ForgeRock

WHITE PAPER

Maximize the Value of Government Identity Solutions with AI-Driven Identity Analytics

Introduction

With the size, number, and frequency of data breaches increasing year over year, pressures caused by external security threats have never been greater. At the same time, the number of identities and volume of activities requiring access, compounded by the uptick in remote working, are expanding at a rapid cadence, increasing the internal threat surface. Many factors are driving this security threat expansion, including new identity types, such as Internet of Things (IoT), Operational Technology (OT), and mobile, among others, as well as the move to cloud and hybrid-based applications.

As external and insider cyberthreats become a bigger challenge for government agencies and organizations, the scope of identity management has grown in response. These threats make securing identities and access more important than ever before. As a result, the regulatory and compliance landscape is becoming ever more complex and rigorous, with a multitude of regulations, such as Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Federal Information Security Management Act (FISMA), and others. Legacy identity and access management (IAM) and identity governance and administration (IGA) solutions (a subset of IAM) are not equipped to handle these growing challenges and requirements at scale.

As the external and internal threat landscape converges with ever-growing identity volumes, the field of identity analytics is maturing to address this development. An identity analytics solution that uses artificial intelligence (AI) and machine learning (ML) empowers government agencies and organizations to analyze large data volumes and activity levels at high speeds.

AI-driven analytics enables the detection of low-, medium-, and high-risk user access patterns across the entire enterprise. It can also automate high-confidence and low-risk decisions, leaving more time and resources for nuanced high-risk decision making by risk and security teams. This maximizes resources and reduces user access errors and security fatigue. By overlaying and integrating identity analytics on existing identity management and governance solutions, government agencies and organizations can dramatically increase the efficacy and value of their IAM and IGA investments.

This white paper discusses the evolving nature of external and internal cyberthreats, as well as the shortcomings of legacy IAM and IGA processes and solutions. It also describes how ForgeRock's AI-driven Autonomous Identity solution provides real-time, continuous user access visibility, control, and remediation across government agencies and organizations.

What Is Artificial Intelligence?

Artificial intelligence, or AI, is the field of computer science dedicated to solving cognitive problems commonly associated with human intelligence, such as learning, problem solving, and pattern recognition. AI systems make decisions that normally require a human level of expertise. These decisions have three common qualities: intentionality, intelligence, and adaptability.[1]

What Is Machine Learning?

Machine learning is one of several methods used in artificial intelligence. It's the process of teaching a computer system how to make accurate predictions when fed data. The key difference from traditional computer software is that a human developer does not write code to instruct the system. A machine-learning model is trained on a large amount of data, either supervised or unsupervised. Supervised learning exposes systems to large volumes of labeled data to learn from, while unsupervised or semi-supervised learning tasks algorithms with identifying patterns in data without human feedback or assistance.[2]

Identity Threats Continue to Rise

According to the 2020 ForgeRock Consumer Identity Breach Report, the number, size, and cadence of external breaches, compromised data, and targets have increased exponentially in recent years. In parallel, the costs and time required to protect government agencies and organizations from these threats are also on the rise.

A few years ago, a breach that compromised the data of several hundred thousand people would have been big news. Now, breaches are measured in the hundreds of millions, or even billions, of people impacted.

The Internal Threat Surface Is Expanding

The internal threat surface is expanding almost as quickly as the scope of external threats. The number of identities and activities government agencies and organizations have to manage and protect has ballooned to an estimated 3.2 billion[9] identities globally. New types of identities are springing up, including consumer, IoT, OT, and mobile. New drivers are also emerging, including requirements for business continuity and resiliency, distributed workforces, and more teams working remotely than ever before. Combined with individual units integrating with cloud applications and cloud providers, the net results are unprecedented interdependencies and vulnerabilities.

All the factors listed above increase the risk of accidental exposure. It is estimated that 62%[10] of breaches not involving an error, misuse, or physical action were triggered by the use of stolen credentials, brute-force attacks, or phishing. In addition, security teams are continually on the lookout for employee data exfiltration, third-party credential theft, unauthorized employee access, and nation-state spies.

The increasing reliance on multiple cloud platform providers like Amazon Web Services (AWS), Google Cloud Services (GCS), and Microsoft Azure can also result in various vulnerabilities. The interdependencies that result when implementing authentication, access controls, and user management across cloud providers can make it easy for things to fall through the cracks. For example, a team managing multiple providers may forget to change the default administrative username and password for one or more cloud environments.

These vulnerabilities are particularly troubling in the face of statistics that show that many government agencies and organizations are overprovisioning employee access to applications, files, and folders.

- In a 2019 survey, data security company Varonis found that, on average, every employee had access to 17 million files and 1.21 million folders.[11]
- In the same survey, 58% of companies found more than 1,000 folders with the same permissions.[12]
- In 2019, unauthorized access was the most common type of breach, 40%, up from 34% in 2018.[13]

This increase in unauthorized access attacks showcases the need for government agencies and organizations to employ a more sophisticated identity solution to prevent nefarious agents from accessing sensitive data.

Quantifying the Cost of Breaches

Due to the increase in both internal and external vulnerabilities and attacks, new compliance regulations, such as the California Consumer Privacy Act (CCPA), are being added to the long list of existing regulations, including HIPAA, GDPR, and FISMA – among many others – to ensure that user data is protected. This is why IAM programs, and specifically IGA, are more important than ever before in today's dynamically changing organizations. Combined with the explosive growth of digital identities, aggressive adoption of cloud-based applications, and increasing regulatory requirements, legacy identity solutions are crumbling under the pressure.

Legacy Identity Management Solutions Fall Short

Most government agencies and organizations have legacy IAM and IGA solutions in place to manage user access and to ensure compliance and data protection. In light of external security pressures and exploding volumes of new identity types, these solutions can't scale to provide a comprehensive, integrated view across the agency or organization. They are also unable to provide contextual analytics for multiple identity data sources.

Identity Silos

To effectively mitigate risk and protect data, government agencies and organizations need a comprehensive view of all user access. Whether on-premises or cloud-based, legacy identity solutions are siloed and likely do not connect to all applications. The result is a lack of agency and organization-wide user access visibility, awareness of high-risk activity, and the inability to recommend appropriate access privileges, like entitlement and role assignments. With no contextual perspective, government agencies and organizations end up with siloed visibility of rapidly growing identity populations (for example, employees, contractors, warfighters, and citizens). The problem is amplified when information is spread across both on-premises and cloud-based environments.

This context is particularly critical for maintaining compliance in a complex regulatory landscape. Security and compliance teams are required to manage and govern identity and access by those standards, but it's impossible to be compliant without complete visibility. A truly effective solution should provide crystal-clear awareness and context of who has access to which applications, how they obtained that access, and what they're doing with that access. Government agencies and organizations must be able to assess risk to protect vital corporate information assets, including personally identifiable information (PII), confidential data, and intellectual property.

ForgeRock Autonomous Identity
Customer Successes

91%

A multinational financial services organization identified and automated 91% of entitlement assignments to a major ERP application.[15]

550K

A major US healthcare service provider identified 550K entitlement assignments as candidates for automated clean-up.[15]

70%

A multinational consumer and packaged goods provider identified a 70% reduction of required roles across the organization.[15]

Operational Inefficiency

In the face of increasing risks, identity volumes, and compliance mandates, government agencies and organizations need to achieve as much operational efficiency as possible. This means that automating and streamlining access requests, approvals, and request fulfilment should be done in a consistent manner. It's difficult to achieve this with tens of millions of access privileges spread across dispersed systems, applications, and environments.

Inefficiencies like these reduce productivity and result in suboptimal business decisions. Most access request approvers have no choice but to manually approve or rubber stamp access requests and certifications without fully described access rights. This unintentionally leads to overprovisioning or granting inappropriate access privileges. While the sheer volume of requests can be overwhelming, this runs counter to the "least privileged access" security approach many agencies and organizations seek to embrace.

Difficult to Integrate

With the ever-increasing volume of identities, it's a challenge to integrate legacy identity solutions with multiple applications and processes. From an architecture perspective, monolithic legacy solutions are inherently complex, which makes integration with applications a daunting and highly resource-intensive task. As a result, these identity solutions are only integrated with a subset of key business applications across the agency or organization. When combined with increasing security and compliance resources needed to manage these legacy solutions, the consequence is massive operational overhead. And, without the ability to collect identity data across all applications organization-wide, it's nearly impossible to get an accurate picture of the entire identity risk landscape.

Traditional Identity Governance Solutions Are Not the Answer

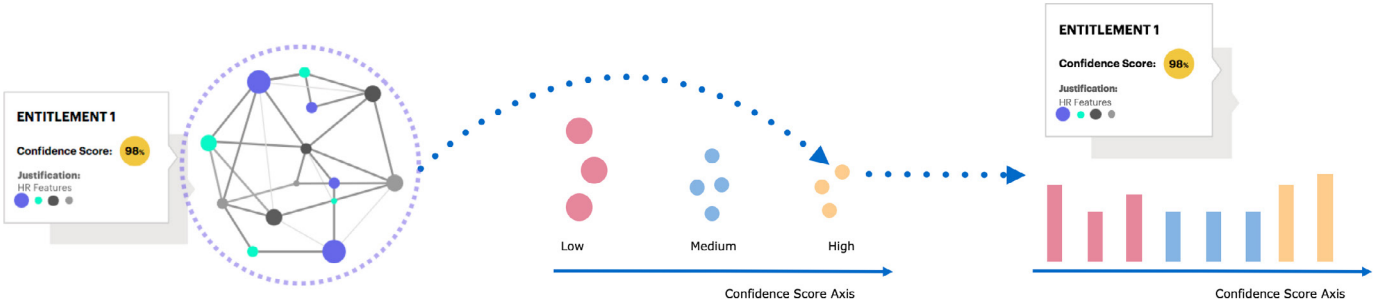
IGA is needed now more than ever before due to increased IT complexity and the increasing risks of data and privacy breaches. It remains an essential ingredient for comprehensive enterprise IAM programs, as it helps maintain compliance, provides data protection benefits, and enables user lifecycle management across the entire agency or organization. However, traditional approaches to IGA have fallen short.

Typically, only a limited number of enterprise applications are integrated into IGA solutions. Consequently, most government agencies and organizations lack enterprise-wide user access visibility, high-risk risk awareness, and the ability to recommend appropriate access privileges, such as entitlement and role assignments. Another reason first-generation IGA solutions provide diminishing value is implementation complexity and the need for heavy customization, which require a heavy investment in staffing and budgetary resources. Because of these limitations, government agencies and organizations are starting to replace their legacy IGA solutions with more modern solutions that require minimal customization and are primarily configuration driven. Agencies and organizations on a fast-track digital transformation path are looking for solutions with 80% coverage at 20% of cost – something that traditional IGA solutions cannot provide.

A Modern Approach: AI-Driven Identity Analytics

Legacy identity and governance solutions can be augmented by AI-driven identity analytics to help scale and streamline access-related operations and clean up inappropriate access privileges. ForgeRock Autonomous Identity provides sophisticated AI-driven identity analytics that can be overlayed onto legacy identity solutions, enabling organizations to automate and accelerate decisions and maximize existing investments.

How It Works



1

All identity data, such as attributes, entitlements, roles, are consumed, analyzed, and modeled across the enterprise.

2

All confidence scores are calculated and distributed in low, medium, and high-risk user access levels.

3

Each confidence score can be reviewed and analyzed individually or displayed by distribution and justification.

How ForgeRock Autonomous Identity Addresses Legacy IAM Challenges

Legacy IAM Challenge	ForgeRock Autonomous Identity
Identity silos	Contextual, enterprise-wide visibility
Legacy IAM solutions present a siloed view of identities and their associated access and permissions. This is because so many different identity, governance, and infrastructure platforms are deployed within government agencies and organizations, Each solution contains a subset of identities (for example, employees, contractors, and citizens), resulting in blind spots with respect to user access risks.	ForgeRock Autonomous Identity collects and analyzes identity data from identity, governance, and infrastructure platforms to gain agency or organization-wide visibility of all identities and their access. This provides security and compliance teams with contextual insight into low-, medium-, and high-risk user access at scale.

Legacy IAM Challenge	ForgeRock Autonomous Identity
Access blind spots	Access risk awareness
To develop a view of all identities, government agencies and organizations either purchase off-the-shelf IGA and IAM solutions or develop them internally. Internal solutions are typically built on storage repositories that store structured and unstructured data in data lakes. Data is static, and these solutions don't offer predictive insights into risk.	ForgeRock Autonomous Identity leverages AI and ML techniques to proactively analyze all identity data and to contextually identify user access and entitlement risk across the entire agency or organization. It quickly identifies and alerts security and compliance teams about high-risk use access and privileged and root account access violations.

Legacy IAM Challenge	ForgeRock Autonomous Identity
Inappropriate user access	Access rights identification
With the explosion of digital identities, most government agencies and organizations are drowning in user access requests, entitlement creep, and access certifications. To keep up with the pace of user access requests, teams manually approve and or rubber-stamp access certifications in bulk. The resulting overprovisioned user access rights increase enterprise risk and vulnerability.	ForgeRock Autonomous Identity automatically examines all identity-related data across the agency or organization, easing the manual burden on security and compliance teams. By analyzing and quickly identifying appropriate user access rights, government agencies and organizations can proactively identify and rectify overprovisioned users, recommend remediation, and automate removal when appropriate.

Legacy IAM Challenge	ForgeRock Autonomous Identity
Inappropriate access privilege patterns	Enterprise-wide access insights
In order to determine if a user should have access to a system, application, or environment with a traditional IAM and IGA solution, security and compliance teams have to manually analyze and review large volumes of identity data. With data growing exponentially, it is not humanly possible to effectively identify inappropriate access privilege patterns across the entire enterprise.	By continuously ingesting new identity data, ForgeRock Autonomous Identity constantly evolves its ML model to understand dynamic changes within an agency or organization. This enables it to predict and identify outliers, including inappropriate access privilege patterns. The intelligence-based approach allows security and risk teams to automatically analyze and model large volumes of identity data, identifying high-risk and unauthorized user access across the entire agency or organization.

Legacy IAM Challenge	ForgeRock Autonomous Identity
Manually remediated user access	Automated user access remediation
It is extremely time-consuming to manually create, review, and approve/remove user access in traditional IGA and IAM solutions. If inappropriate user access is manually identified, security and compliance teams have to manually remediate this access across multiple systems, applications, and environments – both on premises and in the cloud. This requires a great deal of time, effort, and resources to execute and confirm, leaving the agency or organization vulnerable in the meantime.	ForgeRock Autonomous Identity enables the automatic approval and certification of high-confidence, low-risk access requests, as well as automatic revocation of stale user access rights and user removal. This AI-driven analysis reduces operational access request burdens and accelerates certification campaigns across the organization without exposing the agency or organization to unnecessary risk.

Embracing AI-Driven Identity Analytics With ForgeRock

ForgeRock Autonomous Identity Benefits

Contextual Organization-wide Risk Visibility

- Quickly understand agency and organizational user access risk posture
- Get contextual awareness to who has access to what and why
- Continuously identify and monitor high-risk access
- Leverage a single source of truth

Improves Operational Efficiency

- Automated user access risk visibility and reporting
- Automated AI-driven user access risk analysis
- Allows productivity shift, focus on and address higher priority tasks
- Reduces manual access approvals and certifications

Accelerates Decision Making

- Empowers decision makers to allow/ remove user access based on risk
- Take-action based on confidence scores, not static roles and entitlements
- Immediate decision making based on user access data

Future-Ready

- Accelerates new employee/ user access by making recommendations based on confidence scores
- Quicker user provision decision making based on higher confidence
- Saves approvers and certifiers time by automatically approving highly confident scored access requests and certifications

With external cyber threats growing at an unprecedented rate and constant internal challenges, security and risk professionals need to work smarter – not harder – to effectively protect their government agency or organization at scale. Legacy identity and governance solutions and processes need to be enhanced. This can be achieved by proactively embracing an AI-driven identity analytics solution.

The ForgeRock Autonomous Identity solution allows you to integrate identity analytics on top of your legacy IAM and IGA investments. With the solution's actionable information powered by AI and machine learning, government agencies and organizations can meet compliance standards with confidence. They can also quickly and efficiently achieve least privileged access and get a continually refreshed enterprise view of user access rights. Maximizing your current IAM and IGA investments with ForgeRock Autonomous Identity provides contextual organization-wide risk visibility, improves operational efficiencies, and accelerates your security posture in our accelerating digital world.

Learn More about ForgeRock Autonomous Identity

Visit our website for more information on ForgeRock Autonomous Identity or contact us today to start your AI-driven identity analytics journey.

Endnotes

1 https://www.brookings.edu/research/what-is-artificial-intelligence/

2 https://www.zdnet.com/article/what-is-machine-learning-everything-you-need-to-know/

3 https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/

4 https://gizmodo.com/885-million-sensitive-records-leaked-online-bank-trans-1835016235

5 https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1

6 Cost estimated using total identified breaches with Ponemon Institute findings for the cost of a U.S. security breach, as reported in the "Cost of a Data Breach Report 2019"

7 https://www.forgerock.com/resources/2020-consumer-identity-breach-report

8 Ibid.

9 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

10 https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

11 https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

12 https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

13 https://www.forgerock.com/resources/2020-consumer-identity-breach-report

14 https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

15 ForgeRock Autonomous Identity customer success report 2020