

エンタープライズセキュリティにおけるクラウドの優位性

モバイル、ソーシャル、クラウドのセキュリティ対策

概要

ビジネススタイルの急速かつ急激な変化に伴って、エンタープライズセキュリティも一変しました。新しいテクノロジーやトレンドが、エンタープライズという定義そのものに変化をもたらし、働き方や働く場所だけでなく、仕事で使用するツールも様変わりしています。このような変化は、どのようなトレンドによってもたらされているのでしょうか。

モビリティとモバイルデバイスの活用によって、我々の働き方が大きく変わり、従来の企業ネットワーク境界という考え方は消滅しました。BYODが一般化したことで、CISO（最高情報セキュリティ責任者）は、会社の資産ではないデバイスのセキュリティ対策という、新たな課題に直面するようになりました。従業員は、ラップトップを使って自宅で仕事をしたり、公共Wi-Fiを使って会社のネットワークに接続したり、スマートフォンやタブレットで3G/4Gネットワーク経由でメールやメッセージを送信したりするようになりました。PCを会社のネットワークに接続してオフィスで仕事する従業員はもちろん、3G/4Gネットワークを利用して個人所有デバイスで会社のリソースにアクセスする従業員もいるでしょう。これこそが、従来型のセキュリティポリシーでは想定されていなかった、現代社会の真の姿なのです。



Office 365、Salesforce、Workdayなどのクラウドアプリケーションは、クラウドによるコラボレーションと生産性のメリットを企業にもたらしましたが、必要とされるネットワークリソースがはるかに多いことから、従来型のハブ&スポーク方式のネットワークモデルの限界を表面化させることにもなりました。さらには、クラウドベースアプリケーションではユーザがインターネットから直接アプリケーションを利用できるため、ユーザがIT部門のサポートを受けることなく多数のアプリケーションをダウンロードするようになりました。クラウドベースのマーケティングオートメーションシステムのライセンス管理部門、ファイルをDropboxに保存する従業員、BasecampなどのWebアプリケーションを利用する契約社員のいずれであっても、ユーザ自身がやり方を選択するスタイルが定着しました。CISOは、これらのトレンドを奨励しつつ、潜在的なリスクや情報漏洩から会社を保護するという課題に直面しています。

一般ユーザがプライベートで利用するだけであったソーシャルメディアも、ビジネスに不可欠なエンタープライズアプリケーションへと急速に進化を遂げました。マーケティングの目的でTwitter、YouTube、LinkedIn、Facebookが広く使用されるようになっただけでなく、エンターテインメント性の高いソーシャルメディアスタイルのコラボレーションツールを利用するYammerやSlackなどが成功を収めています。

セキュリティ脅威の進化

こういったテクノロジーのトレンドに乗じたサイバー犯罪の増加は、驚くべきことではありません。セキュリティの脅威は、デスクトップベースのウイルスからブラウザベースの脅威、フィッシング攻撃、ポットネットへと進化し、保護されないWi-Fiやセルラーネットワークで会社の資産にアクセスする従業員の増加によって、企業のセキュリティ侵害がこれまで以上に簡単に発生するようになりました。このような脅威には、ユーザのデバイスやロケーションに関係なく、一貫したポリシー、保護、可視性が提供される、新しいセキュリティアプローチが必要です。

デバイスやロケーションに関係なく、一貫性のあるポリシー、保護、可視性が保証されるセキュリティソリューションが必要とされるようになった今、大きな可能性を秘めたクラウドが注目されています。

境界の消滅

モバイルエンタープライズには、明確な境界は存在しません。ビジネスの場は、モバイルデバイスや3G/4Gネットワーク、コーヒESHOPや空港の公共Wi-Fiネットワーク、移動中の航空機など、さまざまです。ユーザがクラウドに直接アクセスし、会社のゲートウェイプロキシやファイアウォールを迂回して、クラウドやモバイルアプリにアクセスしたり、データをアップロードあるいはダウンロードしたり、テキストメッセージやメールを送信したりしています。社内のPCを上回る数のモバイルデバイスが使用されていますが、VPNには3G/4Gモバイルトラフィックが保護されないという問題があります。

