FORCEPOINT
Data Loss Prevention (DLP)

ゼロ境界の世界におけるデータ保護

Human Pointによるセキュリティ

データセキュリティは終わりなき挑戦です。 一方では、IT組織は規制に遅れずについていき、標的型攻撃や偶発的な公開から知的財産を保護する必要があります。 その一方で、クラウドアプリケーションの採用、ハイブリッドクラウド環境、BYODの傾向など、ITがマクロITの動きに適応しなければならないため、データが組織から離れていく可能性があります。

この拡大する攻撃対象領域は、重要なデータを保護するための最も重要な課題です。 データセキュリティチームはデータを追跡するために一見論理的なアプローチを取ります：それを見つけ、カタログ化し、そしてそれを制御します。 それでも、データ損失を防ぐためのこの伝統的なアプローチは、データセキュリティにおける最大の変数で「人」を無視するため、もはや効果的ではありません。

データのみに焦点を当てるのではなく、セキュリティは人々によって始まりそして終わります。 重要なのは、ユーザーがデータやアプリケーションとやり取りする様子を可視化することです。 これが達成されると、特定のユーザーのリスクとデータの機密性または価値に基づいて一定レベルの管理を適用できます。

組織のデータ保護プログラムでは、ユーザー、データ、ネットワークの交差点というHumanPointを考慮する必要があります。さらに、企業は、企業内を移動するときにデータに注意を払い、データを作成、操作、移動する人に注目する必要があります。

データ保護は以下を満たす必要があります:

- **規制されたデータを保護** データを作成、保存、移動するために人々が使用するすべてのアプリケーションを一元管理。
- **知的財産を保護** 高度なDLPを使用して人々がデータをどのように使用しているかを分析し、データを使用して適切な決定を下すように人々指導し、リスクによるインシデントの優先順位付けを行います。

あなたの人々が勤務している場所や日付がどこにあるかにかかわらず、可視性と制御を：

- Cloud Applications (powered by Forcepoint CASB)
- Endpoint
- Network
- Discovery

Forcepoint DLPは、人々が勤務する場所やデータが存在する場所を問わず、可視性と制御によってHumanCentricのリスクに対処します。セキュリティチームは、ユーザーリスクスコアを適用することで最も重要なイベントに焦点を当てることで、グローバルでのデータ保護規制を遵守します。

FORCEPOINT

コンプライアンスを加速

現代のIT環境は、特にクラウドアプリケーションやモバイルワークフォースへの移行に伴って、数十のグローバルデータセキュリティ規制を遵守しようとしている企業にとって困難な課題となっています。多くのセキュリティソリューションは、クラウドアプリケーションに見られるタイプなど、何らかの形の統合DLPを提供しています。それでも、セキュリティチームは、エンドポイント、クラウドアプリケーション、およびネットワークにまたがって個別で一貫性のないポリシーを展開および管理する際に、望ましくない複雑さと追加コストに直面します。

Forcepoint DLPは、事前にパッケージ化されたグローバル規制の適用範囲とIT環境全体の集中管理を組み合わせることで、コンプライアンスへの取り組みを加速します。Forcepoint DLPは機密性の高い顧客情報と規制データを効率的に保護するため、あなたは継続的なコンプライアンスを自信を持って証明できます。

- 規制適用範囲は83カ国の規制上の要求に適用される370以上のポリシーに迅速に準拠し、維持します。
- ネットワーク、クラウド、およびエンドポイントを対象ととしたディスカバリにより、規制対象となるデータを見つけて修正します。
- IT環境全体にわたる集中管理と一貫したポリシー。

人々にデータ保護を強化する力を

予防管理のみのDLPはユーザーをいらいらさせます。誰かがタスクを完了するという唯一の意図でそれらを回避するでしょう。セキュリティを回避すると、不要なリスクと不注意によるデータ漏洩が発生します。

Forcepoint DLPは人が今日のサイバー脅威の第一線として認識しています。

- クラウド内でもネットワーク上でも、電子メールやエンドポイントで、あらゆる場所でデータを検出し、制御します。
- ユーザーの行動をガイドするメッセージを使用して従業員に賢明な決断を下し、ポリシーについて従業員を教育し、重要なデータと対話するときのユーザーの意図を検証します。
- データが組織外に移動するときにデータを保護するポリシーベースの自動暗号化を使用して、信頼できるパートナーと安全にコラボレーションします。
- 主要なサードパーティのデータ分類ソリューションと統合することで、データのラベル付けと分類を自動化します。(例 Microsoft Information Protection, Titus, Boldon James).

