

DLP機能の比較

デモを依頼

従来ベンダー ← → DLPに一部対応したベンダー

幅広いデータ保護機能	FORCEPOINT	TRELLIX (MCAfee)	SYMANTEC	ZSCALER	NETSKOPE	PROOFPOINT	MICROSOFT
ワンクリックによる修復	●						
スクリプトによってエンドポイントやポリシーエンジンでの修復を拡張	●	○	●	○			
標準で1700以上のデータ分類子が提供されており、エンドポイント、ネットワーク、クラウド、Webなどのあらゆる出口チャンネルに対して適用	●	○	○	○	○	○	○
リムーバブルメディアに移動するファイルの暗号化	●	○	○				○
SaaSクラウドアプリケーション (API/インライン) の統合DLPポリシーの施行	●	○	○	○	○	○	○
エンドポイントの検出と実行にネットワーク接続の必要なし	●	○		○	○	○	○
メールのデータを完全に保護 (MSFT、Google、モバイル、エージェントレスなど)	●	●	○	○	○	●	○
900以上のファイルタイプのための高度なツールファイル検出	●	○	○	○	●	○	○
重要なクラウド環境とオンプレミス環境でのデータ検出	●	●	●			○	○
300以上の定義済みの自然言語処理スクリプトで、共通データを正確に識別 (PCI、PHI、PCI など)	●	○	○	○	○	○	○
クラウドアプリ保護:リアルタイムインラインとAPI	●	●	●	●	●	●	○

従来のベンダー

FDLPに一部対応したベンダー

データ保護対象の統合	FORCEPOINT	TRELLIX (MCAFFEE)	SYMANTEC	ZSCALER	NETSKOPE	PROOFPOINT	MICROSOFT
移動中のデータ、保存データ、使用中のデータに対応する一貫したDLPエンジン	●	●	●	○	○	○	○
フレキシブルなデプロイ: クラウド、ハイブリッド、オンプレミス	●	●	●	○		○	●
Web、メール、クラウド、エンドポイント、出口チャンネル全体にわたる単一のDLPポリシーの適用	●	●	○	○	●		
すべてのチャンネルで単一のインシデントアラートUI	●	●		○	●	○	
リスク適応型保護 (UBA)	FORCEPOINT	TRELLIX (MCAFFEE)	SYMANTEC	ZSCALER	NETSKOPE	PROOFPOINT	MICROSOFT
ネイティブエンドポイントユーザーの行動分析	●	○		○	○	●	
130以上の行動指標 (IOB) に基づくリスク分析	●						
リスクベースの統合データ保護行動計画の実施 (文脈とコンテンツベース)	●						○
リアルタイムで調整可能な分析	●			●	●		
統合とエコシステム	FORCEPOINT	TRELLIX (MCAFFEE)	SYMANTEC	ZSCALER	NETSKOPE	PROOFPOINT	MICROSOFT
Exchange PSTファイル (メールボックス)、保存データをスキャン	●	●	●				●
エンドポイントプロビジョニングによるクラウドネイティブデプロイ	●			○	○	○	○
CrowdStrikeとBitDefenderマルウェアスキャン	●	○	○	●	○	○	○
あらゆる分類ソリューションベンダーとの互換性	●	○	○	○	○		
レガシーオンプレミスファイルとデータストレージ (構造化および非構造化) をスキャン	●	●	●				○

免責事項: 製品の比較は、2024年4月1日時点で同じベンダーが提供する製品内機能とクロスポートフォリオ統合に基づいたものです。第三者ベンダーとの統合は含まれません。機能の比較は、2024年4月1日時点で各ベンダーが提供する最新バージョンに基づいています。情報は、2024年4月1日時点で公開されているウェブサイトやフォーラム、アナリストレポート、製品データシートから収集されたデータに基づいたものです。