ネットワークに常時接続する個人所有デバイスの増加を考えれば、エンタープライズセキュリティを、「禁止か許可か」ではなく、「管理して監視する」という方法へと切り替える必要があるでしょう。インターネットリソースへのアクセスを禁止してしまうと、全社的なセキュリティ対策を迂回しようとするユーザが増えるからです。

セキュリティベンダが最新のマルウェアやポットネット攻撃に対応するためのパッチを次々と公開し、自社ソフトウェアをアップデートしている現状を見れば、ユーザ、データ、企業にとってのリスクである大きなセキュリティギャップが存在することは明らかです。

「統合セキュリティプラットフォームのクラウドによる提供は、CISOにとって、レイテンシとコストを削減し、セキュリティ対策を強化する絶好のチャンスとなるでしょう。」

FORRESTER®

かつては、データセンタに設置されたサーバを保護するだけで十分でしたが、今は、人、クラウドアプリケーション、多様なインターネット接続デバイスを保護する必要があります。

過去



現在



アプライアンスベースのセキュリティが不十分である理由

クラウドソリューションのメリットとROIが明白であるにもかかわらず、すべてのIT部門がクラウドへの移行に積極的なわけではありません。調査によれば、企業がクラウドコンピューティングの採用を躊躇する主な理由の1つは、セキュリティに関する懸念によるものです。

そして、そういった懸念は、自らが抱えているセキュリティ対策に起因するケースが多く、企業ネットワークセキュリティを前提に設計された従来型のアプライアンスベースのセキュリティ製品がクラウドのユーザやリソースの保護にまったく適していないことが大きな要因になっています。従来型のセキュリティ対策の多くの問題は、セキュリティアプライアンスがアーキテクチャの中核部分となっている現状を検証することで明らかになります。

従来型の対策	この対策に逆行するトレンド	企業に対する影響
ウイルス対策/IDSシグネチャのアップデート	新種や亜種のマルウェアが多い	単一の方法によるセキュリティ対策は時代遅れであり、感染のリスクが高くなる
固定された境界のセキュリティ対策	ビジネスの要件とモビリティによって、ネットワーク境界とは異なる、企業の「情報境界」が生まれている	境界セキュリティでは、新しい場所に移動する際に機密データが保護されない
ネットワーク層セキュリティ	場所が多様化し、すべての場所で単一のWebプロトコルが使用される	従来型のネットワークセキュリティでは、エンタープライズアプリケーションを区別して保護したり、ユーザアクセスポリシーを適用したりできない
インバウンドのセキュリティ	不正Webサイトにユーザを誘導する方が、インバウンド対策を突破するより簡単である	ユーザのWebサーフィンによって会社が感染し、インターネットに接続されているほぼすべての企業がボットネットに参加して犯罪に利用されてしまう恐れがある
エンドポイント制御	コンサルタントや契約社員によるネットワークアクセス、スマートフォンの採用、部門ごとのPCの調達	IT部門がネットワーク上のすべてのエンドポイントデバイス、並びに会社所有のエンドポイントデバイスを管理したり、標準を規定したり、デスクトップセキュリティソフトウェアスイートをメンテナンスしたりできなくなっている
運用セキュリティ管理	パッチ適用、シグネチャの更新、ルールの変更による上記の対策に多くの時間がかかる	セキュリティ部門が運用セキュリティに多くのリソースを配分し、短時間でビジネスの問題を解決しなければならなくなっている

今日の高度な技術を持つハッカーは、このようなエンタープライズITの新たな世界を十分に理解し、さらに高度で目まぐるしく進化する脅威を使って、従来型のセキュリティアプライアンスの弱点を悪用し、攻撃を仕掛けています。モバイルユーザを標的にする攻撃が増え、企業のネットワーク環境を攻撃する突破口としてモバイルデバイスが利用されるようになっています。従業員がインターネットに直接アクセスするようになり、クラウドやモバイルアプリへのアクセス、さらにはメールの送受信に公共Wi-Fiネットワークが使用されるようになっていることが、このような攻撃を容易にしています。

