

Top 20 Microsoft tenant headaches for MSPs...

...and how to cure them

Table of contents

Identity access

- 01. Managing MFA
- 02. Dealing with inconsistent tenant policies
- 03. Hunting down legacy authentication
- 04. Keeping admin privileges under control
- 05. Untangling shared admin accounts

Security configuration

- 06. Chasing configuration drift
- 07. Keeping up with Microsoft's security updates
- 08. Customer "tweaks"

Operational efficiency

- 09. Cleaning up inherited environments
- 10. Keeping everyone on the same page
- 11. Surviving manual tenant audits
- 12. Keeping track of every tenant

Security risk

- 13. Knowing where the real risks are
- 14. Keeping tenants aligned
- 15. Staying ahead of identity attacks

Compliance and reporting

- 16. Proving your value
- 17. Keeping up with compliance

Service delivery

- 18. Packaging Microsoft security as a service
- 19. Growing without the growing pains
- 20. Getting ready for AI

Identity access

01.

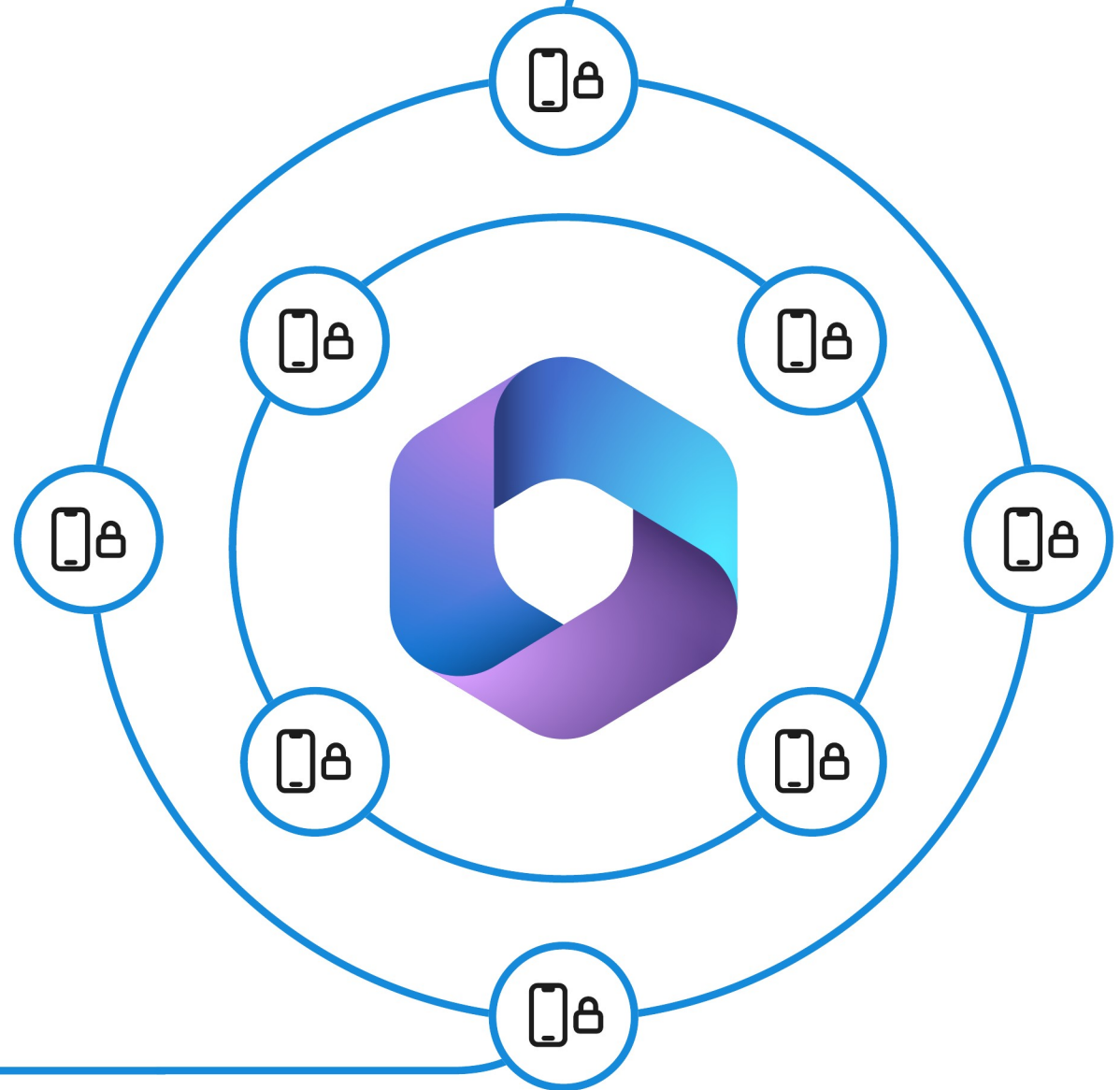
Managing MFA

MFA is one of the easiest ways to protect a Microsoft 365 environment. Yet new users, service accounts, and one-off exceptions have a habit of slipping through the cracks.

The result? MSPs have no easy way to verify that every account is protected without manually checking each tenant.

Did you know?

99.9% of breaches could be prevented by MFA, but only **20%** of Microsoft customers have it enabled properly?



02.

Dealing with inconsistent tenant policies

When every tenant follows a different set of rules, things get messy. Fast.



Inconsistent MFA settings, security controls, and configuration standards don't just create potential security issues. They're a pain to manage.



You waste hours trying to document and troubleshoot each customer's unique configurations, which leads to lower profit margins and an inconsistent client experience.

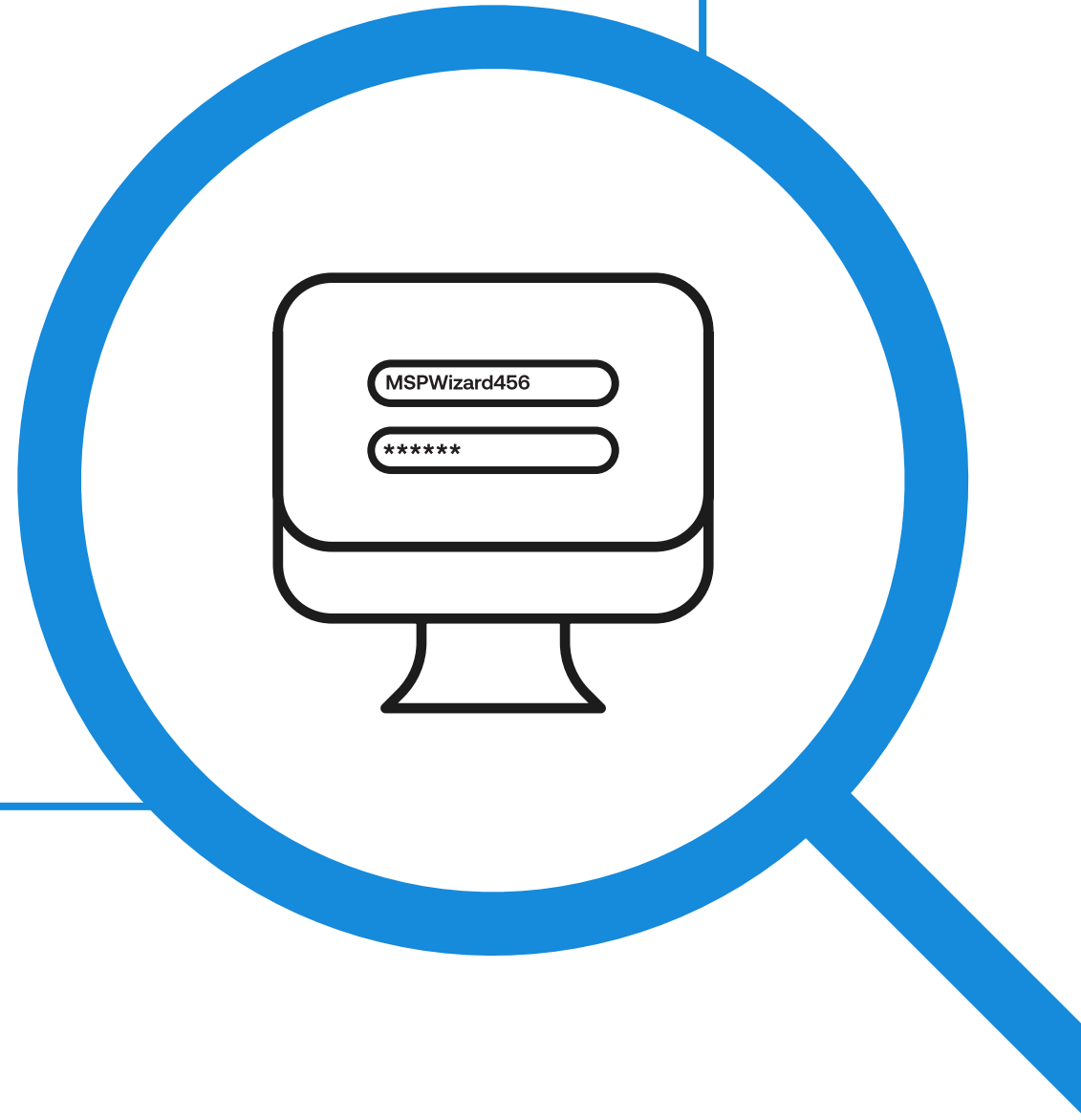
03.

Hunting down legacy authentication

Most MSPs inherit environments that have been around for years. Sometimes decades.

Many of the applications and integrations that have stacked up over the years still rely on legacy authentication, a major identity attack vector.

Finding those dependencies is one thing. Fixing them is another. When critical applications still rely on legacy authentication, updating them is a major lift.



04.

Keeping admin privileges under control

Most MSPs need three aspirins after simply hearing the phrase “admin access.”



There's the CEO who insists on having it. The legacy program no one can update without it. The employee who genuinely needed it, then left the company.



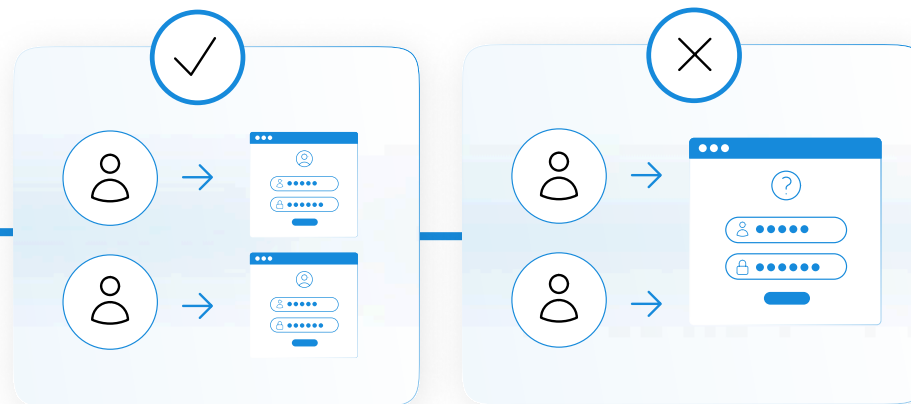
Over time, it becomes impossible to know who has privileged access without spending a month (or three) reviewing each tenant's Entra ID roles and admin groups.

05.

Untangling shared admin accounts

Shared admin accounts make life easier in the short term. You don't have to create individual accounts or manage permissions for multiple users.

In the long run, it's a different story.



When multiple people use the same account, it's impossible to know who made what change, when they made it, and whether their access should have been removed months ago.

Security configuration

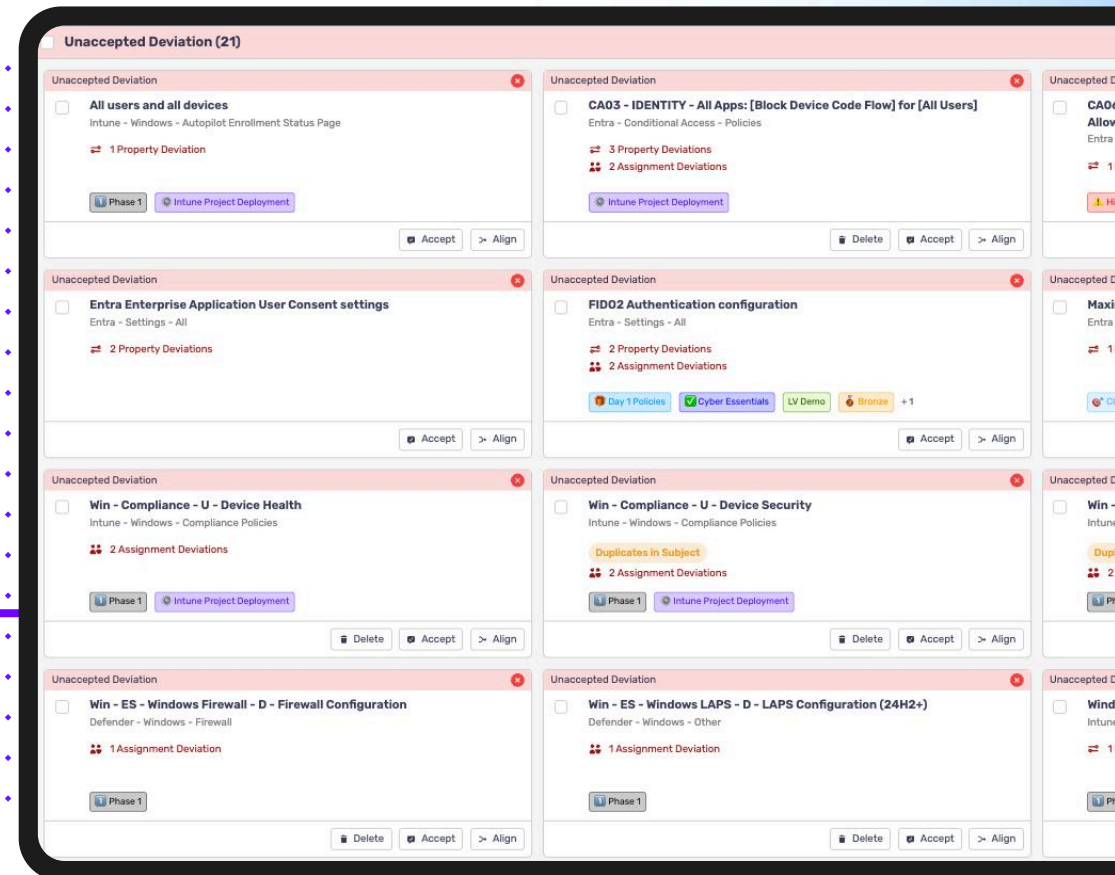
06.

Chasing configuration drift

After hours of updating and adjusting configurations, you finally get a tenant aligned. (Hurrah!) Then real life happens.

A policy gets tweaked to solve a ticket. A new application is added. Microsoft changes a setting.

Before long, the environment looks very different than it did during onboarding. And the only way to find out what changed is every MSP's favourite way to pass the time ... tenant audits.



07.

Keeping up with Microsoft's security updates

Microsoft never stops releasing new security features, controls, and recommendations.

Which is great. Unless you're the one responsible for keeping multiple customer environments up to date.

At the time of publication, Microsoft had more than 700 changes on its roadmap. In the last 12 months alone, Microsoft has pushed out 50 critical updates to Entra ID, Intune, Defender for Office, and Defender for Business.

700

Changes on
its roadmap

50

Critical updates to Entra
ID, Intune, Defender for
Office, & Business.

08.

Customer “tweaks”

Every MSP has that one customer who likes to fiddle.

They disable a policy because it gets in the way.

Or make an exception to accommodate a contractor.
And you don't find out until it triggers a ticket.

Then you're left trying to figure out what changed,
when it happened, and why the environment suddenly
behaves differently than expected.

**Operational
efficiency**

09.

Cleaning up inherited environments

When you inherit a new environment, you inherit every shortcut, exception, and questionable decision made by the customer's previous provider.

Their mess is now your problem. Which means a proper onboarding takes time. Lots of time.

It can take hours to bring the environment up to your standards.

10.

Keeping everyone on the same page

Ask three techs how to configure a tenant and you'll get three different answers.

One person has a favourite naming convention.

Another has a different way of handling exceptions.

Everyone documents things a little differently.

Over time, those small differences add up. When an issue occurs, you spend more time trying to figure out how the tenant was configured than troubleshooting the problem.

11.

Surviving manual tenant audits

Want to know how secure a tenant really is?

Start opening tabs. Entra. Defender. Purview. Exchange. SharePoint. Compliance Center. You know the drill.

Manual audits are a total timesuck. Which is why they rarely get done, despite an MSP's best intentions. There's always something more urgent in the queue



12.

Keeping track of every tenant

Managing one Microsoft 365 environment is (mostly) manageable. **Managing dozens? Or hundreds? That's just not possible.**

As you scale, it becomes impossible to remember which customers have been reviewed, which still need work, and which are up to date.

Spreadsheets and sticky notes help. Until they don't.

Security risk

13.

Knowing where the real risks are

Some security issues need your immediate attention.
Others can wait.

The challenge is knowing the difference.

When you're managing dozens of Microsoft environments, it's easy to spend hours fixing low-risk issues while more serious problems go unnoticed.

14.

Keeping tenants aligned

Getting a new customer's configurations just right is hard enough. Keeping them that way is even harder.

The more customers you support, the harder it becomes to deliver the same level of protection, service, and governance across every environment.

Eventually, keeping tenants aligned becomes a full-time job.

15.

Staying ahead of identity attacks

Attackers never seem to run out of new ways to target Microsoft 365 environments.

Identity is the latest battleground. MFA bypass attacks, compromised accounts, and Conditional Access gaps are all fair game.

The bad guys only have to find one weak link. MSPs have to find — and fix — them all.



Compliance and reporting

16.

Proving your value

You know how hard your team works to keep customers secure. But proving it isn't always easy.

Customers don't see all the policies you enforce, the risks you've reduced, and the issues you've prevented.

Without clear reporting, all the work that happens behind the scenes goes unnoticed.



17.

Keeping up with compliance

Just when you think you've figured out the latest CIS or NIST requirements, they change.

And then there's cyberinsurance. It seems like every week those questionnaires get longer and longer.

The finish line just never stops moving.



Service delivery

18.

Packaging Microsoft security as a service

Many MSPs treat tenant management as an optional upgrade for customers in highly regulated industries. Not as a core part of their security services.

It's not you. It's the tools that have been available to you to date.

None make it easy to see and manage tenants at scale. So your services stay ad-hoc.



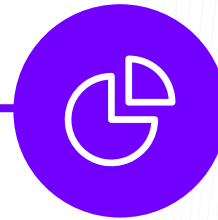
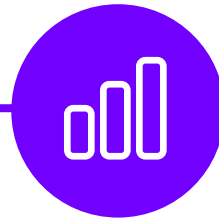
19.

Growing without the growing pains

Most MSPs don't notice their processes breaking down.

A few extra customers mean a few extra exceptions.

It seems like no big deal until even the simplest task requires multiple steps, multiple people, and far more time than it should.



20.

Getting ready for AI

Every customer has questions about Copilot.

The excitement is real. But so are the concerns. Who has access to what? Is every piece of sensitive information secured? Are the right governance and compliance guardrails in place?

The last thing you want is for AI to expose a problem that was hiding in the tenant.



How to cure your Microsoft 365 headaches

At first glance, these seem like 20 different problems. In reality, these headaches are all symptoms of the same condition: trying to manage Microsoft 365 manually.

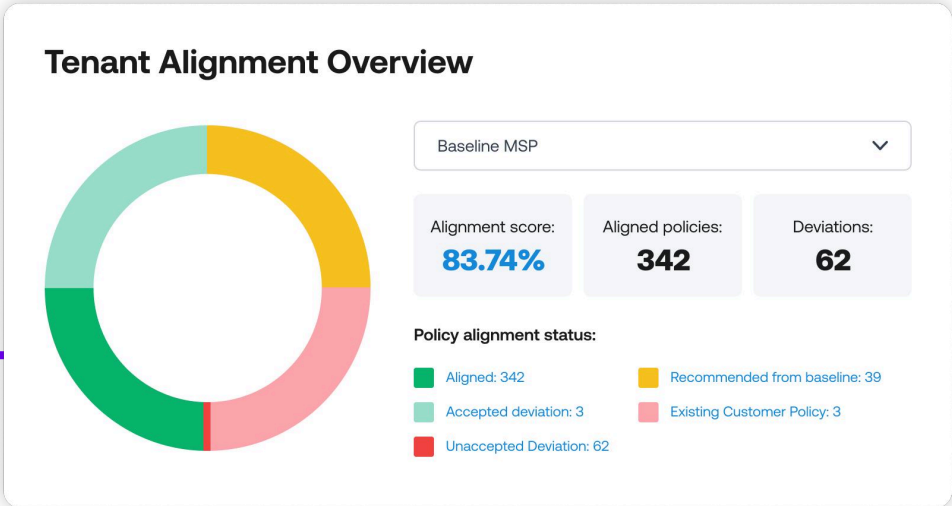
The truth is, the more customers you support, the harder it becomes to keep every tenant aligned.

inforcer is here to change that.

Instead of logging into each individual tenant and managing security settings one by one, inforcer lets you create standardized security baselines and roll them out consistently across every environment you manage.

Monitor MFA, Conditional Access, legacy authentication, and other critical security controls from a single dashboard.

Now you can identify configuration drift and security gaps automatically (no more manual audits!), and know that every tenant is aligned to your baseline — no exceptions.





Let's get started

See how inforcer 365 Manager can help
you solve your Microsoft tenant headaches.

Book a demo