IBM Security Guardium Vulnerability Assessment

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

Highlights
Reduce risk by uncovering and remediating data source vulnerabilities

Simplify compliance and policy management with pre-built workflows

Scale data security without requiring changes to data sources

Integrate seamlessly with existing technologies

Data infrastructures are highly dynamic. User privileges, roles and configurations are constantly changing and new versions or patches release regularly. To maintain security requirements, businesses need to clearly see what data is being accessed when, where, how and why. But many organizations lack either the high-value resources or the centralized visibility and control to review such changes both systematically and continuously while checking for security gaps.

IBM Security® Guardium® Vulnerability Assessment helps you understand, improve and manage your security posture by reinforcing data infrastructures and platforms. It does so by scanning targeted systems on a scheduled basis and detecting vulnerabilities or issues—a capability that works across databases, data warehouses and big-data environments whether on-premises or in the cloud.

IBM Security Guardium uses the summarized results from these scans to recommend direct action, down to command line instructions, aimed at strengthening security. This helps mitigate the risk posed by unsecured data repository configurations, missing patches, weak passwords and other common vulnerability exposures (CVEs).

Reduce risk by uncovering and remediating data source vulnerabilities
IBM Security Guardium offers many capabilities aimed at mitigating risk from CVEs:

- Data infrastructure vulnerability scans proactively identify potential security risks.
- 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 Security Content Automation Protocol (SCAP).
- Database protection knowledge base subscription allows you to access automated updates from the IBM Vulnerability Assessment development and research team about the latest CVEs, zero-day threat exposures and remediation plans.
- Database discovery and data classification empower you to probe specific network segments on a schedule or as-needed basis, integrate current inventory from configuration management databases and reconcile assets for complete coverage.
- Custom audit system configuration allows you to assess CVEs in your operating system and data configurations, create alerts based on those configurations and automatically track all changes that can affect the security of data environments outside the scope of the database engine.

Simplify compliance and policy management with pre-built workflows
To help support compliance, IBM Security Guardium Vulnerability Assessment provides built-in compliance workflows complete with vulnerability reports. It also integrates with other vulnerability management tools through API connections and/or CSV uploads to provide deeper visibility into vulnerabilities and risk. This capability helps you achieve compliance with regulations like Sarbanes-Oxley, Payment Card Industry (PCI) and the Health Insurance Portability and Accountability Act (HIPAA).

Advanced user and role management allows you to run reports without oversight by IT staff and without escalating to higher-privileged users through siloed processes. Administrators can integrate with various password management tools like AWS Secrets Manager, CyberArk and HashiCorp with pre-built integrations to create users with read privileges limited to scanning.

Scale data security without requiring changes to data sources

IBM Security Guardium Vulnerability Assessment can scale efficiently from one data source to tens of thousands—including networks and applications—without disrupting operations. Support for batch operations through GuardAPI facilitates integration with any IT process, further enhancing the scalability of the platform. Users can also merge vulnerability assessment reports from multiple sources to produce enterprise-wide reports across heterogeneous platforms both on-premises and on hybrid multicloud.

You can implement this solution in most use cases with little to no impact on overall performance. Users can even perform vulnerability assessments that take only minutes to complete, using minimal read-only access permissions, without affecting database performance whatsoever.

Integrate seamlessly with existing technologies

IBM Security Guardium Vulnerability Assessment provides deep insight into data source infrastructure vulnerabilities while seamlessly integrating into existing security solutions like IBM Security Qradar and HP ArcSight. The solution also provides a "snap-in" model to facilitate integration with existing IT systems—simply "snap it into place." This is ideal for data management, ticketing and archiving systems.

IBM Security Guardium Vulnerability Assessment also supports integration with ServiceNow. One plug-in is capable of pulling data from the solution via RestAPI, which synchronizes the solution's database type, database group and test result entries for tighter integration with ServiceNow Configuration Management Database (CMDB).

The app will show all IBM Security Guardium Vulnerability Assessment results within ServiceNow, enabling users to start scans and tests directly within the ServiceNow user interface. Alternatively, you can keep using the primary IBM Security Guardium Vulnerability Assessment user interface and simply send failed vulnerability scan results to ServiceNow without having to rely on the ServiceNow interface.

Conclusion

IBM Security Guardium Vulnerability Assessment helps to reduce risk, identify threats and security gaps, and accelerate remediation across your organization. It automatically scans your data infrastructure to detect vulnerabilities and provide insight-backed recommendations. Through pre-built templates, automated alerts, custom reports and user access management, this solution simplifies security processes and streamlines compliance.

Why IBM?

IBM Security offers one of the most advanced and well-integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help you drive security into the fabric of your business, empowering you to thrive in the face of uncertainty.

IBM® operates one of the broadest and deepest security research, development and delivery organizations in the world. IBM uses insights gained from these activities to monitor more than one trillion events per month in more than 130 countries and holds over 3,000 security patents.

For more information

To learn more about IBM Security Guardium Vulnerability Assessment, contact your IBM representative or IBM Business Partner or visit ibm.com/products/ibm-guardium-vulnerability-assessment.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
September 2023

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 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 NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.