IBM Security Guardium Vulnerability Assessment

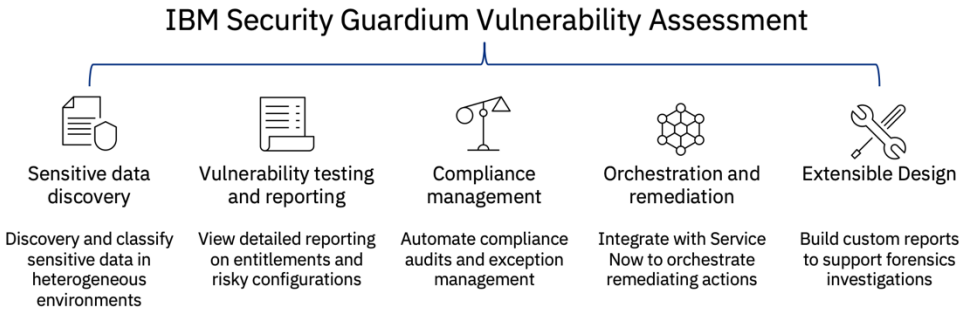
Improve your data security posture management by scanning data sources, detecting vulnerabilities, and orchestrating remediation

IBM® Security Guardium® Vulnerability Assessment helps clients get an understanding of their data security posture and improve and manage that posture by hardening data infrastructures and platforms. Vulnerability Assessment scans by scanning targeted systems on a scheduled basis to detect vulnerabilities and issues. Ongoing scanning is important because 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 visibility and control or skilled resources to review changes systematically to determine if they have introduced security gaps.

Guardium Vulnerability Assessment identifies weaknesses that could be exploited by malicious actors to access sensitive data. This capability works across all types of databases, data warehouses and big-data environments, whether on-premises or in the cloud. The solution recommends concrete actions—down to command line instructions—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): This helps you better understand and then improve your data security posture. Its summary results can provide an understanding of your overall security posture.

Highlights

- Better understand and manage data security posture
- 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
- Simplify operations with dynamic reports and precise recommendations for remediating data - centric threats and



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: Easily update groups, configurations, tests and other configurable parameters with one click or through APIs.
- Database discovery and data classification: Configure database discovery to probe specific network segments on a schedule or whenever it's needed. Establish areas of interest, then use the solution to identify and classify sensitive data. Integrate current inventory from the configuration management databases and reconcile assets for complete coverage.
- Advanced user/role management: Run reports without support from IT staff or elevated privileges via segregation of duties. Enforce administrative action through role-based access controls, including hierarchical controls. All operations performed by the solution are audited to help maintain controls mandated by regulations. Administrators can integrate with various password management tools like AWS Secrets Manager, CyberArk, and HashiCorp Vault with pre-built integrations to create users with read privileges limited to scanning.
- Built-in compliance workflow: Integrate the solution with other vulnerability management tools through APIs and/or a CSV

upload for further correlations of vulnerabilities and risk. Use this to support regulations such as Sarbanes-Oxley, Payment Card Industry (PCI) and the Health Insurance Portability and Accountability Act (HIPAA).

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. Capabilities include:

- 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 the IBM Vulnerability Assessment development and research team about the latest vulnerabilities for supported platforms. Receive Rapid Response Data Protection Service (DPS) for any vulnerability exposed in public domain with a Common Vulnerability Scoring System (CVSS) score of 7 or higher. Plan scanning to understand zero-day threat exposures and plan remediation.
- Configuration audit system: Assess vulnerabilities in your operating system and data repository configurations, then create alerts on configuration changes. Automatically track all changes 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. The solution includes built-in best

practices such as those developed by CIS and the STIG as well as support for SCAP.

Performance

Guardium Vulnerability Assessment can be implemented with zero to minimal performance impact. 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 Snowflake, 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 security systems and standards: Automatically update users, groups, roles and authentication to databases and applications. This can be done directly from sources such as Lightweight Directory Access Protocol (LDAP), Radius and Microsoft Active Directory.

- Integration with ServiceNow: • A certified ServiceNow application is available for clients that prefer having that teams leverage ServiceNow as their response control center. The Guardium Vulnerability Assessment plug-in is available on the ServiceNow site and can ‘pull’ data from Guardium Vulnerability Assessment via RestAPI. The app helps synchronize Guardium Vulnerability Assessment database type, database group, and test-result entries for tighter integration with ServiceNow CMDB. The app will show all Guardium Vulnerability Assessment results within ServiceNow, and users can start scanning jobs and tests right from the ServiceNow user interface. Additionally, the app can be used to centrally manage all tools and can automatically assign tickets via ServiceNow. For clients that do not want to use ServiceNow as the front end, Guardium Vulnerablity Assessment also provides more traditional integration with ServiceNow, helping operationalize and orchestrate vulnerability assessment remediation. This out-of-the-box integration allows users to send failed vulnerability scan results from the solution to ServiceNow.

Scalability

Guardium Vulnerability Assessment can scale from one data source to tens of thousands, across multiple data centers and multiple geographical locations, without disrupting operations. Support for batch operations via GuardAPI facilitates integration with any IT process. GuardAPI is a script-based command-line interface to Guardium that 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-prem 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