CrowdStrike、Okta、Zscaler: クロスドメインの保護によるセキュリティ統合でAI時代のサイバーレジリエンスを強化

課題

攻撃者の動きはかつてないほど速くなっており、2024年に確認されたサイバー犯罪におけるネットワーク内での拡散開始まで時間の平均は、過去最短の48分にまで縮まり、最速の事例ではわずか51秒でした[1]。同時に、攻撃の79%はマルウェアを使用せず、アイデンティティーの悪用、ソーシャル エンジニアリング、クラウドの設定ミスによって検出を回避していました[1]。従来の事後対応型セキュリティ戦略では、現代の攻撃の進化する戦術にもはや対抗できません。脅威アクターはAIを悪用した自動化やステルス性の高い戦術など、ますます高度な手法を駆使して侵入し、検出されることなく環境内を移動します。断片化したポイント セキュリティ ソリューションでは、複雑さが増して対応が遅れ、最終的には全体的なセキュリティが弱体化するため、課題を克服するには、これに代わる新たなアプローチへの移行が必要です。

必要なもの

今こそセキュリティへのアプローチを見直し、AIを活用してスピードとスケールを向上させるときです。組織には、シームレスに連携して多層的な保護を提供し、複雑さを軽減しながら運用効率を向上させる高度なセキュリティ プラットフォームが必要です。

ソリューション

AIによってさらに進化する脅威に対処するため、CrowdStrike、Okta、Zscalerは完全に統合されたクロスドメイン セキュリティ ソリューションを提供します。これは、死角を排除し、可視性を高め、応答時間を短縮して強力な脅威対策を実現するように設計されています。この統合アプローチは、アイデンティティーの保護と認証、コンテキスト認識型の動的ゼロトラスト アクセス制御、分散したエンドポイントの保護を可能にするとともに、次世代SIEMを活用したリアルタイムの脅威の検知と対応を実現します。

アイデンティティー、エンドポイント、クラウド、ネットワーク層などにわたるリスク シグナルを関連付けることで、セキュリティ部門は攻撃者の動きを統合的に把握し、被害が発生する前に脅威を検知して封じ込め、無効化できます。AIを活用した自動化、双方向の脅威インテリジェンス共有、そして連携した対応により、この共同ソリューションは脅威を検知するだけでなく、深刻化する前に阻止します。

セキュリティ部門は攻撃者の戦術を予測し、対応を自動化するとともに、リアルタイムに行動することで、攻撃が拡大する前に封じ込めることができます。

サイバー脅威が高速化、高度化するなか、組織は攻撃者と同じスピードで機能するAI活用型のプロアクティブな防御を採用し、ビジネスに影響が及ぶ前に脅威を無力化する必要があります。

一体的に機能するセキュリティ：新たな時代に対応する統合型の保護

ゼロトラストに取り組んでいる組織や、既存の投資を最大限に活用しながらゼロトラスト ソリューションを設計する組織にとって、CrowdStrike、Okta、Zscalerとい

1. CrowdStrike 2025 Global Threat Report, https://www.crowdstrike.com/en-us/global-threat-report/

リーダーによる強力なパートナーシップと実証済みの統合は、ユーザーからエンドポイント、アプリケーションまでに対応するエンドツーエンドのゼロトラスト ソリューションを構築するうえでモデルとなる存在です。

この統合を活用することで、管理者は脅威の状況やエンドポイントおよびアプリケーションのセキュリティ態勢をリアルタイムで把握できるようになります。また、重要なアプリケーションへのアクセス許可は、ユーザー、エンドポイント、アクセス ポリシーに基づいて調整できます。

攻撃が発生した場合には、クロスプラットフォームでの修復が迅速にトリガーされます。さらに、防止ポリシーが統合全体に適用されることで防御がいっそう強化され、将来の同様の攻撃が阻止されます。

結果として、クラウドネイティブかつ動的なコンテキスト活用型の最高のゼロトラスト ソリューションが実現し、AIを悪用した最新の脅威に対処できるようになるほか、リスクを低減し、展開を簡素化できます。これにより、ゼロトラストを独自で構築する場合の複雑さを排除することが可能です。

