



# Understanding and Selecting a Database Assessment Solution

## Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the [Securosis blog](#) but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

## Licensed by Application Security Inc.



### About Application Security Inc.:

Founded in 2001, Application Security, Inc. (AppSec) has pioneered database security, risk, and compliance solutions for the enterprise. AppSec empowers organizations to assess, monitor and protect their most critical database assets in real time, while simplifying audits, monitoring risk, and automating compliance requirements.

As the leading provider of cross platform solutions for the enterprise, AppSec's products – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – deliver the industry's most comprehensive database security solution. With over 2,000 customers in 42 countries, AppSec is headquartered in New York City and has offices throughout North America and the United Kingdom.

The award-winning AppSec product line, acknowledged as the industry's only complete database security, risk, and compliance solution, enables organizations to extend existing data protection measures to include the database, thereby tightening security and bolstering compliance. Our security experts, combined with our strong support team, deliver up-to-date database protection that minimizes risk while enabling business operations.

AppSec customers include over 250 unique federal, state, and local government organizations, eight out of ten of the world's largest global banks, three major credit card companies, two stock exchanges, several of the largest financial services companies in the U.S., five of the top ten global telecommunications companies, several of the world's largest retailers, major hotel and hospitality chains, three global clothing retailers, top grocery chains, and major electronics and manufacturing organizations, leading colleges and universities including Harvard, Columbia Presbyterian Teaching Hospital, Swarthmore College and the Georgia Board of Regents, major healthcare organizations including several divisions of BlueCross/BlueShield, major hospitals, and government-contracted health organizations.

For more information, please visit [www.appsecinc.com](http://www.appsecinc.com).

## Copyright

This report is licensed under Creative Commons Attribution-Noncommercial-No Derivative Works 3.0.

<http://creativecommons.org/licenses/by-nc-nd/3.0/us/>

# Table of Contents

<b>Introduction</b>	<b>5</b>
Types of Database Assessment	5
Database Assessment Features	6
<b>Business Requirements</b>	<b>7</b>
Business Drivers	8
<b>Data Collection</b>	<b>9</b>
Data Collection Options	9
Special Considerations for Database Settings at OS Level	10
Discovery	11
<b>Policy Management</b>	<b>13</b>
Vulnerability and Security Policies	13
Compliance and Operational Policies	15
<b>Management &amp; Administration</b>	<b>18</b>
<b>Database Assessment Selection Process</b>	<b>20</b>
Define Needs	20
Formalize Requirements	20
Evaluate Products	21

<b>Internal Testing</b>	<b>21</b>
<b>Conclusion</b>	<b>22</b>
<b>Who We Are</b>	<b>23</b>
<b>About the Author</b>	<b>23</b>
<b>About Securosis</b>	<b>23</b>

# Introduction

Few people understand the internal complexities of database systems. Historically, as long as databases ran without visible trouble, database administrators (DBAs) enjoyed implicit trust that the systems under their control were secure. Unfortunately, many attackers have recently demonstrate how easy it is to exploit unpatched systems, gain access to accounts with default passwords, and leverage administrative components to steal data. Database security cannot be assumed, but must instead be verified. Further, databases are leveraged across enterprises — such that a breach of a web application can cascade across financial systems, business intelligence, sales, and partner sites. Those tasked with security and compliance of those systems — security teams and internal auditors — lack the technical skills to examine database internals in sufficient detail. Database assessment tools bridge this gap by capturing DBA utilities for automation of complex tasks, analysis of obscure settings, and separation of duties between audit and administrative roles — in such a way that non-DBAs can use them.

When we started our research on database vulnerability assessments, several security professionals asked the simple question “Why?” “Why are you writing about database assessment? Why now? Don’t most people already know what assessment is and check their databases?” IT and security professionals understand how general network and OS assessment products work, often assuming that databases are no different. While this is conceptually true, in practice general assessment techniques translate poorly to the database world. Assessing databases is a very different challenge than OS and network level scans. This is due partially to the complexity of database management systems, and even more to where and how database configurations and operations are managed. Database security and compliance requirements have been at issue for many years now, but only recently have assessment platforms matured sufficiently to deliver on their promise — they must do far more than simply check for missing patches.

The reasons to purchase a database assessment product have also changed. They used to be primarily for educating DBAs on configuration guidelines and finding vulnerabilities, but are now focused on operations management and compliance. Yes, the tools still find which databases you forgot to patch, the places where the CEO was granted administrative access, and the default passwords that were never changed; they also help determine which patch fixed the problem you were worried about. Assessment scanners are no longer funky little homegrown tools, but instead mature enterprise-class products. Assessment is not only an essential step for security, but also for meeting compliance requirements, discovering important assets, separating duties between operations personnel, and communicating results to both technical and non-technical stakeholders.

If you initiate a database security program, assessment is a likely starting point for the entire process. It enables discovery, verification of access control settings, configuration review, removal of dangerous or unwanted features, and prevention of common SQL injection and buffer overflows. In the database security requirements we see included in end-user RFP/RFI submission requests, a full 60% of the technical requirements can be addressed through database assessment technology. Even the vendors who provide these technologies are changing. If you reviewed database assessment products more than two years ago and were dissatisfied, it's time for another look.

## Types of Database Assessment

Assessment technologies for database platforms have continued to evolve, and are now completely differentiated from OS and network level scans. As a result they must be evaluated against a different set of requirements than other solutions. Relational database platforms have multiple communication gateways, include their own complete access control and authorization schemes, and may combine multiple databases and database schemas within a single installation. To address this complexity requires more than a cursory inspection of patch levels and default passwords. We define database assessment as the following:

Database Assessment is the analysis of database configuration, patch status, and security settings; it is performed by examining the database system both internally and externally — in relation to known threats, industry best practices, and IT operations guidelines.

