

Data Sheet

Modernize Guardium with Imperva Data Security Fabric

thalestct.com

THALES
Building a future we can all trust

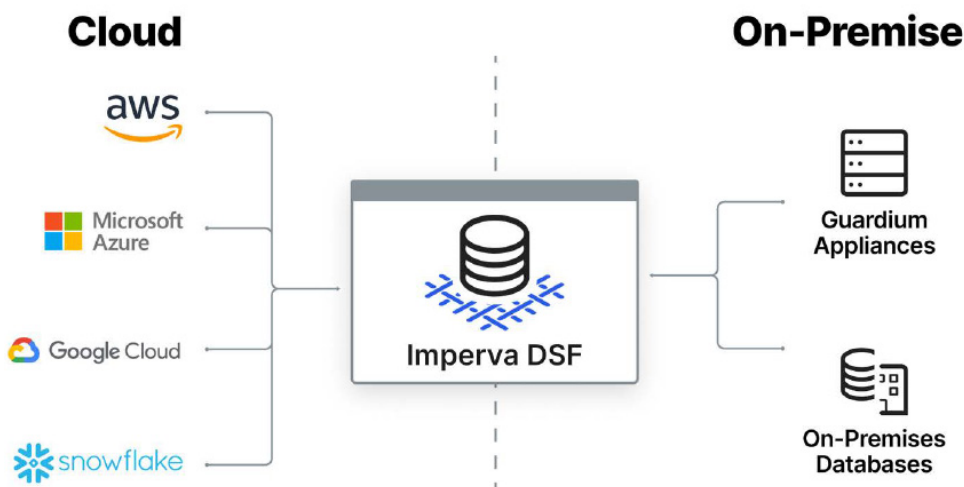
Close critical monitoring gaps, reduce complexity and cost, and significantly improve the security and compliance out-comes delivered by your Guardium solution

Contemporary demands for data security and compliance have likely pushed your Guardium Database Activity Monitoring (DAM) program to its limits. Imperva Data Security Fabric (DSF) protects your Guardium investment while extending coverage to more databases, reducing manual efforts and operational costs, and improving governance effectiveness. Imperva DSF was designed by the original architects of Guardium, so it seamlessly integrates with Guardium compliance features, while upgrading your capability to proactively manage data risk in a modern technology environment. Imperva Data Security Fabric is the fastest path for safely moving database workloads to the cloud, while preserving oversight, ensuring your compliance and security controls keep pace with new use cases and requirements.

Imperva DSF is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

With Imperva Data Security Fabric, Guardium customers gain full enterprise control - including cloud

Create a single enterprise view of all data assets, regardless of where they are hosted. Imperva DSF makes it easy to extend database security into the cloud, across hybrid cloud environments, and even across multiple clouds. It is purpose-built from the ground up for the demands of hybrid cloud computing. Imperva DSF seamlessly merges risk indicators from various Discovery, Classification, DAM, User Rights Management and Vulnerability Assessment tools in order to effectively manage database risk enterprise-wide



Centralized management enterprise wide. Can be deployed on-premise or in-cloud

Agility, simplification and scalability

Imperva DSF has the performance and capacity to extend data monitoring across your entire enterprise while reducing infrastructure footprint. Imperva DSF will streamline audit data collection and management and leave you more time to focus on delivering results. Typically, with a single server, you can eliminate many Guardium appliances (such as aggregators) and improve your storage efficiency by 30X. You will finally have cost-effective access to all the audit data and insights you need for world-class security instead of just compliance reporting.

Coverage of any data repository

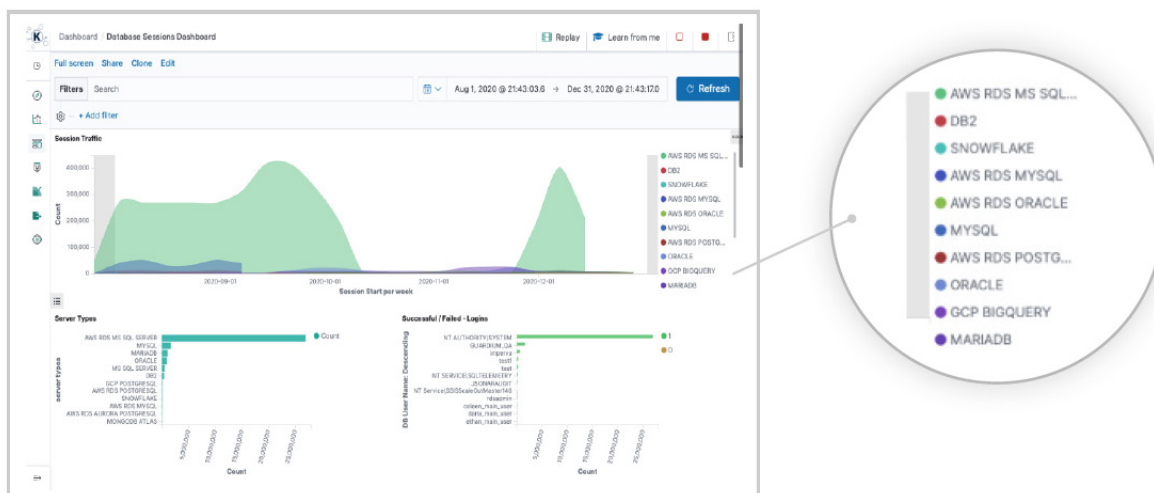
Imperva DSF utilizes modern database capabilities to deliver uniform and comprehensive coverage for all data-centric workloads without requiring an agent. Expand monitoring to more than 65+ modern databases out-of-the-box including services from all major cloud providers such as AWS, Azure, Google Cloud, Snowflake, and MongoDB Atlas. In addition, if your organization finds a new database not yet supported, we'll add support for it in as little as one month.

