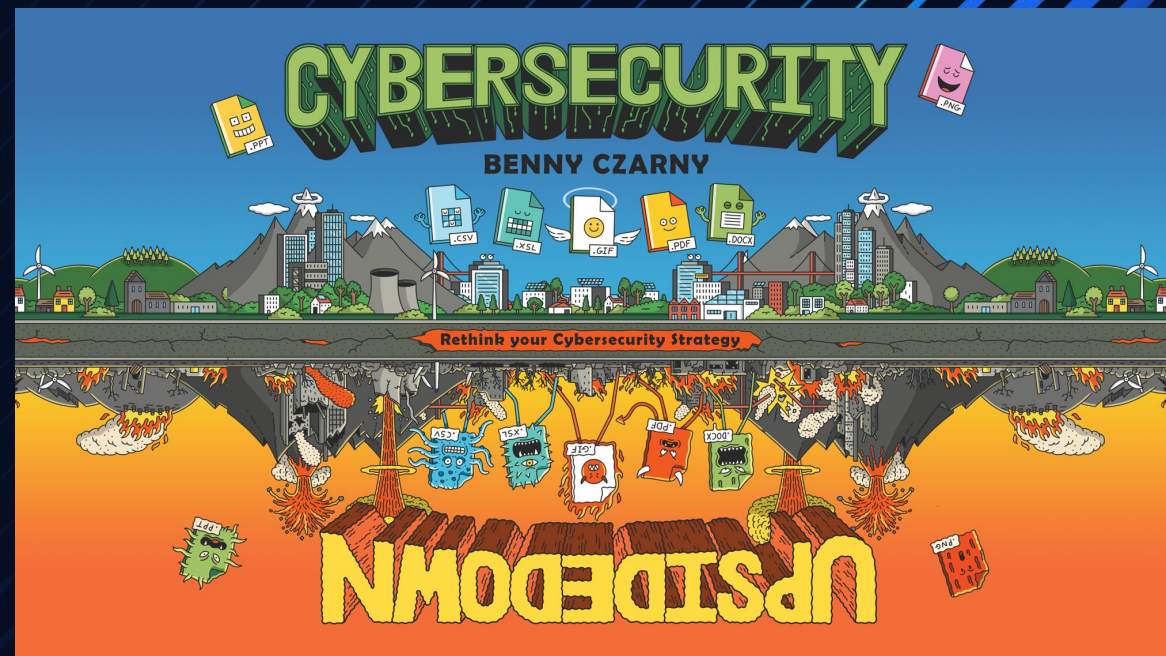


OPSWAT.

DOWでも採用された検知技術！

AI駆動型サイバー攻撃の脅威 — 防衛・重要インフラの「最後の砦」

OPSWAT JAPAN株式会社
Regional Sales Manager
野田 芳裕
2026年10月09日



免責事項

本書は情報提供のみを目的としています。

OPSWATが現在提供している製品およびその例をご紹介します。

本書の内容は予告なく変更されることがあります。

お客様は、ご自身の責任においてこの文書に記載されている情報 およびその使用について、評価を行います。

OPSWATの製品またはサービスは、現状有姿のまま提供されます。

本書における内容は、明示または黙示を問わず、いかなる種類の保証も行いません。

本書における内容により、いかなる保証、表明、契約上のコミットメントも生じません。

本日のご案内

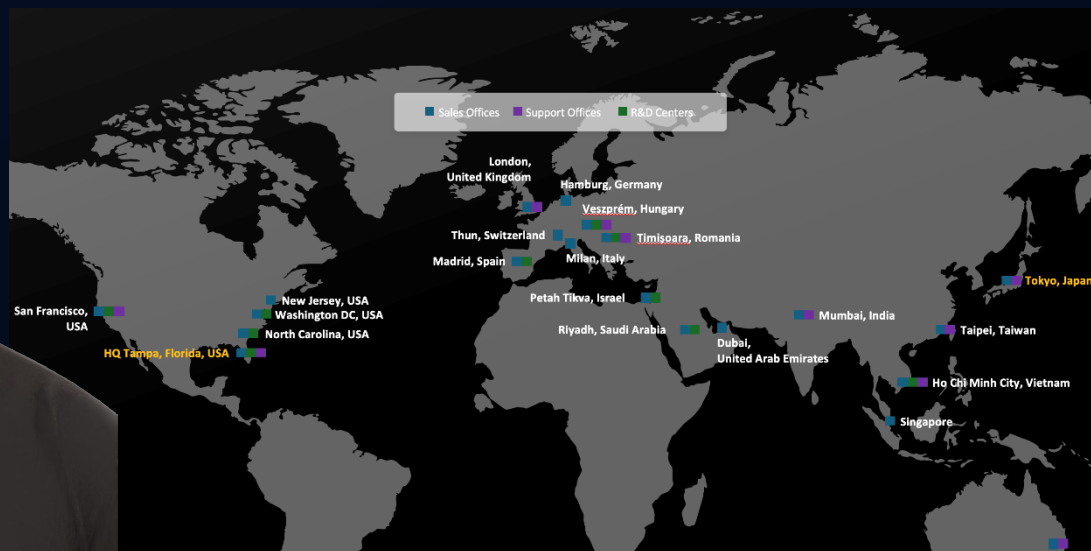
- OPSWAT Inc, 会社概要
- OPSWAT製品概要
- ユースケース
- まとめ

