CrowdStrike テクノロジーパートナー

zscaler™

CROWDSTRIKE

ソリューション概要

クラウドストライクとゼットスケーラーの連携

ゼロトラストで境界のない活動を保護

課題

現在、従業員の働く場所は物理的なオフィスの境界の中に限定されていません。従業員はどこからでも仕事を行うことができます。パートナーと彼らが利用するデバイスもオフィスネットワークに接続され、かつてデータセンターに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するか、サービスとしてのソフトウェア（SaaS）に置き換えられています。一方で、企業ネットワーク外での作業が増えるにつれ、企業ネットワークを通ることが減っており、その周囲に境界を構築するために設計されたゲートウェイアプライアンスは廃止されつつあります。

従来のセキュリティ対策はネットワークセキュリティの重要性を強調し、ネットワークリソースにアクセスするデバイスのセキュリティ状態を考慮していないことがありました。過去の「お城」を「城壁」で守るという、企業内ネットワークを境界防御で守るアーキテクチャは、クラウドの採用が普及している現在では、アプリケーションへの安全なアクセスを制御できないことを意味しています。

ユーザーがどこから接続しているかに関係なく、ユーザーからアプリケーションへの接続をエンドツーエンドで保護する必要があります。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

境界を越えてユーザーの作業を保護するために、IT部門はゼロトラストモデルの採用を開始しました。ゼロトラストは、アイデンティティ、ユーザーデバイスの状態、アクセスポリシーの3つの主要な基準で構成されています。これらの3つの基準は、ゼロトラストを始める手段として使用され、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手段として使用されます。

主な利点

- リアルタイムで確認されるデバイスの状態を使用し、プライベートアプリへのアクセスポリシーを適用
- 時間の経過とともに変化するデバイスの状態に基づきアクセスポリシーを適用可能
- この連携により、ユーザー、デバイス、およびネットワークの可視性を侵害の痕跡（IOC）に統合し、全体的なシステムとしてワークフローを自動化して、セキュリティ体制を強化
- ユーザーが悪意のあるファイルにアクセスした際、トリガー設定機能でデバイスの隔離を自動的に行うことで、その後のマルウェア拡散を防止
- 可視性の向上により、より強力なレポートと修復が可能になり、攻撃の量と高度化に対応する組織の能力を最大化

CrowdStrike テクノロジーパートナー

クラウドストライクとゼットスケーラーの連携

ZSCALERとCROWDSTRIKEを組み合わせることで、ゼロトラストの採用が簡素化されます。ZSCALERとCROWDSTRIKEの共同イノベーションは、エンドポイントからアプリケーションまで、エンドツーエンドのセキュリティソリューションを提供します。この統合により、管理者はデバイスのセキュリティ状態をリアルタイムで確認でき、重要なアプリケーションへのアクセスはきめ細かいアクセスポリシーに基づきます。エンドポイントのCROWDSTRIKE FALCON®センサーとZSCALER ZERO TRUST EXCHANGE™間でデータを共有することにより、アクセスを、ユーザーのコンテキスト、デバイスの状態、またはZSCALERからの更新されたアクセスポリシーに基づいて自動的に適応できます。

CROWDSTRIKE FALCON ZERO TRUST ASSESSMENT（ZTA）は、エンドポイントのリアルタイムでのセキュリティおよびコンプライアンスチェックを提供し、組織によって承認されたセキュリティ状態を持つデバイスにのみ認証と認可が付与されるようにします。

ZSCALER CLOUD EXCHANGEは、世界中の150か所にPOINT OF PRESENCE（POP）を持ち、ポリシーに基づいてユーザーをSAAS、インターネット、またはプライベートアプリに安全に接続します。CROWDSTRIKEは、デバイスのセキュリティ状態をスコア化した値と脅威インテリジェンスをZSCALERに提供し、プライベートアプリケーションへのアクセスポリシーを状態に応じて適用したり、カスタムブロックリストを介して悪意のあるURL、IPアドレス、またはドメインをブロックする機能を提供します。セキュリティ管理者は、ZSCALERからCROWDSTRIKE FALCONが隔離を行う様にトリガー設定し実行させることで、マルウェアが問題のあるデバイスから拡散するのを防ぐことができます。

プラットフォーム間での脅威インテリジェンスの双方向共有、可視性の向上、および自動ワークフローは、組織が脅威の防御、検知、および修復の適時性と有効性を高めます。

両社連携ソリューションのメリットは、ITセキュリティだけにとどまりません。企業は従業員がどこからでも働くことができる環境を実現しようとしています。この連携ソリューションにより、日常の従業員の活動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ります。すべて、ゼロトラストを基盤として実現できるようになります。

どう機能するか？

プライベートアプリへのゼロトラストアクセス

ステップ1：CROWDSTRIKE FALCONが、ZERO TRUST ASSESSMENTを使用してデバイスの状態を評価

CROWDSTRIKE FALCON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、そのZTAスコアを計算します。設定を変更すると、ZTAスコアの再計算が自動的に行われます。ZTAスコアを組織のベースラインスコアと比較することにより、CROWDSTRIKEは、組織のベースラインおよび推奨されるベストプラクティスと比較したユーザーのデバイスの状態を経時的に測定できます。

ステップ2：ZSCALER PRIVATE ACCESSTM（ZPATM）がアクセスポリシーを実装

ZPATMは、ゼロトラストアクセスポリシーを2つのレイヤーで実装します。まず、ZSCALER CLIENT CONNECTORは、CROWDSTRIKE FALCONセンサーがエンドポイントデバイスで実行されているかどうかを確認します。次に、CLIENT CONNECTORはデバイスのZTAスコアを読み取り、選択したプライベート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ると、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、アクセスは許可されません。ZSCALERダッシュボードのアクセスポリシーを調整して、組織の要件に基づいてスコアのしきい値を変更できます。

CrowdStrike テクノロジーパートナー

クラウドストライクとゼットスケーラーの連携

ゼロデイ検知と修復

ステップ1：ZSCALER CLOUD SANDBOXが、ゼロデイマルウェア検知をCROWDSTRIKE FALCONテレメトリと関連付ける

ZSCALER CLOUD SANDBOXは、ゼロデイ脅威を検知するためにクラウドエッジにインラインで配置されます。悪意のあるファイルがサンドボックスで起動され、FALCON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が作成されます。ネットワーク側で検知された脅威がエンドポイントデータに関連付けられます。

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を使用して脅威を隔離および修正

相関関係により、環境全体で感染したエンドポイントが自動的に識別され、FALCONプラットフォームへのワンクリックトリガーで、迅速な隔離実施が実現します。エンドポイント調査のためにデータが自動的に追加され、ZSCALER INSIGHTLOGからFALCONコンソールにアクセスできます。

CROWDSTRIKE脅威インテリジェンスによるZSCALERインラインブロッキングの強化

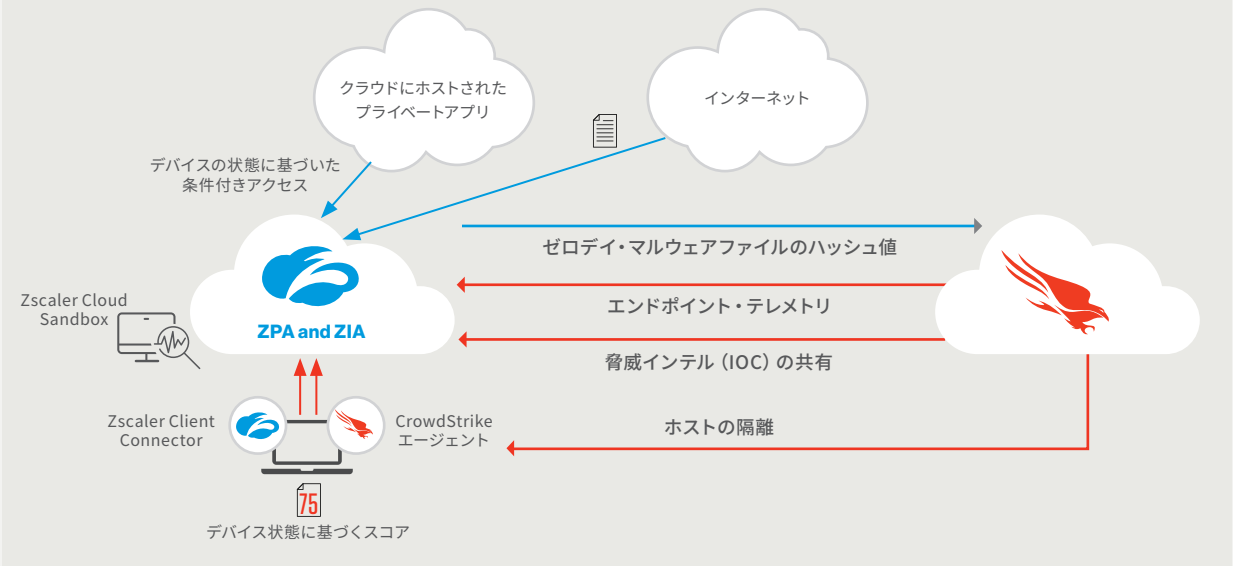
ステップ1：ZSCALERがカスタムブロックリストを取り込む

ZSCALERは、顧客環境内ですでに利用可能なCROWDSTRIKE脅威インテリジェンスを取得し、URL、IPアドレス、ドメインなどの信頼性の高い脅威データをカスタムブロックリストに自動的に取り込みます。カスタムブロックリストにある共有された侵害の痕跡（IOC）は、ZSCALERのグローバル脅威フィードに追加されるものであり、お客様自身の環境に固有のものです。IOCを共有することで、URL/IP/ドメインへのアクセスの試みは事前にブロックされます。ZIA（ZSCALER INTERNET ACCESS）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ことを保証します。

ステップ2：管理者がアクティビティの重大度を評価

ZSCALER ZERO TRUST EXCHANGEは、CROWDSTRIKEのイベントストリームAPIに接続して、特定の顧客の重大度の高いIOCを取得し、これをカスタムブロックリストに自動的に追加します。ZIAは、IOCの継続的な更新に基づいて脅威をブロックし、クラウドアプリケーションとエンドポイント全体で脅威をより迅速に防御します。

アーキテクチャー紹介



CrowdStrike テクノロジーパートナー

クラウドストライクとゼットスケーラーの連携

主な機能

CROWDSTRIKEとZSCALERの統合により、脅威インテリジェンスが共有され、自動ワークフローが可能になり、組織はセキュリティインシデントの数を減らすことができます。また、インシデントが発生した場合は、検知と修復までの時間を短縮できます。

さらに、この統合により、ZTAスコアを介してデバイスの状態とコンプライアンスを監視し、CROWDSTRIKEで検知されたIOCに基づくゼロトラストアクセスポリシー制御とインラインブロッキングを使用してギャップを迅速に修正できます。ZSCALERとCROWDSTRIKEを組み合わせることで、ユーザーの生産性を損なうことなく、最大限状況に基づいたアクセス制御で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。

ゼットスケーラーについて

ゼットスケーラー（NASDAQ:ZS）は、世界中の有力企業のネットワークおよびアプリケーションのモバイルおよびクラウドファーストな世界へ向けて、セキュアなトランスフォーメーション（転換）を実現します。ゼットスケーラーの代表的サービスである Zscaler Internet Access™およびZscaler Private Access™は、デバイス、場所、ネットワークなどに影響されることなく、ユーザーとアプリケーション間の高速でセキュアな接続を構築します。これらのサービスは100%クラウドで提供されるため、従来のアプリケーションとは比較にならない容易さ、高度なセキュリティ、優れたユーザーエクスペリエンスを提供します。185か国以上で使用されているマルチクラウド分散型セキュリティプラットフォームを運営し、サイバー攻撃とデータ消失から数千社の顧客企業を保護しています。詳細については、zscaler.comもしくは、Twitter（@zscaler）をフォローしてください。

CROWDSTRIKEについて

CrowdStrike® Inc.（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、セキュリティ侵害を阻止するためにゼロから構築したエンドポイント・ワークロード保護プラットフォームにより、クラウド時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、軽量なシングルエージェントによるアーキテクチャで、クラウドスケールの人工知能（AI）を活用し、リアルタイムで組織全体の保護・可視化を提供するとともに、ネットワーク内外でエンドポイントに対する攻撃を防止します。独自のCrowdStrike Threat Graph®を採用したCrowdStrike Falconは、世界で最も高度なセキュリティデータプラットフォームのひとつとして、世界中から取得した週5兆件超のエンドポイント関連イベントをリアルタイムで相関分析しています。

次世代アンチウイルス
無料トライアルにアクセス

Crowdstrike.jp で詳細をご覧ください