

Okta、CrowdStrike、Zscalerの 統合で実現する、クロスドメイン およびコンテキスト主導の ゼロトラスト セキュリティ ソリューション

課題

デジタルトランスフォーメーションの取り組みを推進し、分散する従業員をサポートするうえで大きな課題となっているのが、ユーザー、エンドポイント、アプリケーションの保護です。そして、進化し続ける脅威によってこの課題はさらに複雑化しています。

主な攻撃ベクトルとなっているユーザーのアイデンティティ、エンドポイント、アプリケーション、ネットワークは攻撃対象領域を拡大し、リスクを高めます。セキュリティのポイントソリューションは1つの領域に対処するものの、他のソリューションとは適切に統合されず、セキュリティに対する誤った認識を生み出します。このようなアプローチでは、セキュリティに穴が生じ、組織はサイバー リスクやコストのかかる修復作業にさらされることになります。これが、サイバーセキュリティソリューションに多額の資金が費やされているにもかかわらず、サイバー攻撃の件数が減らない理由です。

必要な対策

組織は長年にわたって、セキュリティアーキテクチャーのギャップを解消するために、ポイントソリューションをさらに追加することで、攻撃者に対抗しようとしてきました。しかし、こうした製品を追加しても十分な効果は得られないばかりか、複雑さや対応時間、安全性の問題がさらに悪化する恐れもあります。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。最適かつ高度なセキュリティソリューションをシームレスに連携させることで、セキュリティに対する多層的なアプローチが実現し、運用効率を高めながら複雑さを軽減できます。

ソリューション

ゼロトラスト アプローチでは、リスクに基づいてユーザー アイデンティティ、エンドポイントのコンテキスト、ビジネス ポリシーがリアルタイムかつ継続的に検証されます。このアプローチを採用することで、組織のセキュリティ レベルが向上します。また、サイロ化した従来のポイントソリューションよりもシンプルであると同時に、セキュリティとビジネスのアジリティが強化されるため、デジタルトランスフォーメーションを成功に導くことができます。

強力なセキュリティを実現する統合型セキュリティ

ゼロトラスト アーキテクチャーには、次の3つの基本的な柱があります。



アイデンティ
ティ



エンドポイント



アプリケーション

市場を牽引するOkta、CrowdStrike、Zscalerは、ゼロトラスト ジャーニーに着手したい組織や現在の投資を最大限活用するゼロトラストソリューションを構築したい組織をサポートします。3社の強力な連携と事前テスト済みの統合により、ユーザーからエンドポイント、アプリケーションまで保護するエンドツーエンドのゼロトラストソリューションが実現します。

このソリューションを導入することで、管理者はエンドポイントとアプリケーションの脅威の状況や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。

重要なアプリケーションへのアクセスは、ユーザー、エンドポイント、アクセス ポリシーのコンテキストに基づいて動的に変更できます。また、攻撃が発生した場合、さまざまなプラットフォームで迅速に修復できます。同様の攻撃が今後発生しても阻止できるように、統合全体に防御ポリシーが追加されるため、防御力はさらに強化されます。

コンテキストを活用するクラウドネイティブなゼロトラスト ソリューションは、リスクを軽減するとともに、自社ですべて行う必要があるセキュリティソリューションの複雑さを解消しながら展開を簡素化します。

