ABHAY SALPEKAR

VP, Cloud & Platform Engineering

ANOMALI

ANOMALI

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 350+

REVENUE: Private Company

K LOGIX PARTNER PROFILES

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.