データシート

Zscaler ITDR™

アイデンティティーファーストのセキュリティで ゼロトラストを強化

Zscaler ITDR (アイデンティティー脅威の検知と対応) は、資格情報の窃取や権限の悪用、Active Directory への攻撃、リスクの高い権限付与などのアイデンティティーベースの攻撃を検知し、防御します。

アイデンティティーが新たな攻撃対象領域に

多くのサイバー攻撃者が、高度な手口を用いてアイデンティティーとアイデンティティー システムを標的にし始めたことで、アイデンティティーベースの攻撃は増加の一途をたどっています。こうした状況から組織を守るには、攻撃者による企業のアイデンティティーの悪用や窃取を検知できる機能が必要です。従来の脅威検知技術やアイデンティティー システムは、アイデンティティーベースの脅威に対応するよう構築されていないため、十分な効果を発揮できない場合が少なくありません。Zscaler ITDR は、アイデンティティーやアイデンティティー インフラ (オンプレミスの Active Directory) を標的とするサイバー脅威のリスクを軽減します。

Zscaler ITDR

Zscaler ITDR は Active Directory をモニタリングして、権限昇格や水平移動のリスクを高める設定ミスや脆弱性を確認するとともに、アイデンティティーを保護しながら、アイデンティティーの攻撃対象領域を広範囲に可視化することで、アイデンティティーベースの攻撃をリアルタイムで通知します。Zscaler ITDR は資格情報の窃取、多要素認証の迂回、権限昇格戦術といったアイデンティティーベースの攻撃を検知して阻止します。

メリット

- **リアルタイムでアイデンティティー脅威を検知：**アイデンティティー システムでは、構成や権限の変更が常に行われます。リアルタイムのモニタリングで新たな脆弱性、リスク、問題に関するアラートを受信できます。
- **アイデンティティーの攻撃対象領域を削減：**可視化して、漏洩の原因となる設定ミスや危険な権限を修復します。
- **アイデンティティー攻撃のリスクを軽減：**GPP パスワードの漏洩や制約のない委任、古いパスワードなど、新たな攻撃経路になり得る危険な構成を検出します。
- **迅速な調査と対応：**アイデンティティー評価で生成されたリスク スコアに基づいて、セキュリティ部門がアラートの調査に優先順位を付けられるようにします。
- **修復を合理化：**セキュリティ部門は、動画チュートリアル、スクリプト、コマンドとともに、Zscaler ITDR のステップバイステップの修復ガイダンスを活用して、対応を迅速化できます。
- **簡単な展開：**追加の VM を必要とすることなく、同じ Zscaler Client Connector が新たなセキュリティ レイヤーを提供し、アイデンティティーベースの脅威を阻止します。

5/10

Active Directory 攻撃を受けた組織の割合

出典：EMA

80%

近年の攻撃の中でアイデンティティーが狙われた割合

出典：Crowdstrike

90%

AD に関係した Mandiant の IR サービスの割合

出典：Dark Reading

Zscaler ITDR の仕組み

Zscaler ITDR は、アイデンティティー セキュリティにロータッチでシンプルなアプローチを採用しており、ユーザーとアプリケーション、ユーザーとリソースの間の接続を安全に仲介する統合エージェントの Zscaler Client Connector に組み込まれています。

