ClientIQ

Revenue opportunity report

My Clients name • 2026-08-04

EXECUTIVE SUMMARY

This scan of My Clients name's Microsoft 365 environment, run on 4 August 2026, found a combination of unused licences and low Copilot adoption that together account for an estimated USD 1,200 per month in avoidable spend. On top of that, gaps in login security and email protection leave the organisation exposed to account compromise and email fraud. Addressing the licence waste alone would recover roughly USD 14,400 over a full year at the current seat cost of USD 60 per user per month.

> **Identified opportunity: USD 1200.00/month**
> Based on USD 60/seat/month at 11 inactive M365 seats + 9 unused Copilot seats

LICENCE EFFICIENCY

Of the 47 licences currently assigned, 9 belong to users who have not logged in for 90 days or more, and a further 2 are held by accounts that have already been disabled. Together that is 11 licences, or around 23% of the total, generating no business value. To a finance director, an inactive licence is simply a recurring monthly charge for a service no one is using. Those 11 licences cost an estimated USD 660 per month at the current seat rate. We can audit the full list with your team, confirm which accounts can be safely removed or reassigned, and implement a regular review so unused licences are caught early rather than running on indefinitely.

COPILOT ADOPTION

My Clients name has 12 Copilot licences assigned, but only 3 of those users actively used the tool in the last 28 days. That is a 25% adoption rate, meaning 9 licences are sitting idle at an estimated cost of USD 540 per month. For a finance director, the concern is straightforward: the organisation is paying a premium for a productivity tool that most assigned users are not yet using, so the return on that investment is currently very low. We can run a short, practical onboarding session with the affected users and set a 60-day adoption target to make sure the spend starts delivering measurable benefit.

SECURITY POSTURE

Of the 47 user accounts checked, 37 have multi-factor authentication registered. That leaves 10 users, roughly one in five, able to access company systems with a password alone. A stolen or guessed password is enough to give an attacker full access to any of those accounts.

Microsoft rates the organisation's overall security configuration at 41 out of a possible 100 points. That score reflects how well the Microsoft 365 environment is configured against Microsoft's own recommended controls. A score of 41% indicates that more than half of the available protections are not yet in place, which means the organisation is carrying a meaningful level of avoidable risk in its day-to-day operations.

EMAIL SECURITY

My Clients name currently has no email authentication policy in place for its domain. This means there is no technical control preventing an outside party from sending emails that appear to come from the organisation's own address. Without this protection, the domain can be used in phishing attacks targeting customers, suppliers, or staff, and the organisation has no visibility of when that happens.

RECOMMENDED ACTIONS

1. Remove or reassign the 11 inactive and disabled-account licences to stop the USD 660 per month in wasted spend.
2. Schedule a 30-minute Copilot walkthrough with the 9 non-active licence holders and set a review date 60 days out.
3. Enable multi-factor authentication for the 10 users currently accessing the environment without it.
4. Publish an email authentication record for the organisation's domain to close the spoofing exposure.
5. Book a Secure Score review session to prioritise the highest-impact configuration changes and build a short remediation plan.

RISK OVERVIEW

19% inactive	79% covered	41%	Not configured
LICENCE EFFICIENCY	MFA COVERAGE	SECURE SCORE	DMARC

We are ready to walk through any of these findings in more detail and can begin remediation work at a pace that suits your team.