クラウド ワークロード セキュリティの変革

ハイブリッド クラウド環境のワークロードから出力されるトラフィックやデータの検査が可能なゼロトラストベースのアーキテクチャーが重要な理由

機能しなくなった従来のモデル

NGFW/VPN ベースのソリューションは管理が複雑なうえ、
脅威のラテラル ムーブメントを防ぐことができず、機密データの漏洩につながります。

組織がクラウド ワークロードの保護に使用する方法

クラウド ネイティブ セキュリティ ソリューション

Azure aws Google Cloud

サードパーティー ツール

ファイアウォール
VPN
TLS/SSL インスペクション
DLP

オンプレミス インフラ

オンプレミスへの
トラフィックのバックホール

従来のクラウド向けセキュリティのリスクと課題

TLS の可視性のギャップ
配布された証明書の管理、ピンニングされたワークロードの例外処理によって運用上の課題が発生し、コストの増加につながります。

脅威のラテラル ムーブメントの増加
ワークロードを発見できるネットワークベースのモデルでは、脅威が拡散しやすくなります。

複雑さとパフォーマンスの低下
仮想ファイアウォールやプロキシなどでは、セキュリティ機能ごとに仮想アプライアンスが必要となり、レイテンシーが発生します。

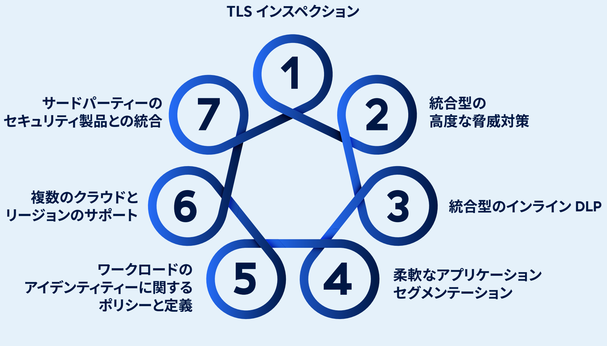
コストの増大
複数のポイント製品の利用は、高額な人件費とネットワーク セキュリティ インフラのオーバープロビジョニングにつながります。

ログとイベント管理
さまざまなクラウド環境からログにアクセスして中央の SIEM インフラに保存すると、複雑さとコストの増大を招きます。

包括的なワークロード セキュリティ モデルで実現できること

- **外部脅威の防止 / 検出**
  大規模な TLS インスペクション
- **内部脅威の防止 / 検出**
  ゼロトラストによる最小特権アクセス
- **ラテラル ムーブメントの阻止**
  ワークロード単位のきめ細かいセキュリティ ポリシー
- **マルチクラウド全体でのセキュリティの統合**
  マルチクラウドでの接続と監視のためのクラウド型ソリューション
- **開発者のためのツールの簡素化と合理化**
  コードとして提供されるセキュリティ
- **リスクとコンプライアンス要件への準拠**
  ワークロードの詳細な監視とトラフィック制御

ハイブリッド クラウドのワークロードを保護するための 7 つの重要機能



ワークロードからのエグレス トラフィックの大規模な監視と制御

セキュリティ部門とエンジニアリング部門は、
ワークロードから出力されるデータとネットワーク トラフィックを
大規模なハイブリッド環境全体で追跡する方法を決めなくてはなりません。
その意思決定に役立てていただけるよう、Zscaler は SANS と提携して、
パブリック クラウド ワークロードのエグレス トラフィックを保護するための
ソリューションの購入ガイドを作成しました。

+ 今すぐダウンロード(英語)

zscaler | Experience your world, secured.

© 2024 Zscaler, Inc.All rights reserved.Zscaler™および zscaler.com/jp/legal/trademarks に記載されたその他の商標は、米国および / または各国の Zscaler, Inc. における (i) 登録商標またはサービス マーク、または (ii) 商標またはサービスマークです。その他の商標はすべて、それぞれの所有者に帰属します。

* すべての数値は、米ドルの年間推定節約額を示しています
** サードパーティーの費用に基づく見積もりです

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com/jp