ソリューション概要

Zscaler™ Cloud Sandbox

ランサムウェアやポリモーフィック型脅威からの保護

Zscaler Cloud Sandboxは、高度行動分析手法を使用してゼロデイ脅威を発見し、ブロックします。世界最大のセキュリティクラウドのサービスとして提供されるZscaler Cloud Sandboxは、他のどのソリューションよりも高レベルの脅威防御を実現します。

ZSCALER CLOUD SANDBOXを選択すべき理由

スケーラビリティ：高価なアプライアンスやアーキテクチャの制限から解放されます。Zscaler Cloud Sandboxは、容易な拡張によって、リモートオフィスやモバイルユーザを含む組織全体の保護を可能にします。

高レベルの保護：Zscaler Cloud Sandboxは、SSLトラフィックを含むすべてのトラフィックのネイティブかつインラインの保護を可能にする、Zscaler Cloud Security Platformに統合されたサービスです。

クラウドのメリット：Zscaler Cloud Sandboxで発見されたすべての新しい脅威は、Zscaler Cloudでただちに共有され、全ユーザの保護に活用されます。他のサンドボックスでは得られない優れた可視性を活用し、効率的な方法でユーザを保護できます。

コスト効率：Zscaler Cloud Sandboxはサービスとして提供されるため、アプライアンスのパフォーマンスを確保するための過剰なコストは発生しません。ニーズに合わせて従量制で利用でき、機能に合わせた拡張が可能であるため、能力不足に悩まされることもありません。

従来型のセキュリティ対策では見逃されてしまう脅威もブロック

最近では、従来型のシグネチャに頼るセキュリティ対策だけでは不十分であることが広く認識されるようになりました。この方法には、シグネチャを使って脅威を阻止するには、その脅威を事前に認識しておく必要があるという大きな欠点があります。ゼロデイランサムウェアやポリモーフィック型マルウェアの急増を考えれば、シグネチャベースの検知だけでなく、サンドボックスを新たな防御層として追加した対策が間違いなく必要になるでしょう。サンドボックスは、動的分析を使用して、隔離された環境でのファイルの動作を監視することで、ゼロデイ脅威からのユーザの保護を可能にします。

アプライアンスベースのサンドボックスでの問題として、中央のゲートウェイにアプライアンスを導入する方法が採られており、すべてのトラフィックを一元的にルーティングするハブ&スポークアーキテクチャが必要である点が挙げられます。つまり、リモートオフィスからのトラフィックの場合は、高コストのMPLS（マルチプロトコルラベルスイッチング）を使用してバックホールする必要があり、しかも、モバイルユーザは低速のVPN接続を使用しなければなりません。

サンドボックスアプライアンスそのものにも処理能力の限界があり、この制約によって、マルウェアの大部分が隠れている可能性があるSSLの場合は特に、検査可能な量が制限されることになります。管理、ソフトウェアの更新、さらには他のセキュリティアプライアンスとの適切な統合コストが所有コストに加算されるため、予算やITの要件の増大という問題もあります。

> 「大規模データセットを使った我々の分析で、マルウェアハッシュの99%は継続時間が58秒以下であることがわかりました。この結果から、検出を回避するために短時間でコードが変更されていることがわかります。」
>
> **– *Verizon***, 2016年データ侵害調査レポート

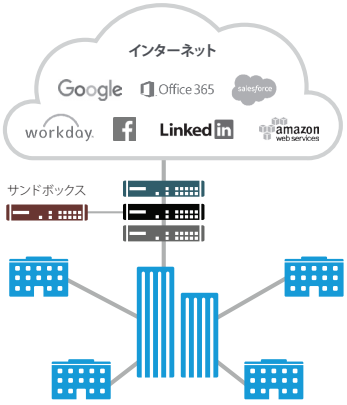
ZSCALER CLOUD SANDBOX

Zscalerでは、トラフィックをデータセンタにバックホールすることなく、不審ファイルや未知のファイルをサンドボックスで処理できます。Zscaler Cloud Sandboxはクラウドから実装されるため、あらゆる場所のユーザが保護されます。つまり、リモートオフィスやモバイルのユーザであっても、高コストのMPLSリンクや面倒なVPN接続を必要とすることなく、本社のユーザと同じレベルで保護されます。

