クラウドの保護：ゼロ トラスト クラウド セキュリティ

概要

不必要なアクセスは決して良いことではないため、アクセス制御は優れたセキュリティの出発点となります。アクセス レベルが過度に高いと、ユーザー (またはボット) が本来アクセスしてはならないものまで目にしてしまう可能性があるため、リスクにさらされる可能性が高くなります。最悪の場合は、エクスプロイトを使用したりデータを盗んだりできる余地を与えてしまう可能性もあります。悪意を持っていないユーザーが、アクセスできるはずのないデータを入手した場合も、権限のない者がアクセスしたものと見なされ、データ侵害通知プロトコルが実行される可能性があります。

アクセスを制限すると、攻撃対象領域が狭まるため、攻撃者が目標に到達することがはるかに困難になります。また、企業では、考えられる攻撃経路の数が減って重要な問題に集中的に対処できるようになるので、他の保護機能の効果もより高まります。たとえば、データ保護制御機能でアプリケーションへのすべてのトラフィックが検査されるときにも、その効果がより高まります。

残念ながら、クラウドではすべてのトラフィックが検査されるわけではなく、アクセス レベルが不必要に高いのが普通のことになっています。クラウドに移植または移行されるアプリケーションの数の増加に伴い、クラウド チームは適切に確立されたアクセス管理方法を実施しているものと予想されます。一方、クラウドの採用が急速に進み、さまざまなクラウド アプリケーションやプラットフォームが使用され、異なった DevOps チームがアプリケーションを構築することを考えると、クラウド アクセスの断片化が見られるのもうなずけます。クラウドの採用が拡大し、クラウド環境内のセキュリティに対する責任がさまざまな機能グループに分散するにつれて、問題はさらに悪化します。

企業ネットワークに見られた過度の信頼レベルから得られた教訓によると、ゼロ トラストの原理は有用である可能性がありますが、企業ではどのようにクラウドにゼロ トラストを実装すればよいのでしょうか。

現在のクラウド アクセスの課題

現在、特定の種類のアクセス制御を実装するシステムはいくらでもあります。問題は、それらのどれもが、多種多様なクラウド アーキテクチャにおけるアクセスに関する問題を処理するように設計されていないことです。

ネットワーク エッジでのアクセス制御

従来のアクセス制御のモデルは、リモート アクセス virtual private network(仮想プライベート ネットワーク - VPN) の場合と同様に、特定のネットワークに接続できるユーザーを単純に制限するというものです。これはプライベート クラウド (内部データ センター) 内のアプリケーションに対しては賢明な方法ですが、パブリック クラウドや Software as a Service(Software as a Service - SaaS) に使用するには非効率的なネットワーク パスです。このため、ほとんどの企業では、内部リソースへの一時的なアドホック接続にはリモート アクセス VPN を使用していますが、プライベート クラウドへのアクセスが不要な場合は完全にその使用を避けています。

アプリケーションでの認証

もう 1 つの従来のアプローチは、一元化された ID 管理と連携して、アプリケーション自体の内部ローカル認証を変更 / 置換するというものです。連携認証では、この方法で使用可能になったアプリケーションの使いやすさも大幅に簡素化されています。ただし、課題は、すべてのアプリケーションで企業 ID 管理プラットフォームがサポートされるようにできるとは限らないことです。さらに、アプリケーションへのフロントドア アクセスの安全性が確保されている場合でも、有効な資格情報を持たない第三者によるエクスプロイトや悪用から、application programming interface(アプリケーション プログラミング インターフェイス - API) などの他の経路を保護する必要があります。

CASB プロキシ

アクセスをゲーティングするもう 1 つのアプローチとして、cloud access security broker(クラウド アクセス セキュリティ ブローカー - CASB) を介してクラウド アプリケーションをプロキシする方法があります。プロキシは、ユーザーとアプリケーション間のネットワーク境界を確立し、アクセスを制限する基本的な分離を生み出します。ただし、一部の Web ベースのアプリケーションをサポートするために CASB プロキシがよく使用されますが、他のチームではサポートされていないアプリケーションを処理するために software-defined perimeter(ソフトウェア定義境界 - SDP) と VPN を展開する必要があります。

