データシート

Zscaler Deception

侵害されたユーザや水平移動の検出と排除

Zscaler Deceptionは、Zscaler Zero Trust Exchangeの一部として提供されるデセプションベースの脅威検出プラットフォームです。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、既存の防御機能を回避してネットワークに侵入する高度な脅威を検出します。そして、侵害されたユーザの検出、水平移動の阻止、人手によるランサムウェア、ハンズオンキーボード攻撃、サプライチェーン攻撃、悪意あるインサイダーからの防御を実現します。

今日のセキュリティにおける主な課題

1. **侵害されたユーザ：**フィッシング攻撃やダークウェブからのキットを使用した資格情報の窃盗が増加傾向にある今、アイデンティティ侵害は重要な課題となっています。信頼できるアイデンティティを入手した攻撃者は、そのアイデンティティと同じIT資産にアクセスできるようになります。アイデンティティには正当なアクセス権があるため、この種の攻撃を検出するのは難しくなっています。

2. **水平移動：**今日のネットワークは非常に複雑で、限られた可視性しか提供されません。信頼できるアイデンティティを入手した攻撃者は、この限定的な可視性に乗じて水平移動し、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むことから、水平移動が攻撃において最も時間の長いフェーズであることがわかります。

3. **ランサムウェアと高度な脅威：**従来の防御アプローチは、シグネチャや悪意のある活動を手がかりに脅威を検出します。ところが、ランサムウェア、サプライチェーン攻撃、国家が支援する攻撃者などの人間が操作する脅威にとって、これらの防御を回避するのはそれほど難しいことではありません。こういった攻撃のステルス性により、従来の検出ツールでは、早い段階で攻撃を阻止したり、活動範囲を制限したりすることはほぼ不可能です。

「デセプションプラットフォームを使用することで、初期侵入の段階でランサムウェア攻撃を特定できます。これは、キルチェーンの初期のフェーズにあたります。エンドポイントデコイは、キルチェーンのさまざまなフェーズで窃取したファイルや資格情報の暗号化の試行などのランサムウェア攻撃を検出することで、エンドポイントをそれらの攻撃から簡単に保護します。」

— Gartner

「他にはないデセプション防御の形態で、プライベート脅威インテリジェンスを提供する唯一のベンダです。」

— Gartner

Zscaler Deceptionとは

攻撃対象領域のリスクの低減、水平移動の検出、高リスクな人手による攻撃の阻止を可能にする実用的なアプローチです。

水平移動の阻止
ネットワークに仕掛けられたデコイのサーバ、アプリケーション、データベースが水平移動を試みる攻撃者を検出して遮断します。

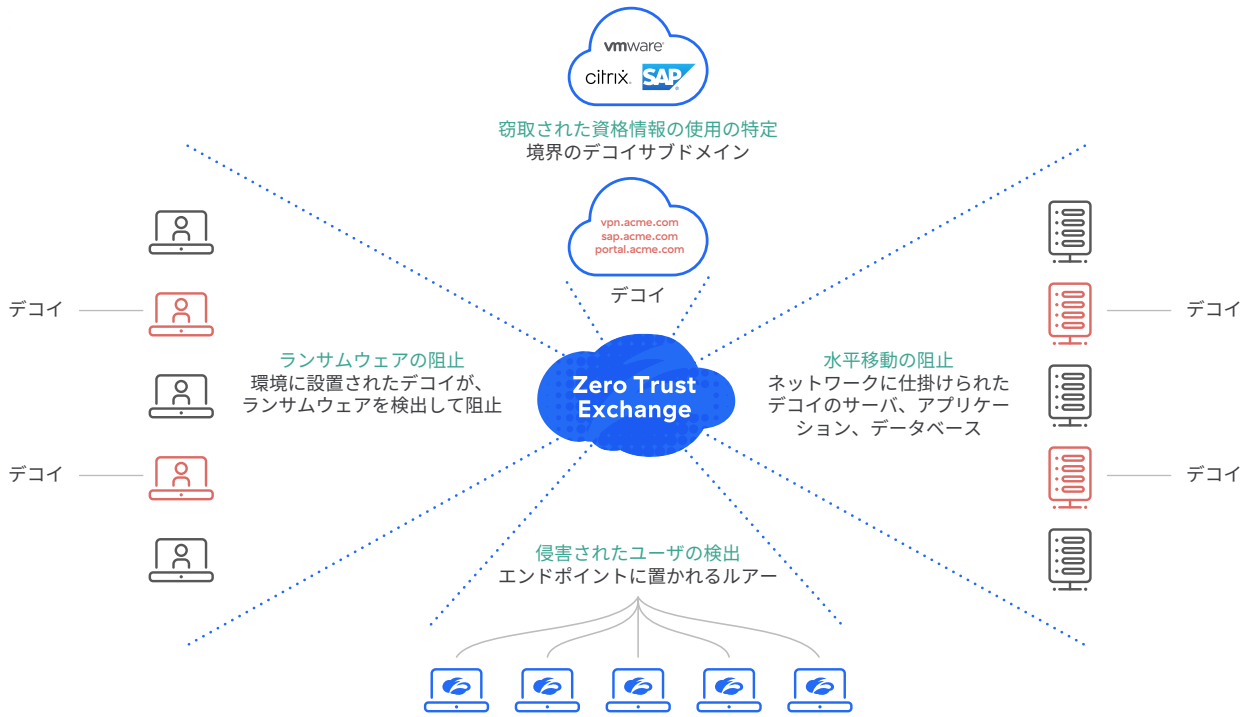
ランサムウェアの阻止
環境に設置されたデコイが、キルチェーンのあらゆるフェーズでランサムウェアを検出して減速させ、活動範囲を制限します。

