OPSWAT.

巧妙なサイバー攻撃の侵入を最先端テクノロジーで防御

Who We Are

OPSWATは、ITインフラストラクチャを保護および管理するための
ソリューションを提供するサイバーセキュリティソフトウェア会社です。
サンフランシスコに本社を置くOPSWATは、既知および未知の脅威から
組織を保護するソリューションとテクノロジーを提供します。

目次

MetaDefender®

優れた脅威検知・防御プラットフォーム

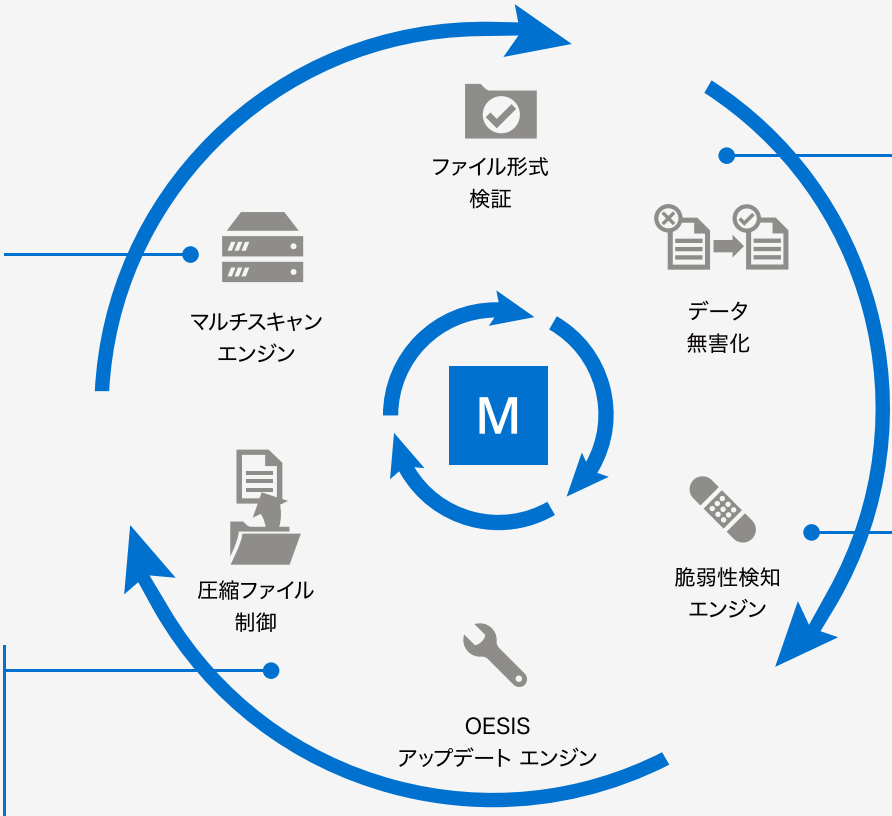
30以上 アンチマルウェア エンジン

AhnLab
ESET
SOPHOS
Symantec
Bitdefender
Quick Heal
CYREN
KASPERSKY
LAVASOFT
TREND MICRO
McAfee
IKARUS
total defense
Avira

30以上 対応する 圧縮ファイル形式

AR	EXT	LZH	RAR
ARJ	FAT,	LZMA	RPM
CAB	GPT	MBR	UDF
CHM	HFS	MSI	UEFI
CPIO	IHEX	NSIS	VDI
CRAMFS	ISO	NTFS,	VHD
DMG	LZH	QCOW2	And more...

MetaDefenderワークフローエンジン



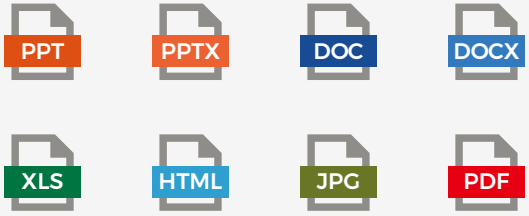
導入構成

オンプレミス | エア・ギャップ | クラウド

MetaDefender 提供製品

API
フレームワーク
Kiosk
エンドポイント コンプライアンス
エンドポイント フォレンジック

90+ データ無害化エンジン



20,000以上 アプリケーション脆弱性検知エンジン

脆弱性エンジンは、バージョンチェックと報告された脆弱性により、普及している何千もの製品に属する100万以上のバイナリーをサポートしています。

Eメール

ICAP

セキュア
ストレージ

MetaDefender は、効果的で効率的な脅威検知プラットフォームを構築するために、単一システム上でデータ無害化（CDR: Contents Disarm & Reconstruction）、複数のアンチマルウェアエンジンによるマルチスキャン、そして脆弱性検知エンジンを組み合わせています。

