データシート

Zscaler™のAPT（標的型攻撃）対策

Zscalerによる徹底したAPT対策

ハッカーは、人、システム、データに潜むさまざまな脆弱性を見つけ出して悪用し、現状のセキュリティ対策を迂回するようにカスタマイズしたAPT（標的型攻撃）を仕掛けてきます。Zscalerは、シグネチャに依存しない包括的なアプローチにより、APTライフサイクルに対するプロテクションの総合機能を提供します。Zscaler Cloud Security Platformで展開されるプロテクションの総合機能により、企業は、ロケーション、ユーザ、デバイスを問わず、容易かつコスト効率の高いソリューションを実現することができます。

主なメリット

高度なサイバー攻撃を阻止

- 高度なサンドボックス機能とフォレンジック機能を備えた多層型防御フレームワークを活用し、ゼロデイ攻撃などの複合型脅威をブロックします。
- アラート送信だけでなく、特定されたゼロデイ攻撃、インバウンドのマルウェア、感染したデバイスからのアウトバウンドのボットネット通信、およびアウトバウンドのデータ漏えいを自動的にブロックします。
- 250億件／日以上のトランザクションを活用し、包括的な脅威分析、高い検出率、誤検出率の抑制、高速ブロックにより、1,500万超のZscalerの全ユーザを保護します。

本社、支社、モバイルワーカーの保護

- インフラにおいて最も脆弱で、APT攻撃の標的となる、リモートオフィス、モバイルワーカー、デバイス、IoTを万全に保護します。
- 全ユーザのSSLトラフィックを含む双方向のインターネットトラフィックをすべてインラインで検査します。

コスト削減とセキュリティ強化の両立

- 多層型セキュリティをクラウドで提供し、幅広いセキュリティソリューションを統合型SaaS（Security as a Service）プラットフォームで実現します。
- 管理者の生産性向上を可能にし、初期費用／運用費用を削減し、ネットワークパフォーマンスを向上し、セキュリティイベントのコストを削減します。
- アプライアンスベースの従来型アプローチによるエンタープライズセキュリティの複雑性やセキュリティギャップを解消します。インターネットゲートウェイごとにセキュリティアプライアンスを用意する必要はありません。

機能と特長

高速双方向インラインインスペクション

Zscalerは、高速双方向コンテンツインスペクションを可能にする独自アーキテクチャによって、リアルタイムですべてのインターネットトラフィックをスキャンし、脅威を特定して自動的にブロックします。

統合型SSLトラフィックインスペクション

Zscalerは、100%クラウドのサービスであるため、SSLトラフィックインスペクションを双方向インラインスキャンにシームレスに統合できます。パフォーマンスの低下は発生せず、ハードウェアやソフトウェアの追加も不要です。

行動分析と自動ブロック

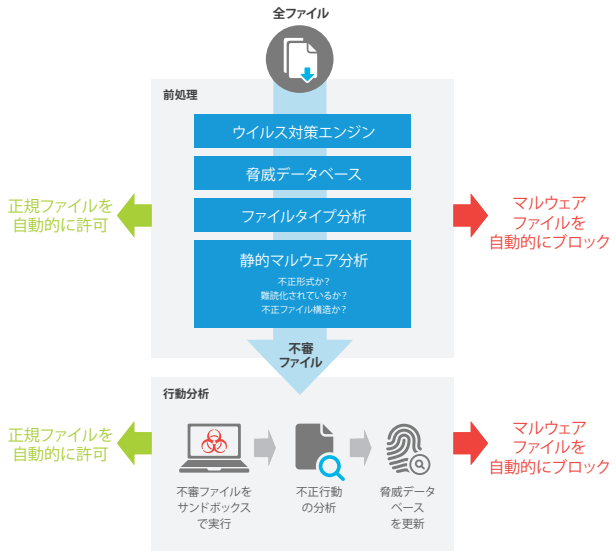
不審オブジェクトは、適切に管理されたサンドボックス内で自動的に実行され、監視されます。ゼロデイマルウェアなどの不正行動は、自動的に記録・分析され、15万超のZscalerユーザを保護します。

ハイパフォーマンスのマルウェア／不正URL対策

Zscalerは、既知の不正URLに対する要求を特定し、シグネチャおよびヒューリスティックの複数のテクノロジを利用して既知のウイルスやワームを検査し、ユーザを保護します。Zscalerのクラウドアーキテクチャは、レイテンシのない高速での保護を実現します。