## Database Assessment Features

The core database assessment feature set consists of:

- Configuration data collection options
- Security & vulnerability analysis
- Operational best practices
- Policy management and remediation
- Security & compliance reporting
- Integration, workflow, & advanced features

We will also cover developments in database platform technology; as well as how assessment technologies have adapted, and must continue to adapt, to meet new challenges.

# Business Requirements

If you are looking for a business justification for database assessment, the joint [USSS/FBI advisory](#) illustrating common database attack vectors should be more than sufficient. The advisory's contents are not a checklist of exotic security measures or esoteric vulnerabilities — it lists several fairly basic security steps that should be implemented in every production database. The preventative controls listed in the advisory are, for the most part, addressed with database assessment scanners. Detection of known SQL injection vulnerabilities, detection of use of external stored procedures like `xp_cmdshell`, and avenues for obtaining Windows credentials from a compromised database server (or vice-versa) are basic policies included with all database vulnerability scanners — some freely available for download. It is amazing that large firms like Heartland, Hannaford, and TJX — who rely on databases for core business functions — failed so badly to follow basic database security practices, and thus suffered the consequences. As surprising as it may seem, known vulnerabilities remain common and provide avenues for anyone who cares to break into your database servers. Many have been around for a decade or more and are trivial to exploit. If you don't think you are a target because you are not storing credit card numbers, think again — there are plenty of ways for attackers to earn money or commit fraud by extracting or altering the contents of your databases.

Adoption of database specific assessment technologies has been sporadic outside the finance vertical because the business justification is not always simple. For one thing, many firms already have generic forms of assessment and inaccurately believe they thus have databases covered. If they discover missing policies, they often get the internal DBA staff to paper over the gaps with homegrown SQL queries. But this approach fails in multiple ways: it lacks appropriate configuration data, lacks suitable security and compliance oversight, provides no segregation of duties, and requires costly maintenance. Security personnel, IT operations, and internal and external auditors are all now interested in the scan results, not just DBAs.

When considering business justifications for the investment into database assessment, you are unlikely to find any single irresistible reason you need the technology. Product marketing claims tend to say “You are compelled by compliance mandate GBRSH 509 to secure your database with this technology”, or some nonsense like that, are simply not true. There are security and regulatory requirements that compel certain database settings, but nothing that mandates automation. But there are two very basic reasons you need to automate the assessment process: The scope of the task, and the accuracy of the results. The depth and breadth of issues to address are beyond the skill of any one of the customer audiences for assessment tools. Let's face it: the ongoing changes in database security issues alone are difficult to keep up with — even aside from compliance, operations, and evolutionary changes to the database platform itself. Combined with the boring and repetitive nature of running these scans, the territory is ripe for shortcuts and human error.

Understanding database vulnerabilities and knowing how to remediate — whether through patches, workarounds, or third party detection tools — requires significant skill and training. Policy research is expensive, as is writing and testing these policies. In our experience it takes an average of 3 days to construct a policy after a vulnerability is understood: A day to write and optimize the SQL test case, a day to create the description and put together remediation information, and another day to test on supported platforms. Multiply by 10 policies across 6 different platforms and you get an idea of the costs involved. Policy development requires a full-time team of skilled practitioners to manage and update vulnerability and security policies across the half dozen platforms commonly supported by the vendors. This is not a reasonable burden for non-security vendors to take on, so don't try to do this in-house, and don't rely on non-database-specific tools that are unable to access anything beyond basic patch levels and configuration settings.

## Business Drivers

When considering a database assessment solution, the following are common drivers for adoption. If your company has more than a couple databases, odds are all these factors will apply to your situation:

- **Configuration Auditing for Compliance:** Periodic reports on database configuration and setup are needed to demonstrate adherence to internal standards and regulatory requirements. Most platforms offer policy bundles tuned for specific regulations such as PCI, Sarbanes-Oxley, and HIPAA.
- **Security:** Fast and effective identification of known security issues and deviations from company and industry best practices, with specific remediation advice.
- **Operational Policy Enforcement:** Verification of work orders, operational standards, patch levels, and approved methods of remediation are valuable (and may be required).

There are several ways this technology can be applied to promote and address the requirements above, all of which improve efficiency and effectiveness, and reduce manual costs:

- Automated verification of compliance and security settings across multiple heterogeneous database environments.
- Consistency in database deployment across the organization (especially important for patch and configuration management) as well as detection and remediation of exploits commonly used to gain unauthorized access.
- Centralized policy management so that a single policy can be applied across multiple (possibly geographically dispersed) locations.
- Separation of duties between IT, audit, security, and database administration personnel.
- Non-technical stakeholder usage, suitable for auditors and security professionals without detailed knowledge of database internals. Assessment platforms act as a bridge between policy and enforcement, or serve to verify compliance for a non-technical audience.
- Reduction in development time, removing the burden of code and script development from DBAs and internal staff.
- Integration with existing reporting, workflow, and trouble-ticketing systems. Assessment is only useful if the data gets into the right hands and can be acted upon.

Forensic studies on database breaches illustrate that known weaknesses are commonly exploited in real-world attacks. Every week you can read about a new event in the paper, which should provide ample motivation to adopt database assessment in order to uncover such common weaknesses to address. These stories should serve as a wake-up call for companies to verify their baseline security, and sufficient incentive for you to evaluate database assessment technologies.

Thus the business justification for investing in database assessment technology is:

- Reducing the risk of security incidents through consistent, automated database assessment.
- Reduced operational costs through automation.
- Reduced compliance costs due to automation and reporting.

