ソリューションの概要

CrowdStrike と Zscaler の統合

ゼロトラストで境界を超えてビジネスを保護し、
IT 環境全体のセキュリティを最新化

課題

ハイブリッド ワークが新たなビジネス スタイルとして定着しつつある中、従業員はあらゆる場所で作業し、パートナーとそのデバイスはオフィスのネットワークを出入りし、かつてデータ センターでホストされていた多くのアプリケーションはパブリック クラウドに移行したり、Software as a Service (SaaS) に置き換えられたりしています。より多くの業務が企業ネットワーク外で行われるようになった今、ネットワークの周囲に強固な境界を構築するゲートウェイ アプライアンスはもはや意味をなさなくなっています。

従来のソリューションではネットワーク セキュリティが重視されていたため、ネットワーク リソースへのアクセスが許可される前にデバイスの状態が検証されることはほとんどありませんでした。しかし、クラウドの普及により、過去の「城と堀」のアーキテクチャーではアプリケーションへのセキュアなアクセスを制御できなくなっています。ユーザーがどこから接続しているかに関係なく、ユーザーとアプリケーション間の接続をエンドツーエンドで保護する必要があります。セキュリティ部門がこれまで以上に多くのデータにアクセスでき、適切なコンテキストとタイミングでデータを可視化できるツールが求められています。これには、境界を超えたセキュリティが必要です。

ソリューション

境界を超えてビジネスを保護するために、多くの IT 部門がアイデンティティー、ユーザーのデバイス ポスチャー、アクセス ポリシーという 3 つの重要な基準を持つゼロトラスト モデルを採用し始めています。これらの基準はコンテキストに基づいてゼロトラストを確立し、コンテキストの変化に応じてアクセス権を適応させるための手段です。

CrowdStrike と Zscaler の統合によって実現したエンドポイントからアプリケーションまでの「エンドツーエンドのセキュリティ ソリューション」は、IT 部門がゼロトラストを簡単に採用できるよう支援します。また、管理者はデバイスのセキュリティ態勢をリアルタイムで把握でき、重要なアプリケーションへのアクセスはきめ細かなアクセス ポリシーに基づいて行われます。エンドポイントの CrowdStrike Falcon® と Zscaler Zero Trust Exchange™ の間でデータを共有することで、ユーザー コンテキストやデバイスの正常性、そして新たに検出された IOC に応じてアクセス ポリシーを自動的に適応させることができます。

CrowdStrike Falcon Zero Trust Assessment (ZTA) は、エンドポイントのセキュリティとコンプライアンスを継続的かつリアルタイムでチェックし、組織が承認したセキュリティ態勢を持つデバイスのみに認証と承認が付与されるようにします。

Zscaler Zero Trust Exchange はポリシーを使用して、ユーザーをインターネット、SaaS、プライベートアプリに安全に接続させます。CrowdStrike はデバイスの状態をスコア化した ZTA スコアや脅威インテリジェンスを活用する機能を提供し、Zscaler がアプリケーションにアクセスするためのポリシーを適応的に施行したり、悪意のある URL、IP アドレス、ドメインをカスタム ブロックリストを介してインラインでブロックしたりできるようにします。また、セキュリティ管理者は Zscaler から CrowdStrike Falcon プラットフォームへの隔離アクションを開始して、問題のあるデバイスからのマルウェアの拡散を阻止することができます。このように脅威インテリジェンスをプラットフォーム間で双方向に共有し、可視性を強化し、ワークフローを自動化することで、脅威の防御、検知、修復をスピーディーかつ効率的に行えるようになります。

CrowdXDR Alliance の一環として、Zscaler は CrowdStrike と統合して関連する Zscaler のログを共有し、エンドポイント、ネットワーク、クラウド アプリケーションからのテレメトリーでエンドツーエンドの可視性を向上させます。このインテリジェンスの共有によってクロスプラットフォームの効果が最大化し、調査を加速できます。CrowdStrike Falcon Fusion はクロスプラットフォームの対応ワークフローを実行することで、Zscaler Zero Trust Exchange が柔軟なアクセス ポリシーを迅速かつ効果的に適応できるようにします。

