OPSWAT.

MetaDefender® for Secure Storage

Secure Your Storage

クラウドストレージソリューションは、アクセス性、共有、共同作業を容易にする一方で IT 部門とセキュリティ部門にとっては、マルウェアや機密データ損失の盲点になっています。これは重大なセキュリティホールで、2020年のレポートでは、80%の企業がクラウドデータ侵害を経験しています。

MetaDefender for Secure Storage は、企業・組織のデータとして保存されたファイルや画像などを保護するための堅牢な保護レイヤーを提供します。クラウドやオンプレミスストレージでのデータ侵害、ダウンタイム、コンプライアンス違反の防止に役立ちます。

分析・是正・レポート

組織ユーザーのファイルは、マルウェア検査、潜在的なデータ損失や未承諾のプライバシーデータを分析します。疑わしいファイルは無害化し、ファイル内の機密データは自動的にレポートし秘匿化することができます。

多くのクラウドストレージサービスとのネイティブ統合により、容易なソリューション導入が可能です。実用的な自動監査レポートにより、ITプロフェッショナルはユーザーとサービスに関連する脅威とリスクを特定し、迅速な是正処理を実現します。

MetaDefender for Secure Storage により、組織内で安心してデータを共有できます。

利点

ゼロデイ攻撃防止

未知のコンテンツを非武装化し、ユーザビリティを維持した安全なファイルを出力。OPSWAT Deep CDR 技術は、攻撃発生前の防御に注力。100 種類以上のファイルタイプから、潜伏または未知のマルウェアを無害化

高度な脅威検知

最大 30 種類以上のマルウェア対策エンジン（Mcafee, ESET, Avira, K7, Crowdstrike, TrendMicro, Sophos 等）の検知メカニズム（シグネチャ、ヒューリスティック、AI / 次世代アンチウイルス）を組み合わせたマルチスキャンによる高度な脅威検知を実現

コンプライアンスリスクの軽減

機密データの検出、秘匿化、ブロック。OPSWAT Proactive DLP 技術の機密データ損失自動レポートと是正処理により HIPAA, PCI-DSS, GDPR などの規制要件に対応

広範囲な統合

Microsoft OneDrive, Azure, Amazon S3, Box, Cloudian, Dell Isilon, SMB 互換、S3 互換ストレージ等 とのシームレスな統合により、迅速な健全性検査が可能

OPSWAT.

