zscaler™

ソリューションの概要

Data Fabric for Security を活用した統合型リスク管理

サイロ化したポイント製品とデータでは、効果的なリスク管理に必要なコンテキストを提供できない

セキュリティ態勢を改善するには、リスクを一元的に把握する必要があります。現代の多くの組織は数十ものセキュリティツールを保有していますが、こうしたツールが生成する検出結果やデータは分離した状態で存在し、統合されたインサイトは提供されません。さらに、分散したシステムが無秩序に増加することで、侵害を検出して緩和する能力が制限されます。

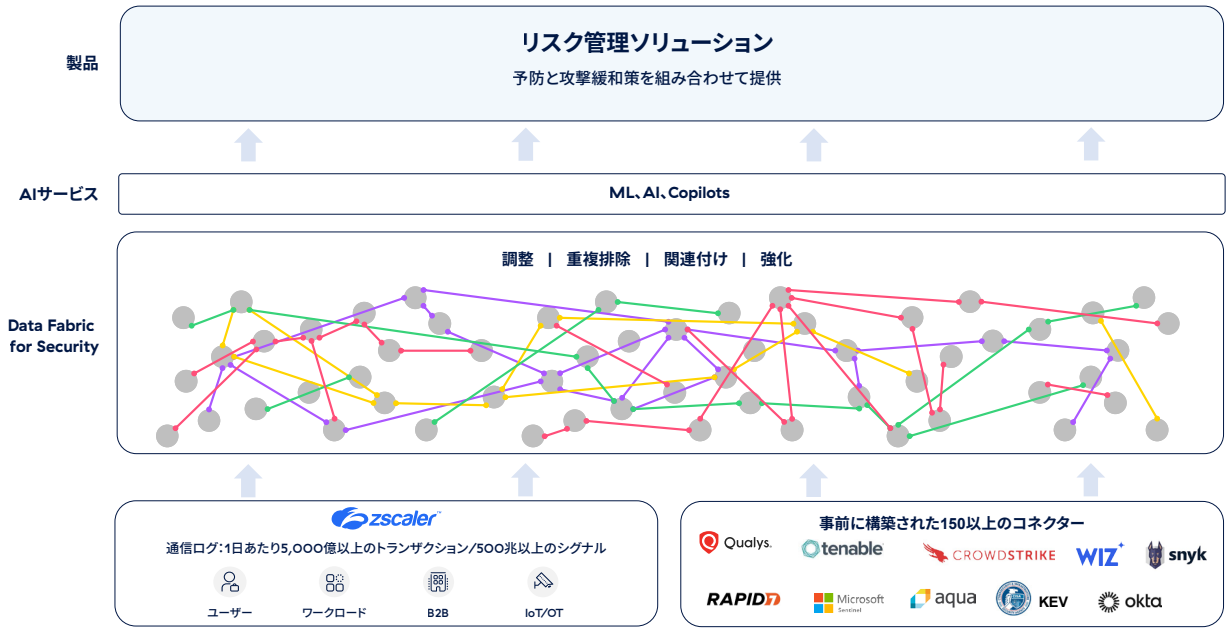
Data Fabric for Security の強力な機能

Data Fabric for Security は、セキュリティ データとビジネス コンテキストを集約して関連付けます。セキュリティ態勢に関する独自のインサイトを促進することで、悪意のある人物を早期に検出できるよう組織をサポートします。Data Fabric for Security は、Zscaler とサードパーティーの数百のソースからデータを取り込み、調整し、重複を排除して、統合された結果を生成します。その後、それらの結果を関連付けて強化し、独自のインサイトとコンテキストを提供します。これらを活用することで、以下が可能になります。

