imperva

DATASHEET

Imperva Database Security

データコンプライアンスの作業をシンプル化し、情報漏洩を阻止

ビジネスの価値を高めるために、より多くのデータが利活用され、今日のデジタル経済と知識経済は、データの爆発的な増大の要因となっています。そこで、企業のデータとビジネスを保護するには、データ保護中心のアプローチを採用した、コンプライアンス/セキュリティ・ソリューションが必要です。Imperva Database Securityは、コンプライアンス違反やセキュリティ侵害のインシデントのリスクを軽減することで、企業によるデータの有効的な利活用をサポートします。

データリスクのより効果的な管理方法

大規模エンタープライズにとって、データのコンプライアンスとセキュリティの確保は複雑かつ困難な作業です。プラットフォームの急速な変化や、セキュリティ・リソースの不足により、自前での対応を続けることはほぼ不可能です。また、複数のセキュリティ・ツールから大量のアラートが発信される結果、セキュリティ担当者にとっては大きな負担となるケースも往々にしてあります。

Impervaの自動化ソリューションは、コンプライアンス・プロセスを合理化し、深刻な事態に陥る前にデータリスクを特定することで、セキュリティ担当者をサポートします。Imperva Database Securityを使用すれば、最重要資産を広範囲、かつ確実に防御することが可能です。

大規模かつ複雑なエンタープライズ・データベース環境を対象に、監査とセキュリティ・コントロールを標準化することで、Impervaはオンプレミス、クラウド、マルチクラウドの環境で機密情報に対するリスクを軽減します。

Impervaのリスクベース分析機能は、誤検知を排除し、最重要問題の優先順位を明確に決定することで、限られたセキュリティ担当者をサポートし、高リスクまたは疑わしい行動のより効果的な検知を可能にします。

主な特長とメリット

データサイエンス、機械学習、行動分析を通じ、データの脅威を検知し、優先順位を決定

特権ユーザーを含むすべてのユーザーを対象に、高リスクのデータアクセス・アクティビティを特定

すべてのデータベース・アクティビティの監視・監査を通じ、可視性を獲得

リアルタイムでのアラート発信や、ポリシー違反ユーザーのアクセスブロックにより、データを保護

データの発見、分類、脆弱性評価を通じ、隠れたリスクを特定

静的データのマスキングを通じ、攻撃対象領域を低減

可視性を獲得し、脆弱性を修正

すべての機密情報の保存場所や、情報漏洩の有無について、多くの企業は把握できていないのが現状です。こうした盲点は、ケアレスミスを伴うセキュリティリスクの要因となるほか、隠れた脆弱性やデータベースの構成ミスなどにより、攻撃者による悪用の機会にもなりえます。Imperva Database Securityは、機密情報を探し、情報漏洩へとつながる可能性のある脆弱性を特定することで、企業によるコンプライアンス違反と不正アクセスのリスク軽減をサポートします。

Imperva Database Securityは、ネットワークとクラウド上にあるデータベースを自動的に発見します。こうしたプロセスでは、ディクショナリやパターンマッチングなど、さまざまな手法を用いることで機密情報を自動的に特定・分類できます。

Impervaの脆弱性評価機能は、CISやDISA STIGのベンチマークに準拠した、1,500件以上の事前定義済みの脆弱性試験によってデータベースのスキャンを行い、企業のデータベースを最新の脅威から保護し続けます。

実用的な洞察を通じ、より効果的な業務遂行を実現

Imperva Database Securityには、先進的なデータリスク分析機能が採用されており、すべてのデータベース・サーバーを対象に、ユーザーのデータアクセス・アクティビティの経時的な相関関係を示します。

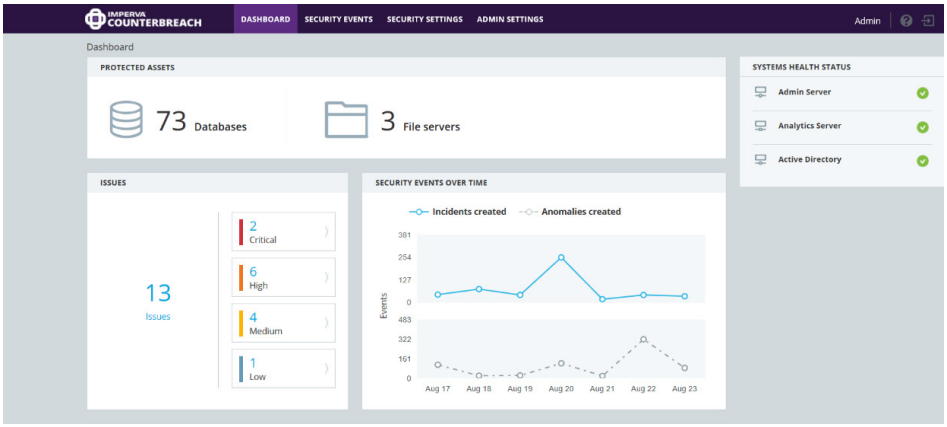

図2：分かりやすいダッシュボードを通じ、セキュリティ・プロフェッショナルは、少数の高リスク・インシデントに集中可能

これにより、回避的な行動であっても、高リスクまたは悪意の可能性のあるデータアクセス行動を特定できます。フラグの設定されたすべてのインシデントは、カテゴリー別にラベリングされ、一連のリスク指標によってスコアが計算され、優先順位が決定されます。インシデントは平易な言語で説明されるため、セキュリティチームは容易な対応が可能です（図3を参照）。

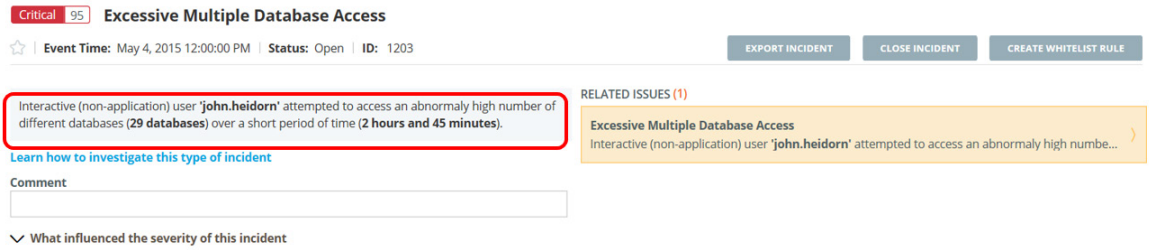

図3：各インシデントには、リスクスコアが割り当てられ、関連インシデント別にグループ化されるため、セキュリティ・プロフェッショナルは実用的な洞察による迅速な対応が可能

リアルタイムの保護

Imperva Database Securityは、異種混合のデータ環境を対象に、コンプライアンスポリシーとセキュリティポリシーを施行します。PCI、GDPR、CCPAなどの幅広い規制に対応した、初期設定不要、あるいはテンプレート化されたセキュリティポリシーにより、個人を特定可能な情報（PII）などの機密情報は、限定的なアクセス制御下に置かれるか、あるいは境界内に封じ込められます。専門的な要件に合わせ、カスタマイズされたポリシーを作成することも可能です。Imperva Database Securityはデータ中心型のソリューションであり、データベース自身に対してセキュリティの障壁を作ることで、SQL命令での脅威や攻撃を探し出します。脅威が検知されると、フラグを設定し、アラートを作成してから、必要に応じて、攻撃的なデータアクセスの試みをブロック（終了）します。

継続的な監視

企業データの保護に関しては、暗号化やロールベースのアクセス制御のみに頼るべきではありません。情報漏洩のリスクを軽減するには、データにアクセスする人物、データの内容、データアクセス・アクティビティの善悪に対する継続的な可視性が求められます。

Imperva Database Securityの継続的な監視機能は、アプリケーションと特権ユーザーのアカウントの両方を対象に、あらゆるデータベース・アクティビティのキャプチャと分析を行い、詳細な監査証跡を提供することで、データにアクセスする人物、データの内容、時期、データに対するアクションを示します。

さらに、多様なオンプレミス・プラットフォームの監査を一元管理することで、リレーショナルデータベース、NoSQLデータベース、メインフレーム、ビッグデータ・プラットフォーム、データウェアハウスを監視します。このほか、Azure SQLやAmazon Relational Database Services（RDS）などのPaaS製品を含む、Microsoft AzureとAmazon Web Services（AWS）でホストされるデータベースもサポートします。詳細なデータ・アクティビティは自動でキャプチャされるため、監査要求は容易に行なえます。

開発・テスト段階でリスクを軽減

企業が保有データの価値を活用しようとする場合、開発、試験、研究、分析、アウトソーシングなどの非本番環境向けに、本番データの複製が作成されます。業界アナリストによると、企業の82%は、各本番データベースについて、10件以上の複製を所有していると推定されます[1]。このように非本番環境で機密情報が広く利用される状況では、情報漏洩やコンプライアンスのリスクは大幅に拡大します。

Imperva Database Securityのマスキング機能は、事前の制御を行うことで、開発プロセスの遅延を招くことなく、不要な漏洩から機密情報を保護します。さまざまな変換技術を駆使し、機密情報を含む実データを、架空でありながら高品質で、機能的・統計的にも正確な現実的データに置き換えることで、開発のシミュレーションや試験を行いつつ、リスクを回避できます。

ライセンスと導入の柔軟なオプション

Imperva FlexProtectは、エンタープライズ全体でデータセキュリティを実現するための、柔軟なライセンス・オプションです。単一のライセンスを採用することで、Imperva Database Securityの導入は、必要な時に、必要な形態で行えます。これにより、企業の保護は、使用するデバイスやサービスの数、場所、種類に関わらず行えます。FlexProtectは、クラウド、オンプレミス、ハイブリッドの構成に関わらず、企業のデータ保護をサポートします。

FlexProtectのメリット

- クラウド移行時の不確実性に伴うコストを削減
- クラウド内およびオンプレミスのインフラストラクチャの経時的な変更に伴うコストも予測
- ビジネス規模の変化に応じた柔軟な対応

Impervaは、アナリストに支持される**サイバーセキュリティのリーダー**として、保存場所を問わず、あらゆる**データとアプリケーションのセキュリティ保護**に取り組んでいます。

[1]Copy Data Management report, IDC, April 2016

imperva.com
03-6263-0671