最新のデータセンターにはセキュリティへの新しいアプローチが必要

→ 仮想化、クラウド、ソフトウェア定義型ネットワーキングにより、データセンターが一新

→ ワークロード、アプリケーション、各種データは今やマルチクラウドの各所に点在

→ 社外に出るユーザが増え、モバイルの利用はますます広がり、さまざまなデバイスからリソースにアクセス

→ 今日のデータセンターは非常に複雑で、組織にはセキュリティアプローチの再考が必要

セキュリティ チームは時間の 76% を、以下の分野でデータセンターの保護に費やしています。*

- サーバ（47 %）
- 顧客データ（20 %）
- エンドポイント（24 %）

保護が最も難しいのはパブリック クラウド内のデータだと答えたのは 57% **

データセンターをセグメント化済みなのは、わずか 38% *

セキュリティのリーダーは、セキュリティには人的資本の問題があると広く認めています***

グローバル セキュリティの意思決定者の 25% は、人材不足が大きな課題であり、適切なスキルを持つスタッフを見つけることに苦労しています。連携していないポイント製品が多過ぎて管理できない場合の問題はさらに悪化します。

データの盗難を決定づけるのは人的要素です****

ハッキングによる侵害の 81 % では、盗まれたパスワードや脆弱なパスワードが使用

86% は電子メール（73 %）および Web（13 %）で配布

データ ソース：
* シスコ年次サイバーセキュリティ レポート（2017 年）
** シスコ年次サイバーセキュリティ レポート（2018 年）
*** 「The Zero Trust eXtended (ZTX) Ecosystem」（Forrester 社出版、Chase Cunningham 著）
**** データ漏洩調査エグゼクティブ サマリー - フルレポート（2017 年、Verizon 社）

最新のデータ センターには 3 つの重要なセキュリティ要件があります

可視性
ユーザ、デバイス、ネットワーク、アプリケーション、ワークロード、プロセスを完全に可視化

セグメンテーション
マイクロ セグメンテーションとアプリケーションのホワイトリスト化により、攻撃者によるサーバ 間の移動を防止

脅威からの保護
マルチレイヤ脅威センサーで侵害をすばやく特定し、高速で検出・ブロックして、データの盗難や操作の中断を回避

今こそ、データ、アプリケーション、ダイナミック ワークロードを保護する新しいアプローチが必要です

革新的な新しい技術によるアプローチと最新のデータ センターのために構築された統合型アーキテクチャの登場です。次のようなメリットが得られます。

アプリケーションやマイクロ アプリケーションがデータ センター全体を移動して、トラフィックに悪意があるかどうかというコンテキストで脅威を捉えます

ネットワーク、セキュリティ、アプリケーション ポリシーの統合と自動化に対して、動的で柔軟な制御が可能です

マルチレイヤ脅威検出と緩和では、より多くの脅威をブロックし、データセンターを侵害する可能性のある脅威をすばやく緩和します

シスコはデータ、アプリケーション、ワークロードを保護し、組織の安全性とビジネスの生産性を高めます。

エンタープライズ、クラウド、データセンター全体の全ユーザとネットワーク トラフィックの完全な可視性により、インシデントを高速で検出します

データ センター内でサーバ間を移動する未承認ユーザや高度な脅威を制御し、攻撃対象領域を削減します

データ漏洩や操作の中断を迅速に特定、ブロック、対応します

シスコは、最新のデータセンターを連携して保護する革新的な新技術を開発しました

詳細はこちら

C05-740358-00 04/18