observeIT
a division of Proofpoint

CUSTOMER STORY

Grounding Insider Threats with ObservelT

Aircastle Recruits ObservelT to Safeguard Sensitive Information While Protecting Privacy

AIRCASTLE

THE CHALLENGE

- Safeguard key financial information (earnings, details of M&A, etc.)
- Meet SOX compliance mandates by maintaining detailed records
- Uphold privacy regulations and culture of respect for employees and contractors

THE SOLUTION

- ObservelT Insider Threat Management Platform

THE RESULTS

- Gained full visibility into user activity across
- Received rapid alerts on suspicious activity
- Developed the capacity to conduct investigations in a matter of minutes, not days
- Increased instances of employees reporting out-of-policy behavior to curb insider threats, with the ability to rapidly investigate claims

The Company

Aircastle is a publicly traded company that acquires, leases and sells commercial jet aircraft to airlines throughout the world. Aircastle has built a highly successful organization with a lean and dedicated team of employees.

As of 2019, Aircastle owns and manages 277 aircraft, leased to 87 lessees located in 48 countries. Aircastle has earned its reputation as a company with a unique and necessary position in the commercial aircraft leasing industry.

The Challenge

As a public company, Aircastle must carefully safeguard key financial information—everything from earnings to details of mergers and acquisitions—to ensure it is not leaked prior to regulated disclosure dates. Leaks could endanger the business, exposing them to financial and legal headwinds.

Additionally, Aircastle is beholden to the Sarbanes-Oxley Act, another burden of being a publicly held company. This mandates the company to continually maintain detailed financial and IT records for regulatory bodies. Moreover, as a company with offices located internationally, they must uphold certain privacy regulations. Even outside these laws, Aircastle values their culture of privacy and respect for their employees and contractors.

The Aircastle team had been using a traditional endpoint DLP for data loss prevention, but had run into significant issues with time-consuming set-up, constant monitoring requirements, and system crashes. They tried two different DLP solutions, but both were overly file-focused and required constant hands-on maintenance, straining their small IT team.

"I have a small IT team of six people," says Bill Duenges, senior vice president of information technology, Aircastle. "So it's very difficult to have a product you have to constantly babysit like a DLP."

On top of that, users were far from thrilled with the DLP's effect on their endpoints. "As soon as we started using a DLP, all our users knew it was there, because of the instant slowdown." Some figured out how to bypass the DLPs, and even when they didn't, the tools created mountains of work for Duenges' team while slowing down investigations.

The Solution

After an extensive search process, Duenges and his team conducted a proof of concept with ObserveIT. They were pleased with the results and settled on ObserveIT as a means to help Aircastle gain more context into user activity within the organization. This would let them receive immediate alerts if, for example, an employee attempted to exfiltrate confidential financial information via a cloud storage service.

> "Insider threat investigations that used to take days now take 15-20 minutes on average. I receive good, solid alerts. The information is relevant and doesn't waste my time with searching."
>
> **Bill Duenges,** Senior Vice President of Information Technology, Aircastle

Initially, Duenges admits, "My team saw ObserveIT as a 'nice-to-have' product. We thought it was just something we'd layer into our existing security stack." However, two years into their engagement with ObserveIT, Duenges now describes the platform as a "must-have" that will be part of their security stack "forever."

ObserveIT enables Aircastle's small IT and security team to receive rapid alerts on suspicious user activity and conduct investigations in a matter of minutes, rather than days.

They are now aware of any insider activity impacting sensitive financial data and other valuable business files in near real time. Additionally, team members sometimes report out-of-policy behavior they witness, and now Duenges' team has a tool that can help him verify the claims.

"With a small IT team, we do not have time to constantly babysit a product like DLP. With ObserveIT, there is no babysitting. I receive good, solid alerts. The information is relevant and doesn't waste my time with searching." – Bill Duenges, SVP of Information Technology, Aircastle

"The first tool I go to for investigations is ObserveIT," says Duenges. "We get alerts from other tools, but ultimately use ObserveIT for full context around various incidents. With ObserveIT's easy-to-use, quick-to-set-up and lightweight solution, my team is more productive, users aren't impacted and our valuable assets are better protected."

Finally, ObserveIT's fine-grained privacy settings enable the team to ensure that only the appropriate team members have access, and only after clearing access with their chief legal officer. This ensures user privacy is protected without sacrificing security.

"On top of all that, ObserveIT helps us meet SOX compliance," says Duenges. "So that's one more thing off my plate."

