Box利用のセキュリティ強化

Forcepoint

Brochure

データセキュリティの課題

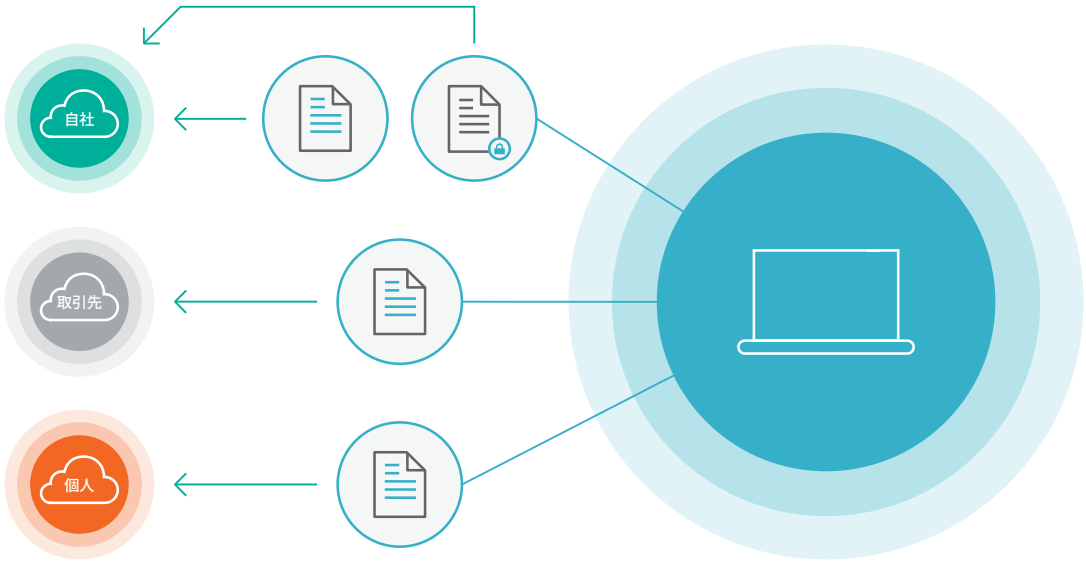
データセキュリティという用語は、例えばデータベース内の機密情報が持ち出された場合に備えたデータベースの暗号化であったり、端末のディスク暗号化であったりを想像されるかもしれません。ただ働き方の変革やクラウドソリューションの利用の促進により、オンプレミスで運用されていたデータベースもクラウドサービスにおいてデータを登録し利用されていたり、端末も社用端末から個人端末の利用を許可されたりすることにより、これまで対策とされていたオンプレミス環境でのデータベースやディスクそのものの暗号化も難しい状況になっています。保護対象となるデータについても、これまではオンプレミス環境のファイルサーバやデータベースに保存されていたものが、様々な場所に保存され利用されている状況となっています。この変革に対応するためにゼロ・トラストに代表されるような新たなセキュリティアーキテクチャや、またEDRやXDR等のセキュリティソリューションが注目を集めています。

ではなぜ今データセキュリティに再注目する必要があるのでしょうか。例えばゼロ・トラストは情報資産やアプリケーションに対するアクセスは全て信頼できないことを前提として検証することを求めるセキュリティのアプローチですが、保護の中核をなすものはデータであり、重要なデータを適切に保護できない限りケアレスミスによるデータの漏えいや、従業員の生産性低下を招きかねません。また多くのセキュリティソリューションは外部攻撃による痕跡に注目し、より効果的にエンドポイントおよびシステム全体を連携・保護することが可能ですが、攻撃の最終的な目的となりえるデータに対する保護としては不十分です。

Forcepointでは、セキュリティを考える上で、「人」と「データ」に着目し、セキュリティソリューションを提供しています。「人」の振る舞いがどのようなリスクとなりえるのか、また企業のリスクとなりえる「データ」をどう保護できるか、その「人」と「データ」を紐づけて分析することで、より効果的なデータセキュリティを提供することを目指しています。

今回は、データセキュリティの課題として、よく利用されているBoxアプリケーションの利用について、Forcepointのソリューションを利用することで、どのように企業のデータ保護に寄与できるかについて紹介します。

Box利用に対するセキュリティ強化



Boxアプリケーションの利用はその利便性のため、多くの企業で採用されています。例えば、Boxアプリケーションの利用方法としては、用途等に応じ以下のように分類されるかもしれません。

