EBOOK

脅威対策の購入ガイド

ファイルベースの攻撃を阻止するための AI 活用型脅威対策ソリューションの選び方

目次

脅威の最新状況を踏まえたセキュリティの再考 **3**

デジタル環境には対応しきれない境界のみのセキュリティ 3

急速に進むクラウドへの移行を悪用する攻撃者 3

進化が求められるゼロデイ マルウェア対策 **4**

クラウド サンドボックスの要件 **5**

大規模な復号と検査 6

一元化されたポリシー管理とルール 7

リスク許容度とパフォーマンスの期待値に合わせたポリシー 7

効率的な分析と脅威インテリジェンス 8

AI を活用したマルウェア対策エンジン 8

脅威インテリジェンスを活用した SOC ワークフロー 8

MITRE ATT&CK フレームワークを活用した SOC 強化 9

購入前に確認すべき項目 10

Zscaler Cloud Sandbox と高度な脅威対策 **11**

真のクラウドネイティブなインライン型サンドボックスとは 11

脅威の最新状況を踏まえたセキュリティの再考

デジタル環境には対応しきれない境界のみのセキュリティ

ハイブリッド ワークやクラウドホスト型のアプリケーションへの移行に伴い、組織のリソースにアクセスする手段が変化し始めています。従業員は、リモート ワークや外出先での生産性を維持するために、管理対象外のデバイスから公共 Wi-Fi などの保護されていないネットワークを使用しており、事実上、インターネットが新たな企業ネットワークとなりつつあります。このアクセス ポイントの拡大により、従来の「城と堀」のセキュリティアプローチでは、ユーザー、アプリケーション、データを保護するには不十分になっています。インターネットへの直接接続アクセスはネットワーク中心の制御を回避し、多くの場合、セキュリティよりも使いやすさが優先されるため、境界型の防御だけに依存するとリスクが増大します。

従来のセキュリティ制御を簡単に回避する次世代のサイバー攻撃に対抗するには、境界ではなく、ユーザー、ワークロード、OT/IoT の保護に焦点をあて、セキュリティそのものをユーザーに近づける必要があります。

急速に進むクラウドへの移行を悪用する攻撃者

セキュリティ部門は難題に直面しながらも、従来のセキュリティ制御を現代のモバイルファースト、クラウドファーストの環境に適応させるために最善を尽くしていますが、ここで生じた「溝」こそが、攻撃側を有利な状況に導いています。組織が複数あるネットワーク エッジの保護に奮闘する一方で、マルウェアに対する防御は不十分であることが、Zscaler ThreatLabz の調査結果からも明らかになっています。

- 暗号化されたチャネルを介して配信される脅威は全体の **86%**（暗号化された攻撃の 78% はマルウェア）[1]
- ランサムウェア攻撃は前年比で **40%** 増加 [2]
- Zscaler Sandbox で確認されたペイロードは **58%** の急増 [2]

このデジタル脅威の急速な進化とクラウドの攻撃対象領域の拡大に対応するために、セキュリティ部門は戦略を再評価し、最新のサイバー リスクに対する防御を強化する必要があります。

1. 2023 年版 Zscaler ThreatLabz 暗号化された攻撃の現状レポート
2. 2023 年版 Zscaler ThreatLabz ランサムウェア レポート

進化が求められる
ゼロデイ マルウェア対策

攻撃者には**スピード**と**拡散**という 2 つの主な強みがあります。マルウェアの開発者は、防御側が定義するよりも速く脅威を作り出し、人工知能 (AI) を活用して、従来のセキュリティ対策や検出方法を回避できる亜種を生み出しています。

悪意のある添付ファイルやリンクを使用したフィッシングは、今日でも最も一般的な手口です。暗号化トラフィックの広範な使用によって、その防御戦略はいっそう複雑化します。現代の脅威は暗号化トラフィックに潜んでいることが多く、すべての Web トラフィックおよび非 Web トラフィックを検査することが重要です。検査を行わなければ、知らず知らずのうちに組織のネットワークへのマルウェアの侵入を許してしまうことになりかねません。

サンドボックスはセキュリティ スタックの重要な機能であり、悪意のあるファイルやコードの実行を防止する手段です。これは本来、既知のマルウェア向けの EDR やその他のスキャンを回避する未知のファイルベースの攻撃に対する効果的な防御策となる存在です。しかし、残念ながら多くのサンドボックスはアウトオブバンドで展開されており、NGFW、クラウド セキュリティ製品、エンドポイント エージェントから転送されるマルウェア サンプルを利用しています。

