Acronis

ホワイトペーパー

MSP 向けガイド DLP サービスの導入から拡大まで

セキュリティ意識の高まり、セキュリティプロトコルや規制が増加したにもかかわらず、何年もの間、あらゆる規模の企業がデータ漏えいのリスクに対応できていません。実際のところ、リスクは以下に示すとおり増加しています。2021年末発行のレポート：Risk Based SecurityのData Breach QuickViewによると、2005年以降、220億件以上の記録がリスクにさらされており、機密データの侵害件数では史上2番目に多い年になりました。これらの多くのデータがデータ漏えいのリスクにさらされていました。データ漏えいとは、極秘、機密、または保護されたデータが偶発的または意図的に組織内外の信頼できない環境や不正なユーザーに暴露されるセキュリティ侵害のことです。

データ損失はなぜ起こるのか？2つの主な原因：

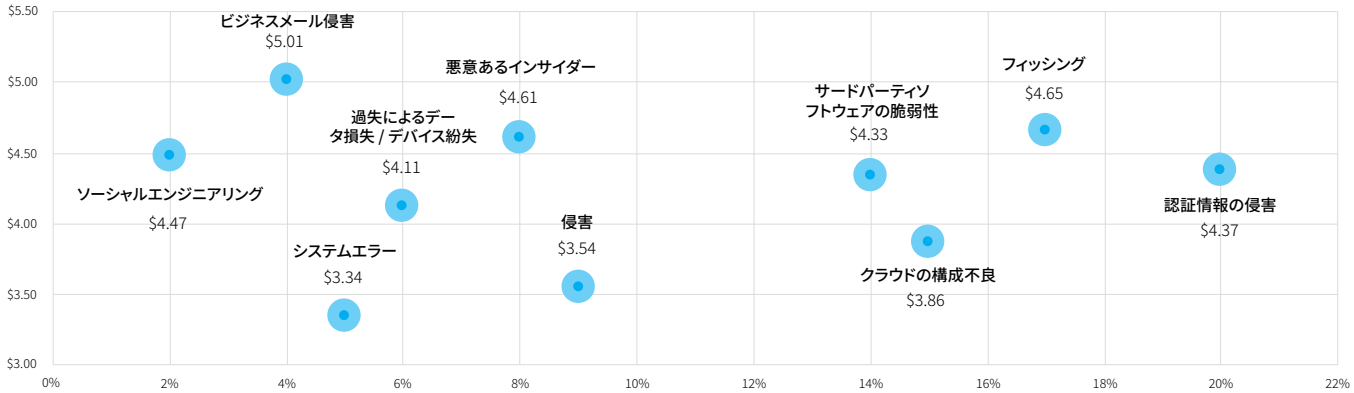
1. 外部からのサイバー脅威

MITRE ATT&CKフレームワークの定義によると、データ抜き出しは攻撃中に悪意ある攻撃者が実行する最終的な手段です。80%以上のデータ侵害における攻撃者の動機は、Verizon 2022 Data Breach Investigation Reportによると金銭の取得です。

そのため、機密データは多くの攻撃において主な標的になっています。悪意ある攻撃者が企業環境へのアクセスを確立すると、様々なチャネル経由でデータの抜き出しを試みることができます。攻撃の複雑さも増し、より多くのセキュリティレイヤーを回避できるようになっているため、組織のデータに対するリスクは指数関数的に増加しています。

2. 内部リスク

マルウェア対策やその他のエンドポイントセキュリティ技術は外部からの攻撃を検出し阻止できますが、組織のデータに対するもう1つのリスクであるインサイダー関連のものは増加しています。その例として、エンドユーザーが知らずに承認されていない人にデータを渡している（Eメールの転送などによって）ということがあります。これは、従業員の間違いやIT構成ミス、悪意あるインサイダーなどによって発生し、これらはすべて組織に対して深刻な脅威となり、コストが高くつくデータ漏えいにつながります。



一部の組織では内部リスクを過小評価していますが、Ponemon Instituteの2021 Cost of Data Breach Report（2021年データ漏えいのコストに関するレポート）が明確に述べているようにデータ漏えいの約3分の1はインサイダー関連のものです。

データ漏えいのビジネスへの影響は何か?

