IMPERVA®

Four Ways Built-in Database Auditing Drains Your IT Budget

WHITE PAPER

Introduction

IT organizations are under pressure to deliver innovative solutions, while keeping overall IT costs in check. Secular technology trends like mobile, cloud, and big data capture the attention of budget holders, making it difficult for IT professionals to locate funding for other important projects. That's why database auditing and protection projects often leverage existing resources, particularly built-in database auditing tools. The problem with built-in database auditing is that it leaves businesses with compliance and security gaps and burdens them with expensive hidden costs.

This paper explores four key built-in database auditing inefficiencies that drain IT budgets. It will also demonstrate how organizations can use an automated solution to streamline database audit and protection and, in the process, free up more than 80% of the IT resources and budget dollars they are spending on database compliance today.

Reality Check

Built-in database auditing mechanisms bring hidden IT infrastructure requirements, high initial and operational costs, and significant impact to application, database and file server performance.

Database Auditing Drivers

The drivers for database monitoring projects are undergoing an expansion. Historically, virtually all database monitoring projects focused on meeting compliance requirements for SOX, PCI, MAS and dozens of other mandated regulations and laws. Following the high-profile breaches of Sony and Anthem, companies began looking for a way to improve data security. That research revealed requirements for data security monitoring overlap the requirements for data monitoring for compliance - with a few notable additions to address larger data volumes, security policy management, and suspicious activity response.

Organizations Use Built-in Database Auditing

Imperva finds that 80% of companies are now looking at a monitoring solutions to improve both compliance and security. The research indicates that 32% currently have no monitoring solution in place and 46% are looking to replace native database auditing tools. Many organizations start with these "free" built-in database auditing tools believing they are an and inexpensive solution for database monitoring, and therefore a simple and cost-effective route to compliance. The reality is that organizations using the built-in approach spend vastly more than they realize and are actually unable to meet compliance requirements.

[1] Closing the Security Gap: 2012 IOUG Enterprise Data Security Survey

Built-in Database Auditing is Inefficient

In order for built-in database auditing solution to provide sufficient information for compliance reporting, they must be configured to record all database access activity resulting in the accumulation of a huge amount of unnecessary information. By capturing everything, built-in database auditing also takes a serious toll on database performance. In addition to a performance hit, storing and administering the audit data imposes additional costs. For example, on the administration front, there is the initial cost of building scripts to analyze data and create reports, and then the ongoing costs of maintaining those scripts. Because built-in auditing is not scalable, even small changes in the database environment require script updates. To extract information from the audit data, hours of specialized IT labor must be dedicated to sorting through the mountains of native database audit logs. In addition to those direct costs, the inability to produce meaningful reports for audit and security can cost organizations a fortune in terms of data breach and non-compliance costs.

Revealing the Hidden Costs

To illustrate the hidden and surprisingly large costs of native database auditing, we walk through an example scenario in the following pages. We look at the very common use-case of monitoring privileged user activities. Our example covers a 100 database environment, with 70 Oracle databases and 30 Microsoft SQL databases.

Why Built-In Database Auditing Is Inefficient

1. Extra hardware and software required
2. Extra storage required
3. Extra labor required
4. Increased chances of data breach and non-compliance

Inefficiency 1:

Extra Hardware and Software

The largest expense related to built-in database auditing is the need for additional hardware and software. Built-in database auditing increases database load by around 20%, a figure reported by Imperva customers and confirmed by database vendor Oracle[2]. A 20% performance hit means that in order to maintain the same database performance level an organization had before built-in auditing was turned on, one extra database server must be added for every five database servers being monitored. Of course, in addition to each new physical or virtual server added to the data center rack, a database software license is also required.

To get an idea of how costly this can be, consider our 100 database environment. Table 1 illustrates the need for $3.5 million in the up-front costs of servers and database license fees to offset the 20% performance degradation caused by built-in database auditing.

Table 1 shows that in our example environment, twenty extra database servers are needed to compensate for the impact of built-in database auditing. Each server is assumed to have twelve cores and a list price of around $10,000. Database software is licensed by server cores, with an average cost per core of $14,000.

COMPONENT	BUILT-IN DATABASE AUDITING SOLUTION	IMPERVA SECURESPHERE DATA SECURITY SOLUTIONS
Auditing Performance Impact	20%	2%
Additional Database Servers Required	20	2
Hardware Cost Per Server	~ $10,000	~ $10,000
Average Database License Cost (Per Server Core)	~ $14,000	~ $14,000
Average Number of Cores Per Server	12	12
Extra Hardware and Software	**$3,560,000** (20 x 10,000) + (20 x 12 x 14,000)	**$356,000** (2 x 10,000) + (2 x 12 x 14,000)

Table 1. (All Pricing at List Price)

Reality Check

Built-in native database auditing requires 20 additional database servers for every 100 database servers being monitored.

Imperva SecureSphere requires 2 additional database servers for every 100 database servers being monitored.

The Imperva SecureSphere Cost Advantage

Because privileged activity is performed directly on databases, Imperva SecureSphere agents are used for auditing access activity. These lightweight agents consume only a fraction of the performance of native auditing (i.e., 2% vs. 20%), because they offload the processing to Imperva SecureSphere network-based gateways. In this example environment, the use of Imperva SecureSphere agents requires that two additional database servers be added, in order to maintain the original database performance level across the one hundred databases. When you compare that to the 20 additional database servers required when using built-in auditing, Imperva SecureSphere reduces the cost by 90%.

[2] "Oracle White Paper–Oracle Database Auditing: Performance Guidelines," August 2010

Inefficiency 2:

Extra Storage

The second largest expense related to built-in database auditing is the storage cost. Most organizations end up capturing and storing all database audit traffic, regardless of relevance, when using built-in database auditing. This necessitates retaining massive amounts of data, which drives additional storage cost.

The reason organizations end up with so much audit data is because it is rarely possible to generate only relevant information with native auditing. Although Oracle and other database vendors offer what is called "fine grained auditing," it is generally not a viable solution. Fine grained auditing is the ability to selectively generate or retain only relevant information by using policies. While fine grained auditing sounds like it would make native auditing practical, it becomes operationally impossible for all but the smallest environments. That is because fine grained auditing requires manually tuning and configuring auditing for each database individually. With a database environment of any significance, this approach is impractical. As a result, many organizations do not use fine grained auditing even when provided.

In a 100 database environment without fine grained auditing, nearly five terabytes of compressed data is captured per day[3]. Using an industry average list price of $0.41 per gigabyte for storage, Table 2 illustrates that it takes nearly a million dollars per year to store this amount of data.

COMPONENT	BUILT-IN DATABASE AUDITING SOLUTION	IMPERVA SECURESPHERE DATA SECURITY SOLUTIONS
Audit Level	Full Auditing	Privileged User
Queries Per Second (Per Database)	500	1
Query Size[4]	25 KB	1 KB
Data Written Per Day	103,000 GB	21 GB
Compressed Data Per Day (20 to 1)	5,150 GB	1 GB
Yearly Additional Audit Data	1,879,692 GB	376 GB
Cost Per Gigabyte	$0.41	$0.41
Yearly Storage Cost (Additional yearly audit data X price per GB)	**$770,674**	**$154**

Table 2. (All Pricing at List Price)

Reality Check

Built-in native database auditing needs to store over 5,000 gigabytes of compressed data per day in a 100 database environment incurring well over a half million dollars in storage costs per year.

Imperva SecureSphere needs to store 1 gigabyte of compressed data per day in a 100 database environment incurring only 154 dollars in storage costs per year.

The Imperva SecureSphere Cost Advantage

While built-in database auditing captures a great deal of information, most of it is irrelevant for monitoring privileged users. In general, privileged user activity accounts for only 1% to 3% of all database activity. Imperva SecureSphere is able to monitor all traffic for security violations while permanently capturing only what is needed. In this example, that means that one gigabyte per day of storage costs are incurred with Imperva SecureSphere.[5] That translates to $200 per year for Imperva SecureSphere, in contrast to nearly $1million for native auditing.

[3] Approximately 500 queries are recorded every second and each query is about 25 kilobytes without fine grained auditing.

[4] Query size based on: Auditing in SQL Server 2008, http://msdn.microsoft.com/en-us/library/dd392015%28v=sql.100%29.aspx

[5] Assumes one kilobyte query per second when using Imperva SecureSphere to capture privileged user activities.

Inefficiency 3:

Labor

The process of setting up and maintaining database auditing rules is complex and requires a certain amount of expertise and communication between developers, database administrators (DBAs), compliance experts, and security staff. Typically, this process diverts already-stretched DBA resources from their core functions, which proves to be extremely disruptive and expensive on an ongoing basis. Given the complexity of database applications in use and the number of people using them in a typical organization, native auditing rules must be constantly updated, in order for the auditing mechanism to remain effective. Typically, this means that the scope of the audit is limited to a small subset of the full database environment. This limitation of scope may prevent an organization from passing an audit. Furthermore, built-in database auditing mechanisms cannot separate legitimate activity from behavior that is non-compliant. Therefore, demonstrating compliance means sifting manually through mounds of unintelligible logs. Built-in database auditing requires extensive time and the use of additional technologies to parse the data and to place it into context, so that humans can make sense of it. Since the native audit logs will store the actual SQL query text used, sensitive data like credit card numbers or social security numbers could be recorded in the logs as plain-text the company could actually put data at great risk of non-compliance and data loss.[6]

Maintaining a built-in database auditing solution requires more full time employees (FTE) compared to an automated database auditing solution. Imperva customers report approximately five FTEs, or $600,000[7] of yearly labor cost to support built-in database auditing in an environment like our 100 database example. Table 3 provides a breakdown of where the FTEs are needed, in terms of administration and auditing cost.

COMPONENT	BUILT-IN DATABASE AUDITING SOLUTION	IMPERVA SECURESPHERE DATA SECURITY SOLUTIONS
Implementation and Training Cost	0 FTE	~ .1 FTE
Administration Cost	~ 4 FTE	~ .9 FTE
Auditing Cost	~ 1 FTE	~ .5 FTE
Total FTE Count	~ 5 FTE	~ 1.5 FTE
Annual System Administrator Salary	$120,000	$120,000
Yearly Labor Cost (Total FTE Count X Annual salary)	**$600,000**	**$180,000**

Table 3.

Reality Check

Built-in native database auditing requires 5 full time employees, or $600,000 of yearly labor cost, to support a 100 database environment.

Imperva SecureSphere requires 1.5 full time employees, or $180,000 of yearly labor cost, to support a 100 database environment.

[6] Oracle Audit Vault and Database Firewall Concepts Guide, #3 Be careful when auditing sensitive information http://docs.oracle.com/cd/E69292_01/doc.122/e49916/agent_deployment.htm#SIGCC90093

[7] Assumes a US$120,000 annual system administrator salary.

The Imperva SecureSphere Cost Advantage

Imperva SecureSphere is easy to install and easy to maintain on an on-going basis. Audit rules can be applied to multiple or all databases in a logical or physical environment,, compared to manually adjusting audit policies for each individual database with built-in auditing. This allows organizations to implement an audit solution in a matter of weeks, compared to months. This also makes the on-going maintenance of the solution very simple when introducing new, moving, or retiring old, databases. In turn, expensive and highly skilled DBA resources do not have to be diverted from their primary responsibilities to manage the audit mechanism. Imperva customers report that approximately 1.5 FTEs, or $180,000 of yearly labor costs, are required to support an environment of the size in our example.

Inefficiency 4:

Increased Chances of Data Breach and Non-Compliance

The extensive amount of data collected by built-in database auditing is meaningless for forensic and audit purposes. Built-in database auditing does not provide intelligence on malicious activity, which forces organizations to manually identify violations. On the other hand, Imperva SecureSphere's Dynamic Profiling technology understands normal usage patterns and can act on suspicious behavior immediately. Imperva SecureSphere's technology has a dramatic impact on reducing the chances of data breaches. Reducing the chances of data breaches is important. The Ponemon Institute reported the average cost of a data breach at $3.8 million per incident.[8]

Furthermore, the complexity and overhead associated with configuration and maintenance of a built-in database auditing solution typically relegates an organization's database auditing activity to a small portion of their actual infrastructure. This leaves most of the enterprise unmonitored, which can be a costly decision, from a risk management perspective. Taking this approach can cost organizations a fortune. Another Ponemon study reports the average cost of non-compliance is $9.4 million dollars[9]

What Data Breach and Non-Compliance Could Cost Your Business

- The average cost of a data breach = **$3.8 million per incident**
- The average cost of non-compliance = **$9.4 million dollars**

[8] 2015 Cost of Data Breach Study: Global Analysis," Ponemon Institute, March 2015

[9] True Cost of Compliance, Ponemon Institute, January 2011

Total Cost of Ownership (TCO) Comparison

The total cost of ownership for built-in database auditing and Imperva SecureSphere can be calculated by summing up the costs for the three major components described earlier: 1) extra hardware and software, 2) extra storage, and 3) labor. For simplicity's sake, we exclude the costs of data breach and non-compliance.

Table 4 compares the cost of using a built-in database auditing solution to using Imperva SecureSphere, over a one year period of time. The total cost with built-in database auditing for this environment is around $5 million, while the cost with Imperva SecureSphere reduces that figure to $930,000, or by 80%.

COMPONENT	BUILT-IN DATABASE AUDITING SOLUTION	IMPERVA SECURESPHERE DATA SECURITY SOLUTIONS
Extra Hardware & Software	~ $3.56M	~ $356k
Extra Storage	~ $771k	~ $154
Labor	~ $600k (~ 5 FTEs)	~ $180k (~ 1.5 FTE)
Imperva SecureSphere Solution		~ $413k
Total Cost of Ownership	**~ $5M**	**~ $950k**
Savings		**~ $4M**
Percentage Saved: 80%		

Table 4. TCO Comparison.

Conclusion

Organizations are under pressure to improve security, while keeping overall IT costs in check. However, using built-in database auditing tools with the hope of minimizing cost is a misconception. Built-in database auditing leaves businesses with compliance and security gaps and expensive hidden costs.

IT organizations that rely on native capabilities built into their databases end up with a manual, inefficient, and partial solution to compliance requirements. Built-in database auditing mechanisms bring hidden IT infrastructure requirements, high initial and operational costs, and significant impact to application, database performance.

Imperva SecureSphere audit and protection solutions automate manual processes with core capabilities that include activity monitoring and auditing, user rights management, and automated business policy enforcement and proactive blocking of suspicious behavior. These capabilities transform time-consuming, error-prone management tasks into efficient processes, and allow institutions to cost-effectively meet data compliance requirements. Imperva SecureSphere Database Security solutions enable organizations to achieve compliance objectives, while dramatically reducing costs through increased IT operational efficiency.

If you would like to apply this ROI/TCO analysis to your own organization, please contact our security specialists.

About Imperva

Imperva® (NYSE: IMPV), is a leading provider of cyber security solutions that protect business-critical data and applications. The company's SecureSphere™, Incapsula™ and Skyfence™ product lines enable organizations to discover assets and vulnerabilities, protect information wherever it lives - onpremises and in the cloud - and comply with regulations. The Imperva Application Defense Center, a research team comprised of some of the world's leading experts in data and application security, continually enhances Imperva products with up-to-the minute threat intelligence, and publish reports that provide insight and guidance on the latest threats and how to mitigate them. Imperva is headquartered in Redwood Shores, California.

Case Study

Global Bank Cuts $90 Million in Excess IT Costs

One of the largest banks in the world replaced the database auditing system they developed in-house with Imperva SecureSphere. This case study reveals how Imperva SecureSphere saved the bank over $90 million by streamlining hardware and software spending, eliminating database server load, and reducing manual processes that relied upon built-in database auditing.

Download Case Study