File Upload Security

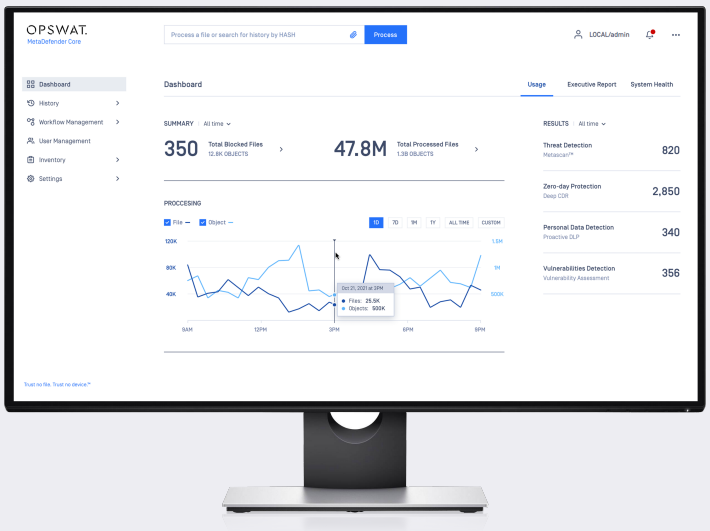
悪意のあるファイルアップロードを防御

ビジネスと技術上の課題

攻撃者が、悪意のあるファイルをアップロードすることで、サーバーまたはシステム全体が侵害され、組織から機密データの漏えいや、サイバー犯罪者から高額の身代金が要求される可能性があります。組織内外部の関係者からのファイル転送を制限することは現実的ではありません。転送されたファイルを受け入れるために保護対策を講じる必要があります。従来のシグネチャや振る舞いによる検出メカニズムが、高度な脅威やゼロデイ攻撃を防ぐには不十分な場合、多くの組織では、一連のセキュリティ製品のセットを自社で組み合わせてシステムの防御を試みます。しかし、これにはコストと時間がかかり、メンテナンスとアップグレードに多くのオーバーヘッドが発生します。

ファイルアップロードの脆弱性を防止する 6 つのベストプラクティス

- 埋め込まれている潜在的な脅威の削除
- ファイルタイプの検証
- 複数のマルウェア対策エンジンでファイルをスキャン
- 特定のファイル拡張子を制限
- ファイルの脆弱性を確認
- ユーザー認証



OPSWAT™ ソリューション

OPSWAT は、ネットワーク、アプリケーションから顧客の操作に渡って、安全なデータ転送を実現するために、脅威とゼロデイ攻撃の防止に取り組んでいます。約 20 年の重要インフラのセキュリティ保護の経験を有した OPSWAT のテクノロジーにより、ご利用の IT ソリューションやアプリケーションに、高度なマルウェア防御と検知を統合することができます。

MetaDefender - ファイルアップロード用の高度な脅威防止ソリューションは、重要インフラ、政府機関、金融機関など、最高レベルのセキュリティを必要とする組織で使用されています。

主な差別化要因

1. 高度な脅威検知と防止テクノロジー

業界をリードするサイバーセキュリティ テクノロジーのマルチスキャンと Deep CDR （コンテンツの非武装化と再構築）により、既知・未知の脅威の検知と阻止

2. シンプルで柔軟な展開

REST API または ICAP 対応製品と連携した オンプレミスまたは クラウドでの迅速・スケーラブルな実装

3. 高性能とスケーラビリティ

パフォーマンスに影響を与えることなく ファイルを高速にスキャンし再構築。ビルトインの高性能アーキテクチャと負荷分散機能により スケーラビリティを提供

4. カスタマイズ可能なポリシー

ユーザー、ファイル送信元、ファイルタイプに基づいた設定可能なワークフローと分析ルール

OPSWAT の支援

既知の脅威をほぼ 100% 検知

OPSWAT マルチスキャンテクノロジーは、30 種類以上のマルウェア対策エンジンを活用し、既知・未知の脅威の検知率を大幅に向上し、マルウェアのアウトブレイク検出時間の短縮を提供します。

ゼロデイ攻撃と高度なマルウェアの脅威を防止

Deep CDR（コンテンツの非武装化と再構築）テクノロジーは、ファイルを無害化し再構築することで、ファイルに潜む、検知できない可能性のある脅威から保護します。ファイルに埋め込まれている潜在的な脅威を無効化し、安全なコンテンツでユーザビリティを維持します。

