MetaDefender 脅威検出・防御プラットフォーム

MetaDefenderのテクノロジには、多くのマルウェア対策エンジンを使用したスキャン、ヒューリスティック検知の活用、拡張子偽装の検出、データ無害化、アーカイブスキャン等の機能が含まれ、組織が既知・未知の両方の脅威を検出、防御することを可能とします。

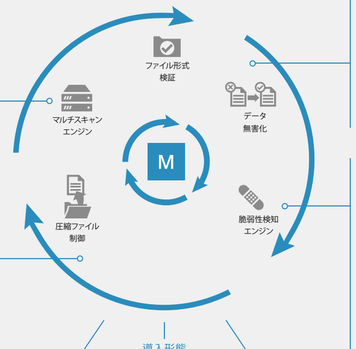
30＋ 組込み型 マルウェア対策 エンジン

AhnLab, ESET, SOPHOS, Symantec, Bitdefender, Quick Heal, K7, NANO, CYREN, KASPERSKY, LAVASOFT, TREND MICRO, McAfee, Zillya, IKARUS, TACHYON, TOTAL DEFENSE, Avira

30＋ 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



導入形態：オンプレミス / エア・ギャップ / クラウド

90＋ 組込み型 データ無害化 エンジン

PPT, PPTX, DOC, DOCX, XLS, HTML, JPG, PDF

15K＋ アプリケーション 脆弱性検知 エンジン

脆弱性検知エンジンはアプリケーションのバージョンチェックと報告された脆弱性に対応するために何千もの最も利用頻度の高い製品に属した100万以上のバイナリに対応しています。

Skype, Adobe, Java, Word, Excel, PowerPoint

METADEFENDER アドオン

- MetaDenfender Kiosk
- MetaDenfender Vault
- MetaDefender Email Security
- MetaDefender ICAP Server
- MetaDefender Client

特長

- 最大32種類のウイルススキャンエンジンで、最高水準のウイルス検出率をワンサーバで実現。(各ベンダーと個別契約は不要です)
- ファイルを無害化するサニタイズ機能。(別途ファイル無害化エンジンが必要です)
- メールの添付ファイルやインターネットブラウジング時のダウンロード及びアップロードファイルをスキャン可能。(別途MetaDefender Email SecurityやMetaDefender ICAP Serverが必要です)
- ウイルス対策エンジンのヒューリスティックスキャン機能。
- 開環境のみならず、閉環境のウイルススキャンもサポートし、シグネチャはオンラインでもオフラインでも更新が可能。
- 任意の間隔で最新のシグネチャを自動でダウンロード、更新します。
- Webベースの管理コンソールとユーザロール機能。
- ハッシュ突合メカニズムによりファイルの白黒判定にかかる所要時間を短縮します。
- 多層型や自動解凍型アーカイブをはじめ、豊富なファイルタイプをスキャンできます。
- 他のシステムと連携を容易にするAPIを提供。
- 複数のスキャンのノードを設けることでスキャンの負荷を分散させ、スキャンのスループットを向上できます。

1台のサーバに複数のウイルススキャンエンジンを搭載し、マルウェアをスキャン。スループットを維持しながら強力なウイルス検出及びファイル無害化を実現します。このソリューションを導入することにより、水際でのマルウェアの対策がより一層確実なものになります。

ライセンス体系

Windows MetaDefender Core 8/12/16/20 ＋ ワークフローエンジン ＋ カスタムエンジン ＋ アドオン

- Core 8: AhnLab, Bitdefender, Avira, Quick Heal, ESET, total defense
- Core 12: TACHYON, CYREN, K7, IKARUS
- Core 16: KASPERSKY, EMSISOFT, Zillya
- Core 20: McAfee, NANO, SOPHOS

Linux MetaDefender Core 5/10 ＋ ワークフローエンジン ＋ カスタムエンジン ＋ アドオン

- Core 5: ESET, total defense, Bitdefender, K7
- Core 10: Avira, IKARUS, CYREN, Quick Heal

