ForgeRock

WHITE PAPER

SELF-DRIVING GOVERANCE

AI-Driven Identity for Financial Services

Table of Contents

Executive Summary

Decision-makers in the financial services sector agree: we are living in exciting and challenging times. Across the industry, organizations are moving quickly to replace manual processes, increase automation, and harness vast amounts of data in order to improve efficiencies. New applications are coming online at breakneck speed and cloud applications are being adopted aggressively: some 94% of businesses already use some type of cloud services.[1] Each technology requires a clear identification of which users need access to it, what resources they need, and how access can be controlled to prevent unauthorized usage.

Financial services organizations have long used identity governance and administration (IGA) solutions to address user provisioning and regulatory compliance requirements. These solutions are designed to automate access requests, approvals, and certification reviews. Today, the sheer number of such requests outstrips the capabilities of many traditional IGA solutions, creating extensive complexity and identity governance fatigue.

As a result, financial services organizations can no longer adequately constrain access to sensitive data, files, and information, thereby exposing themselves to unauthorized access. Industry research conducted across banking, insurance, and investment segments shows that an average employee has access to more than 11 million files.[2] Meanwhile, the 2021 ForgeRock Consumer Breach Report[3] shows that unauthorized access accounted for a staggering 43% of all breaches in 2020. Relying on outdated IGA solutions that fail to mitigate this risk is no longer an option.

Automation can help to mitigate unauthorized access and overcome identity governance fatigue. A solution that leverages artificial intelligence (AI) and machine learning (ML) can correlate and analyze massive amounts of data, spot anomalous behavior, recommend access, and hyper-automate existing IGA processes so that business processes become self-driving.

ForgeRock Autonomous Identity is the industry's first AI-powered digital identity analytics solution. It provides complete enterprise-wide visibility into the access landscape, incorporating data from a vast array of sources and utilizing AI transparently to provide contextual insights, guidance, and automated remediation. Autonomous Identity enables self-driving identity governance through hyper-automation to integrate identity silos and automate and augment identity governance.

The results speak for themselves: one major multinational financial services organization leveraged ForgeRock to drive an 80% click-rate reduction in access certifications to improve user experience, while strengthening security with a 20x increase in revocation rates. ForgeRock Autonomous Identity is proven to help financial service providers achieve regulatory compliance, mitigate risks, and reduce costs.

11 Million

Number of files accessible to an average financial services worker.

Challenges Facing Today's Financial Services Organizations

The Identity Explosion

Multiple technology and industry trends contribute to the proliferation of identities whose access needs to be managed: digital transformation; the exponential growth in applications; the proliferation of DevOps identities; the use of robotic, machine, and device identities; and outsourcing to third parties. It doesn't take long before an organization realizes it faces a real problem managing so many identities, roles, and entitlements. This "identity explosion" problem places a huge burden on security and risk teams, with the need to ensure that each identity has only the access rights and privileges it needs. Without enterprise-wide visibility of the identity landscape or context around access requests and certifications, teams often find themselves overwhelmed. As a result, they end up rubber-stamping access requests and certification approvals. They simply don't have the time to ensure that each request is truly necessary.

Increasing Regulatory Compliance Pressures

The task of security and risk teams becomes even more difficult in the face of a patchwork of government and industry regulations[4], such as FISMA[5], SOX[6], and CCPA[7] in the U.S., GDPR[8], PSD2[9] in the European Union, and CDR[10] and others in the Asia-Pacific region. Designed to protect against insider and external cyberthreats that could result in data breaches, these regulations generally call for restricting access rights to those minimally necessary to perform job functions — the principle of "least privilege."

The explosion of identities makes it even more difficult to ensure least privilege, especially today when many employees work remotely, often using personal devices with lax security measures. The cost of compliance can be steep: the GDPR, which applies to organizations outside as well as within the EU, costs the average Fortune 500 company $16 million a year.[11]

Penalties for regulatory noncompliance are equally impactful. At a time when businesses face mounting cost pressures, a weak understanding of users' access and justification for why they need it can prove costly. These market drivers present a unique set of business challenges for security and IT professionals. Their activities have grown exponentially as they deal with the vast volume of data generated by digital transformation, as well as the identity issues relating to multiple applications and the explosion of identities, roles, and entitlements. Further complicating matters is the increasing difficulty of ensuring continuous regulatory compliance. Unfortunately, growth in security and risk teams' resources and budgets is not keeping pace. This places an enormous burden on the teams tasked to do more with less while ensuring identity governance and compliance.

