IMPERVA®

Imperva SecureSphere File Security

データシート

ランサムウェアや内部の脅威から非構造化データを保護する

ランサムウェアや内部の脅威から非構造化データを守る

Imperva SecureSphere File Firewallは、重要なファイルへのアクセスをリアルタイムでモニターし、不正なアクセスを阻止することで、非構造化データに対する最高レベルのセキュリティを確保します。これによりセキュリティ担当チームは、全てのファイルアクセスに関する監査証跡を使用した迅速なフォレンジック調査と報告書の作成が可能となります。またシステム管理者は、インタラクティブな監査分析によって詳細情報までドリルダウンを行い、疑わしい活動やドキュメント上の問題を特定することができます。SecureSphere File Firewallの業界最先端のセキュリティポリシーフレームワークにより、不正なファイルアクセスに警告を発信したり、アクセスを阻止することで、セキュリティレベルを次の高い段階へと引き上げることが可能となります。

2015年、およそ 40% の企業がランサムウェアの攻撃を受けています

出典： OSTERMAN RESEARCH

Imperva SecureSphere File Security製品

- 重要ファイルのセキュリティを確保し、データ漏洩による損害発生を防止
- ランサムウェア攻撃を即座に検知して阻止
- IT部門による迅速なセキュリティ インシデント対応を可能に
- 柔軟で詳細なレベルのセキュリティポリシーに立脚した、機密ファイルへのアクセス制限

発見次第ランサムウェアを阻止

リアルタイム ファイルアクセス
モニタリング ソリューションの主要機能:

- ユーザのファイルアクセスをリアルタイムでモニタリングして分析
- 誰が、どのファイルに、いつ、どこで、どのようにアクセスしたかを詳細なレベルで可視化
- 不審な動きを検知してアラートを発信
- 不正アクセスやランサムウェアによるアクセスを検知して阻止
- 分析機能によるセキュリティ インシデント調査の迅速化
- 最新の調査結果を基にランサムウェアの活動に対する理解を促進

Imperva File Securityの機能

リアルタイム モニタリングと監査機能

Imperva SecureSphere File Firewallは、ファイルサーバのパフォーマンスや可用性に影響を及ぼすことなく、全てのファイル操作をリアルタイムで継続的にモニターし、監査することができます。SecureSphereは、ユーザ名、アクセス対象ファイル、親ディレクトリ、アクセス時刻、アクセス操作内容などを含む詳細な監査証跡を生成します。特権ユーザの操作を含め、企業全体のあらゆるファイルに対する完全なアクセス記録を残すことで、セキュリティインシデントへの対応を加速し、シンプルなコンプライアンス対応プロセスを実現できます。また職務分離を適用することにより、監査証跡の安全性確保と信頼性の強化を図り、ロールベースのアクセスメカニズムによって、監査証跡の改変を許さない読み取り専用ビューの提供を可能にします。

ランサムウェアをリアルタイムで検知して阻止

ランサムウェアへの対応は時間との勝負です。ランサムウェアから企業を守るという際に、より効果的な方法があります。被害が広がる前にランサムウェアを検知し阻止するためのリアルタイムファイルモニタリングです。ファイルのアクセスパターンに基づいて、自動的にランサムウェアを検知し、ファイルを保護するためのポリシーを適用することで、このような活動を阻止します。

SecureSphere File Firewallは、短時間でのファイル上書きや、ファイル名変更の繰り返しなど、ランサムウェア特有の操作パターンを特定します。ソリューションには、ディセプションベースの検知機能が備えられており、ストレージシステムに戦略的に配置された隠しファイルを使って、攻撃初期段階でマルウェアを検知することができます。このような隠しファイルに対する全ての書き込み処理やファイル名変更が、感染ユーザやエンドポイントを自動的にブロックするためのトリガーとなります。

異常なアクティビティをリアルタイムで警告してブロック

Imperva SecureSphere File Securityソリューションは、異常なファイルアクセスが発生した場合、即座にそれを通知します。また、SecureSphere File Firewallは、予め定められた企業ポリシーから逸脱したアクセス行為を警告することで、ネイティブファイルへのアクセス権限を強化します。さらに、ポリシーベースのブロッキング機能を活用することで、ディレクトリやファイルレベルのアクセス権限における許可設定の誤りを排除することができます。

業界最先端のImpervaセキュリティポリシーフレームワークをベースとした、このような柔軟な対応によって、ファイルのメタデータ、組織の事情、アクセス状況などを加味したポリシーの作成が可能となり、システム管理者は、好ましくない活動を検知した場合、即座に対抗措置を講じることができます。

セキュリティインシデントの調査と対応

SecureSphereは、数クリックの操作で視覚的にデータにヘアクセスし、画面上で監査分析ができるようになっています。セキュリティ担当者は、この分析機能を利用してファイル操作に関する傾向、パターン、リスクなどを特定することができます。さらに、監査データに関するニア・リアルタイムの多次元ビューや、インタラクティブな監査分析によって、フォレンジック調査やおよびセキュリティインシデント特定作業の効率化を図ることが可能です。