# Data Collection

Database assessments are a simple concept. Inspect the database setup, compare what you found with established policies, and either report or fix mismatches. But databases are complex platforms, and in practice assessments are never quite that easy. The first step is understanding the basic components of assessment options available. We begin this process by dissecting the technology, then take a close look at data collection and deployment options, and finally discuss the strengths and weaknesses of each. What your requirements are and how to address them are just as much functions of the product implementation as the policies it contains. Architecturally, there is little variation in database assessment platforms. Most are two-tiered systems, either appliances or pure software, with the data storage and analysis engine located away from the target database server. Many vendors offer remote credentialed scans, and some provide an optional agent to assist with data collection issues, as we will discuss later. Data collection is where things get interesting, because that is what sets the boundaries for what is possible and what policies you can enforce.

As a customer, the most important criteria for evaluating assessment tools are how well they cover the policies you need, and how easily they integrate with your organization's systems and processes. The single biggest technology factor to consider for both is how data is collected from the database system. Data collection methods dictate what information will be available — and as a direct result, what policies you will be able to implement. Further, how the scanner interacts with the database plays a decisive role in how you deploy and manage the product. Obtaining and installing credentials, mapping permissions, agent installation and maintenance, secure remote sessions, separation of duties, and creation of custom policies are all affected by the data collection architecture.

Database assessment begins with the collection of database configuration information, and each assessment vendor offers a slightly different combination of data collection capabilities. In this context we are using the word 'configuration' in a very broad sense to cover everything from resource allocation (disk, memory, links, table-spaces), operational allocation (user access rights, roles, schemas, stored procedures), database patch levels, network, and features/functions that have been installed into the database system. Pretty much anything you might want to know about a database.

## Data Collection Options

There are three ways to collect configuration and vulnerability information from a database management system:

- **Credentialed Scanning:** A credentialed database scan leverages a user account to gain access to the database system internals. Once logged into the system, the scanner collects configuration data by querying system tables and sending the results back to the scanner for analysis. The scan can be run over the network or through a local agent proxy — each provides advantages and disadvantages which we will discuss later. Either way, the scanner connects to the database communication port with the user credentials provided, in the same way as any other application. A credentialed scan can have access to everything a database administrator would, and returns information that is not available outside the database. This method of collection is critical as it picks up settings such as password expiration, administrative roles, active and locked user accounts, internal and external stored procedures, batch jobs, and database/domain user account mismatches. It is recommended that a dedicated account with (mostly) read only permissions be issued for vulnerability scanning in case of a system/account compromise.
- **External Scanning (File & OS Inspection):** This method of data collection deduces database configuration by examining settings outside the database. This type of scan also requires credentials, but not database user credentials. External assessment has two components: file system and operating system. Some but not all configuration information resides in files stored as part of the database installation. A file system assessment examines both contents and metadata of initialization and configuration files to determine database setup — such as permissions on data files, network settings, and control file locations. In addition, OS utilities are used to discover vulnerabilities and security settings not determinable by examining files within the database installation. Which user account the database

systems runs under, registry settings, and simultaneous administrator sessions are all examples of information accessible this way. While there is overlap between the data collected through credentialed via external scans, most of the information is distinct and relevant to different policies. Most traditional OS scanners which claim to offer database scanning provide this type of external assessment.

- Network (Port) Inspection. In a port inspection, the scanner performs a mock connection to a database communication port: during the network transaction, either the database returns its type and revision explicitly, or the scanner deduces them from other characteristics of its response. Once the scanner understands the patch level of the database, a simple cross reference for known vulnerabilities is generated. Older databases leak enough information that scanners can make educated guesses at configuration settings and installed features. Some vendors inspect network traffic, examining communications to and from the database to make similar educated guesses as to database version and setup with limited success. These forms of assessment are a “quick and dirty” approach for basic patch inspection with minimal overhead and without agents or credentials. As such network assessment lacks the user and feature assessments required by many security and audit groups, and as database vendors have blocked most of the information leakage from such simple connections, this type of scan is falling out of favor.

There are other ways to collect information, including eavesdropping and penetration testing, but they are not reliable; additionally, penetration testing and exploitation can have catastrophic side effects on production databases.

While you will spend a very small percentage of your product evaluation on understanding data collection, it has a substantial impact on day to day management, so be prepared to spend some time considering tradeoffs. The bulk of configuration and vulnerability data is obtained from credentialed scans, so they should be the bare minimum data collection technique in any assessment of critical systems. The choice you will need to make for this phase is to determine if you want agents or remote scans. To capture the complete picture of database setup and vulnerabilities, you need both: a credentialed database scan *and* an inspection of the underlying platform the database is installed on. You can accomplish this by leveraging a different (possibly pre-existing) OS assessment scanning tool, or obtaining this information as part of your database assessment. In either case this is where things get a little tricky and require careful attention to make sure you get the functions you need without introducing additional security problems.

With credentialed scans, you need to gather the credentials for each database you want to scan and store that information within the assessment tool — this itself is a lot of work. It is recommended that you create a specific credential on the target databases to support scans, with sufficient privileges to read needed information, but no access to alter or execute code. Consider an agent based deployment for credentialed scans as well. You will need to install and maintain the agent, but agents can run and collect data without being in constant contact with a central scanning tool. Older products often stored the credentials within the local agent, which is a security issue. Verify that the credentials are stored centrally, or are obtained dynamically through your access control system, rather than stored on the local file system.

## Special Considerations for Database Settings at OS Level

Traditionally, database assessment products used external stored procedures or locally installed agents to collect both database internals and external configuration information. The problem is that each of these methods poses a serious security risk. External stored procedures are a classic avenue for attackers to access or subvert a database system. They start by getting into the underlying platform and then using stored procedure calls to exercise database functions, or by gaining access to the database and then launching code on the underlying platform. Enabling functions like SQL Server's `xp_cmdshell` or Oracle's `extproc` is considered a critical security vulnerability, so they are no longer available to assessment products for scanning. Historically, agents have been used to address connectivity, network bandwidth, local policy analysis, secure communication, and various other concerns that are no longer relevant. Now their principal value is that they can launch both credentialed internal (database) and external (OS) scans. That also means they provide a way for IT administrators to gain access to database credentials, and DBAs to access the underlying operating system. Multi-purpose agents with mixed credentials violate common security practices, both because they give attackers an avenue for breaching systems, and also because they violate separation of duties between administrative roles.

