. Next is thecloud infrastructure security posture. For example, we are building and managing our systems to hardened configuration baselines. This ensures we're applying best practices at every juncture. Are data stores encrypted? Are they configured well? Then the last pillar is access identity and that's a very traditional space, I think for most CISOs, but it is ensuring that the access layer to data stores is managed.

HOW DO YOU ENSURE SECURITY IS BAKED INTO THE SDLC?

The first principle is to not just partner with the development teams during the SDLC, but to actually let them lead and let them drive the tools of application security. It starts with laying down foundational requirements whether it's threat modeling, SaaS scanning requirements, or penetration testing requirements, and setting those as the policy objectives. Then giving the development teams the opportunity to select and lead the design of processes. For example, when we're implementing a particular code scanning process in the pipeline, we build processes the developers and infrastructure teams have chosen. That gives them the imperative to adopt and use that technology. For Noname, we have our shift left offering used internally for our API development, but we also have the regular commercial off the shelf tools that most application teams are using today. I think product selection is 80% of the battle with developers. When developers own that selection there's a tremendously different option rate and developer self-servicing and owning the security of code because they have a stake in it.

HOW DO YOU ADDRESS THIRD PARTIES?

For our use of third parties, we have a third party risk assessment practice. We ensure due diligence in advance and review that our security certain criteria is met. From a third party risk management perspective, we have an advantage because when we started this journey about two years ago, we were starting from a blank slate and put in place third party assessment practices that have served us well.

On the flip side, as a vendor, we're the recipient of that from customers looking to us to demonstrate evidence around the quality of the software, and the integrity of it against supply chain risks. There's no cheat code in doing that. What I would suggest is that security vendors really need to look at the customer due diligence process as an opportunity to tell a story and give their customers insight. Here's an example: there's a bank in the Midwest that is a pretty large institution, and they sent out a customer due diligence questionnaire with over 1000 questions. Now there's two ways to look at that is - did I just lose a week of my calendar because I'm answering 1000 questions, and some of them are very detailed, or is that an opportunity to differentiate myself from our customers and inform my internal program if there are details we haven't thought about yet? We welcome due diligence because we strengthen our security practices when you take those due diligence requests and make them requirements for your teams, and it has the effect of showing customers that you take into account what they're looking for.

WHAT ARE SOME CURRENT CUSTOMER CONCERNS?

Privacy implications are a big topic. There's European data privacy, Australia, United States, of course, California. We are both subject to those requirements and we're the provider of the answer for those requirements. When a customer is doing due diligence on us and we're talking about privacy restrictions, we are often the customer's answer in terms of enforcing what they need to do on their side to their policy.

HOW DOES YOUR SECURITY BUDGET COMPARE TO END USER ORGANIZATIONS?

As a per employee dollar ratio, we are probably spending three to four times as much. But there's a big caveat that as a security company, we also have the unusual feature of having the IT department report to a CISO and an employee base that readily accepts a high bar for security. My security budget also includes a lot of elements that would normally be IT, such as all Access and Identity platforms and activites. As a combined unit, by and large, our security professionals and our IT professionals are largely cross-functional in their daily routines.

WHAT IS YOUR APPROACH TO AI?

What we've effectively landed on is to look at the AI space as an X and Y axis. On the X axis we have end user on one side and attacker on the other, and for the Y axis product is at the top and developer on the bottom. To give you an example of how this works, take the end user side. I want to be able to establish policy and controls for an employee to use ChatGPT or publicly available productivity pilots. Wonderful, but we must have a policy and controls to ensure use is intentional and approved. On the attacker side, I need to have detective controls with that for sophisticated inbound phishing e-mail, for example, Are my protective controls ready to spot that and capable? On the Y-axis We want to give developers the jetpack of automation and intelligence of AI, but also ensure the source code going in has integrity and that we're not creating more problems than we're solving by giving developers unvetted tools to development. On the product side of the front end, that's the most important thing, which is how do we create experiences for our users, capitalize on AI capabilities for things like event correlation or for identifying sophisticated API attacker behavior that otherwise might be very difficult to detect, so we have to look at all these areas in the space of AI security in its opportunities and its risks.

By seeing what's happening in all these AI subtopics, it will eventually create an AI stack for ensuring you can optimize the business value of using AI. This means ensuring your end users are protected and efficient, and ensuring attackers are countered with AI and defense matters.