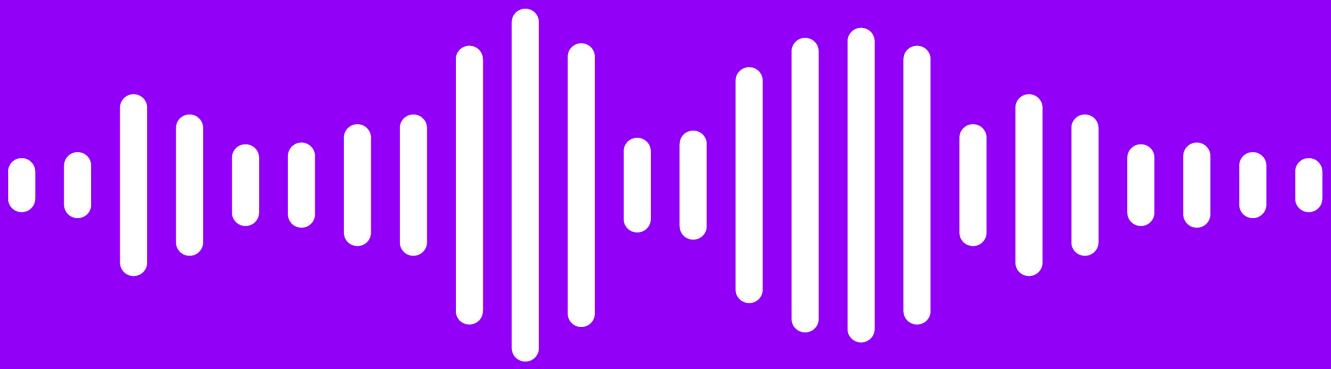
FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE



SPECIAL EDITION

Amplifying the Voices of Security Technology Leaders

READ Q&AS FROM:

Mike Britton, CISO, Abnormal Security
Abhay Salpekar, VP, Cloud and Platform Engineering, Anomali
Harold Byun, Chief Product Officer, AppOmni
Tyler Farrar, CISO, Exabeam
Damian Chung, BISO, Netskope
Karl Mattson, CISO, Noname
Dennis Dayman, Resident CISO, Proofpoint
Avishai Avivi, CISO, SafeBreach
Chris Bates, CISO, SentinelOne
Richard Bird, CSO, Traceable

KLOGIXSECURITY.COM
MAY 2023
617.860.6485

K logix

TABLE OF CONTENTS

May 2023

FROM THE *Editor*

Dear Readers,

The question we asked ourselves before putting together this special edition issue of Feats of Strength was – how do security companies approach their own internal security?

Our goal was to better understand how security vendors approach internal security, protecting their customers, employees, and overall brand. We interviewed CISOs and other security leaders to better understand their approaches, goals, and challenges. The conversations we had were not far off from our typical conversations with CISOs – they are still responsible for justifying their decisions to executives and the board around resources, budgets, and program initiatives. They educate their business counterparts about the importance of a strong security culture and must embed security into all stages of product development. Hot topics included thoughts around AI, third party risk, and securing the SDLC.

This issue is important to us because it covers topics that directly impact our customer base. When they're investing valuable budget in security technologies, we want to make sure they have full transparency into how their vendors approach security. During these interviews, we had customer concerns and goals top of mind, asking relevant questions to gain a better understanding. We hope you enjoy reading these Q&As and learning more about the inner workings of some of today's top security vendors.

Kevin West

CEO, K logix

Magazine Contributors

Katie Haug - Editor
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Graphic Designer, K logix

About K logix

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication Feats of Strength. Through hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

MIKE BRITTON

CISO
ABNORMAL SECURITY

/\bnormal

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 500+

REVENUE: Private Company

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

Our business cannot exist without our customers trusting us with their data. We do not rely on one single point of control, but rather apply a comprehensive program that consists of monitoring and defending our cloud environment, networks, data, and end users from today's most pervasive threats. We leverage multiple industry-leading solutions that use modern capabilities to stop advanced attacks, and are backed by a dedicated team of cybersecurity professionals with an average of 10+ years of security experience, much of which comes from large enterprises across multiple heavily-regulated industries.

WHEN DEVELOPING YOUR ORGANIZATION'S SOFTWARE, HOW DO YOU ENSURE SECURITY IS BAKED IN FROM THE BEGINNING AND NOT A DRAG ON PRODUCTION?

Powerful security starts with the strong relationship and partnership we have with our engineering and development teams. As a cybersecurity company, every employee understands the importance of operating securely–and this especially applies to the teams responsible for creating, deploying, and maintaining our SaaS platform. We provide active training and resources for our developers to ensure they have the necessary skills and knowledge needed to code securely, as well as tools to actively scan code for weaknesses and vulnerabilities. Finally, to ensure our SaaS platform is free from vulnerabilities, we also leverage a third party to conduct regular penetration testing of our web applications, networks, and our API.

