Zscaler AppProtection

プライベート アプリのセキュリティを強化して重大な脅威を阻止

インライン検査で Web ベースの脅威を軽減

プライベート アプリケーションへの HTTP/S トラフィックを検査し、SQL インジェクションやサーバー サイド リクエスト フォージェリー (SSRF) など、OWASP Top 10 に含まれる Web アプリケーションのリスクを軽減します。

Active Directory 攻撃を特定して検出

トラフィックを検査し、Kerberoasting やユーザー列挙などの Active Directory 攻撃に関連する動作を検出することで、Active Directory のセキュリティを強化します。

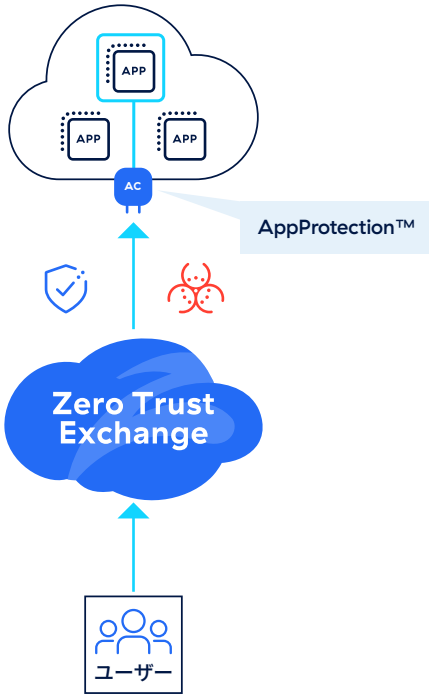
ゼロデイ攻撃とブラウザーベースの脆弱性を防止

Zscaler ThreatLabz が特定した最新の CVE に自動で仮想パッチを適用し、サードパーティー アクセスを保護します。

プライベート アプリケーションのクラウド移行とリモート ワークの普及により、ユーザー、アプリケーション、データが世界中に分散するようになりました。また、インターネット自体が企業ネットワークの一部として機能するようになったことで、従来の「城と堀」のセキュリティ アーキテクチャーはその効果を徐々に失いつつあります。現代の組織に必要なのは、設定ミス、安全でない設計、パッチ未適用のコンポーネントなど、さまざまな脆弱性に対処できる堅牢なセキュリティ ソリューションです。特に OWASP Top 10 で強調されている Web アプリケーションと API のリスクを軽減することが重要な課題となっています。

さらに、Active Directory や LDAP、SMB などの主要なネットワーク サービスの脆弱性は、Kerberoasting やインジェクションなどの攻撃を招く恐れがあるため、きめ細かな監視や高度な暗号化、厳格なアクセス制御の必要性が高まっています。重大な CVE やゼロデイ攻撃が増加している現状に対応するためにも、組織はリアルタイムの脅威検出と予防的なセキュリティ戦略をこれまで以上に優先する必要があります。

Zscaler Private Access™ (ZPA) の重要なコンポーネントである Zscaler AppProtection は、アプリケーション層 (レイヤー 7) のトラフィックを詳細に検査することで、Web ベースおよびアイデンティティーベースの脅威からプライベート アプリケーションを強力に保護します。この高度なソリューションは、脆弱性を悪用したり、アプリケーションの動作を操作したりする悪意のあるトラフィックを検出してブロックします。また、検査機能を ZPA に統合することで、設定ミスや非互換性に伴うリスクも大幅に軽減します。さらに、Zscaler AppProtection はセキュリティ対策と脅威検出を強化するとともに、MITRE ATT&CK フレームワークにも対応しており、Zscaler ThreatLabz チームが提供するタイムリーなシグネチャーと仮想パッチの適用で最新の CVE から組織を保護します。



ユース ケース

プライベート アプリをサードパーティーの Web 脅威から保護
組織は ZPA を通じて、請負業者やパートナー、代理店などのサードパーティーにプライベート アプリケーションへの安全なアクセスを提供するとともに、これらのアプリケーションを Web に起因するリスクから保護し、ブラウザーを通じて実行される不審なアクティビティーを報告する必要があります。

