Beyond the Perimeter 2023

Context-Driven Security for Enhanced Protection

課題

世界各地の従業員が流動的なハイブリッドモデルで働くようになったことで、アクセスや権限を取り巻く状況は、企業のセキュリティ部門にとってより複雑なものになりました。

リモート ワークやハイブリッド ワークといった柔軟な勤務形態はすっかり定着しましたが、時間や場所、デバイスを問わず、ユーザーが必要なリソースにすばやく簡単にアクセスできるようになったことで、多くの企業が重大なセキュリティ上の課題に直面しています。

現在の競争の激しいビジネス環境においては、従業員が企業のアプリや資産に安全かつスムーズにアクセスできなければなりません。しかし、そのアクセスを保護することは、ほんの数年前と比べても格段に難しくなっています。現在、従業員はグローバルに分散した動的な存在となり、システムへのログインは世界中から行われています。気の遠くなるような数の接続デバイス (承認済みデバイスと未承認デバイスのいずれをも含む) が使用されているほか、ログインに使われるアイデンティティーも増加する一方で、そこに紐付く役割や権限は絶えず変化しています。

従来の境界型のセキュリティを基盤とする企業では、組織のアプリや資産を脅威アクターから保護しながら、現代の従業員が必要とする柔軟なアクセスを提供するということは難題かもしれません。この問題を手っ取り早く解決するために非常によく行われているのは、従業員への過剰なアクセス権の付与です。脅威アクターはこれを悪用することに長けているため、結果としてセキュリティ上の重大なリスクを生むことになります。アクセス権の過剰な付与は、本質的には不正な侵入経路を生むことにつながり、サイバー攻撃やデータ侵害の被害を招きます。

権限が複雑かつ動的に拡大し続ける現在の状況下では、業務過多の状態のセキュリティ部門や IT 部門がリアルタイムでアクセスの可否を判断しなければなりません。しかも最近では、ユーザーの資格情報だけに基づいた権限付与は、もはや安全ではないことが明らかになっています。十分な情報に基づいてリアルタイムでアクセスの可否を判断するためには、ユーザーの場所、使用しているデバイスやネットワークなど、さまざまな点を把握する必要があります。これこそがコンテキスト認識型のセキュリティであり、クラウドファーストの企業が将来起こり得る侵害からビジネスを守るには、そのためのツールが不可欠です。

ソリューション

コンテキスト認識型のセキュリティを導入することで、きめ細かく確実に、リアルタイムかつ大規模なアクセス可否の判断を行うことができ、利便性を損ねることなく会社の資産を保護できます。

コンテキスト認識型のセキュリティ ソリューションでは、アクセス要求を受けた際に基本的なユーザー資格情報のみにとどまらない評価を行うため、管理者には、詳細かつ有益なインサイトが大規模かつリアルタイムに提供されます。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共有テレメトリーを活用することで、すべてのユーザー デバイス、利用場所、ユーザーが接続しているネットワーク、その他の重要なコンテキストの詳細を動的に評価し、よりスマートな意思決定を実現します。

Zscaler と CrowdStrike の統合によって、コンテキスト認識型のセキュリティは現実のものとなりました。これによって、脅威インテリジェンス データを簡単に関連付けて解釈できるようになり、ラテラル ムーブメントのリスクの最小化、データ流出の防止、新たな脅威に見舞われた際の迅速な検出および修復が実現します。共有される情報の活用により、デバイス、サーバー、パブリック クラウド、クラウド アプリケーションにわたって機能するコンテキスト主導のセキュリティ制御を確立できます。

コンテキスト認識型のセキュリティを導入することで、どのような組織でも、信頼性の高い安全でスムーズなアクセスを、世界各地のモバイル環境の従業員に提供できるようになります。また、サード パーティーに対するアクセス制御の改善、内部アーキテクチャーの簡素化、脅威アクターに隙を与えるようなセキュリティ ギャップの解消を図れます。Zscaler と CrowdStrike の緊密な統合によって、各ユーザーやデバイスに固有のきめ細かいコンテキストを詳細に可視化できるようになり、アクセス可否をより迅速かつスマートに判断するための情報が提供され、特に高度なランサムウェアやサイバー攻撃に対しても防御を強化できます。

この統合は、ゼロトラストの強力なセキュリティ態勢を支えるもので、企業は正規の認証されたユーザーを必要なアプリに安全に直接接続できるようになり、不要な摩擦を回避できます。Zscaler と CrowdStrike は、データ センターやクラウド上の重要なビジネス アプリケーションへの安全でシームレスなアクセスを可能にするとともに、脅威アクターに侵害の足掛かりを与えないようにすることで企業の防御を強化します。

