Symantec Data Loss Prevention for Cloud

クラウドのデータを検出/監視/保護

データシート: Data Loss Prevention

多くの企業にとって、アプリケーションをオンプレミスからクラウドに移行するのは、俊敏性を強化してコストを削減する有効な手段となります。そこで問題となるのは、クラウドに移行した後でも機密情報に対する可視性と制御を保持するには、どうするかということです。

Symantec Data Loss Prevention（DLP）for Cloud Storage と Cloud Prevent for Microsoft Office 365 は、クラウドベースのストレージと電子メールに適した強力な検出/監視/保護機能を提供することでこの問題を解決します。

- **Symantec DLP for Cloud Storage** を導入すれば、共同作業における安全性を確保できます。また、ビジネスユーザーが Box に保存して共有する機密ファイルをすべて詳細に可視化できます。
- **Symantec DLP Cloud Prevent for Microsoft Office 365** は Office 365（Exchange Online）とシームレスに連携するので、電子メールをクラウドに確実に移行できます。また、ビジネスユーザーが送信する機密情報を含んだ電子メールを詳細に可視化して制御できます。

Symantec DLP 製品はすべて、統合管理コンソールと強力なレポートツールを搭載しています。データ漏えい防止ポリシーの集中管理、インシデントの修復、DLP の価値測定などが簡単に実行できます。

Cloud Storage

DLP for Cloud Storage は強力なコンテンツ検出機能を提供しているので、Box の Business アカウントと Enterprise アカウントを簡単にスキャンできます。また、保存された機密データの内容、使用状況、共有者を詳細に可視化できます。DLP for Cloud Storage では Box のファイルにビジュアルタグが付けられ、ポータルである Symantec DLP Self-Service Portal からは直感的な操作でインシデントの修復が可能なので、ユーザーはポリシー違反を自分で修復することもできます。

主な機能

- 記述、フィンガープリント、学習などの先進的なコンテンツ認識型検出テクノロジにより、Box ファイルの使用をきめ細かく制御します。
- ユーザーが Box や DLP Self-Service Portal から自力で修復できます。
- クラウドのデータ漏えい防止ポリシーの管理が簡単で、インシデントを自動的に修復します。直感的に使用できる管理コンソール（Symantec DLP Enforce）からすべての操作が可能です。

Cloud Prevent

DLP Cloud Prevent for Office 365 には Exchange Online 向けの強力なコンテンツ監視機能と保護機能が搭載されているため、クラウド電子メールの導入を推進できます。Cloud Prevent を導入すれば、企業の機密情報を検出するとともに、ユーザーにポリシー違反を通知したり、安全な送受信を行えるように電子メールを暗号化ゲートウェイにリダイレクトしたり、重要データの漏えい防止のために電子メールをリアルタイムでブロックしたりするなど、適切なタイミングで適切な対策をとることができます。Cloud Prevent によって、オンプレミスの導入や Rackspace 社がホスティングする環境への導入を柔軟に行えるようになります。

主な機能

- 記述、フィンガープリント、学習などの先進的なコンテンツ認識型検出テクノロジでクラウド電子メールの使用をきめ細かく制御します。
- 最終的に電子メールを送信する Symantec Email Security.cloud サービスとシームレスに統合されています。
- クラウドのデータ漏えい防止ポリシーの管理が簡単で、インシデントを自動的に修復します。直感的に使用できる管理コンソール（Symantec DLP Enforce Platform）からすべての操作が可能です。

一元化された管理とレポート機能

多種多様なデバイスやストレージ環境にデータの分散が進むにつれて、ポリシーを一貫して定義し適用することがますます重要になっています。Symantec DLP は、統合管理コンソールである DLP Enforce Platform、ポリシーを設定してどの場所にも適用可能とするビジネスインテリジェンスレポートツール IT Analytics for DLP を搭載しており、情報に関わるリスクを大幅に低減できます。**DLP Enforce と IT Analytics** により、次のことが可能です。

- **単一の Web ベースのコンソール**を使用し、すべてのエンドポイント、モバイルデバイス、クラウドベースサービス、オンプレミスネットワーク、ストレージシステムを対象として、データ漏えい防止ポリシーの定義、インシデントのレビューと修復、システム管理を実行できます。
- **60 種類を超える事前構築済みのポリシーテンプレート**と便利な**ポリシービルダー**を活用して、DLP ソリューションの効果をすぐに発揮できます。
- 強力な**ワークフロー機能と修復機能**を活用して、インシデント対応プロセスの合理化と自動化を進めることができます。
- 高度なレポート機能とアドホック分析機能を提供する**先進的な分析ツール**によって、**ビジネスインテリジェンス**をお客様の DLP への取り組みに適用できます。システムデータを多次元キューブに抽出して集約する機能を利用すると、さまざまな利害関係者に向けてレポート、ダッシュボード、スコアカードを作成可能です。

DLP Enforce を使用すれば、情報に対して一貫したポリシーを適用して安全に保護することができます。

情報保護に今すぐ着手

シマンテックは、セキュリティとコンプライアンスポリシーをファイアウォールの外側にまで拡張して情報を徹底的かつ効果的に検出/監視/保護できるように、いつでもお手伝いいたします。実証済みの導入アプローチや直感的に操作できるポリシー/インシデント管理ツールを提供し、リスクの高い経路すべてを包括的にカバーするので、総所有コストは最小となります。

詳しくは www.symantec.com/ja/jp/data-leak-prevention/ にて、最新のモバイル化されたクラウド中心の環境に対応した包括的な情報保護ソリューションのメリットをご覧ください。

システム要件

Symantec DLP for Cloud Storage と Cloud Prevent for Office 365 は、1 つの統合管理プラットフォームと複数のコンテンツ認識型検出サーバーで構成されています。オンプレミス、ハイブリッドクラウド、マネージドサービス（Symantec DLP スペシャリゼーションパートナーが提供）など、柔軟な導入オプションをご用意しています。Symantec DLP は、分散が進んだ環境での利用や、何十万ものユーザーやデバイスが存在する環境への拡張が実証されています。この点で、他社のソリューションとは異なっています。

オペレーティングシステム	Microsoft Windows Server 2008、Microsoft Windows Server 2012 Red Hat Enterprise Linux VMware ESX および VMware ESXi
プロセッサ	3.0 GHz CPU 2 基
メモリ	6 GB ～ 8 GB
ストレージ	140 GB
ネットワーク	1 Gbps/100 Mbps イーサネット NIC（銅線または光ファイバー）1 枚
データベース	Oracle 11g Standard Edition

詳細情報

シマンテックの Web サイト

http://www.symantec.com/ja/jp/data-leak-prevention/

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec と Symantec ロゴは、Symantec Corporation またはその関連会社の米国およびその他の国における登録商標です。その他の会社名、製品名は各社の登録商標または商標です。製品の仕様と価格は、都合により予告なしに変更することがあります。本カタログの記載内容は、2015 年 6 月現在のものです。

株式会社シマンテック

〒107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ

www.symantec.com/jp

お問い合わせ

E1506DS0-IN-21350066