データ漏えいはビジネスに深刻なリスクをもたらします。機密データの不正ユーザーへの流出の影響：

- **規制の非遵守**：従業員や顧客の個人を特定できる情報（PII）、保護された医療情報（PHI）、カードの所有者データなどの保存、アクセス、保護は、GDPR、CCPA、HIPAA、PCI-DSSといった地域的および国際的規制によって厳しく規制されており、GDPRのような一部の規制はさらに決められた時間内に速やかにインシデントを報告する必要があります。規制データの侵害報告が遅れた場合、組織には高額の罰金が課せられ、コンプライアンス認定を失う可能性もあります。
- **金銭的損害**：データ漏えいが発生すると、MSPの顧客に課される可能性のある規制上の罰金に加えて、サービスプロバイダーは顧客のセキュリティに対する責任からくる金銭的損害のリスクにもさらされており、これは訴訟に発展する場合もあります。また企業秘密や知的財産の流出は企業に金銭的損害を引き起こしたり、さらには市場での立場を不安定にする原因になる可能性があります。
- **風評被害のリスク**：不名誉なデータ漏えいのニュースになるのは企業にとって有害です。これによって顧客の解約につながるだけでなく、既存のパートナーシップや新規顧客を獲得する能力も損ないますまた顧客のデータ漏えいは評判やビジネスにも影響を与える可能性があります。

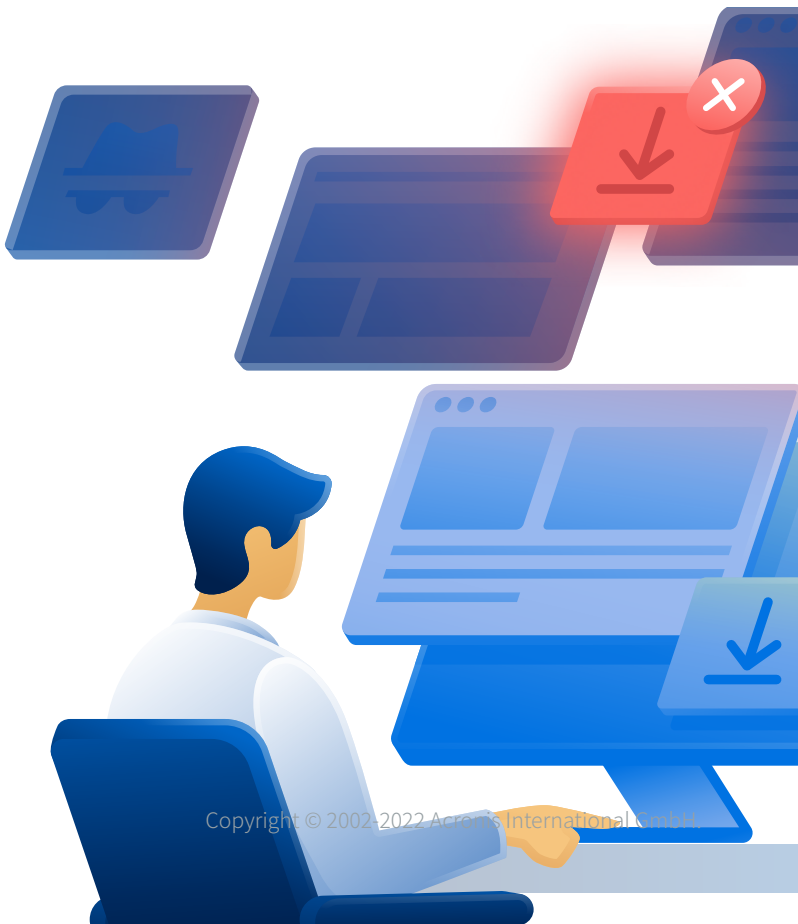
データ損失防止とは?