MetaDefenderは、オンラインとオフラインネットワークでファイルと任意のエンドポイントを分析し、潜在的な脅威と脆弱性に関する詳細情報を提供します。

また、MetadDefenderは、大量のネットワークトラフィック環境でも利用することができます。

MetaDefenderは既に1,200社以上のお客様が導入し、様々なネットワーク、エンドポイント、電子メールシステムの保護に使用されています。

F5 BIG-IP、FirePass、RSA NetWitness Endpointなどの主要なサイバーセキュリティソリューションと容易に統合できます。 ユニークで強力なテクノロジーを搭載するMetaDefenderは、優れた脅威検知と防御プラットフォームです。

MetaDefender 主要機能

データ無害化

データ無害化エンジンを使用しファイル型マルウェアから保護

脅威は、Excel、Word、またはPDFなどのように、一見すると無害な文書を介して持ち込まれることがよくあります。
ファイルには、さまざまな方法でセキュリティリスクが発生する可能性があります。例えば、マルウェアをダウンロードするマクロや安全でないサイトに接続されるハイパーリンクが含まれている可能性があります。
OPSWATのデータ無害化エンジン CDR（Contents Disarm and Reconstruction）では、MetaDefenderは、すべてのドキュメントにマルウェアが含まれている可能性があるとみなし、ファイルの潜在的に安全でない可能性のある部分をすべて除去し、ファイル形式を維持したまま再構築します。
このエンジンは、Microsoft OfficeやAdobe PDFファイルを含む、最も一般的に利用されているファイル形式や画像ファイルフォーマットがサポートされています。 また、さらにファイルはより安全なファイル形式に変換することもできます。

- **未知の脅威を未然に防ぐ**
  潜在的な脅威を排除するために、スクリプト、マクロ、およびその他の悪用可能なオブジェクトをドキュメントから削除
- **標的型攻撃の防御**
  ファイルを無害化することで、攻撃者が既知の脆弱性を悪用するのを防止
- **ゼロデイの脅威を排除**
  ファイルを再構築し、未知の脆弱性の悪用を阻止

脆弱性検知

100万以上の識別された脆弱性ファイルの高速な検査

脆弱性は重大なセキュリティリスクを引き起こします。攻撃者はパッチ適応前にアプリケーションの脆弱性を悪用しようとします。MetaDefenderは20,000を超えるアプリケーションとバージョンの組合せを含む数百万の特定された脆弱性データベースに対してアプリケーションをチェックします。MetaDefenderは脆弱性をバイナリと関連付ける独自の特許申請中のテクノロジを使用して、ほとんどのアプリケーションに対して迅速で正確な脆弱性評価を提供します。
脆弱性エンジンは、OESIS脆弱性評価モジュール（OESISフレームワークのセクション参照）を活用しています。

- **インストール前にスキャン**
  インストール前に特定種類のソフトウェアの既知の脆弱性をチェック
- **ブート前にスキャン**
  システムの電源を入れずに、既知の脆弱性をスキャン

起動中にスキャン

- 実行中のアプリケーションとそのロードされたライブラリの脆弱性を迅速にスキャン

既知の脆弱性があるアプリケーション例

マルチスキャン

複数のアンチマルウェアエンジンでより多くのマルウェアを検知

あらゆるアンチマルウェアエンジンには長所と短所があります。短所を補完するために複数のアンチマルウェアを利用するマルチスキャンがマルウェアをスキャンする最も効果的な方法です。MetaDefenderには、より高いマルウェア検知率を実現するためにオンプレミスには30以上のエンジン、クラウドには40以上のエンジンが搭載されています。

MetaDefenderのマルチスキャンは、既知・未知の脅威から保護するために、複数のアンチマルウェアエンジンのシグネチャとヒューリスティックスキャンを利用して、迅速かつ効果的にマルウェアを検知します。IT管理者は、個々のエンジンのヒューリスティックを有効または無効にすることで、ニーズに合わせたマルチスキャンを実行することができます。さまざまなマルチスキャンパッケージが利用可能です。