Zscaler と CrowdStrike の統合による主なメリット

- 高品質なテレメトリーの共有を通じ、重要なコンテキストをリアルタイムで可視化できる
- 人工知能 (AI) と機械学習を活用し、既知および未知の脅威をリアルタイムで阻止できる
- 広範な検出と対応 (XDR) を使用したワークフローの自動化により、調査および脅威ハンティングを迅速化できる
- 修復および検疫の自動化により、侵害されたユーザーを特定し、ラテラル ムーブメントを防止できる
- 優れたプラットフォームに支えられ、緊密に統合された業界をリードするプラットフォームによって組織を保護できる

アクセス要求における「コンテキスト」の具体的な意味

「コンテキスト」は、ある状況に関する理解を深めるのに役立つ細かい追加情報を指す言葉として広く用いられています。ハイブリッド ワークやリモート アクセスに関する文脈では、アクセス要求の適格性を判断するにあたり、セキュリティ部門や IT 部門がより多くの情報を利用できるように提供される追加情報を「コンテキスト」と言います。追加のデータ ポイントとなり得るのは、アイデンティティー (従業員か請負業者か、役職や集団内での地位など)、デバイス (管理対象のデバイスかどうか)、場所 (制限されたリージョンまたは IP アドレスから送信されたリクエストでないか)、リクエスト内容 (要求されているリソースにはどのようなセキュリティ ポリシーが設定されているか、要求されているのは上書き / 削除が可能なフル権限か読み取り専用のアクセスか)、アクセスしようとしているアプリケーションの種類や場所などです。

CrowdStrike と Zscaler の統合は、こうしたコンテキストの企業全体での活用を可能にするものです。この共同ソリューションの導入によって、アクセスは単なるポリシー適用ポイントではなく、事実上の新たな境界となります。絶えず供給される統合データに基づいて機能するこの境界は、エコシステムの変化に対応しながら流動的でリアルタイムかつ継続的な検証を可能にし、効率性を妨げることなく企業の安全を守ります。

企業がコンテキストを活用してセキュリティを強化する方法

では、Zscaler と CrowdStrike の製品がどのように機能するかを見ていきましょう。両者はお客様の技術スタックやデバイスと緊密に統合され、連携してすべてのアクセス要求の背後にある重要なコンテキストについて画期的な可視性を提供します。

CrowdStrike はユーザーおよびデバイスのアクティビティーのモニタリングを行い、Zscaler はアクセス トラフィックを管理してアプリケーションに直接アクセスする権限を発行します。CrowdStrike Falcon® プラットフォームは、エンドポイント データを組み合わせ、デバイスの状態をリアルタイムでスコア化するなどしてコンテキストを生成します。このコンテキストはアクセス要求に付加されて Zscaler の Zero Trust

Exchange に送られ、ここでアプリへのアクセス ポリシーが適用されます。可視性の向上により、ケースごとの調査の負担が軽減され、より迅速かつ安全で迷いのない対応が可能になります。このコンテキスト認識型のセキュリティ ソリューションを導入することで、継続的かつ自動的なポリシー適用のための強固な基盤を確立でき、アイデンティティーが侵害されたと思われるユーザーを自動的に隔離する新たなポリシーを導入するなどといったことも可能になります。

CrowdStrike と Zscaler：よりスマートで安全なアクセス許可を実現するコンテキスト認識型のセキュリティ

現代の企業エコシステムは急速に進化しています。その保護をめぐる課題は拡大し続けており、当面は落ち着きそうもありません。高まり続けるセキュリティ上の懸念よりも、スムーズなアクセスがもたらす効率性を優先し続け、過剰な特権アクセスの付与が招くリスクを受け入れている組織もあるかもしれません。しかし、昨今のセキュリティ侵害の増加を考えれば、この姿勢はますます危険なものになっています。Zscaler と CrowdStrike は、より良いアプローチを持っています。

必要とされる重要なコンテキストをリアルタイムで豊富に提供する共有インテリジェンスを利用できるほか、スマートなツールにより、発生した異状を既知の脅威や新たな脅威と照合することが可能になります。また、実際の状況をより明確に把握できるようになるため、ポリシーに基づいて、アクセス可否の判断を高速かつ信頼性の高い形で行い、修復アクション (ユーザーの隔離を含む) を自動的に実行できます。Zscaler と CrowdStrike の緊密な統合によって、アクセス効率の最大化とリスクの最小化、攻撃対象領域の削減、脅威アクターによるラテラル ムーブメントの防止、迅速な対応と修復が実現し、お客様は成長と発展に集中できるようになります。

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 SASE 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 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。

CrowdStrike: We stop breaches.
詳細はこちら：https://www.crowdstrike.jp/

フォローはこちら：ブログ | | LinkedIn | |

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