WITH THIRD PARTY RISK ON THE RISE, HOW DO YOU PROTECT YOUR ORGANIZATION, AND YOUR CUSTOMERS, FROM A SUPPLY CHAIN ATTACK?

Protecting our organization from supply chain attacks starts with a strong third-party risk management program. This program is an integral part of the procurement process. We assess and classify each vendor's risk, then perform regular re-assessments based on those determined risk levels and the criticality of the supplier. Finally, we work closely with our legal team to ensure data processing agreements (DPAs) and security requirements are in place for any supplier processing personal data on our behalf. We require our suppliers to meet the stringent requirements that our customers expect.

HOW DO YOU EFFECTIVELY COMMUNICATE WITH CUSTOMERS THAT THEIR DATA IS SAFE WITH YOU?

We proactively maintain a Security Hub and Trust Center where we provide customers with a library of our security documentation, independent reports including our SOC2 report, penetration test reports, and others, as well as the

certifications we actively maintain as a company: ISO27001, IASME Cyber Essentials Plus, and more. In addition to security information, we also provide a product privacy guide, as well as resources and documentation on how we actively comply with data protection laws.

AS A SECURITY ORGANIZATION, DO YOU BELIEVE YOU SPEND MORE, LESS OR THE SAME ON CORPORATE SECURITY AS COMPARED TO END USER ORGANIZATIONS?

Even though we are a security company, where securing our customers and data is held in the highest regard, it is still important to be good stewards of our resources. We must be able to provide the best protection and maintain the ability to innovate in order to meet customer needs and expectations.

As a result, we are continually focused on maturing our security controls and ensuring we leverage automation and continual improvement to make us better. As a security team with full support of our Board and executive leadership, we have the budget and resources to ensure we run a security program that establishes and maintains customer trust.

ABHAY SALPEKAR

VP, Cloud & Platform Engineering

ANOMALI

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 350+

REVENUE: Private Company

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

Data security is a critical part of our data management strategy. We ensure end-to-end encryption, i.e., data in transit and data at rest encryption. We encrypt data, not just encrypt volumes that hold data. We also have a policy to rotate encryption keys periodically. We keep all our secrets in vaults and use dynamic credentials and keys where possible.

Access to data is based on the least privileges policy. The least privileges policy is enforced on the segregation of duties (SODs policy), and it is also tied to the data classification policy.

The robust Observability platforms based on metrics, logging and tracing pipelines continuously monitor access patterns and scrutinize abnormal non-contextual behavior patterns to ensure data security. We also assess our security posture regularly to ensure data security is adequate, sufficient and meets our business obligations to customers.

Protecting customer data requires a multi-layered approach that involves both technology and processes to ensure that sensitive information is secure and protected from unauthorized access or use. We have a well-defined unified security posture management plan to ensure this.

WHEN DEVELOPING YOUR ORGANIZATION'S SOFTWARE, HOW DO YOU ENSURE SECURITY IS BAKED IN FROM THE BEGINNING AND NOT A DRAG ON PRODUCTION?

We have security measures built into our SDLC. Our development philosophy is based on security first mindset. The Applications are designed to ensure code security. We use peer programming and integrate SAST, DAST, IAST & SCA tools in our pipeline. Repositories are scanned in real-time. Pre-prod and prod environments are pen-tested regularly to assess the attack surface, and if any issues are identified, they are remediated at the highest priority. We do use RASP tools for the production environment.

We always appreciate the use of security tooling in our day-to-day development as it pre-empts any occurrence of attack into the application. We introduce such tooling early into the SDLC, which is always the best approach to secure software.

Our security tooling is automated and embedded in the CI/CD pipeline, and we continually monitor the efficiency and performance of our pipeline. Security tooling is costly, but we take security seriously, which is a requirement of our development process.

WITH THIRD PARTY RISK ON THE RISE, HOW DO YOU PROTECT YOUR ORGANIZATION, AND YOUR CUSTOMERS, FROM A SUPPLY CHAIN ATTACK?

We have a rigorous vendor risk assessment process. Every vendor in the supply chain, including our partners, has to go through this and qualify to work with us. They also need to ensure that their internal security processes meet and are aligned with our standards. They also need to meet the compliance requirements that our customers demand from us. We also conduct periodic audits of their systems and environments and also conduct pen tests. We also ensure they have an incident response process that meets our requirements. As a security solution provider, we take third parties' adherence to our security standards seriously.

HOW DO YOU EFFECTIVELY COMMUNICATE WITH CUSTOMERS THAT THEIR DATA IS SAFE WITH YOU?

It is essential for us that our customers have confidence in our security posture and unified security posture management process, including cloud (CSPM); we allow our customers to conduct audits of our environment so they can ensure that we meet their security requirements or exceed them. We also conduct periodic security audits and pen tests of our environments from third-party professional entities and share the results with our customers.

We are open and transparent with customers about our organization's data security policies and practices. We clearly explain and share our policies about data protection, measures we have in place to prevent data breaches, and how we respond to any incidents.

As a security organization, do you believe you spend more, less or the same on corporate security as compared to end user organizations?

We are a well-established cyber security product company. We provide security solutions to our customers to secure their environments. Security is in our corporate DNA. Every activity in the organization is performed with security first mindset. It will be hard to say how our security spend is compared to other organizations as we develop security products that help our customers to secure their environments. In our organization, being a security product developer, everyone eats, breathes, and sleeps security.

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.

TYLER FARRAR

CISO
EXABEAM

exabeam

HEADQUARTERS: Foster City, CA

EMPLOYEES: 669

REVENUE: Private Company

DESCRIBE YOUR ROLE AT EXABEAM?

My role is classified into three major areas. First is more traditional corporate or enterprise cybersecurity – looking internally into the organization and protecting our enterprise infrastructure and the endpoints that our employees use. The second area is within product security, securing the products that we sell to our customers. The third area is related to external engagement and telling the story about myself, our company, the industry, and our product. Because we use the product internally, I am able to share my experience of how Exabeam uses Exabeam.

HOW DO YOU ENSURE SECURITY IS BROUGHT IN AT THE BEGINNING OF THE SDLC?

It's all about building a risk-aware culture. It's a change in mentality with a group that is used to working quickly and deploying software to build a product. There are obviously tools that can do the work of identifying the issues or shoring up various prevention controls, but when those issues arise, it's about teaching and partnership.

So, how do you then engage and try to do it in automated means? Maybe the engineering manager is going to know that the developer didn't clear a specific finding or vulnerability, and they deployed vulnerable code to production. It puts the onus and responsibility on the manager, not just the CISO or the cybersecurity organization, to hold their team members accountable and own their part in securing the organization.

HOW ARE YOU APPROACHING THIRD PARTY RISK?

Our third party risk program spans from being able to inventory all of our vendors to classifying the criticality of these vendors to Exabeam. I'm talking about how vendor dependencies can impact our business operations. It enables us to determine how long we can be down for.

From a security perspective, it's about defining a discrete set of criteria. So when we go through the procurement process, my team is always able to assess the vendor risk to the business. This is executed through the assessment of specific criteria; from compliance certifications to policies to diagrams and system security plans, etc.. We want to uncover: What is the true risk to Exabeam, and are we comfortable with that risk score?

WHAT CONVERSATIONS DO YOU HAVE WITH CUSTOMERS ABOUT THIRD PARTY RISK?

We highly value all aspects of cyber assurance. Just as Exabeam conducts its own third party risk assessments, our customers perform the same on Exabeam. We're not only expected to be able to provide answers to these questions, but also provide the evidence to show that policies and controls have been implemented to manage and mitigate risk. This is all about partnering with our sales teams and assisting with RFPs. We must be able to effectively deliver on requested information, as well as be in tune to what best practice industry standards are and what our customers expect of us. In regards to what we demand of our vendors, we try to have that coalescence

of equality – being able to say that we feel comfortable with the business relationships that we're in.

WHEN YOU'RE SPEAKING TO CUSTOMERS WHAT OTHER CONCERNS DO THEY HAVE?

Ensuring adherence to various regulations and compliance certifications are important to our customers. Outside of that, I've seen a growing number of inquiries around crisis management; how does Exabeam respond when something bad happens? Business disruptions can and will happen. Therefore, Exabeam has prepared for these operational disruptions to ensure continuous availability of our product and our business. So, I see questions come in - What are your SLAs around this? Do you have an incident response plan? Do you know how to manage the business through a crisis? These questions are really centered around business continuity and disaster recovery.

HOW DO YOU APPROACH BUDGET SPEND?

Just like we approach security - it's everyone's responsibility. Security doesn't stop where my team ends from a functional organization perspective. At Exabeam, there are people focused on security within research and engineering, as well as product security and compliance management. They don't have to report to me to do that. We are all responsible for instilling a culture of security.

HOW DO YOU COMMUNICATE EFFECTIVELY WITH EXECUTIVES AND THE BOARD?

