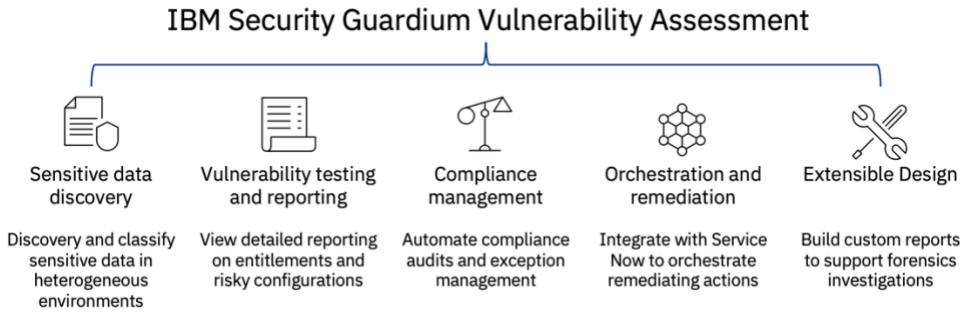
IBM Security Guardium Vulnerability Assessment

Scan data environments to detect vulnerabilities and orchestrate remediation

IBM® Security Guardium® Vulnerability Assessment helps harden data infrastructures and platforms by scanning targeted systems on a scheduled basis to detect vulnerabilities. Data infrastructures are highly dynamic. With changes in user privileges, roles or configurations and new versions or patches releasing regularly, many organizations lack the centralized control or skilled resources to review changes systematically to determine if they have introduced security gaps.

Guardium Vulnerability Assessment identifies threats and security holes in databases, data warehouses and big-data environments hosted on-premises or in hybrid multicloud that could be exploited by malicious actors to access sensitive data. The solution recommends concrete actions to strengthen security and eliminate the enormous risk created by insecure data repository configurations, missing patches, weak passwords and other common vulnerability exposures (CVE's). Its summary results can provide an understanding of your overall security posture. Guardium Vulnerability Assessment provides a single offering supporting multiple data platforms for high scalability, lowers total cost of ownership, improves security and helps address compliance requirements through a set of core capabilities.



Highlights

- Scalable platform helps protect and secure customer data stores and manage compliance with security regulations
- Enforce security best practices with specific tests and customization options for each data source type
- Dynamic reports for recommendations to help remediate data threats and vulnerabilities, simplifying security operations

Streamlined management

Guardium Vulnerability Assessment helps organizations streamline data security without requiring changes to data sources, networks or applications, with management capabilities that include:

- **Automatic updates of reports and policies to adapt to IT changes and security events:** Groups, configurations, tests and other configurable parameters can be updated easily with one click or through API's.
- **Database discovery and data classification:** Discovery can be configured to probe specified network segments on a schedule or on demand. Once instances of interest are identified, the solution identifies and classifies sensitive data. Integrate current inventory maintained in configuration management databases and reconcile assets for complete coverage.
- **Advanced user/role management:** Segregation of duties between allows security professionals to run reports without support from IT staff. Access for administrators can be enforced through role-based access controls, including hierarchical controls. All operations performed by the solution are audited to help maintain controls mandated by regulations. Users can integrate with various password management tools like CyberArk with pre-built integrations to create users with read privileges limited to scanning.
- **Built-in compliance workflow:** Supports regulations such as Sarbanes-Oxley, Payment Card Industry and the Health Insurance Portability and Accountability Act. Integration with other vulnerability management tools can be done through API's and/or a CSV upload for further correlations of vulnerabilities and risk.

Risk reduction

Guardium Vulnerability Assessment reduces risk by uncovering and remediating data source vulnerabilities. To help support compliance, the solution also provides vulnerability reporting and alerts.

- **Custom dashboard reports and drill-down capabilities:** Monitor summary counts for each major test category: Center for Internet Security (CIS), Database Security Technical Implementation Guide (STIG) and Common Vulnerability Event (CVE).
- **Vulnerability assessment:** Scan data infrastructure for vulnerabilities to identify security risks, such as missing patches,

weak passwords, incorrectly configured privileges and default vendor accounts.

- **Database protection knowledgebase subscription:** Leverage automatic updates from IBM Vulnerability Assessment development and research team about the latest vulnerabilities for supported platforms. Receive Rapid Response DPS for any vulnerability exposed in public domain with a CVSS score of 7 or higher. Plan scanning to understand Zero-day threat exposures and plan remediation.
- **Configuration audit system:** Assess operating system and data repository configuration vulnerabilities and create alerts on configuration changes. Track all changes automatically that can affect the security of data environments outside the scope of the database engine
- **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.

Performance

Guardium Vulnerability Assessment can be implemented with minimal or zero performance impact through key capabilities. Users can perform vulnerability assessments within minutes, with minimal read-only access privileges, without affecting database performance.

Integration

Guardium Vulnerability Assessment provides deep insight into data source infrastructure vulnerabilities while seamlessly integrating into existing security solutions, such as IBM Security QRadar®, HP ArcSight or Splunk. It also provides a "snap-in" integration model with existing IT systems—such as data management, ticketing and archiving solutions—in order to complement existing IT solutions. Capabilities supporting integration include:

- **Integration with IT operations:** 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, MongoDB, Cassandra, Cloudera and others.
- **Support cloud and containerized databases:** Built-in, ready-to-use support for AWS RDS and Azure SQL databases, the solution can also connect to containerized databases.
- **Integration with Service Now:** Helps operationalize and orchestrate vulnerability assessment remediation. Out-of-the-box integration allows users to send failed vulnerability scan results from the solution to ServiceNow.
- **Integration with security systems and standards:** 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.
    - Out-of-the-box integration available with CyberArk for managing data source credentials in Guardium Vulnerability Assessment
    - Generate whitelists or blacklists. Audit information can be sent 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

Guardium Vulnerability Assessment is equipped to scale from one data source to tens of thousands without disrupting operations across multiple data centers and multiple or geographical locations. Support for batch operations via GuardAPI, its script-based command line interface, GuardAPI facilitates integration with any IT process. GuardAPI is a script-based command-line interface to Guardium that and allows any operation to be performed remotely. Users can also merge vulnerability assessment reports from multiple sources to produce enterprise-wide reports across heterogeneous platforms, on-premises and on hybrid multicloud.

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, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

Discover how IBM Security Guardium solutions can help you take a smarter, integrated approach to safeguarding critical data across your hybrid, multicloud environments. Visit ibm.com/Guardium