Akamai

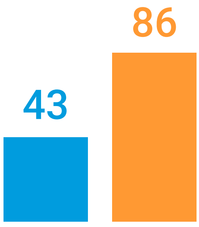
インフォグラフィック

セグメンテーションの現状 2023

導入の障害を克服することが変革に繋がる

ランサムウェア攻撃が倍増する状況で、より高度なセグメンテーションを実装した組織だけが防御を変革しています。

ランサムウェア攻撃（成功と失敗どちらも含む）の数は、過去 2 年間で倍増しました。



2021 年には平均 43 回だったが、2023 年には平均 86 回に。

93%

の IT セキュリティの意思決定者が、攻撃による損害を防ぐためにはセグメンテーションが重要であると答えています。

89%

の回答者が、マイクロセグメンテーションは組織にとって少なくとも優先事項であり、中でも 34% が「最優先事項」だと答えています。

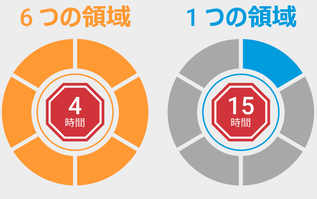
テクノロジーに対する信頼は得られているものの、セグメンテーションの導入は進んでいません。2 つ以上の重要なビジネス領域をセグメント化した組織は 2023 年で 30%（2021 年は 25%）にとどまり、2 年以上前にネットワークのセグメンテーションプロジェクトを開始した組織は 44% にすぎません。このことから、導入の取り組みが停滞していることがわかります。

ゼロトラスト・フレームワークの採用は、組織がセグメンテーションプロジェクトを開始した理由の上位に挙げられていますが、ゼロトラスト・フレームワークの導入が完全に定義され、完了していると答えているのは、5 分の 2（40%）にすぎません。

石の上にも三年、といいます。6 つの重要なビジネス領域をセグメント化してきたことが、防御の変革に繋がりました。

セグメンテーションの範囲が重要

6 つの領域をセグメント化すると、ランサムウェアによる侵害から完全な停止までを、11 時間短縮することができます。



セグメンテーションの導入を加速させるためには？

ソリューションに必須の機能：

- IT 環境全体で行われているすべての接続に関する、インタラクティブなビューを作成できる
- ソフトウェアベースで、物理的な場所に関係なく、すべてのオペレーティングシステムとデバイスに対応している
- 時間を節約し、AI を活用したポリシーの推奨事項と、すぐに使用できるポリシーテンプレートを提供している
- 最高クラスのテクニカルサポートが、導入プロセス全体を通して連携

レポートの全文をダウンロード