imperva

データシート

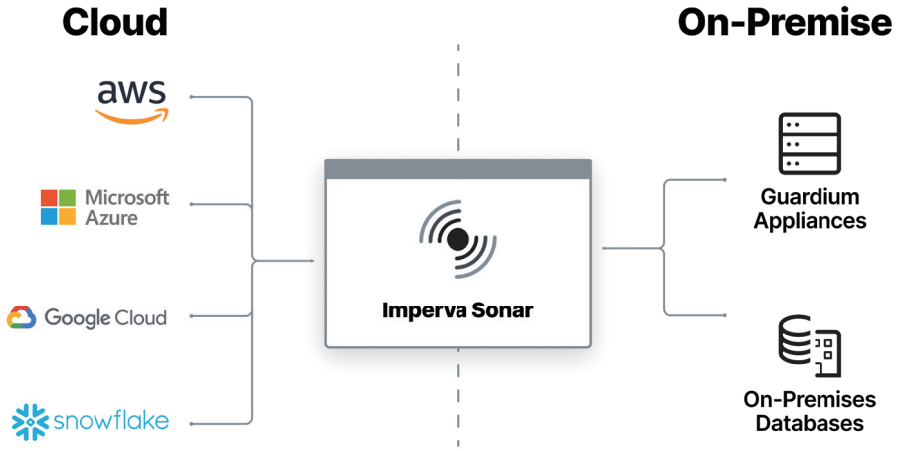
Imperva SonarによるGuardiumの最新化

重要な監視に関わるギャップの解消、複雑さとコスト削減によって、Guardium におけるセキュリティやコンプライアンスを大幅に改善

昨今、データセキュリティやコンプライアンスに求められるレベルが非常に高くなっており、Guardium Database Activity Monitoring (DAM) プログラムの対応力も限界を迎えつつあります。Imperva Sonar を使うことで、管理対象とするデータベースを増やせる上、手作業や運用コストを削減し、ガバナンスの有効性を向上させ、Guardium への投資を有効に活かすことができます。Imperva Sonar は、Guardium の設計者によって作られました。そのため、Guardium のコンプライアンス機能とシームレスに統合し、最新の技術環境におけるデータリスクを積極的に管理する能力をアップグレードすることが可能です。Imperva Sonar プラットフォームはデータベースのワークロードを安全にクラウドへ移行する最速の手段であり、監視機能を維持しながら、コンプライアンスとセキュリティの管理を新たなユースケースや要件に対応させることができます。

Imperva Sonar によって、Guardium 利用者はクラウドを含む企業全体の管理が可能に

Imperva Sonar は、データがホストされている場所に関係なく、すべてのデータ資産を単一のエンタープライズビューで表示します。Imperva Sonar を使用すると、クラウドやハイブリッドクラウド環境、さらには複数のクラウドに対してデータベースセキュリティを容易に拡張させることができます。Imperva Sonar は、ハイブリッドクラウドコンピューティングの要求に応えるために、ゼロから構築された製品です。そのため、様々なディスカバリー、分類、DAM、ユーザー権限管理、脆弱性評価ツールのリスク指標がシームレスに統合され、企業全体のデータベースにわたるリスク管理を効果的に行うことができます。



企業全体の管理を一元化。オンプレミスでもクラウド内でも導入可能。

敏捷性、簡素化、拡張性

Imperva Sonar には、インフラストラクチャのフットプリントを削減しながら企業全体にデータ監視を拡張する機能があります。

さらに、監査データの収集と管理を合理化し、成果をもたらす作業により多くの時間を費やすことができます。一般的に、1 台のサーバで多くの Guardium アプライアンス（Aggregator など）が排除されることで、ストレージ効率が 30 倍に引きあがります。最終的には、単なるコンプライアンスレポートに代わって、ワールドクラスのセキュリティに必要な監査データやインサイトにコスト効率よくアクセスできるようになります。

