Office 365のセキュリティにおける6つのユースケース

Microsoft Office 365は事実上、大小を問わず、企業や組織における標準的なオフィスソフトとなりました。クラウドベースのソフトウェアアプリプラットフォームを通じて、組織全体で協業やコミュニケーションを促します。クラウドベースのコラボレーションプラットフォーム「Office 365」は、作業場所に関わらずWord、Excel、PowerPoint、Outlookを従業員と共有することができます。SharePoint、OneDrive、Yammerなどのオフィスアプリケーションをシームレスに統合し、職場の生産性の向上や協業の強化も可能です。

しかし、Office 365などのクラウドベースのアプリケーションに移行する場合、企業はデータのセキュリティやコンプライアンスに対するアプローチを変える必要があります。本書では、CASB(Cloud Access Security Broker:キャスビー)でミッションクリティカルなOffice 365環境の保護に関して評価する際のポイントを主な6つのユースケースでご紹介します。

netskope

01

OneDriveとSharePointから機密データの公開リンクを削除する

OneDriveとSharePointは、企業ユーザー間の協業をサポートするクラウドベースのコラボレーションツールです。多くの企業に展開されていて、文書作成、アップロードおよび共有が容易に行えることから、セキュリティチームは組織内や組織間で共有する大量の文書を適切に管理できなくなっている可能性があります。

多くの企業が、プロジェクトや協力の終了後、かなりの時間が経過した後も、サードパーティのビジネスパートナーや、さらには一般人もアクセス可能な機密データへの共有リンクをインターネット上に放置しています。このように忘れられたリンクは、重大な脅威が見つかった際に発見され、セキュリティチームがその後始末を迫られます。時間と共にOffice 365から公開リンクや、機密データへの自由なアクセス、また許可設定関連の大問題が大量に発生し、時間のかかる細かいセキュリティリスク評価が必要になる可能性があります。Netskopeは、OneDriveやSharePointを含む、企業のMicrosoft Office 365環境を分析し、データ共有におけるポリシー違反を検知します。企業は、テラバイト規模に及ぶ膨大なファイルを保存しています。Netskopeは、保存される企業データのすべてに素早く包括的なDLP(情報漏えい対策)分析を展開し、セキュリティチームが定めた会社のセキュリティポリシーに適合していない、機密データが含まれた共有を見つけることができます。すべての違反を即座に解消し、不必要な共有リンクを削除します。

01

機能要件

- 外部または一般向けに共有されている機密データを見つけ、報告する
- マネージドクラウド内の保存データに包括的なDLPを適用する
- 一般または外部向け共有設定の削除や閲覧限定のアクセス制限などを推奨するポリシーを継続的および遡及的に適用する

環境要件

- API（アウトオブバンド接続）

アドバイス：

ご利用のCASBベンダーに、Microsoft Office 365との統合レベルについてお問い合わせください。機密データを含む公開リンクや外部共有設定をすべて発見することが可能なレベルでしょうか

02

Office 365での危険な活動をリアルタイムに可視化および制御する

Office 365はITの中枢システムとして、分散型グローバルチームの協業をサポートします。Office 365のようなシステムは生産性に多大なメリットをもたらしますが、それと同時に、機密データを外部へ漏えいさせる危険性もあることが知られています。セキュリティチームには、日常業務に影響を与えず、危険な振る舞いの監視や制御を行えるツールが必要です。従来のセキュリティツールでは、Office 365などのクラウドベースアプリケーション全体を可視化したり、ユーザー活動を制御することもできません。

Netskope for Office 365は、セキュリティチームがOffice 365や数千ものクラウド全体にわたる活動、データおよびコンテキストを詳細に把握することをサポートします。Office 365を使った会社全体での活動やデータフローを細かく詳細に可視化させることで、データへのアクセス方法やアクセスするユーザーとグループについて、重要な知見を取得することができます。これを基に、Office 365におけるすべてのトランザクションに規定のセキュリティポリシーをリアルタイムに適用するための土台を築くことができます。Office 365などのクラウドサービスのトラフィックは、フォワードプロキシ経由でNetskope Cloudに送信され、リアルタイムにセキュリティ分析が行われます。Cloud XDでクラウドアプリをデコードし、暗号化されたトラフィックを検査し、数千ものクラウドアプリをマネージドとアンマネージドに分類後、特定のリスク評価を適用することで、粒度の高いコンテキストを取得することが可能になります。セキュリティチームは、内部から機密データを流出させるためのツールとして悪用される可能性の高いクラウドアプリを発見次第、該当するアプリをすべて封じ込めます。

02

機能要件

- Office 365および数千ものクラウド全体にわたる活動、データおよびコンテキストを詳細に把握する
- ポリシーをOffice 365アプリ全体にリアルタイムで適用し、危険な行動に対して制限をかける
- Office 365および数千ものクラウドのDLP分析を行う

環境要件

- フォワードプロキシ（リアルタイム制御）

アドバイス：

ご利用のCASBベンダーに、Office 365を保護するための展開オプションについてお問い合わせください。APIのみでの展開の場合、対応可能なユースケースは限りがあります。APIとCASBのリアルタイム(インライン)モードを組み合わせることで、最も幅の広い保護がOffice 365に適用されます。

03

Office 365からアンマネージドクラウドサービスへのデータ流出を防ぐ

多くの組織は、Office 365のセキュリティ強化や保護のために多大な費用をかけます。セキュリティポリシーの多くは、Office 365の会社リソースから権限のない個人やデバイスへのアクセスを制限することに重点を置いています。しかし、よく見落とされがちですが、Office 365の会社インスタンスにアクセスできるマネージド(管理)デバイスにアンマネージド(非管理)アプリケーションが存在するという事実があります。例えば、Office 365の会社インスタンスからファイルをいつもどおりダウンロードする従業員が数多くの組織にいるはずです。そのような従業員は、ファイルをマネージドデバイスにダウンロード後、そのファイルをそのままOffice 365の個人インスタンスなど、アンマネージドクラウドアプリケーションにアップロードすることができます。

Netskopeは、データが組織から流出するルートを封じ込め、機密データを外部に漏えいさせないCASBセキュリティプラットフォームを1から設計しました。組織内で実行される数千ものクラウドアプリケーションをリアルタイムに把握し、適切な使用を促すためのセキュリティガイドを設置し、危険な活動を防止する粒度の高いセキュリティポリシーを設定することができます。Netskopeは、Cloud XDで、マネージドやアンマネージドに関わらず、数千ものクラウドアプリケーションを特定し、Office 365の企業インスタンスと個人インスタンスを識別することもできます。一方、粒度の粗いセキュリティ制御は、Office 365へのアクセスを許可またはブロックすることしかできないうえに、Office 365向けに導入されたそれらのセキュリティを完全に回避される場合もあり、間接的に機密データをOffice 365の個人インスタンスや他のアンマネージドクラウドアプリケーションにアップロードする機会を与えてしまいます。

03

機能要件

- Office 365および数千ものクラウド全体にわたる活動、データおよびコンテキストを詳細に把握する
- Office 365から他のアプリへのデータの流出について警告、またはそのような行動を防止する
- Office 365および数千ものクラウドのDLP分析を行う
- Office 365の各種インスタンス（例：個人または会社）を区別する
- インスタンスに基づき、クラウドのカテゴリ別に許可やブロックを行うポリシーを適用する

環境要件

- フォワードプロキシ(リアルタイム制御)

アドバイス：

ご利用のCASBベンダーに、セキュリティクラウドアプリ保護対象領域についてお問い合わせください。安全に見えるOffice 365環境は、アンマネージドデバイスを使用するユーザー、または制御されていないアンマネージドクラウドアプリへのアクセスを見逃している場合もあります。

