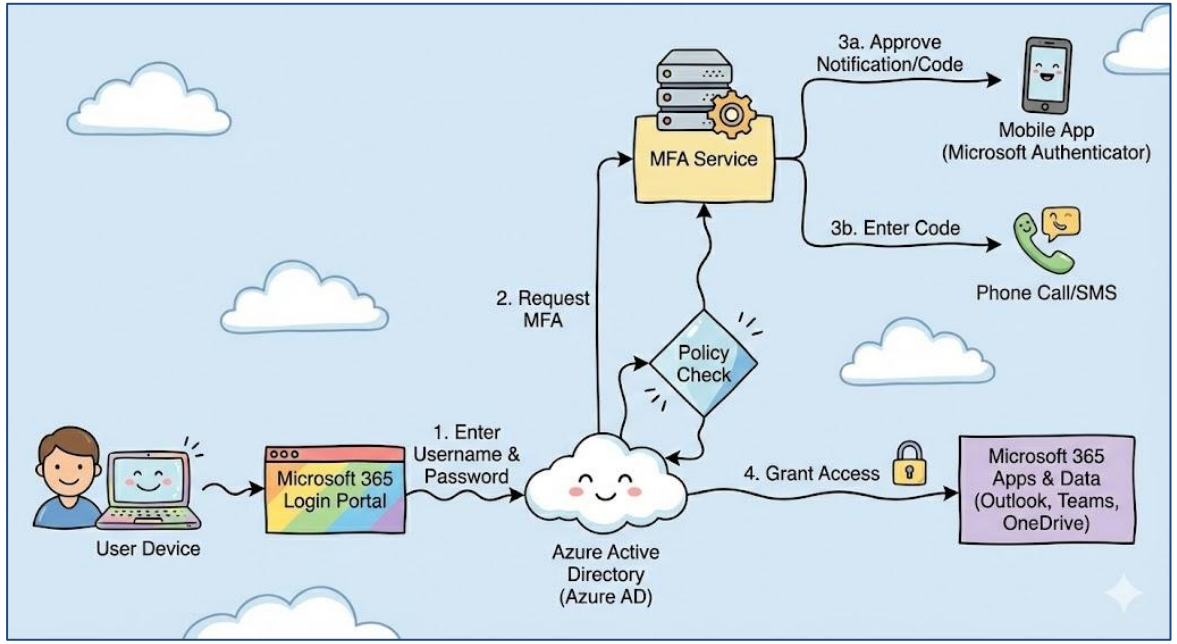

CLOUD EXPERTS
MICROSOFT 365
SECURITY
BEST PRACTICES &
VENDOR SOLUTIONS
365apps.pro
Cloud Experts

Identity & Access Management

The First Line of Defense

Multi-Factor Authentication (MFA)

- **Crucial Protection**: MFA blocks 99.9% of automated account compromise attacks.
- **Universal Coverage**: Enable for *all* users, not just administrators.
- **Best Experience**: Use the Microsoft Authenticator app for secure, passwordless-ready verification.
- **Move Beyond SMS**: Transition away from SMS/Voice codes which are susceptible to SIM swapping.



Conditional Access & Zero Trust

Conditional Access

Automate access decisions based on real-time signals. Policies act as "if this, then that" gates.

- User location & risk
- Device compliance status
- Application sensitivity

Zero Trust Principles

Move away from the "trust but verify" model to a modern security posture.

- **Verify Explicitly**: Authenticate every request.
- **Least Privilege**: Limit access to Just-In-Time.
- **Assume Breach**: Segment networks and encrypt data.

Threat Protection

Defending Against Modern Attacks

Email Security

Phishing is the #1 Entry Point

Microsoft Defender for Office 365 provides critical defenses against malicious emails.

- **Safe Links:** Scans URLs in emails, Teams, and Office docs in real-time to block malicious sites.
- **Safe Attachments:** Detonates files in a virtual sandbox environment to check for malware before delivery.
- **Strict Policies:** Enable "Strict" preset security policies for high-value targets

Microsoft Defender Suite

Defender for Office 365

Protects against threats in email, links (URLS), and collaboration tools like Teams and SharePoint.

Defender for Endpoint

Enterprise-grade endpoint security designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Defender for Identity

Cloud-based security solution that uses your on-premises Active Directory signals to identify and investigate advanced threats.

Data Protection & Governance

Securing Your

Assets

Information Protection

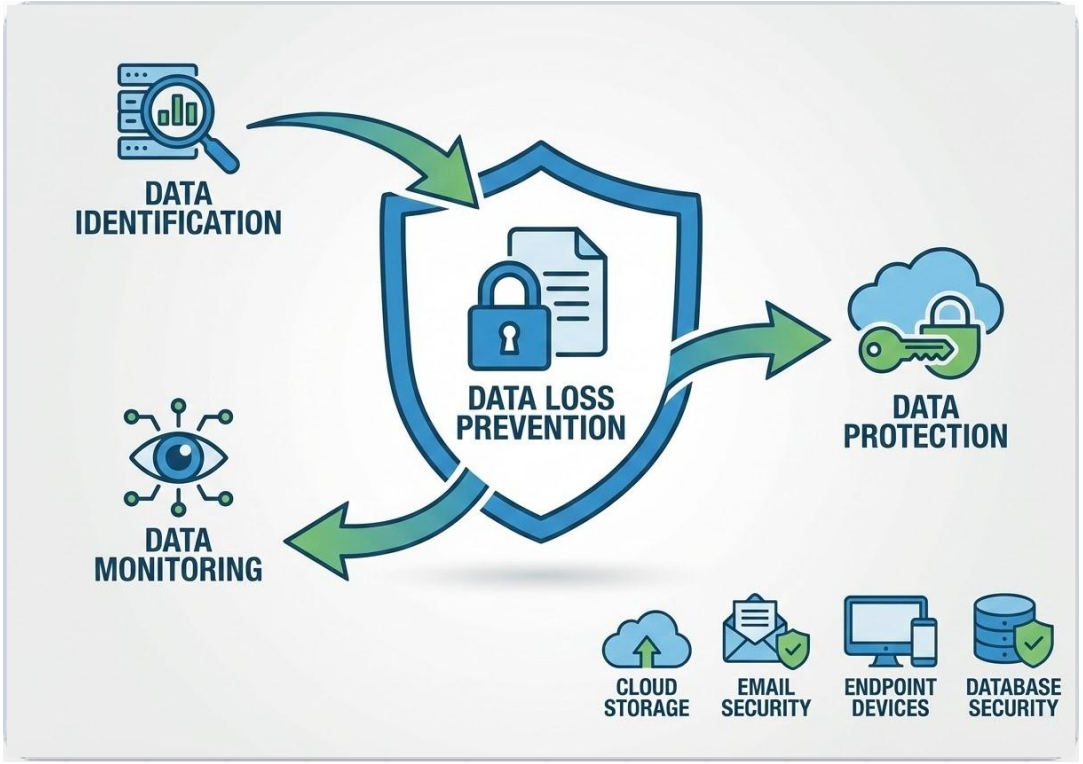
Classify
Identify data based on sensitivity (Public, Internal, Confidential).

Encrypt
Apply automatic encryption to sensitive content, ensuring safety even if leaked.

Control
Manage access rights (IRM) to prevent unauthorized printing, forwarding, or copying.

Data Loss Prevention (DLP)

- **Identify Sensitive Info:** Automatically detect financial data, PII, and medical records across your tenant.
- **Prevent Accidental Leaks:** Block users from sharing sensitive data externally via email or Teams.
- **User Education:** Show "Policy Tips" in Outlook to educate users why an action is blocked before they send.
- **Enforce Compliance:** Ensure your organization meets regulatory standards (GDPR, HIPAA) by controlling data flow.



Admin & Operational Excellence

Microsoft Secure Score Regularly check your score to discover and prioritize security improvement actions tailored to your tenant.

Unified Audit Logs Enable and monitor audit logs to investigate suspicious activities and gain visibility into user actions.

Admin Account Security Use dedicated "cloud-only" accounts for admin tasks. Never use Global Admin accounts for daily email or web browsing.

Shared Responsibility Microsoft ensures platform uptime; you are responsible for data retention. Consider third-party backups for critical data.

Microsoft 365

Security Best Practices

A comprehensive guide to securing your organization's digital workspace against modern threats.

Identity & Access Management

The perimeter has shifted from the firewall to the identity.

Identity Essentials

MFA & Security Defaults

MFA is the most effective control, blocking 99.9% of account compromise attacks.

- Enable "Security Defaults" baseline.
- Use Microsoft Authenticator app.
- Enforce MFA for all admin accounts.

Role-Based Access Control

Minimize the attack surface by limiting access rights to the bare minimum permissions.

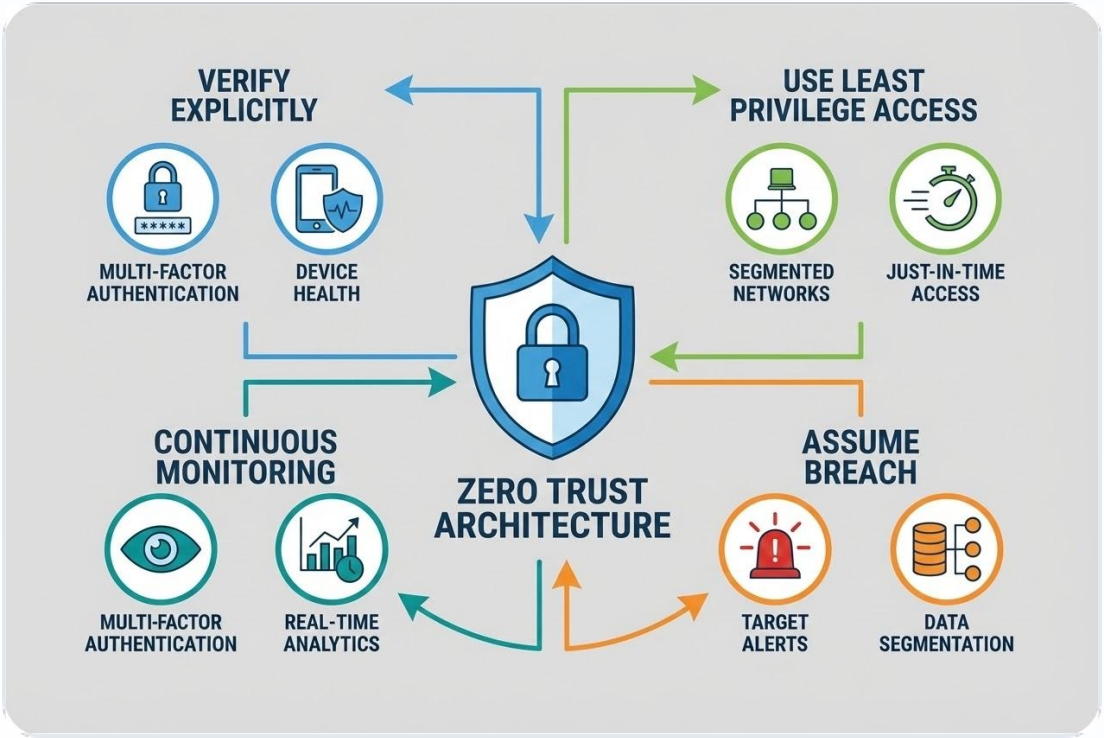
- Limit Global Admins (max 3-5).
- Use Privileged Identity Management.
- Regularly review role assignments.

