

Database Security In the Cloud

Many organizations are looking to Cloud-based IT infrastructures as a means of solving scalability, performance, availability and cost problems. There are three basic deployment models for Cloud infrastructures:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Regardless of deployment models, as companies begin to move their databases into the Cloud, database security programs need to follow.

Cloud infrastructures providing database hosting, offer very basic security in the form of network-layer firewalls configured with port-based access control lists. Database platforms are often provided as a service where the security details are abstracted away from the user. Those users are offered nothing more than a contract or Service Level Agreement which makes empty claims about security. This basic layer of security, coupled with the increased exposure database applications receive from being deployed in shared and possibly public infrastructures, require organizations to review their database security strategies and implement a comprehensive program of database security process control.

An important question in Public and Hybrid Cloud infrastructures is: "Who owns responsibility for securing the database and sensitive data?" Ultimately, the data owners need to take responsibility for securing their sensitive data. Data owners

should formulate their database security strategies and then partner with their Cloud providers to ensure effective implementation. Cloud providers offering database hosting need to consider database security as a critical service to their customers.

Whether in Traditional, Private cloud or Public cloud infrastructures, Application Security, Inc. believes it is important for organizations to protect their sensitive data where it lives – in the database. DbProtect Precision Database Activity Monitoring (DAM) helps organizations to protect their Cloud-based data assets by providing control over the security processes that impacts their sensitive data.

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.

FIVE STEPS TO COST-EFFECTIVE DATABASE SECURITY IN THE CLOUD

Step 1: Isolate Sensitive Databases

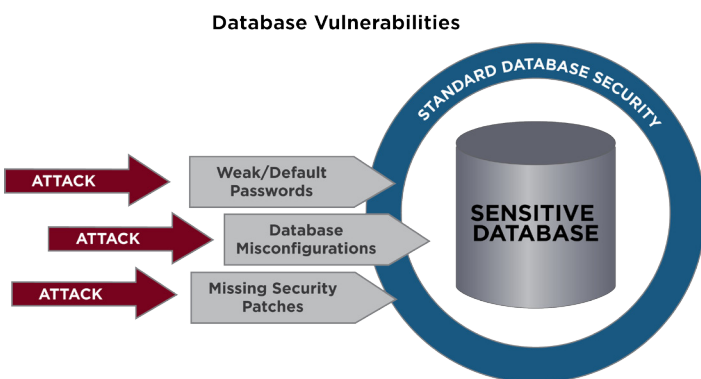
The first step to effective database security in the Cloud is to isolate all databases containing sensitive data. DbProtect's Database Discovery feature generates a complete inventory of all databases deployed cloud-wide. It identifies all production, test, and temporary databases, and more importantly, any unauthorized databases. DbProtect's Sensitive Data Discovery identifies and locates all sensitive data residing on those databases. DbProtect helps organizations and Cloud providers to protect sensitive data by:

- Ensuring sensitive data is located on authorized and secured databases.
- Restricting access and use of sensitive data.

Step 2: Eliminate Vulnerabilities

Default and weak passwords, database misconfigurations, and missing security patches provide avenues of attack through standard database security to sensitive data. DbProtect's Vulnerability Management provides unparalleled database vulnerability assessment, allowing organizations to identify and eliminate vulnerabilities and fix misconfigurations that put their sensitive data at risk.

Vulnerability Management is driven by a powerful policy development engine that begins with proven database security templates. DbProtect's policy development is fed by the SHATTER Knowledgebase, the most comprehensive and up-to-date vulnerability and threat knowledgebase in the industry. Each check in the SHATTER knowledgebase provides clear and detailed remediation instructions to insure that the vulnerabilities exposing sensitive data are fixed in a timely manner.



DbProtect's Risk Analysis maps vulnerabilities to risk level and business impact. This helps organizations and Cloud providers to prioritize their remediation plans and ensure the most serious threats to sensitive data are addressed quickly

Step 3. Enforce Least Privileges

Over time, users accumulate more privileges than they need to do the job. This can lead to Segregation of Duties (SoD) violations that enable insiders to make fraudulent changes or steal sensitive data.

