

Managing Segregation of Duties (SoD) for Sarbanes-Oxley (SOX) Compliance

Sarbanes-Oxley (SOX) Sections 404 C and D define compliance regulations enacted to insure the integrity of the financial results reported by public companies. A key component of SOX compliance is managing Segregation of Duties (SoD).

A SOX Segregation of Duties violation occurs when an organization cannot sufficiently prove that users do not have conflicting privileges that allow them to manipulate financial data, thus altering the results reported by the public company. Ensuring that proper SoD controls are in place is a key consideration of external auditors when validating an organization's financial results. Auditors specifically evaluate

the appropriateness of privileged users' access to databases containing financial data.

Ensuring proper SoD controls is directly related to the assignment and auditing of database user rights and entitlements. In any organization, there are users with excess privileges providing them access to financial data in excess of what they need to do their jobs. Clearly, organizations must modify the privileges assigned to these users to ensure the integrity of financial data. However, there are users whose jobs require privileged access to databases containing financial data. These users include DBAs, internal application developers and system administrators. SOX regulations require monitoring the activities of these privileged users to ensure they are not compromising the integrity of the company's financial data.

In addition SOX requires identification and remediation of database vulnerabilities and misconfigurations that leave financial data exposed to unauthorized manipulation.

DbProtect helps organizations to manage Segregation of Duties at the database layer and meet SOX compliance in three simple and cost effective steps.

THREE STEPS TO COST-EFFECTIVE SOX COMPLIANCE

Step 1: Enforce Least Privileges

Over time, users accumulate more privileges than they need to do the job. DbProtect Rights Management provides a detailed view of an organization's data ownership, access controls, and rights to sensitive information. Organizations can apply this knowledge to help manage against Segregation of Duties violations by enforcing the Principle of Least Privileges - grant their users only the privileges that they need to do their jobs.

Rights Management enables you to restrict access to databases containing financial data to a business need-to-know basis and

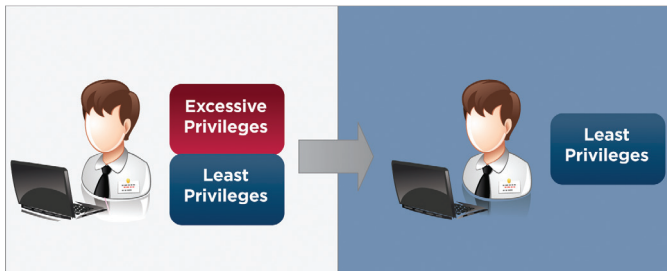
5 Key Steps to Database Security Process Control

In order to effectively secure their databases, organizations must address five critical requirements:

- 1. Isolate Sensitive Databases:** Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing on those databases.
- 2. Eliminate Vulnerabilities:** Identify and fix vulnerabilities that are exposing the database on a continual basis.
- 3. Enforce Least Privileges:** Reset user access controls and privileges to allow access to only the minimum data required for employees to do their jobs.
- 4. Monitor for Deviations:** Implement appropriate policies and monitor for any and all activity that deviates from normal and authorized activity.
- 5. Respond to Suspicious Behavior:** Alert and respond to any abnormal or suspicious behavior in real-time to minimize risk of attack.

to mitigate against shared accounts. In this way, organizations can reduce the number of users that can result in SoD violations. Rights Management also provides an audit trail on how privileges were granted, to help prevent against privilege escalation in the future.

Rights Management



Step 2. Monitor for Deviations

In every organization, there are users who require highly privileged access to databases containing financial data in order to do their jobs. SOX compliance requires monitoring the activity of these privileged users to prove they are not tampering with the organization's financial data. DbProtect Database Activity Monitoring tracks privileged users, identifies and alerts on unusual or suspicious behavior, and blocks attacks and attempts to exploit database vulnerabilities. Precision Monitoring provides SOX specific auditor-ready reports to identify Segregation of Duties violations and verify compliance.

DbProtect's powerful policy development engine allows organizations to focus only on the specific database events that require attention to meet SOX compliance. Monitoring policies can be defined to focus on specific activities, performed by specific users, accessing specific data, in specific databases. This approach analyzes all access down to the column level and provides fine grained monitoring policies that serve to eliminate any false positives or negatives.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

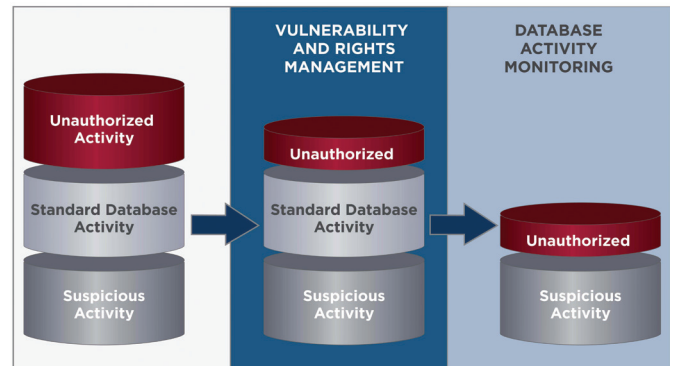
Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: www.appsecinc.com | www.teamshatter.com

For a free database vulnerability assessment visit: www.appsecinc.com/downloads/appdetectivepro

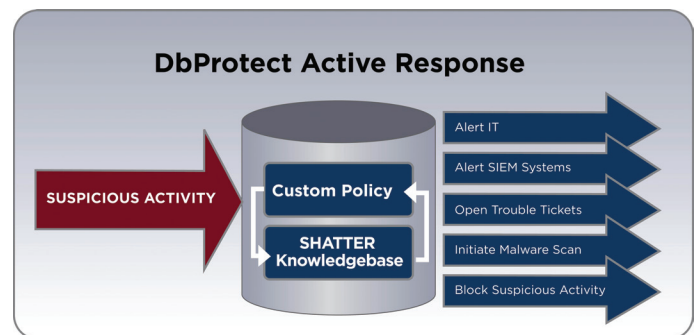
Follow us on Twitter: www.twitter.com/appsecinc | www.twitter.com/teamshatter

Precision DAM



Step 3: Respond to Suspicious Behavior

DBProtect's Active Response provides an additional layer of SoD control. Active Response can be configured to take action when an unauthorized and suspicious database activity is performed on financial data. For example: a privileged user adds, deletes or modifies financial data. Active Response can be configured to send an alert, terminate the database session, and lockout the user account until the situation can be investigated.



Incorporating a comprehensive and disciplined program of database security process control and address managing these three basic steps will help agencies to:

- Meet SOX compliance
- Secure their databases and financial data

**APPLICATION
SECURITY, INC.**
www.appsecinc.com