



Check Point
 makes
DLP work

製品の概要

DLP Software Blade™は、機能とプロセス両面からDLPを実現する業界唯一のソリューションです。データ流出の検知と防止を同時に実現し、重要情報の意図せぬ漏洩を未然に防ぎます。

DLP Software Blade

機能とプロセス両面からDLPを実現

課題

情報漏洩事件が増加の一途をたどる昨今、企業において機密データの万全な保護対策が不可欠となっています。とりわけ、機密扱いの社員データや顧客データ、法的文書、知的財産データなどの重要情報は高い流出リスクにさらされています。こうした問題について多くの組織では、従業員の生産性を妨げることなく、また、ITスタッフの運用負荷を増やすことのない解決策が求められています。検知技術は進化しているものの、ユーザの意図を理解した判断といった面では最終的に不十分です。また従来型のDLP製品には、長時間の導入作業や煩雑な管理は避けられず、また高コスト体質の問題もあり、機密データを保護する取組みは困難な課題となっています。

概要

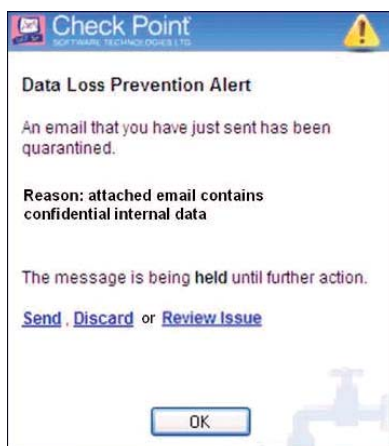
DLP Software Bladeは、技術とプロセスを兼ね備え、情報漏洩の検知と未然の防止を同時に実現する革新的なDLP（Data Loss Prevention：データ損失防止）ソリューションです。画期的なデータ分類技術MultiSpect™により、ユーザ、コンテンツ、およびプロセスを総合的に分析してポリシー違反かどうかを正確に判断し、新技術UserCheck™により、ユーザ自身が問題をリアルタイムに是正できるようにします。ネットワーク・ベースのDLPソリューションであるDLP Software Bladeは、データの取り扱いポリシーについてのユーザ教育を自動的に行ってIT/セキュリティ担当者が問題処理にかかる工数を削減し、不正な意図の有無にかかわらず企業の機密情報の漏洩を防ぎます。

Check Point UserCheck™

UserCheckは、ユーザ自身がインシデントをリアルタイムに是正できるようにする画期的な技術です。ユーザの行為がポリシーに抵触する可能性がある場合はその場で問題を是正するよう警告し、ポリシーに適合した行為については直ちにそれを承認します。ユーザ自身にインシデント対応（送信、破棄、確認）を行わせ、データ利用ポリシーについてのユーザの意識を高めることで、セキュリティの向上につながります。通知は、シン・エージェントが表示するポップアップ、またはエージェントのインストールが不要な専用の電子メールによってリアルタイムに実行されます。

UserCheckがもたらす利点

- 完全な防止：情報漏洩の検知と防止を実現
- ユーザの自己学習：データ共有ポリシーについて自動的にユーザ教育を行えるため、IT/セキュリティ担当者の問題処理への関与が不要



UserCheckは、ユーザ自身が問題をリアルタイムに是正できるようにする画期的な技術です。

主な利点

■ 重要な企業情報の損失を防止

新技術 UserCheck により、ユーザ自身が問題をリアルタイムに是正

■ 技術とプロセスの組み合わせで実現する DLP

革新的なデータ分類エンジン MultiSpect が、ユーザ、コンテンツ、およびプロセスを総合的に分析し、ポリシー違反の有無を極めて正確に判断

■ 導入が簡単ですぐに情報漏洩対策を実施することが可能

事前定義されたポリシーやファイル形式およびデータ・タイプの幅広いサポートにより、すぐに運用開始が可能

製品の特徴

- Check Point UserCheck
- Check Point MultiSpect
- ネットワークの全域を保護
- ポリシーの集中管理
- 迅速かつ柔軟な導入展開



Check Point MultiSpect™

革新的なデータ分類エンジンであるMultiSpectは、ユーザ、コンテンツ、およびプロセスを総合的に分析し、ポリシー違反かどうかを正確に判断します。DLP Software Bladeは、個人を特定可能な情報 (Personally Identifiable Information: PII) や法令遵守関連データ (HIPAA、SOX、PCI DSSなどが適用されるデータ)、機密性の高い企業データなどの重要情報を極めて正確に識別できます。この機能は、次のような特徴を持つ強力な3層型の検査エンジンであるMultiSpect技術によって実現されます。

- 複数のパラメータに基づくデータの分類と相関分析および複数のプロトコルの検査とポリシーの実施: コンテンツ・フローを検査し、広く使用されているTCPプロトコル (SMTP、FTP、HTTP、Webメールなど) に対するポリシーの実施、パターン・マッチング、およびファイル分類を行って、ファイルの拡張子や圧縮の有無に関係なくコンテンツ・タイプを識別
- 機密性の高い形式を認識して保護: 事前定義のテンプレートに基づき、ファイルや形式のマッチングを実施
- 一般的ではないビジネス・コミュニケーションを識別: そのまま利用できるベスト・プラクティス・ポリシーを装備