- **ハイ・パフォーマンス**
  脅威の検知と防御の強化、および大規模データベースのスキャン
- **ヒューリスティックとシグネチャー**
  各エンジンのシグネチャーとヒューリスティックを活用
- **超高速スキャン**
  MetaDefenderのマルチスキャンエンジンが瞬時にスキャンし、マルウェア感染を迅速に検知
- **優れた検知範囲**
  国際的な場所のアンチマルウェアエンジンによるスキャンで、新しい脅威を迅速に特定

WINDOWS パッケージ
追加のエンジンをカスタムパッケージとして追加することができます。

LINUXパッケージ

ファイル形式検証

セキュリティ対策を講じる前に、偽装されたファイル形式を検知

不正なファイル拡張子を持つ悪意あるファイル（「なりすまし」ファイル）は、特定のファイル形式のみを通過させるシステムを回避し、ユーザに誤って開かせるために、セキュリティ上の大きな脅威になります。MetaDefenderのファイル形式検証は、1,000種類以上のファイル形式を識別し修正します。さらに、MetaDefenderは識別したファイルの種類に応じて異なる方法で効率的にスキャンします。

- **偽装されたファイルの検出**
  他のファイル形式に偽装された実行ファイルを含むなりすましファイルをブロック
- **標的型攻撃の防御**
  ユーザーエラーにより危険なファイルが開かれるのを阻止
- **効率的なスキャン**
  アンチマルウェアがファイル形式検証を利用することでスキャン速度が高速化

圧縮ファイルの処理

圧縮ファイル内からファイルを抽出する前に、マルウェアとアーカイブ爆弾（繰り返し圧縮されたファイル）をチェック

圧縮ファイルの脅威は、ファイルサイズが大きく、アーカイブ爆弾（アンチマルウェアプログラムを無効にするよう設計された悪意ある圧縮ファイル）などの仕込まれた脅威を覆い隠す機能があるため、検出が困難です。

アーカイブの抽出スキャン、つまり圧縮ファイル内の各ファイルを個別にスキャンすることで、MetaDefenderはマルウェアを完全にチェックします。また、MetaDefenderは、より徹底的なマルウェア対策チェックのために、ファイルを抽出することなく圧縮ファイル全体をスキャンすることもできます。

- **優れた検知**
  潜在的な脅威を排除するために、スクリプト、マクロ、およびその他の悪用可能なオブジェクトをドキュメントから削除
- **短時間で高効率**
  圧縮ファイルのスキャンを重複しないことで、スキャン時間と処理時間を短縮
- **アーカイブ爆弾の防御**
  再帰制限の設定により、アーカイブ爆弾によるシステム停止を防御

OESIS自動アップデート エンジン

主要なSSL-VPN/NACソリューションとの互換性のための容易なコンプライアンス パッケージのアップデート

OESIS自動更新エンジンは、統合パートナーおよびエンドユーザー管理者によるきめ細かな更新管理を可能にし、OESISシグネチャーの更新版が利用可能になるとすぐに配布します。
OESIS フレームワークは、一定かつ自動的に更新されます。 （詳細は、本カタログのOESIS フレームワークをご確認ください。）

- **ネットワーク接続性の維持**
  エンドユーザは、OESISの署名が古くなることで、アクセスが拒否されることはありません
- **自動シグネチャー更新**
  製品の更新とは別にシグネチャーの更新を配信
- **バージョン コントロール**
  最新の５つのバージョンのOESISを保存し、以前のバージョンへ容易に戻すことができます

ワークフロー エンジン

利用状況に応じたカスタマイズ可能で柔軟なワークフロー

ほとんどの組織では、他の組織と異なるセキュリティポリシーでファイルとデータを処理します。MetaDefenderのワークフローエンジンにより、管理者は異なるファイルおよび異なるユーザーに対してセキュリティポリシーをカスタマイズすることができます。例えば、管理者は、最初に複数のマルウェア対策エンジンですべての外部ファイルをスキャンし、その後それらを無害化したり、最初に無害化し、その後複数のエンジンで脅威をスキャンしたりすることができます。
ワークフローエンジンにより、両方のシナリオが可能になり、IT管理者は比類のない柔軟性を得ることができます。

- **無制限のカスタムワークフロー**
  異なるセキュリティポリシーで複数のワークフローを定義
- **ネットワーク管理**
  様々なネットワークソースに対して異なるワークフローを定義
- **ユーザ主導のワークフロー**
  異なるレベルのユーザに固有のワークフローを定義

