IBM Security Guardium Vulnerability Assessment

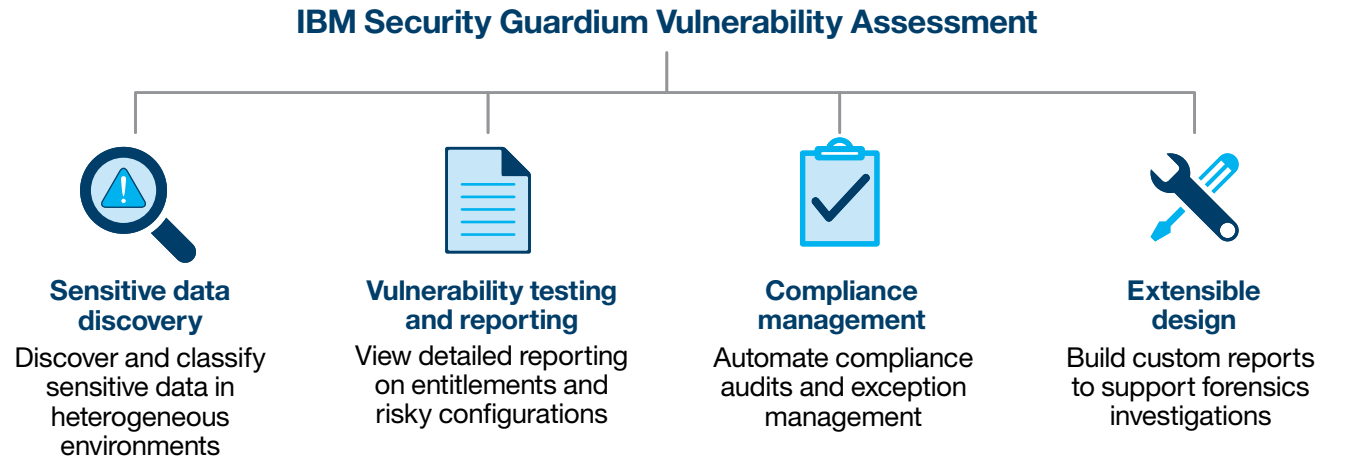
Scan data environments to detect vulnerabilities and suggest remedial actions

Highlights

- Provide a scalable platform to help protect and secure customer data repositories and manage compliance with the latest security regulations
- Enforce security best practices with specific tests and customization options for each data source type
- Leverage dynamic reports for recommendations on how to fix each data source vulnerability to help remediate data threats and simplify security operations

IBM® Security Guardium® Vulnerability Assessment helps harden data 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.

Guardium Vulnerability Assessment is essential as it identifies threats and security holes in databases, data warehouses and big-data environments that could be exploited by intruders and hackers to gain access to sensitive data. Guardium Vulnerability Assessment recommends concrete actions to strengthen security and eliminate the enormous risk created by insecure data repository configurations, missing patches, weak passwords and other vulnerabilities. Guardium Vulnerability Assessment produces summary results that can provide an understanding of your overall security posture, along with detailed drill-down reports containing concrete recommendations for improvement. Guardium Vulnerability Assessment provides a single offering supporting multiple data platforms for high scalability, lowers total cost of ownership, improves security and supports compliance requirements through a set of core capabilities. These capabilities are available in a single offering.



IBM Security Guardium Vulnerability Assessment includes core capabilities to help you analyze risk, automate compliance and harden your data environment.

Streamlined management

Organizations do not have the time and resources to manage vulnerabilities at the data layer. Manual processes to check vulnerabilities become tedious and time consuming for security operations and are risky and error-prone. As your business grows and the scope of security projects increases, you need security solutions to become more streamlined. In the era of big data where data is growing in volume, variety and velocity, security strategies should be optimized and transparent, not more complex or obscure. Guardium Vulnerability Assessment provides key capabilities to help organizations streamline data security management without requiring changes to data sources, networks or applications. The management capabilities include:

- **Automatic updates of reports and policies to adapt to IT changes and security events:** Maximize protection across heterogeneous environments. With one click, groups, policies, tests and other configurable parameters can be updated to adapt to the constantly evolving nature of the data infrastructure and associated threats.
- **Single management console:** Provide centralized management through a single web-based console to create assessment for multiple data sources. Assessments can be modified, added and deleted through a single web console.