このため、多くの場合、検出が行われるのはマルウェアがユーザー デバイスにダウンロードされた後になり、ペイシェント ゼロにマルウェアやランサムウェアへの感染を許してしまいます。当然、これはゼロトラストの概念に反しています。また、生産性を損なうことなくペイシェント ゼロの発生を防ぐインラインの防御を提供するには、大規模な AI/ML 分析を活用して未知の脅威や疑わしいファイルを自動的に検出して検疫することが重要ですが、多くのサンドボックスはそのような機能を備えていません。

シグネチャーベースのウイルス対策や侵入防止システム (IPS) だけでは、ゼロデイ脅威やポリモーフィック型の脅威を防止できません。

クラウド サンドボックスの要件

これまで、攻撃者はクラウド環境で変化していくアーキテクチャーを不正利用することで優位に立ってきました。

ペイシェント ゼロからの感染を防ぎ、高度な標的型攻撃によるネットワークへのアクセスを阻止するためには、適切なクラウド サンドボックスを選択することが重要です。

次のセクションでは、クラウド サンドボックスを選択する際に考慮すべき具体的な要件を解説しています。

大規模な復号と検査

プライベートな通信や機密情報を安全に保護する暗号化は、その効果の高さからセキュリティのトレンドになりましたが、残念ながら、サイバー犯罪者は悪意のあるペイロードを隠すために暗号化されたトラフィックを利用しています。

トラフィックの復号と検査は計算負荷の高いプロセスのため、高性能のサンドボックス アプライアンスでも役に立たないほどパフォーマンスが低下し、許容範囲を超えたレイテンシーでビジネスの中断を招く可能性があります。

最新のサンドボックス ソリューションを評価する際は、レイテンシーのない無制限の復号と検査をインラインで提供できるベンダーを選ぶことが重要です。

HTTPS 経由の脅威は前年比で 24.3% 増加し、2023 年の暗号化攻撃は 300 億件に上りました。[3]

購入時のチェックリスト：

- ☐ SSL トラフィックの復号に追加のハードウェアや仮想マシン (VM) のインストールを必要としない
- ☐ レイテンシーや容量制限なしで以下の種類のファイルを検査、分析できる

EXE	DOC(X)	TAR
DLL	XLS (X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	ZIP ファイル内のスクリプト ファイル
SWF	BZ2	

3. *2023 年版 Zscaler ThreatLabz 暗号化された攻撃の現状レポート*

購入時のチェックリスト：

- ☐ 企業ネットワークの内外を問わず、すべてのユーザーにすぐにポリシーを施行し、同一の保護を提供できる
- ☐ 不審な送信元からのファイルに対する高度な検疫ルールと機能を搭載している
- ☐ 一元化されたポリシー管理によってサンドボックス操作をきめ細かく制御できる (ファイル タイプの許可や疑わしい送信元からの自動保留など)

一元化されたポリシー管理とルール

クラウド型の一元的なポリシー管理とルールによって、ルールの管理ミスがなくなるだけでなく、各ゲートウェイのサンドボックスを手動で構成する必要もなくなります。**NIST 800-207** で説明されているゼロトラストの原則に則した、動的かつ適応性のあるポリシーを備えたソリューションが求められます。ゼロトラストでは、ユーザーの役割や場所、デバイス ポスチャー、リクエストされたデータなどのコンテキストに基づいてアクセスとセキュリティ ポリシーを確立し、攻撃対象領域を最小化します。クラウド型のソリューションには、組織内のすべてのユーザーを対象に脅威をブロックするというメリットもあるため、ファイルの事後検証 (例：帯域外の検査や事象発生後の保護の適用など) が不要となり、より同期性の高いセキュリティが実現します。サンドボックス ポリシーの重要な側面として、異なるユーザー グループ、場所、URL カテゴリー、アクションに対してきめ細かいルールを設定し、ビジネスを柔軟にサポートできることが挙げられます。きめ細かい制御により、組織のリスク許容度とパフォーマンスの期待値に合わせてポリシーを調整することが可能です。

