データ シート

Zscaler Cloud Sandbox

業界初の AI 活用型インライン サンドボックスで未知の攻撃をわずか数秒で阻止

Zscaler Cloud Sandbox は無制限の検査を遅延なく実施することで、ゼロデイ脅威がユーザーやエンドポイントへ到達する前にブロックします。

従来のセキュリティ ソリューションには、進化し続ける現在の脅威環境に対応できないという課題があります。ファイアウォールやエンドポイント ソリューションなどの従来の防御では、悪意のあるファイルが侵入するのを防ぎきれないだけでなく、暗号化されたトラフィックに潜む脅威の検知や効率的な拡張が困難な場合があります。現在、インターネット トラフィックの 87.2% が暗号化されている状況下で[1]、安全なチャネルを通じて配信される脅威の数は増加の一途を辿っています。また、これらの攻撃の 86.5% はランサムウェアなどのマルウェアに関連しており、組織はこれらの脅威に対して一層の脆弱性を抱えるようになっています。

より速く高度な攻撃を仕掛けるために、多くの攻撃者が人工知能 (AI) を悪用しています。AI は十分な知識を持たない攻撃者でも簡単に複雑なサイバー攻撃を実行できるようにします。AI を悪用した攻撃や暗号化された脅威が日常になっている環境で組織を保護するには、脅威がすり抜ける前に効率的に検出し、無力化できる最新のソリューションが必要です。

ビジネス上のメリット

- **ゼロデイ脅威の瞬時の阻止：**マルウェアと高度な脅威をインラインで検出 (AI 活用型の即時判定を含む) し、ファイルベースの未知の脅威を阻止します。
- **セキュリティの強化と生産性の維持：**Zero Trust Browser Isolation とサンドボックス機能を統合することで、脅威を自動的に検出して隔離し、ユーザーの生産性を維持しながらセキュリティを最大化します。
- **SOC ワークフローの最適化：**アウトオブバンドでのファイル分析、サードパーティーの脅威検出ツール、パッチが適用されていない VM とパッチが適用された VM の両方を使用したマルウェア分析を SOC ワークフローにシームレスに統合することで、効果的な脅威の検出と調査を可能にします。
- **簡単な導入とグローバルな拡張:**コストを削減し、古いハードウェアやソフトウェアにかかる労力を軽減します。シンプルなポリシー構成により、すぐに価値が実現し、強力な ROI が促進されて戦略的な成長が可能になります。
- **世界中のサンドボックス ノードによるデータ レジデンシーとコンプライアンスの確保：**世界中に展開されているエッジを活用し、データ レジデンシーとコンプライアンスを確保します。Zscaler Internet Access™ と完全に統合され、Zero Trust Exchange™ の一部である Zscaler Cloud Sandbox は、完全に統合された保護と優れたユーザー エクスペリエンスを実現します。

[1] 2024 年版 ThreatLabz 暗号化された攻撃の現状レポート

Zscaler Cloud Sandbox

プロキシベースのクラウド ネイティブなアーキテクチャー上に構築された Zscaler Cloud Sandbox は、世界初の AI 活用型のインライン マルウェア対策エンジンであり、ファイルベースの未知の脅威がエンドポイントに到達する前にブロックします。リアルタイムの分析、AI を活用した即時判定、継続的な脅威インテリジェンスの共有により、生産性を損なうことなく、高度な攻撃に対処できるようにします。

