



IBM InfoSphere Guardium Vulnerability Assessment

Scan database infrastructures to detect vulnerabilities and suggest remedial actions

Highlights

- Lowers total cost of ownership, improves security and supports compliance requirements through a set of core capabilities
 - Provides key capabilities to help organizations streamline data security management without changes to databases, networks or applications
 - Generates security health report card and recommends concrete action plans to strengthen database security
-

IBM® InfoSphere® Guardium® Vulnerability Assessment helps harden database infrastructures by scanning targeted systems on a scheduled basis to detect vulnerabilities. Data infrastructures are highly dynamic, with changes in accounts, configurations and patches occurring regularly. Most organizations lack the centralized control or skilled resources to review changes systematically to determine if they have introduced security gaps. Database vulnerability assessment is essential, as it identifies threats and security holes in databases or the underlying operating system which could be exploited by intruders and hackers to gain access to sensitive data.

InfoSphere Guardium Vulnerability Assessment evaluates the database and operating system configurations and recommends concrete actions to strengthen security and eliminate the enormous risk created by insecure database configurations, missing databases patches, weak passwords and other vulnerabilities. InfoSphere Guardium Database Vulnerability Assessment produces summary results that can provide an understanding of your overall security posture and history, along with detailed drill-downs containing concrete recommendations for improvement.

InfoSphere Guardium Vulnerability Assessment lowers total cost of ownership, improves security and supports compliance requirements through a set of core capabilities. These capabilities are available in three simple offerings: *Vulnerability Assessment Standard Edition*, *Vulnerability Assessment Advanced Edition*, and *Central Management and Aggregation*. Figure 1 explains the core capabilities and the value they provide. All core capabilities are included in Standard Edition, except for those marked with an “***”, which are available in the Advanced Edition. Central Management can be purchased separately, and the capabilities included in Central Management are marked with a “c.”



Streamlined Management	TCO	Security	Compliance
Automatic update of reports and policies to adapt to IT changes and security events	x	x	
°Single console to manage, use and update InfoSphere Guardium	x		
Database discovery and data classification	x	x	x
Advanced user/role management (separation of duties)	x		x
Built-in compliance workflow (review, escalations, sign-offs)	x		x
Adaptive scheduling	x		
Performance			
Quick response time on VA tests	x		
No impact on production database performance	x		
Scalable 64-bit appliance platform	x		
Integration			
Integration with IT operations	x	x	x
Integration with security systems and standards (QRadar, HP Arcsight, Radius, LDAP etc.)	x	x	
Integration with security systems and standards (QRadar, zSecure etc.)	x	x	
Scalability			
Support for batch operations (GuardAPI)	x		
°Aggregation — merge audit reports from multiple sources to produce enterprise-wide reports	x		x
Risk Reduction			
Custom report builder with drill-down capabilities	x		x
Best practice recommendations — predefined reports and alerts	x		x
Vulnerability assessment		x	x
Database protection knowledgebase subscription		x	
Best practice recommendations for vulnerability remediation	x	x	
**Configuration audit system (CAS)	x		
**Entitlement reports	x	x	x
Custom report builder with quick search and drill down capabilities	x		x

°Also available in InfoSphere Guardium Central Management and Aggregation

**Available in InfoSphere Guardium Vulnerability Assessment Advanced Edition Only

Figure 1: InfoSphere Guardium Vulnerability Assessment lowers total cost of ownership, improves security and supports compliance requirements through a set of core capabilities available in three simple offerings: Vulnerability Assessment Standard Edition, Vulnerability Assessment Advanced Edition and Central Manager.

Streamlined management

No organization has the time or resources to spend time on low-level security operations or manual processes. Not only do manual approaches slow down the business, they are also risky and error-prone. As your business grows and the scope of your security projects increases, you need security solutions to become more streamlined, reliable, and repeatable. In the era of big data, where data is growing in volume, variety and velocity, security strategies should be more optimized and transparent, not more complex or obscure. InfoSphere Guardium Vulnerability Assessment provides key capabilities to help organizations streamline data security management without changes to databases, networks or applications.

- **Automatic update of reports and policies to adapt to IT changes and security events**—Maximizes the protection afforded by InfoSphere Guardium. With one click, groups, policies, tests and other configurable parameters can be updated to adapt to the constantly evolving nature of the organization, database infrastructure and associated threats.
- **A single console to manage, use and update InfoSphere Guardium**—Provides centralized management via a single web-based console. The scalable multitier architecture supports large and small environments with built-in health-check dashboards.
- **Database discovery and data classification**—Discover and classify sensitive data. The discovery process can be configured to probe specified network segments on a scheduled or on-demand. Once instances of interest are identified, the content is examined to identify and classify sensitive data.
- **Advanced user/role management (separation of duties)**—Keeps security and data administration separate. All operations completed by InfoSphere Guardium Vulnerability Assessment, including administration and configuration, are audited to maintain compliance controls. Security professionals can run reports without support for IT staff. InfoSphere Guardium organizes access for administrators through RBAC controls, including hierarchy.
- **Built-in compliance workflow (review, escalations, sign-offs)**—Supports SOX, PCI, HIPAA and more with predefined reports for top regulations. An easy-to-use graphical user interface allows a wide variety of processes to be created to match the unique needs of the tasks and individuals involved. Numerous audit tasks are supported, including reviewing the results of automatically generated vulnerability assessments, asset discovery, and data classification. InfoSphere Guardium also exports reports to different formats, including: PDF, CSV, CEF, Syslog forwarding, SCAP, or custom schemas.
- **Adaptive Scheduling and multidatabase report consolidation**—Centralize and automate oversight processes enterprise-wide, including report generation, distribution, electronic sign-offs and escalations. Create custom processes by specifying your unique combination of workflow steps, actions and user and enable automated execution of oversight processes on a report line-item basis, maximizing process efficiency without sacrificing security. Ensure that oversight team members see only data and tasks related to their own roles and store process results in a secure centralized repository.

Performance

Business moves fast, and clients demand 24x7 access to data. As a result, IT environments, including databases, transactional applications, analytics platforms and emerging big data applications, are required to meet aggressive service-level agreements for availability, performance and responsiveness. Compliance requirements need to be addressed and security strategies implemented without impacting performance. InfoSphere Guardium Vulnerability Assessment can be implemented with negligible performance impact.

- VA test completes within minutes!
- No impact on production database performance
- A scalable 64-bit appliance platform—Leverage an appliance platform that can grow with your implementation and delivers the throughput to handle traffic analysis for thousands of data sources.

Integration

Most organizations have some security solutions in place today. This could include a Security Information and Event Management (SIEM) solution or application-level access controls. However, most existing security solutions don't provide deep insight into database infrastructure vulnerabilities. InfoSphere Guardium Vulnerability Assessment provides this insight, while seamlessly integrating into existing security solutions such as IBM Security QRadar or HP ArcSight. In addition, InfoSphere Guardium Vulnerability Assessment provides a "snap it" integration model with existing IT systems, such as data management, ticketing and archiving solutions. The goal is to shield you from the integration burden, enabling you to quickly extend your security posture.

- **Integration with IT operations**—Exploit existing data management environments. Built-in, ready-to-use support for Oracle, DB2, Sybase, Microsoft SQL Server, Informix, MySQL, Teradata, pureSystems and PostgreSQL databases across all major protocols including: HTTP, HTTPS, FTP, SAMBA and iSeries connections to CSV text file data sources.
- **Integration with security systems and standards** (QRadar, HP Arcsight, Radius, LDAP, SCAP, and more)—Adapt to changes automatically. Users, groups, roles and authentication to databases and applications can be updated automatically and directly from directories like LDAP, Radius, and Active Directory. You can automatically handle any staff or user change while keeping the policies and reports intact, avoiding the need to constantly modify them. Groups are used to facilitate the upkeep of the policies despite the constant change in the IT environment. It also allows for the generation of white lists or black lists. In addition, send all audit information to a SIEM such as IBM Security QRadar. Integration with zSecure Audit gives Guardium the ability to identify the effective entitlement for sensitive data on DB2 for z/OS.

Scalability

Managing database security and compliance has become increasingly challenging. Not only has the rate of cyber attacks continued to grow, but the complexity of the environments has increased dramatically. Driven by a rapidly changing business landscape that includes mergers, outsourcing, workforce adjustments and accelerating business automation, databases continue to proliferate over geographical and organizational

boundaries. Given the current resource-constrained environment, the complexity of environments being managed, and escalating workloads, organizations are now seeking means to increase automation in their database security and compliance operations. InfoSphere Guardium Vulnerability Assessment is equipped to scale from one database to tens of thousands without disrupting operations.

- **Support for batch operations (GuardAPI)**—Facilitates integration of any IT process with InfoSphere Guardium Data Activity Monitor. GuardAPI is a script-based CLI interface to InfoSphere Guardium, allowing any operation to be done remotely.
- **Aggregation**—Merges audit reports from multiple sources to produce enterprise-wide reports across heterogeneous platforms.

Risk reduction

Risk is the potential that a chosen action or activity, including the choice of inaction, will lead to sensitive data exposure. A probability or threat of damage, liability, data loss, or any other negative occurrence that is caused by external or internal vulnerability must be avoided through preemptive action. InfoSphere Guardium Vulnerability Assessment reduces risk by uncovering and remediating database infrastructure vulnerabilities. To support compliance, InfoSphere Guardium Vulnerability Assessment also provides vulnerability reporting and alerts.

- **Custom report builder with quick search and drill-down capabilities**—Generate security health report card, and dashboard like reports with VA Assessment Statistics Reports: Summary counts (#tests, #passed) for each of the major test categories: Center for Internet Security (CIS), Database Security Technical Implementation Guide (STIG) and Common Vulnerability Event (CVE). Quickly find the tests you are interested in without sifting through innumerable reports.
- **Best practice recommendations (predefined reports and alerts)**—Recommends concrete action plans to strengthen database security and receive alerts in real time when vulnerabilities are introduced. You can also define custom tests and schedule automated audit tasks incorporating scans, distribution of reports, electronic sign-offs, and escalations.

- **Vulnerability assessment** — Scans database infrastructure for vulnerabilities to identify security risks such as missing patches, weak passwords, misconfigured privileges, and default vendor accounts. The solution allows you to simplify deployment in large-scale environments, as multiple data sources (DB name, type, server IP, ports and roles) can be loaded and linked to assessments automatically. Assessments are grouped into multiple categories, such as privileges, authentication, version, behavior, file permissions, and configuration. This provides an ongoing evaluation of your security posture, using both real-time and historical data.
- **Database protection knowledgebase subscription** — Leverages automatic database vulnerability remediation updates with the latest vulnerability standards. Content provided includes: software patch levels, version levels, vulnerable objects, sensitive objects (tables with SOX, PII or PCI data), stored procedures, administrative programs, commands and more. A wide variety of sources are used to identify this information, including internal IBM research, relationships with other vendors and cross-industry cooperative efforts like CVE. This feature proactively updates InfoSphere Guardium with the latest information on vulnerabilities, best practices policies, and sensitive tables in common enterprise applications (SAP, Oracle EBS, PeopleSoft, and more) to eliminate hours of up-front and on-going labor to identify new vulnerabilities.
- **Configuration audit system (CAS)** — Assesses operating system and database configuration vulnerability, and alerts on configuration changes. This feature tracks all changes that can affect the security of database environments outside the scope of the database engine, such as database configuration files (SQLNET.ORA, NAMES.ORA), environment and registry variables, shell scripts, operating system files and executable files. Staying abreast of changes in the variety of database systems is challenging; each has their own unique architecture, documentation and release schedules. InfoSphere Guardium Vulnerability Assessment tracks everything automatically.
- **Best practice recommendations for vulnerability remediation** — Hardens databases based on hundreds of comprehensive, preconfigured tests. Built-in best practices such as those developed by the Center for Internet Security (CIS) and the Database Security Technical Implementation Guide (STIG) are included, as is support for SCAP.

About IBM InfoSphere Guardium

InfoSphere Guardium is part of the IBM InfoSphere integrated platform and the IBM Security Systems Framework. The InfoSphere integrated platform defines, integrates, protects and manages trusted information in your systems. The InfoSphere integrated platform provides all the foundational building blocks of trusted information, including data integration, data warehousing, master data management, and information governance, all integrated with a core of shared metadata and models. The portfolio is modular, so you can start anywhere and mix and match InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The InfoSphere platform is an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster.

For more information

To learn more about IBM Guardium, visit ibm.com/guardium.



© Copyright IBM Corporation 2013

IBM Corporation
Software Group (or appropriate division)
Route 100
Somers, NY 10589

Produced in the United States of America
October 2013

IBM, the IBM logo, ibm.com, BigInsight, DB2, Guardium, InfoSphere, iSeries, and PureSystems are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.



Please Recycle