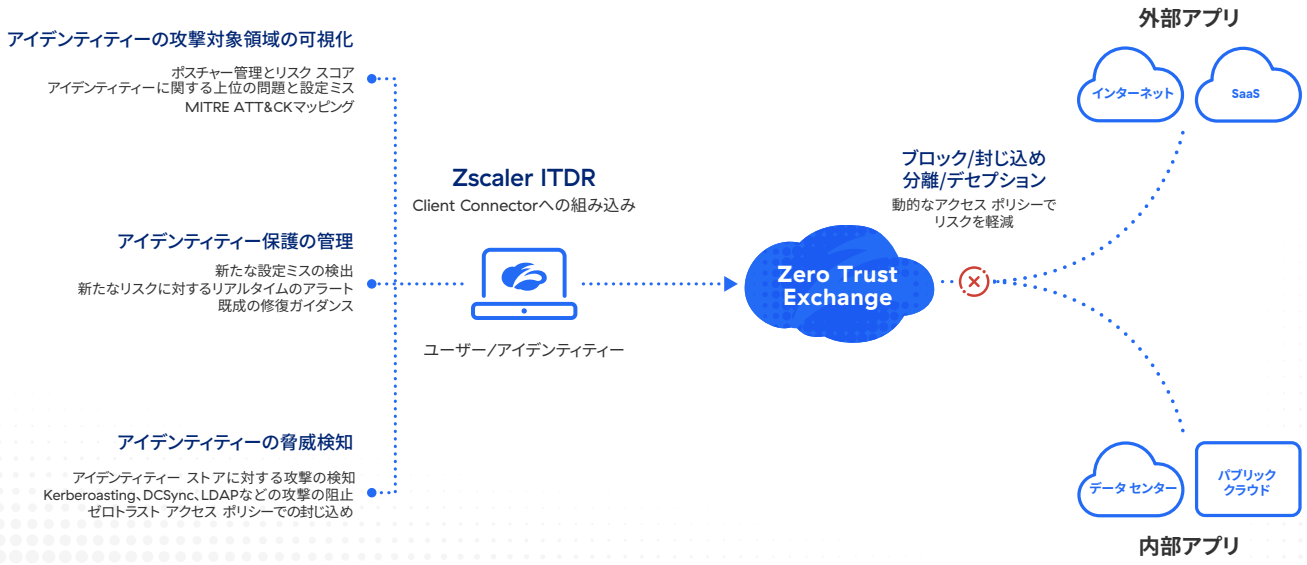
Zscaler ITDR には 3 つの機能が備わっています。

- アイデンティティーの攻撃対象領域の可視化
- アイデンティティーの変更検知
- アイデンティティーの脅威検知

攻撃対象領域の可視化

Zscaler ITDR は、LDAP クエリーを実行してアイデンティティー ストアにあるスキーマ、ユーザー、コンピューター、OU、その他のオブジェクトのマップを作成することで、Active Directory を監査します。その後、これらのオブジェクトに対してチェックを行い、Active Directory 内に存在する設定ミスや脆弱性を検出します。

- Active Directory を評価するには、ドメインに参加している Windows マシンにインストールされた Client Connector 上で Zscaler ITDR を実行する必要があります。
- セキュリティ部門はアクセスする Active Directory ドメインを指定し、スキャンを実行する Client Connector がインストールされたマシンを選択して、スキャンを設定します。
- 評価が完了するまでの時間は Active Directory の規模に応じて異なりますが、15 ～ 30 分程度です。
- 評価が終了すると、結果はダッシュボードに表示されます。
- 評価には、ドメイン リスク スコア、修復を優先すべき重点領域、最もリスクの高いユーザーとコンピューターのリスト、重大度とリスク分類の基本的な分析、MITRE ATT&CK キル チェーン マッピング、検知された設定ミスすべてのリストが含まれます。



各設定ミスに対し、ソリューションからは以下が提供されます。

- リスク分類
- 重大度
- 修復作業
- MITRE ATT&CK ID および戦術
- 問題点の説明
- 想定される影響
- 影響を受けるユーザー、コンピューター、オブジェクトのリスト
- 修復ガイダンス
- 動画チュートリアル
- スクリプト
- コマンド

アイデンティティーの変更検知

評価が構成されると、セキュリティ部門は Active Directory ドメインの変更検知をオンにできます。変更検知によって、Active Directory のセキュリティ態勢に影響を与える設定がほぼリアルタイムで表示されるため、セキュリティ部門とディレクトリー管理者が迅速に対応できるようになります。

- Zscaler ITDR は、Active Directory に対して一連の優先度の高い設定チェックを実行します。
- このチェックでは、敵対者に悪用される可能性が最も高い問題の検出に範囲が絞られます。
- このチェックは、指定されたドメインの Client Connector がインストールされたエンドポイントから 15 分ごとに実行されます。
- 変更は、良い影響または悪い影響があるとマークされます。
- 良い影響とは、問題が解決されたことを意味します。
- 悪い影響とは、潜在的な問題が発生していることを意味します。

