exabeam

Case Study

Helping Meissner Make Sense of Masses of Security Data

Industry
Manufacturing

Exabeam Products
SaaS Cloud Archive | SaaS Cloud Essential SIEM | SaaS Essential Cloud Connectors | SaaS Cloud Essential Entity Analytics

Founded in 1984 and headquartered in Camarillo, CA.

Meissner serves the pharmaceutical, biotechnology, microelectronics, ultrapure chemicals, food and beverage and allied industries.

The problem

Operating in the research and manufacturing industry creates a host of endpoints both physical and digital. Add to that the fact that Meissner manufactures equipment essential for the biomedical industry in a climate where things are moving at break-neck speed; and you end up with volumes of endpoints generating network and physical access logs. For the team at Meissner, they didn't have a solution that could efficiently aggregate the date their systems were generating. Additionally, storing this data was a challenge.

MEISSNER FILTRATION PRODUCTS

> We're generating event logs across hundreds of systems and that's getting sent to a central location, and with Exabeam, it was so easy just to tie that central location and send all that data to Exabeam. So that was one of our key requirements. And it was definitely easier with Exabeam than a lot of the other solutions we tried.

Zane Gittins
IT Security Specialist
Meissner

"A lot of our endpoints were generating logs, but we needed a way to translate that into security data and ultimately store and correlate what we were collecting," says Zane Gittins, IT Security Specialist at Meissner.

Finding the right solution

The key concern straight out of the gate was to find a solution that lets the team quickly index and search their data, so a solution that was based on an elastic stack was something they knew would tick that box. For a team punching above its weight, efficiency and accuracy was a must and so a cloud solution would also be better. Ease of integration was another requirement, and the ability to integrate their existing logging stack.

"We did look at ELK originally, even setting it up on-prem, but Exabeam just ended up being so much better because we are such a small team. Another one of our requirements was SaaS, because we just didn't have the bandwidth to do it on-prem, our team would be managing the ELK stack instead of actually searching for threats and writing rules," says Gittins.

Why Exabeam?

Having identified the need for efficiency, visibility and accuracy, the Meissner team ultimately chose Exabeam above the competition. Exabeam's ability to automate labor-intensive activities meant that Zane's team could get down to more specialized tasks.

"We're generating event logs across hundreds of systems and that's getting sent to a central location, and with Exabeam, it was so easy just to tie that central location and send all that data to Exabeam. So that was one of our key requirements. And it was definitely easier with Exabeam than a lot of the other solutions we tried," says Gittins.

Seeing security data in context

Straight away the Meissner team liked how they'd be able to handle alerts using Exabeam.

"In traditional SIEMs you'd write rules, each rule may trigger and then an analyst is expected to triage each of those rules. But in Exabeam, you're just adding that score for a specific user or asset to a timeline, and then you're having your analysts triage timelines," says Gittins.

This helps their team write better rules, because they can base them on things that aren't expressly always malicious on their own, but when looked at in context they could well be. At the same time, it saves a lot of time for analysts who don't have to triage tens of thousands of alerts, they're just looking at timelines of users and assets.

"We had no idea you could integrate the physical access logs into Exabeam, and that's something we hadn't even really considered correlating with our other security data. So that was huge for us, because there's a lot of really great alerts based around those physical access logs like someone physically badging in, but then the same day, they also start a VPN connection to the corporate network," says Gittins.

Key benefits

- Improved efficiency
- Cost savings
- Improved visibility

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Management platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm. For more information, visit **www.exabeam.com**.

To learn more about how Exabeam can help you visit exabeam.com today.

exabeam