

MetaDefender® ICAP Server

ネットワークトラフィックの信頼性

サイバー犯罪のビジネス化と、さらなる高度化・巧妙化により、マルウェアから組織ネットワークを保護することは、かつてないほど困難になっています。

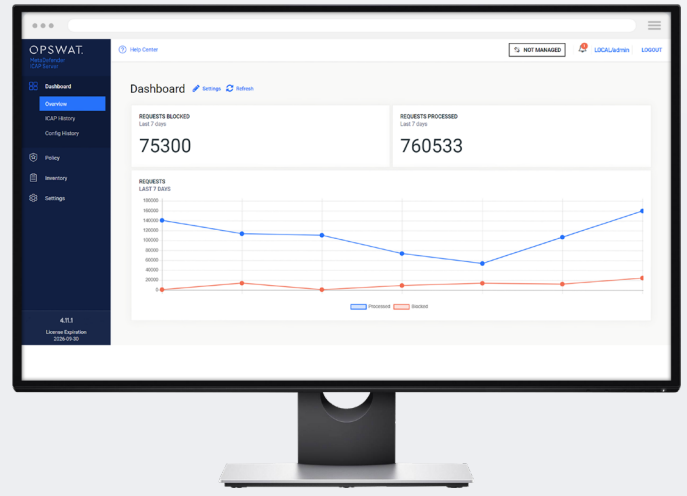
今この瞬間にも、悪意のあるファイルや機密ファイルが、内部や外部ユーザーによって意図的または意図せずにネットワーク経由で転送されている可能性があります。ファイルは、Webアプリケーションファイアウォールによって傍受され、Webゲートウェイのアンチウイルスに送信されることがあります。しかし、ファイルに高度な回避型マルウェアやゼロデイ脅威が含まれている場合はどうでしょうか。また、機密データや予期しないPII(個人情報)が含まれている場合はどうなるのでしょうか。

設定・分析・対応

MetaDefender ICAP Server と MetaDefender Core によりネットワークを通過するすべてのファイルを検査することで、ユーザーとシステムは悪意のあるインターネットコンテンツから包括的に保護されます。

MetaDefender ICAP Server は、MetaDefender Core と、ICAP プロトコルをサポートするクライアントアプリケーション(セキュアゲートウェイ、プロキシ、Webアプリケーションファイアウォールなど)との間のICAPインターフェイスを提供します。すべてのファイルは、クラス最高の脅威検知と防止テクノロジーで処理されます。

その結果、すべての疑わしいファイルは、エンドユーザーがアクセスできるようになる前にブロックまたは無害化されます。機密データは秘匿化、削除、またはブロックされ、組織のセキュリティコンプライアンス基準への対応を支援します。



「当社がさまざまなシステムでOPSWATの技術を使い始めて数年になります。業界内でのOPSWATの評判は素晴らしいものでした。この業界で30年働いてきましたが、OPSWATは信頼のおける、素晴らしいパートナーです。」

Joe Peck 氏

Senior Director of Product Management, F5®

利点

- ネットワーク上の脅威をリアルタイムで包括的に検知・防御
- ゼロデイ攻撃や高度な標的型攻撃に対する保護
- インストール前に、ファイルベースの脆弱性を検出
- 組織に出入りする機密データを検出
- 独自のセキュリティニーズに対応するカスタムポリシー、ワークフロー、分析ルール
- ICAP対応機器との容易な連携

OPSWAT.

MetaDefender ICAP Server

統合

MetaDefender ICAP Server は、ICAP (Internet Content Adaptation Protocol) をサポートする製品と統合し、様々な交点に設置することでファイル転送の安全性を確保します。

MetaDefender ICAP Server の典型的な統合は以下のとおりです。

仕様

オペレーティングシステム

- Windows
Windows 7, 10, Server 2012, Server 2016, Server 2019 or newer [64 bit]
- Linux
Red Hat [7.x, 8.x], Ubuntu [14.04, 16.04, 18.04, 20.04], CentOS [7.x, 8.x], Debian [8.x, 9.x, 10.x, 11.x]

ハードウェア要件

最小 RAM: 2GB

最小 SSD: 2 GB + ~500MB x [スキャンエンジンの数]

ブラウザ

Chrome, Firefox, Safari, Microsoft Edge

ポート

インバウンド [1344, 8048], アウトバウンド [8008]

ファイルシステム

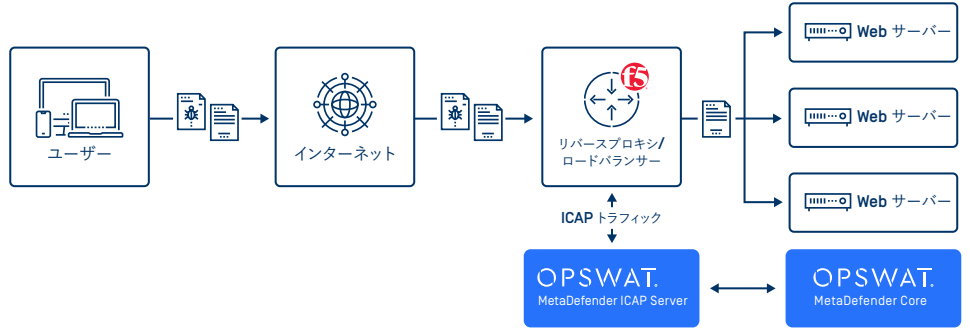
NTFS, FAT32, AFS, Linux EXT2, 3 & 4

導入形式

オンライン/オフライン, 物理/仮想

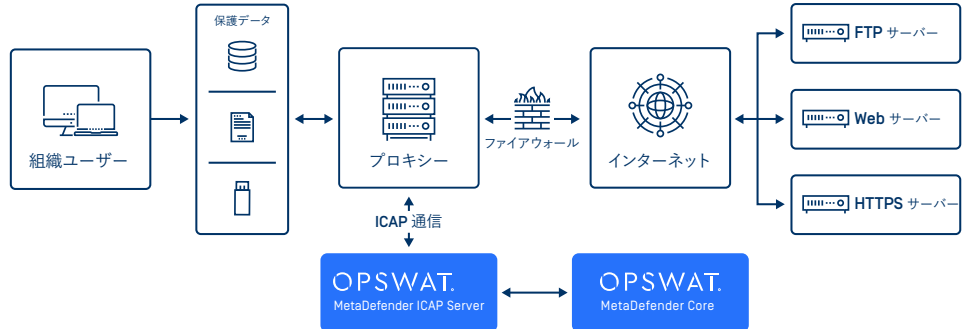
リバースプロキシ / Webアプリケーションファイアウォール / ロードバランサー / ADC
悪意あるファイルのアップロードからアプリケーション Web サーバーを保護

サポート: F5® Advanced WAF™, F5 Big-IP® ASM™, F5 Big-IP® LTM™, Citrix ADC, Avi Vantage (VMware), Symantec™ Blue Coat ProxySG



フォワードプロキシ / Webゲートウェイ / ファイアウォール
Webトラフィックがセキュリティで保護されたネットワークに到達する前に検査

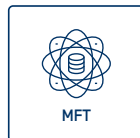
サポート: Squid, ARA Networks JAGUAR5000, McAfee Web Gateway™, Fortinet FortiGate®



SSL インспекション

Webトラフィックがセキュリティで保護されたネットワークに到達する前に検査

サポート: F5® SSL Orchestrator™, A10 Networks Thunder® SSLi®



マネージドファイル転送

データリポジトリを移動するすべてのファイルトラフィックをスキャン

サポート: GoAnywhere MFT, Progress MOVEit, Axway B2Bi, Axway SecureTransport



ストレージソリューション

リポジトリ内のファイルの読み取り、書き込み、静止画のスキャンを高速に実行

サポート: Dell EMC Isilon OneFS, Nutanix Files, Huawei Oceanstor

OPSWAT.

Trust no file. Trust no device.

MetaDefender ICAP Server の詳細
opswat.jp/products/metadefender/icap

[OPSWAT.jp/contact](https://opswat.jp/contact)