脆弱性検出の最大化

多くの組織が、ファイルの脆弱性を悪用する攻撃にさらされています。アップロードされたファイルは、ライブラリ/アプリケーションの脆弱性を引き起こす可能性があります。OPSWAT のファイルベースの脆弱性評価テクノロジーは、ファイルが組織に入る前に、ネットワークゲートウェイで、インストーラー、バイナリファイル、IoT ファームウェアの脆弱性を検出します。

ファイル内の機密情報や重要情報を保護

アップロードされたファイル内の PII（個人を特定できる情報）等のコンテンツを OPSWAT Proactive DLP（情報損失防止）テクノロジーでチェックすることで、特定コンテンツがエンドユーザーに到達する前、または環境を出る前にブロックまたは秘匿化します。

コンプライアンス要件への対応

違反やプライバシー侵害を最小限に抑えるために、規制コンプライアンス要件が適用されます。コンプライアンスへの対応には時間がかかり、要件が満たされない場合はコストがかかる可能性があります。OPSWAT テクノロジーは、包括的な可視性と詳細なレポート機能を提供し、OWASP ガイドラインの要件対応を支援します。

利点

カスタムセキュリティポリシーとワークフロー

管理者は、ユーザー、ファイルソース、ファイルタイプに基づいた、さまざまなセキュリティポリシーを処理するために、複数のワークフローを作成することができます。

継続的な可視性と制御

リアルタイムの視覚的なセキュリティ ステータス ダッシュボードの一元化された UI は、資産を完全に可視化し、潜在的な脅威を即座に警告します。

包括的な保護

重要システムのリスクを軽減し、防御を回避した可能性のある脅威を防止します。

低総所有コスト (TCO)

TCO を削減する柔軟な製品です。単一プラットフォームの強力なサイバーセキュリティの制御により、ROI の向上、採用の増加、オーバーヘッドの減少、そして、複雑なシステムを監視するためにトレーニングされた専門家の必要性が少なくなります。

私たちが提供するもの

ファイルアップロードセキュリティア セスメントサービス

OPSWAT プロフェッショナル サービスチームは、組織のファイルアップロードサービスのセキュリティホールと、脆弱性を明らかにするために設計された一連のテストを実行します。実証済みの方法論に基づいて、組織の特定ニーズに合わせて評価を調整し、OPSWAT の専門技術者が、さまざまな推奨事項と次のステップについて説明します。

