Optimal Microsoft 365 Management: The Microsolve Advantage

1. Proactive Environment Management with CIPP

Microsolve leverages the Cyberdrain Improved Partner Portal (CIPP) for consolidated, proactive management across all client M365 tenancies.

CIPP enables our technicians to:

- Centrally view, manage, and report on policy settings, user roles, and license usage for every client environment.
- Quickly identify misconfigurations or risky deviations from security baselines, minimizing the window of vulnerability.
- Ensure policy consistency and compliance reporting, supporting business and regulatory requirements.

Value: Faster incident response times, consistent enforcement of best practices, and clear reporting for audit and compliance needs.

2. Yubikey Hardware Tokens for Technician Authentication

To ensure the highest security for privileged technician accounts, Microsolve utilises Yubikey hardware tokens for authentication. Each technician is issued a pair of dedicated, company-managed Yubikeys.
Access to all privileged operations - including tenant administration, security policy changes, and break-glass recoveries - requires physical authentication using Yubikey's phishing-resistant multi-factor technology.

Value: Even in the face of phishing, credential theft, or social engineering attacks, only Microsolve's authorized personnel can perform sensitive changes, greatly reducing the risk of unauthorized access.

3. Bitwarden for Password Management and Break-Glass account Segregation

All break-glass (emergency access) and administrative credentials are stored securely within Bitwarden, an industry-leading password management platform:

- Break-glass credentials are kept in dedicated, segregated vaults that are accessible only to a select group of authorized technicians.
- Every access to these credentials is individually logged and audited, maintaining a record of who accessed what, when, and why.
- Passwords for emergency accounts are rotated regularly and managed in accordance with Microsoft and ASD best practices.
- Segregation prevents single points of failure and upholds the principle of least privilege.

Value: Encrypted, audited, and role-restricted storage of emergency credentials meets the highest standards for data protection and compliance.

4. Delegated Access via GDAP

Microsolve securely manages client environments through a dedicated support/management M365 tenancy, using Granular Delegated Admin Privileges (GDAP). This allows for:

- Scope-limited delegation of precise administrative rights, ensuring only essential access for only as long as needed.
- Isolation of support operations, eliminating the risks of broad, standing global admin access across multiple client sites.
- Automatic expiration and review of privilege delegations in accordance with contract and security requirements.

Value: Clients benefit from secure, auditable, and easily revoked access, ensuring that privilege is never more than what is necessary for a given support task.

5. Additional Layers! Monitoring, Customisation & Reporting

- Automated monitoring and alerting: Real-time visibility and notification of unusual activity, weak configurations, or failed login attempts.
- Environment customisation: Tailoring policies, workflows, and integrations to fit unique client needs without sacrificing core security.
- Comprehensive reporting: Regular, actionable insights into security scores, user activity, policy compliance, and licensing, supporting internal reviews and audits.

Value: Enhanced operational readiness, flexibility for business change, and evidence-backed compliance for every environment.

Microsolve's M365 management process isn't just secure - it's strategic and measurable.
Integration of CIPP, Yubikey, Bitwarden, and GDAP forms the backbone of a robust, modern, and auditable management solution.
This ensures your data is not only safe, but compliant and always available—delivering serious value where it matters most.

microsolve
Comprehensive Technology Solutions