本日のご案内

- OPSWAT Inc, 会社概要
- OPSWAT製品概要
- ユースケース
- まとめ

OPSWAT Inc, 会社概要

会社名： OPSWAT Inc
CEO（創業者）： ベンジャミン・チャーニー
従業員数： 1100人+
住所： 5411 Skycenter Dr, Ste 900 Tampa, FL 33607
設立日： 2002年
事業内容： ソフトウェア・ハードウェアの開発・販売
OPSWATは、企業向けのセキュリティソリューションを提供するサイバーセキュリティ企業



OPSWAT OPX ラボ (重要インフラIT/OT機器ショールーム)

場所：東京都千代田区神田錦町2-11-6 森紙業神田ビル 4階
(地下鉄大手町駅：C2b出口徒歩5分、竹橋駅：3b出口徒歩4分)

OPSWAT.

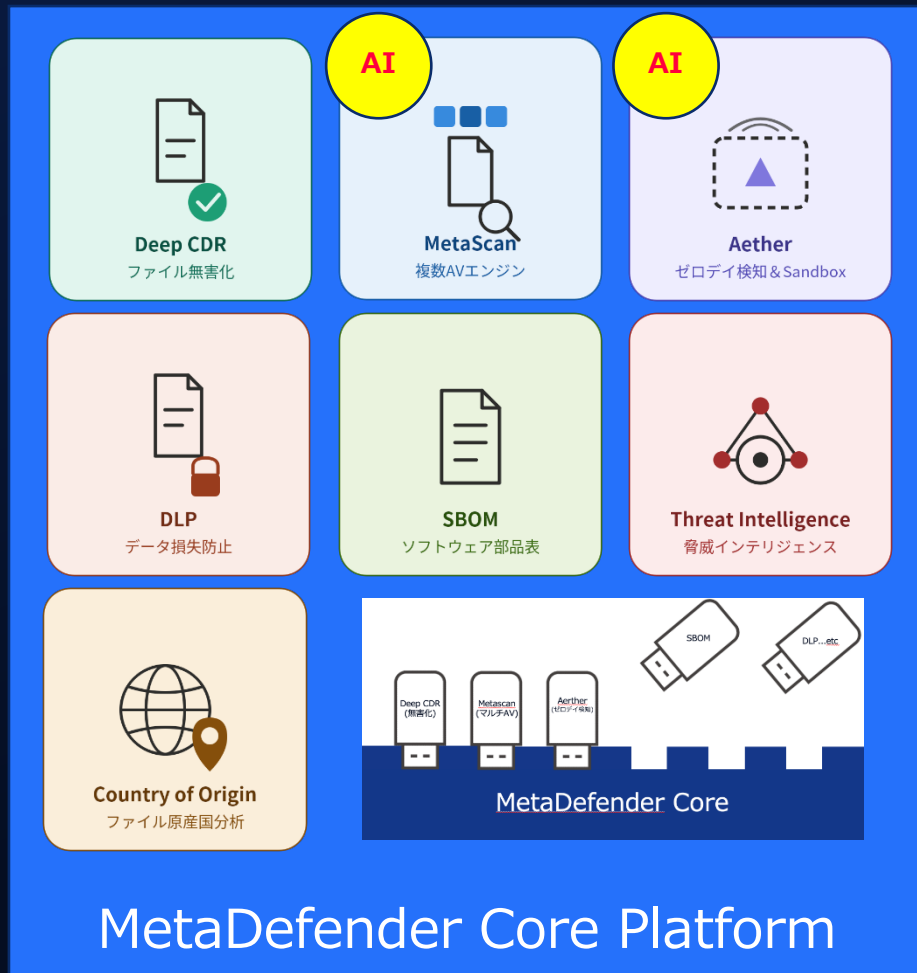


本日のご案内

- OPSWAT Inc, 会社概要
- OPSWAT製品概要
- ユースケース
- まとめ

OPSWAT 製品群

ネットワーク境界防御サーバー製品
(ソフトウェア)



物理的侵入（流出）防御製品
(ハードウェア)