Identity Governance Fatigue

Security and IT professionals have long used IGA solutions to address user provisioning and regulatory compliance requirements. Such solutions were designed to automate access requests, approvals, and certification reviews. Today, the sheer number of such requests outstrips the capabilities of many traditional IGA solutions. Teams that face a seemingly impossible task invariably end up suffering from identity governance fatigue. They are called on to quickly make informed identity access decisions where a mistake could have serious consequences for the organization. The reasons for this are fourfold.

First, existing IGA processes and solutions are slow and cumbersome.

Older systems are primarily human-driven, putting the burden of approving access requests and certifications on the shoulders of security and risk teams. These systems, often decades-old, can't keep pace as employees take on multiple roles, change groups, and add responsibilities throughout the course of their employment. With too many reviews to tackle, security professionals resort to rubber-stamping access requests and certifications. This inevitably leads to entitlement creep, where employees gradually acquire additional — perhaps unwarranted — permissions over time.

As a result, they may have over privileged access to systems, applications, and sensitive information. Industry research shows that nearly two-thirds of organizations in the banking, insurance, and investment sectors allow an employee to access over 1,000 files, on average.[12]

Second, many IGA solutions operate as islands of identity, role assignments, and entitlements.

Once simple solutions, they are now required to work across multiple siloed environments, legacy applications, and cloud services. They are often integrated with one or just a few authoritative identity sources and are thus unable to provide a consistent view of access across the entire enterprise. Security and IT professionals are left to manually correlate and coordinate separate data stores. In other words, the teams must address this operational inefficiency through brute-force methods, greatly increasing their workload. Of course, such an approach can't scale and wears down the teams.

Third, existing IGA solutions fail to provide context around identities, entitlements, or the reasons behind access decisions.

Without context, it is impossible to determine whether overall access is in line with requirements or is excessive, whether entitlements are needed or are even being used. Traditional IGA solutions rarely, if ever, provide any transparency into who has access to what and why. Beyond a failure to provide context, they don't empower teams with actionable data.

Fourth, most legacy identity governance solutions are based on fixed identity sets and data sources, with static rules, roles, and peer group-based predictive analysis.

This leads to stale roles, assignments, and entitlements. In a world where employees, partners, contractors, and others come and go, change jobs, or are given new assignments, static rules and roles are woefully inadequate in ensuring they have access only to what they need.

Identity governance fatigue, like physical fatigue, leads to inefficiency, slowed response and suboptimal decision-making — which leads to mistakes. It's no wonder organizations are looking to automate identity governance solutions to combat identity governance fatigue.

Why Are Identity Governance Solutions Falling Short?

IGA Processes and Solutions are **Slow, Cumbersome**

IGA Solutions operate as **Identity Silos**

IGA Solutions provide **No Context**

IGA Solutions are based on **Static Rules and Roles**

Automation Overcomes Identity Governance Fatigue

Identity and risk professionals in the financial services industry experiencing identity governance fatigue are dealing with an overwhelming number of identities, roles, and entitlements. They are also facing the proliferation of machine and Internet of Things (IoT) identities, the demands of organizational changes, and the added impact of unplanned events, such as the pandemic with its dramatic increase in remote working. New automated, self-driving approaches are needed to replace antiquated manual efforts. Automated identity governance is the optimal solution, and also provides an ideal domain to achieve the potential benefits of automated intelligence and machine learning.

Automation streamlines intelligence, making sense of the mountain of uncorrelated data that is being created daily. It spots anomalous behavior before it represents a threat and enables solutions to proactively identify access risks and highlight excessive privileges. Artificial intelligence (AI) is used to make informed recommendations that can be communicated to decision makers. An ideal IGA automation solution does not stop there. It goes on to automatically implement the recommendations, freeing up security teams to focus on more complex tasks, such as investigating high-level threats that require their skilled intervention. Automation can even dramatically simplify the process of recommending low-risk accounts for certification and re-certifying high-risk accounts: a solution based on AI will enable smarter, more efficient certification campaigns with fully described access rights.