Falcon Insight XDR は Zscaler Zero Trust Exchange と統合され、XDR の検知または自動化された Falcon Fusion (SOAR) ワークフローによる対応アクションを実行します。これらの自動対応アクションには、検出の重要度に基づいた適応型アクセス制御ポリシーによるアプリケーションへのユーザー アクセスの制限または更新が含まれており、プラットフォーム全体で完全なクローズドループ修復を提供します。

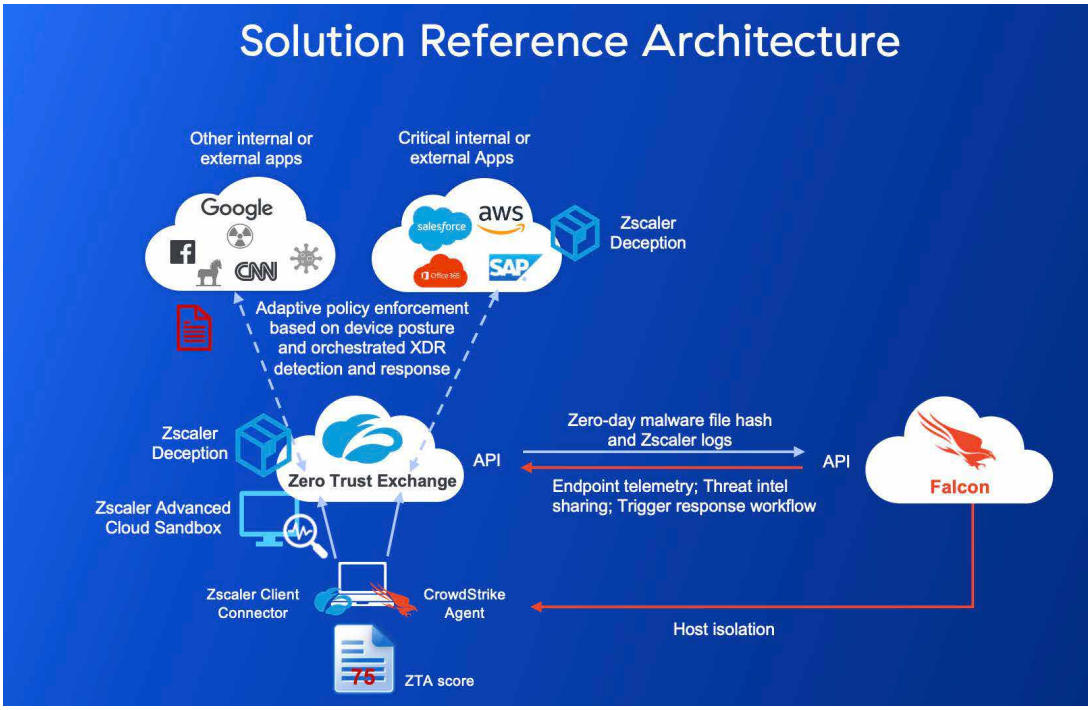
また、Zscaler Deception はエンドポイント、ネットワーク、クラウド、アイデンティティー システムにデコイ (おとり) を展開して、標的型攻撃に関するテレメトリーを提供し、忠実度の高いアラートを発動します。これにより、管理者は CrowdStrike Falcon プラットフォームに対してオーケストレーションと手動の両方の封じ込めリクエストを開始し、侵害されたホストからのラテラル ムーブメントをリアルタイムで防ぐことができます。

2 社の統合ソリューションのメリットは、IT セキュリティだけではありません。この統合ソリューションにより、従業員は日常的な業務に不可欠なビジネス アプリケーションにシームレスかつ安全にアクセスできるようになるため、場所を問わない働き方を加速させることができます。これらはすべて、ゼロトラストを基盤として実現できます。