ネットワークセキュリティアプライアンスに存在する上記のギャップによって、企業が重大なリスクにさらされます。このようなギャップが生まれる背景には、いくつかの理由が考えられますが、今日のエンタープライズ環境に共通する要因として、次の3点を挙げる事ができるでしょう。

- 従来型の対策は迅速な更新が困難であり、進化する脅威に対抗できない
- 新たなエンタープライズテクノロジーやビジネスの移行に必要とされる柔軟性が欠如している
- イノベーションを妨げ、ビジネスに軋轢が生じる原因になっている

アプライアンスベースのモデルにおける制約:

ロケーションへの依存:セキュリティアプライアンスは、場所という古い概念に基づいているため、ビジネスの可能性を広げるものではなく、ビジネスに限界を強要するものになっており、ビジネス活動を強制的にロケーションに結び付けたり、トラフィックを監視ネットワークセグメントにリダイレクトさせたりすることで、セキュリティ対策を実装します。

パフォーマンスの問題:ロケーションに依存するというアプライアンスの特性によって、パフォーマンス、障害発生点、セキュリティの脆弱性の問題が発生します。たとえば、URLフィルタアプライアンスを本社に設置した場合、他の拠点やモバイルユーザにとって不利益なアーキテクチャを選択せざるを得なくなります。リモートユーザは、低速のVPN接続を使ってインターネットにアクセスするか、会社のセキュリティ対策を無効にするかの選択を迫られることになるでしょう。

アプライアンスの過負荷:アプライアンスは、1つのセキュリティ機能専用設計されることが多いため、新たな脅威に対応しようとする、データセンタに次々と新しいアプライアンスが追加されることになり、すべてを個別に購入、

インストール、メンテナンス、更新する必要があります。

コストスパイラル:アプライアンスには、購入、インストール、定期的なパッチ適用、ログファイル管理、アクセス制御、統合などの多額の関連コストが必要です。IT部門にとっては、アプライアンスの必要なすべてのシグネチャファイルを更新するのは困難であるため、セキュリティのギャップが必然的に発生します。

キャパシティの制限:アプライアンスではオンデマンドのキャパシティが提供されないため、IT部門が「余裕を持たせて」ソリューションを構築する必要があります。たとえば、アプライアンスは、100、500、または2,000といったユーザ数を想定して設計されています。余分なキャパシティを購入するために過剰なコストが発生したり、ビジネスの成長に追いつけない不十分なソリューションを購入したりすることになるでしょう。

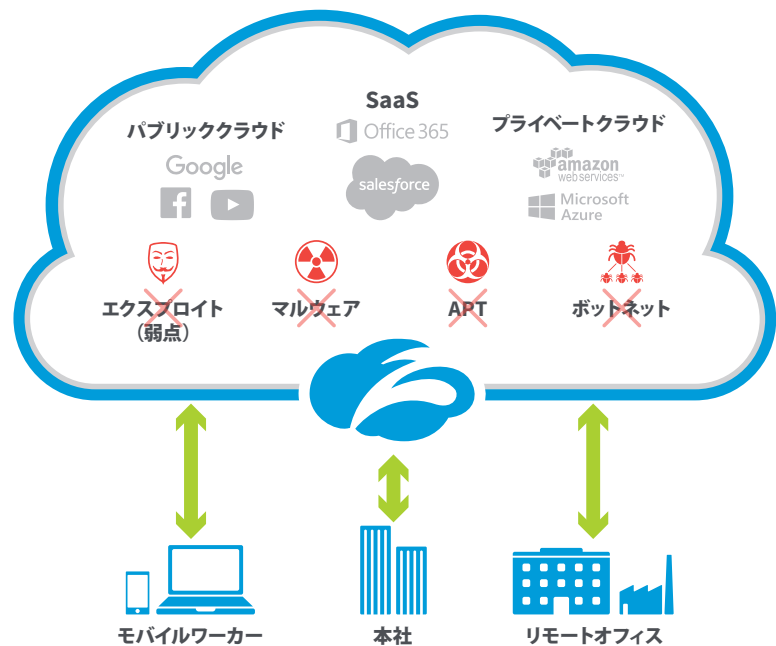
シングルテナント:アプライアンスは、単一の組織向けに設計されており、マルチテナント構成の概念は考慮されていません。したがって、契約社員、パートナー、サプライチェーン、ベンダによる現代のコラボレーションネットワークのメリットが制限されます。

セキュリティアプライアンスでは、今日の俊敏でグローバルなモバイルエンタープライズのニーズを満たすことはできません。ビジネスを拡張する安全な方法は、ハードウェアやソフトウェアを買い足すことではなく、セキュリティ戦略に存在するギャップを見逃すことなく解消できるようにすることです。

エンタープライズセキュリティにおけるクラウドの意味とは何なのでしょう。

クラウド活用のメリット

クラウドコンピューティングやSaaSアプリケーションの経済効率と競争優位性が認識され、移行が進んでいる今、エンタープライズセキュリティも転換期を迎えています。もちろん、クラウドコンピューティングが市場に変化をもたらすという考えは、新しいものではありません。Office 365、Salesforce、Workdayなどによって、クラウドが市場の破壊的テクノロジーであることが証明され、これらのアプリケーションを使用することで、企業の競争力、効率性、イノベーションの推進と大幅なコスト削減が可能であることが実証されました。



この10年間でオンプレミスのエンタープライズハードウェア／ソフトウェアが独占していた分野でもクラウドへの移行が加速し、クラウドコンピューティングのスケラビリティ、優れた機能、利便性がもたらす経済性が注目されるようになりました。そのために、巨大なデータセンタを構築して企業情報を保存し、アプリケーションやWebサイトをホスティングしようとする企業は減少し、AWSなどのクラウドサービスが代わりに利用されるようになりました。

クラウドアプリケーションの信頼性が向上し、普及したことで、クラウドのスケールメリットは無視できないほど拡大し、反対に、従来のオンプレミスのハードウェアやソフトウェアの欠点が浮き彫りになりました。オンプレミスのハードウェアやソフトウェアに初期投資するよりも、戦略的なプロジェクトに資金やリソースを配分したいと考えるのは当然のことでしょう。アプライアンスベースのセキュリティ製品では、需要予測に基づいて購入する必要がありますが、クラウドベースのセキュリティでは、企業は実際の利用量に応じて購入量を増減できます。

しかしながら、企業がデータやアプリケーションをクラウドに移行する理由は、コスト削減だけではなく、柔軟性、俊敏性、競争優位性という観点からクラウドコンピューティングを検討するCIOが増えていきます。

また、クラウドのスケールメリットによって経済性が飛躍的に向上するだけでなく、従来のアプライアンスベースのセキュリティでは不可能な、高度なセキュリティを実現することもできます。

次世代セキュリティ

クラウドにおけるビジネスの保護では、モバイル、ソーシャル、エンタープライズの新しい現実に対応できる、まったく新しい方法で、エンタープライズセキュリティを構築する必要があります。そのためには、社内はもちろん、社外のインターネット上に存在するすべてのデジタル資産とユーザ活動をCIOやCISOが制御し、認識できるソリューションが必要です。可視性は、従来のセキュリティの概念を上回るほどではないにせよ、極めて重要な要素であることに変わりありません。今日の複雑なIT環境では、企業ネットワークにアクセスするすべてのユーザ、デバイス、アプリケーションを可視化することは、ビジネスにとっての「付加的」要件ではなく、「絶対的」命題です。

次世代エンタープライズセキュリティに必要なのは、脅威対策だけではありません。脅威検知が重要であることに変わりありませんが、次世代セキュリティは、イノベーションを加速し、俊敏性や柔軟性を向上し、数年前から計画や投資が必要とされる旧来の初期／運用費構造にとらわれることなく、ビジネスを推進し、競争力を向上させるものでなければなりません。