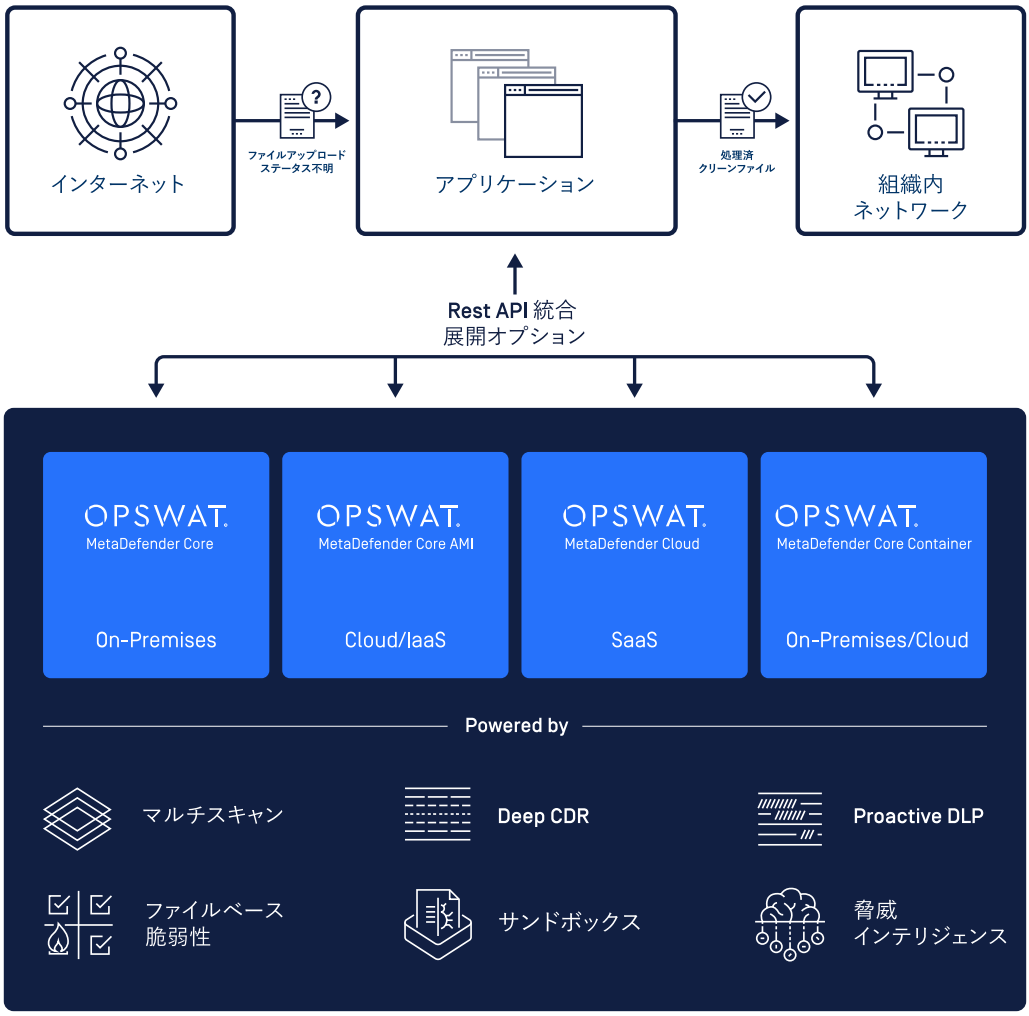
カスタムアプリケーション と 統合サービス

OPSWAT 製品とのインターフェースに必要なアプリケーション統合を、OPSWAT のエンジニアが構築します。当社のセキュリティ製品を強化するアプリケーションの構築や、既存のワークフローと当社のセキュリティ製品との統合も対象です。

最適な MetaDefender スイート

MetaDefender は、オンプレミス、クラウドインフラ内、または MetaDefender Cloud との統合で展開できます。データが存在する場所に応じて、ネイティブコネクタ、またはさまざまな展開シナリオをサポートする REST API による統合を提供します。

- オンプレミス - 厳しい制約のあるオンプレミスの展開では、多くの場合、MetaDefender Core が最適なソリューションです。
- SaaS - SaaS 製品と統合する MetaDefender が必要な場合は、容易なスケーラビリティ、24 時間の可用性、最小限のオーバーヘッドの MetaDefender Cloud を検討してください。
- クラウド/ IaaS - IaaS 環境に展開する場合でも、MetaDefender Cloud を検討してください。ただし、組織外にファイルを送信する場合は、MetaDefender Core をクラウド環境に展開できます。AWS の展開には、容易な実装でシームレスなスケーラビリティのために MetaDefender AMI を検討してください。