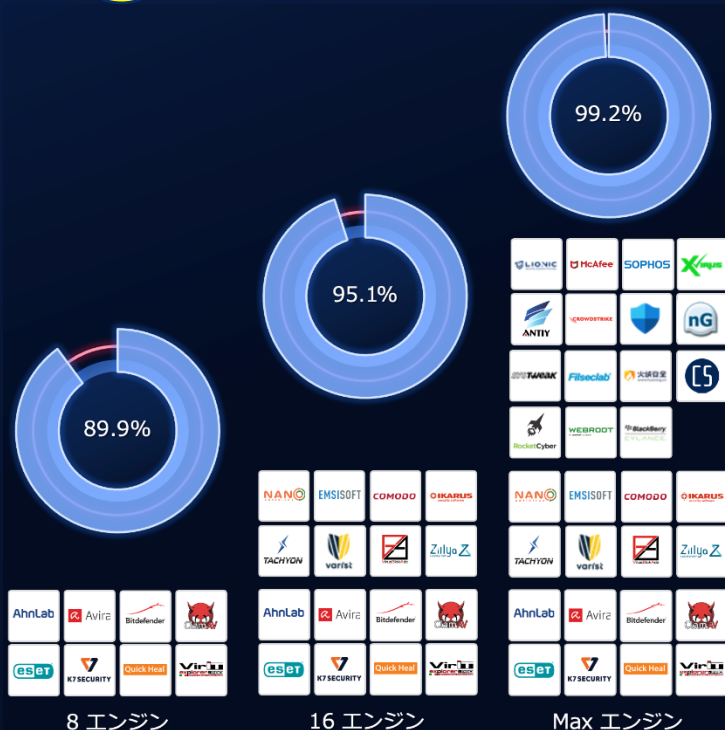


ネットワークを経由しないファイル対応製品
(ハードウェア + ソフトウェア)

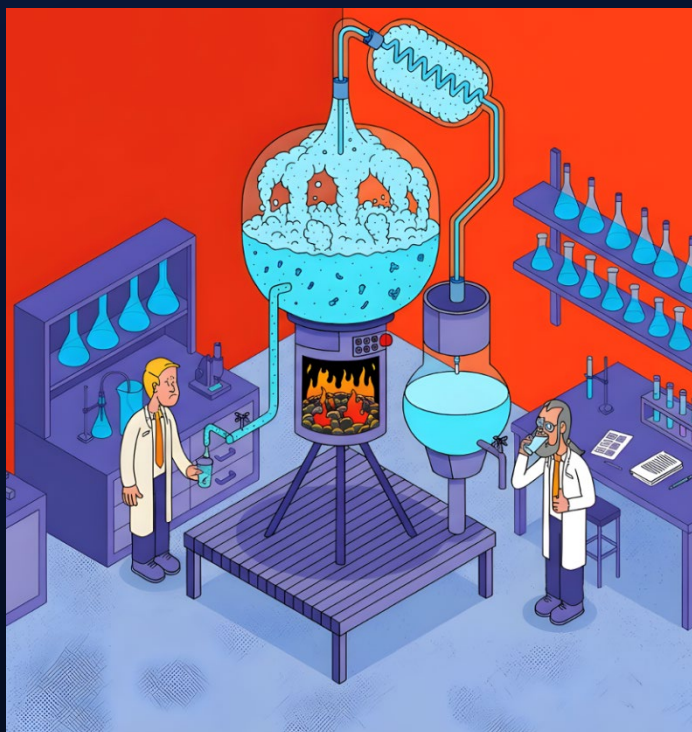


OPSWAT ソフトウェアの3種の神器

AI マルチスキャン



ファイル・脅威の無害化



AI 統合型ゼロデイ検知



OPSWATのソフトウェアはネットワーク経由で流通するファイルに対して『Trust No File.』と、とことんファイルの安全性を追求します

AIが進化する中、未知の脅威に対する侵入防御は実質不可能なため、正常を装って侵入する悪意のファイルに対する、「マルチスキャン」「無害化」「サンドボックス&脅威判定」を行うことで、そのファイルへの安全性を高めます

New! MetaDefender Alin

(予測型AIエンジン)

実行前に悪意のあるファイルを予測

Alin エンジン 5つのメリット

実行前に検出

機械学習によるミリ秒の判定、デトネーション不要

低い偽陽性率

エンタープライズグレードでプライバシー保護のデータストリームで学習

脅威検出の加速

最小限のリソース負荷でミリ秒レベルのスキャン時間を提供

精度の向上

より高い検出率と低い誤陽性を実現

オフライン稼働

オンラインでもオフラインでも同じ信頼性で動作

ゼロデイアドバンテージ

サンドボックスで確認されたゼロデイで再学習

マルチスキャンニングを強化

従来のAVエンジンに追加し検出率Up

リソース効率の最適化

小さなメモリフットプリントを維持

シームレスに統合

MetaDefenderプラットフォームおよびOPSWAT製品全体で利用可能予定

New! MetaDefender Aether AI

(統合型ゼロデイ検知)



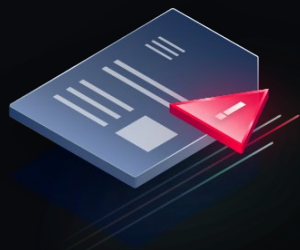
統合型ゼロデイ検知ソリューション
組み込みの脅威インテリジェンスを用いた動的分析を用いて
ゼロデイ脅威や回避型マルウェアを検出します

- ボリューム:幅広いファイルタイプを分析
- 従来20倍高速
- ゼロデイ有効性99.9%

NEW! Alin & Aether 他のエンジンとの相違

AI

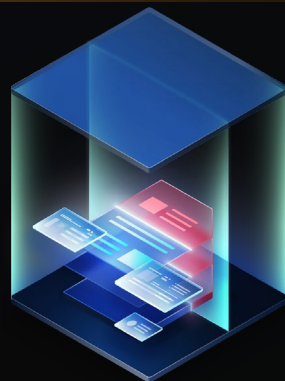
OPSWAT Predictive Alin AI vs. Other AV Engines



