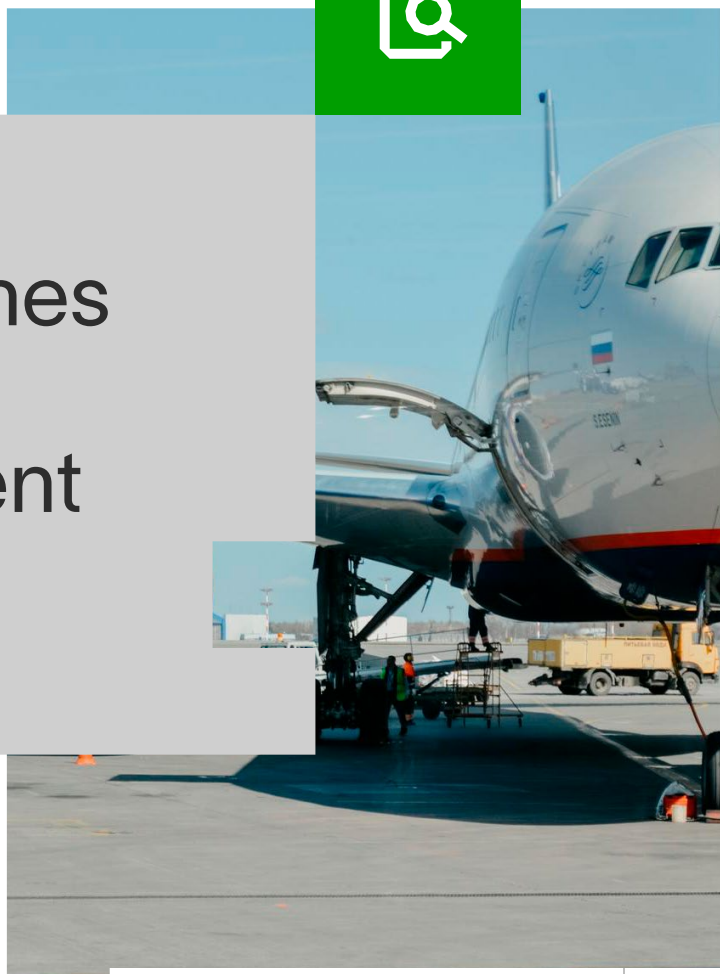
exabeam

Case Study

Helping United Airlines Keep Track of a Dynamic Environment for Insider Threat Management



Industry
Aviation

Exabeam Products
Advanced Analytics | Threat Hunter | Incident Responder | Cloud Connectors | Entity Analytics

Securing an organization that relies heavily on creative, iterative processes and the subsequent volumes of touchpoints.

Headquartered at Willis Tower, Chicago, United Airlines is the fourth largest airline in the world and third largest in the United States. The airline operates a large fleet both inside the US and across all six continents and is a founding member of Star Alliance, the world's largest airline alliance.

UNITED

> Understanding what's going on inside our environment, from the perspective of data movement and data loss gives us a holistic view to make it easier to identify abnormal events.

Deneen Defiore
VP & Chief Information Security Officer
United Airlines

The Challenge

Most major airlines are subject to the same cybersecurity concerns as businesses operating in other industries, but there are unique elements that set them apart. While data privacy is always a concern, an airline's intellectual property extends to things like pricing strategies and route planning, which can be key competitive advantages.

To that end, the team at United has to be able to cast a pretty wide net, to protect internal data across their entire landscape, and not just monitor what's happening externally.

"What we're looking at is a different set of risks around confidential information, because the strategy around how you plan your routes, networks and pricing, that's how you differentiate yourself," said Deneen DeFiore, VP & Chief Information Security Officer, United Airlines.

Why Exabeam

The unique needs within the organization meant that Deneen's team had to be able to keep an eye on an environment that includes activities around social media messaging for certain competitive announcements, financial planning from a customer point of view and generally, a lot of activities that take place outside of an operations or engineering environment.

Users are reviewing documents in a dispersed environment and there isn't always a defined process for how this happens, so the team at United needed a tool that could roll with this creative, iterative process.

"We were able to learn how people are working because it's not always a defined, structured process," says Deneen, adding that whatever security platform they landed on would need to be able to flex to their creative needs AND their needs around data protection loss and insider threat management.

In Exabeam, Deneen's team has a tool that's purposebuilt for insider threat management, flexes with their needs, is easily implemented and allows them to add additional functionality and rules to incorporate data sources from across the organization.

High Value Insights with Fast and Reliable Outcomes

Exabeam was brought in as the initial solution for insider threat management, and Deneen's team has seen an improvement in the speed with which they are able to carry out investigations. Additionally, the team is now able to automate more processes to free up team members to tackle different tasks.

Straight off the bat, the team at United was able to proactively identify data loss use cases, but also expand on the kinds of activities that might contribute to data loss.

"We have thousands of employees that we need to be able to reach and communicate business decisions and key policy changes to, that have to be disseminated very widely," says Deneen.

Deneen's team had to keep an eye on information being shared widely throughout United for dissemination, to make sure that it stays within the relevant areas of authority, for instance HR documentation and processes. With Exabeam the team was able to incorporate more touchpoints than before, and ensure that information sprawl was being monitored.

Tackling Insider Threats with a 360 Degree View

Insider threats come in different forms, both wittingly and unwittingly. In an organization the size of United Airlines, that's been operating for as long as it has, you're bound to end up with employees who've spent decades in their job. Throughout anyone's tenure, you end up with personal emails, documentation saved to several devices, things you might not consider as a possible insider threat, but that could contain sensitive information.

Using Exabeam, the team at United has been able to gain even greater visibility across a sprawling environment, giving them insights into what assets people are gaining access to both physically and online to protect physical property as well as digital assets and take stock of everything at potential risk of insider threats, whatever those may be.

"Understanding what's going on inside our environment, from the perspective of data movement and data loss gives us a holistic view of behavior across our environment to make it easier to identify abnormal behavior," says DeFiore.

Key Benefits

- Easily scalable
- Improved visibility across diverse environments
- Better user behavior baseline analysis
- Improved speed and efficiency

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit www.exabeam.com.

exabeam

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