組織のさまざまなニーズに対応するために、Zscaler Cloud Sandbox には次の 2 つのオプションがあります。

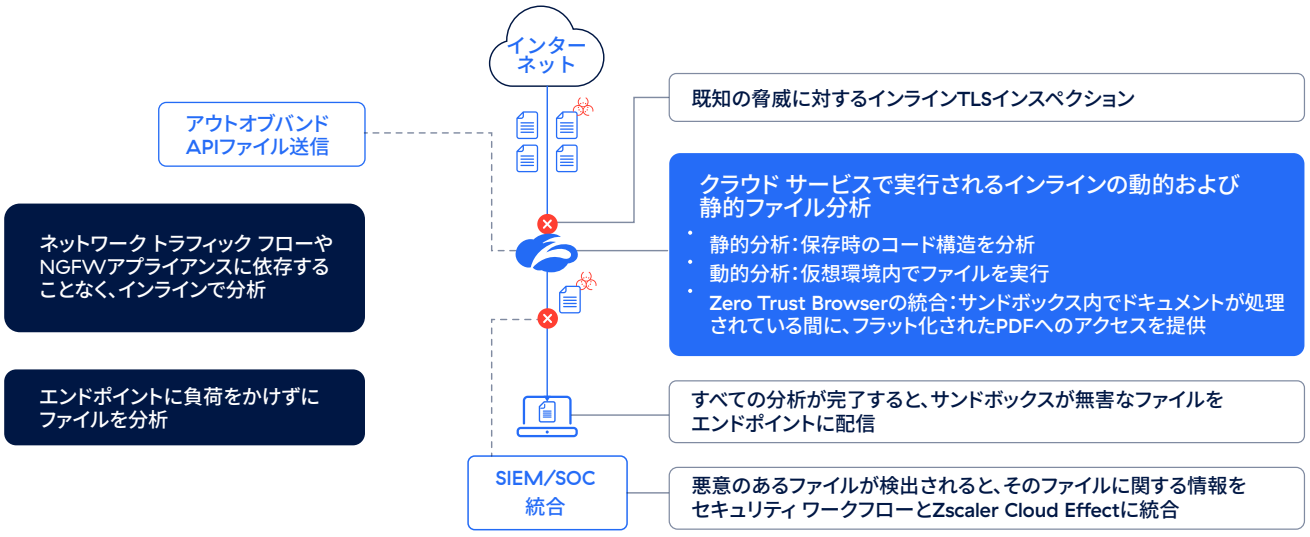
- **Cloud Sandbox:** Zscaler Internet Access (ZIA) に含まれ、ベースラインの保護に不可欠な脅威対策を提供します。
- **Advanced Cloud Sandbox:** より堅牢な防御を必要とする組織向けに、AI による即時判定、きめ細かなポリシー制御、API を活用した分析、詳細な脅威調査などの拡張機能を提供します。

従来のサンドボックス ソリューションではネットワーク ファイアウォールやエンドポイントに負荷をかけるエージェントが必要になりますが、Zscaler Cloud Sandbox はクラウドから直接動作するため、エンドポイントの負荷が軽減し、ネットワーク トラフィック フローに依存する必要がなくなります。また、SOC ワークフローとシームレスに統合するため、より迅速で効果的な脅威の検知と対応が可能になります。

Zscaler Cloud Sandbox は主に次の 2 つのモードで動作し、柔軟で包括的なセキュリティを確保します。

- **インライン検査：**トラフィックがクラウドを通過するとファイルが分析され、AI がリアルタイムの判定を下して遅延なく脅威をブロックします。
- **アウトオブバンド検査：**必要に応じてファイルを API 経由で送信し、クイック スキャンまたは詳細な分析を実行します。

Zscaler は基本と高度なオプションを提供することで、あらゆる規模の組織がニーズに合わせて階層化されたセキュリティのメリットを受けられるようにします。



仕組み：アーキテクチャーと主なプロセス

不明なファイルや不審なファイルは、最初に事前フィルタリング分析エンジンを通じて送信されます。このエンジンは、ファイルの内容を 40 以上の脅威フィード、ウイルス対策シグネチャー、YARA ルール、AI/ML モデルと照合してチェックし、同様に既知の脅威をブロックしながら迅速な判定を下します。最初のトリアージ後、ファイルは制御および分離された環境でのファイル実行を含む、堅牢な静的分析、動的分析、二次的分析を経て、実施可能な判定を受けます。最後の後処理のステップで、Zscaler の脅威データベースと組織のポリシー施行を更新します。

AI ベースの判定により、無害なファイルは即座に配信され、悪意のあるファイルは世界中の Zscaler ユーザーに対してブロックされます。このクラウドならではの効果がもたらす保護の共有により、デバイスやロケーションに関係なく、すべてのユーザーがペイシェント ゼロからの感染や新たな脅威から保護されます。