ZSCALER™ CLOUD:安全、簡素化、ビジネスの変革

新規ビジネスの推進

今日のCIOに求められているのは、インフラプロジェクトを淡々と進めることではなく、変革の実践によってビジネス価値を推進する戦略的イニシアチブを主導する力です。セキュリティのクラウドへの移行は、そういった変革の実践の1つの手段であり、ビジネスの俊敏性の向上とROIの創出を期待できます。このアプローチによって、CIOやCISOのリソースが解放され、セキュリティ機能をビジネスの推進につなげる戦略的なプロジェクトに集中できるようになり、セキュリティインフラに配分していた予算を使ってその取り組みを推進できるようになります。



イノベーションの加速

新たなテクノロジーとプロセスによって、生産性と効率性が大幅に向上し、結果として、利益率や顧客満足度などのビジネス指標が改善します。モバイルやクラウドの新たなテクノロジーが浸透し、ユーザーに受け入れられるようになりましたが、テクノロジーの進化は速く、ユーザーが必要とするレベルのセキュリティを実現するのは容易ではありません。セキュリティをクラウドに移行することで、CIOやCISOの職務が軽減され、全社的なポリシーの準拠に必要な可視性と制御を手に入れ、イノベーションを確実に推進できるようになります。

競争力の強化

イノベーション能力、およびイノベーションを加速する新しいテクノロジーとプロセスがなければ、競争の厳しい市場を勝ち抜くことはできません。セキュリティインフラをクラウドに移行することで、企業の俊敏性が向上し、進化する脅威はもちろん、市場の変化にも迅速に対応できます。

真のクラウドと呼べる条件は何か

「クラウド」セキュリティソリューションと称する製品やベンダは数多く存在します。どのベンダも自社のソリューションですべての問題を解決できると主張しているため、現実と誇張された宣告文句を区別するのは容易ではないでしょう。

真のクラウドとは何かを理解するには、以下の用語の意味を知っておく必要があります。

MSSP: MSSP (マネージドセキュリティサービスプロバイダ) を利用すると、オンプレミスの機器の管理をアウトソーシングできます。基本的には、アプライアンスとその関連コスト、アーキテクチャやスケーラビリティの制約、障害点は維持しつつ、人件費をサービスプロバイダに移行できます。MSSPの例としては、ファイアウォールやデスクトップの分散展開を管理するベンダなどがあります。

ハイブリッドセキュリティ: 多くのアプライアンスベンダが、自社が販売する「ボックス」を補完する「クラウド」ソリューションを提供するようになりました。しかしながら、このようなソリューションでは、マルチテナントクラウドアーキテクチャの真のクラウドソリューションだけが実現可能な、インテリジェンス、スケールメリット、パフォーマンスなどのメリットが何一つ提供されません。

ハイブリッドソリューションでは、セキュリティアプライアンスが基本的にはクラウド内に共存するため、トラフィックをバックホールすることなく、支社にサービスを提供できます。ただし、パフォーマンスの問題が発生したり、障害発生点が見つかったりすると、ハイブリッドアプローチという選択肢を諦めざるを得ない場合もあります。また、モバイルユーザが保護されないという問題もあります。

真のクラウドネットワークの主な要件

クラウドは、他のセキュリティアーキテクチャとは根本的に異なります。真のクラウドソリューションは、次の2つの重要な特性を備えています。

1.柔軟性: 需要予測ではなく、実際の使用料に基づく料金体系になっています。

2.マルチテナント: この方法によってスケールメリットが実現し、すべてのCPUサイクルが無駄なく利用されるため、価格競争力の高いサービスを提供できるようになります。

前述のアプローチとは異なり、真のクラウドソリューションは、柔軟性、冗長性、高パフォーマンスを実現するように一から設計されています。人、デバイス、または企業の周囲に境界を固定するのではなく、ユーザと連動する動的な境界を提供します。