データを追跡する高度な検出と制御

悪意のある、または偶発的なデータ漏えいは、単一のイベントではなく、複雑な事件です。Forcepoint DLPは、Gartner、Radicatiなどのアナリスト企業が業界のリーダーとして認めている実証済みのソリューションです。ForcepointのDLP製品は２つのバージョンで利用可能です：Forcepoint DLP for Complianceと、DLP for Intellectual Property (IP) Protection.

Forcepoint DLP for Complianceは、以下のような機能によりコンプライアンスを遵守する役割を果たします:

- 光学式文字認識（OCR）は、保存されたまたは利用中データで画像に埋め込まれたデータを識別します。
- 個人識別情報（PII）に対する識別は、データ検証チェック、実名検出、近接分析、およびコンテキスト識別子を提供します。
- カスタム暗号化識別は、発見および適用可能な管理により隠されたデータを見つけます。
- ドリップＤＬＰを検知（例、時間をかけてゆっくり漏れるデータ）するため累積的に分析します。
- Microsoft Information Protectionとの統合により、暗号化されたファイルを分析し、対象データに適切なDLP制御を適用します。

知的財産保護用Forcepoint DLPには、上記の機能が含まれています。さらに、以下のような機能により、潜在的なデータ損失へ最も高度な検出と制御が適用されます:

- 機械学習により、ユーザーはシステムをトレーニングして、関連性のある今までに見たことのないデータを識別できます。ユーザーは、類似のビジネス文書、ソースコードなどにフラグを立てるために、エンジンに対してポジティブまたはネガティブな例を提供します。
- 構造化データと非構造化データのフィンガープリントを使用することで、データ所有者はデータタイプを定義し、ビジネス文書、設計計画、およびデータベース全体の完全一致および部分一致を識別し、データに一致する適切なコントロールまたはポリシーを適用できます。
- 分析は、個人の電子メールの使用増加などのデータのやり取りに関連するため、ユーザーの行動の変化を識別します。

リスクへの対応と修復

DLPへの従来のアプローチでは、データを失う危険性があると同時に、誤検出でユーザーの負荷が高まります。ForcepointDLPは高度な分析を適用して、一見無関係のDLPイベントを優先順位付けされたインシデントに相関させます。ForcepointDLPヒューズとともに提供されるIncidentRiskRanking（IRR）は、データ盗難やビジネスプロセスの破綻などのデータリスクシナリオの可能性を評価するために、異なるDLP指標をベイジアンビリーフネットワークのフレームワークにまとめたものです。

- **レスポンスチームを最大のリスクに集中させる** 優先付けされたインシデントは発生したリスクに責任ある人、危険にさらされている重要なデータ、およびユーザー間での一般的な行動パターンを強調します。
- **調査および対応** さまざまなイベントをリンクし、危険にさらされているデータのコンテキストを表示し、アナリストに行動を起こさせるために必要な情報を提供するワークフローを使用します。
- **ユーザーのプライバシーを保護する** 匿名化オプションとアクセス制御を使用します。
- **データのコンテキストを追加** Forcepoint Insider ThreatおよびForcepoint Behavioral Analyticsとの密接な統合により、より広範なユーザー分析にデータのコンテキストを追加します。

人が働いているところはどこでも可視、データが存在する場所をどこでも制御

今日の企業は、データがいたるところに存在し、企業が管理または所有していない場所でデータを保護する必要があるという複雑な環境に直面しています。クラウドアプリケーション向けForcepointDLPは、分析とDLPポリシーを重要なクラウドアプリケーションに拡張して、データがどこにあっても保護します。

- **データを識別して保護する** クラウドアプリケーション、ネットワークデータストア、データベース、管理対象エンドポイントにまたがるデータが対象です。
- **視認性を高める** O365、Google Apps、Salesforceなどの企業で利用されている最も人気のあるクラウドアプリケーションでのデータの共有と保存に加えアップロードとダウンロードができます。
- **ポリシー施行を統一する** 単一のコンソールを介して、クラウド、ネットワーク、エンドポイントのすべてのチャネルにわたってデータ検出ポリシーを定義および適用します。
- **Forcepointがホストするソリューション** フィンガープリントや機械学習などのエンタープライズDLP機能をクラウドアプリケーションに拡張します。

ForcepointDLPには、展開ごとに一元管理された高度な分析および規制ポリシーテンプレートが含まれています。企業は、自社のIT環境に合わせて展開オプションを選択します。

