

# ゼロトラスト データセンターが お客様の お城を守ります

データセンターは、企業の重要資産であり、最も機密性の高いデータとアプリケーションをオンプレミスまたはクラウドで保持します。場所を問わず、データセンターを保護することは不可欠です。ゼロトラストデータセンターの構成要素を理解し、データを安全に保つために企業を保護する安全策を講じることが非常に重要です。

**可視性の欠如**  
アプリケーションとネットワークの状態をすばやく評価し、潜在的な悪意のあるアクティビティを特定するためには、ネットワーク全体の可視化が重要です。見えないものから身を守ることはできません。

**重要資産**  
重要資産とは、オンプレミスかクラウドであるかを問わず、最もビジネスクリティカルで機密性の高いデータやアプリケーションのことで、この情報が悪用された場合、企業に壊滅的な影響を与える可能性があります。

**経路での脅威**  
脅威はさまざまなベクトルからネットワークに入り込み、その攻撃目的もさまざまです。どのようなインテント（意図）で、どのような技術を用いているかにかかわらず、適切なツールを使ってお城を守ることが重要です。

**イントラデータセンター**  
ファイアウォールは、サービスとアプリケーションのグループ間の水平（east-west）および垂直（north-south）方向の通信を保護して、サーバー間でもう1つのチェックを実行し、異なるサーバー上のすべてのリソースとアプリケーションが危険にさらされないようにします。私たちは、トラフィックが特定のアプリケーションにアクセスする方法と、特定のユーザーがそのアプリケーションにアクセスする方法を決定することができます。

**Cloud Workload Protection**  
私たちは、個々のアプリケーションを保護する必要があります。コンテナ型ファイアウォールはアプリケーションごとに展開ことができ、これがもう1つの検問所になります。重要資産のあるポイントに侵入されてしまった場合でも、攻撃を止める警備員がいます。Cloud Workload Protectionは、アプリケーションの中に存在します。重要資産が動かされると、ゲートが下がり、攻撃者を捕らえ、地下牢に追いやります。

**お城の包囲網**  
どのような対策を講じたとしても、脆弱性を悪用してお城を襲撃しようとする攻撃者は常に存在します。そのため、備えが必要です。セキュリティは、「見て、知って、行動すること」が重要です。お城を保護するためには、クライアントからワークロードまでのすべての接続ポイントに可視性、インテリジェンス、ポリシー適用を拡張して、脅威認識ネットワークを実現する必要があります。

**データセンター相互接続**  
データセンター相互接続は、データセンター間の通信のための通路です。ほとんどの企業では、複数のデータセンター環境が混在しています。クラウドとオンプレミスの環境間のトラフィックを保護するためには、堅牢なルーターを用意することが不可欠です。それにより、攻撃者がお城に侵入したとしても、すべての場所に侵入することはできなくなります。

**データセンターWANゲートウェイ**  
データセンターWANゲートウェイは、データセンターへの入り口であり、受信トラフィックと送信トラフィックをチェックするファイアウォールによって保護されており、ユーザーとデバイスがデータセンターに正しくアクセスできるようにします。お城の中に入るための検問所のように、受信トラフィックをチェックして、隠れたマルウェアが忍び込んでいないかを確認します。

**ビジネス継続性**  
企業には信頼性の高い接続が必要です。また、企業のデータセンターがどこにあっても、ビジネス継続性を維持し、質の高いエクスペリエンスとサービスへのアクセスを備えた一貫したセキュリティポリシーを確保する必要があります。保安官がデータセンター間の通路にいるように、運用管理者はオンプレミスやクラウドなど、あらゆる場所での展開においてオーケストレーションとモニタリングを提供できるようにします。

## クラウド時代の脅威認識ネットワーク

ゼロトラストデータセンターは、脅威認識ネットワークを実現し、最終的にセキュリティを向上させると同時に、複雑さを軽減し、管理を合理化します。企業のネットワークが脅威を認識できるようになれば、攻撃がより早く検知され、攻撃者がネットワーク内で足掛かりを得る可能性が低くなり、ユーザー、アプリケーション、インフラストラクチャ、そしてもちろん、企業の重要資産を保護することができますようになります。