Zscaler Cloud Sandboxは、インライン保護によって、ネットワークに侵入する前に脅威をブロックするように設計されています。ポリシーの定義によって、不正ファイルを直ちにブロックすることも、隔離することも、フラグを設定することもできます。アプライアンスベースのサンドボックスで、スキャン中にランサムウェアがエンドポイントに到達してしまった場合、仕方のないことと諦められるでしょうか。

ハブ&スポーク方式のサンドボックス

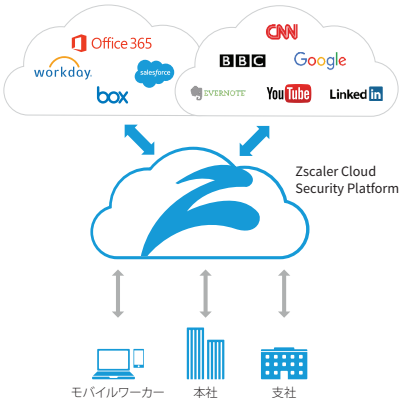
高コストで不十分な保護



- アプライアンスとバックホールリンクのコストが高い
- サンドボックスがインライン処理されないことが多い
- ネットワークの外部のユーザが保護されない

Zscaler Cloud Sandbox

コスト効率が良く完全な保護



- ユーザエクスペリエンスの向上と導入／管理コストの効率化
- あらゆるロケーションのユーザに同じレベルのインライン保護を提供

Zscaler Cloud Sandboxのハードウェアベースのサンドボックスに対する優位性：

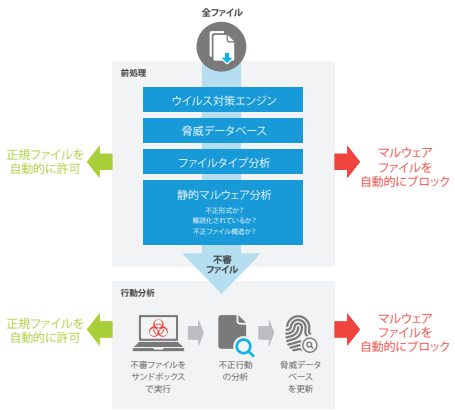
- 警告だけにとどまらない、真のゼロデイマルウェア対策
- モバイルユーザやリモートオフィスユーザを含む全ユーザの全デバイスに同じポリシーを適用
- SSLを含むすべてのトラフィックを検査
- インバウンド／アウトバウンドトラフィックのインスペクションにより、ボットネットの通信とデータの流出を防止
- 未確認のロケーションからのすべての未知のトラフィックとファイルをサンドボックスで処理し、すべての実行可能ファイルをブロック
- 継続的にアップデートされる最新の脅威情報を使用 - 毎日120,000件以上の一意のアップデート

独立して動作するアプライアンスとは異なり、Zscaler Cloud Sandboxは、Zscaler Cloud Security Platformに完全統合されているため、最大限の脅威の可視性と多層型の保護が実現します。Zscalerはサービスとして提供されるため、導入して管理する必要があるハードウェアも、更新を必要とするソフトウェアも存在しません。

SSLを含むすべてのトラフィックをサンドボックスで保護

Zscaler Cloud Sandboxでは、その優れた処理能力によって、あらゆる不審ファイルや未知のファイルが効率的に検査されます。複数のセキュリティエンジン間でのデータの関連付けにより、従来のアプライアンスでは検出できない高度な脅威を特定し、ブロックできます。