We understand that not all products offer both credentialed or external scanning capabilities, so when in doubt, select one that offers credentialed scanning — it will cover a greater number of security and compliance tasks. If you have the option, choose a platform that does both securely, meaning a vendor that offers both must provide one of the following options:

- Use *separate* tools for internal and external data collection, and merge data on the back end inside the policy analysis or reporting tools. As many firms already have OS assessment in place, this is a cost-effective yet slightly clumsy option.
- Deploy external database inspection scripts in ‘push’ mode, where the local software agent has the ability to execute file and OS scripts, and then push results out to the database assessment scanner. In this way the scanning tool can perform remote credentialed scans, but does not need to store both OS and database credentials, preserving separation of duties.
- Audit your database assessment vendor’s platform to verify it offloads one or both sets of credentials to a third party access control service, and that there is proper separation of duties within the UI so access to internal and external scanning functions are not commingled.

There are other options, but these are the ones available in commercially available products. As we said before, data collection has a significant impact on the policies you implement and how you manage the installation. Of all the technology aspects we will cover, this is the most important one, and data collection should be a focus in your product evaluation. Please make sure you understand this section and ask questions of your vendor if their options are not clear.

## Discovery

Discovery is an important part of assessment, as it can locate databases and data types that were un-cataloged and require protection. Further, it can locate sensitive data, often discovering copies within databases where it should not reside. Many applications come bundled with databases, and while they may be managed ‘seamlessly’ by the application, such databases are frequently insecure. Large, complex applications often contain as many as 50,000 tables, creating a nightmare for auditors trying to determine if sensitive data is stored under the right credentials.

Discovery is particularly valuable in these two use cases:

- **Database Discovery:** Database discovery is the act of locating databases within your organization. You could do so manually by inspecting each machine within your organization, but this is clumsy and time consuming, and fails for many organization that use virtual servers or have databases embedded within applications. Most often, discovery is performed through network scanning of servers, looking for accessible database network services. By examining the network ports databases normally reside on, these scanners can quickly locate databases, and can compare their findings over time to detect new additions. Such scanners only find databases within the local area network, and often only databases using default ports, but provide fast and effective discovery. These scans cannot determine what each database is used for, or who has ownership — only that the database exists. Database discovery is very effective at locating databases that are undocumented or otherwise invisible to IT staff.
- **Data Discovery:** Data discovery is performed under a credentialed scan, by traversing internal database structures, and in some cases by inspecting content. The analysis to identify sensitive data is commonly performed by looking at metadata. For example, if we wanted to discover credit card information, we would look for 9-digit numeric fields, or column names such as “CC”, “CreditCard”, etc. This may be augmented with content scanning, such as using “LUHN” checks to verify a field contains real credit card numbers. Basic policies are provided by vendors for common data types such as personally identifiable information and credit card numbers. More advanced (and often more accurate) discovery requires tuning and adjustment by users. Several vendors provide data discovery through network analysis, but the results are unreliable, as they depend on which data appears on the network during the scanning window.

Analysis of discovery options should be part of any commercial scanner evaluation. Vendor literature frequently states that Discovery is the starting point for assessment. Their argument is that you need to discover what you have before you

can protect it. The argument is logical if you are coming into an organization for the first time, but is generally inaccurate and not pragmatic approach in the real world. Many security and compliance efforts collapse under their own weight by trying to catalog & control all data in one fell swoop. The critical databases and data types are typically known, with existing policies that may be under-served and under-enforced. We recommend scanning and securing critical databases first, and moving on to other databases once your policies and processes are settled. Then use database and data discovery to broaden your scope.

# Policy Management

Policy Management is the second major phase in database assessment. Data collection defines the scope of what you can assess, and policies define what you will scan. We have broken our discussion of policy management into two sections: one for vulnerabilities and security issues, and another for operations and compliance issues. The market initially had a heavy security focus, then added compliance and operations capabilities to meet evolving market demands. The rapid and ongoing propagation of the Slammer worm, beginning in 2003, showed the limitations of traditional network scans for managing database vulnerabilities — spurring investment into database-specific assessment tools. Since then, due to growing regulatory requirements, more of the market has been driven by compliance and operations concerns. Major commercial products now contain a good blend of security and compliance policies to meet both needs.

To understand how an assessment scanner can meet your business requirements you must understand policies: how they are created, what they apply to, and how they work. The following focuses on buying criteria for database assessment solutions as they pertain to policy management — this is where you will spend the bulk of your time analyzing the available products.

## Vulnerability and Security Policies

What specific vulnerability checks should be present in your database assessment product? In a practical sense, it does not matter. Specific vulnerabilities come and go too fast for any static list to remain relevant. What you need to consider is how responsive the vendor is in creating updated policies for vulnerabilities, and good general security practices that cover ranges of database threats. These policies must cover the database platforms and versions you use. Most organizations will not have security researchers on staff to write new policies, so choose a vendor with a documented good track record in policy development — you will be relying on their expertise. To help determine the depth and breadth of the policy set provided, we provide a lists of general security checks that should be present, and list the classes of vulnerabilities any product you evaluate should have policies for.

### General Database Security Policies

- List database administrator accounts and how they map to domain users.
- Product version (security patch level).
- List users with admin/special privileges.
- List users with access to sensitive columns or data (credit cards, passwords).
- List users with access to system tables.
- Database access audit (failed logins).
- Authentication method (domain, database, mixed).
- List locked accounts.
- Database communication services (listener / SQL Agent / UDP).
- Network configuration (passwords in clear text, ports, use of named pipes).
- OS level DB configuration settings.
- System tables (subset) not updatable.
- Ownership chains on database objects.
- Database links.
- Sample databases (Northwind, pubs, scott/tiger).
- Remote systems and data sources (remote trust relationships).

