データシート

Zscaler Sandbox

世界初の AI 活用型マルウェア検知、防止、隔離エンジン

Zscaler Sandbox はゼロ号患者からの感染を防ぎ、高度な標的型攻撃によるネットワークへのアクセスをブロックします。

モバイルファースト、クラウドファーストが主流となりつつある昨今、多くのユーザーが外出先からインターネットや SaaS アプリケーションを介してファイルに直接アクセスしています。複数のセキュリティ レイヤーに囲まれた企業オフィスからメール クライアントを立ち上げる時代は過ぎ去りました。ネットワーク中心のセキュリティ対策では使いやすさへの強いニーズに対処できず、また、攻撃がより悪質になり、攻撃者が従来のセキュリティ スタックのギャップを利用する中で、組織の攻撃対象領域が拡大しています。

企業や個人の機密データを保護するため、現在はほぼすべてのインターネット トラフィックが暗号化されています。これによって一部の攻撃を阻止できるようになったものの、暗号化はセキュリティに対する誤った認識を生み出しています。パススルー アーキテクチャーを持つ従来のサンドボックスでは、十分に可視化できないばかりか、暗号化されたトラフィックに潜む悪意のあるファイルが、徹底した検査や隔離を受けずに意図せずすり抜けてしまう場合があります。この問題を解消する手段として後付けの SSL 復号デバイスを導入することもできますが、これはほとんどのハードウェアと同様に、拡張性や管理上の問題を生み出し、コストのかかるデバイスを無秩序に増加させます。その結果、未知のマルウェアによるゼロ号患者からの感染がネットワークに広がり続け、IT 部門やセキュリ

Zscaler Sandbox のメリット：

- **AI 活用型のマルウェア対策エンジン**
  高度な AI/ML を使用して、未知の脅威や不審な脅威をインラインで効果的に特定、隔離、阻止します。無害なファイルは再スキャンしません。
- **隠れた攻撃を検知する完全なインライン検査**
  制限や遅延のない検査を実行することで、Web プロトコルやファイル転送プロトコル全体の暗号化されたトラフィックに潜む回避的な脅威やマルウェアを検出し、阻止します。
- **世界中で共有される一貫した保護**
  すべてのユーザーにリアルタイムで共有される統合型の脅威インテリジェンスで、未知の脅威に対する自動的な保護を実現します。
- **脅威インテリジェンスで強化された SOC ワークフロー**
  堅牢な API を使用して、マルウェアの振る舞いに関するインサイトや脅威情報、高度なレポート機能を共有することで、迅速な調査と対応を可能にします。
- **高価な物理アプライアンスやソフトウェアは一切不要**
  ハードウェアの購入やソフトウェアの管理は必要ありません。サンドボックス ポリシーを構成して実装するだけですぐに展開でき、価値を実感できます。
- **グローバル エッジに配置されたクラウド配信型の保護**
  Zscaler Zero Trust Exchange™ の一部である Zscaler Internet Access™ により、完全統合の優れたセキュリティとユーザー エクスペリエンスを実現します。