さらに、カスタム・データ・タイプを作成できるオープンなスクリプト言語も用意されています。柔軟性に優れたチェック・ポイント独自の言語により、事実上あらゆる機密データの保護に対応できます。

ネットワークの全域を保護

チェック・ポイントのDLPソリューションは、インラインで動作するネットワーク・ベースのSoftware Bladeとして提供されており、チェック・ポイントのすべてのゲートウェイで動作します。先進の情報漏洩対策ソリューションであるDLP Software Bladeは、SMTPやHTTP、FTPを含む幅広いトラフィック転送タイプに対応し、アプリケーションを深いレベルで認識してネットワーク中を流れるデータを保護します。DLPポリシーでは、ポリシーやネットワーク・セグメント、ゲートウェイ、およびユーザ・グループの各単位で防止対象を定義できます。

ポリシーの集中管理

DLP Software Bladeは、チェック・ポイントのセキュリティ管理機能であるSecurity Management™の使いやすいインターフェースを使用して集中管理できます。管理インターフェース上からセキュリティ・ポリシーを強力に活用および制御できるほか、ユーザとグループの定義、ネットワーク・オブジェクト、アクセス権、およびセキュリティ・ポリシーをセキュリティ・インフラストラクチャ全体にわたって単一のリポジトリで管理できます。統一されたアクセス・ポリシーを分散環境全体で自動的に実施でき、場所を問わずセキュリティ管理へのアクセスを可能とします。

集中管理機能では、統一されたポリシーを複数のゲートウェイにわたって展開し、ポリシーごとに実施アクションを制御できます。実施アクションには、検知 (ログへの記録のみ) と隔離 (ユーザによるインシデント対応) があります。ポリシー管理には、次の機能とオプションが用意されています。

- データ・タイプとユーザ・グループの選択: Active Directoryを併用
- 例外の設定: 一部ユーザのみ許可
- トラフィックの転送: 発信トラフィックまたは部門間トラフィックに適用
- 事前定義されたポリシーとコンテンツ・データ・タイプ

- 特定のポリシーをユーザ・グループごとに段階的に実施
- ログインとイベント相関分析の統合
- 隔離のカスタマイズ
- きめ細かく設定できる保護機能: 使い勝手に優れた保護プロファイルを使用し、ネットワーク環境のセキュリティ要件に合わせてシグネチャや保護機能の有効化ルールを定義
- 事前定義されたデフォルト/推奨プロファイル: セキュリティまたはパフォーマンスが最適になるようにチューニングされたプロファイルを事前に用意



情報漏洩を防止するためのDLPルールは簡単に定義できます。

イベント管理

SmartEventを使用すると、膨大なイベントの中から真に重要なものだけを抽出して監視およびレポートできます。イベント管理には、次の機能とオプションが用意されています。

- DLPイベントのリアルタイム情報と履歴情報をグラフ化およびレポート
- 容易なインシデントの相関分析
- インシデントのタイムラインをグラフィカルに表示
- 容易に設定できるカスタム・ビュー
- イベントおよびインシデント管理のワークフロー

迅速かつ柔軟に導入

事前定義のテンプレートを適用すれば、どのような規模の組織でもすぐさま運用を開始できます。法令遵守、知的財産保護、利用規程など、一般的な要件に合わせた幅広いポリシーとルールがあらかじめ用意されています。

DLP Software Bladeは、チェック・ポイントのすべてのセキュリティ・ゲートウェイ (チェック・ポイント・アプライアンスまたはオープン・サーバプラットフォーム) にインストールできます。既存のセキュリティ・インフラストラクチャを活用して容易かつ迅速に導入できるため、時間とコストも節約できます。また、高機能で拡張性に優れたアプライアンス版のDLP-1も用意されており、あらゆるネットワーク・セキュリティ要件に対応することができます。



仕様

アプライアンスの技術仕様

		
パフォーマンス	DLP-1 2571	DLP-1 9571
ユーザ数	1,000	5,000
時間あたりのメッセージ数	70,000	350,000
スループット	700Mbps	2.5Gbps
インタフェース		
搭載インタフェース	1GbE Copper x 6	1GbE Copper x 10
オプション・インタフェース	Copperバイパス・カード (内蔵4ポート)	LOM (Out-of-Band Management)、 1 GbEファイバ2 x 4、1 GbE Copper 2 x 4、10 GbE 2 x 2、 Copperバイパス・カード (モジュラー4ポート)
ストレージ		
ディスク容量	500GB	2TB x 2 (ミラーリング - RAID 1)
ハードウェア仕様		
筐体デザイン (高さ)	1U	2U
寸法 (mm)	443 x 381 x 44mm	431 x 509.5 x 88mm
重量	6.5kg (14.3lbs)	16.5kg (36.3lbs)
電源		
ホットスワップ対応デュアル電源	No	Yes
電源	100 ~ 240V : 50 ~ 60Hz	
電源仕様 (最大)	250W	400W
消費電力 (最大)	77.5W	200.7W
使用環境	温度: 5°C~40°C、湿度: 10%~85% (結露なきこと)、高度: 2,500m	
適合規格	UL 60950; FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3AS/NZS 3548:1995; CNS 13438 Class A (検査合格、国家認証申請中); KN22KN61000-4 Series, TTA; IC-950; ROHS	