主な機能

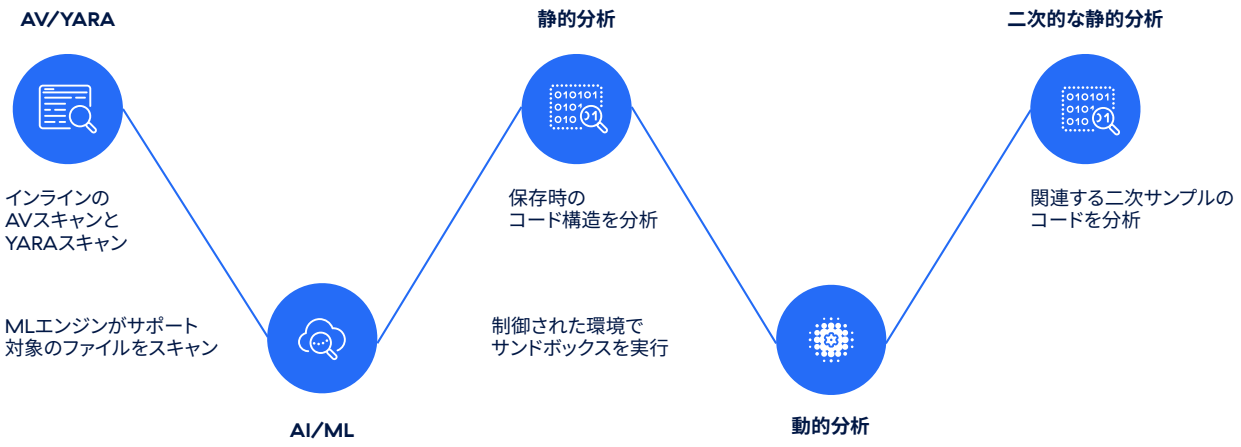
AI を活用したセキュリティ

6 億以上のサンプルでトレーニングされた AI/ML モデルを活用し、未知のファイルに対して信頼性の高い判定を瞬時に提供します。AI による即時判定エンジンは、ファイルが悪意のあるものか無害なものかをリアルタイムで予測します。悪意のあるファイルはすぐにブロックされ、安全なファイルはユーザーに迅速に配信されます。「疑わしい」と識別されたファイルについては、カスタマイズ可能な最小脅威スコアを使用してポリシーの動作を微調整すれば、セキュリティと生産性の適切なバランスを取ることができます。確認された脅威はすべて Advanced Cloud Sandbox でさらに検証され、詳細なレポートが生成されます。このレポートを活用することで、脅威を包括的に分析できるようになります。

また、サポート対象のファイル タイプを PDF ファイルにまで拡張することで、進化し続ける脅威に対する保護を拡大します。これを補完するのが、広範な Zscaler Internet Access の一部である AI 対応の PhishCatch です。PhishCatch はネットワーク レベルで動作することで、AI を悪用したフィッシング攻撃を検出してブロックし、包括的な多層型の防御を確保します。

多層型のマルウェア検出

Zscaler Cloud Sandbox は、1 日あたり 500 兆を超える脅威シグナルからリアルタイムで更新される情報と、Zscaler Cloud Effect を活用した多層的な脅威検出を提供します。Zscaler Cloud Effect では、脅威が特定されると、すべての顧客に対して既知の脅威が即座にブロックされます。このプロセスは静的分析から始まり、ファイルが保存された状態でそのコード構造が精査されます。その後、動的分析が行われ、



ファイルを仮想環境内で実行することで振る舞いを観察します。そして、二次的な静的分析を実施し、隠れたペイロードや二次的なペイロードを検出します。

この多層型のアプローチは、インライン保護と無制限の TLS/SSL インスペクションを組み合わせて Single Scan, Multi-Action エンジンを使用することで、最も高度な進化する脅威に対しても低遅延で高性能な脅威対策を実現します。

Zero Trust Browser の統合

Zero Trust Browser は、Advanced Cloud Sandbox とシームレスに統合されているため、セキュリティを損なうことなくユーザーの生産性を維持できます。この機能により、ユーザーはクラウドベースの分離された環境で元のファイルを安全に操作しながら、ファイルのサンドボックス分析を実行できます。リスクのあるファイルや不明なファイルは自動的に隔離されますが、分析中でもこれらのファイルに安全にアクセスできます。サンドボックス分析でファイルが安全であると判定された場合、遅延なく元のバージョンをダウンロードできます。

ファイルに悪意のあるフラグが付けられた場合、すべてのアクティブ コンテンツを削除したフラット化された PDF バージョンをダウンロードするか (CDR-1)、適切な場合は有害なコンテンツのみを削除した編集可能なバージョンをダウンロードするか (CDR-3、追加のライセンスが必要な場合あり) を選択できます。この柔軟な統合により、ユーザーの生産性を維持しながら、ゼロデイ脅威を徹底的に調査し、必要に応じてブロックできます。なお、Zero Trust Browser はオプションのモジュールであり、Advanced Cloud Sandbox と連携して全体的なユーザー エクスペリエンスを向上させる機能であることに注意してください。

API を活用した分析

Zscaler Cloud Sandbox の API 統合は、サンドボックスにファイルを直接送信して分析できるようにすることで、調査を効率化します。セキュリティ部門は、API を介してサンドボックスの結果に簡単にアクセスし、SIEM や SOAR プラットフォームに取り込んだり、EDR ソリューションと共有したりできるため、シームレスな SOC ワークフローが可能になります。サンドボックスはファイルの実行後に包括的なレポートを生成します。このレポートには、ポリモーフィズム、コールバック動作、攻撃ライフサイクルが詳細に示され、それらの概要は MITRE ATT&CK フレームワークにマッピングされます。これらのインサイトを運用化することで、脅威の検知と対応や事前予防的な脅威ハンティングを強化できます。

柔軟性を高めるには、**高度なサンドボックス送信 API** によって未知の脅威のオンデマンド送信とレポート作成をサポートする帯域外のファイルを徹底的に分析できます。また、**詳細なインスペクション スキャン API** によってファイル サンプルの判定を瞬時に入手できます。どちらの API も、調査時間を短縮し、セキュリティ スタック全体の連携を強化します。

きめ細かなポリシー制御とレポート作成

Zscaler Cloud Sandbox を使用すると、管理者は特定のユーザーのロールやロケーション、アプリケーションのカテゴリーに合わせたきめ細かなセキュリティ ポリシーをわずか数クリックで設定し、施行できます。直感的なインターフェイスにより、ポリシーの作成と展開を迅速かつ簡単に行い、時間とリソースの投資を最小限に抑えることができます。ルールの順序などを正確に実行するためのポリシーは簡単に管理でき、ユーザーやグループがどこに移動しても自動的に適用されます。

より詳細に制御するには、カスタム ハッシュ ブロックリスト、YARA ルール、自動化された JA3 フィンガープリンティングを構成し、脅威検出を強化できます。MITRE ATT&CK マッピングなど、コンテキストに応じて事前構成されたレポートを作成することで、コンプライアンスと監査の要件を満たします。クラウド型のソリューションでは、ハードウェアやソフトウェアの管理が不要なため、業務の複雑さを軽減しながら、強力で柔軟なセキュリティを実現できます。

AI による即時判定を備えた Zscaler Advanced Cloud Sandbox を活用し、わずか 20 分で世界中の組織のファイルのセキュリティを強化して生産性を確保：

- **91%** のファイルが安全なものとして瞬時に配信され、ワークフローの中断は発生しませんでした。
- **9%** のファイルがその性質の判定に高度な動的分析を必要としました。
- **5%** のファイルが悪意のあるファイルとしてフラグが立てられ、ブロックされました。結果として、潜在的な侵害が防止され、組織全体が保護されました。

ユース ケース

ランサムウェアなどのマルウェアに対する防御力の向上

ファイルベースの動的分析やハッシュ ブロックリスト、ヒューリスティック スキャンなどの多層型の脅威検出を活用することで、ファイルベースのランサムウェアやスパイウェアなどの高度なマルウェアを阻止します。

Zscaler Cloud Sandbox では、悪意のあるファイルが拡散する前に検知、ブロックされるため、より強力で事前予防的なセキュリティ態勢を維持できます。

セキュリティ オペレーション センター (SOC) の強化

SOC には、実用的な脅威インテリジェンス、マルウェアのインサイト、MITRE ATT&CK フレームワークにマッピングされた詳細な分析レポートが提供されるため、脅威検出と調査の迅速化や応答時間の短縮が可能になります。これはすべて、世界最大のセキュリティ クラウドが提供する優れたスケーラビリティーとインテリジェンスによって実現します。

マルウェアを検査するためのアウトオブバンドの API 分析の有効化

ファイル内に潜んだ脅威をアウトオブバンド API 送信を通じて検出し、業務を妨げることなくマルウェア検査を迅速に実施します。サードパーティー ソースやクラウド リポジトリーのファイルだけでなく、合併や買収などのビジネスの重要なイベントが発生している間のファイルもシームレスに検査することで、脅威に対する包括的な保護範囲を確保し、中核となるシステムへのリスクを最小限に抑えます。