ティ部門は、最初の段階で防止すべきラテラル ムーブメントと情報漏洩を阻止するために奔走することになります。

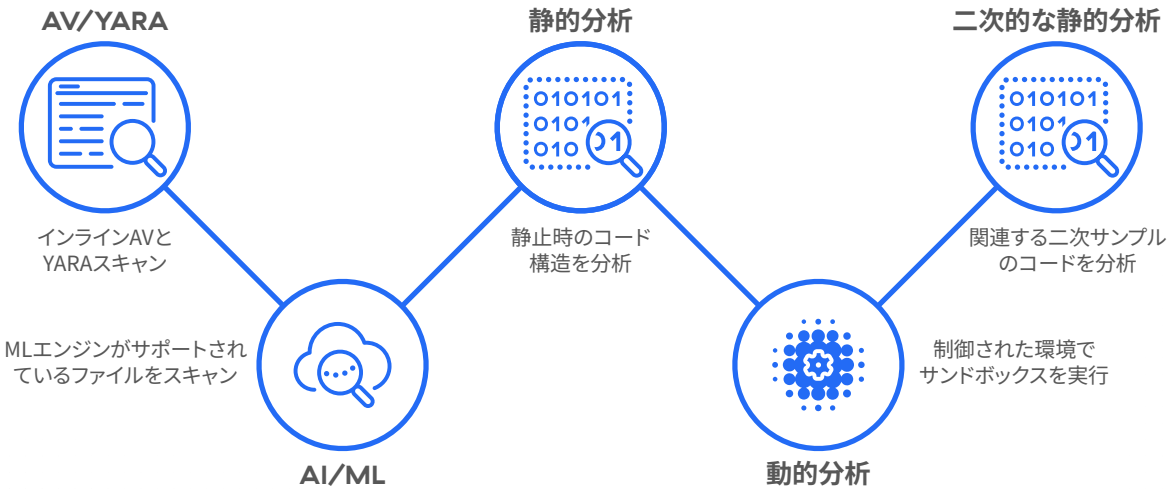
Zscaler Sandbox

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、その目的は悪意のあるファイルやコードの実行を防止する手段を提供することです。Zscaler Sandbox は、最初の侵入が発生してから保護を提供するアウトオブバンド方式のサンドボックスとは異なり、回避技術を用いて従来のサンドボックスの弱点を突く、検知が難しい最新の脅威を捕らえて阻止するために構築されています。

プロキシベースのアーキテクチャー上に構築されたクラウドネイティブな Zscaler 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、効果的に隔離する、世界初の AI 活用型マルウェア対策エンジンです。このクラウド型サンドボックスは、SSL/TLS を含む Web プロトコルおよびファイル転送プロトコル (FTP) に対して制限や遅延のない検査を実行し、リアルタイムで詳細かつ動的に分析を行うことで、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。

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顧客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。これは、クラウドならではの効果を利用した保護の共有の成果といえます。これにより、デバイスや場所に関係なく、すべてのユーザーに対するゼロ号患者からの感染と新たな脅威が阻止されます。



クラウド型サンドボックスのメリット

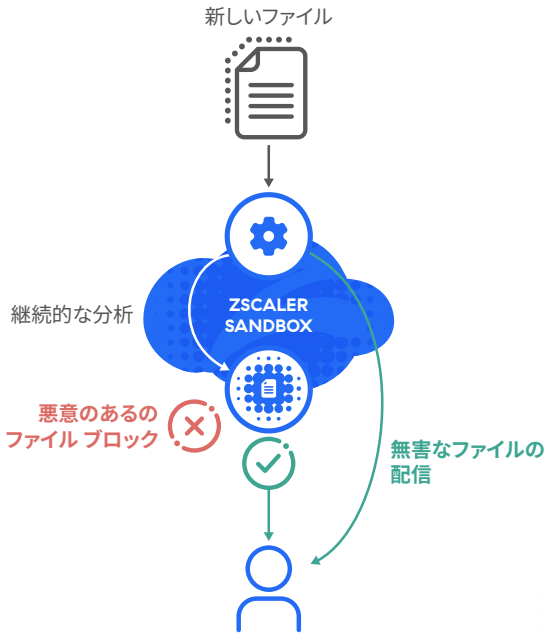
Zscaler Sandbox は不審なファイルをインラインで隔離し、AI ベースの分析をリアルタイムで実行して即座に判定を下します。また、最後の防御線となっていたサンドボックス処理が、Zscaler Sandbox の詳細かつ高度なレポート機能によって、インテリジェンスを活用したアクションの最初のステップになります。組織を狙う実際のマルウェアの振る舞いに関するインサイトを適用することで、SecOps ワークフローを改善し、セキュリティ スタック全体の防御を強化できます。

新たな脅威とゼロ号患者からの感染を効率的に阻止
攻撃者は暗号化と信頼されたクラウド アプリを悪用してステルス攻撃を仕掛けています。実際、最新の ThreatLabZ レポートでは、Google Drive、AWS、OneDrive からマルウェアが配信されていることが確認されています。Web や FTP 上のファイル、特に暗号化されたトラフィックをスキャンする機能は、可視性を確保すると同時に、攻撃者がネットワークへのアクセスを入手できないようにします。

マクロが隠された悪意のある新しい Office ドキュメント (Maldocs) を従業員が誤ってダウンロードして開く前に、Zscaler Sandbox の AI 活用型インライン隔離機能が作動します。詳細なファイル分析で脅威の可能性が高いと評価された場合、そのファイルは従業員に対してブロックされ、他の Zscaler ユーザーもアクセスできなくなります。ファイルを再スキャンせずに即座に判定し、未知のファイルや悪意のあるファイルを自動で隔離、ブロックすることで、従業員の生産性低下を防ぐとともに、IT ヘルプ デスクのチケット数を抑制します。

