IMPERVA®

5 REASONS TO EXTEND DATA AUDIT AND PROTECTION TO MAINFRAMES WITH IMPERVA SECURESPHERE

It's critical that your organization protects sensitive customer and business data from cyber attacks and internal threats. Here are five reasons to make sure mainframes are included in your data audit and security programs.

1. Data Protection: Mainframe databases store and process sensitive data – customer PII, health information, and financial data. Cybercriminals are intent on stealing this data.

2. Internet Connected: Mainframes are no longer islands of data. They are connected to the Internet and often power critical business applications. Sensitive data often leaves the mainframe.

3. Insider Threats: Mainframe databases are vulnerable to insider threats, particularly compromised, careless or malicious privileged users such as systems programmers and DBAs.

4. Compliance: Mainframe data is subject to data protection and privacy regulations such as PCI, SOX, HIPAA and GDPR. Regulators don't stop at the door of a mainframe.

5. Unified Visibility: Security and compliance teams require a comprehensive view of security policies, alerts and reports across all database platforms, including mainframes.

Imperva SecureSphere can be easily extended to monitor and protect mainframe databases while meeting unique mainframe operational requirements. SecureSphere monitors DB2 and IMS database activity with a single, easy to deploy agent that minimizes the performance impact on your mainframe environment. Learn more out how SecureSphere monitors and protects for mainframe databases.