Zscaler Deception

既存のセキュリティ制御を回避する攻撃を検出

データシート

Zscaler Deception は、Zscaler Zero Trust Exchange に統合された脅威検出プラットフォームであり、デセプション技術を活用して高度な脅威を特定します。この統合機能はデコイやハニーポットを設置することで、既存の防御をすり抜けたネットワーク内の高度な脅威を検出します。Zscaler Deception により、侵害されたユーザーの特定、ラテラル ムーブメントの阻止、人為的なランサムウェアやハンズオンキーボード攻撃、サプライ チェーン攻撃、悪意のある内部関係者からの防御が可能になります。

現代の組織が抱える主なセキュリティ課題

1. **侵害されたユーザー：**フィッシング攻撃やダーク Web 上の攻撃ツールによって認証情報は日常的に盗まれており、アイデンティティー侵害は深刻なセキュリティ リスクとなっています。攻撃者が信頼されたアイデンティティーを乗っ取ると、そのアイデンティティーを悪用して組織の IT 資産にアクセスします。このような攻撃では、正規のアクセス権が使用されているように見えるため、検出が非常に困難です。

2. **ラテラル ムーブメント：**現代のネットワークは非常に複雑で、可視性が制限されています。信頼されたアイデンティティーを入手した攻撃者は、この可視性の欠如を悪用して水平に移動し、価値の高い標的を発見します。攻撃者は平均 280 日もの間ネットワーク内に潜伏するとされており、ラテラル ムーブメントは攻撃全体の中で最も長期間に及ぶフェーズとなっています。

3. **生成 AI アプリに対する攻撃：**生成 AI チャットボットや生成 AI アプリケーション、LLM API は攻撃者の新たな標的となっており、プロンプト インジェクション、データ ポイズニング、ジェイルブレイク、敵対的サフィックス、学習データの抽出などの攻撃が急増しています。これらの侵入後の攻撃は従来の脅威検出制御では検知が難しく、ラテラル ムーブメントや生成 AI インフラの悪用、さらにはデータ窃盗といった深刻な被害へと発展する可能性があります。

デセプション プラットフォームを使用することで、ランサムウェア キルチェーンの早期の段階である「初期侵入」フェーズで攻撃を特定できます。エンドポイント デコイは、ランサムウェア キル チェーンの各段階でファイル暗号化の試みや認証情報の窃取といった攻撃を検知し、エンドポイントを効果的に保護し ます。

GARTNER

Zscaler Deception の主な特長

- **侵害発生前の攻撃の検出**
  攻撃者が組織の環境を偵察している段階でアラートを発信します。これらの脅威をブロックし、テレメトリー データを活用して相関分析を行い、環境内で攻撃者の活動がないかを確認します。

- **侵害されたユーザーの検出**
  デコイ アプリケーションに偽のパスワード、Cookie、セッション、ブックマークを仕込み、攻撃者がこれらを使用した際に侵害されたユーザーを検出します。

- **窃取された認証情報の使用の特定**
  脆弱なテスト環境用アプリケーションや VPN などのリモート アクセス サービスを模倣したデコイ Web アプリを設置し、窃取された認証情報を使用してログインしようとする攻撃者をあぶり出し、阻止します。

- **権限昇格の検出**
  環境を侵害し、Active Directory を列挙して権限昇格のために価値の高い標的を見つけようとしている攻撃者を検出してブロックします。

あらゆる角度から標的型脅威を検出する包括的なアプローチ

Zscaler Deception は IT 環境にデコイを配置することで、攻撃者を検出してその活動を妨害し、重要な資産へのアクセスを阻止します。

プライベート脅威インテリジェンスという独自のアプローチで、他社にはない形態のデセプション防御を実現する唯一のベンダーです。

GARTNER

デセプションを検出または回避しようとする攻撃者を積極的に検知して対処します。

GARTNER

© 2025 Zscaler, Inc.All rights reserved.

- **ラテラル ムーブメントの検出**
  ネットワークにデコイのサーバー、アプリケーション、データベースを配置し、ラテラル ムーブメントを試みる攻撃者を検知してブロックします。

- **クラウド攻撃の検出**
  S3 バケットや IAM キーなどにアクセスし、AWS や Entra のクラウド ワークロードを狙う攻撃者を検出します。高精度のアラートにより、クラウドでのラテラル ムーブメントや悪用を阻止します。

- **ランサムウェアの阻止**
  環境に設置されたデコイが、キル チェーンのあらゆるフェーズでランサムウェアを検出して減速させ、活動範囲を制限します。

- **生成 AI アプリに対する攻撃の検出**
  プロンプト インジェクション、データ ポイズニング、ジェイルブレイク、敵対的サフィックス、学習データの抽出などの高度な攻撃手法を用いて、チャットボットや API を含む生成 AI アプリケーションを悪用しようとする攻撃者を検出します。

機能

- **生成 AI デコイ**
  デコイ チャットボット、デコイ LLM API、適応型デコイ、デコイ エージェントを活用し、環境内の生成 AI インフラを標的とする攻撃者を検出します。

- **脅威インテリジェンス デセプション**
  インターネットからアクセス可能なデコイを使用し、特定の組織を狙う侵害前の脅威をヒューリスティックに検知します。

- **エンドポイント デセプション**
  エンドポイントに偽のファイル、認証情報、プロセスを仕掛けて攻撃者を誘い込むことで、実際の資産を保護します。

- **クラウド デセプション**
  デコイの Web サーバー、データベース、ファイル サーバーを設置し、クラウド環境でのラテラル ムーブメントを検出します。

© 2025 Zscaler, Inc.All rights reserved.