It can be broken down into a step by step process. Every month, the core technical metrics are compiled, which conveys key trends and risks. At the end of the quarter, these metrics tell the story; Are we where we want to be in our journey? What are our key risks? I then take all of this information and distill it for the next phase: telling our story to senior Exabeam leadership. We then go meet with the board, ensuring that we are communicating what the overall security posture is across enterprise and product infrastructure, key accomplishments, key risks, and key priorities.

WHAT PREVIOUS EXPERIENCE DO YOU HAVE PRESENTING TO BOARDS?

In my previous role, I presented to the Board Risk Committee. During my military service, I was responsible for leading various cybersecurity operations. Following each operation, I was responsible for conducting a briefing on the result and effectiveness of the operation to senior military leadership. While the military and private sector are different, there are many parallels in how we analyze and present our overall program.

DAMIAN CHUNG

BUSINESS INFORMATION SECURITY OFFICER

NETSKOPE

HEADQUARTERS: Santa Clara, CA

EMPLOYEES: 2500

REVENUE: Private Company

TELL US ABOUT YOUR ROLE AS CISO NETSKOPE?

My main role is to run security operations for Netskope internally on our corporate side. But as you know, I'm also a practitioner talking about how we see security in the future and trying to drive operational efficiency within security operations. As such, I also work in a customer-facing capacity, in addition to my primary role. While I'm not part of the sales organization or the sales cycle, I should point out that I do run our product as one of our core tools, but also integrate that with a lot of other security products in our stack. This affords me the opportunity to honestly and authentically go out there and talk about our experiences, best practices, and how to drive efficiencies and business value from our internal security program.

FROM A SECURITY OPERATIONS PERSPECTIVE, WOULD YOU SAY NETSKOPE RUNS THAT PROGRAM SIMILAR TO ANY OTHER NON-SECURITY ORGANIZATION?

Before working at Netskope, I was part of a large security team with 60,000 total users across the enterprise. So, running a security program like that, as you can imagine, is a lot bigger, but it's very similar. The difference with Netskope is they don't have a lot of legacy systems. We're very cloud-forward. Thinking about how we deploy security across that type of platform, four years ago would have been a challenge, but today it's different because of better tools. It's not like we need to be scared of digital transformation anymore. Security has always been known as the "Department of No". But what we want to do is promote security as a business enabler, so the only difference is that I can be a little bit more strategic and cutting edge, and I want to say take more chances, but in reality we're not taking more chances. We are pushing the boundaries of how we think security should be in the future and leading by example, not just talking about it, actually doing it and then publishing best practices.

HOW DO YOU ENSURE SECURITY IS PART OF THE SDLC?

It's part of building the culture, really. SDLC is huge for us. Just trying to make sure that our product itself is developed securely, takes a lot of culture and education. One aspect is that we have a "security warrior" program where we're instilling that kind of culture within our developers so they are doing the best practices according to their software development and making sure that we are testing that through our own internal red team and purple team against our own product. For companies that don't develop their own products that might be new to them, but for us it's a major part of our program.

HOW DO YOU APPROACH THIRD-PARTY RISK?

We go through frameworks and get the certifications that give us some standards to work toward, and if our customers are asking us questions on how we manage our security, we can point to some of those certifications. We also have a dedicated GRC team that can answer questions on how we handle our own data, our customers data, development of our code and even business

resiliency for the product, because a lot of customers are depending on us. I look at third-party risk as trying to understand my vendors because we are on both sides of this; I have to be a customer of other vendors as well.

I'm worried about protecting my organization and our data through potential issues with our third-parties, and so on the flip side of that, we are a third-party for our customers and they have the same questions. So, because we're in between, we play both sides of that. I totally understand the importance of making sure that we hit our compliance, making sure that we are up to date with our security and vulnerability management and making sure that we're communicating those with our customers so that they're aware of how we're addressing zero-day vulnerabilities and trying to make sure that we hit our own SLA's in terms of patching and remediation.

HOW ARE YOU THEN COMMUNICATING THAT WITH CUSTOMERS?

At Netskope, we treat our customers as partners. If they have a question, we have a whole GRC team that can answer anything about governance, risk, and compliance. We have a very strong community online where a lot of our customers can ask those questions as well or just email us directly. If there's a major vulnerability in a tool that we use, we will let them know whether we're using that tool or not. It may not be something in our environment, but we will still send an email to our customers letting them know this is not a tool that we use within our environment, so the vulnerability does not affect us. Or if it is a tool that we're using within our environment we tell them that we've successfully patched it and we've covered it. A lot of that communication is really, really important, just to give the customers peace of mind. Because if you don't communicate with customers, they just don't know where you stand, and they don't know what the status is for any kind of issues that may come up throughout the lifecycle.