あらゆるデータリポジトリをカバー

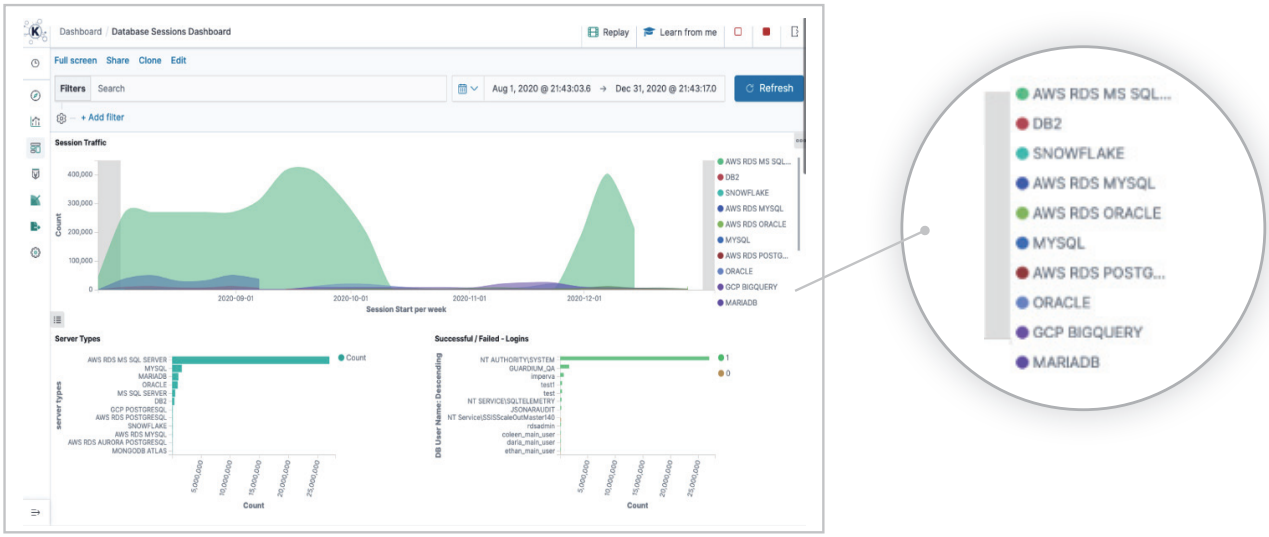
Imperva Sonar には、最新のデータベース機能が搭載されています。そのため、エージェントを介さなくてもデータ中心の全ワークロード均一かつ包括的にカバーすることが可能です。そして、AWS、Azure、Google Cloud、Snowflake、MongoDB Atlas といった主要なクラウドプロバイダーのサービスを含む、65 以上の最新データベースへの監視を広げることができます。さらに、サポートされていない新しいデータベースを見つけた場合は、最短 1 ヶ月でサポートの追加を行います。

自動的かつ長年にわたる監査データ保持

Imperva Sonar は、1 コアあたり 50,000 以上のイベントを自動的に統合、重複排除、圧縮するため、コスト効率よくデータを 1 か所に集め、長年にわたって保持することができます。また、数百テラバイトまで容易に拡張することが可能なため、単なるコンプライアンスの遵守に留まらず、堅牢なセキュリティやフォレンジック調査にも貢献します。さらに、このプラットフォームでは元から所有している費用対効果の高いストレージインフラ（AWS S3 や Azure Blob など、オンプレミスとクラウドの両方）を利用できるため、さらなるコスト削減が見込めます。

常に作動する監査データ

Imperva Sonar では、すべての監査データが「ライブ」状態です。そのため、ファイルのアーカイブにアクセスをしなくてもリアルタイムでデータを探索することができます。さらに、数年分の監査データに関して、フォレンジックレベルの検索を数秒で行うのに役立つ、インタラクティブなレポートやダッシュボードを提供します。