データ漏洩／不正通信対策

Zscalerは、非許可コンテンツを含むすべてのインターネット接続トラフィック（SSLを含む）を自動的にブロックし、許可されていないポート、プロトコル、およびクラウドアプリケーションを禁止することで、攻撃者がこれらのチャネルを通信やデータの不正持出しに使用できないようにします。インラインスキャンによって、ボットネットのコマンド＆コントロール（「C&C」）サーバを含む感染マシンによる通信を識別し、自動的にブロックします。



ブラウザ制御

Zscalerのブラウザ制御は、インターネットアクセスを特定のブラウザバージョン、パッチレベル、許可プラグイン、およびアプリケーションに制限するポリシーを適用することで、既知の脆弱性に対する攻撃を回避します。

行動分析	スタンダード	アドバンスド
Zscalerクラウドベースサンドボックスに送信されるもの	Zscalerの多層型セキュリティによる処理後に不審ファイルを自動的にサンドボックスに送信	同じ
Zscalerクラウドベースサンドボックスに送信されるファイルタイプ	• Windows 32ビット版と64ビット版の実行可能ファイル • Windows 32ビット版と64ビット版のダイナミックリンクライブラリ、システムファイル、ActiveXコントロール、およびスクリーンセーバー	• Windows 32ビット版と64ビット版の実行可能ファイル • Windows 32ビット版と64ビット版のダイナミックリンクライブラリ、システムファイル、ActiveXコントロール、およびスクリーンセーバー • Microsoft Office文書 • Adobe PDFファイル • Adobe Flashファイル • Javaアプリケーション／アプレット • 最大5段階の圧縮によるZIP／RARアーカイブ • Android APKファイル
保護対象のトラフィックタイプ	インターネットの不審な場所を起源とするファイル	インターネットのあらゆる場所を起源とするファイル
クラウドのメリット：他のZscalerクライアントで不正としてすでに特定されているファイルが見つかった場合の動作	• Windows 32ビット版と64ビット版の不正DLL／EXEを瞬時にブロック • その他の悪意のあるファイルは許可するが、フラグを設定	すべての不正ファイルをポリシーに基づき瞬時にブロック、隔離、またはフラグ付け
隔離機能と隔離ポリシー	• 隔離機能なし • 隔離ポリシーなし	• 完全隔離機能 - イベントによる被害を回避 • ファイルの種類、場所、ユーザなどによるきめ細かな隔離ポリシー
インスペクションポータルへのアクセス（不審ファイルをZscalerクラウドベースのサンドボックスに送信して検査が可能）	×	○
ログ、レポート、分析	包括機能	同じ
フォレンジックレポート／分析	なし	詳細 - お客様の環境で発生し、Zscalerのクラウドサンドボックスによって検出されたすべての不正ファイルの全情報

Zscalerについて

Zscalerでは、インターネットセキュリティに革命を起こす業界初のSaaS（Security as a Service）プラットフォームを提供しています。350億ドル規模のセキュリティ市場における革新的な企業として、ZscalerはFortune 500の50社を含む5,000以上の著名な企業・団体に利用されています。企業ポリシーや法規制を遵守しつつ、サイバー攻撃や情報漏えいからワールドワイドで1,500万超のユーザの安全を守っています。

Zscalerは、ガートナーマジッククアドラントのセキュアWebゲートウェイ部門でリーダとして評価されており、100%のクラウド環境にて、ロケーションやデバイスを問わずあらゆるユーザに安全かつ生産性の高いインターネットエクスペリエンスを提供しています。マルチテナントの分散型クラウドセキュリティプラットフォームを通じて、効果的にセキュリティ環境をインターネットバックボーンに構築し、世界中100ヵ所以上のデータセンタで運用されています。妥協を許さない卓越したプロテクション機能とパフォーマンスの元に、組織がクラウドおよびモバイルコンピューティングを存分に活用することを可能にしています。Zscalerは、オンプレミスのハードウェア、アプライアンス、あるいはソフトウェアを必要とせず、統合されたキャリアグレードのインターネットセキュリティ、次世代ファイアウォール、Webセキュリティ、サンドボックスを活用したAPT（標的型攻撃）対策、DLP（情報漏えい防止）、SSL暗号化、トラフィックシェイピング、ポリシー管理、そして脅威インテリジェンスを提供しています。詳細は www.zscaler.com をご覧下さい。

お問い合わせ

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

SNS

- facebook.com/zscaler
- linkedin.com/company/zscaler
- twitter.com/zscaler
- youtube.com/zscaler
- blog.zscaler.com