→ 社内ストレージとして、データの管理・チーム内共有

→ 社外ユーザに対するデータ公開、データ共有

リンク共有
ユーザを明示しての公開
コラボレーション機能

メールで添付ファイルとして取引先などの社外ユーザに送付するより、共有用リンクを送付するだけで、必要に応じてデータを削除する等、データ管理が容易であるというメリットがあります。またBox Editを利用しての編集や、コラボレーション機能を利用しての外部との共有という利用方法もあります。

ただ情報連携が容易な反面、例えば社内の情報セキュリティ担当者は、以下のような情報漏えいリスクについて考える必要があるかもしれません。

→ 自社の従業員が他社ドメインに対して不用意にデータをアップロードしていないか。もしくは個人（プライベート）用のBoxアカウントへアクセスしデータをアップロードしていないか。

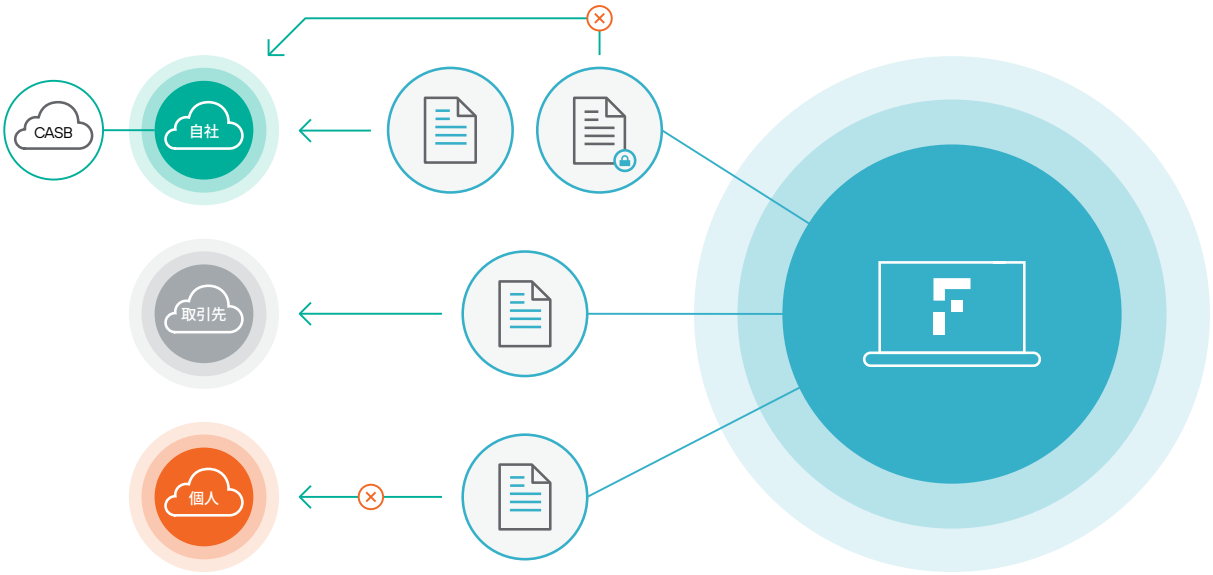
- o データ流出が発生する可能性

→ 自社で契約しているBoxへ本来はクラウドストレージに保存すべきではないデータが保存されていないか。コラボレーション等で外部へ一般公開や、取引先と共有されていないか。

- o 意図しないデータ流出が発生する可能性

→ データをアップロードする際に、対象のファイルが暗号化されたことにより、コンテンツが精査できないファイルがBox上に存在しないか。

- o セキュリティ上およびデータ管理でのリスク



外部要因によるセキュリティ脅威から会社の重要なデータを複数のシステムに守ることと同じように、意図しないデータ流出や、情報漏えいに対するリスクを減らすため、多層防御のアプローチが必要となります。データ流出や情報漏えいに対応するためのソリューションとして以前よりData Loss Prevention(DLP)ソリューションが提供されていました。従来では個人情報や顧客情報等が制限された社内の特定の環境にあり、その情報が正しく利用されているかを監査するために利用されていましたが、働き方の変革および利用するシステムの多様化に伴いより効率的にデータを保護するために再び耳目を集めています。そのため多くのネットワークセキュリティベンダーやエンドポイントセキュリティベンダーがDLPを提供可能な機能の一部として展開を開始しています。