## Vulnerability Classes

- Default Passwords.
- Passwords: weak, blank, or same as usernames.
- Public roles or guest accounts to anything.
- External procedures: `CmdExec`, `xp_cmdshell`, active scripting, `exec`, or any programmatic access to OS level code.
- Buffer overflow conditions: XP, admin functions, Slammer/Sapphire, HEAP, etc.
- SQL Injection: `1=1`, most admin functions, temporary stored procedures, database name as code, etc.
- Network: Connection reuse, man in the middle, named pipe hijacking, etc.
- Authentication escalation: XStatus / XP / SP, exploiting batch jobs, DTS leakage, remote access trust, etc.
- Task injection: Webtasks, `sp_who`, MSDE service, reconfiguration, etc.
- Registry access: SQL Server.
- DoS: named pipes, malformed requests, IN clause, memory leaks, page locks creating deadlocks, etc.

There are many more specific things to check for, but make sure that each of these classes of threat is covered. You will need to investigate whether policies exist for specific issues you are concerned about, and if not how you can create them. Every policy should include basic information that describes the threat and how it is addressed. As the audience for any given policy may be non-technical, most vendors offer several levels of technical and non-technical description, along with links to external sources for additional research. Criticality, database component, and database version are among the standard elements. Some vendors provide mechanisms to attach your specific policy references and internal remediation data.

It is very important to understand that the total number of policies in any given product is *irrelevant*. As an example, let's assume that your database has two modules with buffer overflow vulnerabilities, and each has eight different ways to exploit it. Comparing two assessment products, one has 16 policies checking for each exploit, and the other has two policies checking for two vulnerabilities. These products are functionally equivalent, but one vendor touts an order of magnitude more policies with no added benefit. Do **not** let the number of policies influence your buying decision, and don't get bogged down in what we call a "policy escalation war". You need to compare functional equivalence and realize that if one product can check for more vulnerabilities in fewer queries, it should run faster! It will take work on your part to comb through the policies in order to make sure your requirements are met, but you need to perform that inspection regardless to ensure the product meets your requirements.

You will want to carefully confirm that the assessment platform covers the database versions you have. And just because your company supposedly migrated to Oracle 11 some time back does not mean you get to ignore Oracle 9 database support, because odds are that you have at least one instance still hanging around. Perhaps your company does not officially support SQL Server, but it just happens that some of the applications you run have it embedded. Furthermore, mergers and acquisitions bring unexpected benefits, such as database platforms you did not previously have in house, and you can find yourself unexpectedly supporting Informix, Sybase, or MySQL. Plans to migrate off a current platform have a tendency to changing suddenly, with the database sticking around in your organization many years longer than anticipated. Broad database coverage should weigh in your buying decision, even if you don't expect to need it.

The currency of policies (at least for coverage of the latest vulnerabilities) is also very important. Check to make sure the vendor has a solid track record of delivering policy updates no less than once a quarter. The database vendors typically release a security patch each quarter, so your assessment vendor should as well. A 'plan' to do so is insufficient and a warning sign. Press vendors for proof of delivery, such as release documentation or policy maintenance update announcements, to demonstrate consistent delivery of updated vulnerability policies.

Cross reference policies against database vendor information. One of the interesting friction points between database vendors and vulnerability scanning vendors is the production of complete and detailed information on vulnerabilities. You need to have a clear and detailed explanation of each vulnerability to understand how it affects your organization and what workarounds are at your disposal. Assessment vendors are motivated to provide detailed information on the vulnerability itself, and typically provide more information than the database vendors would like you to have. For whatever reason, some database vendors tend to offer overly terse descriptions of threats and corresponding patches. Press the assessment vendor for detailed information, but keep in mind the database vendor must be considered the primary source of complete and accurate *remediation* information. It is wise, either during an evaluation or in production, to cross

reference the information provided, and weigh how well the assessment vendor is providing the whole picture with the policies.

Finally, database security advice comes from many different sources. The database vendors usually supply best practice checklists for free. CERT & MITRE offer links to current threats. Assessment products usually list the policies they have developed over time based on what their research teams have learned in the field. There are other independent sources, such as the [Securosis blog](#), which offer free and independent analysis. Finally, most database vendors have regional user groups that share information on how to approach database security, which are very useful for getting complex questions answered. Check to see whether your assessment vendor has what you need, and they likely will — given that the major data breaches as of this writing leverage basic vulnerabilities. If you find something missing, find out whether your vendor can provide it for you. Policy customization and policy set management is covered in detail in the next section.

## Compliance and Operational Policies

Technically speaking, the market segment we cover in this paper is called “Database Vulnerability Assessment”. You might have noticed that we titled this paper “Database Assessment”. Our primary motivation for this change was to stress that this is not just about vulnerabilities and security. While the genesis of this market was security, compliance with regulatory mandates and company operational policies drive today’s buying decisions. In many ways, compliance and operational consistency are harder problems to solve because they requires more work and tuning on your part, so customization is a big part of obtaining usable policies for compliance and operations reports.

As an example, consider two installations of IBM DB2. The same version of this database might serve two instances of the same application; but they might be run by different companies, storing different data, managed by different DBAs, with different alterations to the base functions, running on different hardware, with different configurations. This is why configuration tuning can be difficult: unlike vulnerability policies, which detect specific buffer overflows or SQL injection attacks, operational policies are company-specific and derived from best practices.

### Operations Policies

We have already listed a number of common vulnerability and security policies. The following is a list of policies found in most enterprise scanners, which apply to IT operations on the database environment or platform.

- Password requirements: lifespan, composition.
- Data files: number, location, permissions.
- Audit log files: presence, permissions, currency.
- Product version: version control, patches.
- Itemize (unnneeded) functions.
- Database consistency checks: *e.g.*, DBCC-DB on SQL Server.
- Statistics: statspack, auto-statistics.
- Backup report: last, frequency, destination.
- Error log generation and access.
- Segregation of admin role.
- Simultaneous admin logins.

- Ad hoc query usage.
- Discovery: databases, data.
- Remediation instructions & approved patches.
- Orphaned databases.
- Stored procedures: list, last modified.
- Changes: files, patches, procedures, schema, supporting functions.

There are a lot more, but these should give you an idea of the basics a vendor should have in place, and allow you to contrast against the general security and vulnerability policies we listed earlier.

## Compliance Policies

Most regulatory requirements, whether from industry or government, are satisfied by access control and system change policies. PCI adds a few extra requirements in the verification of security settings, access rights, and patch levels; but compliance policies are generally comprised of access rules and operational policies. As the list varies by regulation, and the requirements change over time, we will not list them separately here. Since compliance is likely motivating your purchase of a database assessment product, you must dig into vendor claims to verify they offer what you need. It gets tricky because some vendors tout compliance, for example “configuration compliance”, which only means you will be compliant with *their* list of accepted settings. These policies may not be endorsed by anyone other than the vendor, and only have coincidental relevance to PCI or SOX. In their defense, most commercially available database assessment platforms are sufficiently evolved to offer packaged sets of relevant policies for regulatory compliance, industry best practices, and detection of security vulnerabilities across all database platforms. They offer sufficient breadth and depth for you to get up and running very quickly, but you will need to *verify* your needs are met, and if not then discover what the deviation is. Yes, this is hard work, but it will pay off.

Customization of policies is a weakness for most database assessment scanners and remains an area in which they must mature. Most do not allow for policy customization, multiple policy groupings, policy revisions, branding, and modification of copies of the “out of the box” policies provided by the vendor. Some products that provide these functions make it so difficult you will abandon your efforts. Further, some of the platforms have been known to overwrite your custom policies when updating policy definitions, so you will need to check that you are not going to lose your engineering effort. You need all these features for day-to-day management, so let’s explore each of these areas a little more.

## Policy Customization

Once your database assessment product is deployed, the policies you are interested in will evolve — often quite substantially. This is especially true for regulatory policies, which grow in number and change over time. Most DBAs will tell you that the steps a database vendor advises to remediate a problem can break your applications or processes, so you will need a customized set of steps appropriate to your environment. Further, most enterprises have evolved database usage policies far beyond “best practices”, and greatly augment what the assessment vendor provides. This means both the set of policies, and the contents of the policies themselves, will need to change.

Most commercial assessment vendors advertise policy customization, but what they are referring to is the criticality, and possibly the ‘state’ of the result within a workflow. What you need to customize is the description, remediation, underlying query, and result set that demonstrates conformance. As you learn more about what is possible, as you refine your internal requirements, or as auditor expectations evolve, you will experience continual drift in your policy set. Sure, you will have static vulnerability and security policies, but as the platform, process, and requirements change, your operations and compliance policy sets will be fluid. How easy it is to customize policies and manage policy sets is extremely important, as it directly affects the time and effort required to manage the platform. Does it take a minute to change a policy, or an hour? Can the auditor do it, or does it require a DBA? Learn this *before* you make an investment. On a day-to-day basis, this will be the single biggest management challenge you face, on par with remediation costs.

## Policy Groupings and Separation of Duties

For any given rule, several different audiences may be interested in the results. IT, internal audit, external audit, security, and DBAs may need assessment reports. Conversely, each of these audiences might be disinterested, or not permitted to see the results from certain rules. For example, your SQL Server database group does not need Oracle results, internal audit reports need not contain all security settings, your European database staff likely has no interest in US database reports, etc. Further, separation of duties requires some information to be blocked from different user classes. Managing and grouping policies into logical sets is very important, as the reports derived from the policy set must be specific to certain audiences. You need the ability to group according to function, location, regulatory requirements, security clearance, and so on. The ability to import, update, save different versions, and schedule one or more policy sets is mandatory for modern database assessment tools. Once again, this is an area where most vendors do a poor job and all need to mature.

Enforcement of Separation of Duties (SOD) is also a class of policies unto itself. We listed the requirement to separate administrative roles within the operational policy section, but this warrants additional explanation. It is common, for security and compliance reasons, to keep strict separation between IT, platform and database administrative accounts. This is for fraud detection and to avoid having a platform breach result in a database breach (and visa-versa). It is becoming increasingly common for database administrative responsibilities to be divided up amongst several roles. For example, data archival is performed under a separate account by a different user than the account used for schema changes or encryption key management. This precaution makes it much harder to compromise the database in the event that an admin account is compromised, and makes it easier to track alterations for change management and fraud detection.

You will want to verify that the product you select provides SoD within the product for different classes of users, as well as detection of SoD violations on the target database.

# Management & Administration

In this section we cover third major phase of the assessment process — reporting for compliance and security, remediation, job scheduling, and integration with other business systems. These features, outside the core scanning function, make managing a database vulnerability assessment product easier. Most vendors have listed these features for years, but they were implemented in a marketing “check the box” manner — this area has shown major advancements in product maturity over the last few years.

Here are some management features that warrant closer review:

## Reports

As with nearly any security tool, you’ll want flexible reporting options, but pay particular attention to compliance and auditing reports that support compliance needs. What is suitable for the security staffer or administrator may be entirely unsuitable for a different internal audience, in terms of both content and level of detail. Further, some products generate one or more reports from a single scan’s results, while others tie scan results to a single report; check if your vendor can provide aggregation and/or granular reports as needed.