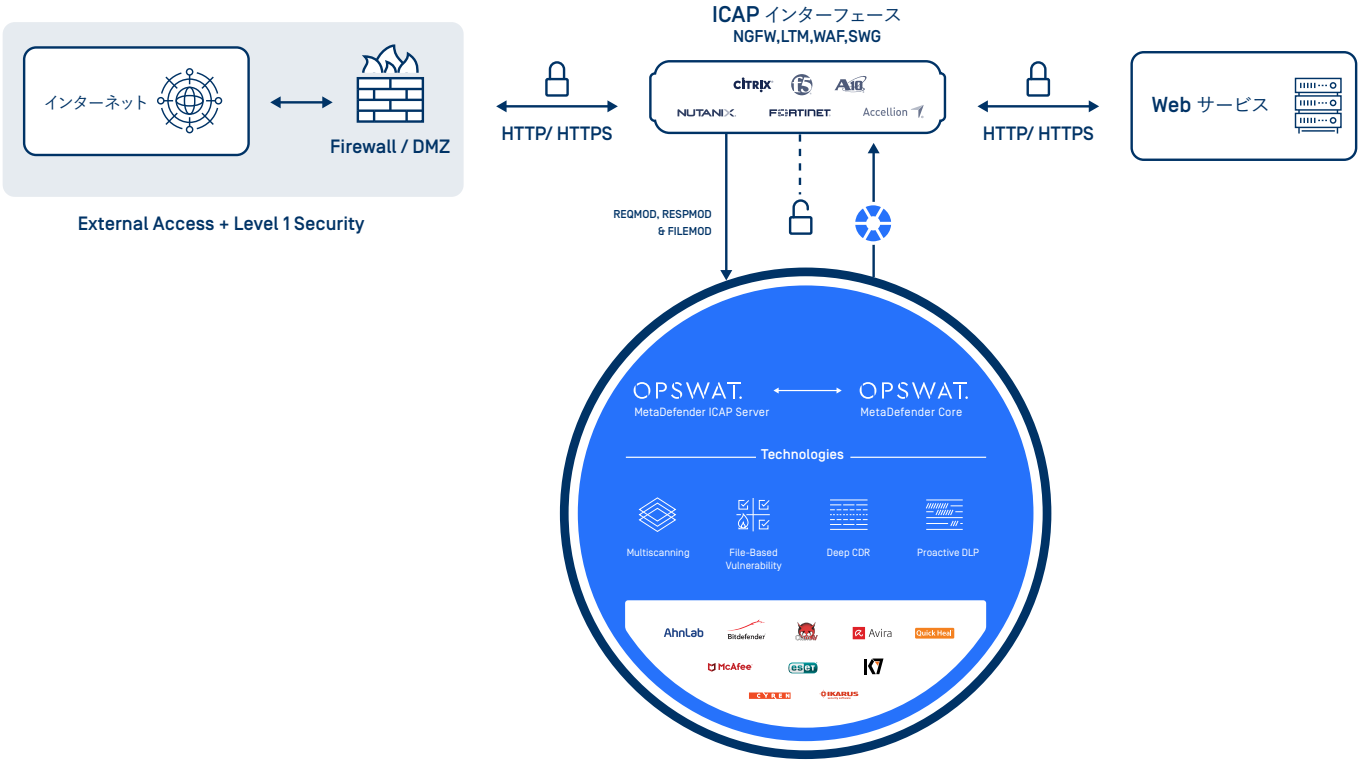


ICAP (Internet Content Adaptation Protocol)

最も利用されているネイティブコネクタソリューションの1つは、MetaDefender ICAP Server です。以下の製品を含む、ほとんどの Web アプリケーションファイアウォール（WAF）、ロードバランサー（LB）との統合を提供します。

- F5 Advanced WAF™
- F5 Big-IP® ASM™
- F5 Big-IP LTM™
- F5 SSL Orchestrator™
- A10 Networks Thunder® SSLi®

> “Upwork では、一般的なアンチマルウェアソフトで 70%しかブロックできなかったゼロデイのファイル攻撃を Deep CDR で 100% 防止することができました。
>
> アクティブなオブジェクトを含む全てのファイルは無害化されます。75% のファイルが 1 秒未満で処理され利用可能になり、 99% は 6 秒未満で処理されます。”
>
> Head of Security at Upwork



