ForgeRock

WHITEPAPER

Boost Zero Trust In Healthcare With AI-Driven Least Privileged Access

Executive Summary

Healthcare organizations are facing a sharp uptick in identity breaches. Unauthorized access is the number one attack method (40%) cybercriminals used in 2020.[1] According to the ForgeRock 2021 Breach Report,[2] for the third year in a row, healthcare was the biggest target in terms of the number of breaches, accounting for 34% of the total. It was also the most costly at $474 per record. Additionally, the Health and Human Services HC3's Cyber Threat Intelligence (CTI) team has tracked a total of 82 ransomware incidents impacting the healthcare sector worldwide so far this calendar year, as of May 25, 2021. 48 of these ransomware incidents (or nearly 60%) impacted the United States health sector.[3]

In addition to breaches, megatrends like digital transformation, cloud adoption, and a historic rise in remote work are redefining the parameters of good identity governance and administration (IGA) in healthcare. Many new identity types (machines, devices, APIs, applications, and microservices) require advanced methods to control access. Legacy role-based access control (RBAC) relies on manual role mining and modeling. This approach fails to keep up with identities at scale in today's fluid healthcare environments, where providers, employees, and contractors frequently change jobs, roles and or organizations. The results are overprovisioned access, orphaned accounts, and entitlement creep, which notoriously escalate insider and external threats.

Modern defenses to mitigate the emerging threats and patterns advocate a Zero Trust model, including advanced access control. Moreover, increased scrutiny on healthcare organizations by various regulations like Sarbanes-Oxley (SOX),[4] Health Insurance Portability and Accountability Act (HIPAA),[5] the 21st Century Cures Act, and California Consumer Privacy Act (CCPA)[6] are also gaining ground.

The combined effect of more regulatory scrutiny, accelerated cloud adoption, remote work, and frequent,

1 2020 ForgeRock Consumer Identity Breach Report, 2020 Consumer Identity Breach Report | ForgeRock
2 2020 ForgeRock Consumer Identity Breach Report, 2020 Consumer Identity Breach Report | ForgeRock
3 https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
4 2021 Sarbanes Oxley Compliance Requirements (sarbanes-oxley-101.com)
5 Health Information Privacy | HHS.gov
6 California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General

unplanned organizational changes expand the gap between what healthcare organizations require and how RBAC is done today. Security leaders must address these business and technical implications to close the gap.

Understanding the challenges of traditional RBAC and the best practices to address them is crucial for maximizing your IGA investments. Static IGA processes with limited context and visibility must become more flexible, scalable, and dynamic. Traditional RBAC must modernize by augmenting manual role management with automation and intelligence. But how can you achieve this?

Take heart. The solution is already here. ForgeRock's Autonomous Identity provides what you need to modernize RBAC by leveraging artificial intelligence (AI) and machine learning (ML). There's no need to replace your IGA infrastructure. ForgeRock Autonomous Identity augments your existing IGA solution to improve your organization's agility and productivity. Modernizing RBAC with ForgeRock also helps you reduce operational costs, mitigate risks, seamlessly integrate Zero Trust, and ensure continuous compliance.

ForgeRock Autonomous Identity Customer Success

Customer Profile:
A major U.S. healthcare provider

14.6 million
assignments throughout the enterprise

550,000
the number of excess entitlements identified

3 hours
the time it took ForgeRock Autonomous Identity to achieve the above

Navigating the New Digital Norm

Several megatrends are shaping today's new digital normal. Organizations are moving at a breakneck pace to replace manual processes with automation and insights from data—the goal: improved efficiencies and an enhanced healthcare consumer (patient/member) experience. According to Facts & Factors Research, "the global Digital Health Market[7] was estimated at USD 84.08 Billion in 2019 and is expected to reach USD 220.94 Billion by 2026. The global Digital Health Market is expected to grow at a compound annual growth rate (CAGR) of 14.8% from 2019 to 2026."

