

Imperva Database Security Agent for z/OS

Effective and efficient auditing of critical mainframe databases

Mainframe databases host sensitive business information and face ever increasing regulatory and security scrutiny. Database auditing and security projects must include these systems in their scope while meeting unique mainframe operational requirements. The Imperva Database Security Agent for z/OS works with both DB2 and IMS databases and delivers comprehensive and efficient auditing of database activities to address regulatory requirements related to these critical systems.

Meet compliance requirements and minimize the impact of a data breach

The Database Security Agent for z/OS enables comprehensive monitoring and auditing of database activities, as required by a variety of government and industry regulations. The audit trail includes details to answer data access questions like: who, what, when, where, how, and why data was accessed.

By using the agent, you will enable Imperva Database Security to help identify potential breaches of sensitive data and provides alerts, reports, and analysis views to enable quick investigation and support risk mitigation efforts.

IMPERVA AGENT FOR Z/OS BENEFITS:

Integrates compliance and security auditing for mainframe environments into overall enterprise processes

Provides full visibility into critical mainframe database activity including: logons and connects, reads, writes, system commands, and database utilities

Provides real-time alerts on policy violations and uses advanced analytics to identify risky user behavior or potentially malicious activity that could lead to a security breach

Centralizes and unifies management of audit policies, agent configuration, and reporting across all enterprise database platforms

Single agent monitors both DB2 and IMS

Minimizes impact on total cost of mainframe computing by using zIIP processors

Avoid performance impact associated with monitoring DB2 and IMS

Traditional approaches for monitoring activity on DB2 and IMS on z/OS are resource intensive, causing performance degradation. The Imperva z/OS Agent is designed to avoid these pitfalls by collecting only necessary audit data and leveraging the mainframe zIIP processors. By using zIIP processors, the agent frees up general computing capacity and minimizes the impact on mainframe operating costs. Imperva z/OS Agents send audit details to a dedicated Imperva system resource so that all audit processing and data storage is performed away from the mainframe, preserving mainframe resources.

Real-time architecture, enterprise scalability

The Imperva z/OS Agent is part of a comprehensive Enterprise Database Security solution consisting of several integrated components. Imperva Database Activity Monitoring (DAM) collects and analyzes database events in real-time and instantly notifies security and operations teams about any violation of corporate data access policies. The agent architecture easily scales to meet the most demanding environments, with each SecureSphere appliance capable of supporting multiple agents. Audit data from DB2 and IMS is processed and combined with audit data from other enterprise systems providing a complete unified view of user access to sensitive data.

Imperva Data Risk Analytics (DRA) complements Imperva DAM by analyzing the behavior of users across all of the data they accessed, including the data on your mainframes. DRA uses advanced detection techniques, assisted by machine learning, to recognize data access behavior that is risky, suspicious, or potentially malicious, and presents the findings in plain language that helps security staff quickly resolve incidents or mitigate risks before they become breaches.

Simple agent deployment and management

The Imperva z/OS Agent installation typically takes less than one hour per LPAR and does not require any changes to the audited systems or a restart of the LPAR. Once the agents are deployed, they can be configured and managed from the same Imperva console used for all monitored databases. Auditing DB2 and IMS does not require deep technical understanding of these platforms or special audit policies. Imperva Database Security provides an easy user interface that simplifies audit management across all enterprise database platforms.

The Imperva solution enables centralized configuration, auditing, and reporting across heterogeneous enterprise databases—a key requirement for effectively addressing PCI, SOX, HIPAA, and other regulations. With its industry-best auditing and real-time protection, thousands of organizations choose Imperva Database Security to safeguard their most valuable assets.

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.

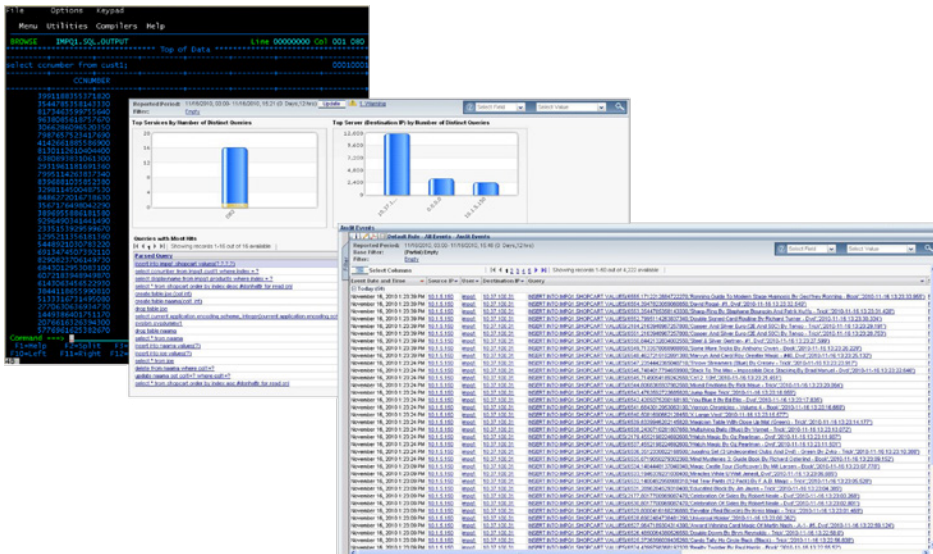


Figure 1: Imperva Database Security Agent for z/OS provides a comprehensive audit trail and detailed analysis views.