データ損失防止は、長期的に確立されたセキュリティソリューションのカテゴリーで、極秘および機密のデータの不正な使用、伝送、保存などを検出し、防止する統合情報セキュリティ技術のことです。

DLPソリューションは、データフローコントロールとコンテンツ分析法を組み合わせて実現されます。このような技術は、ビジネスで認められるデータの使用法や組織全体で処理するポリシーを執行し、機密データの不正受信者（社内外の）への流出を防止します。

データ保護は主にバックアップとリカバリに関連していますが、データ漏えいなどより幅広い脅威に対して機密情報を保護するDLPやノータリゼーション、暗号化のようなその他の基本的技術もあります。

DLPは組織全体を流れ、保存される機密データの可視化と制御を提供する**唯一の技術**です。



データの状態およびそれらを保護するDLPの機能

データは**主に3種類の状態**で組織内に保管されます。

- **使用中のデータ：**使用中またはローカルチャネル（例えば、周辺機器、リムーバブルストレージ）やエンドポイントコンピュータ上のアプリケーション経由で転送中のデータ。このようなデータの例は、エンドポイントコンピュータからUSBドライブに転送中のファイルです。
- **移動中のデータ：**この用語はコンピュータ間で移動中または転送中のデータを指します。例えば、ローカルデータストレージからクラウドストレージへ転送中のデータ、またはインスタントメッセンジャーやEメール経由でエンドポイントコンピュータから他のエンドポイントへ転送中のデータが移動中のデータとみなされます。
- **保存中のデータ：**これは、ローカルまたはネットワークに保存されており、現在アクセス中でも転送中でもないデータを指します。保存中のデータの例は、ネットワーク共有やオンプレミスのサーバーに保存されているデータです。

注意すべき重要な点は、状態は頻繁に、そして継続的に変わりますが、一部のデータはライフサイクル全体を通じて1つの状態を保ちます。さまざまなデータの状態すなわち特性や差異を理解することで、顧客は組織のデータをより安全に処理し、情報漏えいから保護できるようになります。

データの状態に応じてそれぞれを保護する3種類の主なDLPタイプ（機能）があります。

- **使用中のデータ用DLP**
- **移動中のデータ用DLP**
- **保存中のデータ用DLP**

他にもアイデンティティ管理や暗号化といった異なるデータリスク（例えばアクセシビリティ、プライバシーリスク）に対応できる技術があります。しかし、DLPは、データフローの可視性を提供しながらデータ漏えいを防止するという厳格な目的を持ち、複数の状態でデータを保護できる唯一の技術です。

DLP コントロール（コンテンツ対コンテキスト）

組織内のデータフローにはそれぞれのコンテンツとコンテキストがあります。コンテキストは、データフローに関連するユーザーや使用されるチャネル、フローの方向などといった環境要因を指します。コンテンツは、転送されるデータの実際のタイプ/カテゴリー（例えば、患者の医療記録、従業員のPIIなど）を説明します。

効率的なDLPはコンテキストとコンテンツの両方に基くデータフローコントロールを行う必要があります。

- **コンテキスト認識型DLPコントロール**：関連するユーザー、使用チャネル、転送データの方向、宛て先、日時などのような属性を使用しながら操作のコンテキストに基づいてデータ転送操作をコントロールします。

例：ユーザー（誰が）によるデータ（何を）の暗号化されたUSBデバイス（どこに）へのコピーを許可し、暗号化されていないUSBデバイスへのコピーを禁止するポリシー。

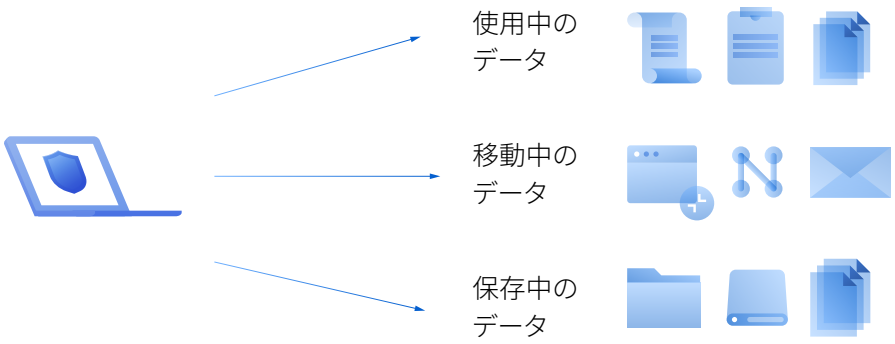
- **コンテンツ認識型DLPコントロール**：転送される実際の情報（コンテンツ）に基づいて転送操作をより詳細にコントロールします。

