CASE STUDY

MICROSOFT 365 SECURITY

Identity, endpoint & email protection

MFA and endpoint security rollout for a multi-site nonprofit

Multi-site nonprofit organization · All staff accounts and shared devices · Role: sole IT administrator

Outcome: Every staff account protected by MFA with zero lockouts during rollout; every endpoint reporting to Microsoft Defender; conditional access designed around real workflows instead of blanket blocks.

The Situation

A multi-site nonprofit ran its operations on Microsoft 365 with no MFA, unmanaged devices shared between staff and volunteers, and no visibility into sign-in activity. One phished password could have impersonated the organization to its entire community. Staff were non-technical, so a heavy-handed security rollout risked locking out the very people it protected.

What Was Built

- **Staged MFA rollout** - plain-English announcement to staff first, a one-page setup guide, then enforcement in waves with a support window for each wave so nobody was stranded mid-workday.
- **Microsoft Defender endpoint onboarding** across all organization devices, including offline/USB onboarding for shared machines that rarely see a normal login.
- **Entra ID app registration** with least-privilege Graph permissions (22 scopes individually justified) for the organization's automation - no over-permissioned service accounts.
- **Conditional access planning** around named locations and device state, designed to be invisible to staff working normally and a wall to everyone else.
- **Plain-English documentation** for every change, written for the next administrator, not for the author.

Results

- 100% of staff accounts on MFA - zero lockouts, zero panicked calls, because the rollout was communicated before it was enforced.
- All endpoints visible in Defender with alerting on; previously zero endpoint visibility.
- Email authentication (SPF/DKIM/DMARC) verified and corrected as part of the same engagement.

Stack & Methods

Stack: Microsoft 365 · Entra ID · Microsoft Defender for Business · Microsoft Graph · PowerShell · Conditional Access · SPF/DKIM/DMARC