

正確で実用的な資産エクスポージャーのインサイト

©2025 Zscaler, Inc. All rights reserved.

ソリューションの概要

サイバー資産アタック サーフェス管理 (CAASM) が依然として難しい理由

正確な資産インベントリーの維持は、物理と仮想のいずれでも問題が絶えません。IT 部門やセキュリティ部門は、スプレッドシートでの資産の追跡に何時間もかけることになるため、これらの資産がもたらすリスクの評価と修復作業の優先順位付けが難しくなっています。特に、コンプライアンス違反が多額の罰金につながる可能性のある規制の厳しい業界では差し迫った問題です。



組織は多数のセキュリティ ツールと IT ツールを所有しており、平均で 60 ～ 75 種類に上ります。



組織が管理するサイバー資産の数は、毎年平均 133% 増加しています。



資産情報は複数のツールに分散しているため、正確な最新の資産インベントリーの作成は困難です。



構成管理データベース (CMDB) を最新の状態に保つのは難しく、不完全かつ不正確な場合がほとんどです。



資産管理のギャップをプログラムで特定して修正するには、統一された包括的な資産インベントリーが不可欠です。



組織には、資産リスクに基づいて自動修復ワークフローやポリシー調整を行う能力が不足しています。

大量の資産をすべて把握するのは極めて困難

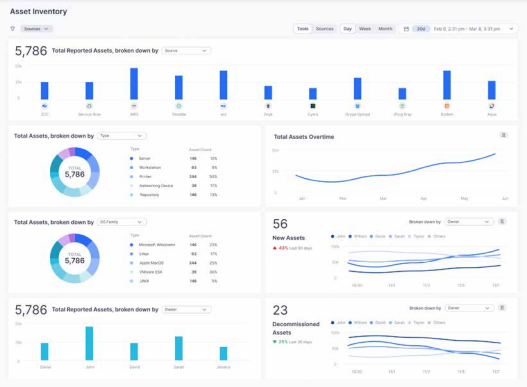
- 実際に所有している資産の数
- 既存の CMDB の精度
- 特定の資産を修復するためのチケットを割り当てるべき担当者
- EDR のような保護ソフトウェアが展開されていない資産
- サポートが終了しているソフトウェアを実行している資産
- リスクの高い資産から主要アプリケーションに接続しているユーザー
- 重要資産に適用されている保護のレベル
- 各資産のユーザー、地域、部門など
- ポリシーを順守している資産の割合

©2025 Zscaler, Inc. All rights reserved.

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 によって実現されるデータの関連付けを活用する、Zscaler 独自の CAASM アプローチで、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、資産リスクの軽減が可能になります。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。

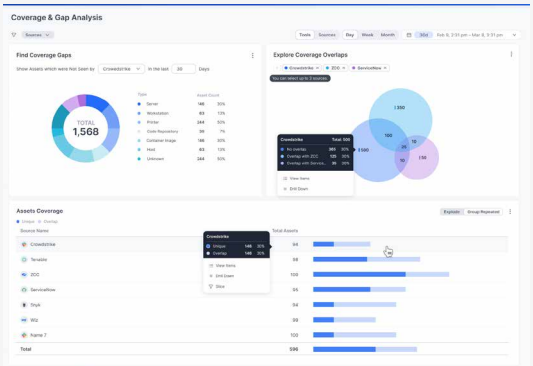
Zscaler Asset Exposure Management は包括的な資産リスク管理を提供するため、組織は次のことを実現できます。



正確な資産インベントリーの作成

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。

- Data Fabric for Security では 150 以上のコネクターを活用
- 異なるツールから報告された資産を統合
- 資産間の関係を視覚的に表示
- すべてのデータを関連付けて、資産の全体像を可視化

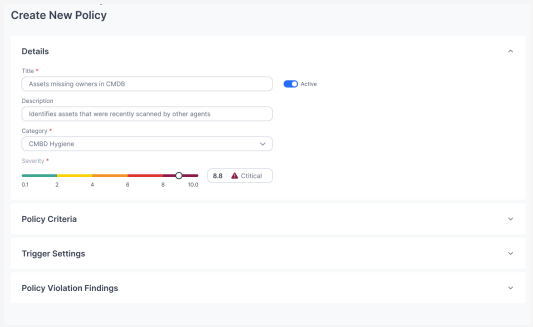


管理範囲のギャップの特定

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。

- 適切なセキュリティ対策が実施されていない資産を特定
- 異なるツール間で矛盾する資産の詳細にフラグ付け
- アクティブでない資産や廃止された資産を特定するための条件を定義
- 監査が行われる前に潜在的な規制上の問題を確認

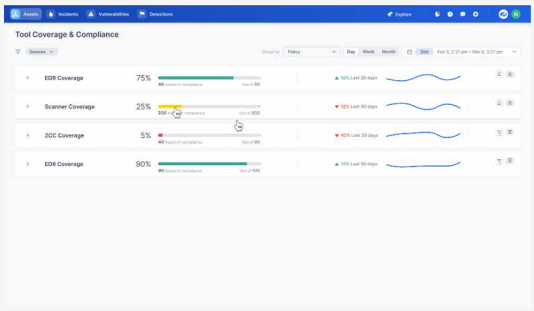
©2025 Zscaler, Inc. All rights reserved.



