Integrated Solution for Data Access Governance

Highlights

- Protect data and user access across hybrid-multicloud data repositories
- Enforce separation of duty and access governance rules on sensitive data
- Comply with privacy and industry regulations

A unified approach to manage user access to applications and data

Most organizations today have enormous amounts of data stored in their databases, shared network drives, collaboration systems, and applications. What they often struggle with is understanding user access to these various repositories and if that access is, in fact, justified. Managing this access can be difficult for many reasons, from users continuously changing job roles, to static enforcement rules to the ever increasing volume of data. When users are over- or under-entitled, the organization suffers from a lack of productivity, dormant accounts that become potential attack vectors, and the risk of insider threats. The potential for violations under regulations like GDPR or CCPA are magnified. Ensuring the right users have the right access for the right reasons is what data access governance is all about.

Current data access governance tools do a binary calculation to decide if users should or should not have access based on their job role and a generic understanding of an application or data repository. This approach misses visibility into the sensitivity of the data and whether a particular user actually needs access to that data to do their job. Similarly, data in repositories is constantly changing. A database that previously held non-sensitive data may one day store credit card numbers, but access controls do not typically adapt as quickly to keep up with these changes. These blind spots in the environment can be exploited because these traditional systems lack context and agility.

Through the integration of Guardium Data Protection and IBM Security Identity Governance &

Intelligence (IGI), two best-of-breed solutions, users now have an end-to-end data access governance solution to protect against these threats. Incorporating identity governance helps manage users' access to data and applications based on the organization's access control policies which help proactively uncover the risk of insider threats and data breaches through in-depth access analysis and remediation.

IGI, a comprehensive identity governance and administration solution, provides a unified view of data access risks and helps determine who should have access to what resources based on their job role, group membership, or other attributes. IGI's key features include user access review and certification, end-to-end user lifecycle and entitlement management, and identity analytics. IGI simplifies the approach to mitigating risk to sensitive data access and separation of duty violations by providing a business activity model that makes it easier for business owners and compliance officers to understand the access that individuals in the organization have and why. In order to have a true view into access risk, visibility into sensitive database and file repository entitlements is required.

Guardium Data Protection provides IGI with that level of data intelligence so it can perform comprehensive separation of duties and access risk assessments. Guardium Data Protection discovers and classifies sensitive data, and monitors and audits user activity to help protect sensitive data across hybrid multi-cloud environments. With Guardium, security teams can set entitlements and access controls, streamline compliance, and get contextual insights and analytics to help detect and block suspicious activity.

Adding IGI to a Guardium Data Protection deployment adds a critical layer of security and risk mitigation through increased visibility into user access at the data layer. Guardium Data Protection surfaces the specific data classification, such as whether a user can access personally identifiable information (PII). Together, through an out-of-the-box integrated solution, IGI and Guardium Data Protection help answer these imperative questions: 1) Where is my sensitive data? 2) What data can my users access? 3) What is my compliance and security risk posture?

A large telco is an example of an IBM client who has put this concept of data access governance into action. As one might expect, the company manages millions of customer records that contain sensitive and private information. The business outsources more than 75% of its workforce to various managed service providers and other third parties. With a turnover rate greater than 20% on a monthly basis, it was extremely difficult to rely on static policy-based systems to ensure consistent, context-based access. Integrating IGI with Guardium Data Protection has enabled the firm to automate onboarding and offboarding as well as implementing risk-based certification approvals for users that may have a role based need to access customer records. This has enabled the business to not only maintain regulatory compliance but to reduce the overall risk exposure as well.

Organizations of all sizes are struggling with the explosion of data and the need to ensure customer trust in their handling of that data. The Guardium Data Protection and IBM Security IGI integrated solution enables clients to have visibility into where data is stored and who has access to it.

This ensures data is handled properly and only by authorized personnel, providing the organization’s leadership and their customers with peace of mind.

Why IBM?

Of the dozens of vendors that offer IAM solutions and services, only IBM infuses deep identity context and expertise into your program, empowering you to give the right people the right access at the right time. That’s why IBM is also the only vendor that leads in identity governance and administration (IGA), access management, privileged access management and professional and managed services. With the industry’s broadest portfolio of IAM solutions and more than 7,000+ experts focused on supporting your transformation, we can help tackle your toughest identity challenges.

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 stop threats, prove compliance, and grow securely. IBM operates one of the broadest and deepest security research, development and delivery organizations. It monitors more than two trillion events per month in more than 130 countries and holds over 3,000 security patents.

For more information

For more information on IBM Security Identity Governance & Intelligence:
https://www.ibm.com/us-en/marketplace/identity-governance-and-intelligence

For more information on IBM Guardium Data Protection:
https://www.ibm.com/security/data-security/guardium

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.