エンタープライズ コンテンツフローに最適

OPSWAT MLベースのエンジンは、企業のファイル移動パターンを再現する厳選されたプライバシー保護データセットで訓練されています

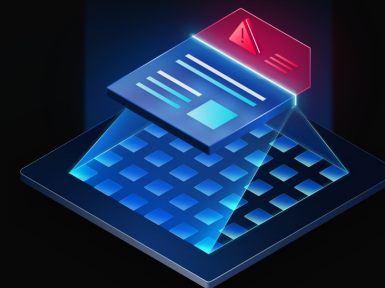
これにより、エンタープライズデータフローの高い検出精度を保持



Zero-Day Retraining Loop

MetaDefender Aetherのサンドボックス認証済みゼロデイで再学習

新たな発見が加わるたびに、Alinは同様の脅威を実行前に予測しブロックする能力が向上

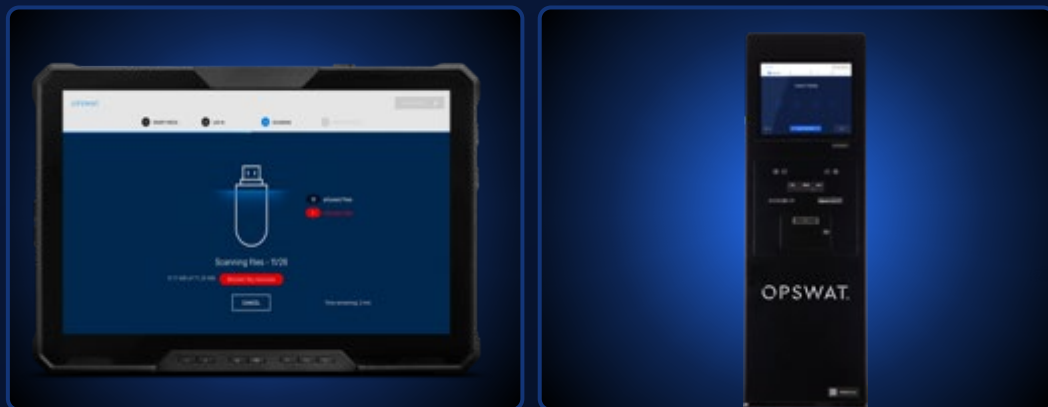


事前実行インテリジェンス層

Alin AIは従来のAVエンジンに先んじて動作し、シグネチャに依存しない構造的および行動的な侵害指標を検出

OPSWAT 最近大注目のハードウェア

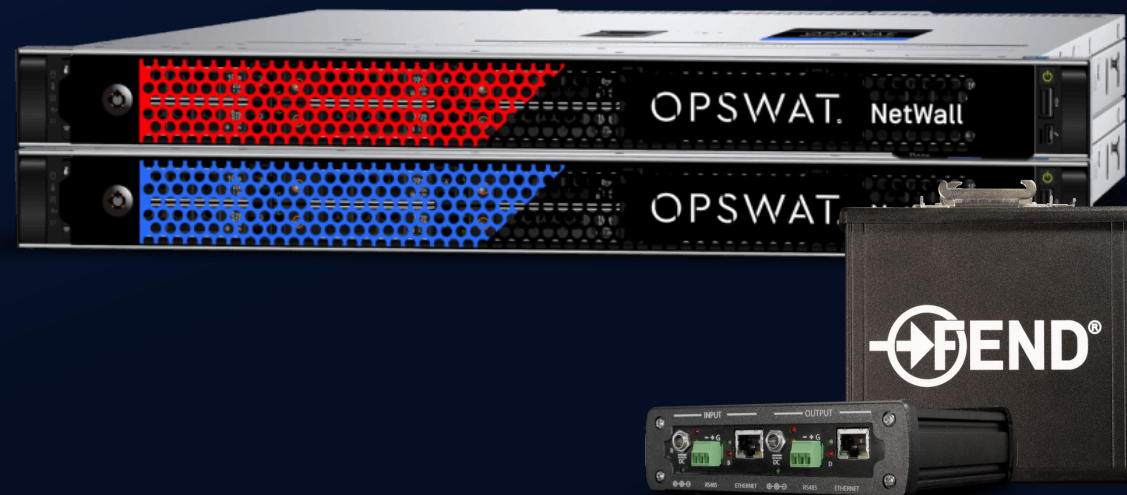
キオスク（検疫専用端末）



ネットワークを経由せず、USBメモリなど手軽に持ち運べて運用できるメディア経由で侵入するファイルに対して、ネットワークに持ち込む前に専用端末（Kisok）で「マルチスキャン」「無害化」「サンドボックス&脅威判定」を行います