主なメリット

- プライベート アプリと SaaS アプリにアクセス ポリシーを施行する際は、リアルタイムのデバイス正常性メトリクスを使用
- 時間とともに変化するデバイスの状態に基づくアクセス ポリシーを施行
- この統合により、ユーザー、デバイス、ネットワークの可視性を侵害指標 (IOC) に集約し、全体的なシステムとしてワークフローを自動化してセキュリティ態勢を強化
- ユーザーが悪意のあるファイルにアクセスした場合、デバイスを隔離する機能でマルウェアの拡散を防止
- 可視性の向上により、さらに強力なレポートと修復が可能になり、増加し続ける巧妙な攻撃に対する組織の対応力を最大化

仕組み



** サードパーティーのロゴはそれぞれの所有者に帰属するものであり、関係や推奨を意味するものではありません。*

すべてのアプリへのゼロトラスト アクセス

ステップ 1: CrowdStrike Falcon プラットフォームが Zero Trust Assessment (ZTA) でデバイスの状態を評価
CrowdStrike Falcon プラットフォームは、エンドポイント デバイスから OS とセンサーの設定を収集して ZTA スコアを計算します。設定が変更されると、ZTA スコアは自動的に再計算されます。ZTA スコアを組織のベースライン スコアと比較することで、CrowdStrike は、組織のベースラインと推奨されるベスト プラクティスに対するユーザーのデバイスの正常性を経時的に測定できます。

ステップ 2: Zscaler Zero Trust Exchange がアクセス ポリシーを実装
Zscaler Zero Trust Exchange は、2 つのレイヤーでゼロトラスト アクセス ポリシーを実装します。最初に、CrowdStrike Falcon センサーがエンドポイント デバイス上で実行されているかどうかを Zscaler Client Connector が確認します。次に、Client Connector がデバイスの ZTA スコアを読み取り、指定されたビジネスクリティカルなアプリケーションに定義されたポリシーしきい値と比較します。これらの条件が満たされた場合、アプリケーションへのアクセスが許可されます。そうでない場合は、アクセスが拒否されます。Zscaler ダッシュボードのアクセス ポリシーは、組織の要件や時間とともに変化する条件に応じてスコアのしきい値を変更できます。

ゼロデイ脅威の検知と修復

ステップ 1: Zscaler Cloud Sandbox がゼロデイ マルウェア検知と CrowdStrike Falcon テレメトリーを関連付け
Zscaler Cloud Sandbox はクラウドのエッジにインラインで配置され、ゼロデイ脅威を検知します。悪意のあるファイルはサンドボックス内で実行され、Falcon プラットフォームからのエンドポイント データと関連付けられたレポートを作成します。これにより、ネットワークのエッジで検出された脅威がエンドポイント データと結び付けられます。

ステップ 2: 管理者がクロスプラットフォームのワークフローで脅威を隔離して修復
この関連付けにより、環境全体で影響を受けるエンドポイントが自動的に特定され、Falcon プラットフォームへの隔離をワンクリックで実行できます。また、管理者は Zscaler コンソールから Falcon コンソールに移動して、さらに詳細な調査のために自動的に入力されたデータを使用することもできます。

CrowdStrike の脅威インテリジェンスで Zscaler のインライン ブロックを強化

ステップ 1: CrowdStrike が侵害指標 (IOC) を Zscaler のカスタム ブロックリストに追加
CrowdStrike のインテリジェンスによって、あるお客様の環境内で脅威が特定されると、その脅威は Zscaler の脅威データベースと比較され、その結果の差分が Zscaler プラットフォーム内のお客様のカスタム ブロックリストに自動的に追加されます。これには URL、IP アドレス、ドメインなどの信頼性の高い脅威データが含まれます。共有されたカスタム ブロックリスト内の侵害指標 (IOC) は、Zscaler のグローバル脅威フィードに追加され、お客様の環境固有のものとなります。