リスク許容度とパフォーマンスの期待値に合わせたポリシー

クラウド サンドボックスのソリューションは、リスクを制御しながら組織固有のニーズに合ったポリシーを施行する必要があります。最初に組織の状況を確認します。

- **悪意のあるファイルに対して許容度が低い場合：**リスクの回避を重視する組織では、未知のファイルまたは不審なファイルに対して、初回アクションに「検疫」を選択でき、ダウンロード前にサンドボックスでファイルを分析することでペイシェント ゼロの発生を防ぐことができます。
- **ファイルの検疫に対して許容度が低い場合：**リスク許容度が高く、遅延や中断を回避したい組織の場合は、初回アクションに「検疫と分離」を選択できます。このアクションにより、サンドボックスがクラウド ブラウザー分離機能と統合されます。ユーザーはアクティブ コンテンツのない読み取り専用 PDF にすぐにアクセスでき、その間サンドボックスは有害な可能性のあるファイルをバックグランドで分析します。

組織が抱えるニーズがどのようなものであろうと、ポリシーは単一のプラットフォームからすべてのユーザー、グループ、部門、場所、場所グループに対して簡単に施行できる必要があります。

効率的な分析と脅威インテリジェンス

攻撃者は以前成功した攻撃を再度利用することが多いため、セキュリティ関連コミュニティーと保護情報を共有して、脅威を速やかに阻止することが重要です。クラウド サンドボックスはテレメトリー データを取得し、新たに特定された脅威から得たインサイトを脅威フィードやセキュリティ関連コミュニティーと共有する重要な役割を果たします。

AI を活用したマルウェア対策エンジン

クラウド配信のサンドボックスは、計算負荷の高い AI/ML モデルを管理して、より優れた保護機能を提供します。

高度な AI/ML を使用して、追加の分析を必要とせず未知の脅威や疑わしい脅威をインテリジェントに特定、検疫、防止するサンドボックスが求められます。

- **ファイルの即時判定：**悪意のある可能性が非常に高いファイルを即座に識別できれば、ユーザーが判定を待たされることはありません。
- **ゼロデイ予防：**信じがたいことですが、すべてのサンドボックスがダウンロードを許可する前に未知の脅威を検疫し、ペイシェント ゼロの発生を防げるわけではありません。

脅威インテリジェンスを活用した SOC ワークフロー

アナリストは、1 つの脅威の調査に何時間も費やすことがあります。悪意のあるペイロードの行動に関するインサイトや脅威インテリジェンスを共有することで、このような負担を軽減し、調査と対応をスピードアップさせるクラウド サンドボックスが求められます。セキュリティ部門は、アウトオブバンドの API 送信を通じたサンドボックス内での直接ファイル分析で調査をサポートできる必要があります。脅威フィードが既存のセキュリティ ツールと統合できることも重要です。具体的には、報告された URL の最新のコンテキスト、抽出された侵害の痕跡 (IoC)、MITRE ATT&CK® などのサイバーセキュリティ フレームワークに沿った戦術、技術、手順 (TTP) が含まれます。

購入時のチェックリスト：

- AI/ML を活用してファイルに対する即時の判定を下し、ファイル分析を必要とせずに脅威を阻止できる AI ベースの検疫機能
- 場所を問わず、ユーザーやネットワーク間で共有される日常的な脅威にプロアクティブに対応できる
- 脅威フィードを既存のセキュリティ ツールと統合できる
- プログラムによる API 活用型「アウトオブバンド」サンドボックス ファイル送信と、API で送信されたファイル用の個別のキュー

脅威スコアを提供するだけでなく、使用されている回避技術の概要を示すことのできるサンドボックスを選択してください。回避技術とは、たとえば以下のようなものです。

- サンドボックスでの検出を回避するためにコードの実行を遅らせる
- ネットワークを通過するトラフィックをキャプチャーして表示する
- リモート接続を許可するためにポートを開放する
- より価値の高いターゲットを見つけるためにラテラル ムーブメントを試みる
- リモート コントロールを許可しようとする

レポート

レポート機能のあるセキュリティ ソリューションは、レポートの実用性が高いほど有益です。クラウド サンドボックスのレポートには、以下が求められます。

- 悪意のある攻撃のライフサイクル全体が含まれる
- シンプルな操作性で簡単に使える
- 概要を簡単に把握できる
- アプリケーション プログラミング インターフェイス (API) を介して利用でき、既存のログと関連付けられる
- コンプライアンス レポートもサポートする大規模なプラットフォームの一部である

