IMPERVA®

Imperva SecureSphere Data Security

データシート

機密データの保護と監査

接続性とインターネット・アクセスの容易性によって、サイバー犯罪は完全にその姿を進化させました。その結果、機密データを保護する責任に対する顧客、企業、政府の見方が変化しています。実際にかかる調査コスト、コンプライアンスに関する罰金、ブランド・イメージの低下の可能性に加えて、新しい懸念も生み出されています。最近の控訴裁判所の判決で「顧客の損害」の定義に変化がありました[1]。個人を特定できるデータを漏えいによって盗まれた顧客に対して集団代表訴訟の形をとることが認められたのです。データ損失のインシデントを起こした企業の債務は、損害の定義が広義になり、訴訟費用や調停金が膨らむにつれ、膨大になっていく可能性があります。

クラス最高のデータ保護と監査

Imperva は、クラウドおよびオンプレミスの機密ビジネス・データとアプリケーションを安全に保護するのに最適な製品です。SecureSphere データ保護ソリューションは、パフォーマンスや可用性に影響を与えない業界最高のデータベース監査およびリアルタイム保護により、データベースのセキュリティおよびコンプライアンスのあらゆる側面に対応しています。SecureSphere は多階層のアーキテクチャをとるため、拡張して、最大規模のデータベースおよびビッグ・データのインストールをもサポートすることができます。セキュリティとコンプライアンスを自動化できるため、幾千もの企業が最も大切な資産を保護するために Imperva SecureSphere を選択したのは自然の流れといえます。

データ損失のインシデントを起こした企業の債務は、訴訟費用や調停金が膨らむにつれ、膨大になっていく可能性があります。

[1] 第7巡回控訴裁判所、Diane Wood判事、ニーマン・マーカスのデータ漏えいに関して原告が勝訴

Imperva SecureSphere for Data

- 機密データベースを検出し、分類を支援
- 過剰なユーザ権限および使用されていないユーザを特定し、完全な権限レビュー・サイクルを実現
- RDBMS、データ・ウェアハウス、ビッグ・データ・プラットフォーム、メインフレーム・データベースを保護
- データベース攻撃および許可されない活動をリアルタイムに警告、隔離、またはブロック
- コンプライアンスに関するタスクとレポート作成を自動化およびスケジュール化

ソースでのデータ保護

コンプライアンスに対応した、SecureSphere のデータ・セキュリティ監視と独立した監査ログ

- すべての活動のセキュリティ違反を監視しながらも、必要な活動だけをログに記録
- トランザクションの多いデータベースを監視および保護
- 疑わしい動作があったときにそれをブロックし、コンテキスト内で調査
- マルチアクション・セキュリティ・アラートを実行し、ボトルネックと遅延を排除
- SecureSphere Web Application Firewall を使用したインターロック・データベース保護、アカウントテイクオーバープロテクション、およびマルウェア防御による、マルチ対策のデータ・セキュリティ

コンプライアンス要件に対応

SecureSphere は、企業が PCI DSS、SOX、My Number、HIPAA などのコンプライアンス規制に対応するのを支援します。

- 事前定義のポリシーとレポートを使用して、データベースの実質上すべてのコンプライアンスに対応
- DBA を必要とせず、新規および変更されたポリシーを迅速に設定および導入
- 不正開封防止の監査データと職務の分離を実現
- 進化する IT 環境とコンプライアンス要件に対応する柔軟性と応答性

