cm FIRST
Rethink Modernization

info@cmfirstgroup.com
888-866-6179

Security

Solution Brief

Secure the data that powers your business

IBM Security Guardium helps analyze, protect and adapt for comprehensive data protection

Highlights

- Adopt a proactive, holistic approach to protecting critical data across all types of platforms, including major databases, data warehouses, big-data platforms, cloud environments, file systems and more
- Lower total cost of ownership by automatically discovering sensitive data, uncovering risks and taking action
- Protect sensitive data against threats with encryption, masking, redaction, activity monitoring, dynamic blocking, alerting and quarantines
- Leverage data compliance automation to get the right reports to the right people at the right time
- Adapt to changes in the IT landscape and support the full data protection journey

These days, data security breaches are more common than ever—and more impactful. Global studies show that the average total cost of a data breach is now USD 4 million.[1] What's more, the loss of trade secrets, product designs or other intellectual property can spell financial ruin for an organization. Because of its value, critical and sensitive data is at the core of business interactions—which also makes it a highly attractive target for attack.

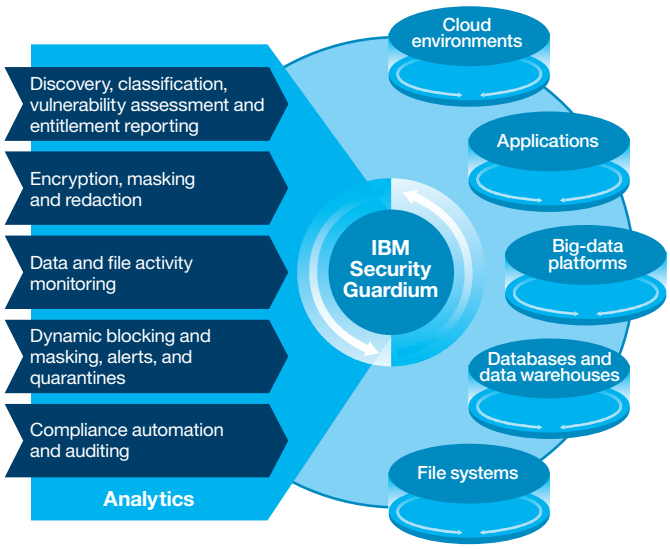
Traditionally, organizations have focused on "perimeter" defenses for protecting their critical information. But traditional tools, such as anti-virus software and firewalls, are not equipped for today's advanced threats, which many times come from inside the organization. Plus, data is constantly growing, changing and moving, so data protection measures must also be able to adapt to follow the data. Increasing numbers of users, applications and systems need instant access to different types of sensitive data—residing in or replicating into databases, data warehouses, file shares, big-data platforms, cloud environments and more. Keeping track of who has access to this dynamic, distributed and disparate data, and who is sharing it (and with whom), can seem like an insurmountable task.

IBM® Security Guardium® is designed to safeguard critical data, wherever it resides. This comprehensive data protection platform empowers security teams to automatically analyze what is happening across the data environment to help minimize risk, protect sensitive data from internal and external threats, and seamlessly adapt to changes that affect data security and compliance.

Count on comprehensive data security

Guardium provides a comprehensive approach to protecting an organization's "crown jewels"—the critical data that is vital for business success and survival. Leveraging its end-to-end graphical user interface, security teams can identify and remediate risks to sensitive data, whether the data is in motion or at rest. And this unified approach extends to a broad range of both structured and unstructured data repositories, including databases, data warehouses, Hadoop, NoSQL, in-memory systems, file shares and so on.

In fact, Guardium has the flexibility to meet a wide range of data security and protection requirements—from basic compliance to comprehensive data protection—in a cost-effective, scalable way. The multi-layered solution includes automated data threat analytics, dynamic data protection and enterprise-wide visibility to adapt to changes in the sensitive data environment.



Guardium uses cognitive analytics and automation to help protect critical data in today's heterogeneous environments.

Analyze threats to sensitive data

For effective data protection, organizations need to understand what exactly they need to protect and then thoroughly protect it. Guardium enables security teams to:

- Discover and classify sensitive data and entitlements—and uncover compliance risks—automatically
- Know who is accessing data, spot anomalies and stop data loss
- Rapidly analyze data usage patterns to uncover and remediate risks
- Support analytics with automated advanced analytics and machine learning to spot and stop unusual and risky behavior
- Leverage specialized threat-detection analytics to spot and stop breaches early—such as by finding and alerting on SQL injections or malicious stored procedures
- Provide a dashboard to help key stakeholders see data security and/or compliance status and progress over time, to better understand how the initiative is adding value to the business—and to understand gaps

Guardium helps security teams automatically discover and classify sensitive information—from within an easy-to-use graphical user interface. Using a series of steps, security staff can discover all data sources containing sensitive information, including uncataloged databases, and then use customizable classification labels and entitlement management capabilities to automate enforcement of security policies. Sensitive data discovery can also be scheduled to execute regularly to help prevent the introduction of rogue servers and ensure that no critical information is missed.

To help enforce policies and protect sensitive data, Guardium can continuously monitor who is accessing (or trying to access) sensitive data in real time. Going beyond traditional data monitoring, Guardium has outlier-detection capabilities with increased intelligence to analyze and understand risk based on

changes in behavior. It uses an advanced machine-learning algorithm to detect abnormal data access based on detailed contextual information—the "who, what, where, when and how" of each data access. With an adaptive learning process, it compares new normal activity patterns against new activities as they accumulate. Its intuitive, cognitive user interface helps pinpoint anomalies, so administrators can drill down to investigate the root cause.

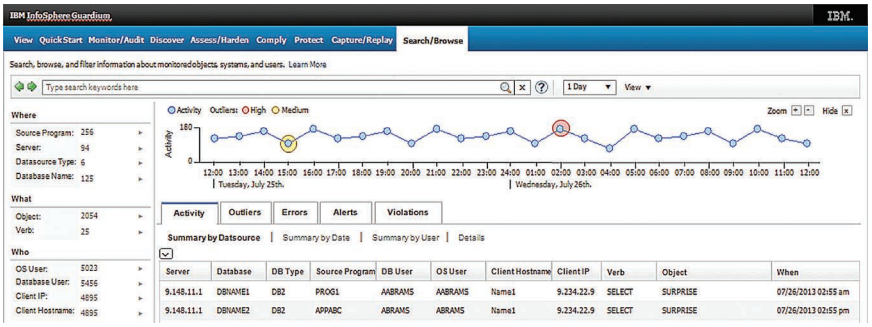
In addition to drill-down capabilities, Guardium enables security staff to quickly search on audit reports and other items within the interface, as well as run quick, enterprise-wide searches on the data itself. There's no need to understand the underlying topology, aggregation or load-balancing schemes. The search requests can help extract insights from specific data access activity, whether focused on specific data sources, users or dates. A new investigation dashboard can also help reveal patterns, anomalies and relationships across the data, helping narrow the scope with best-practice default views. There is also a Connection Profiling tool that reports on all the attempted connections to a specific data source.

Protect sensitive data

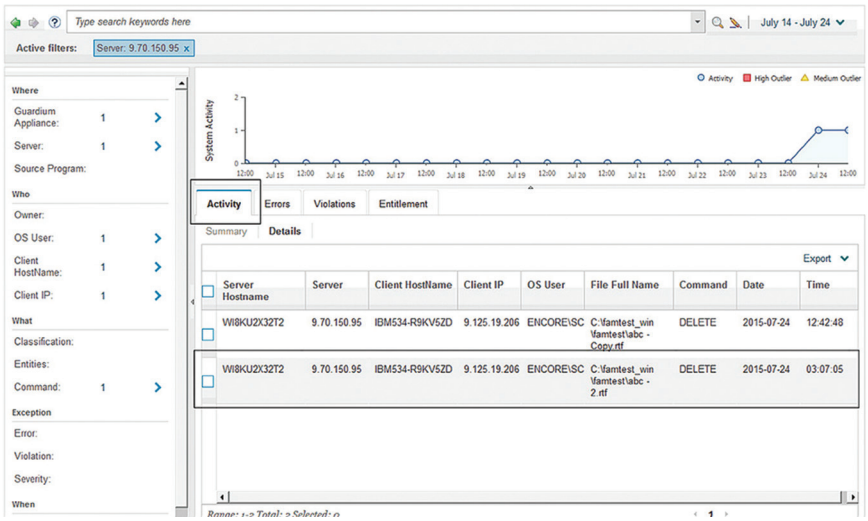
Escalating threats to sensitive data and growing compliance mandates are driving organizations to rethink their data protection strategies. Guardium enables security teams to:

- Shield the business from financial risk with automated data compliance and extensive audit capabilities
- Control critical data through encryption, masking, redaction, dynamic blocking, alerting and quarantines
- Use real-time activity monitoring and blocking to help prevent illicit internal and external data and file access

Guardium helps capture and examine all sensitive data traffic, including local access by privileged users, with a secure, tamper-proof audit trail. In fact, it provides a single, centralized and normalized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics. Organizations can automate the entire data compliance auditing process—including report distribution to oversight teams, sign-off and escalations—with preconfigured reports for Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS) and data privacy.