ステップ 2: Zscaler が新しいインテリジェンスを用いて脅威をブロック
このように IOC が共有されると、Zscaler は URL/IP/ ドメインへのアクセス試行をインラインでプロアクティブにブロックします。Zscaler Internet Access (ZIA) と CrowdStrike Falcon は、同じ脅威ベクトルが他のエンドポイントに感染する前に Zscaler によってインラインでブロックされるようにします。

主な機能と特長

- CrowdStrike と Zscaler の統合により、脅威インテリジェンスの共有とワークフローの自動化が可能になり、セキュリティ インシデントの件数を削減できます。また、インシデントが発生した場合でも、検出と修復までの時間を短縮できます。
- ZTA スコアを通じてデバイスの正常性とコンプライアンスを監視すると同時に、ゼロトラストのアクセス ポリシー制御と CrowdStrike が検出した IOC に基づくインライン ブロックでギャップを迅速に修復できるようになります。また、ユーザーの生産性を妨げることなく、最大限に適応したアクセス制御を用いてアプリケーションとインターネットへのアクセスが可能になります。

CrowdStrike Falcon LogScale のログ管理で可視性を向上

ステップ1: CrowdStrike Falcon® LogScale が Zscaler のログを活用

CrowdStrike Falcon LogScale は Zscaler のあらゆるログを Falcon プラットフォームに取り込むことで、ネットワークの可視性を強化します。

ステップ2:CrowdStrike Falcon LogScale がデータの関連付けと分析を実行

CrowdStrike Falcon LogScale プラットフォームはZscaler からテレメトリーを取得し、データの関連付けと分析を行います。これにより、脅威ハンティングと調査、そしてクロスプラットフォームのトリアージと修復が可能になります。

CrowdStrike Falcon Insight XDR™ で検知と対応を強化

ステップ1: アプリケーションとエンドポイント全体を包括的に可視化

Falcon Insight XDR は Zscaler のログと専用に構築された XDR を統合することで、関連するセキュリティ データを大規模に提供します。これにより、ネットワークとクラウド アプリケーションが可視化されると同時に、クロスプラットフォーム共有を最大化して迅速に調査と対応を進めることができます。

ステップ2: 高度な脅威を検知して効果的に対応

Falcon Insight XDR は、Zscaler のログから特定されたセキュリティ イベントを活用して実用的なインサイトを生成し、プロアクティブな脅威ハンティングを加速させ、サイバー攻撃を阻止するための対応力を高めます。新たに検知されると、CrowdStrike Falcon は Zscaler Zero Trust Exchange でユーザーを制限的なグループに移動させ、ブラウザー分離やネットワーク隔離によるアプリへのアクセスなどの適応型アクセス制御ポリシーを適用します。

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。

CROWDSTRIKE | We stop breaches.

CrowdStrike について

CrowdStrike (Nasdaq: CRWD) は、サイバーセキュリティのグローバルリーダーであり、エンドポイント、クラウドワークロード、アイデンティティ、データを含む企業におけるリスクを考える上で重要な領域を保護する世界最先端のクラウドネイティブのプラットフォームにより、現代のセキュリティを再定義しています。

CrowdStrike Falcon® プラットフォームは、CrowdStrike Security Cloud とワールドクラスの AI を搭載し、リアルタイムの攻撃指標、脅威インテリジェンス、進化する攻撃者の戦術、企業全体からの充実したテレメトリーを活用して、超高精度の検知、自動化された保護と修復、精鋭による脅威ハンティング、優先付けられた脆弱性の可観測性を提供します。

Falcon プラットフォームは、軽量なシングルエージェント・アーキテクチャを備え、クラウド上に構築されており、迅速かつスケーラブルな展開、優れた保護とパフォーマンス、複雑さの低減、短期間での価値提供を実現します。

詳細はこちら：https://www.crowdstrike.jp/

フォローはこちら：ブログ | Twitter | LinkedIn | Facebook | Instagram

今すぐ無料トライアルを開始：
https://www.crowdstrike.jp/free-trial-guide/