

Data Loss Prevention 14.5 の新機能

新機能を活用すると、機密データの安全性をさらに強化できます。

データシート: Data Loss Prevention

Symantec Data Loss Prevention 14.5 は、業界をリードする情報漏えい防止技術を利用した情報保護機能によって、機密データに対する優れた可視性と制御を実現します。

Data Loss Prevention 14.5 には以下の機能が搭載されています。

- **高度なデータ検出** – さまざまな種類のドキュメントや経路から、個人を特定する情報や知的財産を検出できます。
- **クラウドディスカバリの強化** – Box 上で保存され、共有されている機密文書のファイルを保護できるようになりました。
- **より強力なエンドポイント監視** – Mac および Windows で使用されている機密データの制御機能が強化されました。
- **暗号化通信の可視性の向上** – Web トラフィックの暗号化によって生じるセキュリティ上の盲点を見つけて解消できます。

フォーム形式の機密データの保護

企業は、スキャナや携帯電話から取り込んだ文書の画像化を利用したビジネスプロセスのデジタル化に、ますます力を入れています。文書のデジタル化によってお客様やパートナーとの情報のやり取りは簡単になりますが、機密データの追跡や制御が難しくなることも事実です。特に、スキャナによって取り込まれた文書には、個人の身元を特定する情報 (PII) が数多く含まれていることが少なくありません。

Symantec **DLP Form Recognition** を使用すると、納税申告書、保険金請求、患者情報など、PII が含まれている可能性のある画像の手書き文字や入力した文字のデータを保護できます。DLP Form Recognition は、高度な画像処理を実行し、従来の方法では検出が困難な、スキャンや撮影されたフォームの機密データを検出して、その漏えいを阻止する新しいコンテンツ検出技術です。

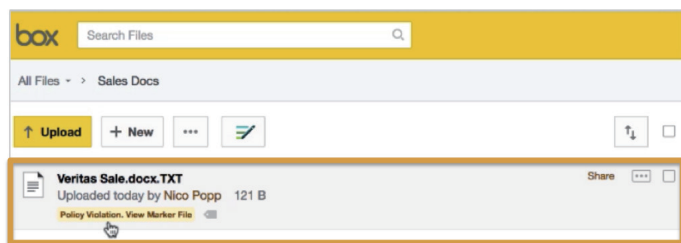
現在 DLP をお使いであれば、ライセンスの購入で簡単に Form Recognition を追加できます。本製品は、Network Monitor、Network Prevent for Email、Network Prevent for Web、Network Discover、Network Protect で利用できます。

クラウド内の機密データの保護

Symantec DLP Endpoint Agent for Windows、DLP Cloud Storage、および DLP Cloud Service for Email によって、Box、Gmail、Microsoft Office 365 などのクラウドアプリを従業員が自由かつ安全に利用できるようになります。

DLP Endpoint Agent for Windows は、Box Sync や Box for Office といったアプリケーションを使用した Box へのファイルアップロードの際に、監視とブロックの新機能を提供します。この新機能では、会社が許可した Box には Box Sync によってすべての種類のファイルをアップロードできますが、許可されていない個人の Box アカウントにはアップロードできません。

DLP Cloud Storage は、ユーザーが Box 上で保管および共有している機密データを追跡し、権限のないユーザーにもオープンアクセスが与えられるような共有リンクの使用など、リスクの高い行為を識別します。DLP Cloud Storage の新しいファイル検疫機能では、ユーザーがポリシーに違反すると、Box 上にある保護された検疫フォルダに不適切に置かれたファイルとフォルダを自動的に移動して、元のファイルがあった場所にマーカーファイルを残すことによってユーザーに通知します。これにより、保護されていないファイルを保護するだけでなく、ファイルに視覚的にタグ付けすることで、機密ファイルやフォルダを自分で修正するようにユーザーに注意喚起することができます。



DLP Cloud Service for Email は、従来のオンプレミスメールアプリケーション、パブリック/プライベートクラウドメールサービス、オンプレミス環境とクラウド環境のハイブリッドミックスなど、そのホスト環境を問わず、企業のメールを監視して保護します。クラウドを利用したこの検出サービスは、Gmail、Microsoft Office 365 Exchange Online に加え、Microsoft Exchange Server とも緊密に統合でき、既存の DLP Enforce Server と簡単に連携させることができます。