04

Office 365のコンプライアンスを維持する

Office 365アプリケーションスイートは、企業データのレポジトリとして機能しています。企業ユーザーがデータを作成、アップロード、ダウンロード、共有および協業する場所であるため、悪意のある内部関係者に不正利用される可能性があります。機密データは簡単に漏えいし、組織のコンプライアンスやデータセキュリティのすべてが危険にさらされます。セキュリティチームは、データの移行場所に関わらず、可視化と制御によって機密データを継続的に監視し、データ取り扱い上のミスが発生するあらゆる可能性を防ぐ必要があります。Office 365を展開するお客様には、規制されるデータへのアクセス方法やアクセスするユーザーとグループを制御するためのコンプライアンスの対応を講じる責任があります。組織全体をコンプライアンス違反にさらさないように、リスクがあるようなデータへのアクセス、閲覧、ダウンロードまたはその他の行動を防ぐためのガイドが必要です。

Netskopeは、組織によるコンプライアンス要件への準拠に対応する新たなセキュリティ制御の層を提供します。セキュリティチームは、粒度の高い可視化と制御によって、重要なデータが外部へ流出することをリアルタイムに防ぐなど、包括的なDLPを強制的に適用することができます。既成のテンプレートからコンプライアンスポリシーを迅速に設定できるだけでなく、組織の要件に合わせてポリシーをカスタマイズすることも可能です。

04

機能要件

- Office 365および数千ものクラウドサービス全体にわたる活動、データおよびコンテキストを詳細に把握する
- Office 365および数千ものクラウドサービスのDLP分析を行う
- 規制コンプライアンステンプレートでDLP分析を行い、ポリシーウィザードでコンテキストを定義する
- コンプライアンス対策を検証する監査担当者のニーズを満たすレポートを提供する

環境要件

- フォワードプロキシ（リアルタイム制御）

アドバイス：

ご利用のCASBベンダーに、提供される既成のコンプライアンステンプレートの数をお問い合わせください。各コンプライアンスポリシーを1から設定しないでください。膨大な数のマニュアル作業が必要となり、ミスが発生しやすくなりま

05

高度な脅威からOffice 365を保護する

サイバー犯罪者が企業ユーザーの協働や通信場所、また機密情報の保管場所へと攻撃経路を移しているため、Office 365が狙われるケースが増えています。クラウド経由で世界中からアクセスできるOffice 365は、サイバー犯罪者が様々な方法で侵害し、会社の機密データにアクセスできる格好の攻撃経路となっている可能性があります。セキュリティチームには、組織を狙う最新のサイバー攻撃を防ぐ、Office 365用の高度な脅威対策が必要です。

Netskope for Office 365は、クラウドフィッシングなどのクラウドベースの脅威をはじめとする高度なサイバー脅威への防御など、セキュリティ脅威に包括的に対応したプラットフォームです。Netskopeのインライン保護は、Office 365のトラフィックを含め、企業のクラウドトラフィックの奥深くに潜む不正リンクやマルウェアによる攻撃をリアルタイムに防ぐことができます。

さらに、Netskopeは、Office 365のトラフィックを掘り下げ、暗号化通信を復号し、サンドボックス機能、機械学習での分析による不正な振る舞いの検知などにより、サイバー脅威の兆候を検知します。Netskopeならば、フィッシング攻撃に使用されるマルウェア防御や不正リンクの防止、検出および封じ込めが可能です。SharePointやOneDriveに埋め込まれたマルウェアは、企業ユーザーのエンドデバイスにダウンロードされる際にブロックされるため、マルウェアが組織内に足掛かりを作ることはできません。

05

機能要件

- OneDriveおよびSharePointに潜むマルウェアを検出および封じ込める
- クラウドサービスやWebトラフィックをリアルタイムに分析し、マルウェアを防ぐ
- 暗号化通信の復号、サンドボックス機能、機械学習による異常な振る舞い検出機能により未知のサイバー犯罪活動または悪意のある内部ユーザーを特定する

環境要件

- API（アウトオブバンド接続）
- フォワードプロキシ（リアルタイム制御）

ヒント：

ご利用のCASBベンダーに、企業ユーザーとクラウドアプリ間を行き来するトラフィックに対するリアルタイムのマルウェア防御や検出が可能であるかをお問い合わせください。不正インスタンスや侵害されたインスタンスを悪用したクラウドフィッシングなど、未知の脅威や潜伏中の脅威防御策をご確認ください。そのCASBベンダーは、不正ファイルやリンクがクラウドアプリに保存されるまで何もできず、API経由でしか修正できないということはないでしょうか。

