10 ゼロトラストデータセンターの10の要素

真のゼロトラストデータセンターとは、以下のエンドユーザーエクスペリエンスを第一に考えたデータセンターである。

- *信頼性と拡張性に優れた高速アクセス*
- *ユーザーとデバイスの保護*
- *アプリケーションとワークロードでのデータ保護*
- *ビジネスの俊敏性を加速させるセキュリティ*

10 見えないものを可視化

見えないものを守ることはできない

各環境にまたがるネットワーク全体を完全に可視化して、クライアントやワークロードなど各要素のセキュリティ状況を把握する必要があります。

9 複数ポイントでのセグメンテーション

細かく分割

ユーザー、デバイス、アプリ、ワークロードなどをきめ細かくセグメント化して制御することで、不正アクセスを防止し、防御の隙間を埋めることができます。

8 ユーザー、デバイス、ワークロードのアイデンティティ

アイデンティティはユーザーだけが持つものではない

デバイスやワークロードにもアイデンティティ（ID）があります。IDは複数の要素で構成されており、これによってネットワーク全体でいつでもリスクを特定できます。

7 場所を問わないシームレスなポリシー

どこに移動しようと、ユーザー、デバイス、アプリケーションに適用

ユーザー、アプリ、ワークロードは常に移動しています。移動先を問わずセキュリティポリシーを適用できるため、潜在的な攻撃ベクトルを抑制できます。

6 ネットワークトラフィックのインテントの把握

トラフィックの宛先や目的は？

暗号化解除を行わないトラフィックも含めて、すべてのネットワークトラフィックとその宛先について、可能な限り把握する必要があります。そのためにまずは、特定のトラフィックの指標や動作を監視します。

5 可能な箇所はすべて自動化

自動化を最大限活用！

仕事が楽になり、複数のチームで効率が向上します。自動化により、データセンターの一部で行われた変更をデータセンター全体に適用することも、攻撃への対応をインシデント化する前に行うことも可能になります。

4 すべての接続ポイントを監視かつ活用

従来の適用範囲を越えた先までセキュリティを拡張

ルーターとスイッチを活用して脅威を検知し、データセンター環境の保護を実現します。

3 基本的な脅威のブロックで効果を発揮

実のところ、既知の脅威を検知できないセキュリティテクノロジーは投資対象に値しない

データは嘘をつきません。どのセキュリティベンダーが脅威の現状に真っ向から取り組み、ネットワークへの攻撃を阻止しているのか、きちんと調べたうえでベンダーを選択してください。

2 アプリケーションの稼働時間を確保

障害の発生などあってはならない

ネットワークの稼働状況とリソースの接続状況がビジネスの成否を分けることになります。効果的なセキュリティの代償としてネットワーク障害が発生するなどということはあってはなりません。超高速のフェイルオーバーと貴社が必要とするスループットを提供する、信頼性に優れたセキュリティソリューションを選択してください。

1 前進し続ける！

決して立ち止まらない

最初からすべてを理解する必要はありません。「ゼロトラストに興味がある」出発点としては、それだけで十分です。次に、何を実装するかを選びます。そうすることで、最終的にゼロトラストデータセンターが実現します。重要なのは、決して立ち止まることなく、一歩ずつでも前進することです。

必ずできるはずです！

エッジのことを忘れずに！

あらゆるセキュリティ対策において、核となるのはデータです。データセンターを保護するための秘訣は、エッジのセキュリティを確保して、エッジにあるデータに対するアクセスを保護することです。データセンター環境内のアプリケーションやデータに対するユーザーやデバイスのアクセスを保護し、そして何よりもネットワーク全体を効果的に保護します。

JUNIPER NETWORKS

3050187-001-JP 2023年8月