DbProtect Rights Management provides a detailed view of an organization's data ownership, access controls, and rights to sensitive information. Rights Management enables the organization to enforce the Principle of Least Privileges – grant only the privileges that users need to do their jobs. It allows organizations to restrict database access to a business need-to-know basis and mitigate against shared accounts. Rights Management also provides an audit trail on how privileges were granted, to help prevent against future privilege escalation.

Rights Management



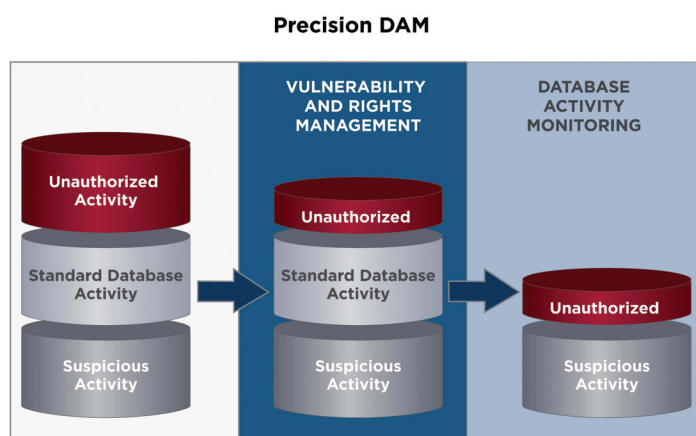
Step 4. Monitor for Deviations

Organizations and Cloud providers should track and monitor access to sensitive data and to regularly test database security processes. DbProtect Database Activity Monitoring (DAM) helps secure sensitive data in the Cloud by:

- Validating remediated vulnerabilities.
- Monitoring unremediated vulnerabilities to ensure they are not being exploited.
- Monitoring privileged user activity to ensure they are not engaged in any unauthorized behavior.
- Monitoring for any new avenues of attack.

DBProtect's unique approach to Database Activity Monitoring (DAM) is precision monitoring. Precision monitoring employs DbProtect's powerful policy development engine to streamline monitoring operations to focus on any suspicious activity threatening sensitive data. DbProtect's precision DAM solution can be customized to a fine level of granularity – A specific activity, performed by a specific user, accessing specific data, in a specific database.

Backed by the SHATTER knowledgebase, DbProtect's DAM reduces risk and offers best-in-class data protection and reporting.

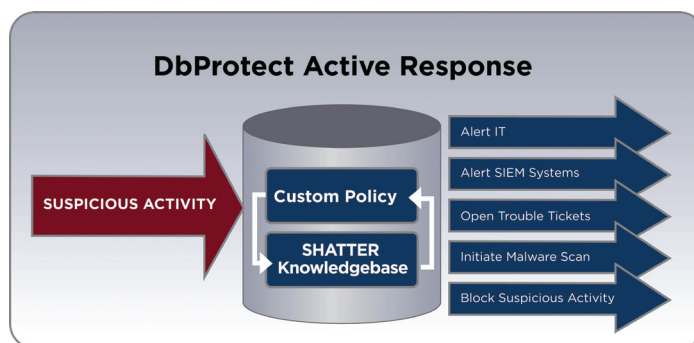


Step 5: Respond to Suspicious Behavior

DBProtect's Active Response provides an additional layer of protection around sensitive data in the cloud. Active Response can be configured to take action when an unauthorized and suspicious database activity is detected. Active response can be customized to a fine level of granularity – A specific activity, performed by a specific user, accessing specific data, in a specific database.

Example: A user with excessive privileges attempts unauthorized access to sensitive data. Active Response can:

- Send an alert to IT Security to prompt further investigation.
- Terminate the user session to immediately stop the unauthorized access.
- Lockout the user's account to prevent further attempts to access the cardholder data.



Incorporating a comprehensive and disciplined program of database security process control and managing these five basic steps will help organizations and Cloud providers to partner together to:

- Implement effective database security strategies.
- Secure their sensitive data.

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](https://twitter.com/appsecinc) | [www.twitter.com/teamshatter](https://twitter.com/teamshatter)

**APPLICATION
SECURITY, INC.**[®]
www.appsecinc.com