Standard Cloud Sandbox と Advanced Cloud Sandbox の比較

特長	メリット	Standard Cloud Sandbox	Advanced Cloud Sandbox
サポート対象のファイル タイプ	幅広いファイル タイプをサポートし、進化する脅威に対する保護を強化	Windows の実行可能ファイル Windows のライブラリー Zip アーカイブ	Adobe Flash Android パッケージ キット アーカイブ HTML アプリケーション 光ディスク イメージ Java Applet Microsoft インストーラー Microsoft Office Portable Document Format Python 2 と 3 のファイル Visual Basic スクリプト Windows のバッチ ファイル Windows の実行可能ファイル Windows のライブラリー Windows PowerShell 画像付きの Zip アーカイブ スクリプト付きの Zip アーカイブ
AI による即時判定 (AI/ML の隔離とブロック)	無害なファイルを許可するか、悪意のあるファイルを数秒で確実にブロック	利用不可	一部のファイル タイプで利用可能
きめ細かなポリシー	ユーザー、ロケーション、URL のカテゴリーなど複数の基準に合わせてセキュリティ ポリシーを調整	利用不可	多くのユース ケースに適したきめ細かなポリシーを簡単に作成
レポート作成	MITRE ATT&CK マトリクスのマッピング、TTP、マルウェアの動作と意図、IOC、PCAP などの詳細なレポートにより、実用的なインサイトを提供	利用不可	複数のレポートとダッシュボードが利用可能で、豊富なインサイトを提供
API	アウトオブバンド API により、オンデマンドのサンドボックス ファイル分析を実行	利用不可	高度なサンドボックス送信 API (動的分析を含む) は、デフォルトで 1 か月あたり 3000 ファイルが対象 詳細なインスペクション スキャン API* (動的分析を含まない) は、1 日あたり 5 ファイルが対象 *API の使用要件に基づいて、追加のライセンスが必要になる場合あり
Zero Trust Browser の統合	リスクの高いファイルを自動的に隔離し、サンドボックス分析中にファイルへの安全なアクセスを許可	利用不可	PDF と Microsoft Office ファイルで利用可能

機能	詳細
事前フィルタリング分析エンジン	AV、ファイルのハッシュ ブロックリスト、YARA ルール、自動化された JA3 フィンガープリンティング検知、ML/AI モデル
静的分析、動的分析、二次的な静的分析	すべてのファイルで、静的分析、動的分析、動的分析中にドロップされたすべてのファイルの二次的な静的分析という 3 段階のサンドボックス分析を実行
サポート対象のファイル	7z、.apk、.applet、.bat、.bz、.bz2、.class、.cmd、.dll、.dll64、.doc、.docm、.docx、.dotm、.dotx、.exe、.exe64、.gtar、.hta、.iso、.jar、.msi、.ocx、.p、.pdf、.pickle、.pkl、.potm、.potx、.ppam、.ppsm、.ppsx、.ppt、.pptm、.pptx、.ps1、.py、.pyd、.pyw、.rar、.rtf、.scr、.slk、.swf、.sys、.tar、.tgz、.vbs、.wsc、.wsf、.wsh、.xla、.xlam、.xls、.xlsb、.xlsm、.xlsx、.xltm、.zip、画像付き .zip (.jpeg & .png) とスクリプト付き .zip (.cmd、.hta .js、.lnk、.ps1、.svg, .vbs)
SSL インスペクション	容量無制限
ファイルの保存期間	Zscaler Cloud Sandbox はメモリー内でのみ動作します。分析中にファイルから識別可能な情報が取り除かれ、分析が完了すると、無害なファイルはメモリーから消去されます。一方、悪意のあるファイルは暗号化されて無期限に保存され、継続的に保護するために Zscaler のすべてのユーザー間で情報が共有されます (Cloud Effect)。
サポート対象のプロトコル	HTTP、HTTPS、FTP、FTP over HTTP
1 日あたりの対応ファイル数	容量無制限 (インライン)
再構成不要でサポートされる最大ファイル サイズ	APK: 50 MB Adobe Flash: 2 MB アーカイブ、画像付き .zip と . スクリプト付き zip: 50 MB HTML アプリケーション：5 MB Java Applet: 5 MB Microsoft Office: 20 MB Portable Document Format: 20 MB スクリプト：5 MB Windows dll、exe、ライブラリー、MSI: 50 MB Windows スクリプト：5 MB
展開方法	クラウド ネイティブのため、オンプレミスのハードウェアや NGFW フックは不要
脅威インテリジェンス統合	40 社以上のセキュリティ パートナーの脅威インテリジェンス フィード
管理とレポート作成	マルウェアの振る舞いと意図、侵害の痕跡 (IOC)、ドロップされたファイル、PCAP を含む完全なレポート

フォレンジック	初期サンプル、二次的なペイロード、PCAP
API サポート	堅牢な API サポート、2 つのサンプル送信 API、要約形式または詳細形式の JSON の API によるレポート取得
きめ細かなポリシー	ユーザー、ロケーション、ロケーション グループ、ファイル タイプ、ユーザー グループ、部門、URL カテゴリー、プロトコルに関するポリシーを簡単に使用および構成
プライバシーおよびコンプライアンスの認定	グローバル企業および政府機関の厳格なリスク、プライバシー、コンプライアンス要件に準拠
業界および国のデータ プライバシー規制	業界固有および各国のデータ プライバシー規制に準拠(プライバシーに関するデータ シートはこちら)
サード パーティーによる独立した検証	CyberRatings による AAA 評価

zscaler™ | Experience your world, secured.™

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、**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