Artificial Intelligence: The Key to Self-Driving Governance

AI based on machine learning (ML) is the ideal foundation for automating identity governance. When AI is supplied with rich data representing an enterprise-wide view of all aspects of identity, it can streamline and automate intelligence across all IGA use cases: access requests, access reviews, and role mining. Rather than forcing analysts to manually correlate masses of data, AI can proactively identify access risks and provide context for quicker decision-making. In addition, AI can accurately identify excessive privileges and provide confidence scoring that teams can use when making actionable decisions.

Identity governance fatigue, like physical fatigue, leads to inefficiency, slowed response and suboptimal decision-making – which leads to mistakes. It's no wonder organizations are looking to automate identity governance solutions to combat identity governance fatigue.

One of the most important benefits of using AI- and ML-based solutions is the ability to hyper-automate existing IGA processes. Defined by Gartner as tools to "...integrate functional and process silos to automate and augment business processes,"[13] hyper-automation goes beyond simply providing information to decision-makers. It can discover, monitor, and improve user access, enabling business processes to become self-driving.

Hyper-automation goes beyond simply providing information to decision-makers. It can discover, monitor, and improve user access, enabling business processes to become self-driving.

ForgeRock Approach to Self-Driving Governance

ForgeRock delivers the industry's first AI-powered digital identity analytics solution, harnessing hyper-automation to pave the way for self-driving IGA. ForgeRock Autonomous Identity provides complete enterprise-wide visibility into the access landscape, utilizing AI transparently to provide insight, guidance, and automated remediation. As a complementary solution to existing IGA tools, it helps organizations achieve regulatory compliance, mitigate risks, and reduce costs.

ForgeRock Autonomous Identity uses AI and ML techniques to collect and analyze all identity data from the business. It collects data from identity and access management systems and other relevant sources of data to identify access and risk blind spots. This ensures a comprehensive real-time view of identity across the entire organization.

Armed with this user access landscape view and a thorough understanding of the principles behind each type of access, the ForgeRock solution looks at how closely the characteristics of a user with a given entitlement match the characteristics of others with the same access. The closer the match, the greater the confidence that this user is justified in being given this specific access.

Autonomous Identity assigns a confidence level for each individual who is provided such access, determining what both good and bad access look like across the entire enterprise. Similarly, it can recommend relevant high-confidence access rights that have not yet been granted to employees.

Importantly, the solution does not force financial services organizations to replace their existing IGA solutions. Instead, it coexists with IGA solutions to augment and maximize the business value of identity investments already made. This breakthrough approach helps CISOs take identity governance to the next level, while maximizing ROI on existing investments and accelerating time to value.

This breakthrough approach helps CISOs take identity governance to the next level, while maximizing previous investments and preserving their budgets.

What Business Outcomes Look Like with Autonomous Identity

The results of self-driving governance are seen in real-world customer experiences. While these business outcomes are focused solely on the automation savings in the first year, it is important to understand that ongoing savings are equally impressive. Removing duplicate access, achieving new levels of process automation, and reducing workload can save organizations massive direct costs and improve productivity.

Customer	 **A Multinational Financial Services Organization**	 **A Global Consumer Packages Good Provider**	 **A Major US Pharmacy Health Care Provider**
Benefits	**91%** Autonomous Identity identified the automated clean up of entitlement assignment for a major ERP application	**70%** Autonomous Identity identified a reduction of required roles across the organization	**550K** Autonomous Identity identified the automated clean up of entitlement assignments across the organization
Scope	**10** Applications **2,370** Entitlements **6,800** Users & Objects **1.1 Million** Assignments	ERP & Active Directory **41K** Entitlements **66K** Users & Objects **1.2 Million** Assignments	**87K** Employee Records **11K** Applications **408K** Entitlements **14.6 Million** Assignments

Why ForgeRock Autonomous Identity?

ForgeRock Autonomous Identity has been architected to address all the major issues related to identity governance in the financial services industry. It also goes a step further to enable self-driving identity governance through hyper-automation. The solution is built on three unique concepts: providing global visibility, being data-agnostic and ensuring transparent AI.

Global Visibility

By leveraging AI-driven identity analytics, financial services organizations can collect and analyze all identity data (examples: accounts, roles, assignments, entitlements, and more) from diverse identity, governance, and infrastructure solutions. Autonomous Identity brings all this information together to provide enterprise-wide visibility to all identities and what they have access to, across the entire organization. In addition to enterprise-wide visibility, Autonomous Identity provides security and risk professionals in the industry with contextual insights into low-, medium-, and high-risk user access at scale.