ソフトウェア定義の境界

リモート アクセス VPN の使用が制限されていることから、一部のベンダーでは、クラウドベースのアプリケーションにブローカリングとトンネリングを組み合わせて適用しています。SDP 市場では、ネットワーク分離用のプロキシの原理が、VPN 用のエンドツーエンド トンネルと融合されています。SDP 市場は、クライアントを使用してリソースにトンネリングするものと、クライアントレスでブラウザベースのプロキシを使用するものとに分断されています。そのどちらにも、サポートしているアプリケーションと、サポートしていないアプリケーションがあります。これまで、多くの SDP ベンダーは、アクセス制御機能を重視し、脅威やデータ保護についてはほとんどまたはまったく重視してきませんでした。そして、そのことがアプリケーションとユーザーの両方にリスクをもたらしています。

クラウド用のゼロ トラスト

上述のように、既存の技術の多くは、理にかなった考え方に基づいていますが、問題空間の一部しか解決していません。過去から得られた教訓を生かすならば、ゼロ トラストの原理は、より包括的なアプローチに向けた良い出発点となります。

自社のネットワークと同じようにクラウド環境でゼロ トラストを確立することによって、企業は可視性を確保し、攻撃対象領域を減らして、既知の攻撃を防御するほか、未知の攻撃を検出して防御することができます。ゼロ トラストに基づくアーキテクチャは、ユーザーとすべてのアプリケーション間の分離を維持し、ユーザーの ID を確立することで、特定のリソースにアクセスできるだけでなく脅威の阻止およびデータの移動の制御を実行できるユーザーに関するポリシーを適用します。

クラウドでゼロ トラストを実現するには、企業は以下のことができなければなりません。

- ユーザーとアプリケーションの分離
- ユーザーとデバイスの識別
- 脅威の防止とデータ保護の強化

クラウド環境におけるゼロ トラスト用の Prisma Access

Prisma™ Access(旧名 GlobalProtect™ クラウド サービス) は、企業がリモート ネットワークとモバイル ユーザーに一貫したセキュリティを提供するのに役立ちます。これは、クラウド セキュリティの世代的な前進の現れであり、クラウド提供型のアーキテクチャを使用してすべてのユーザーをすべてのアプリケーションに接続します。

すべてのユーザーが、居場所 (本社、支社のオフィス、または出張先) に関係なく、Prisma Access に接続して、クラウドとデータ センターのアプリケーションおよびインターネットを安全に使用できます。Prisma Access は、すべてのポートのすべてのトラフィックを一貫して検査し、支社 - 支社間および支社 - 本社間のトラフィックを有効にして制御するための双方向ネットワークを提供します。