カスタムエンジン

Windows: TREND MICRO, Symantec, SYSTweak, Microsoft, netgate, BytesHard, LAVASOFT, 火绒安全, Filseclab

Linux: McAfee, SOPHOS, NANO, AhnLab

仕様

Windows

サポートされるOS	Windows 7/8/8.1/10, Windows Server 2008/2008R2/2012/2012R2/2016　＊64ビットOSのみサポート
CPU	8コア以上(MetaDefender Core 8)、16コア以上(MetaDefender Core 12～16)、32コア以上(MetaDefender Core 20)
ハードディスク*	16GB以上(MetaDefender Core 8)、24GB以上(MetaDefender Core 12)、32GB以上(MetaDefender Core 16)、40GB以上(MetaDefender Core 20)
メモリー*	8GB以上(MetaDefender Core 8)、16GB以上(MetaDefender Core 12～20)、24GB以上(MetaDefender Core 20)

＊アプリケーションの動作には百万件のスキャンデータ毎に1.5GBの空き容量が別途必要です。

Linux

サポートされるLinuxディストリビューション	CentOS 6.6及び7.0以上、Red Hat Enterprise Linux 6.6及び7.0以上、Debian 7.0以上、Ubuntu 14.04及び16.04以上
CPU	4コア以上のプロセッサ(MetaDefender Core 5)、8コア以上のプロセッサ(MetaDefender Core 10)
ハードディスク*	10GB以上(MetaDefender Core 5)、20GB以上(MetaDefender Core 10)
メモリー*	4GB以上(MetaDefender Core 5)、8GB以上(MetaDefender Core 10)

＊アプリケーションの動作には32GB以上が必要です。これ以外に百万件のスキャンデータ毎に1.5GBの空き容量が必要です。

当製品に関する詳細はこちらから ▶ https://next-security.jp/metadefender-core/

販売元：Next Security Inc.
ネクスト・セキュリティ株式会社
〒140-0004　東京都品川区南品川2-4-7 アサミビル5階
[東京本社] TEL：03-5783-0702　FAX：03-5783-0734
[大阪事業所] TEL：06-6362-2007　FAX：06-6362-2008
[E-mail]　info@next-security.jp
[Facebook] www.facebook.com/NextSec.inc
[Twitter]　@Next_Security

この製品のご用命は

Next Security Inc.

OPSWAT. MetaDefender
メタディフェンダー コア

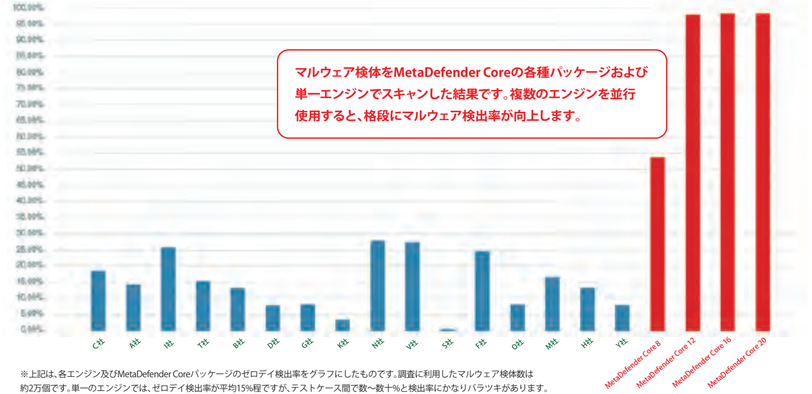
最大32種類のウイルス対策エンジンでマルウェアを検出。メール・ファイルの無害化もこれ一つで！