Data Agnostic

Autonomous Identity, unlike "black box" identity analytics solutions based on static rules, roles, and peer group analysis, relies strictly on organizational data to develop a bias-free analysis. The solution works with existing identity data sources and all identity data types to develop a complete view of the user access landscape. In addition to IGA data, Autonomous Identity collects, normalizes, and analyzes identity data from any disparate data sources. By consuming and analyzing tens of millions of data points quickly, Autonomous Identity can predict and recommend user access rights and highlight potential risks.

Transparent AI

ForgeRock solutions are based on full transparency, providing teams with a deep understanding of how and why risk confidence scores have been determined. The visual presentation of low-, medium- and high-risk confidence scores explains the decisions via key risk indicators that were met, demonstrating the logic behind the decisions, and showing the criteria that went into the decision. It is through this explainable user interface (UI) that allows security and risk professionals to make quicker decisions based on actionable data.

Autonomous Identity, unlike "black box" identity analytics solutions based on static rules, roles, and peer group analysis, relies strictly on organizational data to develop a bias-free analysis.

How Autonomous Identity Fits Into Your Organization

Autonomous Identity works in conjunction with existing identity investments. The solution can provide immediate and continuous ongoing insights into the optimal state of user access for an organization's security and compliance needs (see figure 1).

Autonomous Identity consumes and analyzes tens of millions of data points from existing identity data sources, including Active Directory, LDAP, databases, and more. Based on the identity data collected, it develops a complete view of the user access landscape and highlights underlying risks to eliminate blind spots while providing context. With highly accurate models of what good access should and shouldn't look like, it predicts and recommends actions regarding optimal user access rights.

Because it relies strictly on organizational identity data to develop its analysis, Autonomous Identity is free from any bias that could come from human-derived static rules, roles, or peer group analysis. Security and risk professionals can view confidence levels — low, medium, and high — that relate to user access. AI and ML techniques provide contextual insights into how and why risk confidence scores are determined.

