Is Active Directory your key strategy for access control?

Time to rethink your IAM approach to stay secure.

Ann Fonseca Jørgensen &
Catherine Njeri Gitau
for VENZO_Cyber Security

Is Active Directory your key strategy for access control?

Time to rethink your IAM approach to stay secure.

Have you checked out the new version 8 of the CIS Controls? Identity & Access Management (IAM) disciplines are moving up in the world, covering the 5th and 6th spot of the most important safeguards in the framework (Account Management and Access Control Management).

Of course, this is not news to us. Even so, we regularly hear variations of the phrase "I've got total control of my users & accesses – I have Active Directory". Ouch! Active Directory is a fantastic access management tool, but that is only one out of many IAM disciplines. Used as a standalone, you are leaving yourself open to attacks on multiple fronts!

> *Active Directory is a fantastic access management tool, but that is only one out of many IAM disciplines.*

Statistically, we know that compromise happens. In 2020, 86% of all organizations were affected by a successful cyberattack in some way or other (*Cyber-Edge 2021 Cyberthreat Defense Report*), so it's a question of reducing the likelihood & impact of an attack: Reducing your attack surface, reducing the chance an attacker has to compromise the important stuff (such as privilege accounts), and reducing what an attacker can even do with a compromised user.

Not convinced? Here are some of the main areas where you are missing out, if you are not supplementing your Active Directory strategy with other IAM disciplines, such as IGA & PAM.

Identity & Access Management (IAM)

A framework of policies and technology that authenticate, authorize and govern identities and their access to applications, data and platforms. It is the discipline of ensuring that the right people have the right access – for the right reasons.

Access Management (AM)

Centralizing authentication and enforcing authorization of users before they can gain access to resources. For example, through Active Directory.

Identity Governance & Administration (IGA)

Governance ensuring that access is granted according to business policies and throughout the user lifecycle.

Privileged Access Management (PAM)

Controlling and monitoring access to highly privileged accounts, applications and system assets.

Getting Visibility

If you are relying on Active Directory as your singular IAM strategy, how do you manage visibility of users and their accesses? Where and how are your AD security groups used on target systems? Do they give access to what you expect, or are they perhaps used elsewhere? Are any accesses given directly on the target system, and thereby not visible in the security group?

Without visibility, you cannot be sure you are in control of who has access to what. Active Directory is a fantastic tool to centralize access management, but for some high-criticality or high-compliance systems, you might be better off avoiding this layer of obscurity, or at least adding direct visibility. With PAM and IGA tools, you can make direct connections to the target system and obtain true visibility of the access landscape.

Lifecycle Governance

While Active Directory is good for managing and issuing access to basic systems within a Windows network, it falls short when it comes to governing the entire lifecycle of user and device accesses.

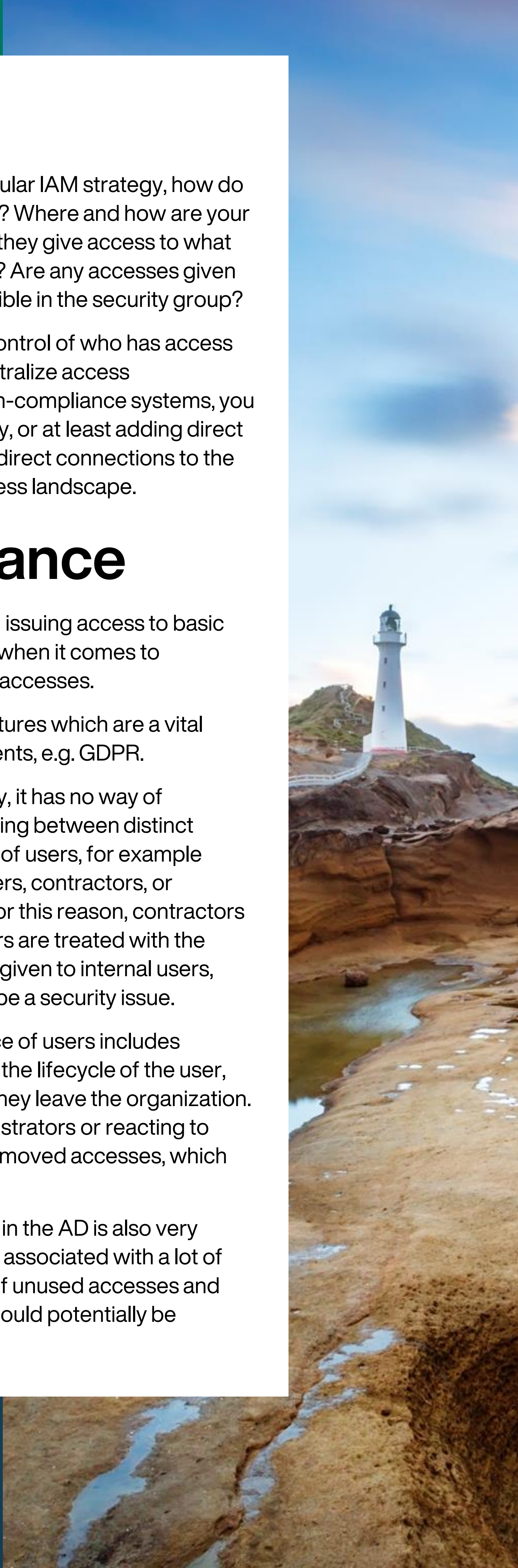
Most importantly, it lacks audit and reporting features which are a vital component to comply with regulatory requirements, e.g. GDPR.

Additionally, because the AD is a simple directory, it has no way of differentiating between distinct categories of users, for example internal users, contractors, or vendors. For this reason, contractors and vendors are treated with the same trust given to internal users, which can be a security issue.

GDPR includes requirements to control and prove access to personal data, as well as securing personal data to an appropriate level.

Governance of users includes reacting to the lifecycle of the user, e.g. when they leave the organization. There is no way of automatically notifying administrators or reacting to such events in the AD, increasing the risk of unremoved accesses, which further increases the attack surface.

Ownership and visibility of non-human accounts in the AD is also very difficult to document and maintain, and it is often associated with a lot of manual work. Again, this leads to accumulation of unused accesses and accounts, also known as privilege creep, which could potentially be exploited by attackers.



So how do IGA tools approach governance?

Access authorization:

Ensuring that business owners have control of approving or revoking accesses. This provides an audit trail ensuring all access is authorized, which allows IGA tools to detect unauthorized access and react on it, e.g. by removing the access or getting it authorized.

Lifecycle of Identities:

IGA tools can track users throughout their lifecycle as they join the organization, change position, go on parental leave, leave the organization, rejoin the organization, and so on. This means actions at each of these states can be automated, e.g. creating initial accounts, automating assignment of access according to business logic, disabling accounts, removing unnecessary accesses, etc. All in all, this frees up service desk & user administration time, and significantly reduces the attack surface by reducing privilege creep and unused accounts.

Access Reviews:

Periodic review of accesses is key to avoid privilege creep and maintain the principle of least privilege. With an IGA tool, such reviews can be initiated automatically and handled through self-service. Some tools can also provide data analytics to assist with reviewing the most critical accesses, simplifying and driving decisions.

Insights and reporting:

IGA tools provide auditing features which include reports and dashboards that give timely insights to the business. These data are often required for enterprises to remain in compliance with regulatory requirements in their industries.

Ownership and Documentation:

With IGA tools, you can register owners of accounts and accesses, and maintain this ownership throughout the lifecycle of the account or access. This ensures that accesses can be approved by the right people who understand the business impact, and that the purpose of an account or access is not forgotten over time.

Enforcement of business policies:

IGA tools can implement, automate and technically enforce business rules, e.g. segregation of duties.

Self-service access requests:

Many IGA tools provide a centralized interface for requesting and approving accesses, freeing up service desk & user administration time and creating that all-important authorization trail.

Privileged Access Management

How do you ensure your administrative user accounts are not compromised?

You may implement password policies & regular password changes, but if human users are to remember complex passwords, they will have to be memorizable – or worse, your users will save them somewhere on post-its or local files, vulnerable to the next data breach.

With PAM solutions you can enforce random generated passwords, store & rotate these securely for personal, shared & emergency accounts. You can even avoid sharing the passwords with the end user by controlling their authenticated sessions, as PAM tools enable isolation, monitoring, recording, and auditing of privileged access sessions and actions.

PAM solutions also allow you to reduce your attack surface by reducing your number of highly privileged accounts (e.g. domain administrators) and governing the access to these accounts.

With an efficient PAM solution, your entire operations team will not need individual access to your domain. Instead, they are pre-authorized to access the privileged shared account via the PAM solution when required for specific work, maintaining the principle of least privilege.

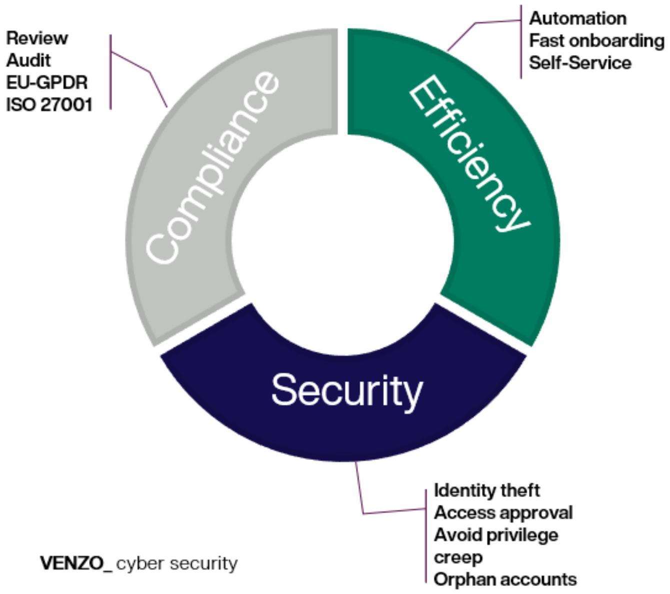
Boost your IAM capabilities

IGA & PAM tools are not meant to replace the AD but provide complimentary functionality to complete the whole IAM picture.

This in turn ensures that the right users have the right accesses at any given time, depending on their identity lifecycle. Having solid PAM, IGA and Access management strategies highly reduces the attack surface as personal, privileged, and non-personal accounts are continuously monitored and governed.

Overall, IGA and PAM solutions add benefits in three main areas:

1. **Increased and enhanced operational efficiency**, which eliminates a lot of manual tasks and frees up IT for other, higher value tasks.
2. **Enhanced security** through visibility, implementation & automation of business logic, and constant monitoring of identities (both human and non-human) and their accesses.
3. **Raised level of compliance** to the different regulatory standards through authorization trail, audit reporting, and better business processes.



Active Directory can't stand alone in today's threat landscape.

Luckily, there's no time like the present to rethink your security strategies and start planning how to increase your security, compliance & efficiency of your organization.

So what are you waiting for?

VENZO_

VENZO_ Insights by our experts

Ann Fonseca Jørgensen

Advanced IAM Specialist

SailPoint Certified IdentityIQ
Security Engineer, CISSP.

Catherine Njeri Gitau

IAM Consultant

Specialized in SailPoint
IdentityNow Cloud IGA

About Us

VENZO_ Cyber Security is a company of the VENZO_ family.

Taking the best from corporate and combining it with the advantages of start-up culture, we organize small to deliver big.

With over 25 experienced specialists, we bring sensible and effective cyber security from the heart of Copenhagen to Denmark and the world. Our goal: Make security work for you – and not the other way around.

Contact us via email or reach out on LinkedIn to talk about the newest trends in cyber security.