例：HIPAA関連の情報を含む文書（何の情報）は、USBデバイスへのコピーを禁止するポリシー。

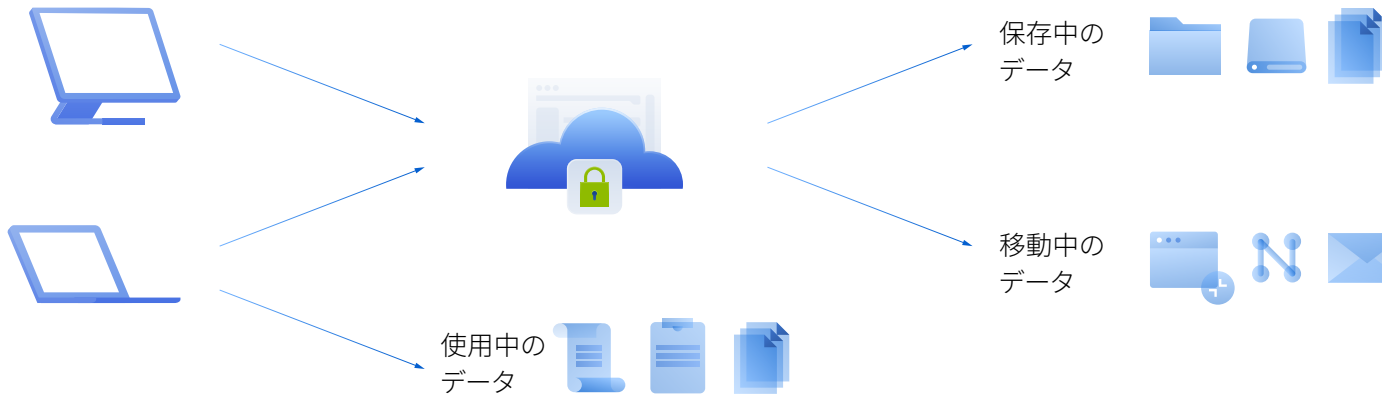
DLP アーキテクチャタイプ

導入と操作の方法に基づいてDLPには3つの主要なタイプがあります。

- **エンドポイントDLP**：エンドポイントコンピュータのDLPエージェントを使用し、企業ネットワーク内またはインターネットで使用されるかどうかにかかわらず、使用中のデータ、移動中のデータおよび保存中のデータの漏えいを防止するソリューション。



- **ネットワーク / クラウドDLP**：移動中または企業ネットワークに配備されるコンピュータに保存中のデータ漏えいを防止するハードウェア / 仮想DLPゲートウェイおよびサーバーを含むネットワーク常駐のコンポーネントのみを使用し、企業ネットワーク外の不正受信者や転送先へのデータ漏えいを防止するソリューション。



- **ハイブリッドDLP**：ネットワーク/クラウドDLPとエンドポイントDLPコンポーネントの両方を使用して、エンドポイントとネットワーク/クラウドDLP両方の全機能を実行するソリューション。

ネットワーク/クラウドDLPは、アーキテクチャ上使用中のデータを保護できず、企業ネットワーク外の不正ユーザーへのデータ漏えいのみをコントロールします。一方、エンドポイントとハイブリッドDLPはすべての状態のデータを保護し、内外両方の不正ユーザーへの漏えいを防止することができます。

