ソリューション概要

組織からのデータ流出を阻止する

多くの組織からデータが流出しています。内部の人間から情報が漏れることもありますが、大半は外部からの攻撃で盗まれています。流出の方法や経路は1つではありません。多くの組織が情報の漏えいを阻止しようとしていますが、その理由は様々で、対策の成功度にも差があります。Intel Securityでは、このような情報窃盗に関与している人物、盗まれるデータの種類、外部への送信方法などを詳しく分析するため、『Intel Security 2016 Data Protection Benchmark Study』（2016年データ保護ベンチマーク調査）を実施しました。

『McAfee Labs脅威レポート: 2016年9月』では、この調査データの詳しい分析結果が報告されています。主な発見は次のとおりです。

- データの流出から侵害検出までにかかる時間が長くなっている
- 医療機関や製造業が標的になっている
- 現在狙われている標的に対して、従来のデータ損失防止は効力を失っている
- データの流出で2番目に多い手法に対して大半の組織は警戒していない
- データ損失防止対策は正当な理由で実装されている
- 可視化が重要である

有効なデータ損失防止を行うための推奨ポリシーと手順

故意か不注意かを問わず、重要なデータの流出を防ぐには、データ損失防止のポリシーと手順を作成することが重要です。データ損失防止対策に成功するには、ビジネス要件を定義する段階で対策を計画する必要があります。たとえば、プライバシー ポリシーやデータ共有の基準を定義するときに、データ分類とデータ漏えい対策のポリシーを組み込みます。明確なビジネス要件を設定することで、データ損失対策の活動を混乱なく推進することができます。

intel Security

次に重要な点は、組織内で重要なデータを識別することです。サーバーやエンドポイントのスキャン技術を使用すると、正規表現、辞書、非構造化データなどに基づいてファイルを分類できます。多くのデータ損失防止対策製品には、クレジットカード情報や医療情報などの標準的なデータを分類し、検出プロセスを加速化する機能が搭載されています。このような分類機能をカスタマイズすることで、組織固有のデータ タイプも識別できます。

IT部門が認定していないアプリケーションの利用や、クラウドへのデータ保管により、問題はさらに複雑になっています。IT部門が承認したデータをクラウドに保管する場合、クラウド サービス購入時のプロセスで重要なデータを識別できます。この場合、重要なデータの分類は比較的簡単になります。

しかし、組織内のグループが事業目標を達成するため、IT部門の承認を得ずに独自にクラウド サービスを購入することも少なくありません。IT部門がこのようなサービスやデータに気づかなければ、データ流出の可能性は増大します。組織内のグループが協力してクラウド上でのデータの存在場所を特定し、このようなデータを事前に分類しておくことが重要です。

重要データの検出プロセスを完了した後で、信頼されたネットワーク内とすべてのエンドポイントにデータ損失防止製品を導入することで、データの可視化を実現し、保存中や移動中のデータを制御することができます。ポリシーは、重要なデータに対する予期しないアクセスや移動を検出するように実装する必要があります。通常のビジネス プロセスとして、USBデバイスやネットワーク経由で重要なデータを外部に送信している場合もありますが、故意か不注意かに関係なく、このような操作はデータ流出につながる危険性があります。

セキュリティ意識向上のためのトレーニングによって、データ流出の可能性を減らすことは可能です。不正な理由を示すことで、重要データの転送に関する適切な行為をユーザーに指示できます。また、通常の業務時間中にデータ保護ポリシーに関する教育を行うことができます。たとえば、重要なデータを転送しようとするユーザーにポリシー違反を通知し、転送前に重要なデータを編集するなど、別の転送方法を提示できます。

通常、データの所有者は、組織内の他のグループよりもデータの使用方法をよく理解しています。したがって、インシデントの優先度を判定する権限をデータの所有者に与える必要があります。データの所有者とセキュリティ チームの役割を分担することで、ポリシー違反の可能性を減らすことができます。

承認するデータ移動を定義し、これらの移動を制御するポリシーをデータ損失防止製品に組み込むことで、重要データの未承認転送をブロックするポリシーを使用できます。ポリシーを有効にすると、それに違反する操作はできなくなります。ポリシーを使用することで、ビジネス要件に合わせて柔軟な対応が可能になり、ユーザーは安全に業務を行うことができます。

ポリシーは、一定の間隔で見直し、調整する必要があります。ポリシーが厳し過ぎると生産性に阻害し、緩すぎると、セキュリティ リスクが高まります。

データ流出から保護するIntel Securityのソリューション

McAfee DLP Discover
データを確実に保護するには、重要な情報がどこにあり、どのようなデータが存在するのかを把握する必要があります。McAfee DLP Discoverを使用すると、このような作業を簡単に行うことができます。

