MIKE BRITTON

CISO
ABNORMAL SECURITY

Abnormal

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 500+

REVENUE: Private Company

K LOGIX PARTNER PROFILES

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.