HOW DO YOU EFFECTIVELY COMMUNICATE WITH EXECUTIVES AND THE BOARD?

Our entire organization is generally more knowledgeable on the cybersecurity front, but we still have to do a lot of communicating across our organization because they may not be up to date with what's going on today for specific attack vectors, for the broader organization. We do have people looking at threat intelligence and recovering that for our customers like any other organization. When I go to our executives, do I need to go and justify purchases? Absolutely. Even for our own products, so I do operationalize the Netskope product within Netskope. That's one of our core programs.

We look at the business value of all of our tools. Every year we'll take a look at the tools we have in our security stack, evaluate them, and also review our total spend across our program. The communication to our executives still has to happen in a way that they understand how we're operating and the maturity of our security program. But it's not like I get a blank check to purchase anything that I want. We don't get to just blindly go out there and implement tools, because at that point you would become inefficient in your security program. You just have tool fatigue, alert fatigue. So, it's a matter of presenting your program to executive leaders so that they understand the business value of the security program. And that is applicable to us on the vendor side as much as it is on the customer side.

DO YOU THINK YOU SPEND MORE ON SECURITY INTERNALLY THAN NON-SECURITY ORGANIZATIONS?

It depends. I don't think I could say yes or no. There are probably customers that spend more per employee on security than we do, and then there's probably a lot that don't spend enough or a lot less than us, so I couldn't really answer whether we spend more or less. It just depends on what vertical, who they are, and how advanced they are. Are we well-funded? I would say yes. Do I have an unlimited budget? No. Do we have a good handle on some of our business use cases and communications with our executives? Yes, we do and that's because we are a security company, so it is a high priority for us to make sure that we have a mature program. What we don't want to do is spend and spend inefficiently. You can't solve a security program by just buying tools, and I think we've addressed that. We want to be able to show that we're part of the business and we are enabling them and spending our dollars wisely.

As I said earlier, we don't get unlimited spend, but we do get funded sufficiently. And if there's a major gap, it's really about communicating what that risk is and doing an evaluation based on how much that remediation would cost versus the risk.

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.

DENNIS DAYMAN

RESIDENT CISO
PROOFPOINT

proofpoint.

HEADQUARTERS: Sunnyvale, CA

EMPLOYEES: 4,500

REVENUE: Private Company

WHAT CONVERSATIONS DO YOU HAVE WITH CUSTOMERS?

The team that I am on is called the Resident Chief Information Security Officer (RCISO) team. Many of us have been in the security arena as CISOs for a long time—and like me sometimes for 30 plus years—so we have a good deal of operational experience. Within our company, this allows the RCISO team to drive and support our people-centric security vision for our clients. Whether they need to understand current cybersecurity trends as revealed in our annual Voice of the CISO and Board of Directors reports, require assistance with account team strategy, or have a customer CISO requesting support for a business case, we are here to help.

The company even has a Customer Advisory Board (CAB) that we meet with regularly to understand their concerns, problems, and what they're seeing in terms of security issues. We share what we've learned in instituting technologies like Proofpoint, and how we would do it from an operational CISO role at those companies.

When talking to customers, I always want to know what's keeping them up at night. And for a lot of them, they're not sure which direction to take. If they come to us and work with our team, but also allow us to listen to them about what technologies are out there and what has not worked in the past, it helps us build a better product and improve customer service for defending their data and protecting their people.

It's going to get even more interesting over the next couple of months, because we're expecting a new rule from the Securities and Exchange Commission (SEC). The SEC is now saying they'd like to see a CISO on the board of publicly traded companies because they want that board to be more aware of what's going on. And also, to put some accountability into what the board may or may not be investing in from a security perspective.

What we're doing from the RCISO program is to bring in as much insight from all over the place, as our team consists of people who have been in healthcare, financial services, and SaaS based technology companies. And this breadth of experience is great as a group because we go and speak at events. We go and listen to understand what have we not been seeing, what have we not been hearing and how can we spread that information too.

WHAT IS MOST IMPORTANT WHEN COMMUNICATING WITH CUSTOMERS?

Number one, hyper transparency is most important. Not hiding behind the issues or the terms and conditions. The Customer Advisory Board is one way that we communicate work with customers. As we're developing new technologies or we're seeing the threats we want them to be aware of, we are always as open and candid as we can be. This is number one for me.

We do a lot of roadshows and go and meet with customers. In fact, over the last couple of weeks, I've been traveling and meeting some of our own partners as well, talking to their customers about what's happening in the world, hearing what they are seeing in their own companies, what's out there, sharing what data policies are and how to implement them with technology. I try to be open and share that with as many people as I can.

HOW SHOULD ORGANIZATIONS PROTECT CUSTOMER DATA?

