IBM Security Guardium Data Protection for Files

Highlights

- *Discover and classify unstructured and sensitive data in files*
- *Continuously monitor and audit all file activity*
- *Block user access by enforcing security policies in real time for all file access, including privileged users*
- *View detailed reporting on all file activity from a single, centralized management console*
- *Support forensics investigations and threshold alerts on file activity*
- *Protect data in heterogeneous environments, including files and file shares*

Every day, organizations must manage a deluge of unstructured content—documents, spreadsheets, web pages, presentations, chat logs, multimedia and more—all with sensitive data that needs to be secured. In fact, nearly 80 percent of the information created and used by the typical enterprise is unstructured data. As attacks on enterprise data increase in frequency, the costs of a data breach are also on the rise. Monitoring the "who, what, where, when and how" of data access is more important than ever, so organizations can meet compliance obligations and reduce the risk of a major data breach.

IBM® Security Guardium® Data Protection for Files is designed to help support the security and integrity of unstructured data in today's heterogeneous environments. Leveraging an end-to-end graphical user interface, security teams can easily discover, monitor and control access to sensitive files, whether they reside on local or networked file systems.

What's more, Guardium Data Protection for Files is part of the IBM Security Guardium platform, which has the flexibility to meet a wide range of data security requirements. The Guardium platform enables security teams to create a comprehensive strategy to safeguard sensitive data—and support it across the entire environment, from databases and files to big-data platforms, applications and cloud environments.

Why use Guardium Data Protection for Files?

- To discover and classify sensitive data in unstructured data repositories – such as NAS, SharePoint, Windows, and Unix
- To protect critical configuration and application files
- To protect access to files with personally identifiable information (PII) without impacting day-to-day business operations
- To protect back-end access to application documents

SAFEGUARD YOUR SENSITIVE DATA

Guardium Data Protection for Files takes the guesswork out of protecting sensitive data in files. Thanks to its automated analytics, security teams can easily discover and classify files that contain sensitive data and track who has access to the data so that teams can help protect it against both internal and external threats.

As part of the broad Guardium platform, Guardium Data Protection for Files continuously monitors all data access operations at the file system level in real time. It can detect unauthorized actions, based on detailed contextual information. Then, it can react immediately to help prevent these unauthorized or suspicious activities—whether they are performed by privileged insiders or external hackers—and automate data security governance controls across the enterprise.

Guardium Data Protection for Files can deploy preventive measures to mitigate security breaches. It can block suspicious access requests and issue alerts on unusual access to help ensure that data is protected while security teams investigate and neutralize the threat. The entire Guardium platform continuously monitors data access and enforces security policies in real time, without performance impacts or requiring changes to file systems or applications.

Discover and Classify Data in NAS devices, SharePoint, Windows, Unix

Guardium Data Protection for Files enables security staff to automatically discover files containing sensitive information, and then use customizable classification labels and entitlement management capabilities to create and enforce security policies. The solution locates files, extracts their metadata (such as the name, path, size, date last modified, owner and privileges), and stores the details in a secure central repository. It also examines file content to help identify those files that contain sensitive data, such as credit card numbers, Social Security numbers, email addresses or source code. Entitlement reports show who has access to this sensitive data. Knowing who has access and what data is sensitive helps organizations manage risk—such as removing dormant sensitive data or dormant entitlements to data.

Some key discovery and classification capabilities include:

- A non-invasive/non-disruptive discovery process that can be configured to specify file directories on a schedule or on demand
- Support for many data file types, including PDF documents, text, Microsoft Office files, comma-separated values (CSV) files, logs, source code (Java, C++, C#, Perl, XML) and more
- Prepackaged classifications for facilitating Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA) compliance, as well as a prepackaged classification for source code

Gain Visibility into Entitlements

Knowing who has access to files—and what those users access—is critical for data security. With Guardium Data Protection for Files, organizations can get a full picture of the ownership and access rights assigned to all files. This information can then be used in audit reports, alerts and real-time policies to help protect sensitive data. Automating group management enables Guardium Data Protection for Files to adapt to changes in user access. Whitelists or blacklists can also be generated on any auditable item, such as user IDs, IP addresses or file names.

Some key entitlement reporting capabilities include:

- A single, centralized and normalized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics
- The ability to quickly search on audit reports and other items within the interface, as well as run quick, enterprise-wide searches on the data itself
- An innovative report builder for creating customizable entitlement reports

- Categorization of which documents are unused and, therefore, probably need to be archived

Monitor and Block Unauthorized Access

To help protect sensitive data, Guardium Data Protection for Files can help users establish preventive measures against unauthorized users accessing (or trying to access) sensitive data in real time. It audits file activity according to security policies, issues alerts on improper access, and selectively blocks access to files, helping prevent data loss. This control even extends to privileged users. For example, the solution can detect a mass copy of sensitive files or directories, detect a sudden spike in file-access activity by a specific administrator, generate alerts about the potentially illicit access, block access to the most sensitive documents and generate custom reports for all activity.

Automate Compliance

Guardium Data Protection for Files automates the entire data compliance auditing process—including report distribution, e-signature sign-offs and activity escalations—through preconfigured reports and policies. It provides a complete compliance picture for unstructured data with support for custom reports and advanced search capabilities. What's more, organizations can deploy Guardium Data Protection for Files to meet specific compliance requirements and protect business assets, even as requirements evolve.

Compliance reporting is enhanced with:

- Support for a wide range of audit tasks in customizable compliance workflows, including report generation, distribution, electronic sign-offs and escalations
- Centralized audit reports from multiple data sources
- Integration with IBM Security solutions, such as IBM Security QRadar® SIEM, to enable more effective correlation of threat activity and proactive risk remediation

WHY IBM SECURITY GUARDIUM?

The IBM Security Guardium platform provides a comprehensive approach to data security. Guardium applies intelligence and automation to enable a centralized, strategic approach to securing sensitive data. Robust real-time and right-time analytics help security teams analyze the risk landscape and quickly uncover internal and external threats. The solution provides a broad range of data protection capabilities, including:

- Automated discovery and classification of sensitive data
- Entitlement reporting
- Vulnerability assessment and remediation
- Data and file activity monitoring for NAS, SharePoint, Windows, and Unix repositories
- Masking, encryption, blocking, alerting and quarantining
- Automated compliance support

Guardium helps security teams secure sensitive data in today's heterogeneous environments, across databases, data warehouses, Hadoop, NoSQL, in-memory systems, files, cloud environments and so on. The solution also easily adapts to changes in the IT environment—whether that includes adding new users, expanding capacity or integrating new technologies.

For more information

To learn more about this offering, contact your IBM representative or IBM Business Partner, or visit: https://www.ibm.com/us-en/marketplace/guardium-data-protection-for-files

IBM Security
75 Binney St
Cambridge, MA 02142

Produced in the United States of America
April 2018