AKAMAI ソリューション概要

ユーザー・アイデンティティ・アクセス管理とセグメンテーション

現代のハイブリッドデータセンター向けの追加の重要な制御レイヤー

今日の IT 環境のアタックサーフェスを縮小するためには、特定のアプリケーションに関して厳密な制御の仕組みを作成して、損害を被ることのないようリングフェンシングするだけでは不十分です。これは大きな第一歩であり、セキュリティ侵害の封じ込めやコンプライアンスなどのいくつかのユースケースにおいて大いに役立つのは確かです。ただし、ユーザー・アイデンティティ・アクセス管理をサポートするセグメンテーションソリューションがなければ、ネットワークを使用する、またはネットワークにアクセスするあらゆるユーザーに関係するセキュリティ上の盲点が組織に残ることになります。

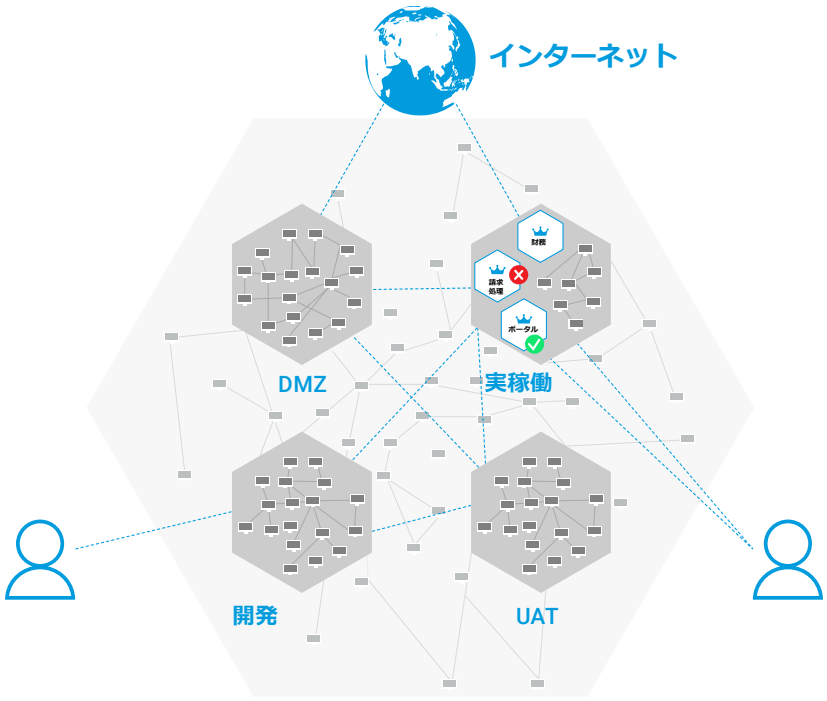
アプリケーションにセグメンテーションを適用できたら、セグメンテーションソリューションを利用して、これらのアプリケーションにアクセスできるユーザーに関するポリシーを作成し、ネットワーク上のあらゆるアーキテクチャでアプリケーションのセキュリティが確保されるようにするのが、次の重要なステップとなります。

ユースケース：ユーザー・アイデンティティ・アクセス管理のためのセグメンテーション

ユーザーアクセスの管理

Akamai Guardicore Segmentation は、Active Directory ユーザーグループを使用して、あらゆる環境からあらゆるアプリケーションやワークロードへのユーザーアクセスを制御できます。特定のユーザーグループは、特定のポートまたはプロセスを介して特定のサーバーにアクセスできますが、他のユーザーグループはアクセスできません。ユーザーグループには固有の権限がありますが、他のすべてのアクセスはブロックできます。中央集中型ファイアウォールを必要としないため、ネットワークの特定のセグメント上のワークロード間できめ細かなアクセス制御を使用できます。

ユーザーアクセス制御



ユーザーアクセス制御にセグメンテーションを活用する理由

場所にかかわらずユーザーアクセスを制御
ポリシーは、ラップトップ、デスクトップ、VDI、仮想またはベアメタルサーバー、クラウドインフラ全体で機能します。

ソフトウェア定義のセグメンテーション
ネットワークやアーキテクチャの変更、ケーブル、システムの再起動が必要なく、サーバーのダウンタイムも発生しません。

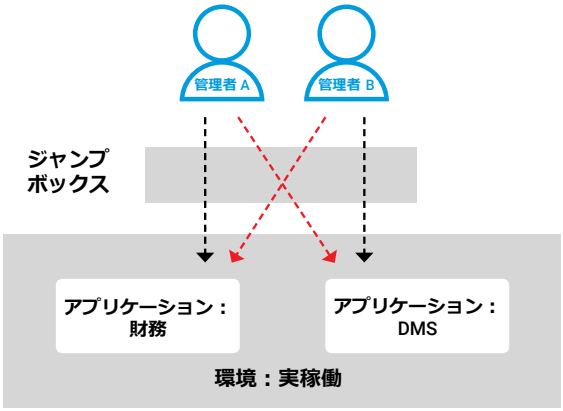
迅速で強力
ポリシーは簡単かつ直感的に作成でき、新たに開始されるセッションと実行中のセッションの両方に対して効果があります。

高いコスト効率
従来のジャンプ・ボックス・インフラで対応していた類似のユースケースと比較して、最大で 60% コストを削減できます。

Akamai

同時ユーザーアクセスの処理

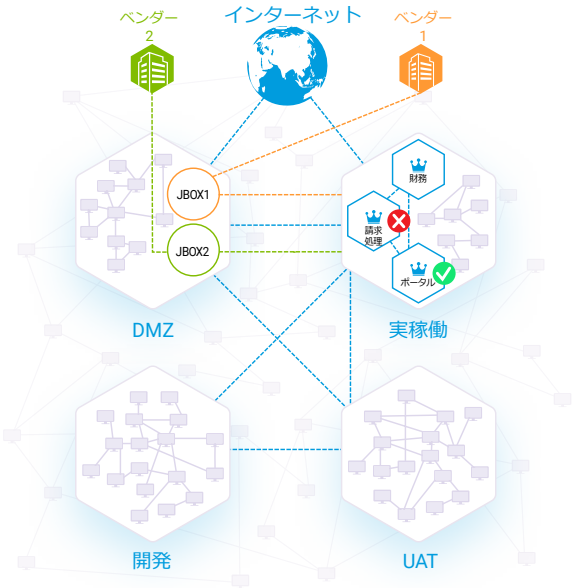
複数の管理者が同時にログインしている場合でも、管理者は同じジャンプボックスまたはターミナルサーバーを通じてさまざまなアプリケーションにアクセスできます。一方で、異なるポリシーはシームレスに機能し、アクセス権のあるユーザーを許可し、他のユーザーをブロックすることができ、それぞれのユーザー自身のサービスやアクセスには一切影響がありません。



サードパーティーのアクセスの制御

Akamai Guardicore Segmentation では、ユーザーのアイデンティティに基づき、外部ベンダーやSaaS プロバイダーなどからのサードパーティーアクセス管理を制御できます。各サードパーティー接続に関して、ユーザーグループを利用してデータセンターおよび個別のアプリケーションの両方に対して独自のアクセスポリシーを定義できるため、ユーザーが自身の役割において必要とする権限のみを付与することができます。

サードパーティーのアクセス制御



アプリケーションのセグメンテーションとユーザー・アイデンティティ・アクセス管理は、先進的なエンタープライズデータセンターを保護するための非常に効果的な組み合わせです。

連携の仕組みの詳細については、弊社エキスパートまでお問い合わせください。