- 組み込みの分類機能（HIPAA、PCI、SOXなど）を使用して、信頼された環境内のデータを分類できます。分類機能のカスタマイズも可能です。
- インベントリ スキャンにより、信頼された環境内にあるデータの種類と場所を特定します。McAfee DLP Discoverのインターフェースで既存ポリシーに対する違反を確認できます。
- 修復スキャンを実行して、未承認の場所に保存されているデータを検索し、許可された場所に移動します。
- インベントリ スキャンと修復スキャンは、ローカルのリソースだけでなく、ネットワーク共有やBoxなどのクラウド リソースにも実行できます。
- McAfee DLP Discoverのスキャン結果に基づいて、新しいデータ保護ポリシーを作成できます。

McAfee DLP Endpoint
McAfee DLP Endpointは、オンプレミス、オフプレミス、クラウドのデータを監視し、侵害を未然に防ぎます。イベントをリアルタイムで監視し、一元管理されたセキュリティ ポリシーを適用できます。日々の業務に支障をきたすことなく、詳細なフォレンジック レポートや拡散レポートを生成できます。

- 検出フェーズの完了後、ポリシー違反を報告するデータ保護ポリシーを作成し、組織内のデータ移動の把握に必要なデータを収集します。その後、ブロック ルールを有効にします。McAfee DLP分類機能（HIPAA、SOX、PCI、ITARなど）を使用して、組織内のデータを識別します。
- ユーザーがデータを転送するときにデータ保護ポリシーの説明を表示できます。このようなポップアップを表示することで、危険なデータ転送を減らすことができます。
- インシデント マネージャーで、未承認の場所に送信されるデータのプロパティを確認できます。たとえば、転送の手段や実行者を特定できます。
- データ保護ポリシーを作成し、組織の要件に合わせて調整した後で、未承認のデータ転送を阻止するルールを有効にします。
- 手動分類を有効にすると、ユーザーが自分で作成した文書を分類できます。自動分類エンジンで構造化データを検出できない場合、データの所有者が文書の重要性を判断できる場合があります。この機能はMcAfee DLP Endpointに組み込まれています。サードパーティのツールを追加する必要はありません。
- McAfee Threat Intelligence Exchangeを使用してアプリケーションのアクセス保護ルールを実装すると、未知のアプリケーションによる重要データへのアクセスを阻止できます。これにより、承認済みのアプリケーションは重要データを転送できますが、未確認あるいは不正なアプリケーションはこのようなデータにアクセスできなくなります。

McAfee DLP Monitor
McAfee DLP Monitorは、ネットワーク全体で送受信されているデータを収集し、追跡、報告を行います。データに対する未知の脅威を簡単に識別し、保護対策を実施できます。

- 関連する組み込みポリシーとルールを有効にして、ネットワーク内で違反の可能性を検出します。
- ポリシーとルールをカスタマイズできます。たとえば、クラウドへの重要データの転送を監視するポリシーとルールを追加できます。
- フォレンジック分析により、現在と過去のリスク イベントを関連付け、リスクの傾向と脅威を識別できます。McAfee DLP Monitorを使用すると、セキュリティ担当者は状況を迅速に把握し、問題を解決するルールとポリシーを作成できます。
- 関連のないデータを除外する収集フィルターを追加し、ルールを調整すると、誤検知を減らすことができます。
- ポリシー違反の発生時に、送信者、受信者、データ所有者、システム管理者に通知を送信するように設定できます。

McAfee DLP Prevent
McAfee DLP Preventは、不適切なデータが外部に送信されないように保護し、データ漏えいを防ぎます。電子メール、Webメール、インスタント メッセージ、Wiki、ブログ、ポータル、HTTP/HTTPS、FTP転送などに対応しています。侵害を早期に検出して回避できれば、重要なデータを保護し、被害を未然に防ぐことができます。

- 組み込みのポリシーを使用してMcAfee DLP PreventをWebプロキシやメッセージ転送エージェントを統合すると、メール ゲートウェイやWebプロキシでの未承認のデータ転送を阻止できます。
- 一致率に基づいて機密文書を許可またはブロックするMcAfee DLP Preventルールを作成できます。
- 組み込みのDLPテンプレートを使用して、クラウドへの重要なデータの転送を阻止できます。
- セキュリティ インシデント レポートを確認しながらポリシーを調整できます。これにより、誤検知を減らし、ビジネスの継続性を維持できます。
- ポリシー違反の発生時に、送信者、受信者、データ所有者、システム管理者に通知を送信するように設定できます。

詳細情報
Intel Security Expert Center Community

- McAfee Data Loss Prevention

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社 〒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）FAX 03-5428-1480
西日本支店 〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所 〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所 〒810-0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com