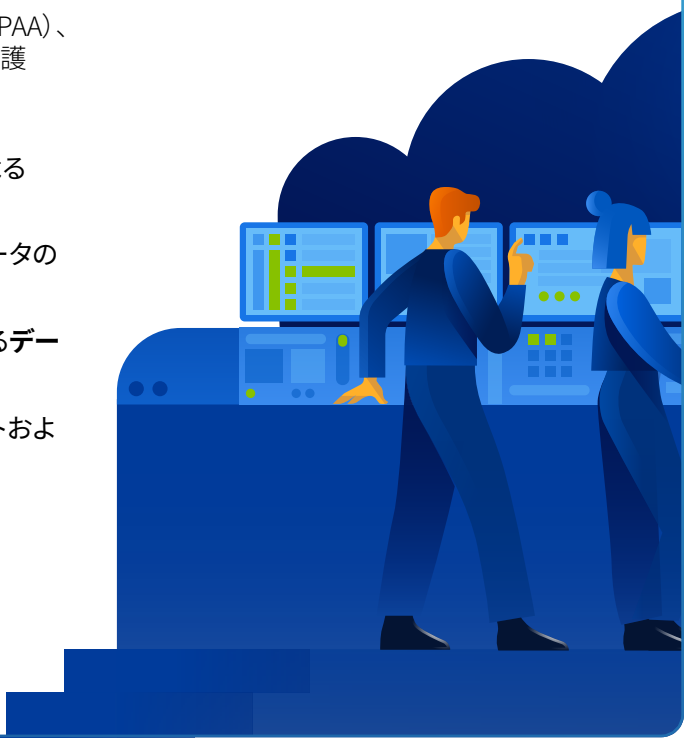
このガイドの目的上、エンドポイントDLPアーキテクチャに基づくDLPサービスの開始、実行および拡張に焦点を絞ります。

顧客にDLPが必要な理由

Ponemon Institute 2021 Cost of Data Breach レポートによると、データ漏えいのコスト合計の世界平均は424万ドルで2020年から10%増加しています。データ漏えいのコストは増加していますが、漏えいを特定し抑制するための実際の平均時間は287時間で、顧客が漏えいを封じ込めるまで大きなリスクに直面するということが分かります。このようなリスクは金銭、風評被害およびコンプライアンスのコストにつながります。

DLPによって顧客のリスク低減を可能にする主要な方法

- **規制の遵守達成**を支援し、PII（GDPR、CCPA）、PHI（HIPAA）、支払いカード情報（PCI DSS）などの規制された情報を保護
- **顧客の知的財産や企業秘密を保護**
- ソーシャルエンジニアリングが原因のマルウェアや攻撃によるデータ流出の**リスクを低減**
- **リモートワークとBYODのセキュリティを強化**し、機密データのプライベートクラウドベースのストレージへの転送を防止
- 従業員の偶発的間違い、過失、不正行為によって発生する**データ漏えいの防止**
- DLPイベントの可視化を継続してデータ漏えいインシデントおよび侵害後調査に対する**迅速な対応を実現**



DLPサービスデリバリーの流れ

DLPサービスの導入、運用、拡大を詳述する前に、まず以下のステップを含む具体的なデリバリーの流れを策定することが重要です。

- **DLPエージェントの導入：**企業データに対して徹底した保護を提供し、DLPエージェントをエンドポイントに導入する目的を持って、どのエンドポイントをDLPサービスを使って設定するかを決定することが、サービスデリバリープロセスの第一歩です。機密データが作成され、保存され、使用される場所のワークロードすべてに設定されたDLPエージェントを持つことを推奨します。そのようなワークロードが保護されないままだと、企業ITセキュリティシステムにデータ漏えいギャップが生じる可能性があります。

- **DLP ポリシーの作成：**もうひとつの初期ステップは、適切なデータ使用とデータ漏えいを防止するための処理ポリシーを保証するDLP ポリシーを作成することです。使用するDLP 技術に基づいて、このステップは導入の前に実行可能です。**注意すべき重要な点**は、DLP ポリシーは顧客特有のもので万能ではないということです。それぞれの組織はそれぞれの内部プロセスを持っており、さらに、異なる規制に従い、異なるデータアクセスや共有ニーズがあるからです。DLP ポリシー作成にはこうした特徴があるため、従来のDLP ソリューションは手作業によるポリシー管理が必要になり、サービスプロバイダーがDLP サービスを構築するために使用するにはかなり複雑でコスト上の障害になります。

- **DLP ポリシーの有効化**：初期DLP ポリシー作成後の重要なステップは、顧客にポリシーを有効化し、ビジネス要件を満足しているか確認することです。MSP では顧客のビジネス特性をそれほど深く理解できません。ポリシーの視覚的表現が複雑で「技術的」であればあるほど、顧客がポリシーを有効化するには、より多くの時間と専門知識が必要になります。

