Zscaler + CrowdStrike

ゼロトラストの拡張による セキュリティ オペレーション センター (SOC) の最新化

ソリューションの概要

主なポイント

- Zscaler は、エンドポイントで発生するセキュリティ インシデントのアクティブなシグナルを CrowdStrike Falcon プラットフォームから収集して分析します。これにより、適応型アクセス制御ポリシー エンジンに充実したコンテキスト レイヤーを追加し、デバイス ポスチャーに基づくゼロトラスト アクセス制御をいっそう堅牢化します。
- Zscaler Risk360 サービスは、CrowdStrike と統合することで組織内のリスク要因に関するインサイトを提供します。また、リスクに関連する情報を Risk360 の攻撃段階カテゴリーに沿って分類し、重要度に基づいて各リスク要因を定量化します。
- Zscaler Data Fabric for Security は、CrowdStrike の CVE データを同時に供給されるデータ ストリームと関連付けて強化することで、IT 資産全体の脆弱性や公開状況に関するインサイトを、リアルタイムかつコンテキスト化された形で提供します。
- CrowdStrike によってネイティブに開発された Falcon Foundry の Zscaler アプリケーションは、CrowdStrike の次世代 SIEM プラットフォームと Zscaler との統合基盤として機能します。この事前構築された製品により、脅威インテリジェンスの共有の自動化とオーケストレーションを行い、協調的なポリシー アクションを通じてセキュリティ脅威への迅速かつ効果的な対応を実現できます。

課題

ハイブリッド ワークによって従来の境界が形を失い、ビジネス環境が変化し続けるなか、組織はサイバー攻撃からビジネスを保護しながら、分散した従業員が場所やデバイスを問わず安全に働けるよう支援するという複雑な課題への対応を迫られています。

働き方のパラダイム シフトによって、企業ネットワークに接続されるデバイスの数は劇的に増加しています。接続されたデバイスはいずれも侵入経路としてサイバー攻撃に利用される可能性があり、セキュリティ対策はいっそう複雑化しています。

こうした課題を抱えるなか、IT 部門やセキュリティ部門は、多様なマルチクラウド環境や日々変化する脅威に対応しながらアプリケーションへの安全なアクセスを担保しようと苦心しています。エンドポイントとアプリケーションの広大なエコシステム全体にセキュリティを拡張し、すべての潜在的な攻撃対象領域を保護するための可視性と制御が必要とされています。

セキュリティ オペレーション部門も独自の課題に直面しています。セキュリティ オペレーション部門は、高度な脅威を検知し、連携されていない大量のデータを通じてリスクを監視する責任を負い、可能な限り短時間でセキュリティ インシデントに対応することを期待されています。同時に、複数のツールやプラットフォームにまたがり対応戦略を最適な形で連携させることも求められます。こうした課題をさらに厄介なものにしているのが、IT セキュリティとセキュリティ オペレーション間の連携不足です。これによってインシデント解決に頻繁に遅れが生じ、組織全体のセキュリティ態勢の弱体化につながっています。

Zscaler と CrowdStrike:
優れた多層型防御アプローチ

Zscaler と CrowdStrike は、ハイブリッド環境におけるエンドポイントとアプリケーション間のセキュリティを簡素化する統合ゼロトラスト セキュリティ ソリューションを提供しています。このソリューションは、ゼロトラストの中核的な機能を拡張し、セキュリティ オペレーション センター (SOC) を変革する新しい強力な統合をスイートとして提供するものです。

Zscaler が提供するクラウド型の Zscaler Zero Trust Exchange™ プラットフォームは、インテリジェントな交換機として機能し、ネットワークや場所を問わず数百万単位のユーザー、デバイス、アプリケーションを安全に接続します。Zscaler は、リスクの定量化とデータのコンテキスト化のための新たな機能を通じて、プラットフォームの能力をさらに拡張し、セキュリティ オペレーション部門が脅威の検知と対応にあたるなかで直面する日常的な課題の解決を支援します。

統合ソリューションでは、業界をリードする Zscaler のゼロトラスト セキュリティと AI を活用したリスク管理機能を、CrowdStrike の高度なエンドポイント保護、脅威インテリジェンス、次世代 SIEM の機能と統合することで、リスク管理、検知、対応のライフサイクル全体を合理化し、IT セキュリティとセキュリティ オペレーション間の連携不足を効果的に解消します。