It really starts with people. We know that you have to defend the data, but you also have to protect the people. And in today's world, a lot of threat actors are not necessarily going after systems anymore. They're going after the VIPs, if you will, the privileged access accounts (PAM) that are out there. And the best thing you can do right now is to build tools and invest in training to help people protect themselves and be better prepared. If you put the right tools into their hands like looking for malicious URLs where they don't really have to always think about it, they still need to be trained on it. But showing them that by looking at a URL and seeing misspellings or looking for misspellings within the domain that the e-mail might be coming from, that's where it really begins.

HOW DO YOU DISCUSS BUDGETS WITH CUSTOMERS?

Customers are naturally concerned about budgets. They do come to us and say — 'okay, how are we going to show that there's going to be a benefit from this?' And we're able to do so with a lot of different tools and methodologies that we've created with customer input. At Proofpoint, we have business case studies that greatly help them show value.

We actually sit down, trying not to oversell them to begin with, as we know a lot of companies want to sell them everything under the umbrella, not necessarily what they need right now. Maybe you might need some things a little bit later and that's fine. Let's start with the most pressing issue right now so that we can make that budget hit a little bit easier, and then move into that flight of products.

We create these business cases not only for the buyer, but for them to be able to give that to their board and their business unit management. They can then show that by not implementing these sorts of technologies, if there was a data breach it would cost them a certain amount of dollars. But by instituting this technology, person by person, license by license, technology by technology, this is really what we're going to save in the long run by investing in it now, and over time as we need, we can then add on more as we see fit.

HOW DO YOU ADDRESS THIRD PARTY RISK?

A lot of companies unfortunately still don't regularly meet or work with their third parties. It's almost like a sign and forget it sort of contractual effort. You're going to go off and do an audit, then internally, why aren't you running those sorts of audits with your third party? Even from a contractual relationship, what sorts of things are you requiring to do in privacy?

I was also a Chief Privacy Officer. We always talked about the principle of "data minimization," meaning that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose or only holding on to the data, using the data for the time that you need it for, and then getting rid of it. If you're working with supply chain and third parties, make sure your third parties are also reducing the amount of data they're holding onto during a specific time period. Make sure that they also meet your own internal policies when it comes to data minimization.

If you've got a policy for a specific thing within, say finance, maybe they should be also meeting that same threshold, whatever that policy could be in data holding time periods. Again, most companies go off, they just sign an agreement and that's it, they never regularly review their third parties. They assume it will make their systems work better, but they have to function the same way you would create or force your own people within your own company.

HOW DOES YOUR WORK AS A PRIVACY OFFICER IMPACT CONVERSATIONS WITH CUSTOMERS?

When you look at what's happening just here at the state level to begin with, we're seeing many more states now coming up with new data breach regulations.

We have about five states with privacy regulations. There are about 52 bills out of 24 states that are being pushed through with all sorts of fines and misuse of data or data being breached. The cost structure is going up. You look at what happened with GDPR once it came out. Being able to fine you a certain amount of your firm's annual revenue from the preceding financial year, you look at that and realize you don't want to be the next example of a fine or loss of trust from PR issues that have untold losses associated with it.

We are also seeing insurance companies not paying out policies when companies have a breach. They are not paying out because when they investigate the case, they find employee malfeasance or employees doing something incorrectly, and they can prove it which invalidates the policy. They say, 'sorry, your policy doesn't pay out for misuse or not having the proper security. So, you're on your own now.' They pull in products like ours to then hopefully be able to get another cyber insurance policy.

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.

CHRIS BATES

CISO
SENTINELONE

SentinelOne

HEADQUARTERS: Mountain View, CA

EMPLOYEES: 2,100+

REVENUE: $422 Million

HOW WOULD YOU DESCRIBE YOUR JOB?

My job is to protect SentinelOne's employees, systems, and fleet from attackers and misuse, and I am also responsible for building trust through proactive transparency with our customers.

I just took on a new role as Chief Security and Trust Officer, and will be enhancing our trust program to drive greater transparency around how we use, store and access data and proactive, honest communications with key stakeholders.

HOW DOES SENTINELONE PROTECT CUSTOMER DATA?

We have a very robust insider threat program through which we monitor usage, and a very robust security program overall. Data is stored in a way of least privilege, and it's encrypted. We monitor all access and there are a lot of trips and gates that allow us to detect abnormal usage in real time. We use a lot of automation to handle responding to and investigating possible malicious activity.

HOW DO YOU ENSURE SECURITY IS BAKED INTO THE SDLC?

I run a team called Application Security and their sole job is to partner with the R&D teams as they're designing things. They start from teaching how to write secure code to actually enforcing the SSDLC, which includes security reviews and how we develop code in a secure way. They also man all of the gateways and checkpoints to make sure that when code is checked in, it's got a threat model applied to it. We have tooling that scans code at commit and blocks it if it has issues. Once the code is deployed via the pipelines into production, then I bring in a Production Security Team to make sure that the only things running in production come from the approved pipelines, from the approved code, and are configured in the approved way. They monitor to make sure nothing running in production is modified in a way that it shouldn't be.

WHAT HAS YOUR EXPERIENCE BEEN LIKE WORKING ON BOTH THE VENDOR AND END USER SIDE?

Since I've worked on both sides, I look for vendors who are going to be partners with us. Vendors can tell you whatever they want, but when stuff goes sideways - and it always goes sideways - are they going to be the people standing next to you to fix it?

I work for a data company, so I ingest a lot of data and I can do a lot of cutting-edge things. For instance, I think right now, 80% of my tickets are fully automated. The SOC never even sees them. From the time it fires to the time it's resolved, the SOC never touches it and it gets into user validation and interaction. And that's pretty cool from an efficiency and productivity standpoint.

HOW DOES SENTINELONE'S SECURITY BUDGET COMPARE TO END USER ORGANIZATIONS?

I report to the CEO and the board. And we receive the funding we need to do what we need to do. We scale the budget by breaking it down per team. For example, the GRC team is based on compliance and sales needs, the security engineering team is based on data and automation. Appsec is scaled with the CTPO's

organization. Each team has its own specific alignment to a business driver, and as that business driver scales up or scales down, we scale the budget.

IS THERE ANYTHING ELSE YOU WANTED TO SHARE ABOUT WHAT YOU ARE DOING AT SENTINELONE?

We've just announced new generative AI capabilities within our threat hunting platform that are going to transform security. Essentially, we're putting the power of AI in the hands of security teams to help them detect and respond to threats at machine speed. And they don't need to know detailed query languages to do it. Through our platform, they can ask a native language question, and not only will the system return the data, it will suggest other questions they may not have thought about and recommend four or five actions they should consider. It's going to change the way people in the SOC and security work.

RICHARD BIRD

CSO
TRACEABLE

TRACEABLE
Intelligent API Security at Enterprise Scale

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 150+

REVENUE: Private Company

HOW WOULD YOU DESCRIBE YOUR ROLE?

Being a CISO at a security solutions company like Traceable is a dynamic role. I am an evangelist for security innovation, security best practices, and the functioning CISO for both internal corporate as well as product, and that takes up about 30% of my time. I am lucky that we have a really great security staff that does all that heavy work. I get involved in any incident reporting and managing the security team. Before transitioning to a dual role about 5 years ago, I spent 20 plus years on the corporate side. I'm not only someone that's been a CISO, I'm someone who has also been a CIO. I came up through IT operations in the first half of my technology career, then I moved into cyber security for the second half. What is awesome about my role is I get to help grow a company, be an influencer driving innovation and coach and lead others on a hard core security team.

About 70% to 80% of my time is customer-facing with other CISOs around things like strategic program creation, like "Why should I buy an API security tool? How do I establish the criteria for buying the right API security tools? What else do I need to do?" This is really new ground everywhere because I have seen this pattern before.

I used to have data governance problems. I used to have IT asset management problems. I didn't know how many things I had. I didn't know how many firewalls or how many firewall rules I had or how many virtual servers I had. So a lot of my conversations with colleagues and peers in the enterprise world are regarding – How do we frame up governance around API security? How do we frame up ownership? Which organizations should actually be responsible for it? All those kinds of mechanics and that's where I get to leverage my 20 plus years of experience, building those programs and helping CISOs and CSOs that have tremendous responsibility in enterprise space.

HOW IS TRACEABLE ENSURING THEIR CUSTOMER DATA IS SAFE?

The way that we ensure customer data is safe, is by providing customers with the ability to never let us have their data, at least not in its raw form.

We provide, as part of our feature and functionality capabilities, the ability for customers to obfuscate any sensitive data or all data that they want to. When you implement Traceable, we typically implement it with obfuscation rules that meet compliance requirements that meet current data privacy standards, like GDPR or the California Consumer Protection Act.

Traceable never actually sees any real data, and that provides a certain amount of comfort for organizations that are trying to maintain strict data privacy. An alternative for highly regulated customers that say 'Wow, APIs handle critical information. There is competitive operational intel that can be derived from all the things that APIs do from a tracing and monitoring standpoint. I really wouldn't like that sitting in your cloud solution. I'd actually like it if you just gave me the software and I installed it.' So we provide both an on-prem and a SaaS solution. And once again, either way, we never see any raw data, we take the whole issue of data confidentiality to heart and that's the way we've designed the application.