アイデンティティー脅威をリアルタイムで検知

Zscaler ITDR は、アイデンティティーの悪用や窃取につながる動きを SOC 部門や脅威ハンターに警告する脅威の検知機能を備えています。

この機能は、指定された Client Connector がインストールされたマシン上のエンドポイント ポリシーとしてオンにできます。

- セキュリティ部門は脅威検知ポリシーを有効にすることで、システム上のイベントを監視し、パターンを分析して選択した脅威ベクトルの兆候を特定できるようになります。
- DCSync、DCShadow、Kerberoasting、セッション列挙、特権アカウント アクセス、LDAP 列挙などの検知機能を利用できます。
- セキュリティ部門は、指定されたエンドポイントで検知機能のすべてをオンにするか、組み合わせてオンにするかを選択できます。
- パターンが検出されると、Client Connector は脅威が検知されたことを Zscaler ITDR に通知します。
- このプラットフォームは、脅威シグナルをユーザーに関連する情報で強化して、調査を実行します。
- セキュリティ部門は、Zscaler ITDR でオーケストレーション機能を構成して、アラートから修復への転送までの自動化されたアクションを実行できます。

主なユース ケース

アイデンティティーの攻撃対象領域の可視化

Active Directory の継続的な評価により、総合的なリスク スコア、設定ミスと脆弱性のリスト、そしてそれらの問題を修正するための修復ガイダンスが提供されます。

- アイデンティティー態勢の定量化と追跡のための総合的なリスク スコア
- アイデンティティーに関する上位の問題と最もリスクの高いユーザーやホストをリアルタイムで表示
- MITRE ATT&CK マッピングでセキュリティの死角を可視化

アイデンティティー保護の管理

Active Directory に新たなリスクが発生するとすぐにアラートと通知を送信し、リスクのある構成と権限の変更をリアルタイムで可視化します。

- 新たな脆弱性と設定ミスを迅速に特定
- アイデンティティー ストアに生じた新たなリスクに対するリアルタイムのアラート
- 修復のための既製のガイダンス、コマンド、およびスクリプト

アイデンティティー脅威の検知と対応

アイデンティティーへの主な攻撃に対するリアルタイムの脅威検知機能です。

- アイデンティティー ストアに対する攻撃を検知
- Kerberoasting、DCSync、LDAP 列挙も検知
- ゼロトラスト アクセス ポリシーを使用した組み込みの封じ込め

他製品との主な違い

Client Connector への組み込み

Zscaler ITDR は Zscaler Client Connector に組み込まれているため、新しい機能や保護をすぐに使用できます。ユーザーをインターネットやアプリケーションに安全に接続する同じエンドポイント クライアントが追加のセキュリティ機能を提供し、アイデンティティー攻撃のリスクを軽減します。

Zero Trust Exchange との統合

Zscaler Identity は、Zscaler Zero Trust Exchange プラットフォームとシームレスに統合して、アイデンティティーベースの脅威に対する優れた検知と対応を提供します。アイデンティティー攻撃が検知されると、Zero Trust Exchange はアクセス ポリシー制御を動的に適用して侵害されたユーザーをブロックします。

シームレスな統合

CrowdStrike、Microsoft Defender、VMware CarbonBlack などの EDR、およびすべての主要な SIEM を含む緊密な統合により、調査と対応を強化します。

Zscaler ITDR でセキュリティ態勢を強化

アイデンティティー脅威に対する防御

アイデンティティーの可視化はアイデンティティーベースの脅威を検知するうえで不可欠です。Zscaler ITDR は、IT 環境全体のアイデンティティーベースのインシデントや異常を詳細に可視化することで、アイデンティティーベースの攻撃を未然に防ぎます。

Active Directory 攻撃の検知

Active Directory は、頻繁にアイデンティティー攻撃の標的にされています。Zscaler ITDR は、AD や Azure AD に脆弱性や設定ミス、危険な構成などがないかを継続的にモニタリングします。

資格情報の悪用や窃取の防止

攻撃者は盗んだ資格情報で Active Directory を攻撃し、権限を昇格させて水平移動します。Zscaler ITDR は資格情報の不正使用を検知して、資格情報が盗まれたり、悪用されたりするのを防ぎます。

水平移動の阻止

Zscaler ITDR は、水平移動するための攻撃経路を作り出す設定ミスや公開された資格情報を特定し、境界ベースの防御をすり抜け、環境内を水平に移動しようとする攻撃者を阻止します。

Zscaler ITDR は、運用やリソースの負荷を増加させることなく、ゼロトラスト プログラムの可能性を高める強力な機能を提供します。

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.jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

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