MITRE ATT&CK フレームワークを活用した SOC 強化

レポート機能を評価する際は、**MITRE ATT&CK のフレームワーク**にマッピングできるサンドボックス インテリジェンスを検討します。この機能により、SOC チームは提供された分析情報を適用してセキュリティ スタックの他の部分で戦術的な防御を構築できます。このように、サンドボックスはセキュリティ運用ワークフローにおいて欠かすことができません。

フレームワークに対する組織の成熟度に応じて、レポート機能は以下のような目的で使用できます。

- 提供された分類情報を使用してラベル付けの負担を軽減する
- エンドポイントでの検知と対応 (EDR) ソリューションを回避する可能性のあるステルス技術を確認する
- 他の各種制御と比較対照する
- 闇雲にすべての戦術や手法を阻止するのではなく、自社をターゲットにしている最も一般的な TTP に焦点をあてる
- リバース エンジニアリング レポートを作成する

購入前に確認すべき項目

ここでは、購入前に確認が必要な項目とその理由を紹介します。

ペイシェント ゼロの感染を (たった 1 件でも) 発生させる可能性はないか

ファイルの分析中にペイシェント ゼロの感染が発生する可能性のあるサンドボックスでは、組織の安全を担保することはできません。

場所に関係なくすべてのユーザーとそのデバイスに対応できるか

ユーザーは、外出先、自分のデバイス、保護されていないネットワークから組織のリソースにアクセスすることがあります。業務に必要なすべてのデバイスを保護することが重要です。[4]

インラインでの検出が可能か、アウトオブバンドでのファイル送信が必要か

インラインで動作するソリューションは、NGFW のネットワーク フローやエンドポイント EDR ソフトウェアに依存せず脅威を特定し、直接ブロックできます。

HTTP、HTTPS、FTP、FTP over HTTP のすべてのプロトコルでトラフィックを検査でき、制約がないか

ステルス性のマルウェアを検知するには、トラフィックの検査が不可欠です。クラウド型のサンドボックスはレイテンシーなしですべてのトラフィックを検査します。

ゼロトラスト要件を含む関連法規に準拠しているか

規制によっては、サンドボックスの処理方法やファイルの保持およびプライバシーに関する厳しい要件が課せられる場合があります。こういった要件を満たすためには、メモリー内でのみ動作し、分析時に識別可能な情報だけを抽出するソリューションが有効です。また、そのソリューションが NIST 800-207 グローバル標準で規定されているゼロトラストの原則に準拠し、その原則を攻撃対象領域を減らしてデータを保護するための指針として使用しているかどうかも重要です。

他のセキュリティ モジュールと連携しているか

1 つの製品で高度な標的型攻撃 (APT) から完全に保護できるわけではなく、脅威の防止、軽減、検出、対応といった多層型アプローチが必要になります。サンドボックスは重要な層の 1 つであるため、他のソリューションやモジュールと問題なく連携できる必要があります。

---

4. us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox と高度な脅威対策

真のクラウドネイティブなインライン型サンドボックスとは

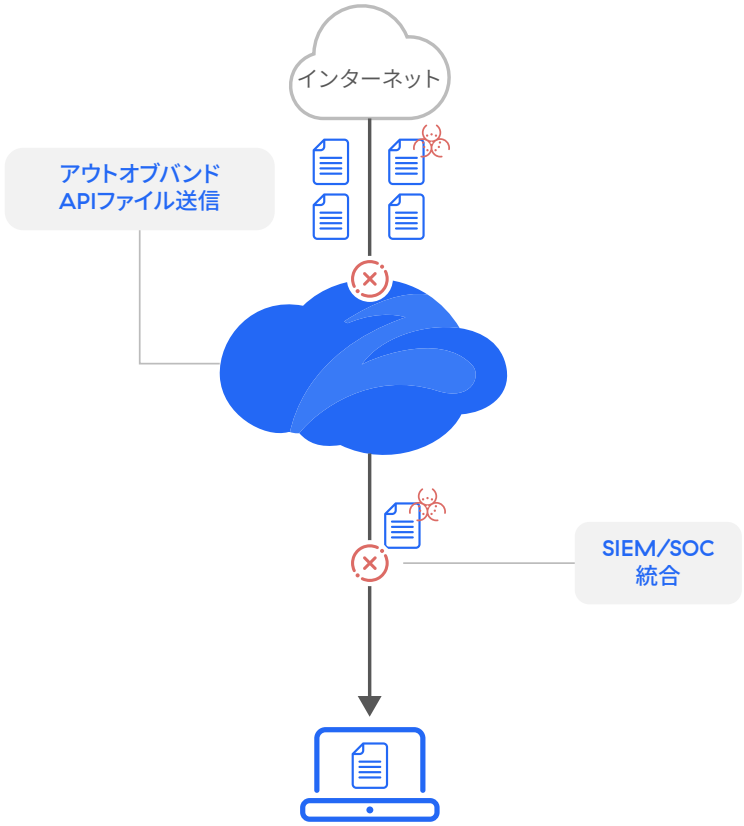
組織が拡大する攻撃対象領域に立ち向かう一方で、攻撃側が従来のセキュリティスタックに生じた「溝」を悪用している現状は、真のクラウドネイティブなインライン型サンドボックスを導入する絶好のタイミングと言えます。Zscaler Cloud Sandbox は、最新の脅威を捕捉して阻止することを目的として構築されており、すべての場所、すべてのユーザーにゼロデイ マルウェア対策を提供します。

