ForgeRock®

Product Brief

ForgeRock Identity Governance

Good security policies and practices should drive your compliance program — and identity access management has become an integral part of governance for most organizations. Today's employees are aware of compliance regulations and expect to work within the parameters of tighter controls. To make it easy for your users to follow best practices and security policies while getting the access they need to do their jobs, modern governance demands centralization of identity access management. An increasingly insecure world requires you to balance ease of use and access for users with a continual security vigilance that puts limits on unnecessary or high-risk access.

Establishing security policies and enforcing them centrally is the first step. As identities are spread across many external systems and services, governance becomes more difficult. You need a governance system that you can leverage as a process orchestration tool to govern and manage all identity-related activities. You then need to prove compliance to both internal and external auditors. They want assurance that your organization is following appropriate security procedures for every user access request and approval and that no one has unnecessary privileges.

ForgeRock Identity Governance allows you to establish policies for user access rights and continuously monitor their proper implementation from a centralized location. Through a periodic access review process — tied to a powerful workflow engine to ensure closed-loop remediation and built-in risk management and reporting — you strengthen your security posture and automatically drive regulatory compliance.

Highlights

- The only identity governance solution on the market purpose-built for people, services, and things.
- Part of the ForgeRock identity and access management (IAM) platform for a single-pane view, giving you full user management, workflow, auditing, and reporting.
- Flexible access review options to meet your regulatory needs including Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and Global Data Protection Regulation (GDPR).
- Closed-loop remediation to quickly and efficiently revoke access when a reviewer declines access during certification.
- Centralized policy verifications to enforce preventive and detective controls for Segregation of Duties (SoD) violations.
- Flexible data modeling and relationship support allows for applying consistency between all identities and downstream applications and data systems.
- Complete role lifecycle management with integrated approval workflows and out-of-the-box templates for faster deployment.
- Detection of rogue access and automatic remedial actions that can revoke access, send notifications to appropriate teams, and initiate an ad hoc certification.
- API-First approach allows you to easily embed the access request and governance capabilities into your existing portals and applications using REST.
- DevOps-enabled for easy deployment on premises, in a hybrid environment, or in the public cloud, including Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP).

Features and Benefits

Access Request

In today's world where simplicity and usability dominate the consumer world, employees expect the same level of service from their organizations. They do not have the time or patience for lengthy and time-consuming processes, especially when they are trying to complete a task but are missing required access. Enabling a self-service, user-friendly Access Request portal provided by the Forgerock Identity platform or through a REST API that can be easily embedded into your existing applications will ensure that your users stay productive while reducing help desk calls and IT workload — without compromising the company's compliance policies and regulations.

Access Review

Managers and application and data owners can review employee access to ensure users can complete day-to-day tasks in a quick and efficient manner, without compromising corporate and security policies.

Access review can run on a periodic basis, on a pre-set schedule, or ad hoc, based on organizational events like Mergers and Acquisitions (M&As) or user events like role and department changes. Establishing an automated process to monitor and handle those changes dramatically increases compliance with regulations such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and Global Data Protection Regulation (GDPR). It reduces risks introduced by unnecessary access proliferation while ensuring that employee productivity is unhindered.

Email Notifications

Promptly notify your reviewers about new and pending review tasks using the out-of-the-box email notifications or create your own based on your needs. Tracking progress enables certifiers and administrators to focus on high-priority tasks and not lose track of critical assignments during daily activities

Multi-Stage Certification

One or more approvers or teams can review employee access during a single review cycle. This ensures that all appropriate stakeholders are given a chance to evaluate users' complete access and make informed decisions on whether that level of access is appropriate based on predefined policies and regulations. Approvers are easily selected during certification creation and can be assigned to any user, user manager, or other owners. If reviews are not completed by the designated deadline, you can define an escalation stage to ensure a timely review based on organizational compliance standards.

Closed-loop Remediation

Identity Governance is tightly integrated with the provisioning and synchronization capabilities provided by the ForgeRock Identity Management platform to ensure that access review is a closed-loop process. When a reviewer denies user access, it is automatically revoked from their identity and propagated to the downstream system or application. This closed-loop process assures that access rejected by an approver is promptly removed from employees through an automated and efficient process.

Flexible Data Model

ForgeRock Identity Governance is built on a flexible data model that can manage identities of users, devices and things along with all the relationships between them. This data model can also be easily extended to fit the needs of any type of user such as an employee, contractor, vendor, and consumer, as well as any non-carbon entities such as a phone, an application or even a service. This extensible identity model with a very flexible relationship model allows you to leverage ForgeRock as an authoritative and centralized repository of all identity information.

Entitlement Management

ForgeRock Identity Governance allows you to associate metadata with any object managed within the product using a user-friendly interface. The business glossary allows administrators to assign a business-facing name for any user entitlements, as well as extending the information presented to users, such as links to help pages, documents, and risk scores. This information helps employees understand the additional privileges they are requesting and provides a transparent view of the overall process and approvals required to successfully complete requests.

Segregation of Duties Policy Enforcement

Identity Governance enables administrators to create policies to govern toxic access combinations in order to proactively prevent Segregation of Duties (SoD) violations or improper access grants to users. You can evaluate SoD policies during access request workflows as a preventive control to make sure such violations do not occur within your organization. You can also schedule policy evaluations to run on a periodic basis on the latest identity data as a detective control to find any established process subversion or to identify rogue accounts.

Role Lifecycle Management

Our solution provides robust and complete role lifecycle management capabilities, including role definition to any changes and deletes. This allows you to implement a flexible, role-based access control (RBAC) model. Roles can be easily assigned to role owners, who can then certify role entitlements, role membership rules, and role members themselves.

Risk Management

Forgerock Identity Governance provides a flexible risk scoring mechanism to allow your administrators to assign a risk score for everything — entitlements, roles, and certifications within the governance platform. Administrators can associate simple classifications for risk scores, such as “low,” “medium,” or “high,” to speed decision making for employees and approvers during their review and approval processes.

Identity Data Cleanup

Corporate teams can maintain centralized policies that govern user identity data quality and perform data cleanup on a periodic basis. This ensures that user identity data is always clean — even where there is a large influx of changes due to organizational transformations, M&As, or seasonal spikes of user hiring activity.

Rest API

Comprehensive and simple RESTful interfaces provide an API for managing all core functions of certification management, access request, and entitlements management. The decoupled user interface enables you to embed custom-tailored solutions into existing applications or create new mobile applications easily and securely.

Workflow Engine

Identity Governance provides workflow-driven provisioning activities for self-service actions, such as requests for access, manager-driven access reviews and certifications, and administrative actions, such as updating entitlements, onboarding and offboarding, bulk sunrise or sunset enrollments, handling approvals with escalations, or performing maintenance. The embedded Activiti engine supports BPMN 2.0 for standards-based, business-focused management.

Reporting and Audit

The Access Review process is extremely critical for organizations that need to streamline the process of who has access to what and ensure employees meet the compliance requirements. ForgeRock Governance offering provides a simple reporting and audit feature based on our flexible auditing capabilities to formalizes the review process for auditing purposes. Administrators and business owners can get up and running day one with a set of predefined report template that compliments the Access review feature as well as the ability to define custom reports per your needs. Reports can run immediately or on a schedule. When completed, an email will alert you that your results await.