これは、ユーザがどこに移動してもインターネットにローカルアクセスできることを意味しますが、ゲートウェイ経由で正規のトラフィックを許可するだけでなく、非正規や悪意あるトラフィックを確実にブロックする必要があります。動的な境界は、5、10、または20のゲートウェイを処理できれば実現するというものではありません。世界中の100を超えるローカルアクセスポイントを処理する必要があり、そのためには、ローカル、高速、セキュア、かつポリシーベースでのロケーションに依存しないインターネット接続を保証する、グローバルクラウドインフラを構築する必要があります。

「Zscalerは、名前に偽りのない数少ない製品の1つです。クラウドを前提に開発され、発展してきたため、サービスの管理や拡大が驚くほど簡単です。」

- Fugro社 最高セキュリティ責任者 Tony Rimmer氏

まとめ

モビリティ、クラウドアプリケーション、ソーシャルメディアの普及によって、エンタープライズネットワークセキュリティの従来の考え方は、もはや時代遅れになりつつあります。ビジネスが流動的になり、多くのモバイルユーザが存在する新しい世界では、ネットワーク境界の保護は出発点に過ぎません。100%クラウドのセキュリティプラットフォームは、今日のモバイル社会で高い競争力を維持するために必要なスケーラビリティ、高度なセキュリティ、柔軟性を備えた、経済性の高い次世代ITセキュリティです。

真のクラウドアーキテクチャであれば、グローバルにビジネスを展開する大企業のお客様であっても、今後10年間、ビジネスのニーズに合わせて環境を拡張し、まったく新しい方法で、ユーザ、デバイス、データを確実に保護できます。クラウドセキュリティは重要な戦略であり、ビジネスの差別化要因でもありますが、そのオンデマンドという特性によって、戦術的な問題解決も可能にし、さらには、データ収集ツールとしても活用できることを考えれば、さまざまな分野にクラウドコンピューティングが導入されているのも当然のことと言えるでしょう。

CISOがクラウドへの移行の評価・検討を今すぐ始めることで、常に化するセキュリティの課題を解決し、将来的なクラウドコンピューティングの導入にも備えた体制作りが可能になるはず。Zscalerにお問い合わせいただければ、クラウド対応エンタープライズへの移行を今すぐ始める方法をご紹介します。

お客様に合わせてカスタマイズしたデモで詳細をご確認いただくこともできます。また、www.zscaler.comからオンラインのライブデモやオンデマンドのWebセミナーをご覧ください。

ZSCALERについて

企業ポリシーや法規制を遵守しつつ、サイバー攻撃や情報漏えいからワールドワイドで企業・公的機関の1,500万人超の従業員の安全を守っています。受賞歴を誇るZscaler Cloud Security Platformは、あらゆるユーザ、あらゆるデバイス、あらゆる場所で、安全で生産性の高いインターネットエクスペリエンスを実現します。マルチテナントの分散型クラウドセキュリティプラットフォームを通じて、効果的にセキュリティ環境をインターネットバックボーンに構築し、世界中100カ所以上のデータセンタで運用されています。妥協を許さない卓越したプロテクション機能とパフォーマンスの元に、組織がクラウドおよびモバイルコンピューティングを存分に活用することを可能にしています。Zscalerは、オンプレミスのハードウェア、アプライアンス、あるいはソフトウェアを必要とせず、統合されたキャリアグレードのインターネットセキュリティ、APT (標的型攻撃) 対策、DLP (情報漏えい防止)、SSL復号化、トラフィックシェイピング、ポリシー管理、そして脅威インテリジェンスを提供しています。






詳細は www.zscaler.com をご覧ください。

お問い合わせ

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

SNS

 facebook.com/zscaler
 linkedin.com/company/zscaler
 twitter.com/zscaler
 youtube.com/zscaler
 blog.zscaler.com



Zscaler™, SHIFT™, Direct-to-Cloud™, ZPA™ は米国および/または他の国におけるZscaler, Inc. の商標または登録商標です。その他のすべての商標は各社に帰属します。本製品は、www.zscaler.com/patentsに掲載されている米国または米国以外の1つ以上の特許の対象となる可能性があります。