WHITE PAPER

Database Security in the Cloud

Trustwave®

Many organizations are moving to cloud-based IT infrastructures as a means of solving scalability, performance, availability and cost problems. However, they often fall short in ensuring the security of their data and assets as they move to the cloud.

There are three basic deployment models for cloud infrastructures:

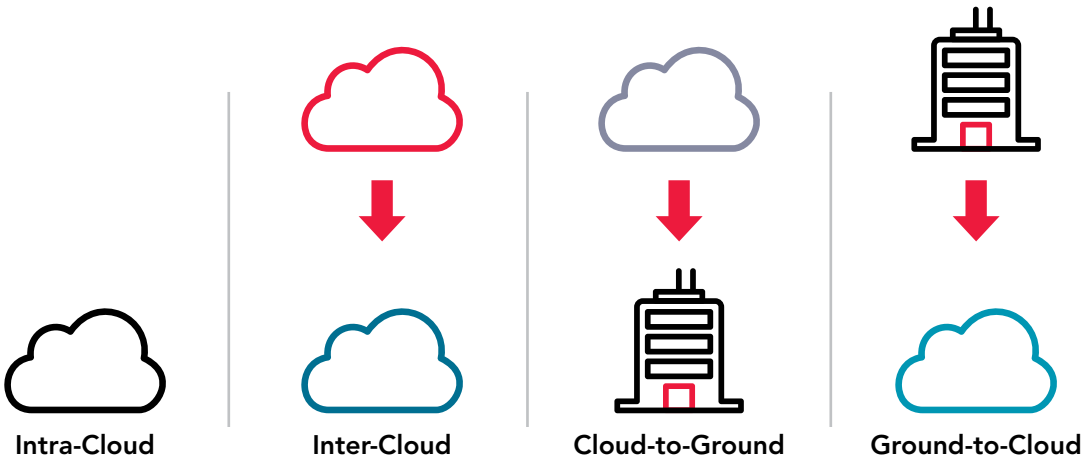
1. **Private cloud:** The cloud infrastructure dedicated to a single organization. It may be managed by the organization or a third party and may exist on premise or off premise.
2. **Public cloud:** The cloud infrastructure is made available to the public or a large industry group and is owned by an organization selling cloud services.
3. **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 (for example, cloud bursting for load balancing between clouds).

Advantages and Disadvantages of Moving Databases to the Cloud

Cloud deployments of databases or 'Database-as-a-Service' (DBaaS) are wonderful options for companies constrained by resources, but can also open a Pandora's box of security issues since responsibility for management of the database and its underlying security is no longer handled by the data owner, but by a third party. Because of this tradeoff of data security for scalability and cost savings, the need for an enterprise database security strategy has never been greater. Adopting DBaaS can significantly alter the security posture of your data estate. Having the right tools to identify traditional, on-premise database security risks as well as those that are unique to the service oriented nature of DBaaS delivery is vital. Examples of security risks inherent to the latter include but are not limited to unsecured APIs and interfaces that can be more readily exploited as well as data loss or leakage risks that can be elevated with DBaaS and unauthorized access through improperly configured firewalls.

DBaaS users are typically left with nothing more than a contract or service level agreement that makes empty claims about security. These basic layers of security coupled with increased exposure because of cloud deployment requires that organizations review their database security strategies and implement a comprehensive program of database security process control.

Whether in traditional, private cloud or public cloud infrastructures, Trustwave believes it is important for organizations to protect their sensitive data where it lives in targeted mass– the database. Whether the protection occurs from the ground (on-premise), the cloud, intra-cloud, or inter-cloud delivered approach to vulnerability management, rights management and activity monitoring, DbProtect helps organizations to protect their cloud-based data assets by providing control over the security processes that impact their sensitive data.



Proven Database Security Methodology

Enterprises can use DbProtect to secure their cloud database investment using the methodology displayed below:

1 Inventory

- Discover, classify and prioritize the databases containing your valuable information whether cloud based or on-premise
- Manage known databases on your network and in the cloud; discover unknown databases outside the scope of current compliance controls

2 Test

- Define and manage security standards and compliance policies to be used to assess database security posture
- Schedule or run ad-hoc job-based assessments to quantify cloud based or on-premise database adherence to selected policies

3 Eliminate Vulnerabilities

- Fix potentially harmful password configurations, table access grants, user roles and other vulnerable areas identified in assessment of database assets.
- Conduct regular and continuous assessments to identify issues and ensure that they are remediated in a timely manner.

4 Enforce Least Privileges

- Ensure employees and applications have only the rights needed to do their jobs
- Understand who has access to what data and how they've been granted that access

5 Monitor for Anomalies

- Inspect database access and activities for policy violations and attempted attacks
- Audit actions of known privileged users as well as administrative activity

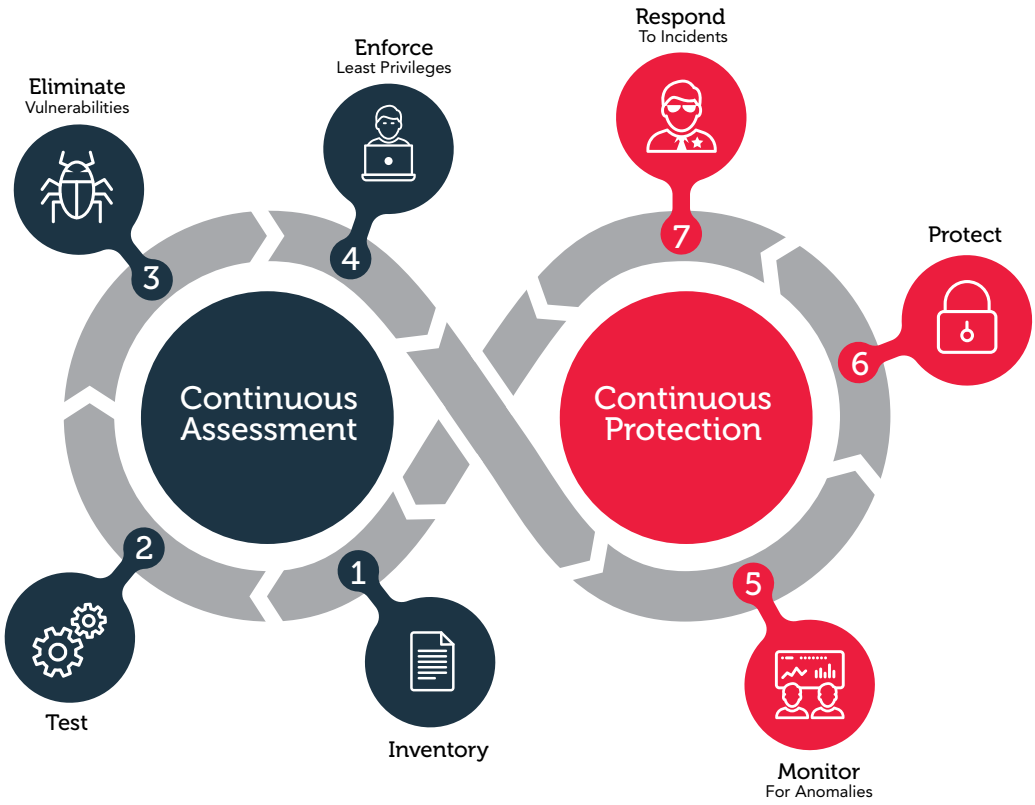
6 Protect

- Deploy policy-based Activity Monitoring to create an easily managed set of actionable security and compliance alerts.

7 Respond to Incidents

- Audit and Respond to suspicious activity and policy violations in real time

Seven Steps to Cost Effective Database Security in the Cloud



Step 1: Inventory

The first step to effective database security in the cloud is to inventory all databases. The DbProtect Database Discovery feature generates a complete inventory of all databases deployed in the cloud as well as on-prem. It identifies all production, test, and temporary databases as well as any unauthorized (and likely unsecured) databases.

Step 2: Test

Determine which business, security or regulatory policies that your organization must conform to. Ensure that your database security strategy accounts for new and updated configurations and settings defined by the newest policies and standards.

Once policies are in place, perform an analysis to associate risk scores with the findings of your vulnerability assessment to help focus efforts where you stand to make the most impact (i.e. reduce the most urgent risk).

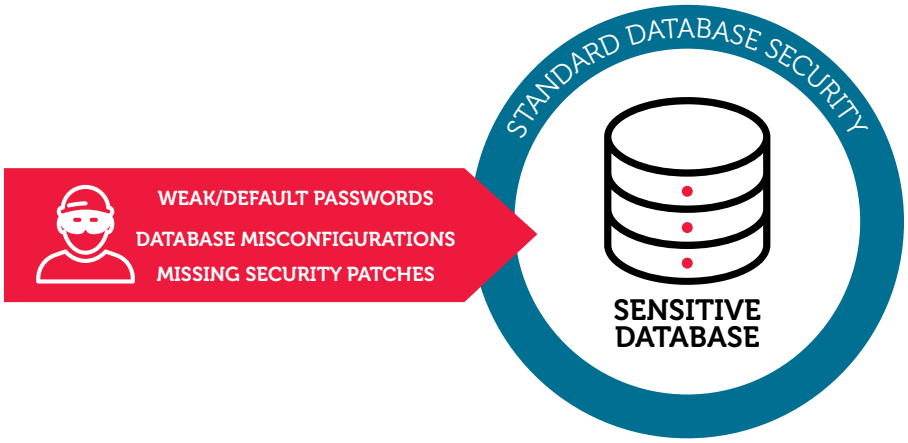
Step 3: Eliminate vulnerabilities

Default and weak passwords, database misconfigurations, and missing security patches provide avenues of attack through standard database security to sensitive data. DbProtect 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 policy development is fed by the SpiderLabs Knowledgebase, a comprehensive and up-to-date vulnerability and threat knowledgebase in the industry. Each check in the Knowledgebase provides clear and detailed remediation instructions to ensure that the vulnerabilities exposing sensitive data are fixed in a timely manner.

Powerful reporting provided in DbProtect helps perform Risk Analysis to map vulnerabilities to risk level and business impact. This analysis helps organizations and Cloud providers to prioritize their remediation plans and ensure the most serious threats to sensitive data are addressed quickly.

Database Vulnerabilities



Step 4. 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.

Step 5: Monitor for Anomalies

Organizations and cloud providers should track and monitor access to sensitive data and to regularly test database security processes. DbProtect's 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 Database Activity Monitoring (DAM) employs a powerful policy development engine to streamline monitoring operations to focus on any suspicious activity threatening sensitive data. DbProtect's 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.

Step 6: Protect

As part of our pragmatic approach database security, we recommend the definition of a policy-based monitoring methodology that meets an organization's specific security and audit requirements and provides a compensating control for known vulnerabilities. A policy-based DAM solution utilizes vulnerability, configuration, and user data, united by a comprehensive vulnerability and threat intelligence knowledgebase, to produce accurate, efficient monitoring policies resulting in a much more manageable set of actionable security and compliance alerts.

Step 7: Respond to Suspicious Behavior

DbProtect 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.

For example, when a user with excessive privileges attempts unauthorized access to sensitive data, Active Response can:

- For example, when a user with excessive privileges attempts unauthorized access to sensitive data, Active Response can:
- Send an alert to IT Security to prompt further investigation.
- Notify the SIEM system to correlate database activity with web application logs.
- Initiate a malware scan to remove any injected code.
- Lockout the user's account to prevent further attempts to access sensitive data.

Summary

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

- Realize scalability, performance, availability and cost savings promised by DBaaS without sacrificing database security.
- Secure sensitive data by implementing effective database security strategies

As organizations are increasingly moving to the cloud to take advantage of cost saving and flexibility, it is important for them to realize that the need to secure their databases is greater than ever before. Ultimately the organization is held responsible for protecting its data and will suffer the consequences, often dire, when a breach occurs. The multi-tenant, on-demand nature of cloud computing brings with it the potential of new types of security breaches. The security methodology described in this paper empowers organizations with the tools, processes and information they need to protect their databases.

Cyber attacks continue to become more sophisticated and attacker techniques refined, DbProtect enables organizations to keep pace by quickly adapting to an evolving threat landscape no matter where data is housed through database discovery, continuous diagnostics and mitigation, monitoring, alerting and active response.

DbProtect provides proven database protection to any cloud service (AWS, RDS, Microsoft Azure, Google Cloud, GovCloud, FedCloud, etc.) across any chosen environment or combination of environments.

Learn more about protecting your prized data and IT assets in an on premise or a cloud delivery model, at **Trustwave DbProtect**.

Trustwave®

TRUSTWAVE.COM