HOW DO YOU ADDRESS THIRD PARTY RISK?

Most supply chain attacks are executed through APIs. Being an API security organization, we have the capability to monitor our own systems, monitor our own transactions with our own tool set.

We're able to see the activity that's going on, where there is connection between endpoints, connection between applications, in a supply chain between suppliers, between third party providers, and see exactly what's being done nefariously.

We basically were built to be part of the solution set that reduces supply chain risk and shrinks the attack surface. Traceable is fortunate that we're in the business of securing the major pathways and the connection points that are currently used for supply chain attacks, so it's something that we are just sensitive to on a day-to-day basis because we are monitoring for any kind of bad outcome across billions of calls every month.

HOW DOES TRACEABLE APPROACH THEIR SPEND ON INTERNAL SECURITY?

I would say that if we were comparing to other companies that are in our stage of growth, of a round B funded startup, I would say that our security spend is probably slightly above average for security solutions providers in our space.

And the reason for that is because, like I said, so many aspects of what we do are tied to key security concepts. Zero Trust is a great example, as well as the supply chain. And since we're a security solution that helps mitigate risks in those spaces, we're probably applying more dollars towards product security and operational security than most of our peers.

But again, we're shoemakers, and everybody wants our shoes, but we also wear our own shoes because we're just in the midst of a transactional layer of security that requires us to be a little bit more rigid around our own security practices.

HOW DO YOU DETERMINE WHAT SECURITY TO PERFORM IN HOUSE VS. OUTSOURCE?

That's tough for all startups. The reality is that I'd love to say that we could go and outsource the assessments necessary, or other certifications such as NIST or ISO certifications, and FedRAMP certifications. But there are investment dollars that are associated with that, and the challenge is that most companies in our size and class don't have the available resources or experience.

And yet when we go to have conversations with external sources to do that work, it's not inexpensive. It creates a really challenging problem for us, in that we have to choose which security assessment credentials are most important to your buying customer.

They would love for us to have all the certifications, but I think the buying population also recognizes the problem in this space, that these certifications require investment dollars that need to be leveraged for other aspects of the company growth, until we reach a certain phase where, being able to pay for them makes sense with in house or outsourced resources depending on the skill and expertise required..

HOW DO YOU APPROACH CUSTOMER COMMUNICATION?

Many of our security interactions and security communication tend to be associated with making sure that we're on the right security footing to be a third party solution provider to enterprise companies. We're a relatively new start up, having come out of stealth less than two years ago for the most part. We're SOC2 certified and we have to go through really rigorous security assessments.

We also have an Advisory Board where we take inputs from our customers around security topics, that we are either addressing them as it relates to operational security, or having conversations about them in relation to product security in future features and functionality requirements for the roadmap.

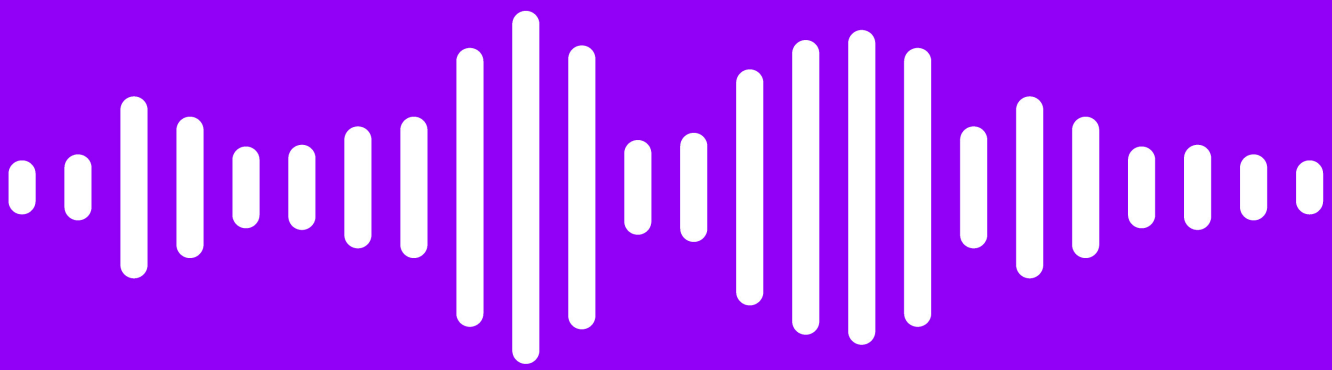
In addition we have a customer success team that is always interacting with customers to improve the nature of all our interactions with them, including communication and improve product performance and capabilities.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

FEATS OF STRENGTH



MAY 2023