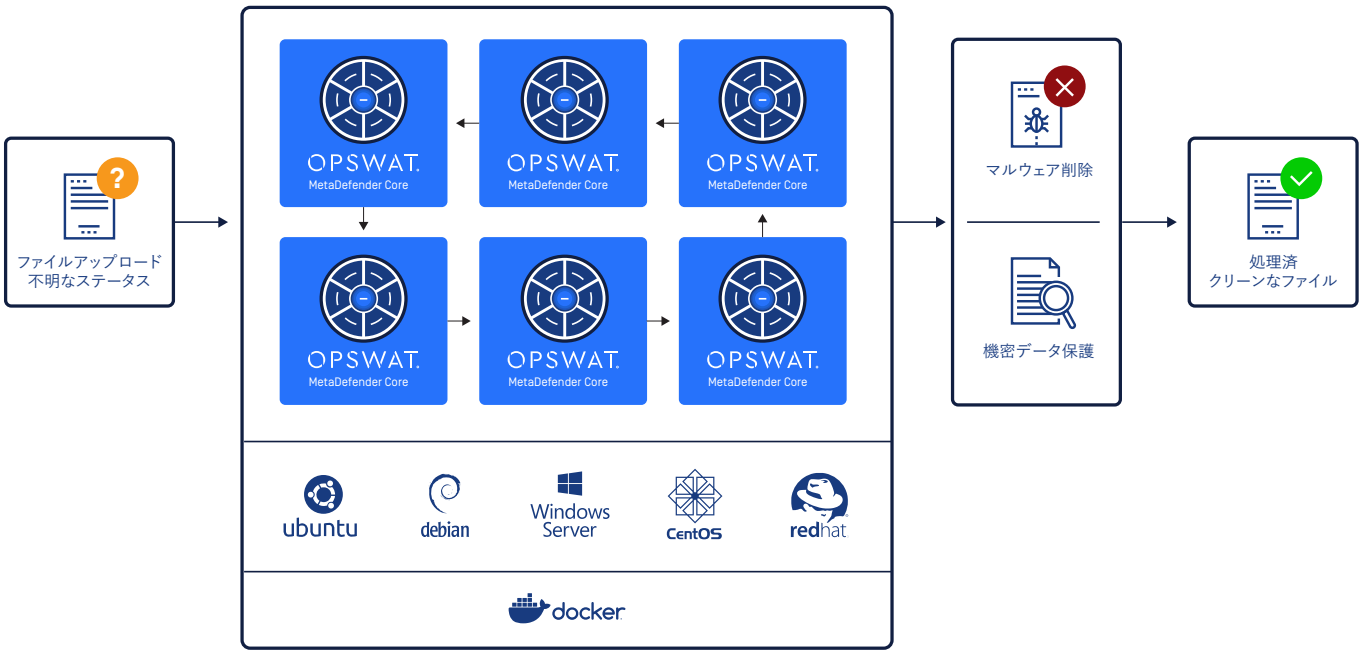
MetaDefender Core Container

私たちの新しいソリューションは、コンテナ化されたエコシステムに MetaDefender Core の展開を可能にします。MetaDefender Core Container により、さまざまな環境やオペレーティングシステムにわたって、アプリケーションの均一性を確保し、環境依存の除去、リソース消費の削減、マルウェア攻撃の防御に集中した、高度な多層サイバーセキュリティプラットフォームを拡張できます。

コンテナ化は、企業を単層のモノリシックアプリケーションから最新の多層マイクロサービスアーキテクチャに推進するステップです。

- 自動化展開と操作性により 統合と保守を簡素化
- 大幅な TCO 削減（総所有コスト）
- 競合するアプリケーションの依存関係等 外部要因 に よって引き起こされる複雑さと不明確さの除去
- 容易で柔軟な水平スケーリング
- 必要なサービスのみのスケーリングで負荷の急増に対応

コンテナ化環境における MetaDefender Core のしくみ



導入事例

ユーザー	Upwork - Web 、モバイル、ソフトウェアの開発や設計など、高度なスキルを持つ知識労働のために、企業とフリーランスの才能をつなぐフリーランスの Web サイト
セキュリティ課題	▪ Upwork は、クライアント企業やフリーランサーから 1 日に数百万のファイルを受信しています。自社システムとユーザーのシステムを保護するために、受信したファイルに脅威がないことを確かにする必要があります。 ▪ 週に 3 〜 4 回のマルウェア攻撃を受けていました。
ソリューション	Upwork は、既存のセキュリティアーキテクチャに Deep CDR を追加しました。MetaDefender Deep CDR は、ファイル（ Microsoft Office 、 PDF 、画像ファイルなど）を、要素に分解し、マクロ、スクリプト、埋め込みファイルなど、悪意が埋め込まれている可能性のあるすべての要素を削除し、安全な要素で再構築します。検知されない脅威が文書に含まれている場合でも、この処理で無害になります。
効果	√ Deep CDR は 残存する攻撃を効果的に無効化 √ Upwork では マルウェア攻撃が 70% 減少 √ 現在 Upwork では ゼロデイのファイル攻撃を 100% 防止 √ さらなる保守やオーバーヘッドはなく、ユーザーエクスペリエンスへの影響は皆無に等しい

有効なサイバーセキュリティを利用

高度化、巧妙化する脅威からインフラを保護する OPSWATの支援を、OPSWATの技術者がご説明します。お気軽にお問い合わせください。opswat.jp/contact

ファイルアップロードセキュリティの詳細は、opswat.jp/solutions/file-upload-security をご確認ください。

お問い合わせ

OPSWAT.
Trust no file. Trust no device.

世界の 1,500 を超える大手企業や政府機関から信頼されています

OPSWAT は、重要インフラを保護しています。私たちの目標は、マルウェアとゼロデイ攻撃を排除することです。私たちは、すべてのファイルとすべてのデバイスが、脅威をもたらすと考えています。脅威は、入口、出口、内部のすべての場所で対処する必要があります。「脅威の防御」と「安全なデータ転送とデバイスアクセスのプロセス構築」に、フォーカスした当社の製品により、侵害リスクを最小限に抑えた、生産的なシステムが実現します。これが、 98% の米国原子力施設に、サイバーセキュリティとコンプライアンスで、OPSWAT が信頼されている理由です。