Capgemini

WHY IT'S TIME FOR AI IN IDENTITY & ACCESS MANAGEMENT

Since its debut late last year, ChatGPT has captured the public imagination and demonstrated the immense potential of Machine Learning (ML) and Artificial Intelligence (AI). Many cybersecurity companies and professionals have already embraced the possibilities of AI and there are few areas of cybersecurity where AI is more welcome – and necessary - than in Identity & Access Management (IAM).

For over two decades, organizations have been grappling with the challenge of providing secure yet user-friendly access to their computer systems and applications. As technology has advanced, systems have become increasingly complex, and users have accumulated more and more accounts and passwords.

The sheer number of identities that many organizations hold has become so overwhelming that it's practically impossible for human beings to keep track of them all, let alone manage access to them. AI's ability to process vast quantities of data in minutes, rather than months, can revolutionise our approach to IAM – and save us a lot of time in doing so.

WHAT IS AI FOR IAM AND WHY DO WE NEED IT?

IAM's raison d'etre is to ensure that the right individuals have the right access to the right resource at the right time for the right reason. To achieve this ideal scenario, it is essential that identity and access systems have accurate information about each user and can apply it at the appropriate moment.

Many organizations have tried traditional approaches to IAM such as role-based access but then faced difficulty understanding all the access entitlements. Unless you have an army of professionals dedicated to the task, it is simply beyond human control.

Resistance, as they say, is futile, and so it's time to bring in the machines.

AI can collect and make sense of the available information and then provide insight, leading to recommendations and ease of use for all users. When it's up and running, it will differentiate normal login behaviour from abnormal, identifying and responding to potential attacks and enforcing greater controls over access where the risk is calculated to be higher than expected.

Here are just some of the key benefits of using AI in IAM:

- Reduce operational costs by automating labour-intensive processes.
- Make processes more friendly for users and managers through use of recommendations.
- Improve compliance and audit performance.
- Deliver fast, efficient access, reducing end-user down-time.
- Improve security by analysing user context and behaviour when making access decisions.
- Provide greater insight into who is accessing systems and how.

The business case really couldn't be clearer, so how do you implement it?

BEST PRACTICE FOR IMPLEMENTING AI FOR IAM

First, it's worth noting that every organization has different needs and AI and IAM must be adapted to the organisation to produce the best results. While AI for IAM makes life easier, there really are no shortcuts to getting it right. Each organisation must be thorough and pragmatic in its approach, starting with the basics.

If you want to get the most out of AI in IAM, we consider the following approach best practice:

Clean up identity data

Every fresh start starts with a clean-up, and we recommend you do this first.

AI for IAM uses data analysis and machine learning to understand user entitlements within an organization. If user data is inaccurate, such as incorrect attributes or entitlements assigned to a user, it will lead to inaccurate results. It is especially important to ensure the manager and owner information is correct to ensure proper approvals and certifications.

You can use **Access Insights** to detect issues in identity data and the results can be exported for a certification campaign, enabling managers to review and either confirm correct access or remove any incorrect access.

Access Recommendations

Following clean-up and certification, identity data is typically in a much better state. This is an ideal time to explore Access Recommendations, which is a feature that utilises peer group analysis to suggest access that the AI thinks a user should have.

Users receive recommendations about the access that the AI believes they should have, based on analysis of their peer group. Managers receive recommendations for approval tasks and certifications.

Access Modelling

After cleaning up identity data and streamlining access requests and approval processes, it is time to look at access and role modelling.

With the help of AI, it is easier to identify patterns in the data that might be difficult for humans to see. This includes finding groups of users that share common attributes and entitlements that could be combined into a role. Once a high-quality role model is created, it can be used to automate the user management process, which can ultimately save significant amounts of time, effort, and resources.

Keep It Going

Now, you will be in a better place. The next step is simple: Keep going!

AI for IAM will continue to monitor changes in identity data and continue to make recommendations for access or new roles. Businesses are constantly changing, so it is crucial that you have the processes in place to follow up on the information that is being provided by the AI engine and keep your identity management up to date.

IAM IS A CONTINUOUS JOURNEY

AI for IAM is not a on-time exercise that will be out of date the day after you have finished. It continues to run in the background, learning from the activity in your systems, constantly evolving as your business evolves.

Identity and Access Management is a journey that never ends. To ensure it is watertight, and the rewards are fully maximized, you need the right partner to guide you. With over 6000 cybersecurity resources and an IAM Delivery capability of over 1000 resources, Capgemini's services empower customers to address challenges, manage cybersecurity risks and take control of new ways of working.

AUTHOR

Mark Lawley
Senior IAM Consultant
mark.lawley@capgemini.com

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fuelled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | **www.capgemini.com**

For further information please contact:
cybersecurity.in@capgemini.com