SCALED ACCESS

WHITEPAPER

Nine Common Access Management Misconceptions Debunked

Believe it or not, authorization technology has evolved, and the common perception of authorization technology is no longer in sync with the solutions that are offered today.

It is common perception, or rather misconception, that keeps organizations from adopting modern solutions in the first place. The words *identity* and *access management* are never uttered in the same sentence as *innovation, digital transformation*, and *customer centricity*.

Let's face it, one doesn't usually ask the bouncer to discuss the floral arrangements.

So, it's about time to clear up some common misconceptions about access management. Here's a list of the traditional views we have encountered, and we will explain, one by one, why they no longer hold true.

1. Authorization Depends on Finding the System Administrator

This misconception originated in access control lists (ACLs), which are still around. An ACL specifies which users are granted access to systems or resources. In many organizations, getting access means finding the system administrator who can add your name to the list.

But automation is already being adopted in security, because it leads to less administration, faster autonomous access, and ultimately less risk. Access management automation means that if the profile of the user who is asking for access checks all the boxes, he or she automatically gains permission.

2. Access Control is Built For Business and Employees

Most access control solutions are role-based. Your role within the organization defines the level of access you have.

The problem is that customers don't have multiple roles. They have one role only, that of the customer. So, as a customer, you either have access to your online banking, health records, Amazon Echo, or you don't.

Modern access management solves this problem by offering fine-grained access to both the workforce and customers. Customers are no longer treated as one and the same. They can be regarded as minors, premium subscribers, or experts in a particular domain. Modern policy-based access control lets organizations select the attributes that describe the customer, the digital asset, and the context to define rules on who has access to what.

3. Centralized Access Administration Raises the Security Level

The principle is simple: if you do not centralize access management, you will soon have a plethora of rules and no one to hold accountable.

However, centralized access administration has its limits. How do you control access for users who know or work for someone within your ecosystem but who are not directly known to you?

Delegated access administration authorizes users to not only gain access for themselves, but to also give access to predefined relationships. Partner organizations can manage access for their staff, subscribers can manage family accounts, and users can invite friends or colleagues to share or collaborate.

And no, that doesn't mean you're opening Pandora's box. All new users need to sign up before any permission is granted. Organizations retain control and are offered

visibility, and they exert control by designing the policies that define who is allowed to invite what type of relationship. Also, organizations can retrieve the data in event logs to monitor activity, relationships, and user growth.

4. Full Control Happens on Premise

Access control was, by default, deployed on the premises of the organization that provides the system, resource, or service that users need to access. If people tried to gain access from anywhere else, they were offered a VPN connection.

Nowadays, we all access different services using different devices such as our smartphones, watches, or embedded devices. Remote working, the sharing economy, cloud computing, IoT, and 5G will only increase the demand for secure ecosystem access — something that VPN does not provide.

By their very nature, VPNs punch a hole in the network firewall and typically provide unfettered access. In the event of a breach, this permits lateral movement and allows access to applications and data beyond those admissible per the user credentials. Traditional VPNs lack intelligence. Simpler and safer access solutions that can help you move to a Zero Trust security model already exist in the cloud.

Think back to the days when you had to explain to people that moving infrastructure or enterprise software to the cloud was, in fact, improving security, and that authentication technology was something that you could buy instead of build.

The same is happening with authorization today.

5. Access Control is Built For a Single Purpose

Access is usually embedded in the application itself. By design, that application is a closed system. Proprietary companies do not share their API, and typically do not make it easy to integrate their products with other technologies.

An open system provides more choice. Progressive software and hardware companies share their API and can integrate with any access management platform or complimentary security technology.

> **Common misconceptions keep many organizations from adopting modern access management solutions.**

Externalized authorization lets a single cloud platform grant permission between different parties, resources, and applications, which streamlines the access process and reduces the administrative burden.

A loosely coupled architecture means more flexibility because it splits access policy management from the application lifecycle itself, and it allows you to reuse the same access component.

6. Authorization is Nothing More Than Permit or Deny

One of the most common misconceptions is that access management only takes place at the entrance door.

Nothing could be further from the truth because some people get to do more or view more than others. This is why authorization accompanies the whole user experience/journey with multiple policy enforcement points (PEPs).

Permissions can vary depending on who you are, where you are located, what time it is, and what it is you came to do.

7. Access is Best Managed In-House

One department you might be better off keeping in-house is your cybersecurity. When you rely on an external resource to handle your access management, you lose control and are at their mercy.

Nevertheless, innovative companies no longer try to build access solutions themselves, mostly because security skills are in short supply and security automation skills are even harder to find. Also, and more importantly, it's because third-party components get updated automatically, are easy to implement, and cut bad practices.

Speaking of which, the system administrator who certain people could ask to handle worthless, logic-defying exceptions has left the building.

8. Access Management is a Trade-off With UX

Access control limits you in what you can do. You need to stay on the path that the organization designated for you and you're asked to exit as soon as possible.

The term *least user access* refers to the concept that all users at all times should get as few privileges as possible, and launch applications with as few privileges as possible. Or, to put it differently, the less that you can do, the less that can go wrong.

Modern Access Management does not – sorry for the false hope – raise the access level, but it does respond to the dual challenge of a smooth user experience and security of access.

Users expect an instant response to their requests. They are offered quick and easy access and can use their mobile devices to access applications or resources. They get to voice their opinions as well.

9. Organizations Hold All the Access Management Cards

A default attribute that needs to be in place, before any access is granted, is user consent. He or she must clearly understand and agree to what personal registration data will be accessed by whom and for what purpose. Ergonomics and clarity make the exchange more mutual.

On that matter, advanced access management solutions also authorize users to give or share access with others. Relationship-based access control defines that if a certain relationship, such as friend, family member, staff, or supplier, is in place—access is granted. ReBAC revolutionizes collaboration and sharing. In my opinion, if I could be authorized to share a paywalled article with three like-minded friends or colleagues without having to share my credentials, what a wonderful world it would be.