侵害されたユーザの検出
アプリケーションをおとりにするためのパスワード、Cookie、セッション、ブックマークのいずれかが攻撃者に使用された際に、侵害されたユーザを検出します。

窃取された資格情報の使用の特定
脆弱なテストベッド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に似せたおとりのWebアプリにより、窃取された資格情報でログインする攻撃者を阻止します。

標的型脅威の検出のための360度アプローチ

Zscaler Deceptionは、IT環境にデコイを設置することで、攻撃者を検出および妨害し、重要な資産から遠ざけます。



攻撃対象領域のリスクの低減

エンドポイント、アイデンティティシステム、ネットワーク、アプリケーション、クラウドの脅威を検出し、攻撃者を標的から遠ざけ、攻撃対象領域のリスクを軽減します。

脅威の迅速な検出

侵害されたユーザ、水平移動、ランサムウェア攻撃を迅速に検出します。デセプションアラートの誤検出率をほぼまたは完全にゼロにし、信頼性の高いIoCを提供します。

リアルタイムでの脅威の阻止

ゼロトラストネットワークアクセスの適用ポリシーを活用して、脅威を封じ込めます。統合の作業は必要ありません。

「デセプションを検出または回避しようとする攻撃者を、能動的に検出して対処します。」

— Gartner

機能

- **脅威インテリジェンスのデセプション：**特定の組織を標的とした攻撃の開始前に脅威をヒューリスティックに検出するインターネットに面したデコイ
- **エンドポイントのデセプション：**おとりのファイル、資格情報、プロセスなどを含むエンドポイントの地雷原
- **クラウドのデセプション：**クラウド環境での水平移動を検出するおとりのWebサーバ、データベース、ファイルサーバなど
- **ThreatParse：**2回のクリックで実行可能な自動フォレンジックと根本原因の分析。ログからインサイトを抽出します。
- **アプリケーションのデセプション：**SSHサーバ、データベース、ファイル共有などのサービスをホスティングするサーバシステムのおとり
- **Active Directoryのデセプション：**列挙アクティビティや不正アクセスを検出するActive Directoryの偽のユーザ
- **ゴールデンイメージのサポート：**多くのインタラクションが発生するOS環境に対する攻撃の詳細な可視化
- **MirageMaker：**さまざまなユースケースに対応するデコイのデータセットを利用することで、デセプションをすぐに開始できます。

「他のベンダにはない独自のデセプション技術を提供しています。」

— Gartner

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集団などの高度なサイバー犯罪者に標的にされている場合も、早期に警告を受け取ることができます。境界のデコイが、密かに進行する侵入前の偵察活動を検出します。

Active Directoryセキュリティ

Active Directory の構成ミスを常に修正できるわけではありません。Zscaler Deceptionは、Active Directoryを悪用する脅威を検出する実用的ソリューションを提供します。次善の対策は、アイデンティティ戦略を再設計することです。

SOC最適化

誤検出率の低いアイデンティティインテリジェンスでSOCをサポートし、信頼性の高いアラートで脅威ハンティングを可能にし、短時間での脅威の検出、理解、レスポンスを可能にします。

