WHITE PAPER

10 Principles of Database Security Program Design

Trustwave®

Executive Summary

Relational databases and big data stores are a prime target for attackers due to the amount of sensitive information residing within, such as customer information, intellectual property and proprietary secrets. Yet many businesses fall victim to database intrusions because of common database flaws. To address their ever-expanding network perimeters that become more porous as they swell, organizations need to push data security deeper. Reducing the risk of compromise and fulfilling compliance requirements requires extending data protection measures all the way through to the database.

An effective database security program requires commitment and discipline across the organization. Policies must be established, standard configurations must be reviewed and approved and production systems must be monitored for compliance. Most importantly, an operational method consisting of not only technology but also people and processes must be documented and institutionalized.

Once it's deployed, properly configured and staff is trained in its use, technology will support these objectives. But technology alone is not a cure-all. In our work we find that organizations that see the greatest positive impact are those that combine people, process and policy and then reinforce those aspects with robust security technology. Only through the development of an effective process and methodology can the program's objectives come to fruition. This requires establishing policy, assigning accountability, defining workflow, and delivering relevant analytics and reporting to each functional area.

For more than 15 years, the database security experts at Trustwave have helped organizations design, implement and maintain database security programs custom fit to their needs. Our clients use our database security solutions (Trustwave AppDetectivePRO and Trustwave DbProtect) and managed database security testing services to protect databases around the world. We've collected and anonymized lessons learned through our client database security engagements in this whitepaper to guide you in designing a pragmatic database security program that fulfills your risk management, data security and compliance requirements. Use this document to guide you in developing and operationalizing an effective database security program with the minimum possible impact on your organization, finances and infrastructure.

The 10 Principles of Database Security Program Design

1. Describe a database security program with actionable processes
2. Clarify a scope baseline through database discovery and inventory
3. Define standards, security and compliance policies
4. Conduct vulnerability and configuration assessments
5. Identify excessively privileged user accounts
6. Implement risk mitigation and compensating controls
7. Establish acceptable user and activity policies
8. Audit privileged user behavior in real-time
9. Deploy policy-based activity monitoring
10. Detect, alert, and respond to policy violations in real time

Technology alone will not reduce your risk of database compromise. A complete program incorporates people, process and technology. Instituting a proven methodology and identifying the individuals directly responsible for delivering on the program objectives will prevent the over-extension of resources, which can include personnel, IT infrastructure, business operations, application integrity, budget or political capital. IT security, risk, audit, database administration, application management and IT infrastructure functions will all play a role in the establishment and execution of your process. Determining and establishing the appropriate policies, roles, accountability, workflow, mitigation, reporting and ongoing management will set all stakeholders on a course to achieve your program goals.

Getting Started

Before embarking on your database security journey, consider asking yourself some preliminary questions. The answers will help prepare you for some of the common challenges that arise during the implementation of an enterprise-wide database security program.

Checklist:

- ❑ What is the ideal operating state of our database security program? How do we get there?
- ❑ Does the selected technology enable rather than hinder an efficient and effective operational state?
  - How does it enable an efficient and effective program?
  - How does it, or might it, hinder an efficient and effective program?
  - Have we chosen the right technology and approach?
- ❑ How do I fit this process and technology into my overall security and infrastructure ecosystem? What are the critical integration points, reporting procedures and aggregation points?

Database Activity Monitoring (DAM) Considerations

Pragmatic database security does not begin with activity monitoring. That's why we've placed Database Activity Monitoring (DAM) at the end of our list. At a minimum, a database security technology must facilitate policy management, asset management, vulnerability management, rights management and activity monitoring to help an organization achieve its database security and compliance goals. In addition, these fundamental capabilities must integrate and inform each other. If they do not, they become islands of information existing in a vacuum, which significantly decreases the efficacy of an operational model.

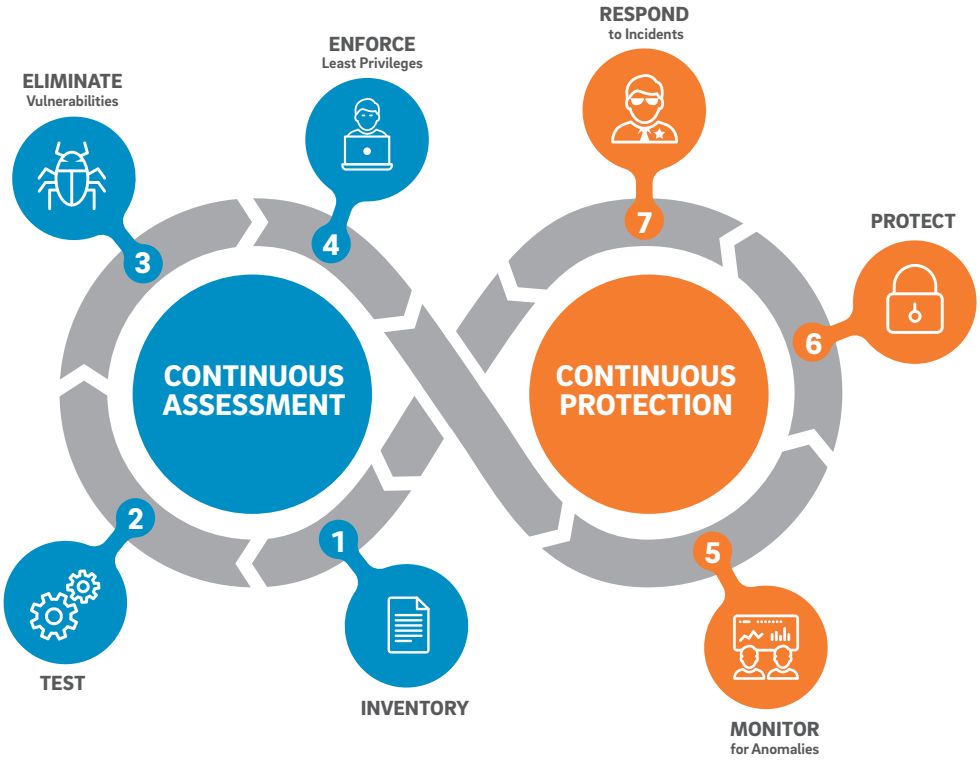
We tell our clients to think about the technology as a set of "push" and "pull" elements. Database discovery/inventory, vulnerability management and rights management capacities are push elements for which you control the throttle. You drive the policy and the frequency and the depth of the assessments (scans). As such, you control the workload and resulting organizational demands, and can restrain it at a manageable volume.

DAM and IDS/IPS are pull technologies, for which you have less control over the workload. These technologies' output depends on how broadly the monitoring policy is defined, and the volume of database activity that matches it. Without a full view of these elements and a structured process regarding how they integrate, DAM technology will likely yield countless false positives and negatives, overwhelming reports, and logs of indeterminate data – resulting in significant resource drain and potentially outright failure. Trustwave's recommended approach to DAM begins with an accurate database inventory and vulnerability and rights management assessments. Starting with an inventory and assessment of databases allows you to identify areas that need remediation and establish a baseline of known database configurations and user privileges. Armed with actionable results from these fundamental activities, you can take control of your database security program and avoid overwhelming staff and resources with massive amounts of potentially irrelevant activity monitoring results. Most importantly an established baseline allows you to monitor for any authorized or unauthorized changes. We strongly recommend that you develop your DAM deployment policy only after performing these base-lining activities and remediating any issues, which will result in more concise, focused DAM policy criteria.

Keep in mind that your database security program will need to accommodate the following:

- On-boarding and retirement of databases
- Addition and removal of users
- Changing of user roles
- Evolving audit requirements
- Ongoing patch cycles
- Constantly shifting security threats.

This approach will likely take the form of two inter-connected database security processes as illustrated in the graphic below: continuous assessment and continuous protection.



1. Define a database security program with actionable processes

A plan is the key to success. With all stakeholders at the table, the project team can identify your existing processes, people, and technologies to help drive the rapid development of your template model. This project team will also define the scope and phases of implementation and identify any gaps in people, process, or technology.

Checklist:

- ❑ What is the program's mission statement?
- ❑ What, if any, documented database standards exist today?
- ❑ What objectives can be achieved with the first phase (and then subsequent phases)?
- ❑ How can we leverage existing processes? What additional processes are needed?
- ❑ Who owns security policy? What compliance requirements are within the project's scope?
- ❑ What reporting output do we seek?
- ❑ How many personnel resources do we need? How will we add resources if/when needed?