あるお客様の IT およびセキュリティ部門は、Zscaler Sandbox をわずか 20 分で導入し、AI ベースの判定を受けた無害なファイルの 91% を安全かつ即座にユーザーに配信しました。残りの未知のファイルは詳細な動的分析のために転送され、その結果、ファイルの 5% にマルウェアまたは悪意のある意図が含まれていることが判明しました。ファイルは対象ユーザーだけでなく、あらゆる場所の Zscaler のユーザーとデバイスすべてに対してもブロックされるため、一貫した保護の共有が確実に実行されます。

AIを活用した隔離で
未知のマルウェアを阻止
無害なファイルの即時配信、ゼロ号患者からの保護、
きめ細かなポリシー制御によるインライン保護



マルウェアに関するインサイトと MITRE ATT&CK で SOC ワークフローを強化

サンドボックスはファイルを詳細に分析し、未知のマルウェアを安全に実行すると、分析レポートを自動で生成します。制御および分離されたサンドボックス環境は分析のスクリーンショットをキャプチャーし、ポリモーフィズムや難読化回避技術、コールバック動作などのアクションを分析者に通知します。このレポートは、攻撃のライフサイクル、イベントのキルチェーン、マルウェアの振る舞い、ペイロードの意図を詳細に説明し、これらを MITRE ATT&CK フレームワークにマッピングします。

コンテキストに応じたサンドボックスの調査結果を ATT&CK フレームワークで運用できるようにすることで、セキュリティ部門や IT 部門はセキュリティ スタック全体でのインサイトの共有が可能になります。これにより、クラウド型サンドボックスは、マルウェアに対する最後の防御線として機能するだけでなく、脅威ハンティングの活動をサポートしながら、検出の最初のステップとして調査と対応を加速させることができます。

きめ細かな制御によるシンプルなポリシー管理

クラウドから提供される Zscaler Sandbox では、ハードウェアを購入して構成したり、ソフトウェアを管理したりする必要がないため、複雑さとリソースを軽減できます。各デバイスをセットアップして接続するためだけに現場に向かうという作業は一切不要で、**条件**と**アクション**のシンプルな 2 ステップの構成で Zscaler Sandbox を起動して実行できます。さらに、ポリシーの管理、構成、展開も簡単です。管理者は数回クリックするだけで、正確に実行するためのルール順序やあらゆる場所のユーザーまたはユーザー グループに追従するポリシーなどを実装できます。

クラウド型サンドボックスでは、自動化された JA3 フィンガープリンティング検知でファイルの静的分析と動的分析を強化し、カスタム ハッシュ ブロックリストと YARA ルールを構成できるため、よりきめ細かな制御が可能になります。また、スコアベースのブロック ポリシーは、通常は脅威スコアのしきい値を超えない、疑わしいグレーウェア ファイルやアドウェア ファイルに対してアクションを実行できます。

クラウドネイティブなゼロトラスト プラットフォーム上に構築

Zscaler Sandbox は、Zscaler Internet Access に統合された機能でもあり、Zscaler Zero Trust Exchange の一部でもあります。独自のプロキシベースのアーキテクチャーがトラフィックを業界最大のクラウド セキュリティ スタックに送信し、あらゆる場所やネットワークのユーザーにインテリジェントで徹底した保護を提供することで、事後ではなくインラインでユーザーを守ります。1 日あたり 300 兆件生成される脅威シグナルを活用したリアルタイムのアップデートやクラウド型の保護、そしてゼロトラストの最小特権の原則を組み合わせて、共有されたグローバルな保護を実現します。

標準のサンドボックスと高度なサンドボックスの比較

	標準のサンドボックス	高度なサンドボックス	
ZIA のエディション	Professional エディション Business エディション	Transformation エディション ELA エディション	高度なサンドボックスはアドオンとして ZIA の Professional エディションと Business エディションで利用可能
サポートしているファイル	.exe、.dll、	.exe、.dll、.scr、.ocx、.sys、.class、.jar、.pdf、.swf、.doc (x)、.xls (x)、.ppt (x)、.apk、.zip、.rar、.7z、.bz、.bz2、.tar、.tgz、.gtar、.rtf、.ps1、.hta、.vbs、zip 化されたスクリプト ファイル	
AI 活用型の隔離	—	✓	
きめ細かなポリシー	—	✓	
レポート作成	—	✓	
API	—	✓	