MetaDefender 利用例

MetaDender は、様々な方法で導入されています

KIOSK / セキュアなファイル転送

マルウェア対策のために外部メディアをチェック

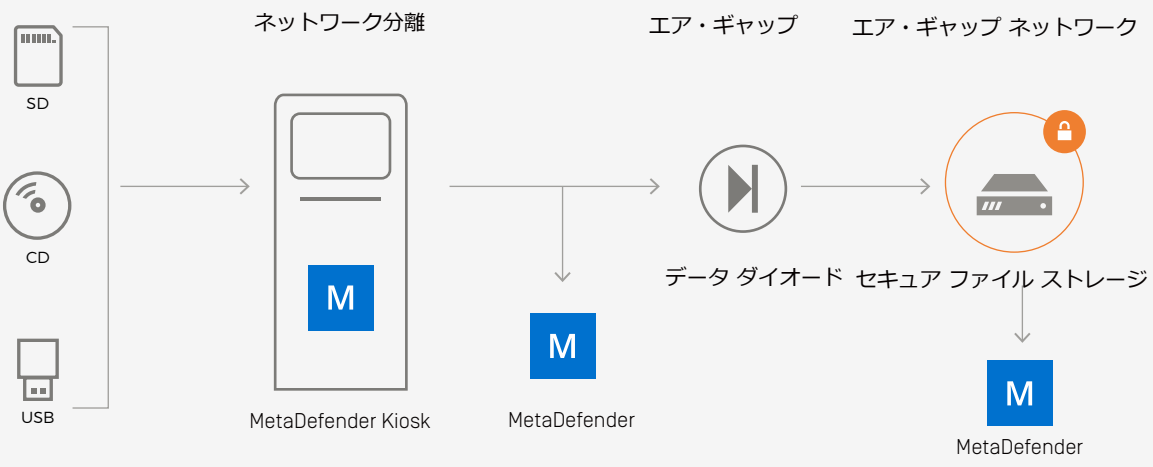
MetaDefender Kioskによるセキュアなファイル転送では、重要なネットワークとの間で、USBドライブ、CD、DVDなどの物理メディアによるデータの送受信に安全なプロセスを提供します。

Kioskは、ポータブルメディアをネットワークに接続する前にスキャンすることができます。あらかじめ決められたアクセス権限を持つユーザーがメディアを挿入すると、MetaDefender Kioskはネットワークから隔離した状態でマルウェアと脆弱性をスキャンします。脅威が発見されない場合、データはデータダイオードを通過し、安全なネットワークに入り、一時的にサーバに保存されます。 ユーザーはそのデータにアクセスし、安全なデータとして利用することができます。

Kioskは、完全な認証とログシステムを提供します。MetaDefender Kioskは、インターネットに接続されたネットワークに加えて、オフラインまたはネットワーク分離の環境にも導入できます。

OPSWATは、MetaDefender Kioskにオフラインのマルウェア対策シグネチャを更新するいくつかの方法を提供しています。ハードウェアオプションも用意されています。

セキュアなファイル転送ソリューション



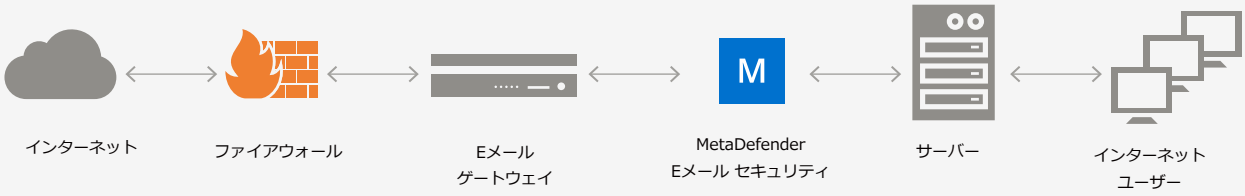
Eメール セキュリティ

マルウェアからメールの受信BOXを保護するためのセキュリティレイヤーを追加

MetaDefender Eメール セキュリティは、MetaDefenderのマルチスキャン、データ無害化（CDR）などのテクノロジの活用で、電子メールシステムに、より強固な保護層を提供します。Cisco IronPort, Proofpoint Email Security, FireEye EXシリーズなどのセキュアEメールゲートウェイ製品と連携して、MetaDefender Eメール セキュリティは高度な脅威検知を最大化します。MetaDefender Eメール セキュリティは、電子メールの本文や添付ファイルからスクリプトやハイパーリンクなどの悪用可能なコンテンツを取り除くことで、システムの脆弱性やユーザーエラーを悪用する潜在的な脅威の侵入を最小限に抑えます。

