Unify Management of User Access to Both Apps and Data

Introducing IBM Security Verify Governance and Guardium Integration

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 needs access to that data to do their job.

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

Adding Verify Governance to a Guardium Data Protection adds a critical layer of security and risk mitigation

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 IBM's Guardium Data Protection and Security Verify Governance, 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.

Verify Governance, a comprehensive identity governance and administration (IGA) 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. The Verify Governance key features include user access review and certification, end-to-end user lifecycle and entitlement management, and identity analytics.

Verify Governance 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. To have a true view into access risk, visibility into sensitive database and file repository, requires entitlements.

Guardium Data Protection provides Verify Governance 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 Verify Governance 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, Verify Governance and Guardium Data Protection help answer these imperative questions:

1) Where is my sensitive data?
2) What data can my users access?
3) What are my compliance and security risks?

One large telco company has put this concept of data access governance into action. The company manages millions of customer records containing 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% monthly, it was extremely difficult to rely on static policy-based systems to ensure consistent, context-based access.

Integrating Verify Governance 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 integrated solution, Guardium Data Protection and Verify Governance enables visibility into where data is stored and who has access. 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?

IBM Security Services professionals can offer virtually unparalleled IAM expertise, broadened by their access to IBM's research and development team. Available worldwide, IBM specialists can tailor their recommendations to your region's unique circumstances. Their approach to IAM strategy and assessment examines impact at every level of your organization—from business strategy to applications to IT infrastructure — to help you implement an IAM program designed to meet your business and IT objectives.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

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

For more information

To learn more about IBM Identity and Access Management Services for identity and access strategy and assessment, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security/services

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing