Seven Keys to a Secure Data Solution

How to choose the right data centric audit and security solution
**Introduction**

Explosive growth in the amount of data they are generating and a marked increase in the number and types of repositories in which it is being stored are driving today’s enterprise to revisit their strategies for data security and governance. Rather than relying on tools and methods that result in numerous disconnected pockets of coverage, the focus needs to shift to data-centric audit and protection (DCAP). However, as with any enterprise class solution, there is considerable variation among available offerings. To help organizations navigate the evaluation process, this paper shares seven ways Imperva SecureSphere solutions for data security and governance surpass the competition.

**The Need for DCAP in the Enterprise**

Every high-profile breach and exposure of customer or proprietary information brings renewed pressure to ensure the sensitive data stored by your organization is adequately protected from a multitude of sophisticated cyber threats and attackers. At the same time, complying with data security and privacy regulations – not to mention internal policies – requires complete visibility and an uninterrupted record of which data is being accessed by which users and systems.

For most enterprises, additional challenges include:

- Exponential growth in the volume and usage of data requiring protection
- The introduction of new types of data repositories, as big data platforms and cloud-based enterprise file-sharing services begin to operate alongside traditional databases, file servers, and data-rich collaboration systems, such as SharePoint
- The inevitable spread of data across these repositories, as the business strives to extract maximum value by using it in support of an ever-expanding array of business processes

The net result is the need for enterprises to abandon approaches to data security and governance that rely on silos of narrowly focused native (i.e., on database) and standalone tools. According to Gartner, future investments should focus instead on more effective and efficient DCAP solutions that combine an extensive set of data security and audit functionality with the ability to eliminate disparate management silos and inconsistencies by coordinating associated policies across numerous types of data stores.¹

**The Imperva Difference**

Whether it is your risk, security, compliance or database team – or better yet, all of them working together – acknowledging the need for something more than silo-specific and single-function tools is only a starting point. Evaluators also need to recognize the considerable variation that exists among available DCAP solutions. After all, making a poor choice can lead to many of the same deficiencies exhibited by the patchwork approach, including inconsistent policies and gaps in coverage that increase the risk of breaches and failed audits, inadequate scalability, and run-away total cost of ownership (TCO).

To help organizations avoid the costs and other consequences of choosing poorly, the following sections describe seven ways Imperva SecureSphere surpasses the competition.

¹*Market Guide for Data-Centric Audit and Protection*, Gartner, November 2014
#1 – Faster Time to Value

Enterprises can ill-afford to leave sensitive data stores exposed and unmonitored for any length of time. Unlike competing solutions where large-scale implementations have been known to stretch from months into years, Imperva customers benefit from considerably faster deployments and quicker time to value – regardless of whether coverage is being established for ten, one hundred, or ten thousand repositories.

Key features that make this possible include:

- A scalable architecture that reduces the number of components that need to be deployed, typically by at least 2X compared to competing solutions (see #4 below)
- The availability of non-intrusive network deployment options that overcome the inter-departmental battles and accompanying delays that often plague efforts to deploy agents on business-critical, performance constrained, or otherwise “touchy” systems (see #2 below)
- A rich API that not only enables automated, bulk configuration of SecureSphere components, but also facilitates rapid integration with the rest of an organization’s security, compliance, IT provisioning, and ticketing systems
- An extensive array of out-of-the-box “content” that eliminates the need to build/configure everything from scratch, including audit policies, vulnerabilities, configuration checks, workflows, and reports for common applications, repositories, and regulations

Rather than having to incur the risks and costs of a drawn-out deployment, SecureSphere enables enterprises to rapidly establish protection and streamline regulatory compliance efforts for all of their important data repositories – both those they currently have, plus the new ones that are being added seemingly on a daily basis.
#2 – Greater Flexibility and Adaptability

SecureSphere is not constrained by being an “agent-only” solution. To be clear, lightweight, low-impact agents are indeed part of the solution. In fact, they are the only option, outside of native features, for monitoring and controlling direct, local access to a repository. SecureSphere also offers enterprises the choice of two, non-intrusive network-based deployment options: an out-of-band “sniffer” mode and an inline, transparent bridge mode that delivers greater blocking capabilities. A hybrid deployment of agent and network based monitoring is used by many SecureSphere clients to ensure they are maximizing coverage and performance.