- リスクの総合的な把握
- 最初に対処すべきリスクの特定
- 侵害されたユーザーの早期検出
- 統合型の攻撃緩和策による侵害の抑制

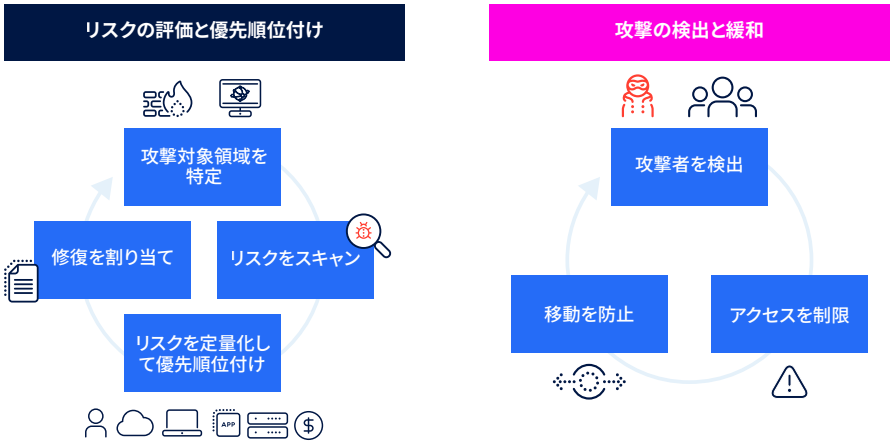
独自のセキュリティ成果を提供する Zscaler のプラットフォーム

業界初の Data Fabric for Security は、豊富なコンテキストと関連付けされた結果を提供することで、リスク管理の各ソリューションを改善します。サイバー リスクを軽減するためにこのようなアプローチを提供しているベンダーは他にありません。



広範な保護が求められる現代のリスク環境

サイバー リスクを把握し、軽減することは簡単ではありません。さまざまな予防策を展開した後でも、「侵害を想定」し、攻撃を迅速に検出して制限できるようにする必要があります。



予防と攻撃緩和策で攻撃対象領域と被害範囲を縮小

Zscaler Risk Management には、予防と侵害の早期検出を備えたツールが含まれています。リスクを最大限に軽減するには、この組み合わせは不可欠です。

予防のソリューション

Risk360

リスクの定量化と可視化

- Zscaler の構成におけるギャップを特定
- サイバー リスク定量化 (CRQ) を提供
- 経営幹部と取締役会向けのレポートとプレゼンテーションを作成

UVM

リスクの優先順位付けと修復のワークフロー

- Zscaler のサービスは不要。ただし、利用できる場合は、Zscaler からのデータをリスク関連の作業に活用可能
- 組織のリスク要因と軽減策を考慮する、カスタマイズ可能なリスク スコアリングを提供
- ワークフローを自動化して修復
- 動的なレポートやダッシュボード、プレゼンテーションに対応

EASM

公開資産におけるリスクの特定

- ドメインなどの公開資産をスキャンし、脆弱性や設定ミスを検出
- インターネットからの脅威の傾向とリスクをほぼリアルタイムで検出
- 外部資産における脆弱性の重大度を評価し、アプリケーションとサーバーに継続的にマッピング

攻撃緩和策のソリューション

デセプション

悪意のあるユーザーを特定するハニーポット

- 内外の悪意のあるユーザーを特定
- 誤検知が少なく高精度な結果を提供
- ZIA/ZPA ポリシー、エンドポイントの隔離、SOC アラートによる封じ込めを実行

Breach Predictor

攻撃の早期検出とパス分析

- Zscaler のログを活用し、侵入の初期の兆候を検出
- ML をログ データに適用してパターンに一致するものを見つけ、潜在的な攻撃経路を特定
- これまでに確認された一連のステップに基づいて攻撃の可能性を予測

アイデンティティーの保護

AD のリスクと悪意のあるユーザーの検出

- Active Directory の設定ミスや公開された資格情報を検出
- DCSync、DCShadow、Kerberoasting などの攻撃を実行している悪意のあるユーザーを特定
- ZPA、EDR、SIEM を活用して侵害されたユーザーを封じ込め

+1 408.533.0288
Zscaler, Inc. (HQ)
120 Holger Way
San Jose, CA 95134
zscaler.jp