Forcepoint では、お客様環境のデータ保護を実現するためにForcepoint Data Loss Prevention（以下、DLP）を提供し、メールやWeb等のネットワーク経由や、端末から印刷やUSBメモリを経由したデータ漏えいに加え、CASBソリューションと連携しクラウドアプリケーション経由でのデータ管理が可能です。

例えば、Forcepoint DLP（Data Loss Prevention）を活用することにより以下のような対応が可能です。

1. エンドポイントエージェントにより、社内・社外であっても社外Boxアカウントへのファイルアップロードを可視化

2. 社内で定義されているデータラベル/キーワードに対応したルールを設定し、社外/個人アカウントへのデータアップロードをブロック

3. パスワードが設定されたファイルのアップロードをブロックまたForcepoint CASB(Cloud Access Security Broker)では、Box上に保存されているデータに対して可視化を行うことが可能です。

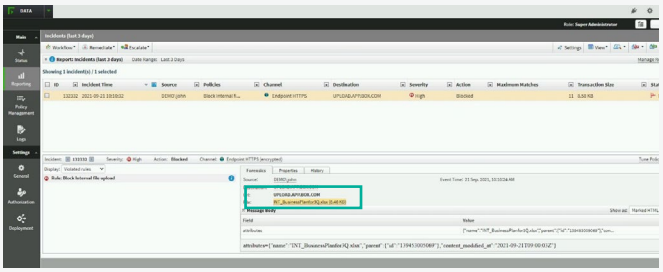
4. 社内で定義されているキーワードに対応したルールを設定し、Boxに対するスキャンを行い、保存されているデータの可視化

さらにForcepoint では、Forcepoint DLPとForcepoint CASBを連携させることにより、例えばクライアントPCにインストールしたDLPエージェントによるデータ持ち出しの可視化だけでなく、CASBと連携させることによりクラウドアプリケーション側で保存されているデータに対しても同じデータ保護ポリシーで可視化・制御を行うことが可能です。

では、それぞれのケースについて詳細を確認していきましょう。

1. エンドポイントエージェントにより、社内・社外であっても社外Box アカウントへのファイルアップロードを可視化

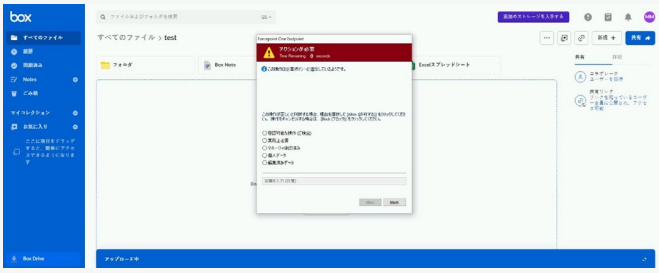
Forcepoint DLPでは、端末にDLP エージェントをインストールすることにより、社内であっても社外であっても端末側にポリシー情報を保持し、DLPポリシーを適用することが可能です。この機能によりBoxにアップロードされるデータについて、可視化し、記録することが可能です。



管理コンソールにて、検知対象データの確認が可能

2.社内で定義されているデータラベル/キーワードに対応したルールを設定し、社外/個人アカウントへのデータアップロードをブロック

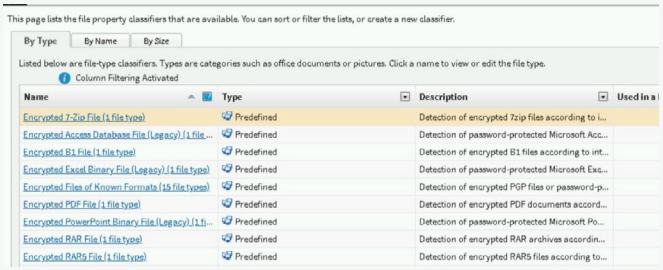
単純なアップロードされるデータの可視化に加えて、「社外秘」等のキーワードが付与されたデータのアップロードを制御することが可能です。その際、Boxアプリケーション側で社用ドメインを指定することにより、それ以外のドメインに対して「社外秘」等のキーワードを含むデータのアップロードを検出した場合には、DLPでのブロックや、従業員に確認を促すポップアップを表示させる等の設定が可能です。



