proofpoint.

導入事例

Proofpoint ITM (Insider Threat Management) 内部脅威の離陸を阻む

Aircastle は機密情報とプライバシーを Proofpoint ITM で同時に保護

AIRCASTLE

課題

- 重要な財務情報（収益、M&A 取引内容など）の安全性を確保すること
- SOX 法コンプライアンスに対応した詳細な記録を保持すること
- プライバシー規制や従業員、請負業者を尊重する文化を促進すること

ソリューション

- Proofpoint ITM (Insider Threat Management)

結果

- ユーザーアクティビティを完全に可視化
- 不審なアクティビティは即時のアラートで把握
- 数日ではなく数分で調査を実行する能力を確立
- 調査が迅速化され、内部脅威の抑止に向けたユーザーによるポリシー外の振る舞いの報告が増加

会社概要

Aircastle は、商用ジェット機を世界中の航空会社にリース販売する上場企業で、少数精鋭組織として大きな成功を収めてきました。

2019年時点で、277台の航空機を所有、管理し、世界48か国にある87の航空会社にリースしています。商用航空機リース業界において、なくてはならない独自の立場を築き、高い評価を得ています。

課題

Aircastle は、上場企業として、重要な財務情報を十分な注意の上、安全に保持する義務を負っています。財務情報には、収益情報から企業買収にかかわる詳細情報までのすべてが含まれ、こうした情報は開示日まで安全に保護する必要があります。万が一リークされれば、事業を危険に陥れ、財務上、法律上の問題となりかねません。

また、Aircastle は **サーベンス オクスリー法（SOX 法）**の適用も受けます。これも上場企業に課される義務で、詳細な財務記録や IT 記録を継続的に保持することが求められます。さらに、海外拠点を持つ企業として、一定のプライバシー規制への準拠も必要です。実際、Aircastle では、法律の規定にかかわらず、プライバシーを保護し、従業員や請負業者を尊重する文化を重んじています。

これまで Aircastle では、データ漏えい対策として従来型のエンドポイント DLP を使用していました。しかし設定に時間がかかる、常に監視作業が必要である、またシステムがクラッシュする、などといった問題がありました。2種類の DLP ソリューションを試しましたが、いずれもファイル管理に過度に重点がおかれ、頻繁なメンテナンス作業も発生したことから、人数の限られた IT チームには負担がかかっていました。

Aircastle の IT 担当シニアバイスプレジデントの Bill Duenges 氏は次のように述べています。「我が社の IT チームは6人の小編成です。DLP のような常時の対応が必要となる製品を使うことは、容易ではありません」

その上、ユーザーによる DLP への反応も好ましいものではなかったと言います。「DLP を導入してすぐに、エンドポイントを使う者は皆、そのソフトウェアがインストールされていることを意識せざるを得ませんでした。導入により動作が確実に遅くなったのです」DLP を回避しようとするユーザーすら出てきました。こうして、DLP は Duenges 氏のチームにやるべきことを山ほど生み出し、調査にも時間がかかりました。

ソリューション

Duenges 氏は慎重に検討を重ね、Proofpoint ITM の概念実証を実施しました。結果に満足が得られたことから、組織内のユーザーアクティビティに関しより多くのコンテキスト情報を得るために Proofpoint ITM の採用を決定しました。Proofpoint ITM により、仮にユーザーがクラウドストレージサービスを経由して財務上の秘密情報を持ち出そうとすると、直ちにアラートが出されます。

Duenges 氏は次のように認めています。当初、「私たちは Proofpoint ITM を『Nice-to-have(あった方がいい)』製品だと考えていました。既存のセキュリティに新たな層を加えるようなものだと捉えていたのです」しかし、Proofpoint ITM を2年ほど使った現在、Duenges 氏は、このプラットフォームについて、同社のセキュリティ対策に「Must-have forever(永久的になくてはならない)」プラットフォームであると考えています。

「小さなチームなので、DLP のような製品に手間をかけている余裕はありません。Proofpoint ITM には、こうした手間がかかりません。受け取るのは、質のよい、確かなアラートです。関連性のある情報が得られるので、検索に時間をとられることもありません」

Bill Duenges 氏 Aircastle IT 担当シニアバイスプレジデント

Proofpoint ITM があれば、人数の少ない Aircastle の IT セキュリティチームであっても、不審なユーザーアクティビティのアラートをすぐに受け取り、数日ではなく、わずか数分で調査を実施することが可能です。

財務上の秘密情報や価値のあるビジネスファイルが関与する内部関係者のアクティビティは、ほぼリアルタイムで把握できます。さらに、ユーザーが見つけたポリシー外の振る舞いについても報告が入るようになりました。こうした報告を検証するためのツールも備わっています。

Duenges 氏は語っています。「調査を始めるときにまず確認するのは Proofpoint ITM です。別のツールからアラートが出る場合でも、インシデントにかかわる完全なコンテキスト情報は Proofpoint ITM を使って確認します。Proofpoint ITM は使いやすく、設定が容易で、軽量なソリューションです。チームは生産的になり、ユーザーは影響を受けることもなく、我が社の価値ある資産はより強力に保護されています」。

さらに、Proofpoint ITM ではきめの細かいプライバシー設定が可能であることから、必要なメンバーのみが、最高法務責任者による許可を得た場合にのみアクセスできる仕組みも実現しました。つまり、セキュリティ対策を理由としてユーザープライバシーがおろそかになることもありません。

「Proofpoint ITM は SOX 法コンプライアンスにも役立ちます」と Duenges 氏は付け加えます。「私のやるべき仕事がまたひとつ楽になりました」

結果

Aircastle の IT チームは、各エンドポイントで行われるユーザーアクティビティについて、完全な可視性を手に入れました。アラートが出されれば、何か起きたのかをすぐに確認することができます。そして、インシデントの前と後に何が行われたのかをコンテキストに照らして把握することができます。

「これまで内部脅威の調査には数日かかっていましたが、今では平均して 15-20 分程度です」

Bill Duenges 氏 Aircastle IT
担当シニアバイスプレジデント

実際に内部関係者がデータを持ち出した場合は、ユーザーやデータアクティビティに関する完全なコンテキスト情報を Proofpoint ITM から確認して、すぐに調査、対応します。

Proofpoint ITM を使えば、何が起きたのかだけではなく、なぜ起きたのかを理解することができます。一部のユーザーは、厳しいセキュリティポリシーの境界を善意で越えてしまったのみであることもわかりました。

Proofpoint ITM の機能を含むセキュリティ対策を証明することで、米国国立標準技術研究所（NIST）ベンチマーク セキュリティスコアが大幅に改善されるという思わぬメリットもありました。

詳細

詳細は www.proofpoint.com/jp/products/information-protection/insider-threat-management をご確認ください。