SD-WANセキュリティで解決すべき4つの課題

SD-WANの最大の課題は、
従来のセキュリティソリューションでは
不十分だということです

SD-WANの導入過程で乗り越えなければならない4つのハードルと、
導入した環境をどうすれば最も効果的に保護できるか検証してみましょう。

ハードル1 SD-WANエッジデバイスのファイアウォールの利用

ネイティブSD-WANセキュリティだけでは、大きな死角が残ります

NGFW、サンドボックス、標的型攻撃からの保護、IPS、DNSセキュリティなどの高度な脅威からの保護を備えているものはほとんどありません。

ソリューションに何を求めるか？

特性 アプリケーション/プロトコル/コンテキスト対応のクラウドベースファイアウォール

特性 すべてのユーザ/アプリ/デバイス/場所のオン/オフネットワークのトラフィックのインスペクションを実施

特性 送信先だけでなく、要求内容に基づいてアクセスを決定

ハードル2 従来のセキュリティアプローチはタスク次第という考えを捨てる

効率化を阻害する要因がいくつかあります

すべてのブランチオフィスにアプライアンスを導入すると、膨大な費用がかかるほか、セキュリティやパフォーマンスの問題も考慮する必要があります。

地域のハブにトラフィックをバックホールする方法も、レイテンシとコストの増加につながることから、正しい答えとは言えません。

ソリューションに何を求めるか？

特性 包括的なクラウド配信型セキュリティによって、すべてのユーザに同一の保護を提供

特性 SSLで暗号化されたトラフィックを含むすべてのポート/プロトコルのブレイクアウトとインスペクションを実施

ハードル3 既存のセキュリティアーキテクチャで暗号化されたトラフィックを処理しない

暗号化されたトラフィックのインスペクションが不可欠です

従来型ファイアウォールによるSSLトラフィックのインスペクションはネイティブではありません。

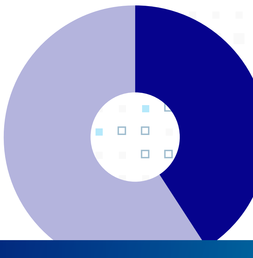
インスペクションをオンにすると多くの場合にパフォーマンスが低下することから、SSLインスペクションを回避する会社もあり、結果としてリスクが高くなります。

ソリューションに何を求めるか？

特性 SSL暗号化トラフィックをネイティブでインスペクションするプロキシベースのアーキテクチャ

特性 パフォーマンスを低下させずにすべてのトラフィックのインスペクションを実施

特性 トラフィックやユーザの増加にも柔軟に対応



41%

以上のネットワーク攻撃が、
暗号化を使用することで検知を逃れています[1]。

ハードル4 複数のセキュリティ管理プラットフォームの罠に陥らない

従来型テクノロジには多くの問題が存在します

アクティビティの収集や関連付けが困難です。

ポリシーの変更を実装するには、多くの場合、個別の管理インタフェースや手動による展開が必要です。

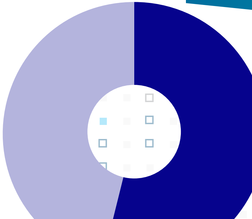
可視化やレポートをタイムリーに提供したいと考えても、すべてのブランチオフィスにアプライアンスが分散しているため、複雑な作業を要します。

ソリューションに何を求めるか？

特性 実用的な洞察を提供する柔軟なフレームワーク

特性 ログを関連付けて表示する単一のプラットフォーム

特性 一元的にポリシーを定義し、すべての場所にすぐに展開できる。



54%

の組織が、現在のさまざまな場所におけるインターネット接続を保護する方法を取ることで、テクノロジがさらに複雑化することを最大の懸念事項に挙げました[2]。

詳細は、別資料にてご確認いただけます。

ホワイトペーパー全文を読む

zscaler™

[1] Ponemon Institute「暗号化トラフィックに隠れる脅威：北米および欧州・中近東・アフリカにおける調査」2016年
[2] Network World, Inc. 100の組織のITディレクタを対象とする調査

© 2020 Zscaler, Inc All rights reserved Zscalerは、米国またはその他の国、あるいはその両方における、Zscaler, Incの商標または登録商標です。その他の商標は、所有者である各社に帰属します。

zscaler.jp