- **ThreatParse**
  わずか 2 回のクリックで自動的にフォレンジック調査と根本原因分析を行い、ログから重要な情報を抽出します。

- **アプリケーション デセプション**
  SSH サーバー、データベース、ファイル共有などのサービスをホストするデコイのサーバー システムを展開します。

- **Active Directory デセプション**
  Active Directory 内に偽のユーザー アカウントを作成し、攻撃者による列挙や悪意のあるアクセスを検出します。

- **RDP のデコイ**
  リアルで高度にインタラクティブな OS 環境を利用して、攻撃の可視性を高めます。

追加機能

- **早期警告システム**
  組織的なランサムウェア攻撃者や APT グループなどの高度なサイバー犯罪者が偵察を行っている段階で、警告を発信します。密かに行われる侵入前の偵察活動は境界デコイによって検知されます。

- **Active Directory セキュリティ**
  Active Directory の設定ミスを完全に修正するのは簡単ではありません。Zscaler Deception は、Active Directory を悪用する脅威を検出する実用的なソリューションを提供します。これは、アイデンティティー戦略全体の再設計が困難な場合にセキュリティを強化する効果的な手段となります。

- **SOC の効率化**
  低い誤検知率とアイデンティティー インテリジェンスを活用して高精度なアラートを生成し、SOC をサポートします。このアプローチにより、脅威の検出、理解、対応に要する時間が短縮され、脅威ハンティングが強化されます。また、境界デコイを用いて、侵害が発生する前のステルス的な偵察活動を特定します。

他のベンダーにはない独自のデセプション技術を提供しています。

GARTNER

© 2025 Zscaler, Inc.All rights reserved.

Zscaler Deception のプラン

Zscaler Deception には以下の 2 つのエディションがあります。

- **Zscaler Deception Standard**
  デセプションを活用した脅威検出を初めて導入する組織向け

- **Zscaler Deception Advanced**
  高度な脅威の検出と環境内の重要資産を保護する、デセプションを活用した包括的なアクティブ ディフェンス ソリューションを求める組織向け

機能	Zscaler Deception Standard	Zscaler Deception Advanced
数量	• 20 個のデコイ • 追加のデコイはなし	• 50 個のデコイから開始 (5,000 ユーザーごとに追加で 50 個、最大 300 個まで可能) • 必要に応じて追加のデコイを設定可能
アプリケーション ルアー、クラウド ルアー、ブラウザー Cookie、ビーコン ファイル	• フル デコイ ライブラリー	• Standard の機能 • カスタマイズ可能なデコイ (VM、コンテナー)
エンドポイント デセプション	• アプリケーション ルアー、ブラウザー Cookie、ビーコン ファイル	• Standard の機能 + ランサムウェアの検出、MiTM の検出、総当たり攻撃の検出、Kerberoast の検出、メモリー内の認証情報の使用の検出、防御回避の検出、トリアージ
Active Directory デセプション	• Active Directory の偵察と攻撃の検出 • デコイ AD ユーザー • 複数のドメインに対応	• Active Directory の偵察と攻撃の検出 • Active Directory デコイ ユーザー • 複数のドメインに対応
SOC と脅威ハンティングの統合	• メール通知のみ	• 完全な SOC ワークフロー：Standard の機能 + SIEM へのデータ転送、オーケストレーションと封じ込め、カスタム通知、ThreatParse のカスタム ルール、Zscaler Sandbox との統合
エンタープライズ機能	• シングル サインオン、監査ログ、標準ロール	• カスタム RBAC、静的 IP ホワイトリスト、API アクセス
提供元の製品	• Zscaler Platform	• アドオン SKU — Zscaler Risk Management

© 2025 Zscaler, Inc.All rights reserved.

Zscaler Deception が選ばれる理由

- **クラウドネイティブでスムーズに導入**
  Zscaler Deception は、Zscaler Private Access (ZPA) との統合を通じて、デコイの作成、ホスト、配信を可能にします。追加の仮想マシンやハードウェアは一切必要ありません。

- **ネットワーク構成は不要**
  VLAN トランキングや SPAN ポート、GRE トンネルといった従来の方法を用いて、悪意のあるトラフィックをデコイにルーティングする必要はありません。Zscaler Deception は Zero Trust Exchange の拡張機能として、これらのトラフィックを自動的にデコイにルーティングします。

- **Zero Trust Exchange への統合**
  デセプション機能が組み込まれた世界で唯一のゼロトラスト アーキテクチャーを活用することで、高度な攻撃者や侵害されたユーザー、内部脅威を検出して阻止すると同時に、複雑な作業やアラート疲れも軽減します。

巧妙化するサイバー脅威を今すぐ検知

ゼロトラストの導入を検討されているお客様や、すでに Zscaler をご利用中のお客様に向けて、Zscaler Deception のデモを提供しています。デモを依頼して、このソリューションがどのようにゼロトラストへの移行を効率化し、セキュリティを強化するかをご確認ください。

デモを依頼する

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™ プラットフォームは、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™ 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。

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

Zero Trust Everywhere.™