サンドボックスの前処理でこれらの手順が実行されるため、不審ファイルの検出が合理化されて、ユーザエクスペリエンスが向上します。さらには、SSL検査がネイティブでクラウドセキュリティプラットフォームに組み込まれているため、暗号化に隠れた攻撃が見逃されることもありません。ポリシーを定義して、不正ファイルを即座にブロック、検疫、またはフラグを設定することができ、ポリシーの範囲を全ユーザに簡単に拡大できます。



Zscaler Cloud Sandboxは、1日あたり300億件以上の要求の処理によって得られたクラウドインテリジェンスを使用し、120,000件以上の一意のセキュリティアップデートを毎日実行しています。Zscaler Cloudのあらゆる場所で脅威が特定され、全ユーザがその脅威から保護されます。Zscaler Cloud Security Platformは、デフォルトですべての実行可能ファイルとライブラリをサンドボックスで処理することで、全ユーザの強力な保護を実現します。Zscalerには、40以上のパートナーの脅威フィードも組み込まれており、最新の脅威情報がクラウド全体に適用されるため、サンドボックス処理が必要なファイルを最小限に抑えることができます。

Zscaler Cloud Sandboxは、以下の優れた機能を備えています。

統合プラットフォームサービス

- 40以上のセキュリティパートナーからの脅威フィードを使用して、既知のあらゆる脅威を事前にフィルタリング
- ネイティブSSLインスペクションによる広範かつ万全のセキュリティ
- 標的型攻撃対策 - インバウンドとアウトバウンドの両方のトラフィック
- 豊富なフォレンジック - ユーザ、ロケーション、起源、回避方法などのインテリジェンス

すべての不審ファイルと未知のファイルのインラインインスペクション

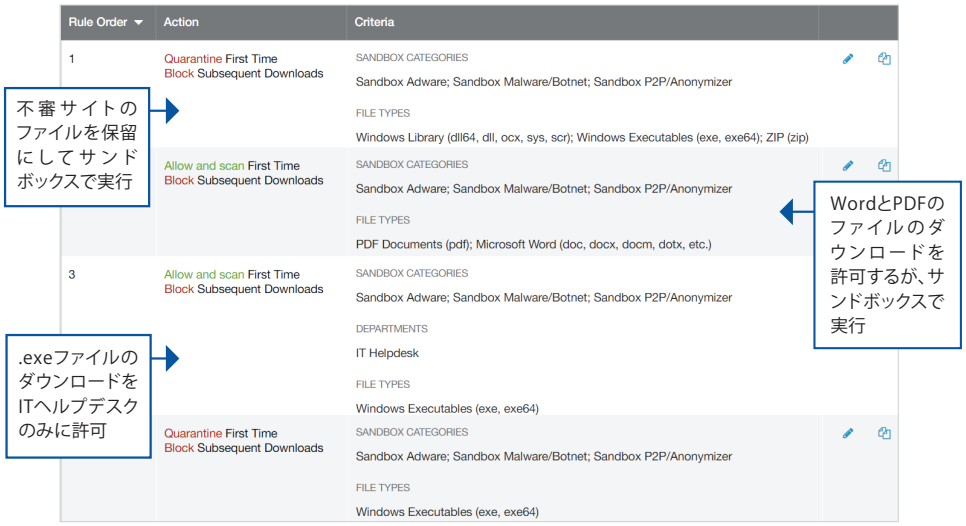
- 実行可能ファイル、ライブラリ、Office文書、アーカイブ、Web、モバイルコンテンツの完全分析
- 強制的な隔離によってあらゆる被害を回避し、サンドボックススキャンポータルによる手動ファイル送信も可能