このアーキテクチャは、クラウド用ゼロ トラスト実装のための適切なモデルを提供します。

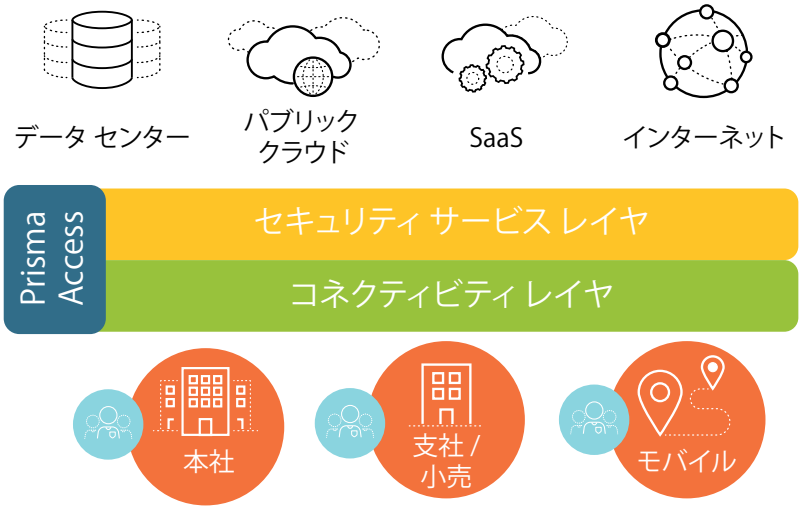

図1: Prisma Accessモデル

- **ユーザーとアプリケーションの分離 :** アプリケーションに直接接続する代わりに、ユーザーは Prisma Access に接続します。ハイブリッド クラウド アプリケーションとプライベート クラウド環境は、コネクティビティ レイヤへの IPsec トンネルを使用してオンボード化されています。
- **ユーザーとデバイスの識別 :** アプリケーション セキュリティ ポリシーの評価には、ID やグループ情報などのユーザー関連属性とともに、ホストやエンドポイント ソフトウェア設定などのエンドポイント基準を使用できます。
- **攻撃の成功を阻止 :** アプリケーションに出入りする悪意のあるコンテンツを阻止し、データの移動を制御するために、Prisma では、企業が安全でセキュアなアクセスを維持するのに役立つ、強化されたセキュリティおよびデータ保護機能を実装しています。

Prisma は、クラウドへの安全なアクセスを可能にするためにこれらの機能を実装しています。

- **すべてのアプリケーションへの制御されたアクセス :** 市販のポイント製品とは異なり、Prisma Access は、インターネット上だけでなく、パブリック クラウド、プライベート クラウド / データ センター、および SaaS のアプリケーションにも接続性と一貫したセキュリティを提供します。
- **アプリケーションへの適応型のアクセス :** セキュリティ チームは、特定のアプリケーションに対して取るべきリスク体制を確立し、コンテキスト コントロールを使用して、アクセス権を持っているユーザーとデバイスの状態を知ることができます。

- **セキュリティの可視性と分析 :** クラウド アプリケーションの使用に関する完全な可視性を維持します。Cortex ™アプリを利用して、セキュリティに関する分析を実行して、リスク要因についての洞察を得ることができます。
- **侵入されたホストからの保護 :** 誤って設定されたデバイスや侵害されたデバイスがデータにアクセスしないようにするために、エンドポイントの情報に基づいてポリシーを適用します。
- **不正な移動からの保護 :** データ保護を使用して、データとファイルの移動を制御します。App-ID ™技術ポリシーを使用することで、潜在的なリスクのある機能をブロックしながら、アプリケーションにアクセスできるようになります。

全体として、Prisma Access のこれらの機能は、クラウド アプリケーション戦略を構築するための基盤となります。一握りのアプリケーションへのアクセスのみに対処するアプローチとは異なり、Prisma Access では、ゼロ トラスト機能、脅威防御、およびデータ セキュリティを組み合わせることによって、すべてのアプリケーションを保護するためにさらなる一歩を踏み出すことができます。

将来に向けて構築

お客様のクラウド導入の進捗状況に関係なく、Prisma は以下の実現に役立ちます。

- クラウド対応のモバイル ワーカー
- クラウドに接続された支社
- ゼロ トラスト クラウド セキュリティ
- クラウドのガバナンスとコンプライアンス
- クラウドのデータ保護
- クラウドの脅威保護
- DevOps の継続的なセキュリティ

Prisma で主要なクラウド イニシアチブを確保する方法の詳細については、www.paloaltonetworks.com/prisma を参照してください。

〒 100-0011
東京都千代田区内幸町
2 丁目 1 番 6 号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
www.paloaltonetworks.jp

© 2019 Palo Alto Networks, Inc。パロアルトネットワークスは、パロアルトネットワークスの登録商標です。商標のリストについては、https://www.paloaltonetworks.com/company/trademarks.html をご覧ください。本書に記述されているその他の商標はすべて、各社の商標である場合があります。
secure-the-cloud-zero-trust-cloud-security-b-052319