ユーザへ確認を促すコーチング画面の表示

3.パスワードが設定されたファイルのアップロードをブロック

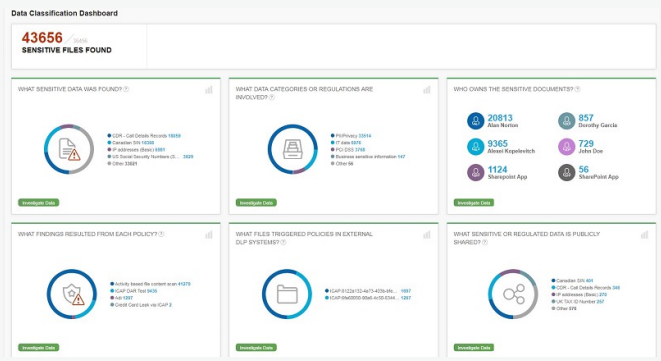
パスワードが設定されたzip圧縮ファイルがクラウドストレージ上に保存された場合、実際に含まれているデータについて可視化が阻害され、また当該ファイルをダウンロードした際には、アンチウイルスによるスキャンが実施できないことからセキュリティ上の懸念ともなりえます。Forcepoint DLPでは、事前定義されたファイルタイプを利用し、様々なファイルタイプについて検出することが可能です。例えばパスワードが設定されたzipファイルや、PDFファイル、オフィス関連ファイルについて検出することが可能です。



定義済み暗号化ファイル検知ルール

4.社内で定義されているキーワードに対応したルールを設定し、Boxに対するスキャンを行い、保存されているデータの可視化

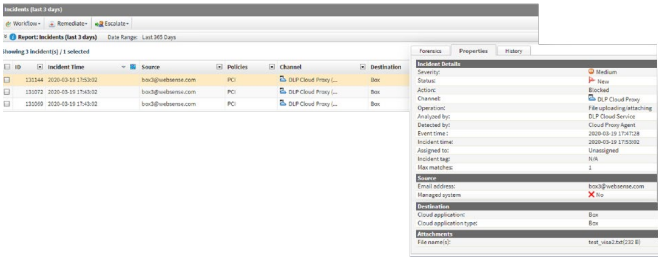
Forcepoint DLPとCASBを連携させることにより、DLPで定義されたDLPポリシーに基づきBoxアプリケーションに対するスキャンを実施することが可能です。実際にどの程度のファイルがBoxアプリケーション側に保存されているのか、保存されているファイルに適切な共有設定がされているのかを把握することにより保存データに対する可視化を行うことが可能です。



CASBソリューションと連携時の検知画面（Forcepoint CASB）

またForcepoint DLPの管理画面上では、CASBと連携し検知したインシデント情報について、DLPの管理画面上で確認することができ、一つの管理コンソール上でインシデント管理を行うことが可能です。

Forcepoint CASBでは、BoxとのAPI連携により、どのユーザがいつ、どんなデータにアクセスしたかを可視化できるだけでなく、特定アカウントに対するログイン試行の有無や他の地域・国からのアクセス試行についても可視化を行うことでBoxを利用する際のセキュリティ向上に貢献できます。



まとめ

今回は、データセキュリティという観点において、Box上のデータについてForcepoint DLPで達成可能なことについて紹介しました。守るべきデータを適切に管理するためForcepointがどのようにお客様のセキュリティに寄与できるか実例等を通してご理解いただければ幸いです。

実際のお客様環境では、Boxアプリケーションを含む様々なクラウドアプリケーションを利用し、端末もWindowsだけではなくMacを利用されている状況かと思います。そのようなマルチOS、マルチクラウドの環境において、従業員や取引先との生産性を損なうことなくデータセキュリティを促進するForcepointソリューションについてご検討ください。

Forcepoint

forcepoint.com/contact

フォースポイント社について

フォースポイント社は、デジタルトランスフォーメーションと企業の成長をより安全に推進するため、ユーザーとそのデータを保護するサイバーセキュリティーのリーディングカンパニーです。人の行動様式に最適化されたフォースポイントのソリューションは、セキュアなアクセスを担保しつつも従業員の生産性を損なうことなく、リアルタイム性を重視したデータ管理を可能にします。

フォースポイント社は、テキサス州オースティンを本拠地とし、世界中の何千ものお客様に安全と信頼された環境を提供しています。

[FP-Enhanced Security for Box Application-Brochure-JP] 16Nov2021