多くの企業では一種類のウイルス対策ソフトウェアしか導入していないため、そのベンダから定義ファイルが提供されるまでの間、脅威に対する保護ができなくなる課題がありました。また、導入しているウイルス対策ソフトウェアの脆弱性が狙い撃ちされた場合、保護が継続できなくなり、ウイルスの侵入を許してしまう事態になります。また、WannaCryやNotPetya等のランサムウェアにも迅速な検知が必要となります。実際、社内ネットワークに侵入を試みるウイルスを水際で阻止するには、複数のウイルス スキャン エンジンを使用して、確実にそのウイルスを検出できる体制を整えることが必要です。単一サーバで最大32種類のウイルス スキャンエンジンでウイルス検知を実現できるオンプレミス版では唯一のウイルス対策ソリューションがMetaDefender Coreです。

マルチエンジンってそんなにいいの？

☑ 検出率の向上	一つのエンジンが持つマルウェア検出のカバレッジもエンジンを複数置く事によって増大させることが可能。これによって、マルウェア検出率が向上します。
☑ 検出の補完性	たとえあるエンジンがマルウェアを検出できなかったとしても別のエンジンで検出が可能です。
☑ 保護の迅速性	搭載エンジンのベンダーの中で最も早く提供された定義ファイルを利用して、最新のマルウェアに対処できます。

複数エンジンによるマルウェア検出率の向上



マルウェア検体をMetaDefender Coreの各種パッケージおよび単一エンジンでスキャンした結果です。複数のエンジンを並行使用すると、格段にマルウェア検出率が向上します。

※上記は、各エンジン及びMetaDefender Coreパッケージのゼロデイ検出率をグラフにしたものです。調査に利用したマルウェア検体数は約2万個です。単一のエンジンでは、ゼロデイ検出率が平均15%程ですが、テストケース間で数～数十%と検出率にかなりバラツキがあります。これに比べ、MetaDefender Coreは複数のエンジンを使用しているため、常に安定した検出率を維持しており、最小構成のMetaDefender Coreでも確実で強力なマルウェア検知を実現します。また、一つのエンジンで検出してもそれが誤検知である可能性があり、より確定的に判断するには、複数エンジンでの確認が必須です。お客様の既存セキュリティの大幅強化に是非MetaDefender Coreをご検討ください。

(弊社調査による)

ワークフローエンジン

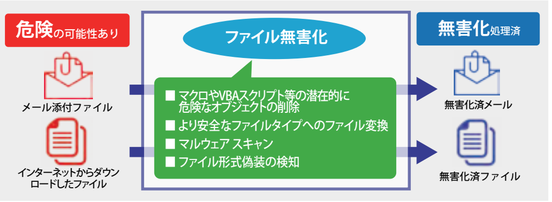
脆弱性解析エンジン

アプリケーションの脆弱性情報を提供するアドオンです。マルウェアは脆弱性を狙い、アプリケーションに不正にアクセスします。このアドオンを使う事により、セキュリティパッチの適用等の脆弱性対策を支援し、マルウェアの感染を予防します。

ファイル無害化エンジン

地方自治体の分野において、ウイルス感染のない無害化通信を図ることが求められております。※1 また、学校のネットワークセキュリティにおいても校務系システムと学習系システムのネットワーク分離が求められており、ファイルの無害化が必要となります。※2 無害化とは、インターネットから取得したファイルから、既知及び未知のマルウェアを除去したり、悪意のある活動を引き起こす可能性のある領域を排除し、安全なファイルとして再構築することを指します。MetaDefender Coreはこの処理を実現できる優れた製品です。

※1『新たな自治体情報セキュリティ対策の抜本的強化に向けて～自治体情報セキュリティ対策検討チーム報告～』より　※2『教育情報セキュリティのための緊急提言（案）』より



- 既知及び未知のマルウェアの除去
- 悪意のある動作を引き起こす可能性があるオブジェクト(マクロ、ハイパーリンク等)の無効化
- 潜在的に危険なオブジェクトが実行されないようなより安全な形式にファイルを変換
- 拡張子が偽装されたファイルをブロック