In addition, the data collection (Gateway) and management (Management Server) components of the solution can be implemented either as purpose-built hardware appliances or dynamic, cloud-ready virtual appliances. This level of adaptability is hard to find in competing offerings.

SecureSphere provides coverage for an extensive set of relational and big data platforms, including: Oracle (including ASO/SSL), Oracle Exadata, Microsoft SQL Server, IBM DB2 (on Linux, UNIX, Windows, z/OS and DB2/400), IBM IMS on z/OS, IBM Informix, IBM Netezza, SAP Sybase, Teradata, Oracle MySQL, PostgreSQL, Progress OpenEdge, Cloudera Enterprise and Hortonworks. It is also the only enterprise-class data monitoring and protection solution with support for the AWS environment.

The net result is immediate, out-of-the-box applicability for the broadest range of enterprise use cases, scenarios, and data infrastructure, both now and as your organization’s needs change going forward.
#3 - Greater Breadth and Depth of Functionality

While native tools are often “monitoring only” and unable to stop egregious activities from occurring, many standalone alternatives suffer from a similar deficiency in that they only provide a limited set of functionality. In comparison, Imperva delivers a single, tightly integrated solution that enables enterprise security, compliance, and database administration teams to:

- Detect all databases requiring attention through automated discovery and classification of sensitive data
- Continuously monitor and audit all access to sensitive data
- Uncover unauthorized access and fraudulent activity by maintaining baselines of normal usage patterns and transactions and then flagging any deviations that are observed
- Alert and block attacks and unauthorized activities in real time
- Exchange and correlate user activity with the SecureSphere Web Application Firewall
- Stop targeted attacks and other advanced cyber threats through out-of-the-box integration with leading anti-malware solutions
- Detect and virtually patch database vulnerabilities
- Accelerate incident response and forensic investigations with advanced techniques for visualizing and analyzing detected events
- Rapidly configure data protection policies and associated compliance reports by taking advantage of pre-defined rule sets and templates for a wide variety of applications, data stores, and regulations
- Establish a repeatable, automated process for compiling, reviewing, and managing user access rights across heterogeneous data stores
- Automate reporting and compliance activities across the entire database environment

With SecureSphere, enterprises are freed from the burden of having to cobble together numerous disparate products to get the essential data protection and audit capabilities they require.

#4 - Greater Scalability and Predictable Planning

With the number of data repositories at the average organization running into the hundreds or even thousands, evaluators need to pay particular attention to the scalability of any solutions they are considering. Poor scalability has the potential to negatively influence everything from time to value, adaptability, and functionality to the costs for product licenses, hardware, daily operations, maintenance, and support.

Major advantages SecureSphere has in this area include:

**The use of big data techniques for collecting and processing audit data.** Compared to solutions that rely on relational database techniques for handling data, using indexed flat-files and taking advantage of other big data methods allows SecureSphere to operate with anywhere from 2-5X fewer data collection gateways.

**Native clustering for data collection gateways.** With SecureSphere, organizations avoid having to purchase and deploy standalone load balancers to scale the collection and processing capacity for audit data. They also avoid having to live with solutions that employ undesirable practices to recover a measure of scalability - such as abbreviating monitoring records or otherwise reducing functionality, both of which could result in missed security or compliance events.
SecureSphere Operations Manager (SOM): A manager-of-managers, SOM helps overcome the “disconnected islands” problem that plagues some solutions. Maintaining consistent data security policies and creating unified enterprise-wide compliance reports remains straightforward even for very large implementations.

Yet another advantage of SecureSphere is the fact that its degree of scalability is predictable. Unlike the situation with solutions where the metrics of how many collectors are needed to audit and protect a given number of data stores are either variable or a closely held secret, Imperva customers can accurately budget and plan their deployments.