※スタンドアローン型、外部サーバー連携型あり

オプティカルダイオード



オプティカルケーブルのほとんどシンプルな特性を活かして物理的な逆流不可能なネットワーク間接続環境を実現します

クロスドメインケースにおける異なるセキュリティレベルのネットワーク間を接続する技術として、ご採用が活性化しております

本日のご案内

- OPSWAT Inc, 会社概要
- OPSWAT製品概要
- ユースケース
- まとめ

某国政府でのOPSWAT導入サマリー

国防関連機関

11機関

7/11

Kiosk

4/11

CDS

政府民生機関

11機関

5/11

Kiosk

6/11

Compliance

政府法執行機関

8機関

8/8

Kiosk

8/8

外部接触

※9月末時点の社内調査結果のため、計測できていないケースもございます

都道府県警様ユースケース

都道府県警のUSB利用は、今後ますます対策が重要です

USB機器の不正利用やマルウェア感染による情報漏えい・改ざんなどのリスクが増大しています。

特に分離ネットワークへのデータ受け渡し時のUSBは対策が急務です。

OPSWAT MetaDefender KIOSKが、都道府県警のセキュリティ強化を強力に支援します。



都道府県警における USB利用の課題



USB経由のマルウェア感染リスク

持ち込みUSBや外部媒体が原因で、ランサムウェアなどのマルウェアに感染するリスクがあります。



Bad USBなどのハードウェア脅威

見た目は通常のUSBでも、キーロガー機能などにより不正操作や情報窃取を行うBad USBの脅威があります。



通常のウイルススキャンでは Bad USBは対策できません！

キーボードエミュレーション等を行うBad USBは検知・防御が困難です。



情報漏えい・改ざんのリスク

不正なファイルの持ち込みや、コピーによる情報漏えい・改ざんのリスクがあります。



これらのリスクにより、捜査・業務の停止、証拠の信頼性低下、県民の安全・安心の確保に重大な影響を招く可能性があります。

対策のベストソリューション

OPSWAT® Metadefender KIOSK

USBの安全な運用を支援します。

USBメモリ
持ち込み



分離ネットワークへ
データ受け渡し
安全に持ち込み

専用端末（通常のPCに
MetaDefender KIOSKアプリケーションをインストール）

多層防御でUSBを安全化（ファイル無害化を適用）



マルウェア
スキャン

30以上のAVエンジンで
マルチスキャン



無害化
(Deep CDR)

ファイルを無害化し、
脅威を除去



未知の脅威検知
(AI解析)