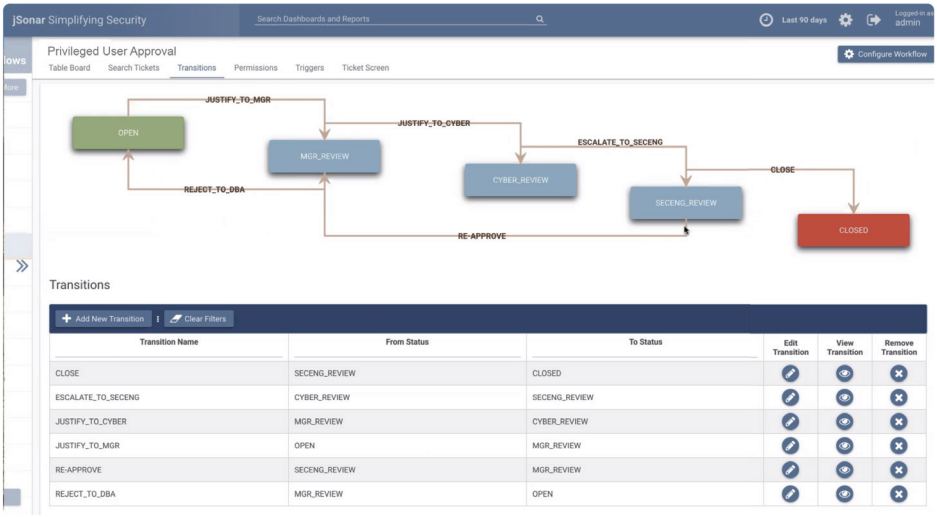
自動的にリテンション、レポート作成、フォレンジック調査を行い、数分で結果を得ることが可能。

大規模な統合レポート

Imperva Sonar のプラットフォームは、バッチ式のレポートシステムとは異なり、既存の Guardium コレクターを含むオンプレミスまたはクラウドのあらゆるソースから監査データを常時収集するため、手作業を必要とせずに数分で統合レポートを作成することができます。高速な読み取りによって、迅速な実行が可能になります。また、他のフォレンジックツール、レポーティングツール、ビジネスインテリジェンスツールと統合することで、セキュリティオペレーションセンター、データベース操作、リスクマネジメントといった他のチームが好みのツールを使用し、セルフサービスで安全なアクセスをすることも可能です。

包括的なワークフローの自動化

Imperva Sonar を使うと、レポーティングのサインオフ、エンタイトルメントのレビュー、変更要求の調整といった手動プロセスが Sonar プラットフォームから自動化され、何日もかかっていた作業が数分で終えられるようになります。組み込みのワークフローがマルチステップの操作を編成し、関係者にアクションを提示することで問題の早期解決につながるほか、見落としがなくなります。Imperva Sonar システムでは、単に Guardium レポートレベルのワークフローを使用するのではなく、イベントレベルのデータやメタデータ、さらには機械学習を組み込んで、効率化とより複雑なユースケースへの対応を可能にする高度な自動化プロセスを作成することができます。



ワークフローの自動化によって、手作業の排除、インシデント解決にかかる時間短縮が可能に。

高度かつリスクベースのセキュリティ分析

Imperva Sonar が提供するキャパシティやパフォーマンス、そして統一された監査データの基盤によって、データセキュリティへのアプローチを変えることができます。Imperva Sonar では、収集したすべての情報を用いて、専用のセキュリティ分析を行います。そのため、Guardium が見逃してしまうような、複雑もしくは回避的なユーザーのデータアクセス行動を検出することが可能になります。また、不適切な行動をとるユーザーや乗っ取られた可能性のあるアカウントの早期発見を行うほか、異常として Guardium に通知されるものの実際にはリスクではない要素をフィルタリングします。こういったインテリジェンスにより、データ保護の強化とプロアクティブなリスクマネジメントが可能となり、SOC やインシデント対応チームにかかるデータセキュリティの負担を最小限に抑えることができます。

以上、Imperva Sonar が Guardium ユーザーに提供する機能の一部をご紹介しました。
詳細については、Imperva の Guardium 専門家にご相談いただくか、imperva.com **にてデモをリクエストしてください。**