ZPA の重要なコンポーネントである AppProtection は、SQL インジェクション、クロスサイト スクリプティング、サーバーサイド リクエスト フォージェリー、リモート コード実行など、OWASP Top 10 に挙げられている Web ベースの脅威からプライベート アプリケーションを保護します。AppProtection はアプリのトラフィックを継続的に監視することで、悪意のあるアクティビティーを検出します。

また、MITRE ATT&CK フレームワークにも対応しており、信頼関係を偽装した攻撃 (T1199)、ブラウザー セッションの乗っ取り (T1185)、Web サービス (T1102) などの手法を用いたサードパーティーの Web 脅威から保護します。

VPN からの移行時にユーザーのログ パスを詳細に可視化
VPN からの移行は、ゼロトラスト環境を採用する際に考慮すべき重要なユース ケースの一つです。ZPA は、AI を活用した業界初の ZTNA ソリューションです。この移行期間中は、Web アプリケーションや API を利用するすべてのユーザーのドメインとパスへのアクセス状況を可視化することが重要です。

AppProtection は、プライベート アプリケーションにアクセスするユーザーのログをきめ細かく監視し、ユーザー トランザクションとレスポンス コードを詳細に可視化することで、悪意のあるアクティビティーを検出します。

M&A プロセス全体を通して Web およびアイデンティティーの脅威から保護し、コンプライアンスを確保
M&A のユース ケースでは、AppProtection が 2 つの重要な領域でプライベート アプリケーションを保護します。1 つ目は、アプリケーションにアクセスするすべてのユーザーを検査および監視し、OWASP Top 10 のリスクを含む Web ベースの脅威を特定します。2 つ目は、Kerberoasting、LDAP、SMB 列挙などの Active Directory 攻撃から保護しながら、悪意のある内部関係者からのリスクにも対処します。このレベルの保護は、異なる認証情報と認証システムを持つ複数のネットワークやアプリケーションを統合する場合に特に重要です。

製品のメリット

組み込み型の強力なアプリケーション保護機能により、プライベート アプリを標的にした悪意のあるトラフィックを特定し、脆弱性を悪用したり、アプリケーションの動作を操作したりする試みを防止します。管理者は、あらゆる脅威や脆弱性に対する保護を自由に調整し、簡単にカスタマイズできるルール セットによって組織固有のセキュリティ ポリシーを実装できます。

トラフィックのインライン検査による Web ベースの脅威の削減

トラフィックのインライン検査により、ユーザーとプライベート アプリ間のすべての HTTP/S トランザクションを分析し、アプリケーション層 (L7) を可視化します。これは、レイヤー 4 (L4) の従来のネットワーク セキュリティ制御では実現できなかったことです。

OWASP Top 10 のリスクからの保護

OWASP Top 10 対策により、SQL インジェクション、クロスサイト スクリプティング、サーバーサイド リクエスト フォージェリー、リモート コード実行など、最も一般的な Web 攻撃に対して包括的に対応します。

Active Directory 攻撃の特定と検出

Kerberoasting、LDAP、SMB 列挙に関連する不審なアクティビティーを検査および検出することで、Active Directory のセキュリティを強化します。

仮想パッチの適用による最新の CVE の検知と対応

Zscaler ThreatLabz の調査チームが事前定義したシグネチャーを活用して、ゼロデイ脅威を含む最新のセキュリティ脅威から保護します。

ブラウザーベースの不審なアクティビティーの検出と報告

ブラウザー セッションの保護では、ユーザーのブラウザー アクティビティーによって生成された一意のフィンガープリントの数を調べ、その数が異常に多いユーザーにフラグを立てることで、リスクの高いユーザーを特定します。

統合による簡単な展開

ZPA コンソールからの管理により、新しいコンポーネントを環境にインストールすることなく、簡単な展開とスケーラビリティーを実現できます。

MITRE ATT&CK フレームワークへの対応

MITRE ATT&CK® フレームワークは攻撃者の戦術と手法をまとめたナレッジベースで、世界中からアクセスできます。セキュリティ部門が攻撃パターンを理解し、防御戦略を見直すうえで役立ちます。AppProtection はこのフレームワークを活用して、組織のセキュリティ態勢を評価し、サイバー攻撃のリスクを分析します。

MITRE ATT&CK フレームワークの詳細は、こちらをご覧ください：
https://attack.mitre.org/

zscaler™ | Experience your world, secured.™

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.com/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.com/jp