クラウド型のコア機能

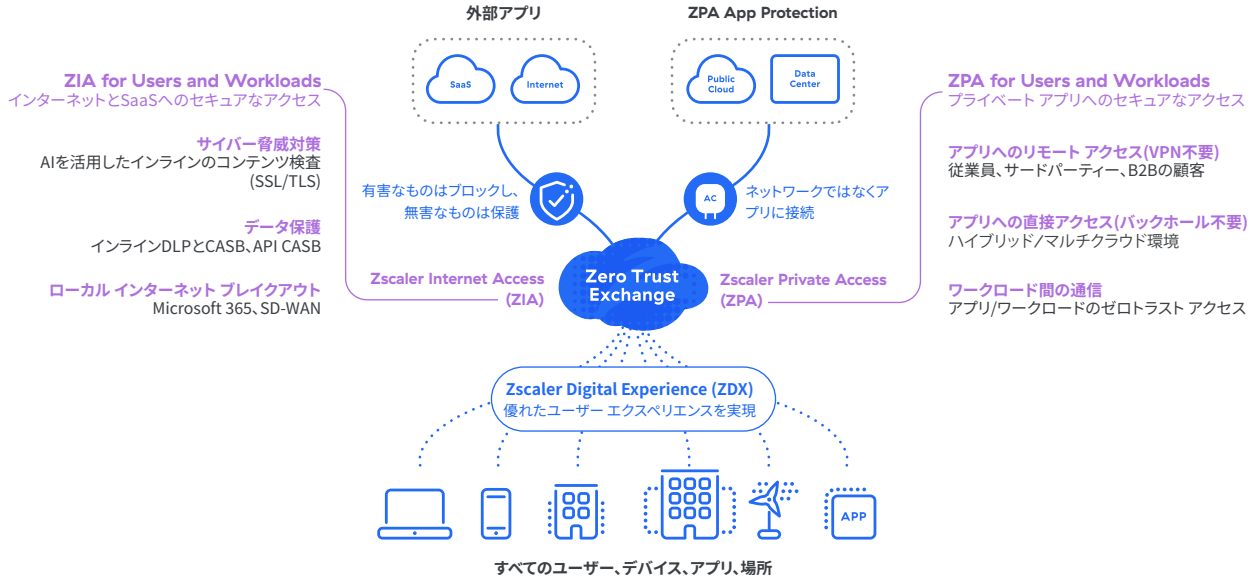
事前フィルタリング分析エンジン	AV、ハッシュ ブロックリスト、YARA ルール、自動化された JA3 フィンガープリンティング検知、ML/AI モデル
静的、動的、二次的分析	静的分析および動的分析 (コード分析や二次的ペイロード分析を含む)
サポートしているファイル	.exe、.dll、.scr、.ocx、.sys、.class、.jar、.pdf、.swf、.doc (x)、.xls (x)、.ppt (x)、.apk、.zip、.rar、.7z、.bz、.bz2、.tar、.tgz、.gtar、.rtf、.ps1、.hta、.vbs、zip 化されたスクリプト ファイル
SSL インスペクション	無制限の SSL/TLS インスペクション
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。
対応 OS	Windows XP、Windows 10、Android
対応プロトコル	HTTP、HTTPS、FTP、FTP over HTTP
1 日あたりの対応ファイル数	無制限
最大ファイル サイズ	Windows は 20 MB、Android は 50 MB
展開方法	クラウドネイティブ
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のフィード
管理とレポート作成	マルウェアの振る舞いと意図、侵害の指標 (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、二次ペイロード、PCAP
API サポート	堅牢な API サポート、JSON 形式の API を介したレポート取得
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、構成できます。
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しています。
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しています。

包括的な Zero Trust Exchange の一部であり、Zscaler Internet Access™ に完全に統合されている Zscaler Sandbox

Zscaler Zero Trust Exchange は高速で安全な接続を可能にし、インターネットを企業ネットワークとして利用することで、場所を問わない働き方を実現します。ゼロトラストの原則である最小特権に基づき、コンテキストベースのアイデンティティーとポリシーを施行して、包括的なセキュリティを提供します。

ユーザー、ワークロード、IIoT/OTにゼロトラストを提供するZscaler

わずか数週間で導入し、サイバー保護とユーザー エクスペリエンスを強化



Gartner

Zscaler は、Gartner® セキュリティ・サービス・エッジ (SSE) の Magic Quadrant™ でリーダーの 1 社と評価され、実行能力において最も高いポジションに位置付けられました。

詳細はこちら →

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.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.jp