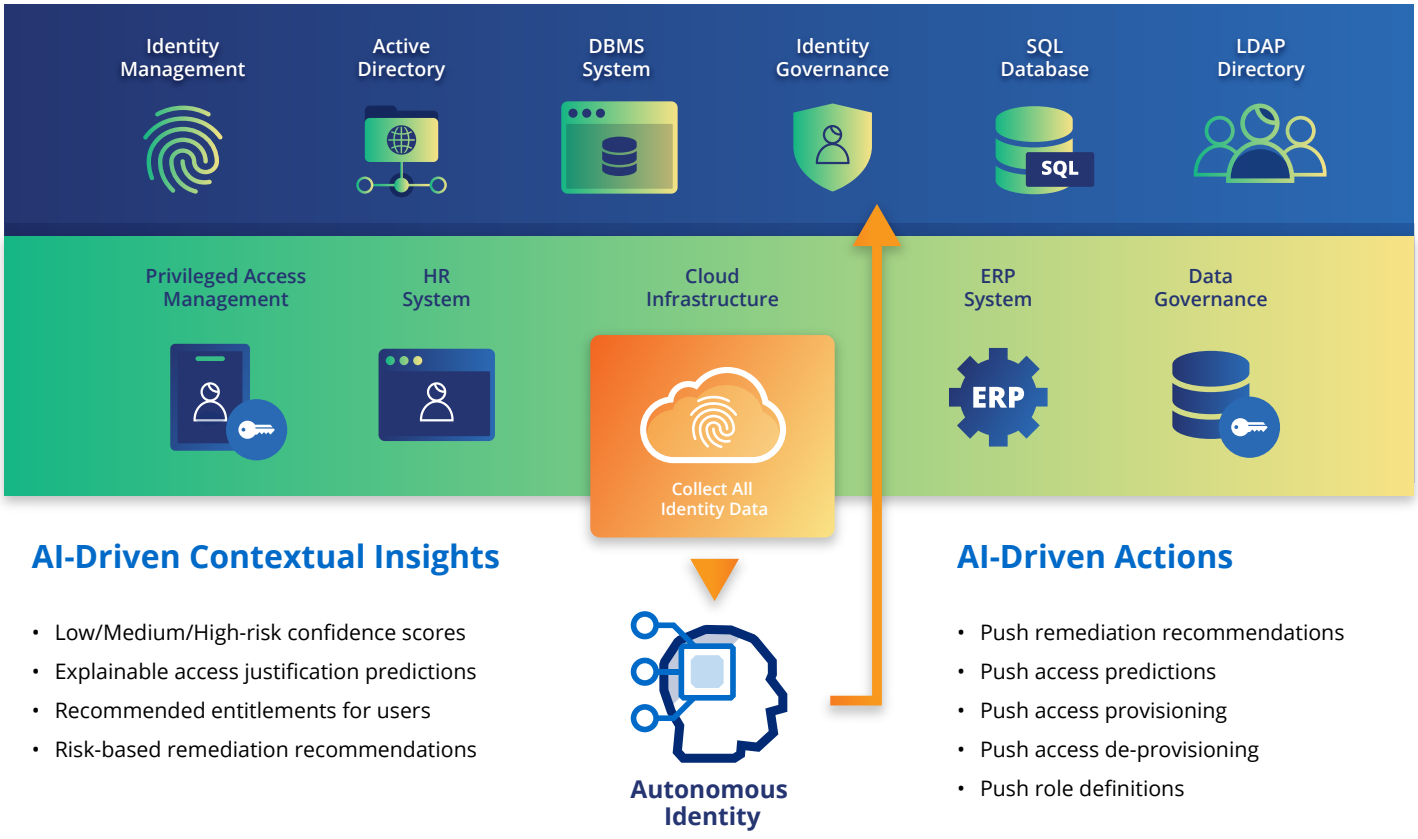


Figure 1: How Autonomous Identity Fits Into Your Organization

Autonomous Identity presents these confidence scores visually (see figure 2), so security and risk professionals can contextually understand what key risk indicators were met. They can zoom in on critical entitlements, seeing the details of the selected entitlement, along with which employees have access to it. This AI-driven approach recommends remediation based on confidence scores that take into consideration access enterprise-wide, not just from the point of view of a traditional identity silo.

This AI-driven approach recommends remediation based on confidence scores that take into consideration access enterprise-wide, not just from the point of view of a traditional identity silo.

Clear visual presentation of information is important, but Autonomous Identity goes beyond showing security and risk professionals a broad view of organizational access and risk. It provides the means for organizations to automatically take action on — or hyper-automate — their existing identity governance processes, as well as their IGA solutions. By automating tasks such as access requests and certifications, Autonomous Identity saves time and cost for the teams and the organization. Because it works hand in hand with existing identity governance solutions, it enables your organization to augment the business value of these investments.

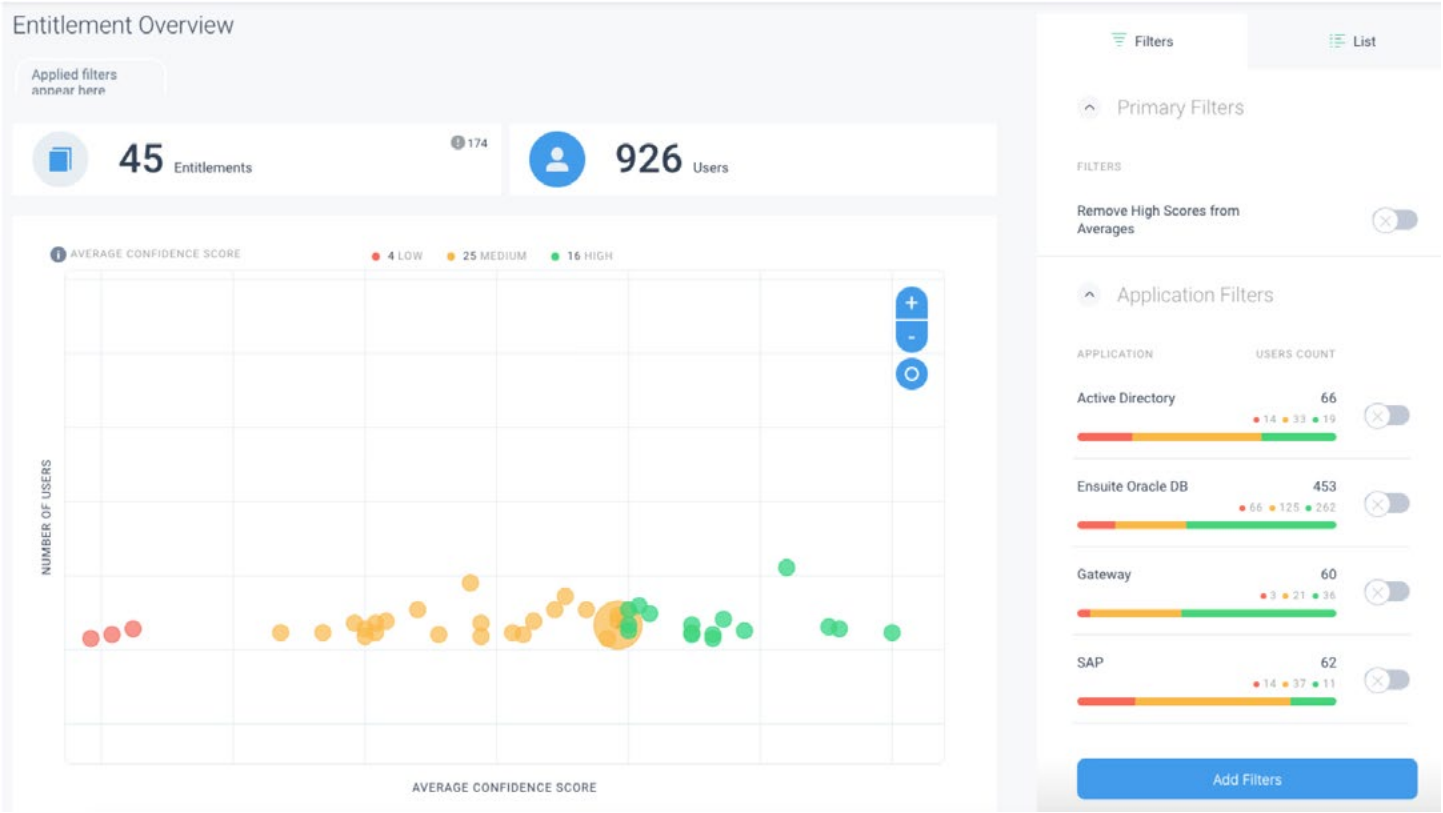


Figure 2. Autonomous Identity Explainable UI.

How ForgeRock Autonomous Identity Works

Step 1

Autonomous Identity starts by ingesting user data from multiple data sources, such as IAM, IGA, HR, LDAP, databases, Active Directory systems, and the like. Data — including attributes, entitlements, roles, and more — are consumed and aggregated across all data sources to develop a comprehensive user access landscape of your entire organization.

Step 2

Autonomous Identity applies AI and ML to aggregated identity data to predict entitlements for a user. Predictions are displayed and explained three ways: through confidence scores, justification, and recommended entitlements. A confidence score is generated for each existing entitlement assignment based on a degree of confidence in whether the employee should have access or not. The solution then produces a fully traceable and explainable justification of how the prediction reached the outcome. Finally, it predicts access for new users, recommending entitlements.

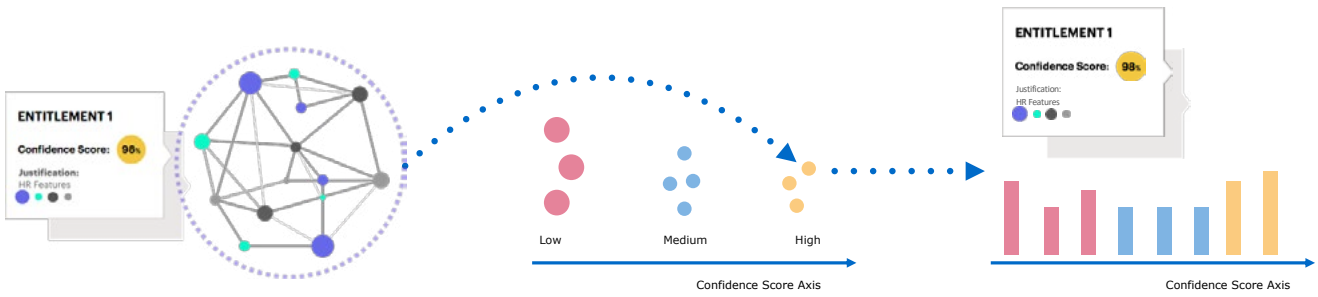
Step 3

Autonomous Identity allows security and IT professionals in the financial services industry to automatically review predictions and take actions, such as approving access requests and certifications immediately. It does this through access insights, hyper-automation, and role reduction, providing context to help security and risk teams operate more efficiently.