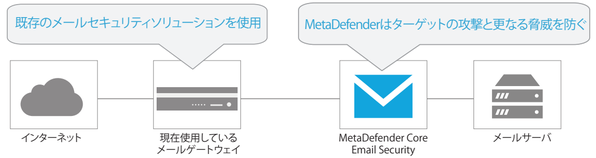
無害化対象ファイル

無害化対象ファイル形式	無害化後のファイル形式
Office製品	
.doc	doc, pdf
.docx /.docm	docx, bmp, html, jpg, pdf, png, ps, svg, tiff, txt
.dot	dot
.dotx	dotx
.hwp	hwp
.jtd	jtd
.odt	odt
.ppt	ppt, pdf
.pps /.pptm /.pptx	pptx, bmp, html, jpg, pdf, png, ps, svg, tiff
.ppsx	.ppsx
.vsdx	.vsdx
.vsdm	.vsdm
.rtf	rtf
.xls	xls, pdf
.xlsb	xlsb
.xlsm / .xlsx	xlsx, bmp, csv, html, jpg, pdf, png, ps, svg, tiff
.xml-doc /.xml-docx/.xml-xls	pdf
画像ファイル	
.jpg / .jpeg	jpg, bmp, eps, gif, pdf, png, ps, svg, tiff
.gif	jpg, bmp, png, tiff, svg, ps, eps, pdf
.bmp / .png	jpg, bmp, png, tiff, svg, gif, ps, eps, pdf
.svg	jpg, bmp, png, tiff, gif, ps, eps
.tiff /.tif	jpg, bmp, png, tiff, svg, gif, ps, eps
.wmf	jpg, bmp, png, tiff, svg, gif, ps, eps, pdf
その他のドキュメント／ファイル	
.pdf	pdf, bmp, html, jpg, png, svg, tiff, txt
.htm /.html	html, bmp, jpg, pdf, png, ps, svg
.xml	xml, pdf
.csv	csv
.dmg	dmg
.emf	emf
.7z	7z, zip, gz, zx
.gz	gz, 7z, zip, zx
.rar	zip, 7z, gz, xz
.xz	xz, zip, 7z, gz
.zip	zip, 7z, gz, xz

アドオン

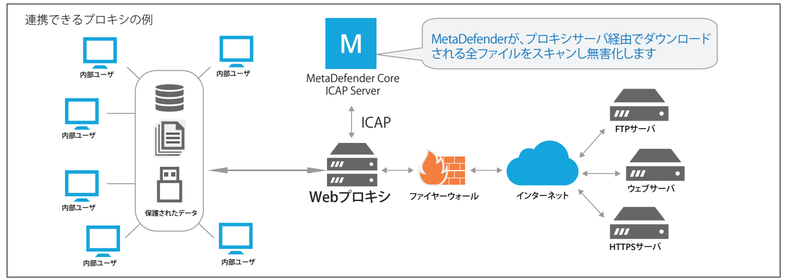
MetaDefender Email Security

MetaDefender Email SecurityはMetaDefender Coreで受信メールや送信メールの添付ファイルを処理するためのアドオンです。
お客様のネットワークを守るために既存のメールゲートウェイソリューションと容易に連携することができます。



MetaDefender ICAP Server

MetaDefender ICAP ServerはMetaDefender CoreでWebブラウジング時にアップロード/ダウンロードされるファイルを処理するためのアドオンです。既存のWebプロキシやリバースプロキシソリューションと連携して安全にWebブランシングを行えます。



MetaDefender Client

エンドポイント上のファイルをスキャンしたり、USB接続時の自動スキャンを行う軽量なスキャニングソフトウェアです。
エンドポイント保護のエンタープライズ用包括的システムは弊社「フォアグラスキャンシステム」もご検討ください。

MetaDefender Vault

MetaDefender Coreで処理したファイルを高レベルセキュリティエリアで利用管理する場合に必要なアドオンです。
クリーンなファイルのアクセス管理が可能です。

外部スキャナー

お使いの解析ソリューションにファイルを転送し、その解析結果をMetaDefender Coreの結果レポートに追加するためのアドオンです。

MetaDefender Kiosk

MetaDefender Kioskは、マルチエンジン型ウイルススキャンソリューション「MetaDefender Core」と連携し、プロファイルに基づくファイルタイプやサイズによるデータ制御や偽装拡張子チェック、ファイル変換を自動で行い、セキュリティレベルの高いエリアに持ち込まれるデータを判定・処理するデータチェックソリューションです。ファイルは「MetaDefender Core」による最大32種類のウイルス スキャン エンジンを使用してスキャンも行われます。

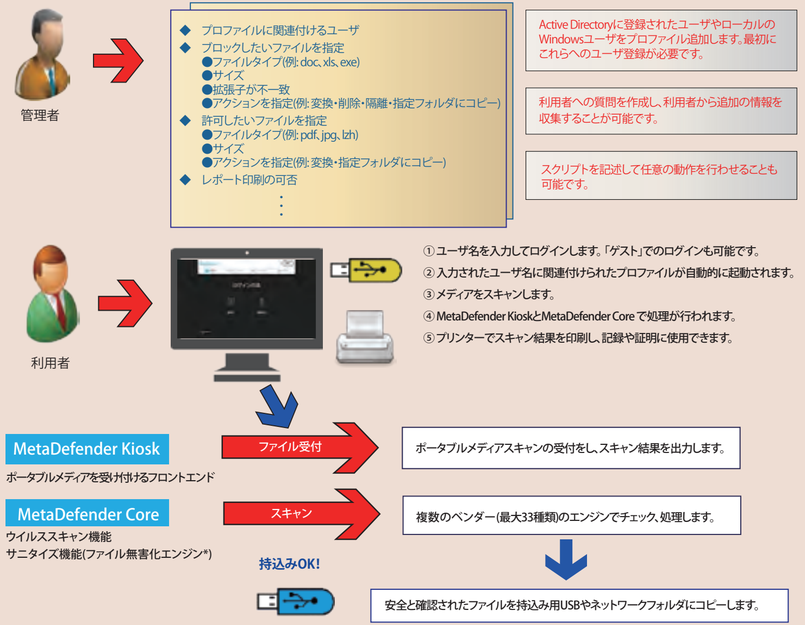
MetaDefender Kioskの特徴

① FD、CD、DVD、Blu-ray、USBデバイス、SDカード等の各種メモリーカード等様々な外部メディアをサポート。
② CD→USBやSD→CD-Rなど、持参したメディアとセキュリティエリア内に持ち込むメディアの種類が異なっていても問題なし。*
③ キオスク利用者から情報を直接入力してもらうためのカスタム質問作成機能。(例: ユーザの会社名、来訪先、来訪目的)
④ プロファイルはユーザ毎に設定が可能です。プロファイル作成のためのユーザ登録は、Active DirectoryやWindowsローカルアカウントのユーザを追加するだけです。
⑤ フルスキャン、特定のファイルのみのスキャンが可能です。
⑥ オールインワンPC・ノートPC・キオスク端末等、シーンに合ったハードウェアに対応。
⑦ メディア内のAutorunを無効化したり、キー入力を制限することで、MetaDefender Kiosk端末への感染を防止。
⑧ 暗号化USB・指紋認証USB(例: Biocryptodisk)をサポート。
⑨ 監査や記録のためのログ(テキストやPDF形式でメール配信も可能)・レポート発行機能。
⑩ Webベースの管理コンソールのため、管理ソフトやそれにアクセスするためのクライアントソフトは不要。

*コピー元メディアとコピー先メディアは同時に接続する必要がありますので、それぞれの空きポートが必要です。

動作の仕組み

事前にプロファイルを作成します。(例えば、従業員・請負業者・その他で個別にプロファイルを作成可能)



*ファイル無害化エンジンはアドオンとなります。アドオンを使用するには、MetaDefender Coreが必要です。