データシート

デバイスからクラウドまでを網羅する McAfee の DLP

統合されたデータ保護

規模の大小を問わず、Microsoft Office 365 などのクラウドベースのサービスを採用する企業が増えています。クラウド サービスを利用することで、仕事で使うコア アプリケーションに社外から簡単にアクセスできるようになります。しかし、このようなクラウド サービスのデータをオンプレミスのデータ保護ソリューションで可視化し、クラウド上で行われている共同作業や共有を制御することはできません。クラウド環境を保護するために別のソリューションの追加を検討している企業も少なくありませんが、その場合、ポリシー管理、レポート、インシデント対応をオンプレミスとクラウドで別々に行わなければなりません。管理作業が煩雑になるだけでなく、デバイス、ネットワーク、クラウド サービスに一貫したデータ保護を行うことも難しくなります。

デバイスからクラウドまでを網羅する McAfee® の DLP は、McAfee® Data Loss Prevention（McAfee DLP）、McAfee® MVISION Cloud という業界最先端の技術を組み合わせ、エンドポイント、ネットワーク、クラウドを保護する統合データ保護ソリューションです。統一されたデータ保護をシームレスに展開できるので、データ損失のリスクを最低限に抑えながら、運用効率を最大限に高めることができます。

データ保護ソリューションの分断

クラウドで使用する DLP を実装する場合、オンプレミス用に作成した DLP ルールをクラウド用に作り直す必要があります。また、オンプレミスの DLP ルールは、クラウド ネイティブの共同作業や共有に対応していません。ルールの再構築に時間がかかるだけではありません。異なる DLP エンジンを使用する結果、矛盾するポリシーが適用される可能性もあります。クラウドの共同作業や共有リンクによるデータ漏洩は、オンプレミスの DLP では検知できません。

オンプレミスとクラウドの DLP を簡単に連携

デバイスからクラウドまでの DLP を実現する上で重要な役割を果たしているのが McAfee® ePolicy Orchestrator®（McAfee ePO ™）です。MVISION Cloud と McAfee ePO を連携することで、クラウドネイティブの共同作業と共有を完全に網羅し、クラウド サービスのデータを以前よりも迅速に保護することができます。2 つのソリューションはワンクリックで接続できます。完了まで 1 分もかかりません [1]。

主な特長

シームレスな統合

- McAfee ePO でデータを分類し、その情報をデバイス、ネットワーク、クラウドに適用
- オンプレミスとクラウドの DLP をワンクリックで簡単に統合

一貫したデータ損失防止機能

- 複数の環境でポリシーと分類エンジンを共有
- 複数のコンソールでの変更は不要

すべてのインシデント管理とレポートを一元管理

- 複数の環境のインシデントを集中管理
- コンソールを切り替えることなく、インシデントとレポートを表示

McAfee とつながる

デバイスやネットワーク用に McAfee ePO で作成した DLP ルールを MVISION Cloud にプッシュし、クラウド サービスに適用できます。また、このルールは、自社のネットワークを経由しないクラウドネイティブのトラフィックにも適用されます。データの分類情報が同期され、エンドポイントとクラウドに一貫したデータ損失防止が実施されます。すべてのインシデントが McAfee ePO に送信されるので、デバイスからクラウドまでの DLP を 1 つのワークフローで管理できます。

デバイスからクラウドまでを網羅する DLP で運用効率を向上

McAfee ePO との統合で、煩雑な作業がなくなり、クラウド サービスに DLP を簡単に適用することができます。ある大手食品サービス会社は、自社のエンドポイントとネットワーク共有ファイルを McAfee DLP で保護しています。クラウドの利用が拡大したため、会社のデータがクラウド上のどこに存在するのかを把握し、その保護戦略を立てる必要が生じました。この会社ではまず、McAfee® Web Gateway で Web トラフィックを分析し、最も多い送信先とクラウド上で会社のデータが最も多く存在する場所を調査しました。その結果、データのほとんどが Microsoft Office 365 に集中していることが判明しました。

データを保護する要件はオンプレミスと変わりませんが、クラウドのデータに対しては、ファイル共有や共同作業など、新しいコンテキストを考慮しなければなりません。オンプレミスと同様に Office 365 のデータをオンデマンドでスキャンし、Office 365 との間で送受信されるデータに DLP ルールを適用する必要があります。しかし、自社でクラウド環境の