- **Database discovery and data classification:** Discover data assets and classify sensitive data. The discovery process can be configured to probe specified network segments on a schedule or on demand. Once instances of interest are identified, the content is examined to identify and classify sensitive data.
- **Advanced user/role management (segregation of duties):** Keep security and data administration separate. All operations performed by Guardium Vulnerability Assessment, including administration and configuration, are audited to maintain compliance controls. Security professionals can run reports without support from IT staff. Access for administrators can be enforced through role-based access controls, including hierarchical controls.
- **Built-in compliance workflow (reviews, escalations and sign-offs):** Support Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA) compliance mandates. 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. Export reports to different formats including PDF, comma-separated values (CSV), common event format (CEF), Syslog forwarding, Security Content Automation Protocol (SCAP), Apache eXtensible Interaction System (AXIS) or custom schemas for better integration to security information and event management (SIEM) solutions or for business intelligence reporting.
- **Adaptive scheduling and multi-database report consolidation:** Throughout the vulnerability testing process, each resource will require a different approach depending on its status. With adaptive scheduling, specific failed tests can be held from running unnecessarily until the vulnerability has been remediated. Data sources can also be grouped for reporting purposes.

Performance

Business moves quickly 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. Guardium Vulnerability Assessment can be implemented with minimal performance impact using key capabilities such as:

- **Fast assessments**—Perform vulnerability assessment tests within minutes.
- **Filtering of database traffic**—Avoid unnecessary database audit traffic for minimal impact on production database performance
- **Support for 64-bit architecture**—Leverage a scalable 64-bit appliance platform that can grow with your implementation and deliver the throughput to handle traffic analysis for thousands of data sources.

Integration

Most organizations have some security solutions in place today, such as a SIEM solution or application-level access controls. However, most existing security solutions don't provide deep insight into data-source infrastructure vulnerabilities. Guardium Vulnerability Assessment provides this insight while seamlessly integrating into existing security solutions, such as IBM Security QRadar® or HP ArcSight. In addition, Guardium Vulnerability Assessment provides a "snap in" integration model with existing IT systems, such as data management, ticketing and archiving solutions. The goal is to complement existing IT solutions and extend your security posture with support for:

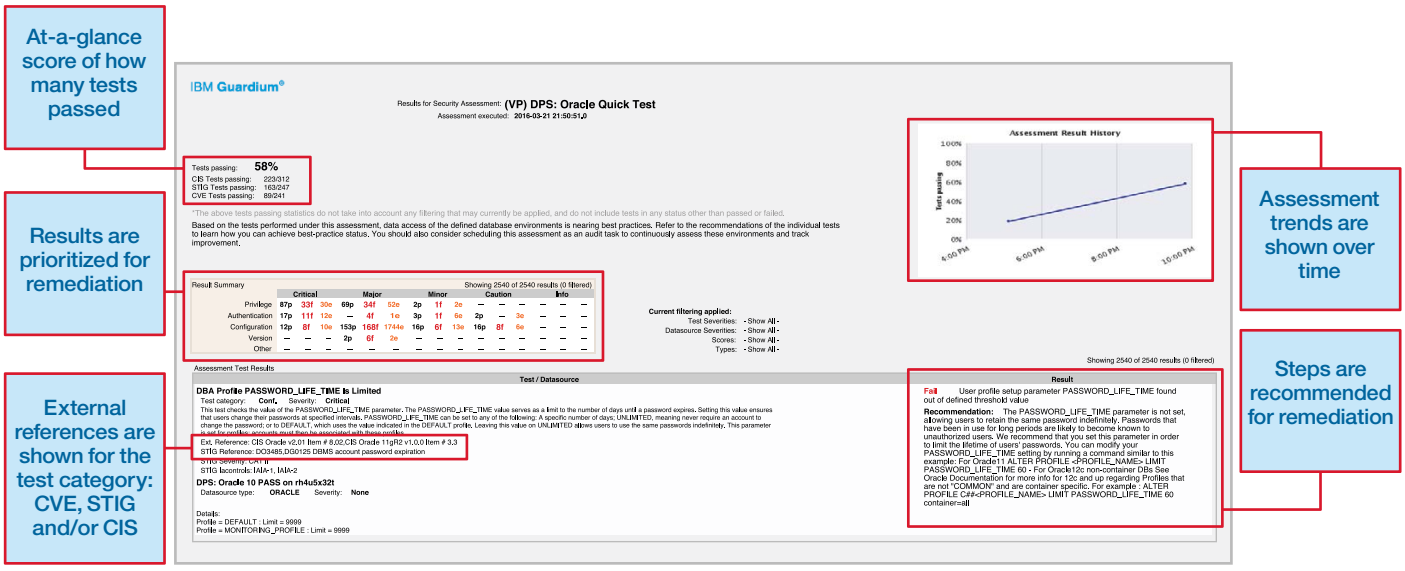
- **Integration with IT operations:** Exploit existing data management environments with built-in, ready-to-use support for Oracle, IBM DB2®, IBM DB2 on z/OS®, IBM DB2 on iSeries®, Sybase, Microsoft SQL Server, IBM Informix®, mySQL, Teradata, Aster DB, IBM PureSystems® and PostgreSQL, SAP HANA, and MongoDB.
- **Integration with security systems and standards:** Adapt to changes automatically. Users, groups, roles and authentication to databases and applications can be updated automatically and directly from sources such as Lightweight Directory Access Protocol (LDAP), Radius and Microsoft 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. This also allows the generation of whitelists or blacklists. In addition, you can send all audit information to a SIEM such as QRadar. Integration with IBM Security zSecure™ Audit gives Guardium the ability to identify the effective entitlement for sensitive data on DB2 for z/OS.