MetaDefender for Secure Storage

特徴

規模に応じた処理

ワンクリックで、ストレージ全体、新規ファイル、または特定ファイルのいずれかを選択

自動レポート

クラウドストレージのステータスは、関係者に送信する自動レポートで容易に把握。包括的なダッシュボードでリアルタイムに確認することも可能

柔軟なスケジューリング

組織のニーズに合ったリアルタイム処理とスケジューリングオプションの組み合わせにより、ゼロデイ攻撃や高度な標的型脅威からストレージを保護

完全な監査性

ユーザー操作履歴は監視しログに記録。企業監査対応のために容易にエクスポート可能

自動ワークフロー

複数の管理者に役割ベース(「読み取り専用」を含む)のアクセス権を付与することで、IT部門がコンプライアンスとデータ侵害のリスクを効果的に管理

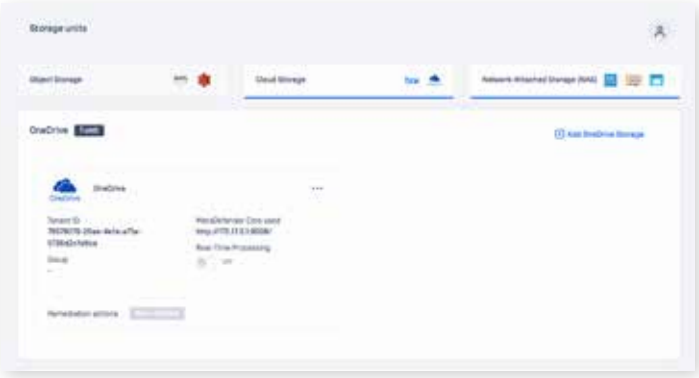
ユーザー管理

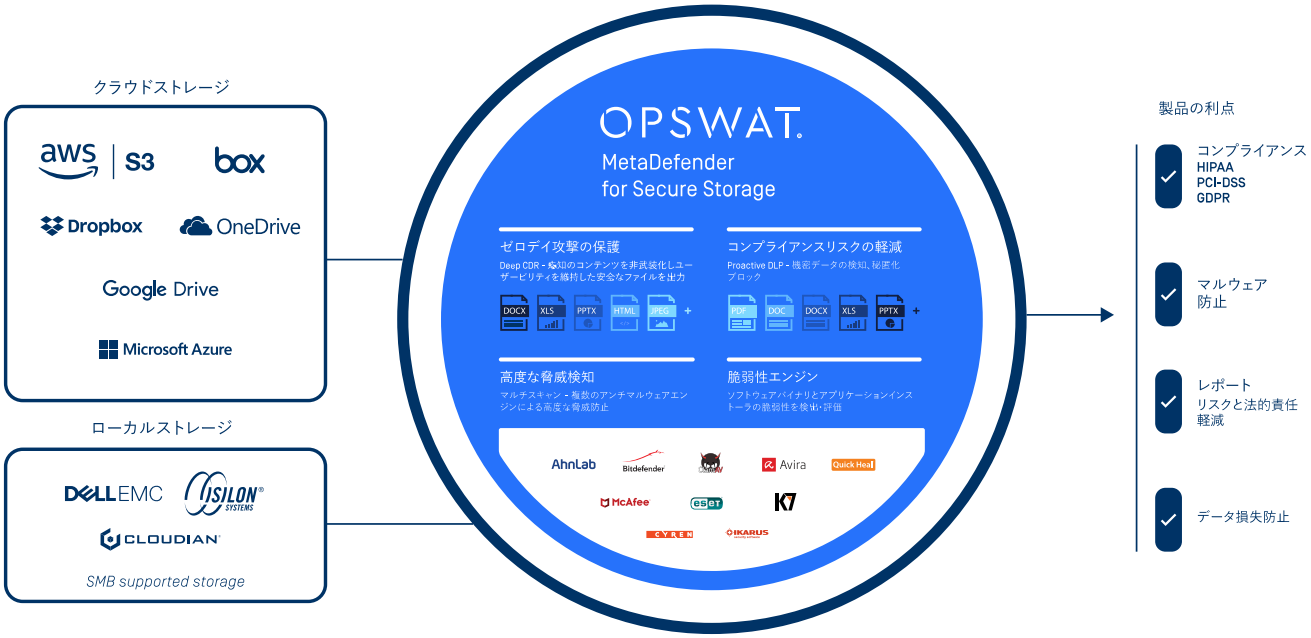
複数の管理者に役割ベース(「読み取り専用」を含む)のアクセス権を付与することで、IT部門がコンプライアンスとデータ侵害のリスクを効果的に管理

統合 (Amazon S3, Dell 等)

複数ベンダー(クラウドまたはオンプレミス)のストレージユニットを迅速にセットアップ・構成し、単一ビューで管理・保護します。ネイティブな API 統合によりオーバーヘッドを最小限に抑えます。

- Amazon S3 インスタンス または S3 互換のストレージと統合
- Microsoft OneDrive, Azure Files, Azure Blob ストレージに保存されているデータを保護
- Dell Isilon または、SMB 互換のオンプレストレージユニットをシームレスに統合
- Box 等のコラボレーションソリューションのストレージユニットの容易な設定





* 対応ストレージの最新情報は以下のサイトをご参照ください
https://docs.opswat.com/mdss/integrations

OPSWAT.

MetaDefender for
Secure Storage

コンプライアンスリスクの低減

規制要件による顧客機密データのプライバシーとセキュリティの義務付け

- OPSWAT は、不注意による公開や、悪意の標的にされる可能性のある機密データをチェックします。役割ベースのNeed to knowアクセス（「読み取り専用」を含む）により、データプライバシー法の違反を最小限に抑えます。当社製品は誤用を警告し、ユーザーによる不審または不注意な活動を可視化します。仮に、この活動が検出されなかった場合、組織が危険にさらされ、莫大な規制上の罰金と社会的信用の喪失につながる可能性があります。
- OPSWAT の高度なテクノロジーパッケージ製品。業界をリードする30種類以上のアンチウイルスエンジンによるマルチスキャン、Deep CDR（コンテンツの非武装化と再構築）によるファイルの無害化、機密データを検出してブロックするプロアクティブ DLP（データ損失防止）など。規定された規制要件の遵守に役立ちます。

OPSWAT が保護するデータの種類

- **PCI DSS（Payment Card Industry Data Security Standard）** ガイドラインの遵守:
  - **クレジットカード番号**

違反のリスク

PCIコンプライアンスブログ（www.pcicomplianceguide.org/faq/#15）による違反の罰則:
決済ブランドは、PCIコンプライアンス違反に対して、自らの判断でアクワイアラバンクに月額5,000～100,000ドルの罰金を科すことができます。おそらくバンクは、この罰金を最終的に業者まで伝えるでしょう。

さらに、銀行はおそらく関係を終了するか、取引手数料を増やすでしょう。ペナルティは公然と議論されることも広く公表されることもありませんが、中小企業にとって致命的な場合があります。

- **GDPR（一般データ保護規則）** の遵守:
  - **データ主体の個人情報（PII）**
    - Eメール
    - 生年月日
    - 電話番号
    - パスポート番号

違反のリスク

GDPRに準拠していない場合の2段階の行政罰金:

- 最大1,000万ユーロ、または事業の場合は年間の世界の売上高の2%-どちらか大きい方
- 最大2,000万ユーロ、または事業の場合は年間の世界の売上高の4%-どちらか大きい方

GDPR違反に対する罰金は、必須ではなく裁量です。それらはケースバイケースで課せられなければならず、「実効性、バランス、抑止力がある」べきです。

ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

- **HIPAA（Health Insurance Portability and Accountability Act）** 違反を防止:
  - **社会保障番号**
  - **生年月日**
  - **電話番号**
  - **住所**

違反のリスク

違反に対するペナルティは過失のレベルに基づいており、違反ごと（またはレコードごと）に$ 100から$ 50,000の範囲であり、同一の規定の違反に対して年間最大150万ドルのペナルティがあります。また、違反は刑務所に入る可能性のある刑事責任を負う可能性があります。

www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

OPSWAT.

Trust no file. Trust no device.