2. Clarify the scope of your program through database discovery and inventory

Do you currently have a single "source of truth" that can identify all the databases across your entire enterprise environment? An accurate inventory of database instances in your environment is a critical-path item in establishing a holistic and effective database security program. It only takes one unpatched, rogue database on the network to potentially expose your datacenter to unchecked, malicious activity. Application developers often complicate matters by "temporarily" copying production data to development systems to test their latest software builds. More often than not, this data is stored on an unprotected (and many times unpatched) system outside the normal scope of compliance and security controls.

You need an accurate inventory of all databases (production and non-production) on the network in order to identify, classify and prioritize systems that require attention. You need to know where your data resides in order to protect it. A baseline inventory of your database systems will also help you identify which systems should be considered in-scope for your security and compliance policies.

Checklist:

- ❑ What, if any, asset management programs are in place? What checks and balances exist to confirm its accuracy? Are there any exceptions?
- ❑ What is the approval process for placing a database on your organization's network?
- ❑ What applications read/write to the database assets?
- ❑ Which of those applications are known to be in scope for regulatory compliance?
- ❑ What sensitive or private information resides in those databases?
- ❑ What local privacy laws might limit access to (or the transfer of) any of this data?

3. Define security standards and compliance policies

Managing policy is a continuous process. Without defined polices and standards to conform to, an organization cannot measure compliance or progress against benchmarks. In our work we find that while many organizations have developed corporate polices for data security, those policies are rarely mapped to the systems that store data—the databases themselves. Database vendors rarely enforce more than the most obvious weaknesses in the out-of-the-box installations of their platforms. When database security weaknesses are remediated, more often than not it's a reaction to an incident rather than proactive response to a standard or policy. When vendors do patch vulnerabilities or ship new versions of software, an organization needs to review policies to ensure they account for new and updated configurations and settings.

Checklist:

- ❑ How often are policies updated?
- ❑ Who is responsible for updating policies?
- ❑ What can trigger a policy change?
- ❑ Who approves a policy change?
- ❑ How are exceptions handled?
- ❑ Who approves exceptions?
- ❑ Which teams are involved in the review process of suggested policy changes?
- ❑ What, if any, communication process is in place to communicate policy changes?
- ❑ How, if an agreement exists, do teams cooperate to enforce defined policies?

4. Conduct vulnerability and configuration assessments

Many organizations need to demonstrate compliance with more than one set of business, security, or regulatory policies. Since databases are often an organization's largest repository of sensitive data, they usually fall into scope for regulatory compliance and the inevitable IT audit. Databases may need evaluation to ensure they fulfill any number of standards and requirements, such as: Sarbanes Oxley, PCI DSS, FISMA, DISA-STIG and more. To demonstrate effective controls surrounding sensitive data, organizations will need to run a baseline assessment and establish a practice of continuous assessment to ensure issues are remediated in a timely manner. The US Department of Homeland Security (DHS) established an excellent example of this process with its Continuous Diagnostics and Mitigation (CDM) mandate. The DHS established standards for database security requiring the scanning of databases at an acceptable frequency to ensure they remain compliant with the vulnerability assessment policy. All civilian U.S. government agencies are required to comply with the program.

Checklist:

- ❑ Who can approve the scan policy?
- ❑ Who can update scan policy?
- ❑ What, if any, risk acceptance (or exceptions) process exists?
- ❑ Who can approve exceptions?
- ❑ What do stakeholder teams agree must be assessed?
- ❑ At what frequency will scans take place? Monthly? Quarterly?
- ❑ What is the process for addressing identified vulnerabilities?

5. Identify excessively privileged user accounts

One particularly challenging question for many organizations is, "Who has access to my sensitive data?". Many database scanning technologies can not only identify vulnerabilities and misconfigurations, but also users, roles and privileges. The only way to establish meaningful controls that track how users interact with the data, or to capture an audit trail for use in a breach investigation, is to know who has access to what data and why/how they've been granted that access. For example, you might not be comfortable with the amount of employee and customer data your HR department's summer intern is capable of accessing.

Checklist:

- ❑ How often, if at all, do we review who has administrative access to our databases?
- ❑ How do we compare users' privileges to a known benchmark?
- ❑ Who should be auditing user activities for compliance and access violations?

6. Implement risk mitigation and compensating controls

Remediating high-risk vulnerabilities and misconfigurations within your database will not only reduce your risk of compromise, it also narrows the scope of any required compensating controls, such as exploit monitoring (e.g., Intrusion Detection). DAM can also be an appropriate compensating control for vulnerabilities you cannot remediate or patch in a timely manner. Using data analytics to associate risk scores with the results/findings of your vulnerability assessment will help identify your most exposed systems or groups. You can then focus your efforts where you stand to make the most impact (i.e., reduce the most risk).

Checklist:

- ❑ Specific to our environment, where do we begin in making the most impactful changes to reduce our risk of compromise?
- ❑ How do we get visibility into where we may need to add compensating controls to cover gaps in our configurations?
- ❑ What is our response plan for the remediation of findings?
- ❑ How do our security policies support the response plan?

7. Establish acceptable user and user activity policies

A number of technologies facilitate user profiling, database auditing being one method. If you currently perform database auditing, you probably have a means of identifying which user accounts have high levels of database privileges. However, as duties change, new employees join the organization and others leave, regular evaluation of database account privileges becomes all the more important. Such an assessment should also identify unauthorized accounts or those with excessive privileges.

Many native database platforms include profiling tools. The best practice is to verify the existence of any native auditing or profiling capabilities, and request access to any related information.

As we warned in the “Getting Started” section of this paper, DAM can create an enormous set of results requiring ever-increasing amounts of storage and making review of the logs time-consuming and expensive. User profiling helps in identifying what activities need to be logged, reducing the volume of DAM alerts and ensuring resources are only spent reviewing relevant, actionable information.

Below we’ve listed and explained some of the more common database user account types.

Database User Account Types and Descriptions

Authorized users	Privileged users	Knowledge users	Outsiders with insider access and/ or vulnerability knowledge
Employees such as clerks, accountants, finance staff, sales people, purchasing staff and others. This type of user includes anyone granted authorized access to the data or systems within a given enterprise.	Individuals with elevated privileges, broad access and extensive database knowledge, such as: DBAs, developers, quality assurance staff, contractors and consultants.	Users with access and knowledge of systems or security protocols like IT operations, network operations, security and audit personnel.	These users may not have the same user rights as “Authorized”, “Privileged”, or “Knowledge” users do, but they may be capable of performing privileged activity.

Checklist:

- ❑ Do we use the native auditing capabilities within our database software? If not, why not and should we enable the capability?
- ❑ If it exists, who is reviewing the collected audit information and for what purposes?
- ❑ How long is auditing data stored?
- ❑ What, if any, reporting is provided and to whom?

8. Audit privileged user behavior in real-time

DAM is a class of technologies that allows you to collect a forensic audit trail of all privileged activities in a database. Many compliance regulations (including Sarbanes-Oxley) require tracking of structural changes in your information, which means auditing privileged (administrative) activity, not just the actions of known privileged users.

Checklist:

- ❑ Who manages our list of database users and their privileges?
- ❑ Who is reviewing audit events and how often?
- ❑ For what purpose are they reviewing audit events?
- ❑ What actions are taken once these audit events are reviewed?

9. Deploy policy-based activity monitoring

Working in tandem with database audit logging technologies, your DAM security and compliance policies should trigger alerts when activity that violates those policies is detected. Be wary—some DAM technologies rely on a "learning" mode that accepts all database activity captured during a certain limited time-window (a learning cycle) as normal transactions representative of all activity that occurs throughout the year (including batch jobs and maintenance activities). Many vendors recommend learning-based activity monitoring policies because manually configuring policies within their products is too complex.

As enterprise database activity evolves with business growth, a learning-based product will need to continually self-modify the monitoring policy (which makes demonstrating compliance with a particular policy to an IT Auditor very difficult), or the administrators of the product will end up turning off learning mode and manually configuring the DAM solution anyway.

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, unified 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.

Checklist:

- ❑ Who and/or what applications should have access to each monitored database and for what purpose?
- ❑ What activities will we define as authorized (e.g., application activities)?
- ❑ What is our policy for retaining log or event data?
- ❑ If reporting is currently available, what information is included and who reviews the reports?
- ❑ What events do we want to be alerted to, who will review them and what actions should be taken in response?
- ❑ What other higher-level event correlation system, such as a SIEM technology, might consume this event information?

10. Detect, alert and respond to policy violations in real time

Most real-time DAM solutions can send alert messages in a variety of formats so that operations center personnel can take action when a security violation is identified. Many organizations then choose to feed these events into a SEIM or network management tool if/when suspicious or malicious activity is detected. Depending on the policy violation and the sensitivity of the affected system or data, automated and scripted responses ("active responses") can contain the threat and give the security team time to investigate and take corrective action. Examples of active responses may include: terminating the user session, locking out the offending
user account and triggering a database vulnerability/configuration scan and/or anti-malware scan of the database host.

Checklist:

- ❑ Who has authority over other security technologies that might consume DAM data?
- ❑ What integrations are available with third-party security and network management solutions (e.g. SEIM)?
- ❑ What types of events will you want your security staff to be alerted to in real time?
- ❑ Is staff sufficiently knowledgeable to take immediate action on alerts? If not, for which critical security events can we implement an automated action ("active response") as a protective measure?

Ongoing Reporting and Integration

Finally, you need to fit the output of the DAM data you receive into your security infrastructure and IT operational eco-system. This should be part of the operational model, but designing proper reporting must begin with an understanding of the program as a whole.

As you design and refine your database security program, the data you need and how you distribute it will become clearer. You'll find that integration with a centralized security solution make the design and planning phases much more efficient. Be sure you collaborate across all the data-consumer communities before taking detailed integration steps that may add extra work if not previously agreed upon and planned carefully.

Checklist:

- ❑ What systems need to be protected for each stakeholder?
- ❑ What level of information sharing will provide them the data they need to make informed decisions?
- ❑ What amount of control over the reporting does each stakeholder require?
- ❑ How will data from a database security solution be consumed by other security programs within the jurisdiction of each stakeholder?

Next Steps

Database security and compliance best practices dictate that organizations regularly scan for vulnerabilities and highly privileged user accounts and then monitor for anomalous activity. A pragmatic database security program requires that organizations implement an automated process for identifying critical vulnerabilities and privileged accounts, remediating issues where possible and then monitoring privileged activity whether it's associated with authorized, recognized privileged accounts or other accounts with excessive privileges. Organizations need to make sure administrators and/or security personnel have sufficient, actionable data to make informed decisions and are not distracted by excessive alerts, false-positives and false-negatives.

Also make sure that you're monitoring known but unpatched vulnerabilities. Commonly referred to as a compensating control, real-time activity monitoring can protect databases during the gap between discovery of a vulnerability and mitigation of that vulnerability. Responsible organizations should proactively deploy activity monitoring, informed by vulnerability and rights review scan results, to ensure the highest, most efficient level of database security.

Checklist:

- ❑ Involve stakeholders early and often
- ❑ Define and document processes (and base them on existing policies where possible to save time and resources)
- ❑ Establish your response plan ahead of time
- ❑ Create policies that support the response plan
- ❑ Understand and document your reporting requirements

How Trustwave Can Help

Trustwave DbProtect is a complete database security platform that automates the securing of critical data where it's stored with database vulnerability management, database user rights management and database activity monitoring (DAM).

Trustwave DbProtect inventories and classifies databases on the corporate network, or in the cloud, and discovers vulnerabilities, configuration mistakes, access control issues, missing patches or any toxic combination thereof in Microsoft SQL Server, Microsoft SQL Azure, Oracle, Sybase ASE, MySQL, IBM DB2 and Hadoop. From there, Trustwave DbProtect composes a detailed picture of database user accounts, data ownership, access controls and rights to sensitive information to then restrict user privileges to the minimum necessary. Finally—after inventorying and assessing data stores (on premise or in the cloud) and enforcing "least privilege"—Trustwave DbProtect monitors for deviations in regular database traffic to detect suspicious activity and provide real-time warnings and build an audit trail.

For more information on Trustwave's database security solutions and how Trustwave can help you design your program, please contact your Trustwave Account Manager, or learn more online at: https://www.trustwave.com/Products/Database-Security/

Copyright © 2017 Trustwave Holdings, Inc.