Scalability

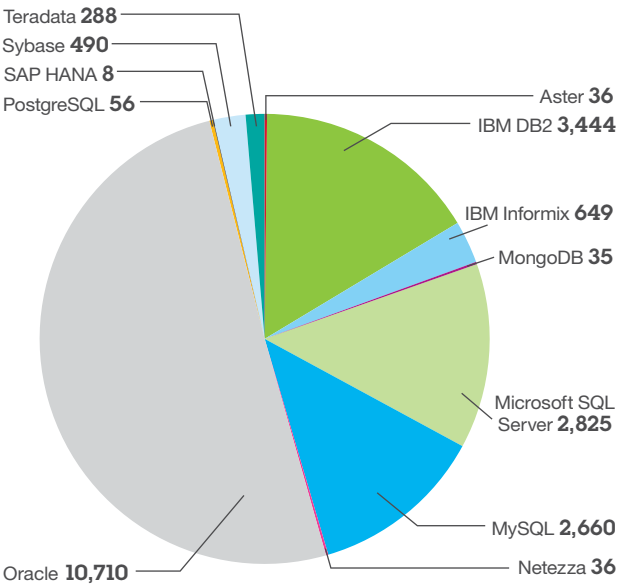
Managing security and compliance has become increasingly challenging for data environments. Not only has the rate of cyber attacks continued to grow, but the complexity of the environments has increased dramatically. Driven by a rapidly changing business landscape that includes mergers, outsourcing, workforce adjustments and accelerating business automation, data repositories continue to proliferate over geographical and organizational boundaries. Given the current resource-constrained environment, the complexity of environments being managed and escalating workloads, organizations want to increase automation in their database security and compliance operations. Guardium Vulnerability Assessment is equipped to scale from one data source to tens of thousands without disrupting operations—across multiple data centers and multiple geographical locations. Automation capabilities include:

- **Support for batch operations (via GuardAPI):** Facilitate integration of any IT process with Guardium Vulnerability Assessment. GuardAPI is a script-based command-line interface (CLI) to Guardium that allows any operation to be performed remotely.
- **Aggregation:** Merge vulnerability assessment reports from multiple sources to produce enterprise-wide reports across heterogeneous platforms.

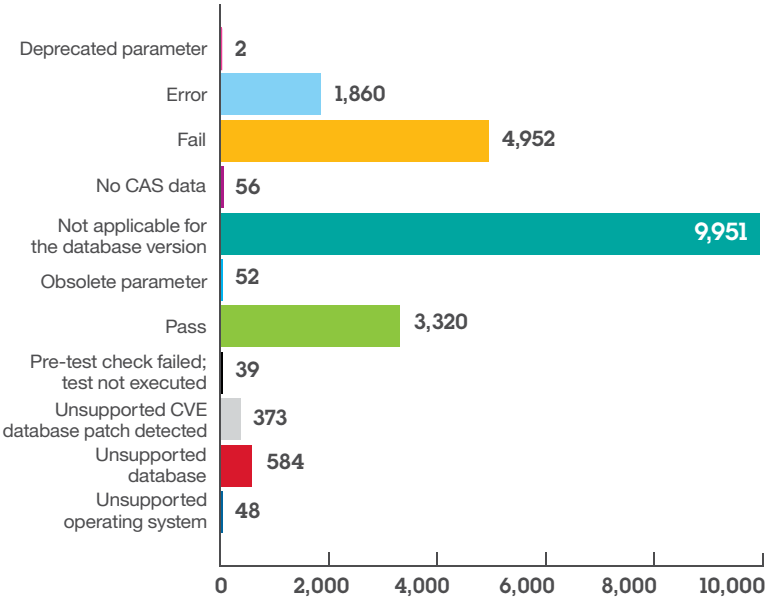
IBM Security Guardium Vulnerability Assessment testing in a client environment



Number of assessments by platform*



Summary of assessment scan results*



* The charts show the number of assessments by platform and summary of assessment scan results in the client environment for a given time period.