Zscaler と CrowdStrike の統合は
多層型防御で複数のユース ケースに対応

- **適応型ゼロトラスト アクセス：**Zscaler は、CrowdStrike Falcon Zero Trust Assessment (ZTA) のデバイス スコアとセキュリティ インシデントのシグナルを活用して適応型アクセス制御を実現し、安全なデバイスにのみアプリケーションへのアクセスを許可します。
- **脅威インテリジェンスの共有：**CrowdStrike が持つ侵害の痕跡 (IoC) の情報を Zscaler の脅威インテリジェンス エンジンにフィードすることで、カスタム ブロック リストを強化し、プロアクティブな脅威対策に活用します。
- **高度なゼロデイ脅威の検知と隔離：**Zscaler Cloud Sandbox を CrowdStrike Falcon のテレメトリーと統合することで、ゼロデイ マルウェアを検知し、影響を受けるエンドポイントでの隔離アクションを迅速化します。
- **デコイによる早期の脅威インテリジェンスの取得：**Zscaler Deception がエンドポイント、ネットワーク、クラウド、アイデンティティー システムにデコイを展開して、早期の攻撃の痕跡 (IOA) に関する高精度のアラートを発し、信頼性の高い脅威インテリジェンスを CrowdStrike と共有します。
- **包括的なサイバー リスクの可視化、評価、管理：**Zscaler Risk360 と Zscaler Data Fabric for Security が、それぞれ CrowdStrike から攻撃チェーンと CVE のデータにおける固有のリスク要因を取り込み、リスクを定量化するとともに、重大な脆弱性を優先的に自動修復ワークフローに組み込みます。
- **クロスプラットフォームのテレメトリーの共有と関連付け：**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得られたテレメトリーによってエンドツーエンドの可視性を向上させ、クロスプラットフォームの有効性を最大限に引き出して調査を迅速化します。
- **クロスプラットフォームの検知と対応：**CrowdStrike Falcon Next-Gen SIEM を Zscaler アプリ向け Falcon Foundry を介して Zscaler と統合することで、ZIA の高度なサンドボックス、CrowdStrike の次世代 SIEM、ZIA のポリシー施行エンジンの間で完全なクローズドループの修復を実現します。

Zscaler と CrowdStrike の最新の統合がサポートする新たなユース ケース

ユース ケース 1

コンテキストに基づく適応型アクセス ポリシーの施行

Zscaler では、適応型アクセス機能の対応範囲を拡張して、CrowdStrike から得られるリアルタイムのコンテキストを活用できるようになりました。これにより、優れたリスク評価とポリシー施行に関する意思決定が可能になりました。この新しい統合により、Falcon ZTA のデバイス正常性スコアに基づいてアクセス制御ポリシーを施行するだけでなく、CrowdStrike の詳細なセキュリティ インシデント データを組み込んでリスクをリアルタイムで評価できるようになりました。

Zscaler は、エンドポイントで発生するセキュリティ インシデントのアクティブなシグナルを CrowdStrike から収集して分析します。これにより、適応型アクセス制御ポリシー エンジンに充実したコンテキスト レイヤーを追加し、デバイス ポスチャーに基づくゼロトラスト アクセス制御をいっそう堅牢化します。

CrowdStrike からのセキュリティ インシデント データの継続的な供給によって、エンドポイントからアプリケーションに至るまで、動的かつ対応力に優れたセキュリティ態勢を確立できます。これにより、Zscaler の適応型アクセス機能が大幅に拡張され、よりきめ細かくコンテキストに基づいたアクセス制御が可能になります。

この新機能によって、Zscaler の管理者はセキュリティ インシデントのしきい値を設定できるようになりました。また、Falcon ZTA のコンプライアンス チェックと指定されたセキュリティ インシデントのしきい値条件の両方をクリアしたエンドポイントに対してアプリケーションのアクセスを許可できます。

CrowdStrike と Zscaler の統合により、脅威インテリジェンスの共有と双方向の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、検知と修復までの時間を短縮できます。