AIが未知の脅威を
振る舞い検知



利用ログ取得
・記録

操作ログを取得し、
追跡・監査が可能

✓ 分離ネットワークへのデータ受け渡しにおけるUSBの安全な運用を支援！

なぜOPSWAT MetaDefender KIOSKがベストなのか



✓ ファイル無害化をUSBにも適用可能

USBメモリ内のファイルを無害化(Deep CDR)してから利用。マルウェアや未知の脅威を除去し、安全な状態で持ち込みが可能です。



✓ Bad USBなどのハードウェア脅威にも対応

キーボードエミュレーション等を行うBad USBを検知。ハードウェアレベルでの不正操作や情報窃取を防止します。



✓ 運用が簡単・負担を軽減

アプリケーションのみの提供で、導入が容易。専用端末は不要で、職員の負担を増やさず、確実なセキュリティを実現します。



捜査・業務の安全性と効率性を両立し、
都道府県警のセキュリティ強化に貢献します。



USB対策は、今からが重要です。
この機会に、ぜひご検討ください！



セキュリティ強化
マルウェア感染・情報漏えいを
未然に防止



コンプライアンス対応
ガイドラインに準拠した
安全な運用を実現

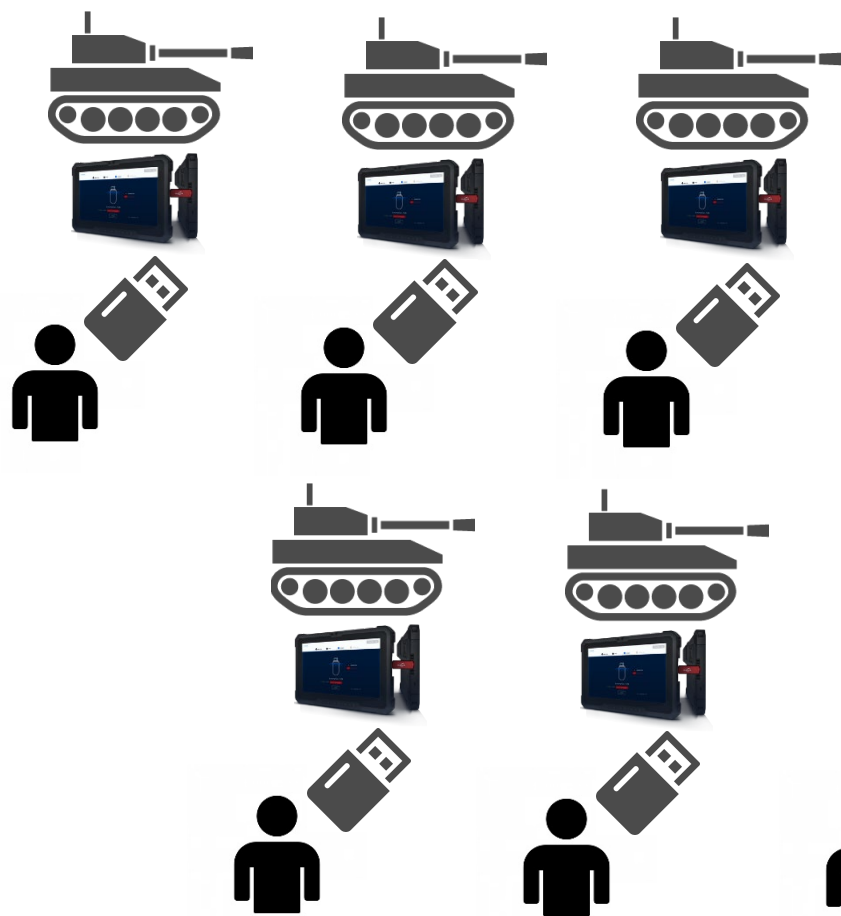


捜査・業務の信頼性確保
証拠の信頼性維持と
業務の安定継続を支援



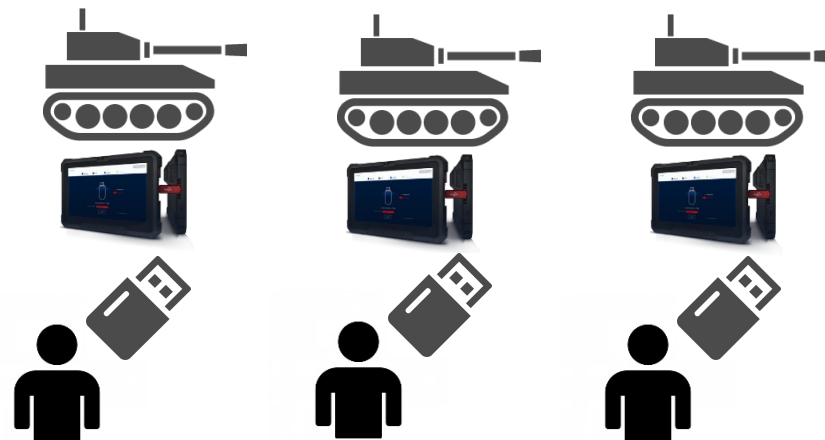
詳しくは担当営業まで
お気軽にご相談ください。

持ち込みUSBへの対応ユースケース（欧州某国軍部）

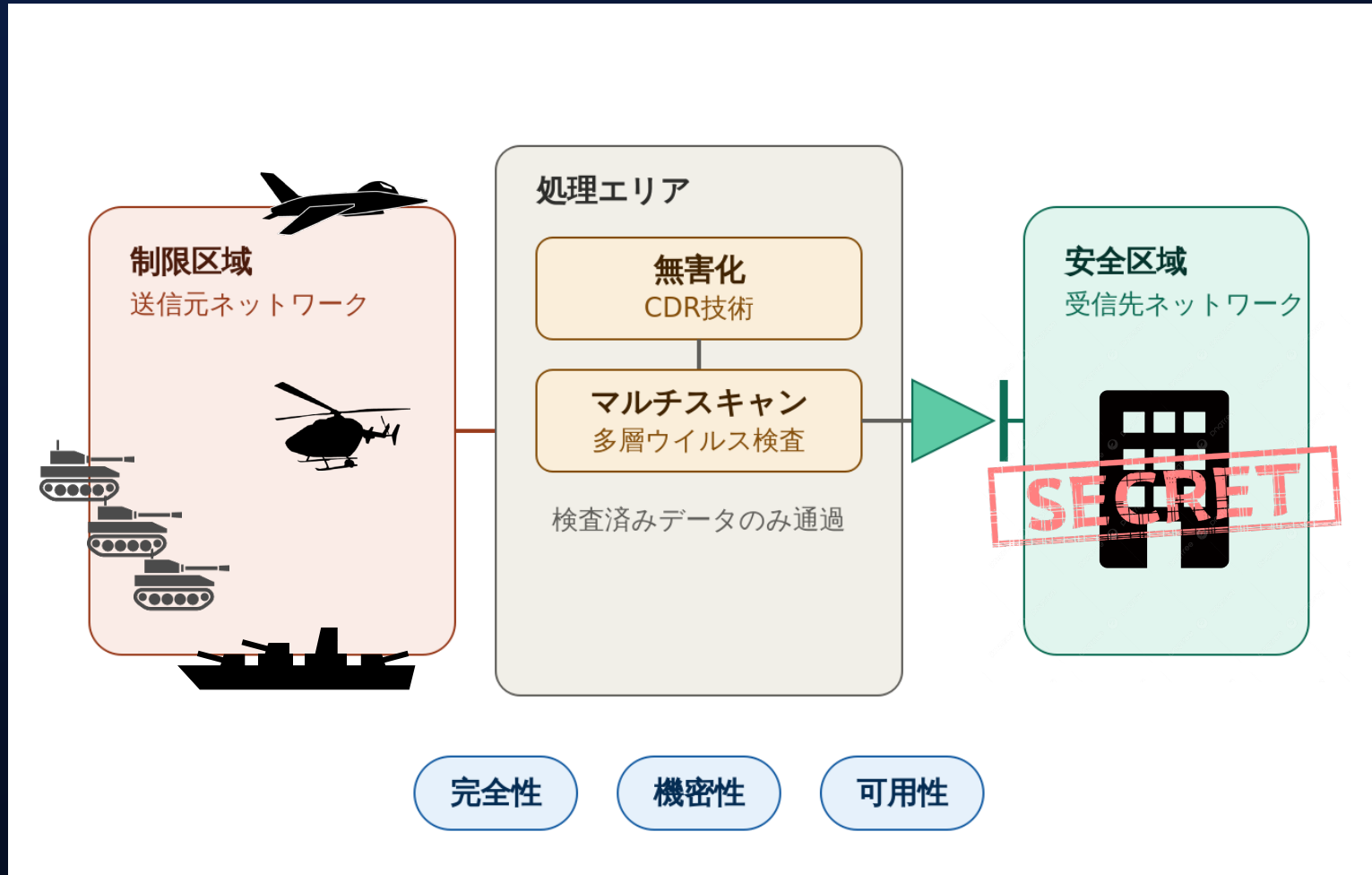


車輛起動時に必要なUSBメモリを
乗車の度にMetaDefender Kiosk
Portableでチェック

どのような場所でもネットワーク
に接続する必要がなく複数のAV
エンジンで処理が可能



欧州国防省・兵站機関（クロスドメインケース）

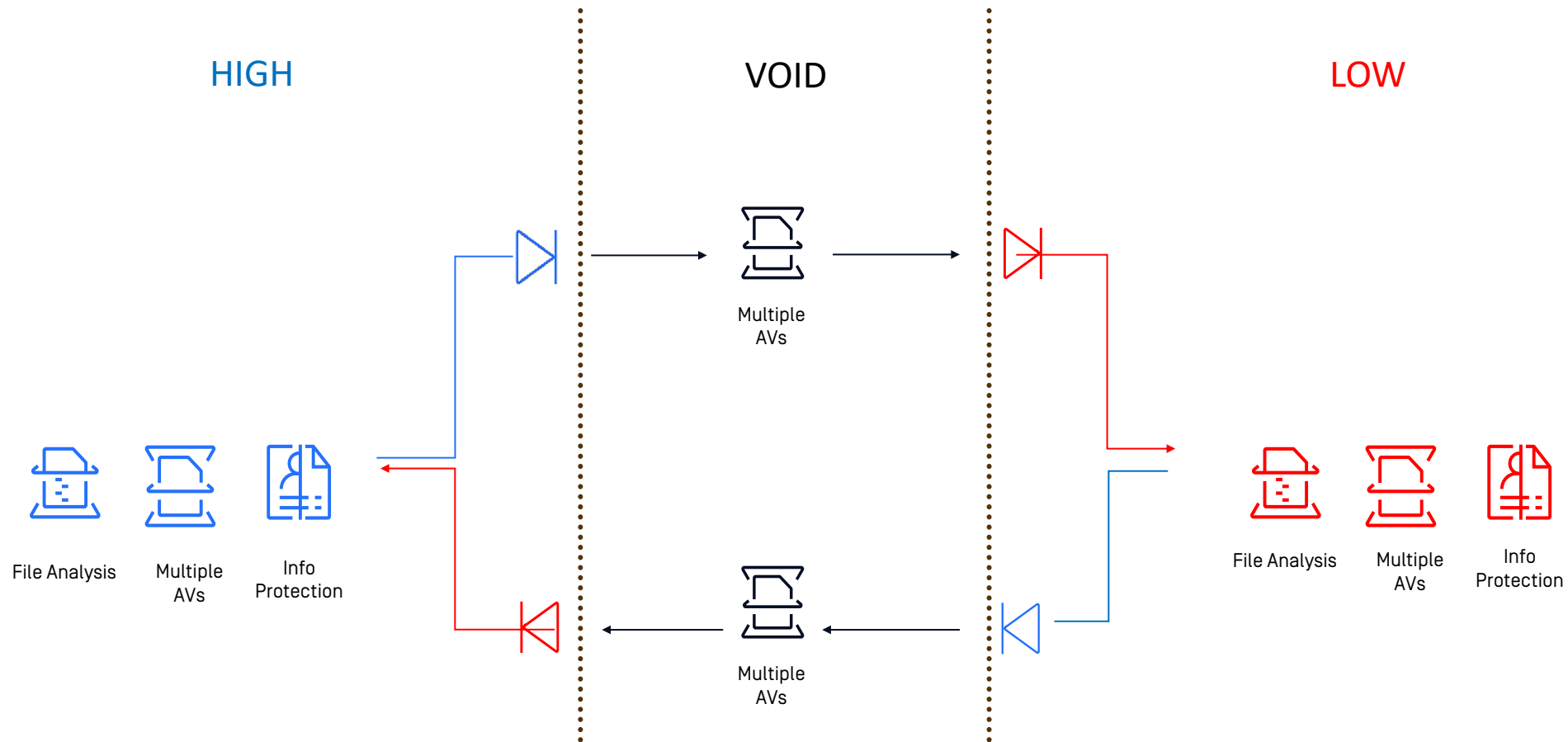


データダイオードとファイルセキュリティ、データ転送の技術を組み合わせ、ドメイン間のデータのやり取りを安全に確実に見守ります。

ダイオードによる物理的な一方向通信により、大切な情報が外に漏れてしまう心配を減らしながら、無害化と、マルチスキャンによる多層的なウイルスチェックを通過した『安心・安全』なデータだけが、ドメインの境界を越えていきます。