Automated, multi-year audit data retention

Imperva DSF automatically consolidates, deduplicates and compresses data at a rate of over 50,000 events per core so you can cost-efficiently collect and retain data in one place to meet any multi-year retention requirement. You can easily scale to hundred of Terabytes, a critical feature if you want robust security and forensics, instead of just compliance views. In addition, the platform allows you to utilize any cost-effective underlying storage infrastructure you already own (both on-prem and cloud such as AWS S3 or Azure blobs) for further cost avoidance.

Always-live audit data

Imperva DSF delivers real-time data exploration as all audit data is “live” and there is no need to go to archives for files. Imperva DSF gives you interactive reports and dashboards to perform forensic-level searches across multiple years of audit data in seconds.



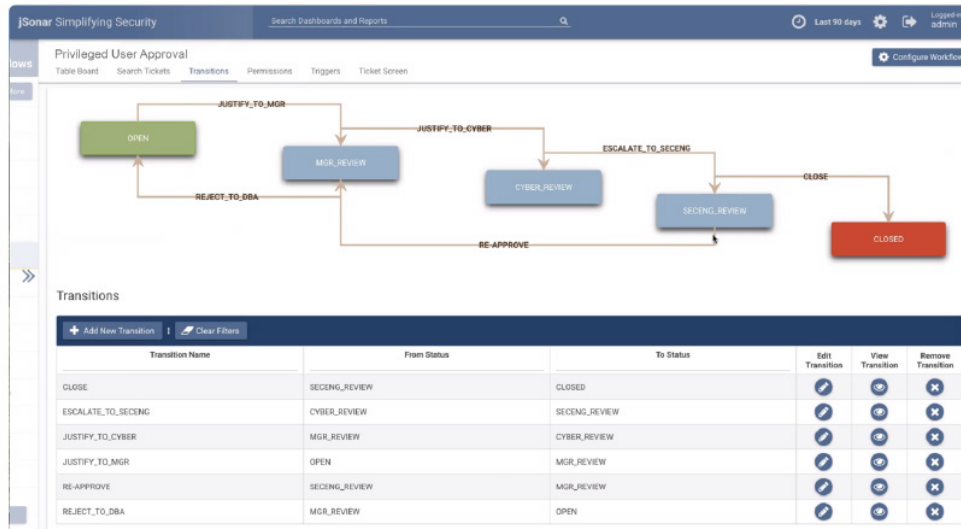
Automated retention, reporting, and forensics produce results in minutes

Large scale, unified reporting

As opposed to a batch-oriented reporting system, the Imperva DSF can produce consolidated reports in minutes without manual labor, because it constantly gathers audit data from all sources, on-prem or in-cloud, including from existing Guardium collectors. Fast reads allow for fast execution. Integrations with other forensic, reporting or business intelligence tools enable secure, self-service access by other teams such as the Security Operation Center, Database Operations, and Risk Managers using their preferred tools.

Comprehensive workflow automation

Turn days of work into minutes. Automate manual processes such as reporting sign offs, entitlement review, and change request reconciliation straight from Imperva DSF. Built-in workflows orchestrate multi-step operations and direct actions to stakeholders, accelerate resolution, and ensure nothing is missed. Rather than simply using your Guardium report level workflow, the Imperva DSF system lets you incorporate event level data, metadata and even machine learning to create advanced automation processes that enable both efficiency gains and more complex use cases.



Automated workflow eliminates manual labor and accelerates incident resolution

Advanced, risk-based security analytics

The foundation of capacity, performance and unified audit data that Imperva DSF delivers can change your approach to data security. Using all of the information you collect, Imperva DSF uses purpose-built security analytics to detect complex or evasive user data access behavior that Guardium misses. Imperva DSF gives you early indicators of users behaving inappropriately, or accounts that may have been compromised, while filtering out false positives that would trigger Guardium as anomalies but are not real risks. This additional intelligence drives better data protection, and proactive risk management, while minimizing the current burden of data security on the SOC and Incident response teams.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com