主なビジネス成果



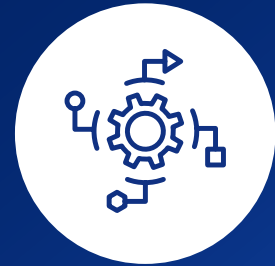
防止

脅威情報とクロスドメインのテレメトリーを共有してゼロトラストのアクセス制御の決定と継続的な検証を行うことで、攻撃対象領域を削減し、不正侵入を防止します。



封じ込め

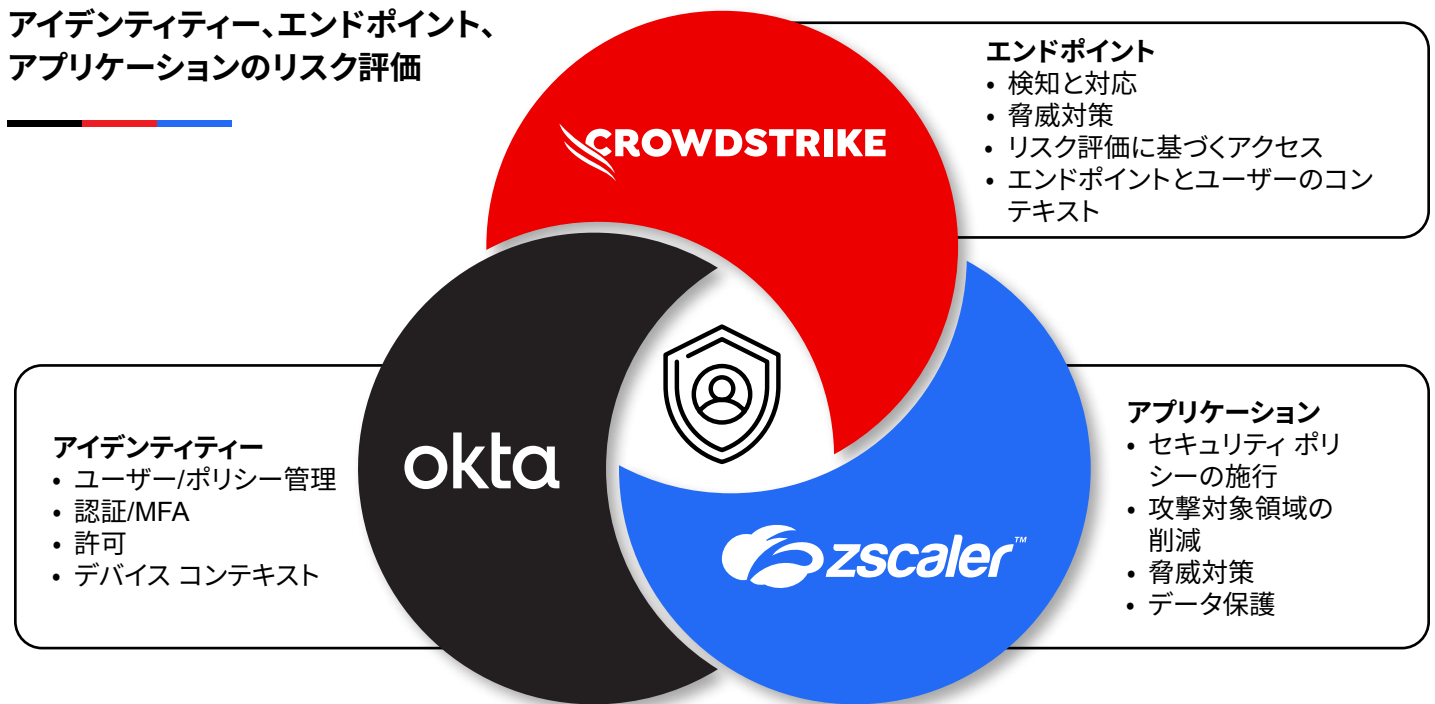
認証情報の侵害やゼロデイ マルウェア、ランサムウェア、内部脅威などの最新の脅威を検知してラテラルムーブメントを阻止し、クロスドメイン施行を実行することで、リアルタイムに脅威を封じ込めます。



対応

コンテキストに基づくテレメトリー共有でマルチドメインの脅威の検知と対応を加速させ、インシデントの発見、トリアージ、調査をスピーディーに行い、より迅速かつ正確に修復します。

アイデンティティ、エンドポイント、アプリケーションのリスク評価



共有テレメトリーと脅威インテリジェンス