Zscaler Deceptionのプラン

Zscaler Deceptionは、次の2つのエディションでご利用いただけます。

Zscaler Deception Standard

デセプションベースの脅威検出をこれから始める企業向け。ZIA（TransformationおよびELA）エディションとZPA（Business）エディションの一部としてのみ利用できます。

Zscaler Deception Advanced

高度な脅威を検出し、環境の重要な部分を保護する、デセプションベースの包括的なアクティブディフェンスソリューションの実装を検討する企業向け。ZPAトランスフォーメーションの一部として、またはスタンドアロンのソリューションとして利用できます。

機能	Zscaler Deception Standard	Zscaler Deception Advanced
以下が含まれます。	• 20 x アプリケーション / ネットワークデコイ（境界デコイを含む） • 1 x デコイコネクタ • 1 x Active Directoryデコイ • アドオンのデコイは利用不可	• 最大150 x アプリケーション / ネットワークデコイ（境界デコイを含む） • 最大6 x デコイコネクタ • 10 x Active Directoryデコイ • アドオンのデコイはアラカルトで利用可
アプリケーション / ネットワークデセプション	• ビルトインされたデコイのすべてのライブラリ	• ビルトインされたデコイのすべてのライブラリ • カスタマイズ可能なデコイ（VM、コンテナ）
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Cookie、ビーコンファイル	• アプリケーションルアー、ブラウザCookie、ビーコンファイル、ランサムウェアの検出、ローカルスキャンの検出、MiTMの検出、特権エスカレーションの検出、防御回避の検出とトリアージ
Active Directoryのデセプション	• Active Directoryの基本的な統合により、ネットワークとアプリケーションのデコイのみをサポート	• Active Directoryの偵察と攻撃の検出 • Active Directoryデコイユーザ • 複数のドメイン
SOC/ハンティング統合	• メール通知のみ	• メール通知、完全SOCワークフロー、SIEM転送、オーケストレーションと封じ込め、SIEMダッシュボード、カスタム通知、カスタムThreatParseルール、クラウドサンドボックス統合、マネージド脅威ハンティング統合
Enterprise機能	• シングルサインオン、監査ログ、標準ロール	• シングルサインオン、監査ログ、完全RBAC、IPホワイトリスト、APIアクセス
利用できる製品	• ZIA–TRANS EDITION以上 • ZPA–BUS EDITION • 1,000ユーザ以上	• ZPA–TRANS EDITION • 1,000ユーザ以上 • スタンドアロンのデセプションソリューションとしても利用可能

Zscaler Deceptionを採用すべき理由

- **シームレスなクラウドネイティブの展開**
  Zscaler DeceptionとZscaler Private Access（ZPA）の統合により、追加のVMやハードウェアを必要とすることなく、デコイの作成、ホスティング、配布が可能です。
- **ゼロネットワーク構成**
  VLANトランキング/SPAN ポート/GREトンネルに頼ることなく、トラフィックをデコイにルーティングします。Zscaler Deceptionが、Zero Trust Exchangeの透過的な拡張機能として、不正トラフィックを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統合された世界で唯一のゼロトラストアーキテクチャにより、複雑さが増大したり、大量のアラートに悩まされたりすることなく、最も高度な攻撃者、侵害されたユーザ、インサイダーの脅威を検出して、阻止します。

高度な脅威検出機能を体験してください

ゼロトラストを導入したばかりのお客様だけでなく、Zscalerをすでにご利用いただいているお客様も、Zscaler Deceptionのデモをぜひご依頼ください。このデセプションソリューションを活用してゼロトラストへの移行を加速し、保護する方法をご紹介します。

デモを申し込む

zscaler™ | Experience your world, secured.™

Zscalerについて
Zscaler (NASDAQ: ZS) は、デジタルトランスフォーメーションを加速させることで、お客様のアジリティ、効率性、耐障害性、セキュリティの向上を支援します。Zscaler Zero Trust Exchangeは、あらゆる場所のユーザ、デバイス、アプリケーションの安全な接続を可能にすることで、数千社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。世界中で運用する150のデータセンタで動作するSASEベースのZero Trust Exchangeは、世界最大規模のインライン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。

03-4243-6320　Zscaler, Inc.(本社) – 120 Holger Way – San Jose, CA 95134　zscaler.jp