ソリューションの主な特長

ゼロトラストの適応型アクセス：

Zscalerは、ユーザーのアイデンティティー、デバイス ポスチャー、リスク コンテキストに基づく最小特権アクセスを適用します。Zscaler Zero Trust Exchange (ZTE)は、Identity Threat Protection with Okta AI (ITP)およびCrowdStrike Falcon® ZTAスコアを統合し、リアルタイムかつリスクベースのアクセス ポリシーを展開します。

自動化されたアイデンティティー ライフサイクル管理：

Oktaは、OktaとSCIMの統合を通じてユーザーのプロビジョニングおよびデプロビジョニングを合理化します。これにより、リアルタイムかつロールベースのアップデートを可能にし、手動での作業による負担を軽減します。

アイデンティティーとエンドポイントの脅威の検知：

CrowdStrikeは、Zscaler DeceptionのシグナルをOkta ITPと共有することで適応型の対応を行い、ユーザーやエンドポイントを標的とする脅威を検知、軽減します。また、CrowdStrikeのテレメトリーは、充実したコンテキストを提供して脅威の検知を強化します。

継続的な認証とリスクベースのアクセス：

Zscalerは動的なアクセス ポリシーを施行し、ZscalerやCrowdStrikeによって検知された異常な振る舞いに基づいてOktaがステップアップ認証をトリガーします。

リスクの一元的な可視化：

Zscaler Risk360とData Fabric for Securityは、Oktaからアイデンティティー ログを、CrowdStrikeからエンドポイント シグナルを取り込みます。