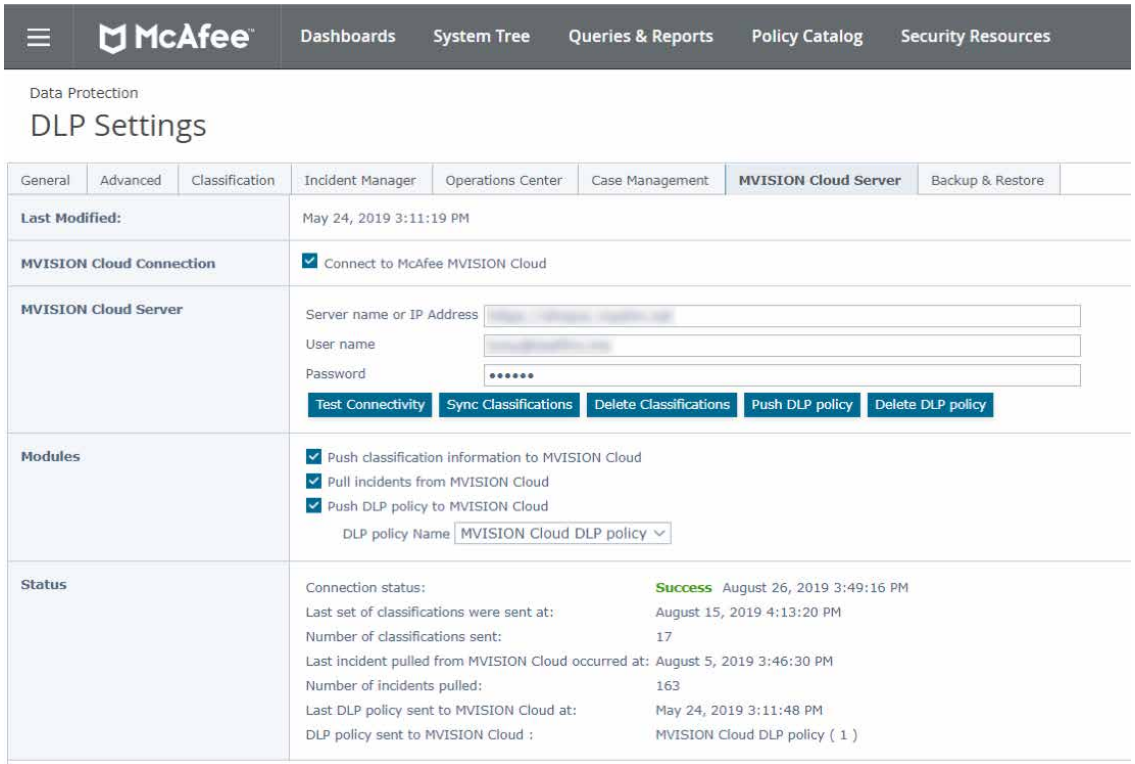

図 1. McAfee ePO で DLP ポリシーを MVISION Cloud と同期

可視化を実現するのは困難です。この要件を満たす最適なソリューションがクラウド アクセス セキュリティ ブローカー（CASB）でした。市場で提供されている複数のサービスを検討しましたが、McAfee ePO との統合で既存の DLP ルールを管理できる MVISION Cloud を採用しました。セキュリ

ティ チームは、オンプレミスのデータ分類情報を McAfee ePO から MVISION Cloud にプッシュし、この情報に基づいて Office 365 用のポリシーを作成しました。現在、この会社ではデータ分類、デバイスからクラウドまでの DLP インシデント、McAfee Web Gateway からの Web トラフィック レポートをすべて McAfee ePO で一元管理しています。

「McAfee MVISION Cloud は、データがどこにあり、誰がアクセスしているのかを簡単に確認でき、クラウド サービスに関連するリスクをすぐに特定できます。この点が CASB として採用する決め手になりました。」

— IoT の世界的メーカーの CISO

インシデント管理とレポートの一元管理

McAfee ePO により、1 つのコンソールですべての DLP 違反を一元管理し、レポートを作成できます。DLP 違反の発生元が社内のデバイスかクラウド アプリケーションかに関係なく、コンソールを切り替えずにインシデントを表示し、レポートを生成できます。この集中管理コンソールで異なる環境の機密データを可視化できるので、監査やコンプライアンス対応の負担を軽減できます。

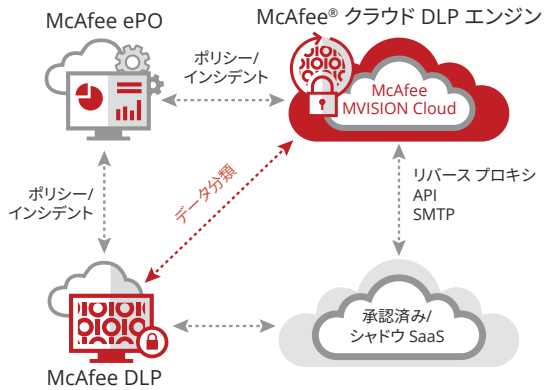

図 2. クラウドからデバイスまでを網羅する McAfee DLP インシデント管理の一般的なアーキテクチャ

まとめ

クラウドで作成され、送受信されるデータは増加しています。社内のエンドポイント、管理対象外のデバイス、ネットワーク、クラウド アプリケーションなど、データの流出経路も増えています。このようなデータを保護するには一貫した DLP ポリシーの実装が欠かせません。

デバイスからクラウドまでを網羅する McAfee の DLP では、統合されたデータ保護を複数の環境でシームレスに展開できます。効率的な運用を実施し、データ漏えいのリスクを最小限に抑えることができます。

詳細情報

詳細は、**mcafee.com/dataprotection** をご覧ください。

1. McAfee 社内ラボでのテスト結果に基づく

〒 150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティ ウエスト 20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp