



---

*Highlights*

- *Seamless User Access Experience*
  - *Simplify self-service user access*
  - *Automate Identity lifecycle processes*
- *Continuous Compliance*
  - *Visualize and certify user entitlements*
  - *Provide insight into user risks/SoD violations*
- *Intelligent Analytics*
  - *Identify and mitigate risky access or users*
  - *Personalized, actionable dashboards*



## Identity Governance & Intelligence (IGI)

IBM Security Identity Governance and Intelligence (IGI) delivers a business-centric approach to Identity Governance and Administration. IGI helps customers maintain strong control over user access to applications and carefully monitor how entitlements align with business roles and responsibilities. IGI empowers business and IT to work together to meet regulatory compliance and security goals across enterprise applications and data.

IGI is packaged as one software appliance and comes in four purchasable options:

- **IGI Lifecycle** – enables user lifecycle management and user self-service to streamline user onboarding, off-boarding and self-service access request processes for on-prem and cloud applications.
- **IGI Compliance** – helps address extensive regulatory and access governance requirements for user access audit, featuring unique capabilities on systems like SAP and IBM z/OS mainframe.
- **IGI Analytics** – helps identify areas of risk and access optimization, providing priceless visual insights.
- **IGI Enterprise** – includes all three options above plus Identity Management Premium Application Adapters.

### Unparalleled Integration Capabilities

IBM IGI is a key part of the IBM Security portfolio addressing compliance, data protection and insider threat requirements. IGI has powerful integrations with both IBM Data Security (Guardium) and IBM SIEM (QRadar), providing a unique platform with cognitive capabilities. The integration with IBM Guardium addresses GDPR requirements, while the integration with QRadar User Behavior Analytics (UBA) tackles insider threat detections and remediation. IGI is natively integrated with ServiceNow, providing access request management entirely from the ServiceNow user interface. Additionally, IGI provides a much deeper integration with Privileged Identity Management products, such as IBM Security Secret Server, among others.

## Full Enterprise-Level Identity Governance and Administration

### Enable certification campaigns

IGI enables the business to run campaigns to reconfirm users access needs with a customizable, self-service user dashboard. This simple experience quickly provides flexible and powerful workflow allowing users to easily recertify access.

### Determine segregation of duties violations

IGI uses a unique business activity-based approach to model segregation of duties violations rather than relying on unmanageable role-to-role comparison. Business activity is immediately readable to the business user and enables a very clear way of showing risk that is both understandable and actionable.

### Consolidate application access entitlements

IGI offers a rich set of mature and compatible application adapters, both on-prem and for the cloud. This allows for better visibility and user access control for role mining, modeling and optimization.

### Provide end-to-end user lifecycle management

IGI provides ease of use by bridging lifecycle management capabilities including powerful role management, multilevel provisioning workflow and integrated password management.

## Key Differentiators

- IGI uses industry-standard business activities taxonomies that enable business managers to make appropriate access decisions, which are based on employees' business functions.
- IGI provides advanced visual analytics for role discovery and optimization as well as the ability to model criteria, measure and trend access risks.
- IGI integrates as a key element of today's Data Protection/Privacy strategy, providing a one-stop-shop approach that goes from the Data Store up to People and Applications. This helps with new regulations, such as GDPR, that require an end-to-end approach that stands up to audits.
- IGI features unique segregation of duties controls capabilities specifically for the SAP environment. Several clients have chosen IBM specifically for this unique combination, often sparing the need to purchase SAP GRC Access Control or similar ERP-Compliance tools.
- IGI has a superior, fine-grained z/OS integration that allows access governance and compliance on z/OS mainframes to identify access policy violations and to help remediate excessive privileges, (e.g. to perform access reviews based on the risk level).

## For more information

To learn more about this offering, contact your IBM representative or IBM Business Partner.



---

© Copyright IBM Corporation 2018

IBM Security  
75 Binney St  
Cambridge, MA 02142

Produced in the United States of America  
January 2018

IBM, IBM logo, ibm.com, are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.



Please Recycle

---