Reports should fall into at least three broad categories: compliance and non-technical reports, security reports (incidents), and general technical reports. Built-in report templates save valuable time by grouping together related policies. Some vendors have worked with auditors from the major auditing firms to help design reports for specific regulations such as SOX & PCI, and automatically generate reports during a review. You will need to verify that these out of the box reports provide the level of granularity you want.

If your organization needs flexibility in report creation, you’ll likely outgrow the capability of the assessment product and need to export its data to a third-party tool. Plan on taking some time to analyze built-in reports, report templates, and report customization capabilities. Performance in this area is often poor, and some vendors require an export of scan results into a secondary repository, increasing cost.

## Alerts

Some vendors offer single policy alerts for issues deemed critical. These issues can be highlighted and escalated independent of other reporting tools, providing flexibility in how to handle high priority issues. Assessment products are considered a preventative security measure, so unlike monitoring alerting is not a typical use case. Policies are grouped by job function, and rather than provide single policy scanning or escalation internally, critical policy failures are addressed through trouble-ticketing systems, as part of normal maintenance. If your organization is moving to a “patch and shield” model, prioritized policy alerts are a long-term feature to consider.

## Scheduling

You will want to schedule checks to run on a periodic basis, and all platforms provide schedulers to launch scans. Job scheduling is provided internally, or optionally via external software or even as UNIX “`crontab` jobs”. Most customers we speak with run security scans on a weekly basis, but compliance scans vary widely. Frequency depends upon type and category of the policy. For example, change management / work order reconciliation is a weekly cycle at many companies, and a quarterly job at others. Vendors should be able to schedule scans to match your cycles.

## Remediation and Integration

Once policy violations are identified, you need to get the information into the right hands so that corrective action can be taken. The people who handle these issues come from either a database or a security background, so look for a tool that appeals to both audiences and supplies each with the information they need to understand incidents and investigate appropriately. Typically this is done through reports or workflow systems. Some assessment providers use reports to notify of policy violations, while others use email, internal workflow tools, or send simple network management protocol (SNMP) traps into external workflow or trouble ticket systems such as [Remedy from BMC](#). As we discussed in the policy section, each policy should have a thorough description, remediation instructions, and references to additional information. Addressing all your audiences is both a policy and report customization effort for your team. Some vendors provide hooks for escalation procedures and delivery to different audiences. Others use relational databases to store scan results and can be directly integrated into third-party systems.

Automated remediation, meaning automatically fixing a problem at the time it is discovered, is not a universal requirement. Only a small percentage of customers we speak with want or use this capability. The issue is that patches or configuration changes may require a system restart, might alter the behavior of the database, could break existing application logic, or can otherwise create any number of unintended side effects. A handful of commercial vendors support automated remediation. Validate that they offer what you need, and can enable/disable it at the policy level.

## Result Set Management

All the assessment products store scan results differently. Some store the raw data retrieved from the database, others store the results of their comparisons of raw data against policy, and still others only store reports rather than their raw scan data. Most vendors use relational databases to store results, while others use flat files. How data is stored and in what form are important. For example, trend analysis (which is necessary to meet certain regulatory requirements) requires storage of scan results for a year or more. If policies change and you are storing only raw data, rerunning reports will return different results. Investigate how each product stores and retrieves prior scan results and reports: by keeping raw result data, just policy violations, reports, or all three. Trend analysis is important for understanding how security is affected by normal administration and patch management. Tools which use an internal database to store the information tend to make third party reporting easy, whereas others use flat files to improve performance at the expense of ease of use. Consider how historic data is presented to ensure it satisfies your requirements.

## Platform and Deployment

Assessment scanners are offered both as appliances and as software. Remote credentialed assessments are available as SaaS as well. Your vendor should provide a web management interface over a secure connection. Proper account management is needed to enforce roles for policy creation, database credential management, and scan results. Some vendors offer integration with external access control systems to reduce administration and setup effort. These scanners require maintenance, like any other platform. If the vendor is using a relational database to store data within their application stack, it will impact security and operations (positively and negatively), and should be included as one of your regularly scanned databases. And as the number of scans increases over time, the internal repository will need to be purged of older results.

As with any product, it's sometimes difficult to cut through the marketing materials and figure out if a product really meets your needs. The following breakdown of functional elements is intended to give you an idea of what is possible with state of the art products, and a basic checklist of functions to review for a proof of concept. While the cost of the assessment features is much less than monitoring or auditing solutions, don't skimp on the evaluation, and make sure you test the products as thoroughly as possible. The results need to satisfy a large audience and be integrated with more systems than DAM or other auditing products.

# Database Assessment Selection Process

## Define Needs

Before you start reviewing products, have a clear understanding of your goals and how database assessment will be employed. Assessment is used by many different stakeholders for management, policy creation, and incident handling.

1. Create a selection committee: Assessment generally involves 4-5 major groups of stakeholders, from both technical and non-technical backgrounds. On the technical side it's important to engage the database, IT management, and security teams to define both policies and workflow. On the non-technical side, audit and compliance personnel tend to specify the requirements. The purchase is typically driven by their requirements and comes out of their budget. Once these audiences see what is possible, projects that started with a limited scope can quickly grow into enterprise-wide programs, so plan accordingly. As the selection process usually comes down to two closely graded solutions, make sure someone on the team has authority to make the final call.
2. Map policy requirements: Determine exactly what you are trying to accomplish and document goals. Non-technical groups should provide detailed policy and report requirements. Policy sets and guidelines should be ready before product evaluation. If compliance is the goal, mapping abstract compliance requirements to database functions is necessary.
3. Map system requirements: Audit and compliance groups are the primary beneficiary, but security and database teams are typically the implementers and define the platform requirements. Define system and management preferences, such as agent vs. non-agent. Determine who will manage databases, the assessment platform, credentials, and reports.
4. Outline process workflow, remediation and reporting requirements: Once issues are found, how are they fixed? By whom? When are the reports re-run to verify changes? Smaller organizations generally use vendor supplied workflow and tracking, while enterprises tend to link assessment into existing workflow systems.
5. Ascertain budget. The scope of your project, priorities, and coverage are shaped by available funds. Assessment is a product where maintenance is not optional. Tier your priorities.