オンプレミス型 メール プロキシ連携

オンプレミスのセキュアEメールゲートウェイに新たな保護レイヤーを追加します。組織のメールサーバーに到達する前に、EメールトラフィックはMetaDefender Eメール セキュリティを通過します。



オンプレミス型 MICROSOFT EXCHANGE連携

MetaDefender Eメール セキュリティは、EXCHANGEサーバーのセキュリティを強化するための高度な保護機能を追加します。Eメールのメッセージは、EXCHANGEサーバーに到達する前に、MetaDefenderを通過しエンドユーザーに配布されます。

クラウドとホスト型 連携

MetaDefender Eメールセキュリティのクラウドまたはホスト型ソリューションにより、組織はパブリッククラウドに容易に製品を導入できます。MetaDefender Eメール セキュリティは、Amazon Web Services、企業データセンター、または他のホスティングサービスプロバイダを介してホスティングできます。

ICAP サーバ

悪意のあるファイルのアップロードまたはダウンロードからの保護

MetaDefender ICAPを介して、すべてのネットワークトラフィックをスキャンすることで、高度な脅威が内部ネットワークに侵入するのを防ぎます。 安全なネットワーク内で脅威が発見された後に脅威を調査する必要がある場合に備えて、MetaDefenderは、ファイルがいつネットワークに入ったかを記録します。

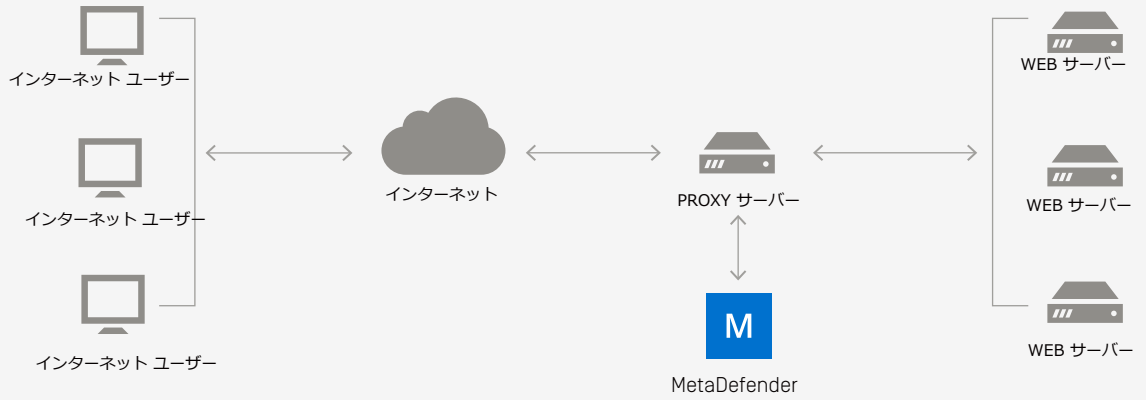
ICAPインターフェイスを通過するファイルは、MetaDefender インターフェイスを介してスキャンされるファイルと同様にアンチマルウェアエンジンと脆弱性検知エンジンでスキャンされ、データ無害化（CDR）で無害化されます。

すべてのファイルはログに記録され、必要に応じて後でアクティビティを確認することができます。 さらに、ファイルスキャン結果をキャッシュすることができます。

MetaDefender は、F5®BIG-IP®Local Trafic Manager™（LTM®）、Blue Coat ProxySGなどのWebプロキシサーバーとリバースプロキシサーバーと統合できます。