エンドポイントでの安全なデータ利用

従業員はネットワーク接続時も非接続時も、無数の危険に直面しています。DLP Endpoint Agent for Mac OS を利用すると、リムーバブルストレージへのダウンロード、文書内でのコピーアンドペースト、Web を介した送信など、さまざまな場面でデータを保護できます。データ漏えいを事前に防ぐために、機密データの共有によく使われるアプリケーション、

ファイルタイプ、オペレーティングシステムのサポートが新たに追加されました。

- Mac OS 10.11
- Microsoft Office 2016 のファイルタイプ
- Microsoft Outlook 2011 メールクライアント
- Chrome、Firefox、Safari の各ブラウザ（HTTP と HTTPS に対応）
- ネットワーク共有へのコピー
- クリップボードからの貼り付け
- Skype インスタントメッセージクライアント

DLP Endpoint Agent for Windows には Mac Agent と同じ強力な機能が数多く含まれていますが、以下のアプリケーションやファイルタイプのデータも保護できるようになりました。

- Microsoft Office 2016 のファイルタイプ
- Box for Office および Box Sync アプリケーション
- Cisco Jabber および Skype for Business のインスタントメッセージングクライアント

各環境にわたるポリシーを簡単に管理

開発環境やテスト環境から本番環境に移行するなど、異なる環境間で情報漏えいポリシーを移行する場合、プロセスをシンプルにして自動化することで、ミスを減らして時間を節約できます。ポリシーのインポートとエクスポートを可能にする機能により、DLP Enforce Server のインスタンス間でポリシーを簡単に移行できます。ポリシーはポリシーグループや応答ルールといったポリシーのすべての詳細を含むファイルにエクスポートされ、インポートの際にエラーが発生することはありません。

部分的にコピーされた文書のエンドポイントでの保護

機密文書の情報は、各種ファイルやアプリケーションで従業員によって無造作に切り取られ、コピーして貼り付けられたりします。しかし、これらの情報には許可されていないものや安全に使用できないものが含まれている場合があります。Symantec DLP を使用すると、Endpoint Indexed Document Matching という強力なデータフィンガープリント機能がこのような情報の断片を簡単に特定します。この機能では、機密データを元の文書だけでなく、二次著作物の中からも検出できます。Endpoint Indexed Document Matching は、非構造化データ（簡単にデータベース化できない情報）をモバイルやリモートから従業員が日常的に使用するような企業で特に役立ちます。

Web 通信の管理の強化

多くの企業は、顧客、パートナー、および契約業者との通信にいくつかの主要な Web プロトコル (HTTPS、HTTP、FTP) を利用しています。しかし従業員がこのような暗号化チャネルや暗号化されていないチャネルで機密データを送信した場合、IT に盲点と脆弱性が生じます。DLP 14.5 では、以下の Web ゲートウェイやクラウドプロキシと DLP Network Prevent for Web を統合できる新機能により、HTTPS、HTTP、FTP で高度な Web 監視と保護が可能になりました。

- A10 ネットワークスのアプリケーションデリバリーコントローラ、SSL インサイト、Thunder Convergent Firewall
- Zscaler Web セキュリティサービス

暗号化通信の可視性の向上

世界のインターネットトラフィックはますます暗号化されつつあり、暗号化された通信プロトコルで会社から漏えいしている機密データを確認することは一層難しくなっています。DLP では、暗号化されたトラフィックを安全なネットワークの外に出る前に検査して、これらのデータを再び制御することができます。業界をリードする SSL 復号アプリケーションと緊密に統合することで、DLP は復号されたトラフィックを分析し、ユーザーによる機密データの投稿や送信を防ぐことができます。DLP 14.5 では、SSL 復号製品と DLP Network Monitor を統合することで、Web、メール、FTP、および IM 通信用の新しい SSL 監視機能が利用可能になります。

- Blue Coat SSL Visibility
- Palo Alto Networks の次世代ファイアウォール

