CASE STUDY

BAKER DONELSON ADVANCES THE MATURITY OF THEIR CYBERSECURITY PROGRAM WITH EXABEAM

ACHIEVING GREATER VISIBILITY INTO END POINTS, CLOUD, AND IDENTITY AND ACCESS MANAGEMENT.

Baker Donelson is an Am Law 100 law firm, with more than 20 domestic offices and 130 years of experience. They employ more than 1400 people, 700 of which are attorneys. The firm represents more than half of the Fortune 100 and a quarter of the Fortune 1000, including large financial institutions, governments and healthcare organizations

BUSINESS CHALLENGE

While law firms aren't always very big, the amount of data they protect is expansive and almost always sensitive, and Baker Donelson needs to safeguard that data, whether it's financial, healthcare, intellectual property or any other client data.

As things stand, they have multiple data centers, 21 offices, plus the cloud, and the nature of the firm's business means there are lots of traveling end points, connecting at hotels and coffee shops across different networks, creating a lot of data relative to their market cap and company size.

> "Exabeam gives us visibility into our end points, cloud, and identity and access management. If you're able to get in there and correlate all that stuff, get that telemetry, you get a pretty good overview of what's going on in your environment."
>
> CARL SCAFFIDI, CHIEF INFORMATION SECURITY OFFICER, BAKER DONELSON

Security framework certifications define requirements for log collection, retention, security monitoring and alerting. Additionally, while law firms aren't heavily regulated, the industries their customers are in often are. So, the firm needs a modern security solution that logs, but also records and illustrates a security incident workflow.

"We have multiple domain controllers, firewalls, IDS…every office is essentially a mini data center, so security data is very distributed. But it all needs to be centralized and monitored." Carl Scaffidi, Chief Information Security Officer, Baker Donelson.

VENDOR SELECTION AND PROOF OF CONCEPT

As they started building out their security solutions, Baker Donelson was faced with a growing number of programs that needed monitoring, data that needed centralizing and parsing and faced growing compliance requirements.

“We quickly realized that we were not going to be able to rely on a traditional SIEM.”

The firm had a small security team with a tight budget and a lot of data to keep tabs on. “We needed something affordable, something that is financially scalable.” At the same time, Baker Donelson knew that they needed confidence in what their systems showed them, without being able to build out a robust security team. “We needed to keep things high fidelity. We couldn’t waste time chasing down false positives.”

Ultimately, the team needed a solution that could help them progress to a more mature security posture, by incorporating activities like threat hunting, to take a much closer look at security events when the need arises.

“Where we are now, operating in a state of assumed compromise, we need to be able to dive a little deeper when it seems necessary.”

Needing to think beyond the Gartner Magic Quadrant-type SIEM solutions on account of their cost and fit, Baker Donelson tested multiple open source SIEM platforms, but in terms of depth, functionality and support, they didn’t work out. In addition, the open source solutions were labor intensive and functionality limited.

“We didn’t have a lot of time to care and feed and learn and build that stuff on our own and limited support from those open source vendors made it really difficult to try the roll-your-own SIEM platform.”

USE CASES

With such a dispersed team, and employees who might not always have security top of mind, it’s important that the Baker Donelson team has visibility and the agility to act quickly when certain actions put their systems at risk.

With the Exabeam proof of concept, instead of going down and chasing every email alert they received from multiple tools, the team was able to look into Exabeam Advanced Analytics and see what was happening with consolidated information and alerting.

“We were able to go clean it up and didn’t really have to worry about it, so that really made things efficient, made things a lot quicker for us. We weren’t chasing our tails, we weren’t overly worried about what are we missing, and it seemed to really prove some value for us.”

PARTNERING WITH EXABEAM TO DRIVE EFFICIENCY

Exabeam also helped Baker Donelson work through their various use cases and identify opportunities for efficiency, particularly around improving anomaly identification and investigation time. They were also able to keep costs down with Exabeam’s more predictable, per user pricing model, versus the legacy SIEM vendor by-the-byte pricing models that increase cost as data inputs grow.

“With legacy SIEM technology, you often need large teams to manage the number of alerts you’re bombarded with at any given point. We needed something cohesive, that could be used by a small amount of people. So, the old SIEMs -- throw all the data into it, get beat to death with a bunch of alerts -- weren’t going to work for us.”

exabeam

Key Benefits

- Faster investigation and anomaly detection
- Reducing false positives
- Greater visibility

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.