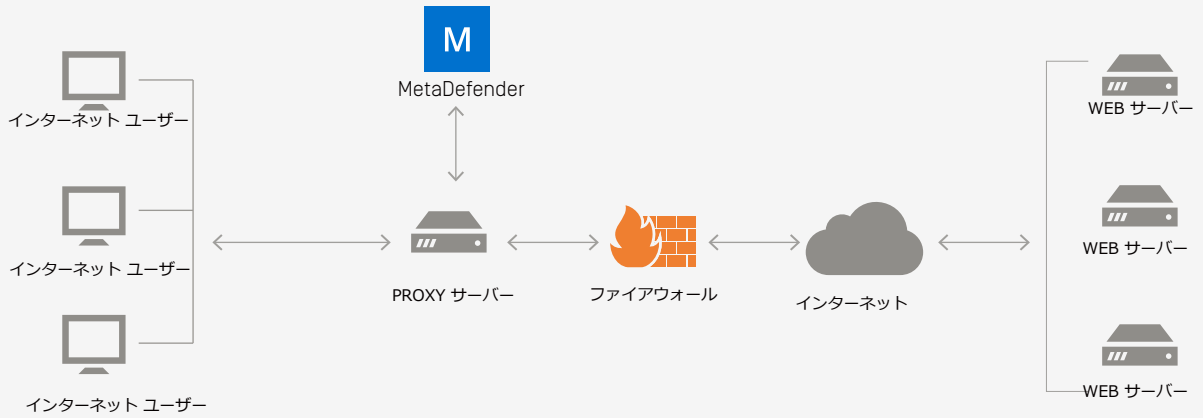
リバース プロキシ連携

MetaDefender ICAPサーバを使用すると、MetaDefender マルチスキャン テクノロジーと既存のリバースプロキシサーバを容易に統合して、すべてのファイル アップロードをスキャンすることができます。



Webプロキシ連携

MetaDefenderをWebプロキシサーバと統合することで、すべてのHTTPアップロードとダウンロードをスキャンできます。MetaDefender ICAPは、既存のWebプロキシサーバと容易に統合することができます。



API

脅威に対する最善の防御をカスタムソリューションに統合

MetaDefenderのREST API により、ソフトウェアベンダーやITプロフェッショナルは、MetaDefenderの脅威防止技術をアプリケーションに容易に統合することができます。 MetaDefender REST APIは、堅牢で使いやすく、サンプルコードで十分に文書化され、高速なパフォーマンスを提供します。

MetaDefenderはOEMまたはホワイトラベルには使用できません。

- **オンプレミス API**
  お手元のセキュリティシステムに、データ無害化（CDR）、バイナリ脆弱性評価、マルチスキャン機能を追加
- **エンドポイント API**
  開発者は、OPSWATのクラウド プラットフォームのエンド ポイント コンプライアンス情報を独自のセキュリティソリューションへ統合できます。

エンドポイント コンプライアンス

MetaAccess

業界最高峰のエンドポイントセキュリティと高度な脅威防止テクノロジを駆使し、端末が企業情報にアクセスする前に広範囲なセキュリティと規制遵守の確認、そして修復処理を実行します。規制遵守を確実にするために、ハードディスクの暗号化、インストールされていないソフトウェア更新、潜在的なマルウェア感染をチェックします。

MetaAccess 機能

- 複数デバイスを管理するためのシンプルなインターフェース
- マルウェア対策遵守の確認
- OPSWAT特許技術によるディスク暗号化状態の確認
- マルウェア感染状況の確認
- エンドポイントの脆弱性の検出
- ユーザー認証と画面ロックの確認

metadefender.com

クラウド ベースのセキュリティ スキャン

MetaDefenderによって提供されるアプリケーションおよび脅威インテリジェンスプラットフォームであるmetadefender.comは、次世代CDR（Content Disarm and Reconstruction）エンジン、脆弱性評価エンジン、マルチ スキャン テクノロジを使用して、提出されたすべてのファイルの脅威と潜在的なリスクを分析します。 metadefender.comは、ファイルの分析とスキャンに加えて、ハッシュの分析、脅威の確認、既知の脆弱性、およびアプリケーションのレピュテーション情報のチェックを実行できます。
OPSWATの、ブラウザと電子メールの無料のプラグインで、Webインターフェイスを介してMetaDefenderクラウドの機能を制限付きで無料で使用できます。
MetaDefenderクラウドへのAPIアクセスは、商用ライセンスで利用できます。ライセンスについての詳細はmetadefender.com/licensingをご覧ください。

1 データ無害化（CDR）

2 脆弱性検知

3 IP レピュテーション分析

4 業界最速のマルチスキャン

5 容易な API 統合

6 制限付き無償版の利用

パブリック API

MetaDefenderクラウドのAPIにより、開発者はMetaDefenderのクラウドベースのマルチスキャン、脆弱性検知、データ無害化（CDR）テクノロジを活用することができます。OPSWATは、MetaDefenderのWebインターフェイスを通じて、無料のファイルスキャンとハッシュ検索を提供します。商用に関しては、担当営業にご連絡ください。

