proofpoint.

CUSTOMER STORY

Grounding Insider Threats with Proofpoint Insider Threat Management (ITM)

Aircastle Uses ITM to Safeguard Sensitive Information While Protecting Privacy

AIRCASTLE

The Challenge

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

The Solution

- Proofpoint Insider Threat Management

The Results

- Gained full visibility into user activity
- 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 investigate claims rapidly

The Company

Aircastle is a publicly traded company that acquires, leases and sells commercial jet aircraft to airlines throughout the world. It 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. It 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. That includes 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 its culture of privacy and respect for its employees and contractors.

The Aircastle team had been using a traditional endpoint DLP for data loss prevention. But they 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 they required constant hands-on maintenance, straining its small IT team.

"I have a small IT team of six people," said 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 its 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 ITM. They were pleased with the results and settled on ITM 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.

Initially, Duenges admitted, "My team saw ITM 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 ITM, Duenges now describes the platform as a "must-have" that will be part of their security stack "forever."

> "With a small IT team, we do not have time to constantly babysit a product like DLP. With ITM, 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

ITM 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.

"The first tool I go to for investigations is ITM," says Duenges. "We get alerts from other tools, but ultimately use ITM for full context around various incidents. With ITM'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, ITM'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 that user privacy is protected without sacrificing security.

"On top of all that, ITM 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 they can now 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 ITM.

ITM 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 dramatically improved its NIST benchmark security score by demonstrating the features that ITM has added to its 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 www.proofpoint.com/us/products/information-protection/insider-threat-management.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.