デプロイメント

インラインまたはノン・インラインの柔軟なデプロイメントモードで、ネットワークに変更を加えることなく、ファイルサーバやNASデバイス、アプリケーション、そしてクライアントをインストールすることが可能です。

- **ノン・インラインネットワークモニタリング**
  パフォーマンスや可用性に何らの影響を与えずに活動をモニタリング
- **透過型インラインプロテクション**
  容易なデプロイメントと業界最先端のパフォーマンスで、プロアクティブにセキュリティを確保

グラフィカルなレポートでセキュリティイベントを迅速かつ効率的に文書化

SecureSphereは、機能豊富なグラフィカルレポートを提供してリスクを計測し、SOX、PCI、HIPPAや個人情報保護法などの規則に従ったドキュメントを作成することができます。対象レポートはオンデマンドでも、定期的なスケジュールに従った形でも作成することができます。リアルタイムなダッシュボードには、ハイレベルなセキュリティイベントやシステムステータスが表示されます。SecureSphereのレポーティングプラットフォームは、セキュリティやコンプライアンス、ユーザ権限管理上の問題などを即座に可視化します。

インサイダーの脅威からファイルを保護

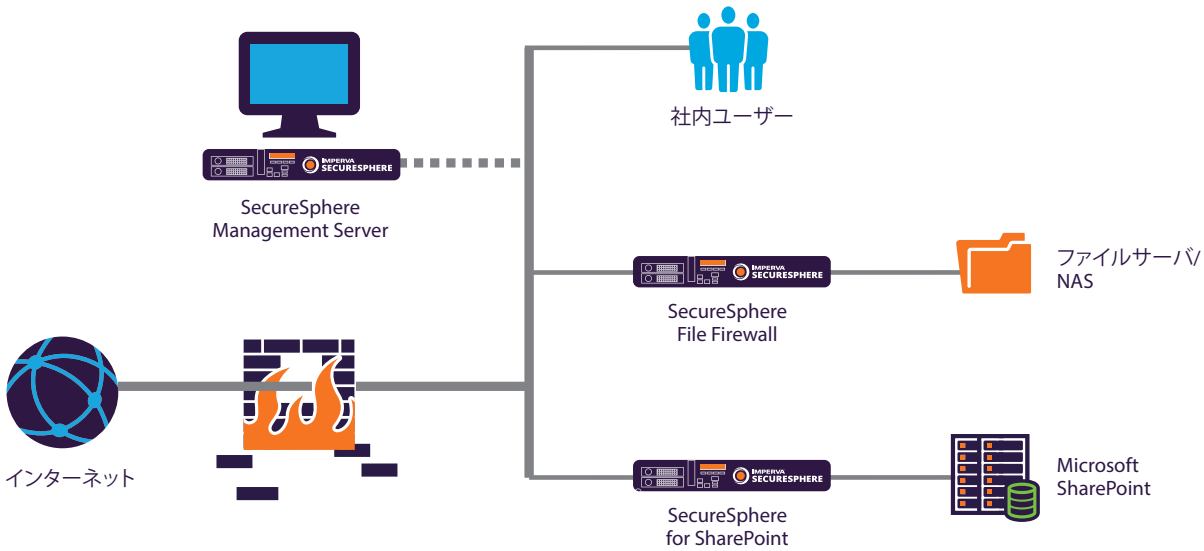
企業のデータは、感染や不用意な対応、不正なインサイダーなどによって、常に盗難の危険にさらされています。たった一人の好奇心によって、知的財産や財務データ、ビジネスプランなど重要な業務データが危険にさらされることになります。.

インサイダーの脅威によるデータの盗難や喪失を防ぐため、Imperva CounterBreachソリューションでは、高度な機械学習テクノロジーを活用し、企業内で共有されているデータやSaaSアプリケーション、データベースなどを保護します。

CounterBreachは、ユーザの通常のファイルアクセスパターンを動的に学習して、不適切または不正なアクセスを特定し、ITチームに対して危険な活動をプロアクティブに警告します。

Imperva SecureSphere サイバーセキュリティ

Imperva SecureSphereは、SecureSphere Web、DatabaseおよびFile Securityを含む包括的で総合的なセキュリティプラットフォームです。Imperva SecureSphereは、どんなに大規模な企業の場合でも、そのサイバーセキュリティの要求に応じて拡張することが可能です。また、進化し続ける脅威に対して、最先端の防御機能が維持できるよう、世界屈指のセキュリティ調査組織であるImperva Defense Centerが、製品に対するサポートを提供しています。



株式会社 Imperva Japan

www.imperva.jp
Mail：FM-Japan@imperva.com
TEL：03-6263-0671