inforcer

The Cost of Microsoft 365 Configuration Drift

Configuration drift occurs when the actual state of an IT environment deviates from its intended setup or baseline. Within Microsoft 365, policies, settings, and controls gradually diverge from how they were originally configured until they no longer function as intended.

Configuration drift is often invisible until a breach. It happens quickly and quietly but can have catastrophic consequences.

Why does configuration drift happen?

Help desk interventions

Technicians create exceptions to solve user issues, moving the tenant away from the baseline. Those changes often don't get reverted.

Microsoft changes and updates

Microsoft regularly introduces new features, updates, and default-setting changes, which creates drift even if no one touches the tenant.

How often does Microsoft make updates?

A single Microsoft 365 tenant contains thousands of unique configurations. Given Microsoft's pace of change, keeping even one tenant fully up to date manually is difficult. Doing so across dozens or hundreds of tenants is nearly impossible.

Microsoft makes **~90-95 changes per month** on average.

50 critical security updates were made in the last 12 months.

Microsoft currently has **700+ changes** on its roadmap.

No native Microsoft **tool reports on drift** across tenants.

The security cost of configuration drift

70% of organizations regularly experience configuration drift, and the consequences can be severe.

55%

of cloud breaches trace back to configuration drift or oversight.

DS

60-80%

of outages are linked to change or misconfiguration.

Cloudhouse™

43%

of breaches exploited system vulnerabilities, many stemming from preventable configuration issues.

verizon

Average cost of a cloud misconfiguration breach is

$4.3 million

DS

Average detection time for a configuration issue is over

180 days

DS

Average recovery time after a configuration-related breach is

~250 days

DS

Stay on top of configuration drift with inforcer

Manual monitoring isn't realistic for today's MSP. inforcer helps detect and remediate configuration drift before it becomes a problem.

Automated drift alerting

inforcer continuously monitors every tenant against its baseline and flags changes the moment they occur. Instantly see what changed, where it changed, and whether it was authorized.

One-click remediation

Quickly identify customers out of alignment, apply recommended policies, and approve customer-specific deviations to restore alignment in just a few clicks.

Shared, best-practice baselines

inforcer provides pre-built best-practice baselines that you can deploy immediately. As Microsoft makes changes, we keep the baseline current for you.

inforcer Dispatches

Keeping up with Microsoft updates is a full-time job. inforcer Dispatches cuts through the noise with monthly updates on the changes that matter most to MSPs.

Want to tackle configuration drift head on?

Book a demo of inforcer today to learn how to eliminate manual effort and proactively manage configuration drift.

Book a demo

inforcer