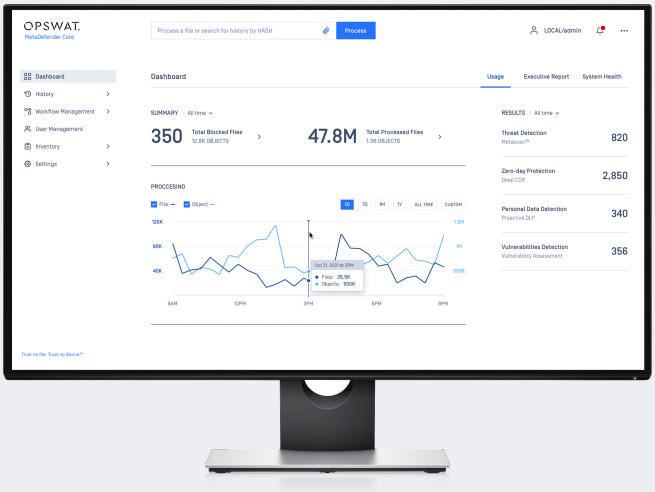
OPSWAT.

データシート

MetaDefender Core®

Advanced threat prevention platform



最重要なビジネス資産を適切に保護するためには検知ベースのサイバーセキュリティシステムだけに頼ることはできません。なぜならゼロデイマルウェアは「検知ベース」の防御を回避する機能を組み込んできているからです。企業は、高度な標的型攻撃に対処するために、より未然防止的アプローチを取る必要があります。

MetaDefender Core により既存の IT ソリューションとインフラに高度なマルウェア防止と検知機能を統合することで、悪意あるファイルアップロード攻撃から Web ポータルを保護しサイバーセキュリティ製品の強化や独自のマルウェア分析システムの開発など、攻撃ベクトルをより適切に処理できます。

> “当社はゼロデイのマルウェアファイルのアップロード対策として、各種サンドボックスやAVベンダー、クラウドのマルチスキャンベンダーを評価した結果、OPSWATのデータ無害化を選択しました。”
>
> Head of Security, Upwork

主な特徴と利点

Deep CDR（コンテンツの非武装化と再構築）

100種類を超えるファイル形式に対応し、ユーザビリティを維持したまま安全なコンテンツを再構築。何百ものファイル再構築オプションが利用可能

マルチスキャン

柔軟なパッケージオプションで30を超える主要なアンチマルウェアエンジンから選択可能。シグネチャ、ヒューリスティック、機械学習により、マルウェア脅威の99%以上をプロアクティブに検知

ファイルベースの脆弱性評価

IoT デバイスを含むエンドポイント端末でバイナリとインストーラーを実行する前に検査分析し、既知のアプリケーション脆弱性を検出

プロアクティブ DLP（情報損失防止）

30種類以上の一般的なファイルで個人を特定できる情報（PII）をチェックし、転送前に機密データのリダクション、ウォーターマークの組み込み

100以上のファイル変換オプション

ファイルのユーザビリティと内容を維持した真の「再構築」を実施。または、ファイルをより複雑ではない形式に変換

カスタムワークフロー

マルチスキャンと Deep CDR の独自のワークフローを作成し、ファイルが処理される順序とプロセスをカスタマイズ

アーカイブ抽出

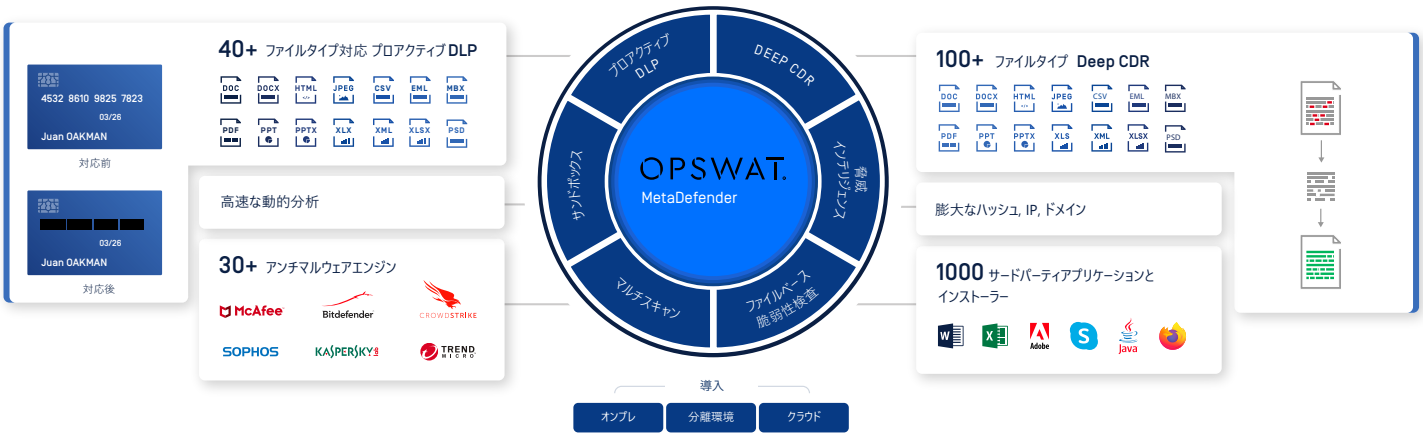
30種類以上の圧縮ファイルのマルチスキャンと Deep CDR（ファイル無害化）. アーカイブ処理オプションの設定構成が可能で、暗号化されたアーカイブもサポート

ファイルタイプ検証

4,500 を超えるファイルタイプを判断する際、信頼できない拡張子ではなく、ファイルのコンテンツに基づいて実際のファイルタイプを検証することで、スプーフィングされたファイル攻撃を防御

OPSWAT.

MetaDefender Core



MetaDefender Core を選ぶ理由

- 重要システムのリスク軽減と、防御を回避する可能性のある脅威を防止
- 組織に出入りする個人機密情報の保護
- 既存の Windows または Linux 環境や、ネットワーク分離環境への容易な導入。当社の SaaS であるMetaDefender Cloud の利用も可能
- REST API により既存環境へ統合。多くのプログラミング言語をサポート
- 集中管理により運用保守の TCO(総所有コスト)削減

OPSWAT について

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。すべてのファイルとデバイスが脅威をもたらすと考えています。脅威は、入り口、出口、静止中のすべての場所で常に対処する必要があります。当社の製品は、脅威の予防、安全なデータ転送のためのプロセス作成、そして安全なデバイスアクセスに重点を置いています。その結果、侵害のリスクを最小限に抑える生産的なシステムが実現します。米国の原子力施設の98%が、サイバーセキュリティとコンプライアンスでOPSWAT を信頼しています。

MetaDefender Coreの詳細
opswat.jp/products/metadefender/core

製品・技術に関するお問い合わせ
opswat.jp/contact

OPSWAT.
Trust no file. Trust no device.