Microsoft 365 Security Review

As your cloud footprint grows, taking action to secure the Microsoft 365 environment, formerly Office 365, is crucial. Everyday hackers are getting more sophisticated and looking for their next target. To prevent downtime and data loss, additional security settings, configurations, and add-ons need to be applied in the Microsoft 365 tenant.

ProArch's Microsoft 365 Security Review analyzes the current state of the Microsoft 365 environment and identifies gaps against the security controls required to protect critical information and assets.

This high-level review provides a clear picture of the Microsoft 365 cloud environment security posture and delivers a plan for reducing risk.

✓ Analysis of Microsoft 365 environment by security experts

✓ Improve security across the Microsoft 365 environment

✓ Receive a clear roadmap for remediation

✓ Understand current security gaps and weaknesses

How the Microsoft 365 Security Review works

The Microsoft 365 Security Review is a flat fee engagement that evaluates the Microsoft 365 environment against 29 security controls that are a combination of ProArch's do-first controls, Microsoft Secure Score, and industry-standard best practices.

The security controls are broken down by risk impact level, from most critical to least.

Critical Impact Controls: Multi-factor authentication, global admin configuration, and email protection ← Greatest impact on your overall security however typically require the most effort to implement

High Impact Controls: Sign-in policies, audit logging, and mailbox security

Medium Impact Controls: Sharing policies, spam filters, and suspicious activity alerts

Low Impact Controls: Custom login portal, application control, and mail flow rules ← Least impactful on your security however typically the easiest to implement

Microsoft 365 Security Review Final Report

ProArch's Security Team provides a 10+ page report that breaks down where the Microsoft 365 environment stands against security controls required to improve protection against malicious actors.

Require MFA for Administrative Roles	Control Category: Configuration
Description	You should enable MFA for all your admin accounts (except one break-glass account) as a breach of any of these accounts can lead to an attacker having a high level of administrative access within your organization.
Findings	1 out of 2 administrators are enrolled in MFA, no break-glass administrator accounts exist
Current Status	☒ **Not implemented** ☐ Already Implemented

Risk Impact Level

Security Consultants prioritize the recommended security controls based on level of risk.

Critical impact, level 1, being the greatest impact on security and requires the most effort to implement. Low impact, level 4, being the least impactful on security and takes less effort to implement.

Findings

Includes unique details for each control that will assist with remediation

Current Status

Documents if the control is not implemented or already implemented

In a separate engagement, ProArch will implement security hardening control recommendations from the Microsoft 365 Security Review.

ProArch was founded on the belief that a future where change is 'business as usual' is fundamentally more exciting than one where it is not.

We accelerate value and increase resilience for our clients with consulting and technology – enabled by cloud, guided by data, fueled by apps, and secured by design.

proarch

proarch.com

United States
Atlanta, GA
Syracuse, NY
Rochester, NY
Buffalo, NY

United Kingdom
London

India
Hyderabad
Bangalore