inforcer

The top 5 Microsoft 365 tenant mistakes that lead to breaches

(and how to prevent them)

When people think about breaches, they might imagine a team of hackers coordinating a sophisticated attack from a dark room full of monitors.

In reality, most breaches are actually … boring. An attacker gets hold of an unsecured account's credentials and bam, they're in.

The good news is, most boring (and not-so-boring) cyberattacks are entirely preventable.

Here are five common Microsoft 365 tenant mistakes that put your customers at risk. And, more importantly, how to prevent them.

Most Microsoft 365 tenant breaches aren't sophisticated. They're the result of a few preventable mistakes.

Mistake #1
Not fully enforcing MFA

1

What happens

You onboard a new customer and spend days getting everything configured correctly. MFA is rolled out. The tenant *looks* secure.

Then real life happens. New users are added. Service accounts get excluded. Temporary exceptions become permanent. Over time, those small changes create big gaps.

Why it matters

Microsoft estimates that 99.9% of account compromise attacks can be prevented by MFA.

The problem? Attackers don't target the accounts protected by MFA. They look for the ones that slipped through the cracks.

And when they find them, they don't have to break in. They simply log in.

If MFA isn't enforced everywhere, it's not enforced at all.

Mistake #2
Letting legacy authentication stick around

2

What happens

You inherit a customer who's been on Microsoft 365 for more than a decade. Over the years, applications, integrations, and workflows were added to their environment. Some of which still rely on older authentication methods.

Is that a POP3 connection? Throwback!

Why it matters

Older authentication methods weren't designed to protect against today's threats. And hackers know it.

They target legacy authentication because it allows them to bypass MFA and other modern security controls.

Your security is only as strong as its weakest link.

Mistake #3
Not standardizing security policies

3

What happens

One customer's compliance requirements mandate strict Conditional Access policies. Another uses an application that requires an exception. A third environment has strict cyber insurance controls.

Before long, it feels like every customer has their own set of policies, exceptions, and requirements.

Why it matters

When every tenant follows a different set of rules, routine work takes longer than it should.

Techs spend more time checking documentation, reviewing exceptions, and figuring out how a tenant works rather than resolving the issue in front of them.

When every tenant is different, every ticket takes longer.

Mistake #4
Not keeping up with configuration drift

4

What happens

You secure a tenant during onboarding and move on to the next fire.

But a few weeks later, an engineer modifies their Conditional Access policies to resolve a ticket. And then the customer gives a contractor access to SharePoint. And then Microsoft introduces a new security control.

Suddenly, the tenant looks very different from the one you onboarded.

Why it matters

A tenant that's secure today may not be secure tomorrow. And you might not realize until it's too late.

Drift is silent until it becomes a breach.

Mistake #5
Pushing back tenant audits (again and again)

5

What happens

When it comes to tenant audits, every MSP has the best intentions. But "I'll do it monthly" quickly becomes "I'll do it quarterly," which basically translates to "I'll do it never."

The more you scale, the harder it is to keep up with tenant management. And before you know it, years have passed since anyone audited the environment.

Why it matters

Security isn't static. New users are added, permissions change, policies are modified, and Microsoft constantly introduces new controls.

Without regular audits, security gaps can go unnoticed for months or even years.

By the time they're discovered, an attacker may have already found them first.

Attackers don't wait for your next audit.

How to get ahead of these mistakes

Option 1
The hard way

In theory, every one of these issues is fixable.

Your team can manually review MFA coverage and Conditional Access policies, check for legacy authentication, compare policies across tenants, and conduct regular tenant audits.

But they don't have the time.

Option 2
The inforcer way

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

Are these mistakes lurking in your tenants?

inforcer gives you full visibility into MFA coverage, Conditional Access, legacy authentication, configuration drift, and other security gaps across every Microsoft 365 tenant you manage.

Book a demo