ライセンス

無料版は、ファイルサイズ、リクエスト回数等に制限があります。クラウドベースのサイバーセキュリティソリューションであるMetaDefenderクラウドでは、商用クラウドの統合が可能です。ライセンスの詳細については、metadefender.com/licensingをご覧下さい。

統計

OPSWATはMetaDefenderクラウドのデータベースから最も検索された脅威をまとめています。ユーザーはMetaDefenderサイトでそれらを確認することができ、MetaDefenderマルチスキャンの検知効果が確認できるデータもあります。

OESIS フレームワーク

OPSWATのエンドポイント セキュリティ マネジメントSDK

OESIS フレームワークは、テクノロジーベンダーやソフトウェアエンジニア向けのエンドポイントマネジメントSDKであり、効果的なサイバーセキュリティソリューションを構築できます。 OESISは、F5, Citrix, Palo Alto Networks, Pulse Secure, Ciscoをはじめとする数多くのセキュリティ、コンプライアンスソリューションを強化しています。

01 検出と分類

このOESISモジュールは、エンドポイントにインストールされているアプリケーションを正確に識別します。
検出・分類モジュールは、15のカテゴリーから数千ものアプリケーションの検出をサポートしており、OPSWATは分類・未分類アプリケーションの詳細情報を収集するためにAPIを提供しています。

02 コンプライアンス

コンプライアンスモジュールは、検出・分類モジュールで検出されたアプリケーションの管理を有効にします。 コンプライアンス モジュールAPIにより、各アプリケーションの設定を確認または修正するソリューションを開発することができます。

03 感染検知

感染検知モジュールは、エンドポイントプロセスおよびネットワーク接続（MetaDefenderまたはMetaDefender Cloud）をリモートで分析するだけでなく、エンドポイントにインストールされたアンチマルウェアアプリケーションによって繰り返し検出される脅威を短時間で分析して、デバイスの健全性状態を迅速に評価します。

04 脆弱性評価

脆弱性評価モジュールにより、OESISパートナーのソリューションは、標的になりうるアプリケーションの脆弱性を評価することができます。これは、20,000以上のアプリケーションのバージョンから100万以上の脆弱なバイナリを報告します。インストールされているアプリケーションと最新バージョンを比較し、既知のアプリケーションの脆弱性と重要度を報告します。

05 ペリフェラル管理

OESISのペリフェラル管理モジュールは、データが完全にスキャンされるまでエンドポイントに接続されているUSBドライブをブロックすることで、USBメディアに関連するセキュリティリスクを軽減します。
OESISにより、USBブートセクタのスキャンを含む高度な脅威検出のセキュリティ機能を構築できます。

06 アプリケーションクリーンアップ

OESISのアプリケーション クリーンアップモジュールは、セキュリティリスクや、過剰なメモリを使用する可能性の高いアプリケーションやファイルをエンドポイントから検出し、修復し、完全にクリーンアップします。 サポート切れのアンチマルウェアソフトウェアや潜在的に望ましくないアプリケーション（PUA）など、実行中のソフトウェアを終了またはアンインストールできます。

OPSWATパートナー

OPSWATとのパートナーシップで、よりセキュアなソリューション

テクニカル パートナー プログラム 01

OPSWATは、最先端テクノロジー企業と協力し、データワークフローを保護し、迅速で信頼性の高い展開を提供します。 これらの統合ソリューションを利用するお客様は、製品スイート全体において完全な相互運用性の恩恵を受けることができます。

マルウェア共有 プログラム 02

この限定プログラムは、マルウェア研究を積極的に行っているパートナーと新しいマルウェアサンプルを共有します。（マルウェアの分析と研究に積極的ではない個人またはサードパーティ企業は、このプログラムに参加することができません。）

MetaDefender エンジン サプライヤー プログラム 03

OPSWATは、MetaDefenderに組み込むためにOEMまたはカスタムエンジン ソリューションを提供するアンチマルウェアエンジン プロバイダと提携しています。 参加パートナーはロイヤリティを受け取ります。

metadefender.com エンジン サプライヤー プログラム 04

OPSWATはmetadefender.com の一部としてソリューションを提供するアンチマルウェアエンジン プロバイダと提携しています。
全ての商用エンジンプロバイダは、ロイヤリティを受け取ります。

認定プログラム

パワフルで信頼性が高く効率的なショーケースアプリケーション

OPSWAT認定セキュリティ アプリケーション プログラムは、エンドポイント セキュリティ ソフトウェアの相互運用性認定の業界標準です。このプログラムにより、独立系ソフトウェアベンダーは、自社アプリケーションと主要な技術ソリューションとの互換性を確保することができます。

すべての認定ベンダーは、自社アプリケーションが強力で信頼性があり、効率的で、世界中の2億ものエンドポイント、そして主要なネットワーク　アクセスコントロールと互換性があることを示すバッジを受け取ります。

www.opswat.jp/certified をご参照してください。

- **互換性**
  全ての主要なCASB, NAC, SSL-VPN および SSOソリューションとの互換性、ネットワーク アドミン管理コンソールの検出と分類を確保
- **品質**
  AV-TEST, AV-Comparatives, ICSA Labs, SDK Labsおよび SE Labsとのパートナーシップを通じ、独立したテストラボによる優れた品質評価
- **誤検知**
  無害なファイルが悪意のあるものと誤って識別されないようにするための誤検知の対応

チャネルパートナー

チャネル パートナー プログラムは、ビジネスに最も革新的なセキュリティ ツールを提供します。

OPSWATのチャネルパートナーは、世界中のデータとインフラをより安全にするという使命を実現するための重要な位置付けです。OPSWATは、世界中の多くの付加価値ディストリビュータ、付加価値リセラー、システムインテグレータと連携しています。

チャネル パートナー トレーニング
定期的なチャネルパートナートレーニングの提供により、チャネルパートナーは、OPSWAT製品とその実装に関して専門知識を有しています。

チャネル パートナー イベント
OPSWATは、世界中のパートナーとイベントを共催し、エンドユーザへサイバーセキュリティ技術の最新情報を学んでいただくと同時に、パートナーの相互成長をサポートしています。

OPSWAT チャネル パートナー

- ネットワンパートナーズ
- Help AG
- Bulwarx
- Prosoft
- Insec Security
- Biztributer
- EMT

チャネル パートナーになることにご興味がある場合は、SALES@OPSWAT.COM　までご連絡ください。

お客様

OPSWATは何千ものお客様へより安全なデータを提供しています。

OPSWATのMetaDefenderは大企業、金融機関、政府、防衛関連、官庁含む千以上もの幅広いお客様から信頼を得ており、包括的な脅威の保護と防御を提供しています。 MetaDefenderは、オンプレミスやクラウド ソリューションからネットワーク分離まで、様々な環境に導入されています。

最新のカスタマイズされた強力なサイバー セキュリティ ソリューションについては、OPSWATへお問合せください。

政府	防衛	エネルギー	金融	製造	ハイテク

グローバルサポート

最高のサービスを24時間365日で提供

OPSWATチームはOPSWAT製品を利用することで、可能な限り最良の経験をお客様へ提供できるようにしたいと考えています。ベトナム、ルーマニア、サンフランシスコのサポートオフィスでは、OPSWATは24時間365日のサポートを提供することができます。OPSWATのスタンダード、ゴールド、プラチナのサポートプランについては、www.opswat.jp/supportをご覧下さい。

オフィス

アメリカ
Headquarters
398 Kansas Street,
San Francisco, CA 94103, USA
(415) 590-7300

ルーマニア
2nd Martin Luther Street, 4th Floor
300054 Timișoara, Romania

ハンガリー
H-8200 Veszprem, Bajcsy-Zs.
u.15. Hungary

イスラエル
Karlibach 10, Floor No. 1
Office No. 6, Tel Aviv-Yafo

ベトナム
Harbour View Tower, 35 Nguyen Hue,
14th floor, District 1,
Ho Chi Minh city, Vietnam

イギリス
20 Market Place,
Kingston upon Thames,
Surrey KT1 1JP, United Kingdom
+44 (0) 20-8328 9830

日本
〒100-0004
東京都千代田区大手町 1-7-2
東京サンケイビルディング 27 階

台湾
18/F, No. 460, Sec. 4, Xinyi Rd.
Xinyi Rd. Dist., 11052 Taipei, Taiwan

技術サポート

スタンダード	ゴールド	プラチナ
8:00-17:00 月曜～金曜 メールによるサポート	7:00-19:00 月曜～金曜 メール・電話によるサポート	24時間 365日 メール・電話によるサポート

OPSWAT.