The massive shift to remote work is another disruptive megatrend. Today, more healthcare providers, employees, and contractors work remotely than ever. According to Findstack, "The industries with the highest number of remote workers [in 2021] are healthcare (15%), technology (10%), and financial services (9%)."[8] In highly distributed work environments, urgency to ensure business continuity and resiliency contributes to an unprecedented increase in internal and external cyber threats.

To protect healthcare organizations and data in this new norm, healthcare organizations worldwide face increased regulatory scrutiny and compliance requirements. Non-compliance fines for large enterprises can hit millions of dollars.

In tandem with these pressing trends, security breaches are making headlines almost daily. The financial implications of breaches have also grown significantly. As stated above, for the third year in a row, healthcare was the biggest target in terms of the number of breaches, accounting for 34% of the total. It was also the most costly at $474 per record.[9]

In this new digital norm, healthcare organizations face a new set of challenges with identities and role management. The total number of identities organizations must manage and protect ballooned. Healthcare is not alone. Across all industries globally, attacks involving usernames and passwords increased by a staggering 450 percent from 2019 to 2020.[10] Just within the United States, the consequence was more than 1 billion compromised records.

The ever-increasing number of identity-related breaches calls for a sobering look at how IGA is done in across the healthcare industry today. Overcoming the pitfalls of traditional identity governance and role management solutions is crucial to protect your organization from costly breaches in this new digital norm. Now, it is more important than ever to replace static IGA processes having limited context and visibility with a more flexible, scalable, and dynamic approach to IGA, including role management. This transition can enable organizations to overcome the identity quandary.

7 https://www.fnfresearch.com/digital-health-market
8 https://findstack.com/remote-work-statistics/
9 Remote Work Statistics That You Need to Know in 2021 (oberlo.com)
10 2021 ForgeRock Consumer Identity Breach Report | ForgeRock

Healthcare's Identity Quandary

Modern healthcare organizations need to move fast. Your workforce wants quick and easy access to apps, tools, and platforms. Providers, employees, and contractors change teams, and teams form and reorganize. When workforce individuals change roles or business units, they may also need different types of access. Most organizations today struggle to keep up with these frequent changes in access requirements using a traditional approach to role management.

In the traditional model lacking an enterprise-wide view of identities, role owners often see only fragments of the complete picture, and that information is usually static, siloed, and time-boxed. It isn't easy to know who has access to what resources and why. Often, providers, employees, and contractors (workers) end up having more access rights than they need, exposing sensitive information they are not supposed to have. Excessive permissions, orphaned accounts, and outliers can quickly escalate security risks.

Each unwarranted access point is also a gap that could expose the organization to errors, compliance risks, and regulatory fines. Security breaches that hit the headlines are often due to access-related errors and lack of oversight into permissions.

RBAC's Great Promise

Decades ago, healthcare organizations embraced role-based access control (RBAC) as an advanced method for managing identities to minimize access risks. It is meant to help organizations on multiple fronts:

1. Control access to sensitive data by addressing the three primary aspects of data security:
   - Creating new provider, employee, or contractor accounts that permit access only to what they need for their jobs, such as the enterprise network, data, apps (on-premises and cloud), and cloud services
   - Maintaining accuracy and relevance of those access rights throughout the worker's tenure with the organization
   - Revoking rights promptly when the worker leaves or changes roles
2. Minimize access gaps to ensure organizations meet privacy and confidentiality regulations (e.g., SOX, HIPAA, 21st Century Cures Act, CCPA, etc.)
3. Improve regulatory compliance (e.g., pass access rights audits)
4. Prevent entitlement creep during the worker's tenure

Why Are Traditional RBAC Solutions Falling Short?

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

RBAC Solutions operate as **Identity Silos**

RBAC Solutions rely on **Rely On Manual Input**

RBAC Solutions Constantly Need **High Cost Maintenance**

One downside of traditional RBAC is the need for role owners to perform role mining and role modeling manually. For healthcare organizations, this time-consuming process could take several months. Moreover, manual role mining and modeling usually lack context since visibility to enterprise data is limited. Worse, in highly fluid business environments, the roles could become outdated by the time the RBAC process is complete, or the number of roles could even outnumber an organization's headcount. The latter nullifies the intended benefits of RBAC.

Pitfalls of Legacy RBAC Solutions

When it comes to managing access, less is more. Giving your workers more access than they need can lead to security risks and regulatory fines. The provision of access should be based on precise knowledge of the person's job role and requirements.

Legacy RBAC tools often rely on guesswork instead of unbiased, human influenced enterprise data to make this assessment. Moreover, role-based systems using a static grouping of access rights cannot keep up with the fluid nature of team composition and individual needs in modern enterprises. The inability to separate individual access rights from role-based groups can lead to overprovisioning.

Bottom line: Role owners struggle to manage access effectively using legacy RBAC tools due to numerous pitfalls explained below.

RBAC Fatigue increases risks

Global organizations expect RBAC to reduce security risks while improving operational efficiency and compliance. However, legacy RBAC technology uses a fundamentally flawed methodology for managing user identities and access permissions. The inherent weakness of this approach lies in its unwieldy administration, reliance on manual input, and constant need for maintenance. This laborious approach increases RBAC fatigue among your staff. The resulting lax increases risk leading to three pertinent role management problems.

Role Explosion

Healthcare organizations often use one RBAC model with detailed access control granularity to manage all user access. The result is an explosion in the number of roles. Role explosion makes it hard to ensure least privilege access. It gets further complicated when workers work remotely, often using personal devices with lax security measures. Role explosion is difficult and costly to manage, making access control more confusing and less effective.

Duplicate Roles

Often, providers, employees, and contractors (workers) end up having too many roles assigned to them. When they change jobs or responsibilities within the company, their roles are often duplicated. Role owners and analysts either forget about the previous roles or consciously decide to leave them in place. As a result, organizations have no idea how many duplicate roles exist. These duplicate roles can lead to security holes that are often difficult to find and plug.

Role Maintenance

When organizational structure changes, IT resources require updates, and so do the associated roles. To keep up with changes, role models need regular maintenance, reviews and updates. Traditionally, role owners do these tasks manually. Manual role maintenance is time-intensive and prone to errors. This manual role maintenance process is further compromised by the quality of underlying data used, often siloed with no enterprise-wide visibility. This fragmented, inaccurate data context severely impacts analysis. The consequences are overprovisioned access, entitlement creep, orphaned accounts, and outdated role models.

Identity silos cause risk blind spots

Legacy RBAC tools make it hard for healthcare organizations to determine what access rights users have, and more importantly, why they have them. These legacy tools integrate with a small set of data sources, such as your organization's Active Directory or Human Resource Management system. Limited integration inhibits access visibility across the entire enterprise. As a result, many little silos of identity are sprinkled across your organization. Lack of unified visibility and context across the enterprise leads to risk blind spots, inappropriate user access privileges, and chances of unauthorized user access.

Manual RBAC increases access errors

Many IGA solutions in the market promise full automation of access requests and certifications. But here's the reality. Because your security and risk teams are already overwhelmed with access requests and certification campaigns, they end up manually approving access requests and rubber-stamping certifications. Attempts to manually resolve a high volume of requests lead to errors and overprovisioned user access privileges across your entire organization. As a result, the fundamental purpose of RBAC is compromised.

Continuous compliance is hard to achieve

Current regulations require compliance not annually but continually. Although legacy role modeling helps in compliance, the downside is that it is only as effective as on the first day of implementation. After that, your organizational role model becomes stale and outdated. Reason: Your organization dynamically changes every hour, every day, every week of the year. Outdated access rights, privileges, roles, and entitlements can cause ad hoc certifications. Certifications based on stale, inaccurate data potentially jeopardize continuous compliance.

Legacy RBAC is not built to quickly adapt to changes induced by new remote work models. There is an urgent need to automate tasks with integrated visibility, insight, and context in the new digital normal.

ForgeRock's Modern Approach to RBAC

ForgeRock flips legacy RBAC thinking on its head with our Autonomous Identity solution. Manual, legacy RBAC processes are not built to manage identities and roles at scale in today's dynamic and distributed business environments. In the new digital norm, the problems role owners face in managing roles at speed and scale are akin to "finding a needle in a haystack." That's where automation powered by AI excels. ForgeRock's Autonomous Identity uses AI and ML to overcome legacy RBAC challenges.

kuppingercole ANALYSTS

"We are convinced that we will see a strong uptake of AI-based solutions in IGA and overall IAM, such as ForgeRock Autonomous Identity."

- KuppingerCole Report, January 2021

How AI-based approach resolves RBAC challenges

ForgeRock Autonomous Identity gives you complete visibility of access to information across your entire organization. The solution starts at a global level and looks at the complete landscape of identity data. It uses this enterprise-wide data as the foundation to manage role-based access.

Machine learning analyses this data to build a dynamic view of entitlements for the entire company. It uses the dynamic view to determine the correct level of entitlements for every individual in your workforce at a given point in time. The view refreshes as organizations change or providers, employees, or contractors change teams and roles.

Step 1
Identity data, such as: attributes, entitlements, roles, are consumed, analyzed and modelled across the organization

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

Step 3
Confidence scores can be reviewed and analyzed individually or displayed by distribution and justification

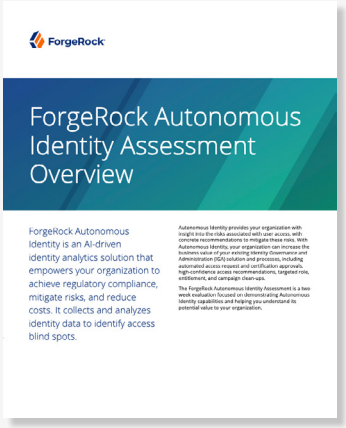
Autonomous Identity provides complete control of access throughout your organization, along with full confidence in granting access. The result is greater efficiency and accuracy in managing access. For anyone who manages access rights, this tool is transformative. Instead of blindly approving access requests, our solution empowers you with a confidence score that helps determine the provider, employee, or contractor's correct level of user access rights. If their score is high, you have peace of mind of making the right decision by granting access. If the score is low, you can avoid a potentially risky situation. What's more, the tool will give you a rationale for the confidence score, providing a reason why someone should or shouldn't have access to a particular tool, app, or platform.

Autonomous Identity serves as the single source of truth that makes the audit process faster and less painful. AI-powered RBAC makes continuous compliance seamless and outliers easier to identify.

ForgeRock Autonomous Identity Assessment

Take advantage of a two-week evaluation to assess and understand the potential value of Autonomous Identity capabilities for your organization.

For more information, go to:
[ForgeRock Autonomous Identity Assessment Guide](#).



Business Outcomes of Modernizing RBAC

Modernizing RBAC streamlines your business by transforming your organization's approach to IGA and role management. Here is an example of customer success with Autonomous Identity.

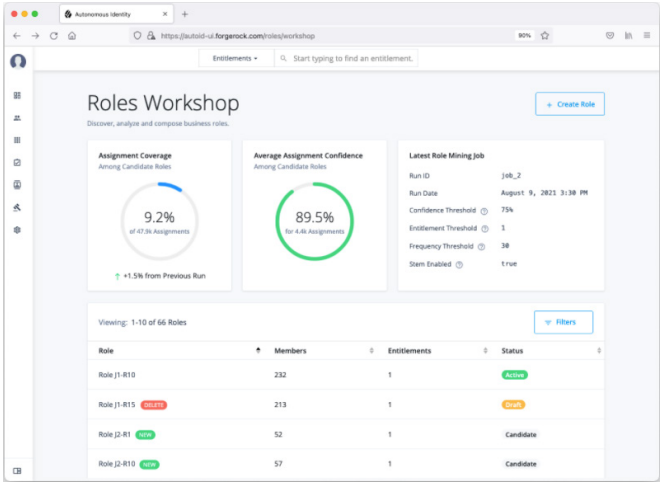
Create Efficient Rules & Roles	Reduce Risk Exposure	Lower Over-Provisioning	Quickly Identify Bad Access	Reduce Operational Costs
244K Fewer IAM Actions	**282K** Low Confidence Access	**52%** Over-Provisioned	**1.5 Months** Faster Remediation	**$850K** Back to the business
Created efficient roles that cover 15% of all access in year 1 and automated birthright user provisioning.	Discovered ~160,000 access points that are un-scorable and likely underutilized entitlements.	Identified 19% of the organization has low confidence scores and access should be removed.	Monitored drops in confidence scores to immediately trigger a certification review.	Shorten certification review and approval cycles and give time back to reviewers.