Guardium provides a convenient graphical interface for identifying and responding to outliers detected by an intelligent algorithm.



With file activity monitoring, Guardium empowers organizations to detect and block suspicious activity on document data—even by privileged users.

What's more, Guardium empowers security teams to protect sensitive data from internal and external threats with file-based encryption, database and big-data vulnerability assessment, static data masking and redaction capabilities. It also supports dynamic, real-time data masking and encryption, as well as blocking, alerting and quarantining of suspicious users. In fact, it can restrict access from rogue actors to sensitive data across most sources, including cloud environments, big-data platforms and file systems.

Guardium also helps enforce segregation of duties by continuously monitoring all sensitive data activities, including real-time monitoring of file-system access. It enables organizations to detect, log and block unauthorized and suspicious activity by privileged users. For example, Guardium 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 improper access, block access to the most sensitive documents and generate custom reports for all activity. Guardium can also help discover exposures with the database and big-data infrastructure to ensure that the foundation for the data is hardened.

Adapt to change

Data infrastructures are constantly changing and growing—making it challenging and costly to keep up with emerging and ever-changing security gaps. Guardium gives organizations the power to:

- Support traditional and disruptive data technologies—such as Hadoop, NoSQL and cloud
- Easily expand the data protection architecture, growing from regulatory compliance to comprehensive data protection
- Reduce costs and improve results using a single data protection infrastructure—one that automatically load balances—across the entire data environment

Guardium enables organizations to adapt to changes in the data environment, expanding data protection to address new users, platforms and types of data. It also provides a platform that simplifies the administration of data security by incorporating the way IT operates, through automation, centralization and integration. Out-of-the-box certifications, such as the Defense Information Systems Agency (DISA) Authority to Operate (ATO), or compliance accelerators for key regulations, such as the General Data Protection Regulation (GDPR), are included for the convenience of end users. The broad platform focus includes support for traditional databases, cloud environments, Hadoop-based systems, NoSQL, in-memory systems and file systems. Guardium provides agile control that can be deployed for specific compliance requirements and then easily scaled to provide additional protection as business needs evolve.

Unlike a point solution, Guardium supports heterogeneous integration with other industry-leading security solutions, vulnerability standards, applications and more. Guardium also provides best-of-breed integration with IBM Security solutions, such as IBM QRadar® SIEM, for proactive data protection. Guardium sends its events and database discovery/classification information to QRadar SIEM, enabling more effective correlation of threat activity. In addition, Guardium can receive status and alert notifications from QRadar SIEM to help defend against rogue IP sources, rogue users and new vulnerabilities, whether in applications, operating systems or other data sources. For example, the Guardium and QRadar integration can help organizations protect against potential attacks through applications; detect database attacks (such as through SQL injection) and block them before data can be extracted; and identify vulnerabilities at the application layer for virtual patching remediation.

Guardium delivers value across a wide range of industries

- **A large insurance firm** can now manage security for approximately 1,000 databases with just one full-time employee.
- **A large utilities company** achieved a 55 percent return on investment in less than one year, helping ensure SOX and PCI compliance for 4.5 million accounts.
- **A global bank** can monitor more than 5,000 data sources, including big-data transactions, in real time—without impacting the performance of critical applications.
- **An international telecommunications company** is now able to centrally monitor and respond in real time to data access activity on thousands of databases dispersed in 16 data centers worldwide.
- **An automotive manufacturer** can monitor and audit 500 production databases to help increase security, while reducing its security staff requirements by 90 percent.

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, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/guardium

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.

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
June 2017

[1] "2016 Cost of Data Breach Study: Global Analysis," *Ponemon Institute*, June 2016. **ibm.com**/security/data-breach/

Please Recycle

WGS03063-USEN-02