06

Office 365にアクセスするアンマネージドデバイスを可視化および制御する

Office 365により、従業員の場所や使用デバイスに囚われない協業や生産性向上のためのプラットフォームが拡充されます。このようにいつでもどこからでもアクセスできることでかなりの柔軟性が生まれ、職場の様々な要件が満たされています。

しかし、従業員が個人デバイスからOffice 365にアクセスする場合、組織にとって新たなリスクが発生します。従業員はOffice 365にアクセスし、会社データを個人デバイスにダウンロードできてしまいます。従業員の行動を可視化できていない組織が多く、セキュリティチームの監視下であってもその目が届かないところがあり、機密データが個人デバイスにダウンロードされるといった潜在的に危険な行動が起きています。

さらに悪いことに、組織を辞める従業員が、セキュリティチームの監視や制御の範囲を超え、会社データを個人デバイスに入れて持ち出すということも考えられます。

Netskopeは、Cloud XDによって会社（マネージド）デバイスと個人（アンマネージド）デバイスを識別し、セキュリティチームが会社データへのアクセス、ダウンロードまたは編集が可能なデバイスを規制するセキュリティポリシーを適用し、細かい制御を行うことをサポートします。これにより、組織のリスクを上げることなく、従業員はOffice 365コラボレーションツールによる恩恵を受け続けることができます。

06

機能要件

- ユーザー、デバイス、活動、データへのアクセスをリアルタイムに制御する
- Office 365にアクセスするアンマネージドデバイスからのマルウェアまたは高度な脅威を検出する
- マネージドデバイスとアンマネージドデバイスを識別する
- データのDLPプロファイルに基づき、アクセス制御ポリシー（閲覧のみ許可、ダウンロードをブロックする、など）を実行する

環境要件

- リバースプロキシ(リアルタイム制御)

アドバイス：

ご利用のCASBベンダーに、マネージドクラウドアプリにアクセスするアンマネージドデバイスへの対策についてお問い合わせください。リバースプロキシを展開している場合は、対応するマネージドクラウドアプリの数をご確認ください。

一般的な展開オプション

Office 365およびその他の認定クラウドサービス内のデータ保護

環境オプション	対応範囲	主な特長	対象
API（アウトオブバンド接続）	マネージドクラウドサービスに保存されたデータの保護と脅威防御	• 保存中のデータを保護	• マネージドアプリのみ • リアルタイムではない
リバースプロキシ	マネージドおよびアンマネージドデバイスのブラウザから実行するマネージドアプリでの操作に対しリアルタイムでのデータ保護および脅威防御	• アンマネージドデバイスの可視化と制御	• マネージドアプリのみ • ブラウザのみ
フォワードプロキシ（Netskopeクライアント）	マネージドデバイスのブラウザまたはネイティブアプリでの操作に対してリアルタイムでのデータ保護および脅威防御	• モバイルデバイスとリモートワーク対応 • ネイティブアプリ対応 • マネージドおよびアンマネージドクラウドサービス対応 • Webトラフィック対応	• マネージドデバイスのみ

これら3つを組み合わせることで、あらゆるユースケースに対応できます。

Netskopeについて

ネットワークの境界線は崩壊しつつあります。今、ビジネスの成長を阻害することなく、あらゆる場所にいるユーザーとデバイスを保護する新しい境界が必要になっています。Netskope Security Cloudはユーザーが利用するクラウドアプリ、Webサイト、プライベートアプリケーションの全てにおいて、比類のない可視性とリアルタイムでのデータ保護と脅威防御を提供します。

Netskopeはクラウドを最も理解して可視化・制御し、世界最高クラスの規模と速度を持つネットワークインフラストラクチャ「NewEdge」により最高のData Centric(データを中心に考える)なセキュリティを提供でききます。これにより、必須のデータ保護、お客様のビジネス速度、目指すべきデジタルトランスフォーメーションの姿において最高のバランスをとることができます。

Netskopeとともに、境界線を再構築しましょう。

netskope.com/jp