CMDB の精度の向上

CMDB を自動で更新し、システム間のデータ不一致を修正することで、データの保護管理を強化します。

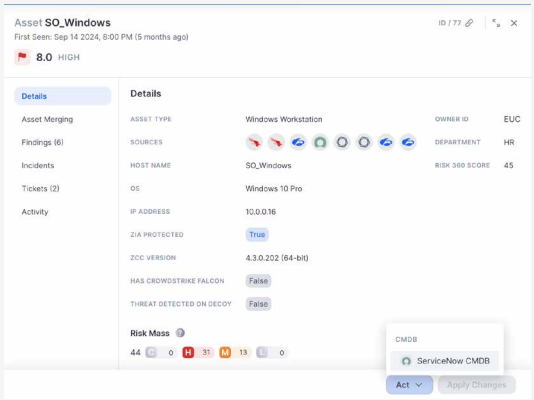
- すべての既知の資産を CMDB に記録
- ネットワーク トラフィックで確認された、未知または管理されていない資産を特定
- 重要な要素 (ドメイン、シリアル番号、所有者、「最も重要」 の指定、部門、地域など) が CMDB に含まれるようにサポート
- CMDB を自動的に更新するワークフローを構築



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

事前構築済みおよびカスタムのダッシュボードとレポートのライブラリーを活用することで、プログラムの健全性などの指標を表示します。

- すぐに利用可能な資産に関する堅牢なダッシュボードとレポートを提供
- 組織独自の要件に合わせてダッシュボードを設計し、必要なデータを測定
- あらゆるデータ ポイントや広範なポリシーでレポートを作成することで、KPI を追跡
- ポリシーごとにコンプライアンス態勢を追跡し、部門や部署、製品、地域などのカテゴリーに分類



効率的なリスク軽減策の推進

自動修復ワークフローとポリシー調整を実行することで、リスクの高い資産に関連付けられたユーザーのアクセスを制限し、リスクを軽減します。

- CMDB を自動更新し、欠落している資産や要素を追加
- リスクの高い資産に対して組み込み型またはカスタムのアクセス ポリシーを実行
- チケット発行システムから自動修復ワークフローを開始
- ポリシー違反を適切な所有者に割り当て、実用的な情報を提供

©2025 Zscaler, Inc. All rights reserved.

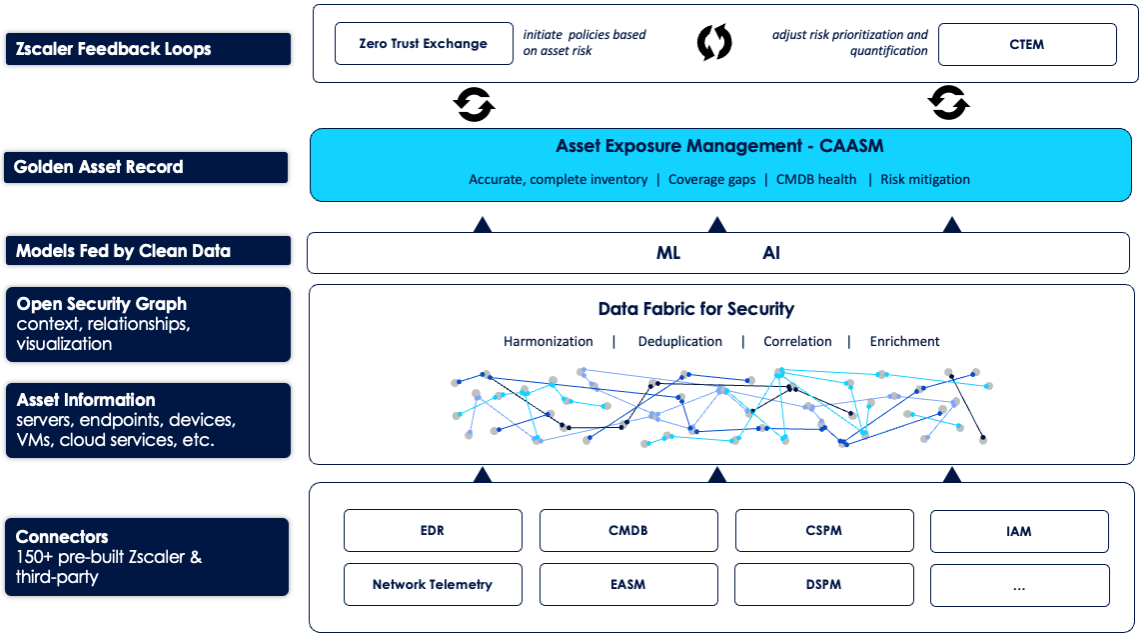
ソリューションの仕組み

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、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。

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、さらに他のアプリケーションやフラット ファイルのデータを取り込む AnySource コネクターから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。Data Fabric により、これらの膨大なデータ ポイントが調整、重複排除、関連付け、強化されるため、資産だけでなく、制御、ギャップ、設定ミスも詳しく把握できます。

Data Fabric for Security がすべてのセキュリティ ツールと IT ツールからのデータを関連付け、資産の「ゴールデン レコード」を作成すると、Zscaler Asset Exposure Management アプリケーションは、ビジネス ルールに基づいてツールの資産管理のギャップや設定ミスを特定します。たとえば、米国のすべてのノートパソコンでは CrowdStrike を実行し、ヨーロッパのすべてのノートパソコンでは SentinelOne を実行するというポリシーが規定されている場合、Zscaler Asset Exposure Management は、誤ったツールがインストールされていたり、重複していたりするエンドポイントや、ツールがまったくインストールされていないエンドポイントを特定します。

アウトバウンド統合 (「アウトグレーション」) では、任意の結果でポリシーを開始できます。たとえば、双方向チケットの自動発行、CMDB 更新の開始、Zscaler ZIA または ZPA のポリシー開始により、ユーザーのマシンが組織のポリシーに準拠していない場合や危険な振る舞いをしている場合にアクセスを制限できます。



Zscaler Asset Exposure Management の詳細は、**https://www.zscaler.com/jp/products-and-solutions/caasm** から CAASM のデモをご依頼ください。

zscaler™ | Experience your world, secured.™

Zscaler について
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 SSE 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