すべてのユーザとロケーションに統一ポリシーを適用

- グローバルポリシーを単一コンソールから定義
- あらゆるロケーションの全ユーザにポリシーの変更を直ちに適用

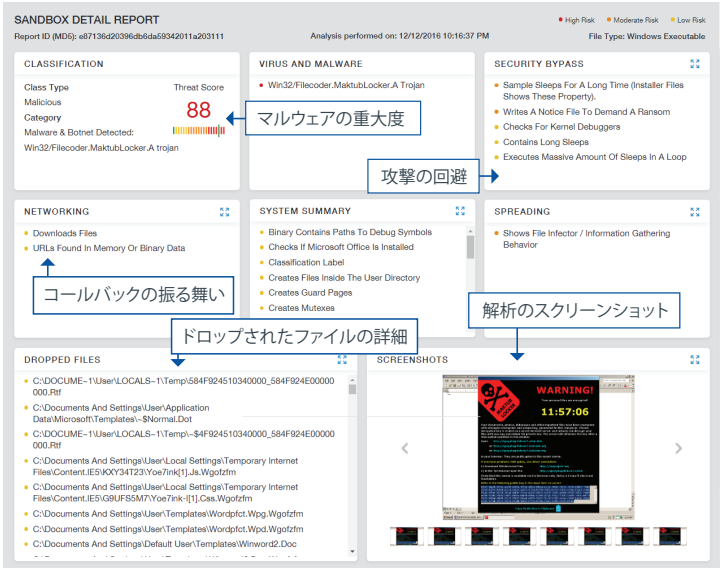
セキュリティポリシーの最適化で強力な保護と優れたユーザエクスペリエンスを実現

Zscaler Cloud Sandboxでは、保護のニーズに合わせて柔軟にセキュリティポリシーを調整できます。ポリシーを記述し、サンドボックス処理するファイルのユーザやファイルタイプなどを指定することもできます。たとえば、CFOがダウンロードしようとした未知のスプレッドシートをサンドボックスで処理して隔離するように指定しておけば、CFOのラップトップの感染を防止できます。



ZSCALER CLOUDのサンドボックス分析を完全可視化

マルウェアの詳細分析が必要な場合には、Zscaler Cloud Sandboxの豊富なレポート機能を利用して、感染と関連性のあるすべての動作を調査できます。また、内部調査を実施する場合であれば、重要なIOC（Indicators of Compromise）を検証できるだけでなく、SIEM（Security Information and Event Manager）にログを転送してセキュリティ対策をさらに合理化することもできます。



CRYPTOLOCKER攻撃：ZSCALER CLOUD SANDBOXの導入効果

グローバルに事業を展開している銀行が、Zscaler Cloud Sandboxの評価を開始し、最小限の構成で運用を開始した直後に、初めてのCryptoLocker攻撃を経験しました。6時間で352件のCryptoLockerに感染したメールが従業員に送信されました。この攻撃では、114件のメールが同行の以前から実施していた対策を突破して侵入しました。9人の従業員が、メールに埋め込まれたリンクをクリックして、マルウェアのペイロードをダウンロードしてしまいました。ランサムウェア被害が深刻なのは身代金を要求されるためだと考えがちですが、生産性への影響も考慮すべきでしょう。

Zscaler導入前のランサムウェア攻撃

- 9人の従業員のアカウントがロックされ、マシンとプロファイルを再構築しなければならなかった
- 6,769のネットワークファイル共有をバックアップからリストアしなければならなかった
- 11のIBMリソースをリストアする必要があり、その作業に121時間を要した
- 9人編成のコンピュータ緊急対応チーム（CERT）でリソースをリストアする必要があり、その作業に108時間を要した
- 5日間に4回の経営陣向け現状説明を実施した
- 管理に45時間を費やした

Zscaler導入後のランサムウェア攻撃

最初の攻撃から1週間以内に、同行は再び、CryptoLocker攻撃を経験しました。ただし、この段階では、全ユーザのZscaler Cloud Sandboxが有効になっていました。6時間で5,405件の感染メールが着信し、そのうちの169件がユーザの受信ボックスに送信されました。また、11人の従業員が感染メールのリンクをクリックしてしまいましたが、今回は感染被害がありませんでした。

「設定した機能が想定通りに正しく動作したことが証明されました。」

- Zscalerの金融機関のお客様

クラウドのメリット：ZSCALER CLOUD SANDBOXと他のソリューションとの比較

Zscaler Cloud Sandboxは、世界最大級のセキュリティクラウドに統合されているため、アプライアンスベースの製品や他のクラウドソリューションでは不可能な規模のゼロデイからの保護が可能です。

2016年3月、Zscalerのユーザである航空業界のお客様が、初めての攻撃を経験しました。Zscaler Cloud Sandboxによる分析で脅威がブロックされ、30秒後には、全世界の1,500万のZscaler Cloudユーザをこの脅威から保護できるようになりました。アプライアンスベースのサンドボックスだったとしたら、どれ位の時間が必要だったでしょうか。

「Zscalerを検討したことで、高レベルの保護を可能にする優れた製品が見つけることができました。」

– Zscalerの航空業界のお客様

ランサムウェア／マルウェア（Nymaim）

Time [GMT]	MD5	Policy Action
Tue Apr 26 **15:48:24** 2016	59b1bceb22f55510dbe919a394e858f5	Quarantined
Tue Apr 26 **16:19:01** 2016	59b1bceb22f55510dbe919a394e858f5	Block
Tue Apr 26 16:20:01 2016	59b1bceb22f55510dbe919a394e858f5	Block

Infostealerトロイの木馬（Banload）

Time [GMT]	MD5	Policy Action
Tue Mar 15 **12:39:13** 2016	e1a1387c22b095cdb3195fa7c6eb0595	Quarantined
Tue Mar 15 **12:40:41** 2016	e1a1387c22b095cdb3195fa7c6eb0595	Block
Tue Mar 15 **12:50:05** 2016	e1a1387c22b095cdb3195fa7c6eb0595	Block
Tue Mar 15 13:05:47 2016	e1a1387c22b095cdb3195fa7c6eb0595	Block
Tue Mar 15 13:05:57 2016	e1a1387c22b095cdb3195fa7c6eb0595	Block
Tue Mar 15 13:06:08 2016	e1a1387c22b095cdb3195fa7c6eb0595	Block
Tue Mar 15 13:06:14 2016	e1a1387c22b095cdb3195fa7c6eb0595	Block

最初の検出から30秒以内に、1,500万のZscaler Cloudの全ユーザをこのマルウェアから保護

ZSCALER CLOUD SANDBOXを選択すべき理由

スケーラビリティ

高コストのゲートウェイベースアーキテクチャから脱却し、あらゆるロケーションの全ユーザの保護をクラウドから容易に拡大可能

強力なプロテクション

完全統合型サンドボックスソリューションにより、SSLを含む全トラフィックのインスペクションをパフォーマンスの制限なく実行可能

高いコスト効率

ニーズに合わせて保護対象を簡単に拡張できるため、最小限のIT取得／管理コストで運用可能

クラウドインテリジェンス

世界最大規模のセキュリティクラウドの機能と可視性でサンドボックス処理を強化

Zscaler Cloud Sandboxを瞬時に有効化

実績豊富なZscaler Cloud Security Platformを既にご利用いただいている場合、ワンクリックでZscaler Cloud Sandboxを有効化できます。

THE ZSCALER CLOUD SECURITY PLATFORM

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5,000超の企業・公的機関の1,500万人超の従業員の安全を守っています。受賞歴を誇るZscaler Cloud Security Platformは、あらゆるユーザ、あらゆるデバイス、あらゆる場所で、安全で生産性の高いWebエクスペリエンスを実現します。セキュリティ環境を効率的な方法で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。詳細は、**www.zscaler.com** をご覧ください。

CONTACT US

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

www.zscaler.com

FOLLOW US

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