- **Access Insights** provides a comprehensive user access landscape across the entire enterprise. Autonomous Identity detects user access patterns and recommends the right level of user access rights. It identifies appropriate birthright user access rights to accounts, applications, systems, roles, entitlements, and more. In addition, it can highlight overprivileged access, excessive permissions, orphaned accounts, and entitlement creep.

- **Hyper-automation** eliminates the manual work of approving and certifying high-confidence, low-risk access requests. At the same time, it automatically revokes stale user access rights, user accounts and role removal. It also pushes remediation recommendations — such as access provisioning/deprovisioning and role definitions — directly back to the existing IGA solution.

- **Role Reduction** leverages AI and ML to review, evaluate, and refine roles and role models. This helps the organization create fewer but higher quality roles over time. While identifying overprivileged entitlement and role access patterns, it simultaneously and automatically removes unnecessary entitlements and roles.



Step 1
All identity data such as attributes, entitlements, roles, are consumed, analyzed and modelled across the enterprise

Step 2
All confidence scores are calculated and distributed in low, medium and high-risk user access levels

Step 3
Each confidence score can be reviewed and analyzed individually or displayed by distribution and justification

Figure 3. How ForgeRock Autonomous Identity Works.

Start Down the Path to Self-Driving Governance

There's no need to wait: the future is here. Financial services organizations facing dynamic business challenges now have at their disposal a dynamic solution to meet and overcome these issues. Teams can now do more with fewer resources. They have full visibility into — and automated assistance in remediating — overprivileged access, excessive permissions, orphaned accounts, and entitlement creep.

Teams can hyper-automate existing IGA processes and solutions, streamlining and automating intelligence across all IGA use cases: access requests, access reviews, and role mining. Risks are proactively identified, and context is provided for actionable decision making. Micro-certifications enable business line managers to approve only small sets of entitlements and roles, easily closing the access gaps between annual or biennial compliance audits.

The business benefits are undeniable. Autonomous Identity, coexisting with existing IGA systems, increases their value through actionable intelligence and automated remediation. Employee productivity is enhanced, thanks to hyper-automation, with approval and certification of high-confidence, low-risk access requests, automatic revocation of stale rights, and micro-certifications. Compliance audit pass rates improve through role reduction and AI-driven remediation recommendations. Unauthorized access can be mitigated once and for all.

Take The Next Step with the Autonomous Identity 2-Week Assessment

The ForgeRock Autonomous Identity assessment is a two-week evaluation focused on demonstrating Autonomous Identity capabilities and helping you understand its potential value to your organization. The process consists of three phases that provide deep insights into risks associated with user access as well as concrete recommendations for mitigating them. Learn more about the 2-week assessment **here**.

We're Here and Ready to Help

Security and risk professionals use ForgeRock to achieve regulatory compliance, mitigate risks, and reduce costs across the entire organization. **Contact us** to learn more about how ForgeRock can help you.

[1] SG Analytics, **94% of Enterprises Already Use Some Type of Cloud Service**, September 2020.
[2] Veronis, **2021 Varonis Data Risk Report for Financial Services**.
[3] ForgeRock, **2021 ForgeRock Consumer Identity Breach Report**.
[4] Gartner, **Gartner Identifies Top 15 Risk Hot Spots for Legal and Compliance Leaders**, December 2019.
[5] **Federal Information Security Modernization Act**.
[6] **Sarbanes-Oxley Act**.
[7] **California Consumer Privacy Act**.
[8] **General Data Protection Regulation**.
[9] **Payments Services Directive 2**.
[10] **Consumer Data Right**.
[11] Forbes, **The GDPR Racket**, May 2018.
[12] Veronis, **2021 Varonis Data Risk Report for Financial Services**.
[13] Gartner, **Move Beyond RPA to Deliver Hyperautomation**, December 2019.

About ForgeRock

ForgeRock® (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit: **www.forgerock.com**.

Follow Us

ForgeRock