SCALED ACCESS

WHITEPAPER

Service Ecosystem Access

How Authorization Technology Will Revolutionize The Way We Collaborate

Back in the day, security was built around the principle that the people who work for the organization are the good guys that we give access to, while everyone outside the organization are the bad guys we need to keep out.

Well, two things have radically changed since then.

First, the concept 'outside the organization' no longer exists. Organizations need to open the network up so that they can be accessed over residential internet connections to enable work from home. The big 2020 shift to remote working will only increase this trend.

Secondly, collaboration often includes both internal and external parties, so it is no longer as simple as cutting off access to everyone outside the organization.

Developing ecosystem strategies has become a priority for many global companies. They work together with third-party experts, partners, and suppliers to add value to their services.

The Privilege of Relationship

From an analytical point of view, the only thing that these stakeholders have in common is that they have a relationship with the organization. So ideally, there needs to be an access control system where stakeholders are entitled to access secured resources based on relationships.

Let's take the example of clinical trials, the research studies performed to evaluate a particular medical intervention. They are the primary way for researchers to find out if a treatment, like a new drug, diet, or medical device is safe and effective for people.

> **Collaboration often includes both internal and external parties, so cutting off access to everyone outside the organization is no longer an option.**

Pharma and BioTech companies partner with hospitals and clinics consortia, who organize those clinical trials for them. The study staff of these hospitals and clinics invite healthy people or patients to participate in the trial.

Relationship-based access control (ReBAC) lets the initiator or organizer of the trial build access policies that include these multi-hop relationships as a condition to get or give access to clinical trial resources.

Hospitals can give access to study staff members who in turn can enroll study volunteers and so forth.

Or to use an energy ecosystem example, energy distributors give prosumers access to solar panel devices who can share the renewable energy usage with other residents in multi-unit buildings.

But advanced access control does more than granting access to relationships. Because everyone wants to access the same digital assets but that doesn't mean that everybody should get full access.

What Can You Do?

Clinical research staff don't need to access the personally identifiable information (PII) of participants, because unlike study staff, they do not intervene or interact with them. Tenants only need to access their renewable energy consumption. Smart device technicians should only access data gathered from the machine sensors for predictive maintenance.

Organizations can use attribute-based access control (ABAC) to design rules on who can access what based on user attributes, action attributes, context attributes (such as time, device, and location), resource attributes (such as a record's sensitivity), and relationships.

A rule-based engine collects the required attributes and checks them with the access policy in place, including that informed consent was given on the use of their personal data, before granting authorization.

Information is the most valuable when it can be securely shared and leveraged across the whole service ecosystem, not just in the organization.

If the clinical trial participant, for example, cannot provide informed consent because of problems with their memory and thinking, we allow an authorized legal representative, or proxy (usually a family member), to give permission for the person to participate.

Revolutionize Collaboration

ABAC delivers a multi-dimensional access control system that — through its use of attributes and policies — facilitates collaboration, increases scalability, and externalizes authorization for ease of management control.

Information is the most valuable when it can be securely shared and leveraged across the whole service ecosystem, not just in the organization.

Modern access control systems combine ABAC with ReBAC to deliver the best solution for facilitating ecosystem collaboration and ensuring compliance and privacy.

Scaling ecosystem access makes it easy for different stakeholders, both inside and outside the organization, to access information, knowledge, and functionalities. And it authorizes them to give access to their teams, suppliers, or partners.