Asset Exposure Management: 正確で実用的な CAASM のインサイト

すべての資産を把握し、ギャップを修正しながらリスクを低減

ビジネス課題

セキュリティ部門は、複数の異なるシステムの情報を調整し、資産の正確なインベントリーを作成するために膨大な時間を費やしています。しかし、こうした懸命な努力にもかかわらず、資産のリストの完全性や正確性は依然として不十分であり、リスク評価に深刻な悪影響を与えています。さらに、欠落している情報や誤った情報を特定した際、現在のツールではデータの更新が非常に困難です。ほとんどの組織は、以下のような重要な点を把握できていません。

- 実際に持っている資産の数
- 使用中の CMDB の精度
- 特定の資産を修復するためのチケットを割り当てるべき担当者
- 重要資産に適用されている保護のレベル
- 各資産のユーザー、地域、部門など
- EDR のような保護ソフトウェアが展開されていない資産

従来の CAASM とは根本的に異なるアプローチで すべての資産に関する高精度の「ゴールデン レコード」を取得

Zscaler Asset Exposure Management は、業界で最も完全で正確かつコンテキストが豊富な資産インベントリーを提供します。特許取得済みの Data Fabric for Security によるデータの関連付けを活用し、Zscaler 独自の CAASM アプローチによって、資産管理のギャップの特定、CMDB 管理の自動化、リスク軽減のためのワークフロー生成、資産のリスク軽減を実現します。これは資産に関する唯一の「真実」となるソースとして機能し、セキュリティ部門や IT 部門などがセキュリティとコンプライアンスの向上に活用できるほか、継続的な脅威エクスポージャー管理 (CTEM) ソリューションの基盤にもなります。

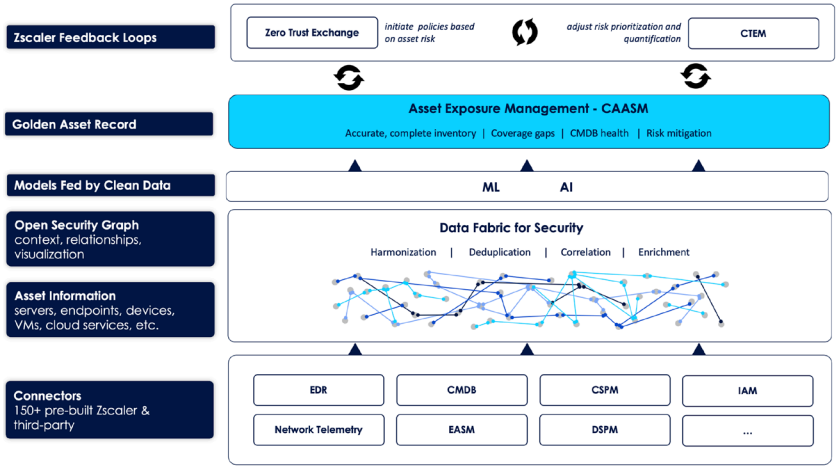
- **信頼できる資産インベントリーの構築**
  多数のソース システムにわたる資産情報を統合し、包括的で正確なインベントリーを作成します。
- **資産管理のギャップの特定と解消**
  資産の詳細を関連付けて、設定ミスや不足している制御を特定します。
- **組織のリスクの最小化**
  リスク軽減ポリシーを有効にし、ワークフローを割り当てて追跡しながら、CMDB を自動で更新します。
- **効果的な CTEM プログラムの推進**
  豊富で完全な資産情報を活用して、エンドツーエンドのエクスポージャー管理プログラムを強化します。

©2025 Zscaler, Inc. All rights reserved.

仕組み

効果的な資産エクスポージャー管理には、これまでサイロ化していた無数のデータ ソースを発見し、関連付けることが求められます。Zscaler は、サイバー資産アタック サーフェス管理 (CAASM) のスケーラビリティーと有効性を根本的に変革するデータ ファブリックの新たな活用方法を開発しました。

Zscaler Data Fabric for Security は、150 以上のセキュリティ ツールとビジネス システムで得られた資産情報のシームレスな集約と関連付けを可能にします。これによって、組織は攻撃対象領域に関する理解を深め、管理できます。膨大なデータ ポイントを調整、重複排除、関連付け、強化することで、資産、制御、ギャップ、設定ミスを詳細に把握することが可能です。また、Zscaler の広範なエコシステム内のフィードバック ループによって、これらの資産エクスポージャーを自動的に軽減する能力がさらに強化されます。



詳細はこちら：zscaler.com/jp/caasm

以下のような機能を通じて、資産の攻撃対象領域を削減します。

- **重複排除された統合資産インベントリーの構築**
  エンドポイント、クラウド リソース、ネットワーク デバイスなど、すべての資産を包括的に可視化します。複数のソースからの重複データの排除、関連付け、資産情報の統合を継続的に実行することで、資産の攻撃対象領域を完全に把握できます。
- **コンプライアンスの問題や設定ミスの 特定と追跡**
  潜在的なコンプライアンスの問題や設定ミス (EDR が展開されていない資産、古いバージョンのエージェントなど) を簡単に特定し、それらを実行可能なタスクに変換してセキュリティ態勢を強化します。
- **CMDB の精度の向上**
  CMDB の正確性と完全性を強化できます。CMDB に登録されていない資産、所有者や位置情報などが不明の資産を特定します。資産管理部門向けのワークフローを作成することで、資産情報を完全かつ正確に保ちます。
- **効率的なリスク軽減策の推進**
  リスクを軽減するためのポリシー調整やその他の制御を実施します。ワークフローを有効にしてポリシー違反を所有者に割り当て、リスク軽減の進行状況を追跡し、CMDB を自動更新して正確性と完全性を確保します。
- **堅牢なレポートとダッシュボードによる部門間の連携強化**
  事前に構築された指標とカスタムの指標を集めたライブラリーを活用し、CMDB の健全性とコンプライアンスに対応したダッシュボードとレポートを生成します。

zscaler™ | Experience your world, secured.™

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SASE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

© 2025 Zscaler, Inc. All rights reserved. Zscaler™、Zero Trust Exchange™、Zscaler Internet Access™、ZIA™、Zscaler Private Access™、ZPA™、**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。

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