The Results

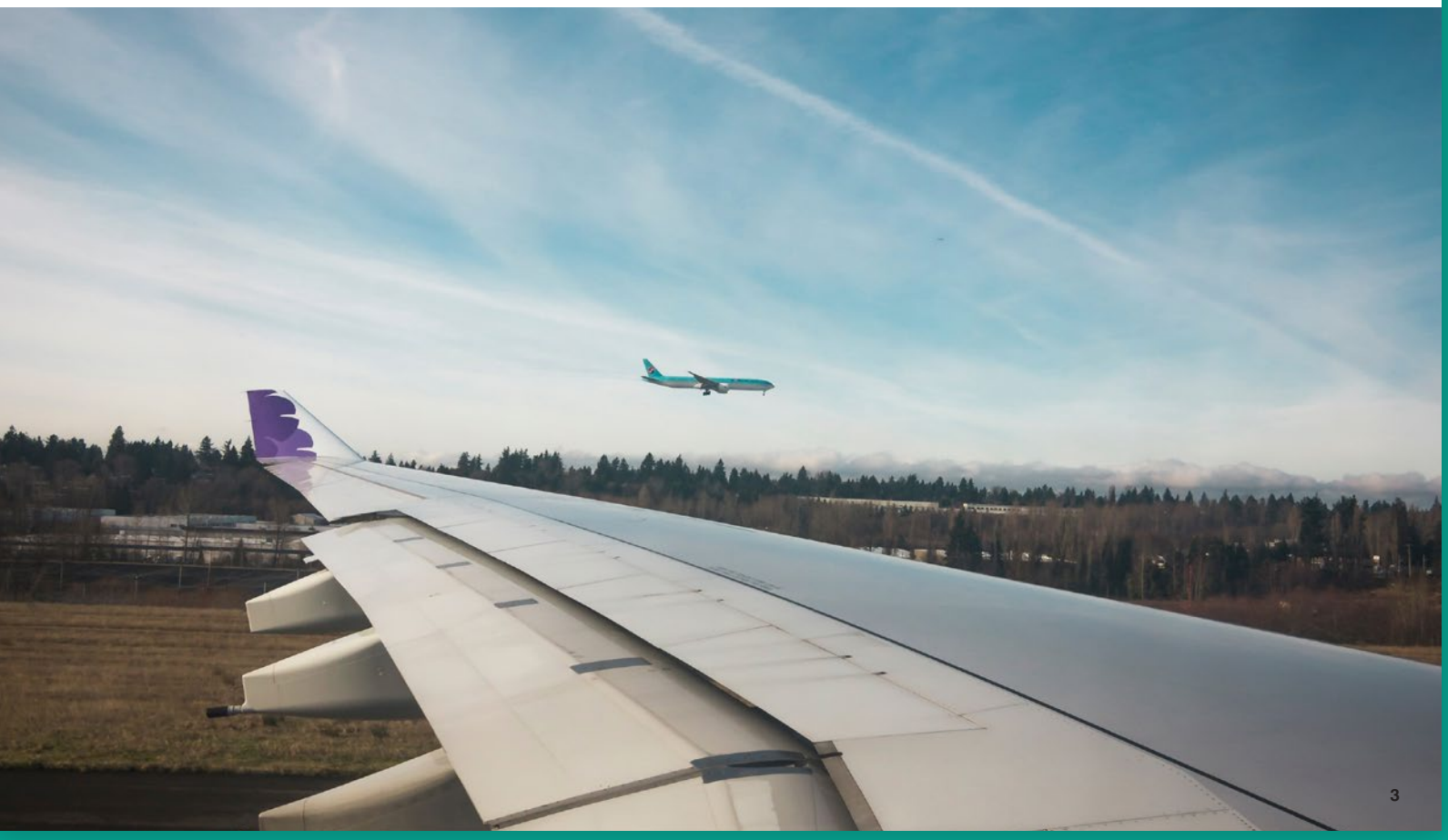
The Aircastle team now has full visibility into user activity across endpoints. When an alert fires, they are able to rapidly determine what happened and understand what took place before and after the incident to place it in context.

When actual insider-caused data exfiltration incidents take place, the team can rapidly investigate and respond to them with complete context around user and data activity from ObserveIT.

ObserveIT enables the Aircastle security team to clearly understand not just what happened but *why*. In several cases, this has enabled them to exonerate employees who were acting in good faith but may have exceeded the boundaries of security policy.

As a side benefit, Aircastle has even improved their NIST benchmark security score dramatically through demonstration of the features that ObserveIT has added to their security stack.

"Insider threat investigations that used to take days now take 15-20 minutes on average." – Bill Duenges, SVP of Information Technology, Aircastle



LEARN MORE

For more information, visit **observeit.com**.

ABOUT OBSERVEIT

ObserveIT, a division of Proofpoint, is the leading Insider Threat Management (ITM) solution with more than 1200 customers globally. ObserveIT helps organizations protect against data loss, malicious acts, and brand damage involving insiders acting maliciously, negligently, or unknowingly.

The ObserveIT platform correlates activity and data movement, empowering security teams to identify user risk, detect to insider-led data breaches, and accelerate security incident response. Leveraging a powerful contextual intelligence engine and a library of over 400 threat templates drawn from customers and leading cybersecurity frameworks, ObserveIT delivers rapid time to value and proven capability to streamline insider threat programs.

observe IT
a division of Proofpoint

0000-0000-00-00 04/20