ForgeRock

SOLUTION BRIEF

Artificial Intelligence-Driven Security and Compliance

ForgeRock Identity Governance and Administration Solutions for Government Agencies and Organizations

ForgeRock Identity Governance and Administration (IGA) is a modern solution that allows government agencies and organizations to add AI and ML to their existing governance solutions to accelerate secure access for internal users, achieve regulatory compliance, mitigate risks, and reduce costs.

The digital "new normal" has quickly changed how government agencies and organizations are planning and executing their strategic plans for digital transformation. They have adjusted to supporting remote work. But obstacles still remain. For remote and on-site employees, contractors, and other internal users, poorly designed and insecure digital access makes it hard to be productive. Excessive access and licensing permissions that are granted and never revoked can leave government agencies and organizations vulnerable to data breaches. Agencies and organizations that cannot secure their workforce will fail to meet compliance requirements, and are at risk for financial penalties.

The ForgeRock Workforce IGA solution helps government agencies and organizations enable an autonomous, self-driving governance process. It uses artificial intelligence and machine learning to automate access and certification processes, clean up user access privileges, and identify security and risk blind spots across the agency or organization. This results in higher audit pass rates, stronger compliance controls, and shorter review cycles.

The Digital Identity Evolution

Today's government security leaders face tremendous pressure to support both on-site and remote work in response to the global pandemic. Remote work has quickly become the new normal, fundamentally changing the way government agencies and organizations acheive their mission. They are still responsible for executing on their strategic plans. Government security leaders must weigh the risks and benefits associated with the workforce, maintain regulatory compliance, and improve operational efficiency.

Employees, contractors, and other internal users such as warfighters need seamless and secure access to remain productive no matter if they're working remotely or on-site. Insider data breach incidents – due to a combination of accidental or inadvertent data misuse or malicious intent – comprised 25% of data breaches, according to a 2019 Forrester security survey.[1] Forrester predicts that the rapid push of users to remote work during the COVID-19 pandemic, fear of job loss, and the ease with which data can be moved will lead to an increase of insider incidents from 25% in 2020 to 33% in 2021.

Government agencies and organizations need to have the right identity governance and access controls in place so that internal users are not provisioned with excessive or inappropriate access privileges to sensitive applications, systems, and data. As agencies and organizations add capabilities for detecting insider threats, they will also be able to identify and attribute more incidents to insider activity than they were previously.

Increased regulatory compliance requirements are pressuring government agencies and organizations to take a hard look at where their processes fall short: weak compliance controls coupled with legacy identity governance solutions limit the ability to visualize, understand, and manage digital identities across the organization.

Government agencies and organizations relying on legacy IGA solutions still find themselves performing manual work, because many of these traditional IGA solutions are slow, cumbersome, and decades old. They have to provision access for internal users such as employees and contractors on day one, review and approve access requests, and close unknown accounts or change inappropriate user access. Most of these legacy IGA solutions integrate with only a few authoritative identity sources, such as the organization's identity store or human resources (HR) system. These identity siloes make it impossible to capture the full purview of where identities are provisioned across the agency or organization. Keeping track of who has access to what and the privilege levels of each account, is impossible for even the most skilled teams. The result is over provisioned access and rubber-stamped certifications that leave government agencies and organizations vulnerable to unauthorized access and potential data breaches.

Self-Driving Governance

Identity governance is heading towards a new paradigm called self-driving governance, in which ongoing processes are automated. Self-driving governance gives internal users the right access to the right resources at the right time – no matter where they are or what platform they are using. With a self-driving governance process in place, government agencies and organizations can fully automate access on day one. They can automatically review and approve access requests, compliance reviews, and close unknown or inappropriate entitlements and security gaps.

Self-driving governance involves multiple processes:

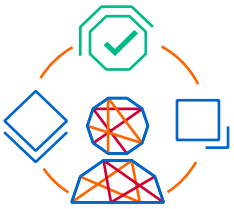
1. **Data Ingestion:** Consuming and normalizing user data from multiple data sources, such as IAM, IGA HR, LDAP, database, Active Directory systems, and others is consumed and normalized.
2. **Data Aggregated:** Collecting data across all data sources and maintaining historical information provides a comprehensive user access landscape of the entire agency or organization.
3. **Artificial Intelligence (AI) Applied:** AI and machine learning (ML) algorithms are applied to the aggregated identity data to predict user access and identify user access risks, inappropriate user privileges, user entitlement creep, and more.
4. **Contextual Analysis:** This type of analysis helps determine, explain, recommend, and justify recommended remediations for user access using low/medium/high confidence scores.
5. **Automated Actions:** Automation pushes recommendations directly back to the agency's or organization's authoritative identity systems, applications, and infrastructure.

[1] Forrester, Predictions 2021: Cyber Security

Why ForgeRock?

ForgeRock helps people safely and simply access the connected world with one platform, supporting all identities, within any environment. ForgeRock Workforce IGA is a modern identity governance and administration solution that allows government agencies and organizations to accelerate secure access, mitigate risks and reduce costs, and achieve regulatory compliance.

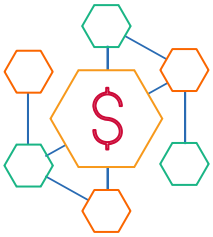
Here are some of the reasons why government agencies and organizations choose ForgeRock:



Streamlined and Simplified Governance

The ForgeRock IGA solution kills "rubber stamp" certifications, while fully automating access and certification processes. Government agencies and organizations can identify entitlement assignments as candidates for automated clean-up and identify and remove licenses for identities with low application usage across the organization.

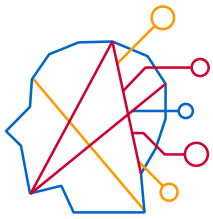
- A multinational financial services organization was able to identify and remove access privileges for 91% of the 1.1 million assignments from a major enterprise resource planning (ERP) application.



Simpler and Faster Time to Value

ForgeRock IGA is a modular, lightweight solution that enables efficient compliance. The AutoID component of the ForgeRock IGA solution lets government agencies and organizations integrate with their existing IGA solution, such as Oracle via application programming interfaces (APIs) or with SailPoint.

- A major U.S. healthcare provider used ForgeRock to identify 550,000 excess entitlements for 14.6 million assignments throughout the enterprise in under three hours.



Smarter and More Secure Operations Using Artificial Intelligence and Machine Learning (AI/ML)

Today, government agencies and organizations are overwhelmed with permissions, entitlements, roles, and groups that are spread across applications throughout the agency or organization. It's impossible to successfully manage all these entitlements manually. To manage entitlements thoroughly and successfully requires AI and ML to automate processing of all the identity data in the agency or organization, find access patterns, and determine the landscape of what good access and bad access looks like.

- A global consumer packaged goods provider reduced 70% of required roles across the organization for 66,000 users and objects.

The Voice of the Customer

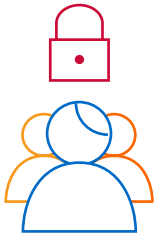
ForgeRock has achieved the highest overall rating (4.5 out of 6) in Identity Governance and Administration according to Gartner.[2]

[2] Gartner Peer Insights Customers' Choice, 31 January 2020.

Benefits

Accelerate Secure Access

- Secure the workforces and other internal users by quickly granting and enforcing secure access to systems, applications, and infrastructure according to established policies.
- Raise workforce productivity and decision-making through AI-driven access approvals, automation, remediation, and recommendations.
- Reduce help desk calls with automated policy-based self-service access to any system, application, and infrastructure.



Achieve Regulatory Compliance

- Pass audits at a higher rate with user access audit trails of every identity in your agency or organization.
- Strengthen compliance controls by ensuring compliance with automated certification and access reviews.
- Accelerate compliance decision making with contextual user access insights.

Mitigate Risk and Reduce Costs

- Leverage AI-driven security insights and machine learning algorithms to evolve user access policies and remediation.
- Automate high-confidence access to eliminate unnecessary requests, reviews, certifications, and approvals.
- Decrease operational costs by eliminating manual bulk approvals and certification rubber stamping.