IBM Security Guardium Activity Monitor for Files

Discover and classify sensitive file data, continuously monitor files, and detect and block suspicious activity

Highlights

- Discover and classify sensitive data in files and continuously monitor and audit all file activity
- Block user access by enforcing security policies in real time—for all file access, including access by 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 sensitive data in heterogeneous environments, including most common types of 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.

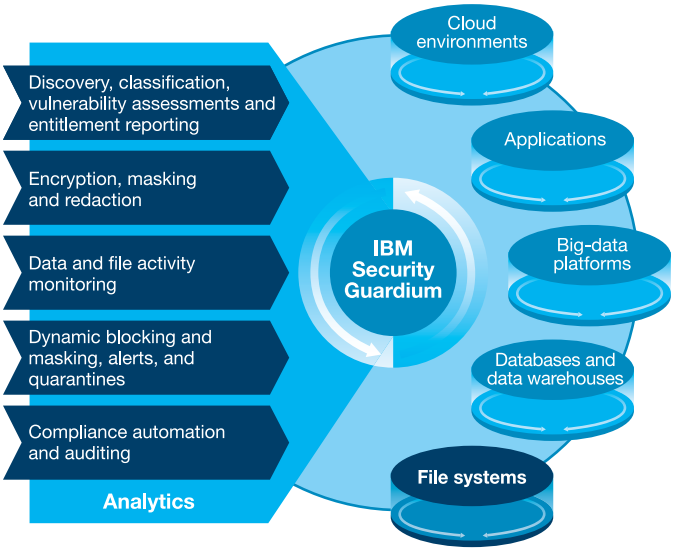
IBM® Security Guardium® Activity Monitor for Files is designed to help assure the security and integrity of unstructured data in today's heterogeneous environments. Leveraging an end-to-end graphical user interface, security teams can easily discover, monitor and control access to sensitive files, whether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

What's more, Guardium Activity Monitor 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.

Safeguard your unstructured data

Guardium Activity Monitor 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 Activity Monitor 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.



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.

Guardium Activity Monitor 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.

Why use Guardium Activity Monitor for Files?

- To protect critical configuration and application files, which can be opened, modified or even destroyed through direct access from within the application or database server
- 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, which can be accessed from within the application
- To protect source code and other intellectual property, which can be accessed on build servers or enterprise file systems

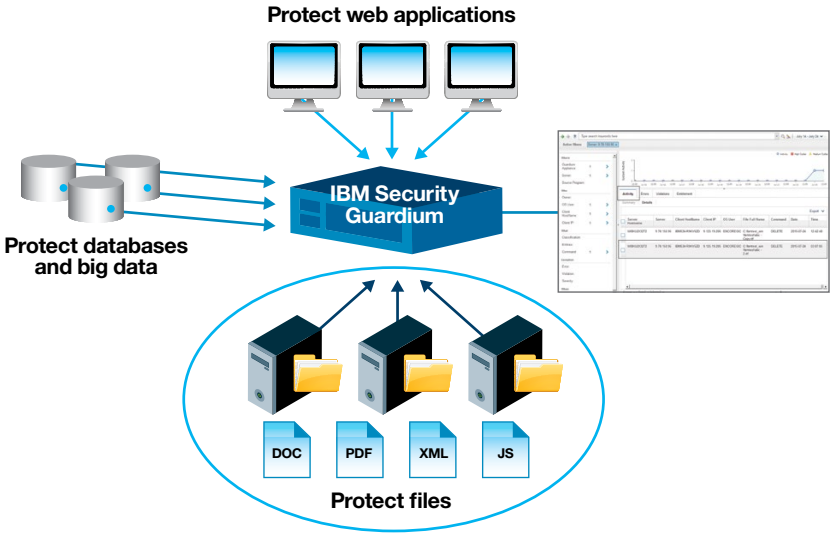
Discover and classify sensitive data

Guardium Activity Monitor 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/nondisruptive discovery process that can be configured to specify file directories on a schedule or on demand
- Support for most common data file types, including PDF documents, text, Microsoft Office files, comma-separated values (CSV) files, logs, source code (Java, C++, C#, Perl, XML) and configuration files
- 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



- Classify files and understand sensitive data exposure
- Visualize ownership and access for your files
- Monitor all file access and review it in a built-in compliance workflow
- Control access to critical data through blocking and alerting

Guardium Activity Monitor for Files provides comprehensive protection. It makes it easy to see which files contain sensitive data—such as a PDF file containing credit card data—monitor file access and take action to help protect against internal and external threats.

Gain visibility into entitlements

Knowing who has access to files—and what those users access—is critical for data security. With Guardium Activity Monitor 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 Activity Monitor 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 Activity Monitor for Files can deploy 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, preventing data loss. This control even extends to privileged users. For example, Guardium Activity Monitor for Files 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 Activity Monitor 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 Activity Monitor 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, tamper-proof 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

Real-world results in the IBM environment

Guardium Activity Monitor for Files is already hard at work at IBM. Deployed on more than 2,000 build servers, the solution helps protect the source code within IBM development environments. The benefits include:

- Ease of use: **Installations on each build server take less than two minutes; IT staff also save time with one-click access to audit reports and risk analysis.**
- Low impact: **The solution monitors, analyzes and audits access to source code with minimal impact to the build environment.**
- Real-time alerts: **If unauthorized or suspicious activity occurs, build administrators are immediately notified to take action.**
- Scalability: **The Guardium infrastructure easily scales to support thousands of data sources, automatically balancing loads and adapting to changes without impacting performance.**

Why Guardium?

The 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
- Masking, encryption, blocking, alerting and quarantining
- Automated compliance support

Guardium empowers security teams to help 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.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for advanced data protection. These proven technologies enable organizations to safeguard their most critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions.

IBM has worldwide service delivery expertise in some of the most highly regulated industries, including government, healthcare and financial services. As a strategic partner, IBM empowers organizations to reduce security vulnerabilities and manage risk across the most complex IT environments.

For more information

To learn more about IBM Security Guardium Activity Monitor for Files, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/ibm-security-guardium-for-files

About IBM Security solutions

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.

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. For credit-qualified clients we can customize an IT financing solution to suit your business requirements, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
December 2015

WGD03088-USEN-00