Privileged Access Is Not a Security Feature

It Is an Operating Model

Most organizations believe they operate *with **Least Privilege***. In reality, they operate with ***Permanent trust***, and permanent trust is exactly what attackers exploit.

Take a look into real environments and the picture is often very different:

- Permanent Global Admin accounts
- Standing Owner rights in Azure
- Shared admin users
- Emergency accounts that are never tested
- Access that is granted but rarely removed

If attackers gain access tomorrow, they will not need to exploit zero-days.

They will log in.

Least Privilege Access is strictly limited to what is necessary and only for as long as needed and applied daily, not just in theory.

The problem is that many security models are built as:

- A one-time project
- A written policy
- An annual security review

But real threats are:

- Continuous
- Automated
- Based on existing access, not only exploits

Most serious breaches do not start with technical hacking. They start with: **Access that already existed.**

This highlights the importance of Privileged Identity Management (PIM), as well as its frequent failures in practice.

Where the real technical hurdle is

The majority of organizations have **PIM enabled**; however, many do not implement PIM optimally in production environments.

Common technical deficiencies identified in practice include:

- Limited roles with PIM enabled
- Inconsistent application of activation policies
- Insufficient enforcement of MFA across all areas
- Underutilization of justification fields
- Approval workflows that are frequently bypassed
- Excessively long activation time windows (8–24 hours)
- PIM limited to Entra ID, excluding Azure RBAC
- Privileged roles assigned directly within subscriptions
- Inconsistent use of Management Groups
- Service Principals and Managed Identities often omitted
- Break-glass accounts not regularly tested in practical scenarios

The primary gap identified is **operationalization**.

Privileged Identity Management (PIM) is often seen as a security feature, configuration task, or project setup. However, it is seldom part of platform lifecycle, change management, deployment pipelines, or compliance reporting routines.

From a technical standpoint, achieving genuine Least Privilege means that all privileged roles must be managed using a Just-In-Time approach. Every activation should be:

- Restricted to a set period,
- Protected by Multi-Factor Authentication,
- Logged,
- Auditable.

Additionally, the scope of privileges needs to be centrally established at the Management Group level. Privileged access should also be integrated into overall platform operations and controlled programmatically rather than through manual processes. Only a few Azure platforms are designed this way from the very beginning.

The real problem is not missing tooling – it's identity still treated as a feature and not as infrastructure.

Why so many organizations still do it wrong

Most IT teams know what Least Privilege is. What they fail at is operating it at platform speed.

In cloud, identity is the control plane. Yet in most environments, that control plane is still designed for human convenience - not machine-enforced security. When incidents happen, operations must move fast and, in that moment, standing access always wins over Just-In-Time. Not because it is secure - but because it is easy.

That is the core design flaw. Organizations consistently choose

- Standing access over controlled activation
- Broad roles over precise scoping
- Local exceptions over global governance
- Human speed over platform discipline

PIM is not avoided because it is unknown. It is avoided because it introduces real design friction:

- Scopes must be modeled.
- Roles must be engineered.
- Approvals must be enforced.

That is architectural work. Not configuration. Without standardization at the management-group control plane, every subscription becomes its own security universe. Compliance may look fine on paper, but production remains exposed by design.

PIM is then reduced to:

- A reporting feature
- An audit checkbox
- A security setting

Instead of what it should be:

- A permanent control-plane mechanism
- A machine-enforced access boundary

The result is predictable:

- Least Privilege exists in documents.
- Standing access still runs your platform.

And when standing access owns the control plane, every workload inherits that risk automatically.

How MyPlatform turns PIM into infrastructure

At MyPlatform, PIM is not a security feature you “add later.” It is part of the platform’s DNA. Built in from day one. Non-negotiable, because in cloud, who can change the platform matters more than what runs on it. Privilege is therefore treated as control-plane infrastructure, not as an identity setting.

We do not rely on manual discipline. We rely on machine-enforced governance.

- All role assignments are deployed as code
- Activation rules are defined at design time
- Scope is locked at management-group level

There is no default standing privileged access in MyPlatform. Global Admin. Owner. Privileged Role Admin. User Access Admin. None of them exist as permanent power.

All privileged access is:

- Just-In-Time
- Time-boxed
- MFA-enforced
- Fully logged

Operations, audit, and compliance are not separate functions in our model. They run on the same control loop. When auditors ask who had access, when, and why, we do not generate reports. The platform already knows.

Governance in MyPlatform is not a project with an end date. It is a living system that updates as Microsoft changes the rules of the platform.

- New roles are absorbed automatically
- Security models evolve without redesign
- Best practices become enforced defaults

Emergency access exists - because reality demands it, but it is never blind. Never permanent and never outside governance.

This is how a cloud platform should operate.

Least Privilege is a management decision

Cloud security failures rarely come from weaknesses in Azure or Microsoft’s tools. They come from too much permanent access. Attackers do not break in anymore. They log in. Least Privilege is therefore not a best practice. It is a business-critical operating decision.

At **MyPlatform**, privileged access is not managed as a security feature. It is engineered as core platform infrastructure – because in modern cloud, who controls the platform is the platform risk.