- **DLP ポリシーの執行および管理：**DLP ポリシーを顧客に有効化すればビジネスの機密データの漏えい保護を開始することができます。DLP技術は組織のデータフローをコントロールし、不正なデータフローを阻止します。しかし、ビジネスは常に進化し、新しいプロセスが導入され、新しいデータ規制が発生し、古いものは変更される可能性があります。このため、初期DLP ポリシーは新規の重要なデータフローをブロックせず、すべてのデータ漏えいの試みを防止するために、変化を続けるビジネスニーズに合わせて継続的に調整する必要があります。これは手作業によるポリシーの微調整または適応型のポリシー自動調整のいずれかを通じて達成できます。

- **DLP サービスのバリューについての報告：**DLP サービスの価値を実証するための、阻止された機密データ転送とDLP 関連のエンドユーザーアクションに関する継続的報告は既存の顧客の維持を助け、データ漏えいの問題を認識していない顧客にリスク削減を示すことができます。

従来のDLP ソリューションに関するMSP の課題

DLP は成熟したエンタープライズ中心のマーケットで、長期的に確立した位置を占める従来のソリューションは、継続的で深い理解、DLP コントロールのビジネス特性マッピング、規制要件の知識、および技術を操作するために必要なデータコンプライアンスの理解などを必要とするため、サービスプロバイダーやSMB 顧客は導入に苦労しています。こうした背景から、DLP 業界は、社内にDLP 管理を専門とする高額な人材を持つ大規模組織に主として焦点を合わせてきました。

DLP サービスの導入と実行時にMSP が直面する主な課題

- **DLP サービスを実行するのはコストがかかり複雑**：従来のDLP サービスでは、初期ポリシーの作成およびフォローアップ調整に複雑な手動プロセスが必要で、効率的なDLP を顧客に導入するために時間と労力がかかりコストも高くなりすぎます。さらに、こうした複雑さを解消するには、DLP 専門家を採用する必要があり、一般的なIT セキュリティの専門家を採用するよりもかなり困難かつ高価になります。

- **効率的なDLPには顧客特有のポリシーが必要**：前述したように、組織のビジネスプロセスやデータ機密性はそれぞれ独自で常に変化しているため、ビジネス特性に合わせてDLPポリシーを調整し続ける必要があります。しかし、MSPには顧客のビジネスプロセスに対するこのような深い理解が不足しているため、継続的に維持する必要があります。これによって障壁が生じ、従来型のDLP技術を有するMSPにとって拡張性についての大きな問題になっています。
- **DLPポリシーの不完全な構成はビジネスの継続性を阻害する可能性**：一方では、手動のDLPポリシー作成および構成は、複雑性や詳細度のためにエラーが発生しやすくなります。他方、DLP技術は不正なデータフローを阻止します。DLPポリシーが不完全であったり、新しいビジネスプロセスがこのポリシーと一貫してマッピングされなかった場合、ビジネスで必要なデータフローを誤ってブロックしてしまい、この複雑性とDLP防止機能が結びつくと、重要なビジネスプロセスを阻害してしまう可能性があります。
- **従業員は顧客の最大の弱点**：DLP技術がMSPや顧客にアクセス可能かどうかに関係なく、人的エラーや従業員を標的にする外部からの攻撃はデータ漏えいの主な原因です。たとえサービスプロバイダーが他のエンドポイント保護レイヤーによって外部の脅威リスクを制限できるとしても、ユーザーが誤って機密データを流出してデータ漏えいが発生した場合に責任を負うのはサービスプロバイダーです。
- **顧客はデータ漏えいの問題に気付かない可能性**：DLPへのアクセスは従来から困難であるため、データ漏えいの問題は顧客が気付かない可能性があります。DLPサービスを開始するということは、顧客が直面するデータ漏えい問題およびDLPこそがあらゆる規模の組織に大きな脅威をもたらすリスクに対応できる唯一の技術であるという事実について顧客を教育する必要があるということです。

常に進化し続けるビジネス要件に対応できるよう、DLPルールを俊敏に変更するという課題に対応することが、振る舞い検知ベースの自動ポリシー作成、拡張、監視といったマーケットの新しいトレンドと技術です。これらの新しい機能はDLPマーケットを効果的に広げ、サービスプロバイダーやその顧客がアクセスできるようにします。今はDLPサービスでポートフォリオを強化する絶好の機会です。

DLPサービスの計画と開始

DLPサービスの計画と開始の最初のステップは、顧客が実際に必要とするDLPを確認することです。

顧客は、以下の事項の一部または全部に該当する場合にデータ漏えいのリスクを減らすためにDLPサービスを必要とします。

- 規制の対象になる機密データがあるワークロードの作成、保存、作業を行う
- 漏えいから保護する必要がある企業秘密または知的財産を所有する
- 高度に規制された業界で事業運営している
- データ漏えいの被害を受け、環境を安全にし、リスクを低減したいと考えている
- コンプライアンス認定を所有/必要としている
- 責任を低減するためにサイバー保険を支払っている/検討している
- 専任のセキュリティスタッフや専門知識を持っていない

さらに、以下の業界の顧客は歴史的にDLPに多大な関心を寄せています。

- 銀行および金融サービス
- ヘルスケア
- 法律
- ITおよび通信
- 政府および公共セクター
- 製造業
- 小売および流通
- 教育
- エネルギー

顧客がこうした事項に該当しているまたは上記業界の場合、サービスポートフォリオにDLPを追加して、データ漏えいリスクを低減するという急速に増大するニーズを満たし、規制コンプライアンスの強化を提案する機会です。

サービス計画とコスト予想

サービス価格を決定する主要な3つの要因は人件費、製品コストおよび健全な利益率です。各要因が価格見積もりに影響を与える可能性があります。

- **人件費：**選択するソリューションの複雑さがサービス技術者がプロビジョニングやサービス管理で費やす時間および必要なITセキュリティ専門知識を決定します。
- **製品コスト：**DLPはこれまで大企業によって使用され、コストが高いため、中小企業では導入できませんでした。主な顧客がSMBの場合、コストが高すぎないソリューションを選択する必要があります。
- **健全な利益率：**平均的なMSPは、定期収益モデルで販売されたリモート配信サービスの粗利益を最大50%獲得しています。

Acronis Advanced DLPによるDLPサービスの提供

アクロニスは、導入や設定に何か月もかけたり、チームを維持したり、理解するためにプライバシー法の専門家を採用したりすることなく、顧客特有のポリシーを自動作成し一貫性を継続的に維持する振る舞い検知ベースのDLPを提供します。

Acronis Advanced DLPを使えば、移動中や使用中のデータに対する包括的なDLP保護をこれまでにないシンプルさで顧客に提供することができます。

- ポートフォリオを拡張してより多くの顧客を獲得。以前は大企業でしか使用できなかったDLPサービスによって顧客当たりの収益を増加させることで、収益機会を拡大。
- 管理の複雑さ、コスト、人員を増やすことなくDLPをビジネスに容易に追加して労力を最小化する。
- 機密データの漏えいを防止して顧客のリスクを軽減する。
- GDPR、HIPAA、PCI DSSなどのすぐ使用できる共通規制フレームワーク用のデータ分類テンプレートを使って、顧客の規制コンプライアンスを強化する。
- DLPサービスの導入、初期ポリシーの設定およびフォローアップの調整を自動化することでサービス導入、設定と管理を簡略化する。
- 変化し続けるビジネス特性に対応するDLPポリシーを振る舞い検知ベースの技術と自動的に一致させることで、ポリシー執行前に顧客とポリシーを確認し、顧客特有のDLPポリシーを保証する。
- DLPイベントにより迅速に対応 し、集中管理のポリシーベースの監査ログ機能やセキュリティアラート機能によってDLPサービスオペレーション、ポリシーメンテナンス、ITセキュリティ監査、インシデント調査を簡略化する。

Advanced Data Loss Prevention (DLP)

Advanced DLPを使えば、不正なユーザーや組織への情報漏えいの心配から解放されます。独自の振る舞い検知ベースの検知技術で各顧客の特性に基づいたDLP ポリシーの作成と継続的改善が可能になり、今までにないシンプルで簡単な導入、設定、運用管理が行えます。

Acronis

詳細については、
www.acronis.comをご覧ください。