クラウドネイティブでプロキシベースのアーキテクチャー上に構築された Zscaler Cloud Sandbox は、未知の脅威や不審なファイルをインラインで自動的に検出、防止して、効果的に検疫する、世界初の AI 活用型マルウェア対策エンジンです。SSL/TLS を含む Web およびファイル転送プロトコル (FTP) に対する無制限でレイテンシーのない検査により、クラウド サンドボックスは詳細かつ動的な分析をリアルタイムで実行します。そして、未知のファイルが悪意のあるファイルのダウンロードとしてユーザーの元に届かないようにします。

Zscaler Sandbox AI のメリット：5 億件を超えるサンプルでトレーニングされ、1 日あたり 300 兆のシグナルをソースとするリアルタイムのセキュリティ アップデートが提供されます。

AIを活用した検疫で未知のマルウェアを阻止

無害なファイルの即時配信、ペイシェント ゼロからの保護、きめ細かなポリシー制御によるインライン保護



複雑性とコストの削減

- 導入が簡単で、ハードウェアやソフトウェアの管理が不要
- 必要のないポイント製品を除去
- MPLS または VPN を介したインターネット トラフィックのバックホールを排除

すべてのユーザーと場所に対する迅速な保護の適用

- 単一かつ一元化されたコンソールでグローバル ポリシーを定義
- ポリシー変更があった際は速やかに施行
- 脅威が特定された時点で、組織内のすべてのユーザーを対象に脅威をブロック

隠れた脅威の検知

- AI 活用型の検疫で既知および新たな脅威からのペイシェント ゼロの感染を阻止
- 分析のためにファイルをアップロード (ファイル チェック ポータル)

統合プラットフォームサービス

- ウイルス対策、ハッシュ ブロックリスト、YARA マルウェア分類ルール、自動 JA3 フィンガープリント検出、ML/AI モデルを使用して、既知の悪質な脅威をすべて事前にフィルタリング
- コレクティブ インテリジェンス フレームワーク (CIF) のフィードにより、Zscaler の顧客全体の数十億件に上るトランザクションを活用した独自の脅威フィードに加え、60 以上の脅威フィードと統合可能
- クラウド サンドボックスを EDR ソリューションで階層化することで、セキュリティ効果を高め、初期アクセス、実行、標的型攻撃を低減

ESG 経済検証の研究で、Zscaler Zero Trust Exchange はセキュリティ アプライアンスを 90% 削減することがわかっています。[5]

- 静的、動的、二次的分析 (コード分析や二次的ペイロード分析を含む)
- 無制限でレイテンシーのない SSL インスペクション
- インバウンドおよびアウトバウンド トラフィックの保護
- ユーザー、発生元、回避戦術などを含む、API でのファイル送信による豊富なフォレンジックでセキュリティの調査と対応を強化

Zscaler Cloud Sandbox™ は、Zscaler Internet Access™ に完全に統合された機能であり、Zscaler Zero Trust Exchange™ の一部でもあります。

詳細はこちら
zscaler.com/jp/technology/cloud-sandbox

5. info.zscaler.com/resources-industry-report-esg-economic-validation-jp

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™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、**www.zscaler.com/jp**をご覧ください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/jp