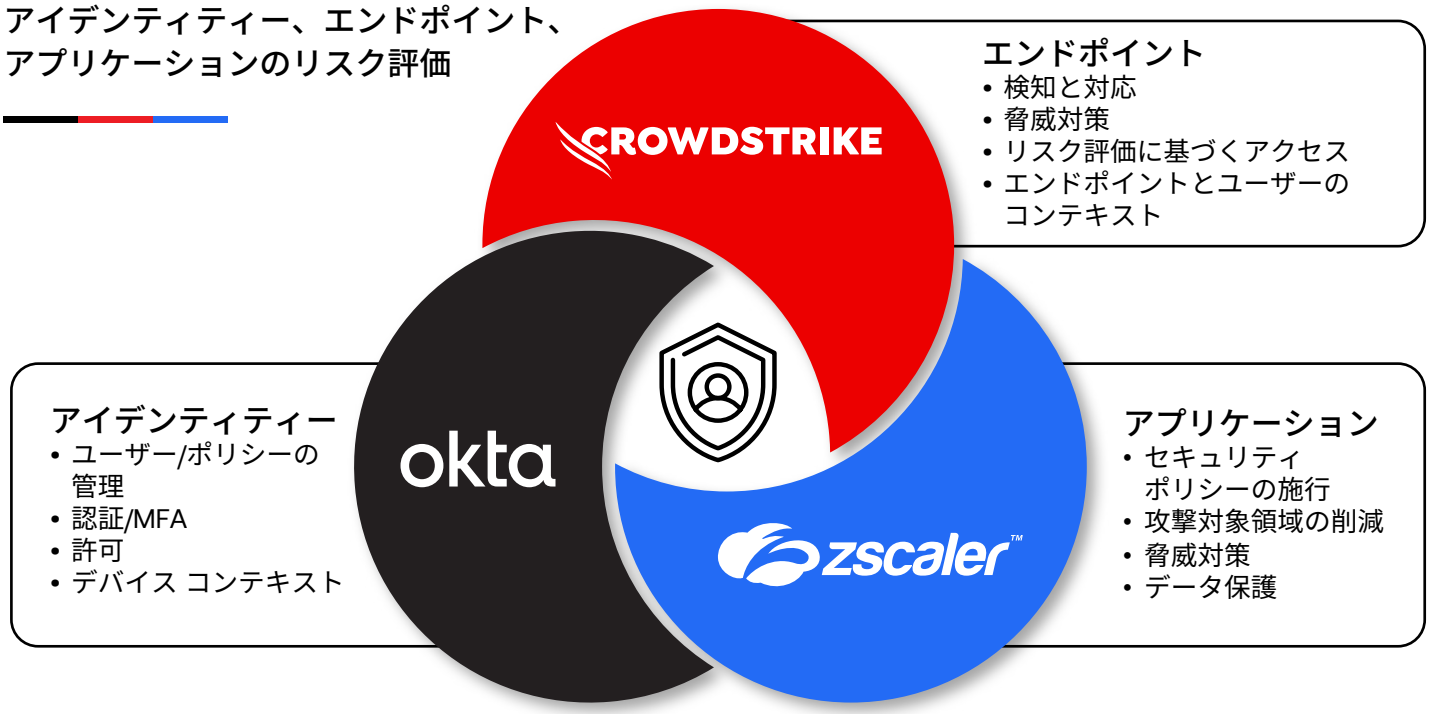
クロスプラットフォームの脅威インテリジェンスの共有：

Zscalerは統合されたテレメトリーを共有することで検知と対応を加速させ、CrowdStrikeはZscalerのカスタム ブロック リストを強化してプロアクティブな保護を実現します。

統合されたクロスドメインの脅威の検知と対応：

CrowdStrikeは、CrowdStrike Falcon® Next-Gen SIEMとCrowdStrike Falcon® Fusion SOARとOktaおよびZscalerとの統合を通じて、エンドポイント、アイデンティティー、アプリケーションにわたる包括的な可視性と協調的な自動対応を提供します。これにより、クロスドメインの脅威を迅速に検知、阻止し、ラテラル ムーブメントを防止します。

アイデンティティー、エンドポイント、アプリケーションのリスク評価



テレメトリーと脅威インテリジェンスの共有

統合による相乗効果がサイバーレジリエンスの強化にもたらすメリット

1. ゼロトラスト アクセスの強化：
ゼロトラスト アクセスは、ユーザーのアイデンティティー、デバイス ポスチャー、リアルタイムの脅威コンテキストに基づく適応型のアクセス ポリシーの施行により、脅威のラテラル ムーブメントを防止します。

2. 脅威の検知と修復の自動化：
リアルタイムの検知と脅威インテリジェンスにより、ポリシーの施行やユニバーサル ログアウトなど、調整された即時の対応をトリガーします。

3. リスクの一元的な可視化：
Zscaler Risk360は、CrowdStrikeとOktaのログを統合することで、コンテキスト化されたテレメトリーとリスクに関する包括的なインサイトを提供し、調査と修復を迅速化します。

4. 迅速な調査と対応： CrowdStrike Falcon Next-Gen SIEMとの統合により、一元的な可視性、AI活用型の検知、ワークフローの自動化を実現し、調査と対応を迅速化してクロスドメインの脅威をすばやく封じ込めます。

5. 効率的なアイデンティティー管理
OktaによるSCIMベースのプロビジョニングを活用することで、ユーザーのプロビジョニングおよびデプロビジョニングを安全かつ自動的に行い、承認されたアクセスのみを許可します。

6. ユーザー エクスペリエンスの改善
OktaのSSO、MFA、Zscalerの適応型ポリシーが実現するシームレスなアクセスによって、セキュリティを損なうことなく生産性を向上させます。

まとめ

CrowdStrike、Okta、Zscalerは、現代の進化するデジタルエコシステムに適した形で保護を強化し、複雑さを軽減しながら、拡張性を確保するシンプルな統合セキュリティソリューションを提供します。

各社のソリューションを組み合わせることで、アイデンティティーベースのアクセスを簡素化し、クロスドメインの脅威検知を強化するゼロトラスト防御を提供します。強力なパートナーシップを通じ、組織におけるサイバーセキュリティ態勢のプロアクティブな強化と、AI時代のためのレジリエンスの構築を支援します。

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。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。

Oktaについて

Okta, Inc.は、World's Identity Company™です。アイデンティティを保護することで、すべての人があらゆるテクノロジーを安全に利用できるようになります。当社のカスタマーソリューションとワークフォースソリューションは、企業と開発者がアイデンティティの力を活用してセキュリティ、効率性、成功を推進できるようにし、同時にユーザー、従業員、パートナーを保護します。世界のトップブランドが認証、認可、その他の機能でOktaを信頼する理由については、okta.com/jpをご覧ください。

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™プラットフォームは、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。

各社のソリューションの詳細はこちら

okta.com/jp、crowdstrike.com/ja-jp、zscaler.com/jp |