Appendix A: DLPソリューションコンポーネントの概要

Forcepoint DLP – Endpoint	Forcepoint DLP – エンドポイントは、企業ネットワークの内外にあるWindowsおよびMacエンドポイント上の重要なデータを保護します。 これには、保存した（発見）、動いている、そして利用中のデータに対する高度な保護と制御が含まれます。 暗号化されたデータを分析して適切なDLPコントロールを適用するために、Microsoft Information Protectionと統合されています。 DLPコーチングダイアログからのガイダンスに基づいて、従業員によるデータリスクの自己修復を可能にします。 このソリューションは、HTTPSを含むWebアップロード、およびOffice 365やBox Enterpriseなどのクラウドサービスへのアップロードを監視します。 Outlook、Notes等のEメールクライアントとも完全に統合しています。
Forcepoint DLP – Cloud Applications	Powered by Forcepoint CASB, DLP – Cloud Applicationsは、Forcepoint DLPの高度な分析と単一制御を、Office 365、Salesforce、Google Apps、Box、ServiceNowなどの重要なクラウドアプリケーションに拡張します。
Forcepoint DLP – Discovery	Forcepoint DLP – Discoveryは、Office365やBox Enterpriseなどのクラウドサービスに保存されているデータだけでなく、ネットワーク全体の機密データを識別して保護します。 高度なフィンガープリンティング技術は、保管中の規制データと知的財産を識別し、適切な暗号化と管理を適用することによってそのデータを保護します。
Forcepoint DLP – Network	Forcepoint DLP – Networkは、電子メールやWebチャネルを介して移動するデータの盗難を阻止するため、重要な対処ポイントを提供します。 このソリューションは、外部からの攻撃や増大する内部からの脅威による悪意のある偶発的なデータ損失を識別して防止するのに役立ちます。 OCR（光学式文字認識）は、画像内のデータを識別します。 分析に基づきDLPは、一度に 1レコードずつのデータ盗難の試みやその他の危険性の高いユーザーの行動を特定し、阻止します。

Appendix B: DLPソリューションコンポーネントの詳細

	Forcepoint DLP – Endpoint	Forcepoint DLP – Cloud Applications	Forcepoint DLP – Discover	Forcepoint DLP – Network
どのように展開されますか？	Forcepoint One Endpoint	Forcepoint Cloud	IT部門管理のDiscovery Server	Network AppliancesまたはPublic Cloud
主な機能は何ですか？	ユーザーのエンドポイントに関する情報の収集	クラウド内またはクラウド提供のアプリケーションを使用したデータの検出とポリシーの適用	データセンター内の静止データの発見、スキャン、修復	WebおよびEメールによる移動中のデータの可視性と管理
保存されたデータはどこで発見/保護されていますか？	Windows endpoints MacOS endpoints Linux endpoints	Exchange Online Sharepoint Online Box	オンプレミスのファイルサーバーとネットワークストレージ Sharepoint Server Exchange Server	
移動中のデータはどこで保護されていますか？	Email, Web: HTTP(S), Printers, Removable media, Mobile devices, File servers / NAS	Office 365, Google Apps, Salesforce.com, Box & ServiceNowへののアップロード、ダウンロード、共有		Email /Mobile email/ ActiveSync proxy Web: HTTP(S) ICAP
使用中のデータはどこで保護されていますか？	IM, VOIP file sharing, applications (cloud storage clients), OS clipboard	クラウドアプリケーションを使用した共同作業中		
インシデントリスクランキング*	含む	含む		含む
光学式文字認識			含む	含む
データ分類とラベリング統合	Microsoft Information Protection, Boldon James, Titus			
どのようなデータをフィンガープリントできますか？*	Structured (databases), Unstructured (documents), Binary (non-textual files)			
統一されたポリシー管理	単一コンソールによるポリシー設定と実施			
堅牢なポリシーライブラリ	幅広いコンプライアンスポリシーライブラリからの発見および執行			

About Forcepoint

Forcepointは、個々のユーザーやマシンによってもたらされる動的なリスクにセキュリティ対応を継続的に適応させることによってデジタル企業を変革する、グローバルな人間中心のサイバーセキュリティ会社です。Forcepointヒューマンポイントシステムは、データとシステムの信頼された使用を継続的に保証するためにリスク適応型保護を提供します。テキサス州オースティンに本拠を置くForcepointは、130カ国以上の何千もの企業および政府機関の顧客のHuman Pointを保護します。

お問合せ先
ForcepointJapan株式会社
〒105-0003　東京都港区西新橋1-2-9　日比谷セントラルビル14階
Tel:03-5532-5602
Email: Japan@forcepoint.com
Web: www.forcepointcom/ja