The Proof is in the Numbers

A global computer manufacturer’s deployment of IBM Guardium took over three years and required 135 virtual appliances to monitor 500 databases. Switching to SecureSphere, it took the same company less than six months to implement monitoring and protection for 1050 databases, using only 60 virtual appliances. Related operating costs were cut by over 70 percent, saving the company nearly $2 million annually.

#5 – Non-stop, Real-time Visibility and Blocking

SecureSphere maximizes protection and minimizes the potential for failed audits by delivering real-time access to event data, proactive blocking of unauthorized and suspicious activities, and non-stop availability of DCAP functionality.

Real-time visibility. The same architecture features responsible for its enhanced scalability also allow SecureSphere to provide customers with real-time access to monitoring data and reports. In comparison, solutions with legacy architectures are forced to batch and periodically aggregate audit data, causing delays of up to a day before administrators can view, analyze, and respond to any detected issues.

Real-time blocking. While many solutions available in the market are “monitoring only,” SecureSphere includes the ability not only to detect but also stop in real-time any activities that represent policy violations, are associated with known threats, or are otherwise suspicious in nature.

Non-stop coverage. The native clustering capability discussed previously is one feature that helps eliminate lapses in DCAP coverage. So too is the Imperva practice of ensuring backward compatibility for all upgrades. This avoids the challenge customers of alternative solutions face when conflicts between versions result in diminished functionality and an incomplete audit record for however long it takes them to transition their entire environment to the new level of software.
#6 – Lower TCO

Every feature covered to this point – from having an advanced architecture and native clustering to real-time visibility – helps in some way to ensure a lower TCO for SecureSphere relative to competing solutions. But the economic advantages do not stop there. Additional market-leading features that deliver comparatively higher operational efficiency include:

- Interactive audit analytics, for rapidly viewing, analyzing, and investigating event data
- Automated workflows, for seamlessly responding to discovered issues and discrepancies
- Centralized management that substantially reduces the need locally administer agents, one at a time
- Automated feeds/updates for various types of DCAP content, including pre-defined policies, vulnerabilities, best-practice configuration guidelines, and report templates

Instead of being saddled with manually intensive mechanisms for configuring, operating, and maintaining their DCAP solution, with SecureSphere, security and compliance teams benefit from streamlined dashboards and intelligent automation.

#7 – Greater Focus and Responsiveness

Data-centric audit and protection is not a secondary solution we maintain to help sell more databases, or just another piece of technology we acquired to help become a one-stop shop for everything security. Instead, it is a core component of our strategy to provide the modern enterprise with the best solutions possible to protect its data, applications, and reputation.

Specific ways customers benefit from our laser focus on what matters most to today’s businesses include:

**Our solution.** SecureSphere is not a legacy, workgroup, or small business product that is constantly being retrofitted in a multitude of ways and stretched beyond its architectural limits in order to meet the needs of the modern enterprise. It was purpose-built from the outset to provide our customers with an enterprise-class DCAP solution that is feature-rich and highly scalable, yet cost effective and easy to use.

**Our expertise.** Focused on solving the challenges of enterprise data protection for more than 12 years, we have never been subject to the disruptions in development and support, or the “brain drain,” that often plague products obtained via acquisition.

**Our responsiveness.** At the tactical end of the spectrum, our dedication to data protection ensures that customers making support requests are not “bounced around,” but instead gain access to a support specialist conversant in data protection right out of the gate. More strategic in nature is the effort Imperva puts in to engage with enterprises, stay abreast of the challenges they face, and ensure SecureSphere remains a market-leading solution that is closely aligned with their needs – however those change over time.
Conclusion

Explosive growth in the amount of sensitive data being generated – not to mention the number and types of repositories in which it is being stored – is driving enterprises to move beyond using native database tools and other narrowly focused products as the basis for their data security and governance infrastructure. Future investments need to focus instead on more effective and efficient DCAP solutions that combine extensive data security and audit functionality with the ability to eliminate disparate management silos and inconsistencies by coordinating policies across numerous types of data stores. Not only is Imperva SecureSphere such a solution, it also surpasses competing offerings in several important areas, including time to value, adaptability, scalability and TCO – just to name a few.

To learn more about SecureSphere and other Imperva solutions for protecting your organization’s data, applications, and reputation, please visit imperva.com.