ユース ケース 2

包括的なサイバー リスクの定量化と可視化

Zscaler Risk360 は、リスクの定量化と可視化を行う強力なフレームワークで、サイバーセキュリティ リスクの修復に役立ちます。外部ソース、お客様の Zscaler 環境、ThreatLabz のセキュリティ リサーチから実際のデータを取り込み、組織のリスク状況に関する詳細なプロファイルを生成します。Risk360 のフレームワークは、攻撃の 4 つの段階をカバーしています。すなわち、外部攻撃対象領域、侵害、ラテラル ムーブメント、データ流出です。資産、アプリケーション、ユーザー、サード パーティーなど、環境内のあらゆるエンティティーが対象になります。

Risk360 サービスは、CrowdStrike と統合することで組織内のリスク要因に関するインサイトを提供します。セットアップが完了すると、Zscaler が Falcon プラットフォームからリスクに関連する情報を引き出し、Risk360 の攻撃段階カテゴリーに沿って分類して、重要度に基づいて各リスク要因を定量化します。

この統合により、ポリシーの更新や修正といったアクションを取ることができます。また、統合には調査ワークフローのガイドも含まれており、特定の問題をより詳細に掘り下げ調査することが可能です。

ユース ケース 3

セキュリティ データのコンテキスト化と UVM

現在、セキュリティ部門は攻撃対象領域の拡大に対応してビジネスを保護するべく、無数のテクノロジーやソリューションを活用しています。各ツールからは、価値あるデータが大量に生み出されるものの、多くの場合そのデータはツール間でサイロ化し、重複しています。その結果、セキュリティ部門は、情報過多、ワークフローの不透明性、サイバーセキュリティ態勢の維持に頭を悩ませています。

Zscaler Data Fabric for Security は、さまざまなツールからのデータを集約し、より実用的で有益な形での利用を可能にします。CrowdStrike によってエンドポイントで検知された共通脆弱性識別子 (CVE) など、150 以上のソースからのデータをシームレスに集約することで、セキュリティ オペレーション部門におけるセキュリティ脅威の管理と対応の方法を変革します。また、CrowdStrike の CVE データを同時に供給されるデータストリームと関連付けて強化することで、IT 資産全体の脆弱性や公開状況に関するインサイトを、リアルタイムかつコンテキスト化された形で提供します。

こうして得た情報を活用することで、セキュリティ アナリストは脆弱性、脅威、調査結果、インシデント、資産、ソフトウェア コンポーネント、ユーザーを動的に結び付けるとともに、相互に関連付けられた実用的なインテリジェンスを活用して、最も重要な脆弱性とリスクへの優先的な対応を効率的に行えます。

ユース ケース 4

脅威の協調的な共有、検知、対応

CrowdStrike によってネイティブに開発された Falcon Foundry の Zscaler アプリケーションは、Zscaler と CrowdStrike Falcon Next-Gen SIEM との統合基盤として機能します。この事前構築されたアプリケーションにより、脅威インテリジェンスの共有の自動化とオーケストレーションを行い、協調的なポリシー アクションを通じてセキュリティ脅威への迅速かつ効果的な対応を実現できます。

CrowdStrike と Zscaler のライセンスをお持ちのお客様は、CrowdStrike Marketplace で入手できる事前構築済みのアプリを使用することで、CrowdStrike の脅威インテリジェンス リポジトリーから得られる侵害の痕跡 (IoC) の情報を活用して、高度な監視と脅威の検知で境界セキュリティを強化できます。さらに、脅威の検知、調査、対応のための特定のユース ケースに合わせたカスタム ワークフローを開発、展開できます。

