Shining a Light on Modern Cyber Threats: Exabeam

"Incorporated in 2013, Exabeam is a leader in the User Behavior Analytics market, one of the fastest-growing segments within computer security."

"We are a leading provider of user be–havior intelligence."

Nir Polak, CEO and Founder

Meet the CEO
Nir Polak, CEO and Founder

Nir has 13 years experience in information security, including executive experience setting company strategy, driving execution, building new products and bringing them to market. While at Imperva, Nir set the company product strategy and launched and managed the worldwide services organization. He also held engineering positions at Adjungo Networks (acquired by Flash Networks) and Shopping.com (acquired by eBay). Nir has a Bachelor of Arts degree in computer sciences from The Interdisciplinary Center in Israel.

Thousands of security events are reported every day, all fighting for attention. Security analysts are entering the workforce with less and less real world experience. There's no longer a place for complex tools that make you click-and-pivot through an ocean of data asking questions of your data one at a time. Exabeam is a user behavior analytics solution that leverages existing log data to quickly detect advanced attacks and accelerate incident response. Exabeam's Stateful User Tracking™ automates the work of security analysts by connecting individual security events and behavior anomalies into a complete attack chain. This dramatically reduces time to respond and uncovers attack impacts that would otherwise go unseen.

Exabeam was founded with the goal of using a novel combination of machine learning and security research to find and respond to increasing cybercrime. The company added its first customer in December 2014 and since then has grown quickly, with a total of more than 1.5 Million employee accounts currently being monitored for compromised credentials or insider threats.

User Behavior Analytics (UBA) is a fast-growing market and is drawing in vendors who are trying to *"hitch their wagons"* to faster growth. There is quite a bit of noise and confusion in the market regarding UBA. Cutting through that noise to help customers understand how different products fit their needs is a challenge. Exabeam positions itself as the security intelligence solution that provides the fastest time to value (typically within a day of installation) while also improving productivity of security operations, on a machine learning platform that customers can extend

as they wish. Automating security operations is especially important since every large organization is struggling to hire the required number of security experts.

Most of the company's competitors require a significant amount of collection technology to be installed, either an agent on every user's PC, or else network taps throughout the network. This means that it can take many months to implement. In contrast, Exabeam works initially on existing log data and can be up and running and showing business value by the next morning. Network and other data are usually added in later project phases, after the customer has proven ROI.

Exabeam was named a *"Cool Vendor in Security Intelligence"* by the analyst firm Gartner in 2015.

Understanding User Behavior with Exabeam

The company's product analyzes the millions of log records that every enterprise already collects and then uses those to create a baseline of normal behavior for every employee and contractor on the network. The product then compares ongoing activity, for every user, to his or her normal baseline, to determine if the employee/contractor is behaving in unusual and risky ways. This is often a signal of stolen account credentials (the common method of attack in most of the large breaches we read about), and allows customers to detect, stop, and clean up attacks before they cause data loss. It is also a signal of potential data loss from malicious insiders.

Clientele

Exabeam's clients are typically in the sectors that hold sensitive data and are targets for hackers: financial services, retail, healthcare, and manufacturing. The company has some of the largest financial services, retail, and healthcare providers in the US as clients. ADP (largest payroll processor) and Safeway (one of the largest grocery chains) are publicly-named clients.

Client Speaks

"Before Exabeam, our analysts took a lot of time to dig in and find security logs present in divergent locations and put a story together. With Exabeam, we actually get a story. Hulu is using Exabeam today, to not only detect suspicious user behavior but also to identify where our service accounts are being used, who had controlled them and what they were actually doing. After installing Exabeam, we have a much better control and insight in to the activity that our users and service accounts have across the organization. We have significantly reduced the amount of time taken for analysts to investigate incidents and show the management very explicitly what is happening on a day-to-day basis. What makes Exabeam different is that it actually uses analytics and behavior to identify problems. It is very easy to deploy and provides you with immediate results."
- Chris Hymes, Director of Information Security, Hulu

Geographies

Exabeam operates globally with operations in North America, EMEA, and Asia-Pacific.

Office Locations

The company is headquartered in San Mateo, CA, USA. It opened its UK and Germany offices in 2015. In January 2016; it opened offices in Singapore, Hong Kong, Japan, and Australia/New Zealand.

Present and Future Focus Areas

Currently, Exabeam is focused on security intelligence related to Security Intelligence and Event Management (SIEM). Its future focus area will be to continue adding new underlying data management systems as well as new applications for its unique data model.

> *We unlock the potential of SIEM and log management repositories helping you change the way cyber attacks are detected and greatly sim–plify security operations.*