データ保護と監査は全社での必須事項

ハッカーやデータ摂取者は企業内のデータ・セキュリティやコンプライアンスの「所有者」が誰であるかなど気にも留めません。彼らの意図は、自分たちの利益のためにデータを盗むことだけです。多方向からの攻撃は、彼らがチームとシステム･サイロを活用してセキュリティを回避できることを示しています。DDoS 攻撃で注意をそらし、同時に多方向からの攻撃により、スピア・フィッシング電子メールやマルウェア経由で取得したユーザ認証情報を使用して何千ものデータ・レコードを盗みます。データ盗難を防ぐのは、手動の監視やスタンドアロンのセキュリティ対策では無理です。相関セキュリティ・ダッシュボードは役に立ちますが、システムにアラートが大量にあふれたら､「真の」攻撃は数週間以上も気づかれずに放置される可能性があります。データ・レベルで導入される積極的なセキュリティ監視が、進行中のデータ攻撃を防御する最後の機会です。これを Web アプリケーション・ファイアウォール、マルウェア対策ソリューション、およびその他のセキュリティ対策と統合すれば、企業がデータを安全に保管できる可能性は高まります。データ盗難は食い止められ、IT チーム、セキュリティ・チーム、コンプライアンス・チームは、データを安全に保管するという共通の目標を達成し、それをコンプライアンスの要件と規制を遵守しながら行っていることを実証できます。

SecureSphere Database Assessment は機密データの場所を特定し、企業がリスク軽減プログラム、システム、およびポリシーを計画するのに役立つ、リスクに基づく優先順位を提供します。

Imperva データ・セキュリティ機能

データ・セキュリティはデータの検出から始まる

データの保護と監視には、機密データの検出と分類が必要です。小規模な企業ではこれは手動による調査とレビューで達成できるでしょうが、企業の規模が大きくなるにつれ、データベースの数も飛躍的に増加します。今までに知られていなかった機密データを含む新規または変更されたデータベース・インスタンスを、定期的および継続的に検出し分類する唯一の確かな方法は、検出と分類を自動化することです。SecureSphere Database Assessment は機密データの場所を特定し、企業がリスク軽減プログラム、システム、およびポリシーを計画するのに役立つ、リスクに基づく優先順位を提供します。

機密データの使用状況に関する継続的な監視

データベース・トラフィックが大量でも、SecureSphere はすべてのトラフィックを同時に監視して、セキュリティ・ポリシー違反を検出し、コンプライアンス・ポリシー遵守の目的を達成します。個々の目的に応じた非常に効率的な監視機能により、企業は単一の統合ソリューションでセキュリティ要件とコンプライアンス要件の両方に対処できます。

SecureSphere は、すべてのデータベース活動をリアルタイムで分析することにより、予防措置的なセキュリティ施行レイヤと、各トランザクションに対する「誰が」、「何を」、「いつ」、「どこで」、「どのように」という情報を示す詳細な監査証跡を企業に提供します。SecureSphere は、データベース・サーバに直接アクセスできる特権ユーザや、ブラウザ、モバイル、デスクトップ型アプリケーションを使用してデータベースにアクセスするユーザを監査します。

ビッグ・データ、SharePoint、ファイル・ストアの監視

データベースがサイバー犯罪者の主なターゲットであり続ける一方、機密データは企業全体のさまざまな種類のシステム内に存在します。SecureSphere は、データベース、ビッグ・データ、SharePoint、およびファイル・ストア全体に対する統一ポリシーの導入と監視という、最も困難な側面を自動化します。

- SecureSphere Agent for Big Data は、MongoDB、Cloudera、IBM BigInsights、Hortonworks の各製品を含む主要なビッグ・データ製品に SecureSphere Data Activity Monitor を拡張します。
- SecureSphere ファイル・セキュリティ製品は、SharePoint、ファイル・サーバ、NAS（ネットワーク接続ストレージ）デバイスに保存されているファイルに対し、リアルタイムなファイル・モニタリング、監査、セキュリティ、およびユーザ権限管理を実現します。

DBA の関与を必要としたり、高額な専門サービスの利用を必要とするソリューションとは異なり、SecureSphere は、何千ものデータベース、ビッグ・データ・ノード、およびファイルを管理するために必要な管理機能および一元化機能を提供します。

許可されないアクセスや不正な活動の検出

SecureSphere は、Imperva の特許取得済みの Dynamic Learning Method (DLM) と Adaptive Normal Behavior Profile (NBP) 技術を使用して、ユーザの通常のデータ・アクセス・パターンを特定します。この技術では、DML、DDL、DCL、読み取り専用活動（SELECT）、保存された手順の使用などあらゆるユーザ活動に対して基準を確立します。SecureSphere は、ユーザが予期しないクエリを実行した場合に実質的相違を検出し、調査のためのアクションやブロックのアクションを引き起こします。

マルチアクション・アラート、一時隔離、および (適切な場合は) 許可されない活動をブロックすることによって、ユーザのアカウントを無効にせずにデータを保護でき、重要なビジネス・プロセスにおける中断の可能性を回避します。自動化された修復ワークフローによってマルチアクション・セキュリティ・アラートが動作し、Splunk、SIEM、チケット・システム、または他のサードパーティ製ソリューションに情報が送信され、より広範な調査プロセスの効率化が実現します。

統一ポリシーの導入と施行

SecureSphere のもうひとつの利点は、主題に対する専門知識が組み込まれていることです。多くの組織では、洗練されたデータ中心のセキュリティおよび監査システムを導入および運用するのに必要な一連のスキルを備えた社内のリソースを確保するのに苦労しています。アクセス制御と監査プロセスをうまく導入するには、そのようなリソースを繰り返し活用できる必要があります。様々なシステムの監査と評価を一元的に管理することで、これらの管理を簡素化できます。一方、自動化によって、コンプライアンスを維持するために必要なリソースの数が減り、投資収益率が改善します。

DBA の関与を必要としたり、高額な専門サービスの利用を必要とするソリューションとは異なり、SecureSphere は、何千ものデータベース、ビッグ・データ・ノード、およびファイルを管理するために必要な管理機能および一元化機能を提供します。事前定義のポリシー、修正ワークフロー、および多数のレポートが用意されているため、SQL スクリプトやコンプライアンスに関する専門知識の必要性が大幅に低下します。継続的な DBA の関与の必要性を排除することで、職務の分離要件においてコンプライアンスを満たします。すぐに使用できるプロセス API、管理コンソール、ワークフロー、レポート、分析ツールを活用することによって、既存の人員でシステムを導入し、管理できます。

効率化されたコンプライアンス・レポート

Imperva SecureSphere には、クライアントから最も頻繁に要求されるニーズに対処する事前定義のレポートが多数用意されています。さらに、企業が固有のレポート要件を満たせるよう、カスタム・レポート・ライタも用意されています。埋め込みのワークフローと自動化により、コンプライアンス・タスクとレポート作成がデータ・セット全体で確実に行われます。

リアルタイムに攻撃を防ぐことが、ハッカーがデータを盗むのを回避できる唯一の効果的な方法です。SecureSphere DAM はすべてのトラフィックを監視して、セキュリティ・ポリシー違反、プロトコルおよび OS レベルでの攻撃、および許可されていない SQL 活動を検出します。

複数のデータベースを対象とする効果的なユーザ権限管理

ほぼすべての規制には、機密データに対するユーザ権限を管理する要件があります。これらの要件を遵守する作業は、企業が大規模なデータ・セット全体に対して手動で実行する必要があるため、最も困難なタスクの 1 つです。SecureSphere は、様々なデータ・ストア全体のユーザ権限を自動的に集計して、過剰なユーザ権限を排除するための自動アクセス権レビュー・プロセスの設定を支援します。これは、SOX や PCI DSS などの規制への遵守を定期的に実証するのを促進します。これらの日常的でありながら重要なタスクを自動化すれば、人件費を節約し、エラーやレポートの欠落を軽減できます。

SQL インジェクション、DoS その他のリアルタイム・ブロック

リアルタイムに攻撃を防ぐことが、ハッカーがデータを盗むのを回避できる唯一の効果的な方法です。SecureSphere はすべてのトラフィックを監視して、セキュリティ・ポリシー違反、プロトコルおよび OS レベルでの攻撃、および許可されていない SQL 活動を検出します。非常に効率的な監視によって、アカウント全体を無効にしてビジネスを中断させることなく、活動の隔離、ユーザ権限認証の保留、または活動のブロックを行います。

ブロックはデータベース・エージェントとネットワーク・レベルの両方で可能で、重要な大量トランザクションのデータベース上のパフォーマンスのニーズと安全のニーズとのバランスを図れるよう、セキュリティ・プロファイルを微調整できます。

積極的なセキュリティを真に向上させるには、SecureSphere データ・ソリューションと同じアーキテクチャおよび管理プラットフォームを活用する Imperva SecureSphere Web Application Firewall を導入をご検討ください。さらにマルウェア防御、SIEM、その他の専門のセキュリティ・システムと統合すれば、組織はプロセスを調整し、セキュリティの抜け道を埋めることができます。

インシデント調査およびフォレンジックのための監査分析

Imperva SecureSphere は、調査中にセキュリティ、コンプライアンス、リーガルチームのために点をつなぎ合わせながらも独立した機能運用を可能にする統合ソリューションを提供します。Imperva は履歴データとリアルタイム・データの両方へのアクセスを提供しながら、インシデント応答チームに実行中の活動に対する正確でコンテキストに応じた可視性を提供します。リアルタイムの機能性、ユーザ・トラッキング、修復ワークフロー、SecureSphere WAF との相関、多数の事前定義のコンプライアンスおよびフォレンジック・レポートは、すべて Imperva の重要な差別化要因です。

導入と設定の自動化は、短期間で価値を実現するための主要な要因です。

ある Imperva のお客様は、自動化ツールを使用して、わずか数か月で 69,000 以上のデータベースへの導入を完了しました。

Impervaのエンタープライズ・レベルの即応力

規模に応じて予測可能なパフォーマンス

Imperva は非常に効率的な監査ログ技術を使用して他に類を見ない拡張性を実現します。SQL データベースに依存したデータ監視ストレージを使用する競合他社のソリューションとは異なり、Imperva は技術的に進歩した多くのビッグ・データ分析ソリューションに見られる技法を活用しています。Imperva はその高速な書き込みとさらに高速な読み込み能力によって、競合他社製品をはるかに上回る拡張性を実現し、市場において独自のメリットを提供しています。

監査のためにさまざまな活動を監視してログに記録しながら、すべての活動のセキュリティ・ポリシー違反を監視するよう設定できます。

SecureSphere は、ソリューションに組み込まれたアクティブな冗長性を使用して単一障害点を排除することで、高可用性を実現します。SecureSphere は、最先端のインテリジェントな高可用性機能を実装します。これには、障害のないデータ保護プログラムおよび中断のない監査ログを維持できるように自身でバランスを取って移動するエージェントなど、強力な新機能が含まれます。

迅速な導入

Imperva は、コマンドを提供し、グローバル・レベルで制御可能な一元管理コンソールを使用して、企業の包括的なビューを取得します。最上位レベルの管理コンソールは、グローバル・ポリシーの迅速な導入と、データ分類などのタスクの自動化を可能にし、それによって実装までの時間をスピードアップします。

また、Imperva は IT プロビジョニングの価値を認識しており、シームレスなソフトウェア配布、設定アップデート、ポリシー配布、データ検出を促進する API セットを提供します。導入と設定の自動化は、短期間で価値を実現するための主要な要因です。例を挙げると、ある Imperva のお客様は、自動化ツールを使用して、わずか数か月で 69, 000 以上のデータベースへの導入を完了しました。

ハイブリッドな監視

Imperva は、すべてのデータベース・サーバにおいてエージェントが必要な一般的な導入シナリオをすべて網羅しています。SecureSphere は、ローカル・エージェント、ネットワーク・トランスペアレント・ブリッジ・オプション、ノンインライン・スニファ・モードを含む複数の導入方法をサポートしています。これらの導入方法を組み合わせて用いることで、企業は単一の「汎用」モデルに縛られることなく、さまざまなニーズを満たすことができます。

Imperva には環境を調べてそれを既知の脆弱性と照合する機能があり、どのデータがリスクにさらされているかを明確に示すことができます。

クラウド対応

Imperva SecureSphere for AWS は、世界で最も信頼性および拡張性の高いデータ保護および監査ソリューションのセキュリティおよびコンプライアンス機能を、Amazon Web Services 環境に拡張します。SecureSphere は、AWS で使用できる唯一のエンタープライズ・レベルのデータ保護およびコンプライアンス・ソリューションです。AWS でネイティブに実行される SecureSphere の BYOL バージョンは、オンプレミス・バージョンと同じ業界最先端の機能を活用します。AWS 環境にいずれかの SecureSphere ソリューション (DBF、DAM、または WAF) を導入するクライアントは、オプションで Imperva SkyFence を有効にして、Office 365 や AWS Management Console などのクラウドベースの Web アプリケーションを保護することができます。

データベースの脆弱性を評価し、仮想パッチを適用

企業データが世界中のさまざまなデータベースに保存されており、それぞれのリリースやパッチ・レベルが異なる可能性がある場合、既知の脆弱性を探し出す簡単な方法を持っていることが不可欠です。Imperva には環境を調べてそれを既知の脆弱性と照合する機能があり、どのデータがリスクにさらされているかを明確に示すことができます。SecureSphere の仮想パッチは、特に、既知でありながらパッチが適用されていない脆弱性を悪用する試みをブロックします。仮想パッチは、攻撃にさらされる期間を最小限に短縮し、データベース・パッチのテストおよび導入中にデータが漏えいするリスクを大幅に削減するのに役立ちます。

短期間で価値を実現

柔軟性に優れた SecureSphere アーキテクチャは、既存の環境における中断を回避しながら成長を促進し、企業はより短い期間でより多くのことができます。Imperva は、効率的で予測可能なエンタープライズ・スケーラビリティを実現します。最近、フォーチュン 500 に名を連ねる大企業が Imperva に移行しました。移行理由は、既存のソリューションでは将来の計画や予算作成に不安があったためです。Imperva に移行したことで、この企業は、フットプリントの監視コストおよび運用コストを大幅に削減できただけでなく、将来の成長を正確に計画し、予算を見積もることが可能となりました。

Imperva SecureSphere のサイバー・セキュリティ

Imperva SecureSphere は、SecureSphere Web、Database and File Security を含む、包括的で統合されたセキュリティ・プラットフォームです。大企業のデータセンタのセキュリティ要求にも応えられるよう拡張でき、ますます高まる脅威に対して製品の最先端の防衛を行っているワールドクラスのセキュリティ研究機関である Imperva アプリケーション・ディフェンス・センタによって支援されています。

IMPERVA SECURESPHERE

	SECURESPHERE DATABASE FIREWALL (DBF)	SECURESPHERE DATABASE ACTIVITY MONITORING (DAM)	SECURESPHERE DATABASE ASSESSMENT (DAS)
検出および分類	○	○	○
監視および監査ログ	○	○	-
リアルタイムのブロック	○	×	-
脆弱性診断[1]	○	○	○
データベース・エージェント[1]	○	○	-
ゲートウェイ・クラスタ	オプション	オプション	-
ビッグ・データ監視	オプション	オプション	-
ユーザ権限管理[2]	オプション	オプション	オプション[3]
拡張アプリケーション特定サービス (Oracle、EBS、SAP、Peoplesoft)	オプション	オプション	-
High Availability for Mangement Server (MX)	オプション	オプション	-
Amazon Web Services (AWS) BYOL での使用[4]	○	○	-

[1] 数はアプライアンスの購入内容に応じて異なります。詳細は、SecureSphereアプライアンス・データシートをご覧ください。

[2] ビッグ・データ・ノードではユーザ権限監視は利用できません。

[3] DASをスタンドアロンとして導入した場合、監査ログ詳細を必要とする機能は使用できません。

[4] AWS環境では一部のオプションが利用できません。

DS-SECURESPHERE-DATBASE-SECURITY-A4-1015-rev1