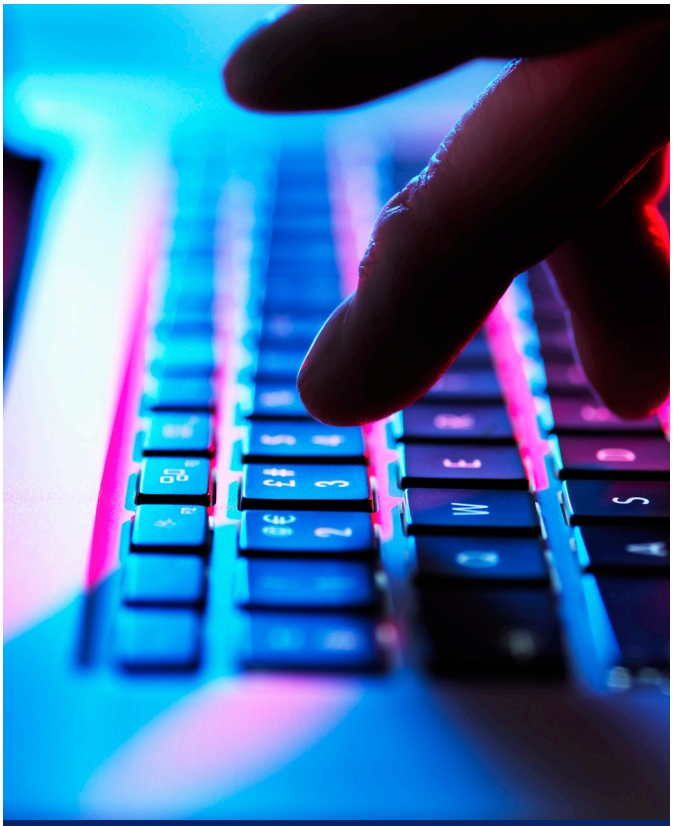
すぐに利用できるこのアプリケーションによって、ZIA の高度なサンドボックス、Falcon Next-Gen SIEM、ZIA のポリシー施行エンジンの間で継続的なフィードバック ループと協調的な対応メカニズムを構築して、セキュリティ ワークフローの自動化とオーケストレーションを合理化し、セキュリティ オペレーションを迅速化できます。

統合のメリット

- **充実したコンテキストに基づく適応型アクセス ポリシー：**変化する条件に動的に適応するゼロトラスト ポリシーを施行することで、エンドポイントとアプリケーション間のセキュリティ態勢を改善できます。
- **サイバー リスク状況の包括的な可視化：**攻撃の 4 つの段階にわたるリスクを正確に把握し、複数のソースを集約したリスク スコアを活用することで、サイバー リスクを完全に理解できます。
- **セキュリティ データのコンテキスト化によるリスク評価の改善：**セキュリティ データを集約、コンテキスト化することで、最大のリスクを優先し、修復ワークフローを自動化できます。
- **すぐに使用できる SOAR 統合：**事前構築された Zscaler 向けの Foundry アプリを使用して、脅威インテリジェンスの共有をすぐに開始できます。Falcon Fusion のカスタム SOAR ワークフローを迅速に構築し、検知、調査、対応をエンドツーエンドで自動化することが可能です。
- **迅速な検知と協調的な対応：**IT セキュリティとセキュリティ オペレーション間の連携不足を解消する協調的な対応およびポリシー アクションの実行により、平均検知時間 (MTTD) と平均対応時間 (MTTR) を短縮できます。

Zscaler と CrowdStrike による セキュリティ オペレーションの強化

Zscaler と CrowdStrike は、ゼロトラストとセキュリティ オペレーションの強化をミッションに、強力な補完機能を提供しています。最新の統合は、シームレスな連携を通じてセキュリティ オペレーションを次のレベルに引き上げます。共に最先端のゼロトラストの拡大に努め、SOC の新時代を創造していきます。



CROWDSTRIKE

CrowdStrike について
CrowdStrike は、現代の企業を動かす人、プロセス、テクノロジーを保護し、円滑な機能を可能にする、世界で最も先進的なクラウドネイティブ プラットフォームを提供し、セキュリティを再定義してきました。CrowdStrike は、エンドポイント、クラウド ワークロード、アイデンティティー、データなど、最も重要なリスク領域を保護し、お客様が攻撃者の一歩先を行き、侵害を阻止できるようにします。CrowdStrike Falcon® プラットフォームは、CrowdStrike Security Cloud を搭載し、リアルタイムの攻撃指標、進化する攻撃者の手口に関する脅威インテリジェンス、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オブザーバビリティーなどをすべて単一の軽量エージェントを通じて提供します。CrowdStrike のソリューションで、お客様は優れた保護、パフォーマンス向上、複雑さの低減、即時の価値実現を達成できます。
詳細は、crowdstrike.com でご確認ください。

詳細はこちら
zscaler.jp/partners/crowdstrike

Zscaler と CrowdStrike の 展開ガイドをダウンロード

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