Guardium Vulnerability Assessment provides detailed reporting of scan results, including recommended steps for remediation. The assessments run on a wide range of platforms, identifying configuration errors, unsupported database patches and more.

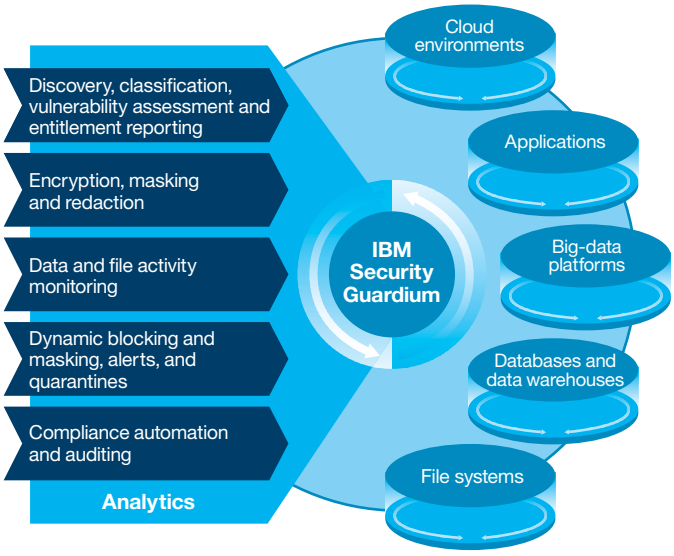
Risk reduction

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. Guardium Vulnerability Assessment reduces risk by uncovering and remediating data source vulnerabilities. To support compliance, Guardium Vulnerability Assessment also provides vulnerability reporting and alerts. Some key risk reduction features include:

- **Custom report builder and drill-down capabilities:** Generate a security health report card and dashboard-like reports with Guardium Vulnerability Assessment Statistics Reports. Monitor summary counts (total number of tests run and number that passed or failed) 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):** Recommend concrete action plans to strengthen data asset 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:** Scan data infrastructure for vulnerabilities to identify security risks, such as missing patches, weak passwords, incorrectly configured privileges and default vendor accounts. Simplify deployment in large-scale environments, as multiple data sources (database 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. Provide an ongoing evaluation of your security posture, using both real-time and historical data.
- **Database protection knowledgebase subscription:** Leverage automatic data vulnerability remediation updates with the latest vulnerability standards. Content provided includes software patch levels, version levels, vulnerable objects, sensitive objects (tables with SOX, personally identifiable information or PCI DSS 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 such as CVE. Proactively update Guardium Vulnerability Assessment with the latest information on vulnerabilities, best-practices policies and sensitive tables in common enterprise applications (SAP, Oracle E-Business Suite, PeopleSoft and so on) to eliminate hours of up-front and ongoing labor to identify new vulnerabilities.
- **Configuration audit system (CAS):** Assess operating system and data repository configuration vulnerabilities and create alerts on configuration changes. Track all changes that can affect the security of data 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 its own unique architecture, documentation and release schedules. Guardium Vulnerability Assessment tracks everything automatically.
- **Best-practice recommendations for vulnerability remediation:** Harden databases based on hundreds of comprehensive, preconfigured tests. Built-in best practices such as those developed by CIS and the STIG are included as well as support for SCAP.

Why Guardium?

Guardium is part of IBM Security Systems Framework and IBM Data Security Privacy Platform. Data Security and Privacy Platform provides end-to-end data protection capabilities to discover and analyze, protect, integrate and manage the critical data in your environment. Guardium provides all the building blocks you need for data protection—from meeting compliance requirements all the way through to broader data protection. The portfolio is modular, so you can start anywhere and mix and match security software building blocks with components from other vendors or choose to deploy multiple building blocks together for increased acceleration and value. The security 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.



IBM Security Guardium is a comprehensive data security platform that helps security teams secure and manage all types of sensitive data consistently, whether it is in big-data platforms, databases or file systems.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

For more information

To learn more about IBM Security Guardium Vulnerability Assessment, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/guardium

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2016

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

WGD03074-USEN-01