データ中心型のセキュリティは、サイバー空間で日々変わり続ける脅威にもしなやかに寄り添えるよう設計され、作戦全体、そして国境を越えた場面でも、ミッションクリティカルなデータの完全性・機密性・可用性を、いつでも変わらず支え続けます。

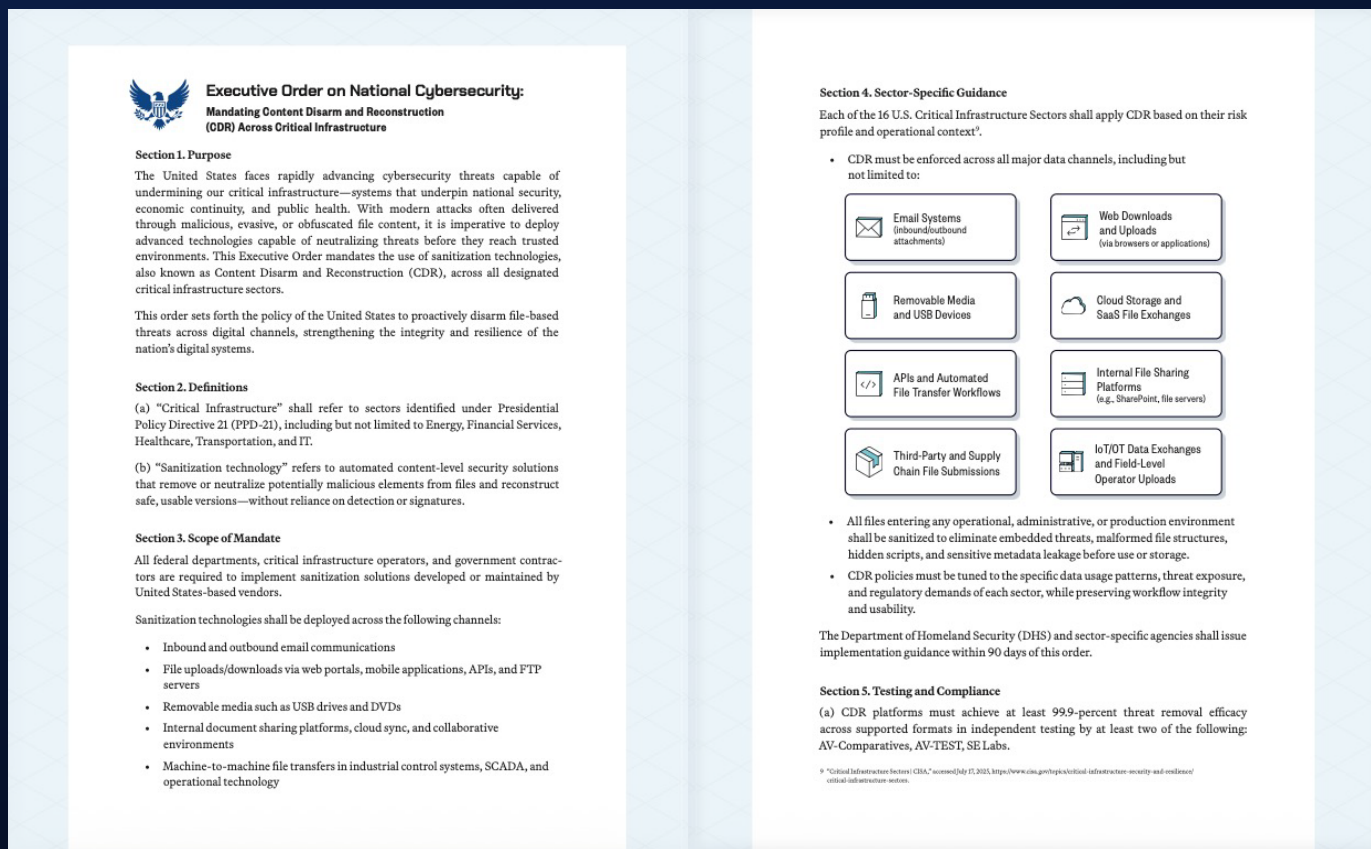
欧州国防省・兵站機関（クロスドメインケース）



本日のご案内

- OPSWAT Inc, 会社概要
- OPSWAT製品概要
- ユースケース
- まとめ

まとめ



OPSWATの技術の背景には、検知という手法が持つ構造的な上限という発見があります。その先にたどり着いたのが、悪いものを見つけて止めるのではなく、最初から安全なものを作るという発想でした。検知に頼らず対応も防御もいらない、ただ純粋な予防。これこそが、私たちが皆様に提供したいと考えている価値の核心です。OPSWATは、いずれこの考え方が一企業の技術にとどまらず、国の重要インフラを守る標準になってほしいと思い、米国の大統領令の草案まで考案しています。

OPSWAT.

ありがとうございました

本資料へのお問い合わせ、ご連絡はこちら

OPSWAT JAPAN 株式会社
防衛省様担当：野田 芳裕 (Yoshihiro Noda)
yoshihiro.noda@opswat.com
070-1580-6718