With ForgeRock Autonomous Identity, you'll always know the why behind the what. You can be fully confident in your decision-making and more accurate in your actions.

How Modern RBAC Accelerates Zero Trust

The line between internal and external is blurring in modern enterprises. Within digital health ecosystems, partners require more access to your corporate network and applications, and data increasingly shifts to the cloud, the security perimeter becomes extremely porous. As a countermeasure, more heathcare organizations are adopting a Zero Trust mindset – "trust nothing, verify everything." Zero Trust provides a dynamic game plan to implement least privilege access in today's fluid business settings.

The privacy, security, and compliance benefits of RBAC arise from the principle of least privilege. While, in principle, RBAC does allow you to verify that access is restricted to only those who need it, it is extremely difficult to achieve Zero Trust using manual RBAC processes and static data due to their aforementioned pitfalls.



AI-based RBAC is the ideal foundation for automating and achieving a Zero Trust architecture. ForgeRock's AI-powered Autonomous Identity ingests rich data representing all aspects of identity across the enterprise and streamlines and automates intelligent access across the entire organization. Autonomous Identity proactively identifies access risks rather than manually correlating masses of identity data to make access decisions. It leverages machine learning techniques to dynamically determine what roles and entitlements to approve or revoke.

With Autonomous Identity in place, healthcare organizations can effectively enforce least privilege access that restricts access to only the resources required for an employee or a contractor to do their job. Implementing AI-driven RBAC ensures that users have access to appropriate permissions and attributes. If more access is needed, it can easily be requested, granted, or even taken away. This AI-driven dynamic approach to RBAC successfully implements the "trust nothing, verify everything" model that further minimizes the attack surface from insider and external threats.

AI-driven Autonomous Identity helps healthcare organizations achieve a Zero Trust architecture with the following role capabilities:

- Discover and analyze role access patterns across the entire enterprise
- Identify high-risk roles and role combinations
- Quickly understand the composition of low-, medium-, and high-confidence roles and entitlements
- Define high-quality roles based on high-confidence access patterns
- Customize risk criteria without the need of a data scientist
- Get role recommendations and impact analysis visibility

Start down the path of achieving a Zero Trust architecture with ForgeRock Autonomous Identity by creating more efficient roles and rules, mitigating overprovisioned access, and reducing your organization's risk exposure.

Why do healthcare organizations select ForgeRock Autonomous Identity?

Global Visibility
Organization-wide user access landscape visibility

Data Agnostic
Data model reflects the entire access landscape

Transparent AI
Explainable AI of access patterns and justifications

High-Fidelity Roles
Create fewer roles to maximize access

Start on the Path to Modern RBAC

The need to modernize RBAC is imminent. In the current threat and regulatory landscape, knowing the "who, what, and why" of access is more crucial than ever. While you can perform RBAC with legacy approaches, they are time-consuming, prone to errors, and do not take advantage of data from all sources. They can't keep up with the sheer scale and speed of modern businesses either. It's time to adopt a modern approach to RBAC using advanced capabilities like AI and ML.

With ForgeRock Autonomous Identity's AI-based approach to RBAC, you can modernize how role owners review, evaluate, and administer roles and role models. You can now define high-quality roles based on role access patterns across your organization. As a result, your role management overhead reduces as well as access-related risks. Autonomous Identity leverages ML to dynamically determine what roles and entitlements to approve or revoke. This capability eliminates overprovisioned access, orphaned accounts, entitlement creep and provides an ideal foundation to integrate Zero Trust.

So why wait? Start down the path of modernizing RBAC with ForgeRock Autonomous Identity to reduce operational costs, mitigate risks, seamlessly integrate Zero Trust, and ensure continuous compliance.