ソフトウェアの技術仕様

DLP Software Bladeは、Software Bladeアーキテクチャに基づくソフトウェア・ソリューションです。オープン・サーバへの導入に関しては、出荷済みおよび出荷前の各種ハードウェア・プラットフォームとの互換性がテストされています。詳細については、ハードウェア互換性リストをご覧ください。

DLP Software Bladeをインストールするための最小ハードウェア要件		
オープン・サーバでの推奨要件	1,000ユーザ未満	5,000ユーザ未満
CPUコア数	2	8
メモリ容量	4GB	4GB
ディスク容量	250GB	500GB
NIC数	2	2

技術仕様

検査	
検査オプション	<ul style="list-style-type: none"> • 250以上のデータ・コンテンツ・タイプを事前定義 • パターン、キーワード・マッチング、辞書 • 複数のパラメータに基づくデータの分類と相関分析 • 構造化コンテンツに基づく高度な検査 • 一般に使用されるテンプレートとの類似性を考慮 • ファイル属性に基づくマッチング • オープンなスクリプト言語を使用してデータ・タイプをカスタマイズおよび作成
ファイル・タイプ	600以上のファイル・タイプのコンテンツを検査
プロトコル	HTTP、SMTP、FTP
サポートする規制	PCI DSS、HIPAA、個人を特定可能な情報 (Personally Identifiable Information: PII) など
規制関連以外のデータ・タイプ	<ul style="list-style-type: none"> • 知的財産データ • 財務および法律関連の用語 • ナショナルIDの番号 • IBAN (International Bank Account Number)
複数言語のサポート	シングルバイトおよびダブルバイト・フォント (UTF-8) を含む複数言語のコンテンツの検知に対応
実施	
タイプ	<ul style="list-style-type: none"> • ユーザへの確認 (UserCheckを使用したエンドユーザ自身による防止) : 隔離のメッセージを表示、エンドユーザに通知を送信、エンドユーザ自身による是正を要請 • 防止: メッセージの送信をブロックし、エンドユーザに通知 • 検知: インシデントをログに記録
UserCheck	<ul style="list-style-type: none"> • ポリシー単位で有効化およびカスタマイズ。エンドユーザに対する通知は個別に編集可能 (複数言語に対応) • ユーザの自己学習: 同じメール・スレッドでインシデント処理が繰り返されることを防止 • 2種類の通知方法: 電子メールでの通知 (エージェントのインストールが不要)、システム・トレイでのポップアップ (シン・エージェントのインストールが必要)
実施機能	<ul style="list-style-type: none"> • ポリシーの例外の定義 (ユーザ、ユーザ・グループ、ネットワーク、プロトコル、データ・タイプ単位) • ポリシーに抵触する行為をデータ資産の所有者に通知 (財務関連の文書であればCFOなど) • すべてのインシデントをログに記録: オプションでイベントの相関分析と問題の監査が可能
インシデントの参照	DLP権限 (専用パスワード) を持つ管理者は送信された実際のメッセージを参照可能 (添付ファイルを含む)。メッセージが参照されるたびに監査ログを記録
すべての電子メールのログへの記録	すべての送信電子メール (問題のない電子メールを含む) について、送信者、受信者、件名を記録
ポリシー管理	
集中管理	<ul style="list-style-type: none"> • SmartDashboardと統合 • ポリシーを容易かつ直感的に作成 • データ・コンテンツ・タイプを容易に作成 • データ・コンテンツ・タイプの強力な分類と検索オプション
イベント管理	<ul style="list-style-type: none"> • SmartEventの統合機能を利用可能 • ログのレポートとタイムラインのリアルタイム監視 • ポリシー違反の分布をユーザまたはネットワークごとに円グラフで表示
導入	
インストール形態	<ul style="list-style-type: none"> • Software Blade (チェック・ポイントのすべてのセキュリティ・ゲートウェイで動作) • 専用アプライアンス
ネットワークへの導入形態	<ul style="list-style-type: none"> • インライン接続 • レイヤ2のミラー・ポート/SPANポートへの接続
インストール・ウィザード	DLP Software Bladeの初期導入をガイドするシンプルなウィザードにより、Active Directoryへの接続や必須の初期設定の変更などが可能

製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F

http://www.checkpoint.co.jp/ E-mail : info_jp@checkpoint.com Tel : 03(5367)2500