With the completion of this phase you should have defined key stakeholders, defined policies, prioritized which systems to protect, and produced a rough outline for your workflow. You should understand your minimum requirements and preferred options. You are ready to begin evaluating vendor solutions.

## Formalize Requirements

This phase can be performed by a smaller team working under the mandate of the selection committee. Take the guidelines and requirements from the previous stage, and formulate a Request For Information (RFI) document. This will require translating business requirements into specific technical features and documenting any additional features or requirements that come to light during this effort. This is the time to come up with any criteria for directory integration, additional infrastructure integration, data storage, change management integration, and so on. You can always refine these requirements after you proceed to the selection process and get a better feel for how the products work. At the conclusion of this stage you will have a formal RFI (Request For Information) for vendors, and a rough RFP (Request For Proposals) to clean up and formally issue in the evaluation phase.

## Evaluate Products

The following steps should minimize your risk and help you feel confident in your final decision:

1. Issue the RFI: Larger organizations should issue an RFI through established channels and contact a few leading vendors directly. If you're a smaller organization, start by sending your RFI to a trusted VAR and email a few of the assessment vendors which seem appropriate for your organization.
2. Perform a paper evaluation: Before bringing anyone in, match any materials from the vendor or other sources to your RFI and draft RFP. The goal is to build a short list of 3 products which match your needs. You should also consult outside research sources and product comparisons.
3. Bring in 3 vendors for on-site presentations and demonstrations: Instead of a generic demonstration, ask each vendor to walk through your specific use cases. Don't expect a full response to your draft RFP — these meetings are to help you better understand the different options and eventually finalize your requirements.
4. Finalize your RFP and issue it to your short list of vendors: At this point you should completely understand your specific requirements and issue a formal, final RFP.
5. Assess RFP responses and begin product testing: Review the RFP results and drop anyone who doesn't meet any of your hard requirements (such as platform support), as opposed to "nice to have" features. Then bring in any remaining products for in-house testing. You'll want to replicate remote testing, scheduling, and workflow situations. Build a few basic policies that match your use cases, then violate them so you can get a feel for policy creation, reporting and workflow.
6. Select, negotiate, and buy: Finish testing, take the results to the full selection committee, and begin negotiating with your top choice.

## Internal Testing

In-house testing is the last chance to find problems during the selection process. Make sure you test as thoroughly as possible. The database assessment platform will be used as a key tool to automate jobs across several business units, so time you invest prior to purchase will be worth it. A few key aspects to test, if you can, are:

- Policy creation and management. Create policies to understand the process and its complexity. Do you need to write everything as SQL? Will built-in policies meet your needs? Are there wizards and less-technical options for non-database experts to create policies? Can you group policies together for common job functions?
- Platform support and installation. Determine compatibility with your database/application environment. Does the platform collect the data you need? Does it offer the deployment options you need?
- Data storage. How does it store results? How is data managed internally? How is it secured?
- Performance. How long do scans take to perform? How many scans can run at the same time? What scheduling options are available? Does the scan impact the database? Can it maintain connections to remote offices? Is SSL an option?
- Incident workflow. Review the working interface with those employees who will be responsible for enforcement.
- Account management, SOD and directory integration. Assessment should provide segregation of duties between IT and DBA staff, and between internal audit and security.

# Conclusion

Database Assessment is not just a security precaution, but an integral part of database operations management. Databases form the backbone of every major application within the data center, which makes their stability and security both critically important to business operations. Timely, accurate scans, in combination with uncovering problems with setup and maintenance, are essential for operations management — just as detection of vulnerabilities is essential to keeping data secure.

This guide should provide the information necessary to evaluate products both individually and head-to-head; and help you avoid many of the problems that pop up after acquiring a product and coming to grips with actual usage. We hope you will review all these topics to avoid pitfalls during the evaluation, even if only a fraction are used in your own consideration. While the evaluation effort can be daunting, we encourage head to head comparisons and diving into operational details, as it is very difficult to replace a product once you have deployed it. And in many cases what is considered ‘the best’ by the industry at large may not meet your requirements, or may not integrate into your organization, outweighing technical benefits others deem important.

# Who We Are

## About the Author

### **Adrian Lane, CTO/Senior Analyst**

Adrian Lane is a Senior Security Strategist with 22 years of industry experience, bringing over a decade of C-level executive expertise to the Securosis team. Mr. Lane specializes in database architecture and data security. With extensive experience as a member of the vendor community (including positions at Ingres and Oracle), in addition to time as an IT customer in the CIO role, Adrian brings a business-oriented perspective to security implementations. Prior to joining Securosis, Adrian was CTO at database security firm IPLocks, where he was responsible for product and technology vision, market strategy, PR, and security evangelism. Mr. Lane also served as Vice President of Engineering at Touchpoint, for three years as CIO of the brokerage CPMi, and for two years as CTO of the security and digital rights management firm Transactor/Brodia. Mr. Lane is a Computer Science graduate of the University of California at Berkeley with post-graduate work in operating systems at Stanford University.

## About Securosis

Securosis, L.L.C. is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services.

We provide services in four main areas:

- Publishing and speaking: including independent, objective white papers, webcasts, and in-person presentations.
- Strategic consulting for end users: including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessments.
- Strategic consulting for vendors: including market and product analysis and strategy, technology guidance, product evaluations, and merger and acquisition assessments.
- Investor consulting: technical due diligence, including product and market evaluations, available in combination with deep product assessments with our research partners.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Securosis has partnered with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis.