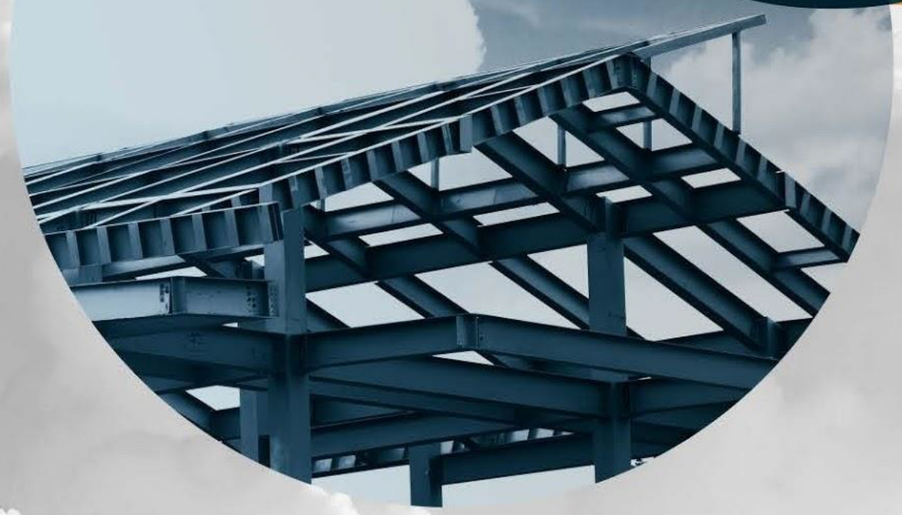
netskope

TOP 5

リモートワーカーを守る SASEのユースケース



リモートワーカーを守る
SASEのユースケース

新型コロナウイルス感染症（COVID-19）が世界的に流行し、各組織はリモートワーカーの数を2～3倍にまで増やした上でさらに管理する必要に迫られています。これをきっかけに、セキュアアクセスサービス エッジ（SASE）アーキテクチャの戦略的な計画と導入が主要な課題として挙げられています。従業員の3分の2以上がリモートで働く現在、SASEを取り入れたセキュリティのユース ケースに目を通せば、状況に即してどのような対策が可能なのかが分かります。しかし、従来のセキュリティ ソリューションでは、その多くを実現できません。ニューノーマルへの対応が求められているなか、この傾向はしばらく続くことになるでしょう。そのため、今後の時代にあったセキュリティを考えることが最優先課題となっています。

リモートワーカーを守る
SASEのユースケース

ユース ケース #1 | 想定外のデータ移動を防止する

ユース ケース #2 |適切な人によるデータの適切な取り扱い

ユース ケース #3 | ユーザー向けコーチング、高リスクのユーザーやアプリの識別を行う

ユース ケース #4 | 条件とコンテキスト情報によるアクセスで、安全なインターネット接続を実現する

ユース ケース #5 | クラウドを悪用したSaaSやWebサイトによる脅威から身を守る

01

想定外のデータ移動を防止する

2020年、リモートワーカーの増加にあわせてアプリをSaaSやクラウドへ移行し、データ移動を制御しようという動きが高まっています。これを牽引するCISO、そしてセキュリティ担当者にとって、ここで紹介するユースケースは有益な情報となるでしょう。 端的に説明すると、クラウドを使用しなくてはならない、もしくはすべき場面が多くなっており、今までのようにクラウドアプリへのアクセスを拒否・許可の2パターンで制御することは困難になっているからです。

こうした方法に代わり、クラウドアプリではデータ移動に関する詳細なポリシー制御を適用する必要があります。また、リモートワークにより、Microsoft TeamsやSlackなど、コラボレーションツールの使用も増加しています。これにより、データの共有も移動も、組織の内外でいっそう簡単に行えるようになりました。

01

本ユースケースでSASEがどのような効果を発揮するのか、以下をご覧ください。

インスタンス認識： 同じクラウド アプリの異なるインスタンス（個人用・企業用など）を識別し、それぞれにポリシーを適用します。企業で使用するアプリについてユーザーが個人インスタンスを持っている場合、企業インスタンスから個人インスタンスへ（例：企業のOneDriveから個人のOneDriveへ）、あるいは異なるアプリ間で（例：企業のOneDriveから個人のG-Drive へ）、極めて容易にデータを移動することができます。

From/Toユーザー制御： 管理アプリ（マネージドアプリ）か非管理アプリ（アンマネージド アプリ）かに関わらず、特定のユーザーあるいはメールドメイン間でデータの移動を制御することができます。こうした制御は、インスタンス認識が効かないアプリの場合にも作動します。データを共有するユーザー、またはアプリへのサインインに必要な認証情報に制限を設け、データの移動が想定外のものであっても、あるいは未承認のものであっても、制御下に置くことが可能となります。

アクティビティコントロール： マネージド アプリかアンマネージド アプリに関わらず、データ移動に関してアプリのアクティビティを制御します。アクティビティの内容として、ダウンロード、アップロード、投稿、閲覧、削除、表示、共有などが挙げられます。

アプリのリスクおよび分類： 特定のアプリにおけるリスク評価によるスコアの範囲、あるいはアプリの分類をもとに、データ移動を制御することができます。アプリを分類しデータの流れを見ることで、まずクラウド ストレージ アプリ間で移動し、そこからからコラボレーション ツール、Web メール、CRM ソリューションへ移動していることなどがわかります。

異常行動の検出： 機械学習（ML）モデルと一連のアノマリ検出ルールを用い、正常値のベースラインを外れた行動を検出します。アップロードやダウンロード、または削除が一括で行われた場合のほか、普段とは違うイベント、ログインの失敗、危険性のある国からのアクセス、クラウド間でのデータ流出なども検出します。ベースラインに照らして機械学習で分析を行うため、コンテキストの豊富なメタデータを収集・保存して使用する特徴です。

02

適切な人によるデータの適切な取り扱い

クラウドの導入はデータ移行を伴うためデータのコンテキスト情報がSASEアーキテクチャの中核を成すという原則が成り立ちます。セキュリティやネットワーク サービスを提供し、ユーザーと密に関わり重要な役割を果たすクラウド エッジはデータを脅威から保護するため、そのコンテキスト情報を中心に構築されています。従来の防御ではマネージド アプリでもアンマネージド アプリでも、アプリにおけるデータの流れが確認できず、クラウド サービスとともに使うには不十分です。

リモート ワークの増加に伴い、融資、求人応募、人事、不動産以外の業務プロセスにおいても、業務がオンラインに移行しています。個人情報（PII）を求めるにあたり、証明書や画像の送信が必要となる状況も増加しています。

02

本ユースケースでSASEがどのような効果を発揮するのか、以下をご覧ください。

データ保護に関する制御：悪意ある危険なWebサイト、高リスクのアプリ、そしてアンマネージドアプリやそのインスタンスへのアップロードをブロックし、承認済みドメインへの共有アクティビティも制限することで、データ漏えい防止（DLP）機能を呼び出す前にその対象領域を縮小します。

高度なクラウド型DLP：マネージド デバイスで作動中のデータにはフォワード プロキシ経由、アンマネージド デバイスで作動中のデータにはリバース プロキシ経由、そして保存データに対してはAPI経由で、クラウドDLPを実行します。AIや機械学習を使って文書や画像を分類するなど、新たな技術の進歩により、身分証明書、パスポート、確定申告書、履歴書、デスクトップのスクリーンショットなど、データの登録がなくても正確な検出が可能となっています。

シングル パス：1度の処理でデータの保護を可能にし、Webサイト、マネージド アプリ、アンマネージド アプリ、IaaSのパブリック クラウドにおけるユーザートラフィック、そしてカスタムアプリなどが対象となります。1つのソリューションとして実行され、コンテキスト ポリシー、コンプライアンス テンプレート、完全データー致を適用するほか、フィンガープリントによる類似度の算出なども行われます。3,000を超える識別子を用い、1,400以上のファイルの種類を識別します。

03

ユーザー向けコーチング、高リスクのユーザーやアプリの識別を行う

多くのCISOは、リスクの軽減に向けて適切な行動を促すにあたり、教育の場を1度設けるより、リアルタイムでユーザーを指導する方が効果的と考えています。クラウド導入に伴い、制御の根幹はユーザーのアイデンティティ、アプリ、データになります。ユーザーとアプリについてはリスクの評価を実施し、データはしっかりと分類します。何をどのように「許可」するかという視点がニューノーマルのかたちだとすると、データのコンテキスト情報を理解すれば、単なる許可・拒否だけでは網羅できない詳細なポリシー制御においても、コーチングが可能となるのです。今までのセキュリティ対策では、レッド ゾーンをブロックし、グリーン ゾーンを許可していました。しかし、クラウド導入とリモート ワークが進む中、中間にあるグレー ゾーンが広がり続け、これを管理することが求められています。

03

本ユースケースでSASEがどのような効果を発揮するのか、以下をご覧ください。

ユーザーのコーチング: 従業員がリスクのあるアプリではなく、より安全性が高くて代替となるようなアプリを使用するようリアルタイムで指導し、アクティビティの妥当性について根拠を示すようユーザーに要求できるほか、データが移動する前に警告を発することもできます。ユーザーが指導や警告を受けた場合、 約90%の確率でデータの移動を思いとどまる、あるいはアクションをキャンセルするということが、多くの顧客事例から分かっております。

アプリのリスク評価: クラウド セキュリティ アライアンス(CSA)が定義する50 以上の属性を用い、7以上の特性にもとづいて数万のアプリのリスクを評価します。このとき、例えばGDPRコンプライアンスの比重を重くするなどのカスタマイズも可能です。ポリシー制御では、アプリのリスク レベルを参照しながら、ポリシー アクションの判断、コーチングの呼び出し、そして安全性の高い代替アプリの推奨やブロックを行います。

ユーザーの信頼度評価: 一定期間にわたり、Webサイト、アプリ、アクティビティなど、ユーザーの行動を分析し、信頼度を評価します。また、そのユーザー信頼度指数において、各イベントを確認して、どの様な行動がどれほど評価に影響を与えたのかを確認できます。こうした評価をもとに、ステップアップ認証やアクティビティのブロックなど、ポリシー アクションを呼び出すことができるべきです。

04

条件とコンテキスト情報によるアクセスで、安全なインターネット接続を実現する

Webサイト、アプリ、そしてクラウド サービスを安全に使えるようにするということは、ブロックと許可の間で、グレーゾーンを定義するということです。条件やコンテキスト情報といった属性を利用する極めて詳細なポリシー制御により、リモートワーカーの安全なアクセスが守られます。ユーザーやアプリにおける現在のリスク評価による条件、そしてデータと脅威保護への分析を、アプリ、インスタンス、分類、ユーザー、デバイス、ロケーション、データ、そしてアクティビティのコンテキスト情報と組み合わせることで、SASEのポリシー制御だけでなく回顧的分析や検証、脅威防御も可能となります。

04

本ユースケースでSASEがどのような効果を発揮するのか、以下をご覧ください。

ユーザー／デバイス／ロケーション: 使用しているデバイスがマネージド デバイスかアンマネージド デバイスかに関わらず、ユーザーとそのロケーションを特定し、データのダウンロードを許可するか、あるいは表示のみとするか、ポリシー制御に基づいて判断します。例えば、ある種のデータについて企業のデバイスではダウンロードできても、個人のデバイスでは表示のみとする、などです。

アプリ／インスタンス／アプリとURLの分類／データ／アクション: 詳細なポリシー制御を実現するには、アプリ、分類、インスタンス、データ、そしてアクションのコンテキスト情報が必要です。機密情報をアップロードしようとしている場所は、会社で認可されているアプリだとして、実は会社ではなく個人のインスタンスかもしれません。会社でつかっているWebメールと同じアプリの、個人用のものである可能性もあります。

ユーザーの指数とアプリのリスク評価: ユーザーやアプリについてリスクなどを把握し（ユーザーに関しては直近の行動分析に基づく）、その信頼度や評価に基づきポリシーによるアクションを実行します。信頼度が低いと判定されたユーザーには、ステップアップ認証を求めたり、データの分類や実行しようとしているアクションに基づいてその行動をブロックする可能性もあります。アプリの信頼度が低いと判定された場合、安全性の高い代替アプリを提案するか、ユーザーに警告を発し、該当するアプリの使用について妥当性の根拠を求めた上で続行を許可する場合もあります。

脅威からのデータ保護: 明確な条件とコンテキスト情報により、適切なアクセスに基づいたユーザー、アプリ、データ、アクションであっても、リアルタイムかつインライン処理でのデータ保護と脅威防御は必要です。そしてこれはユーザーからのWebサイト、アプリ、クラウド サービスへのトラフィック全体に適用すべきです。あらゆるソリューションでこうした対応が可能なわけでないため、この視点からSASEソリューションを選定するというのは大事なことです。

05

クラウドを悪用したSaaSや Webサイトによる脅威から身を守る

クラウド アプリは、多くの組織で導入が進む前からサイバー攻撃に悪用されており、攻撃の拡散につながっています。サイバー攻撃者は、信頼できるドメイン、有効な証明書、攻撃相手が使用しているアプリと同じマネージド アプリの別インスタンスを利用し、検知されることなく従来のインライン防御をすり抜けます（従来のファイアウォールやプロキシでのインライン型制御はクラウド プロバイダーに推奨されていますが、セキュリティ対策としては不十分です）。

APWGのフィッシングトレンドレポートで現在トップのサイバー攻撃は、フィッシングによりSaaSアプリの認証情報を盗み取る行為です。ファイルベースのマルウェア攻撃は、初期の攻撃ベクトルとしては減少傾向にあります。代わりに、偵察からデータの抜き出しまで、サイバー キルチェーンのあらゆる段階で、クラウドが悪用されています。

05

本ユースケースでSASEがどのような効果を発揮するのか、以下をご覧ください。

アクセス認証情報：ID、アプリ、データを指定する認証情報は、新たなセキュリティの制御プレーンです。サイバー攻撃の狙いが、認証情報を盗み出すことやブルート フォース アタックでアクセスを試みることにあっても、不思議ではありません。サイバー攻撃者は、信頼のあるマネージド アプリやインスタンスを装い、不正なWebフォームを作成します。こうした場所にログイン情報を入力していないかどうか、クラウド型の高パフォーマンスなDLPを使って判定しましょう。この種のクラウドフィッシングは、従来のようにエンドポイント、メール、Web

脅威インテリジェンスの共有：Netskopeやエンドポイント、そしてSIEM、SOAR、IRなど、SASEで統合されたセキュリティ スタックでは、各防御ソリューション間で脅威インテリジェンスの共有が行われています。また、脅威インテリジェンス フィードを運用するにあたり、Cloud Threat Exchange（CTE）のようなツールを使えば自動共有が可能となり、Webフィルタリングの設定で頭を悩ませることもありません。

クラウド脅威リサーチ：クラウドを悪用した脅威においては、ユーザー トラフィックを守るためには、アプリやクラウド サービスにおいてデータとコンテキスト情報を可視化する必要があります。従来のセキュリティ ソリューションでクラウド アプリのデータを復号して見ることができないのであれば、脅威を見つけ出せる可能性は低いといえます。クラウドによる脅威の多くはエンドポイントに影響しないため、エンドポイントで防御を強化するとしても限界があります。

脅威に対する高度な保護機能：ファイルの再帰的な展開や難読化解除のほか、事前分析、ヒューリスティック、ベアメタル サンドボックス、機械学習分析など、可能な不正防止チェックをすべて完了すると、脅威の検出に向けて複数の対策が講じられます。内部の脅威、アカウントへの侵入、あるいはデータの抜き出しを検出するための行動分析も行います。

まとめ

SASEアーキテクチャでリモート ユーザーを保護するには、データのコンテキスト情報が必須

従業員が組織のコラボレーション アプリ内の文書にアクセスする場合を考えてみましょう。その文書内には、協働しているサード パーティによって、別のクラウド アプリでホストされている異なる文書へのリンクがあるとします。このリンクが有害なもので、最初の従業員をフィッシング ページに誘導するとしましょう。そのページは、従業員が普段目にするクラウド アプリのログイン ページと全く同じように見えます。そのクラウド アプリは、誰もが知っている「信頼できる」クラウド サービスでホストされています。ここで従業員がうっかり認証情報を入力すれば、その情報は盗まれてしまいます。

この一連の出来事は全てクラウド内で起きています。ファイルやデータなどはエンドポイントに書き込みがされないため、分析されることもありません。マルウェアはファイルとしてダウンロードされるもの、というマインドセットをクラウドを悪用した脅威やクラウド アプリ間における想定しない、あるいは未承認のデータ移動なども考慮するというように変えていく必要があります。ユーザーもデータもクラウドにあり、アプリを自由に選んで業務を進めることができます。データを保護するため、許可と拒否の間に生まれたグレーゾーンを理解し、クラウドへの安全なアクセスを実現することが、Netskopeの役割です。

詳細情報

Netskope のサービスを利用すれば、ロケーションを問わずリモート ワーカーを保護できます。詳細については、お近くのNetskope営業担当や販売パートナーにお問い合わせいただくか、下記のWebサイトをご覧ください。

リモート ワーカーの保護:
https://www.netskope.com/jp/solutions/securing-remote-workers

VPNのさらに先へ:
https://www.netskope.com/jp/solutions/virtual-private-networks

ネットワークの境界がなくなってきています。業務のスピードを維持しながら、あらゆる場所のデータやユーザーを保護する新たな境界が必要とされています。　Netskope のセキュリティ クラウドは、 クラウド サービス、Webサイト、そしてプライベート アプリにアクセスする際、ロケーションやデバイスに関わらず、比類ない可視性を提供し、データを脅威からリアルタイムで保護します。クラウドに対する理解とともに規模とスピードで世界に誇るセキュリティネットワークで、データ中心のセキュリティを提供できるのはNetskopeだけです。保護とスピードのバランスを保ち。世界有数の組織に貢献し、業務の高速化を図りながらデジタル トランスフォーメーションの実現をサポートします。Netskope、とともに今必要なセキュリティを見直しませんか？

netskope.com