Zero Trust & Conditional Access

Never Trust, Always Verify

Transition to "Zero Trust". Conditional Access policies act as a gatekeeper.

- Block legacy authentication protocols.
- Geo-blocking for non-operating countries.
- Require compliant devices for access.



Threat Protection

Defending against phishing, malware, and sophisticated attacks.

Defender for Office 365

Safe Links

Provides time-of-click verification of URLs in email messages and Office documents.

Safe Attachments

Checks email attachments for malicious content in a sandbox before delivery.

Anti-Phishing

Uses machine learning to detect impersonation and spoofing attempts.

Combating Phishing

Phishing is the #1 attack vector. Technology isn't enough; user awareness is critical.

Implement Attack Simulation Training to educate users. Run realistic phishing scenarios to identify vulnerable users.

Report suspicious emails immediately using the "Report Phishing" add-in in Outlook.

Device & Data Governance

Securing endpoints and protecting sensitive information.

Device Management (Intune)

MDM (Device Management)

Full control over corporate-owned devices ensures security standards.

- Enforce disk encryption (BitLocker).
- Require complex PINs/Passwords.
- Remote wipe capability.

MAM (App Management)

Protect corporate data on personal devices (BYOD) without full control.

- Restrict copy/paste functionality.
- Prevent "Save As" to local storage.
- App-level PIN requirements.

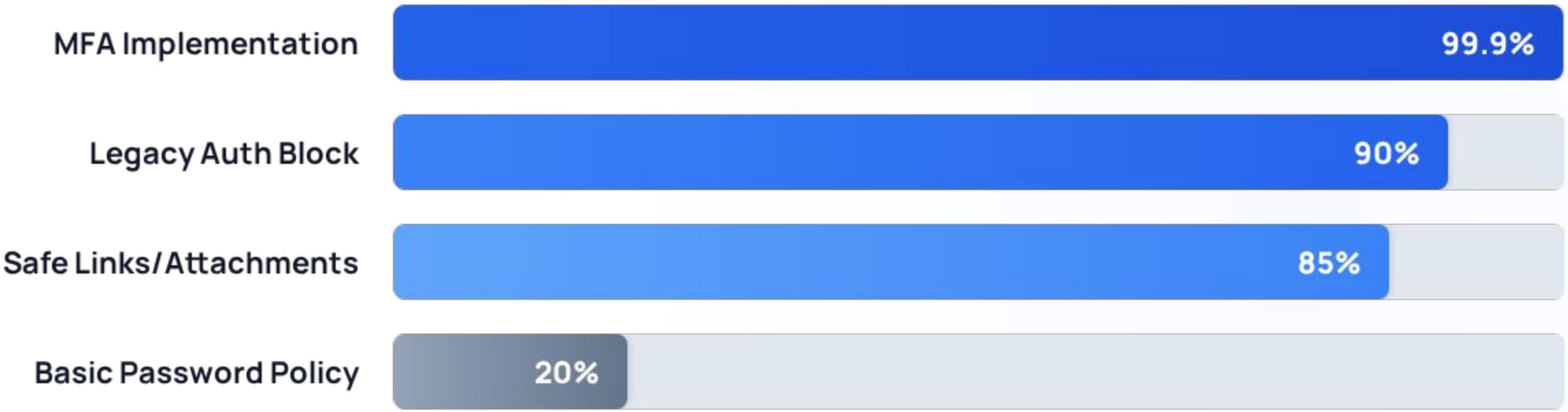
Information Protection

Classify & Protect

Data travels everywhere. Use Microsoft Purview Information Protection to classify documents.

- **Sensitivity Labels:** Tag documents as Public, Internal, or Confidential.
- **Encryption:** Restrict access to specific users or groups.
- **DLP Policies:** Detect and block the sharing of sensitive data.

Security Control Efficacy



MFA provides the highest ROI for security, blocking nearly all automated identity attacks.

Implementation Roadmap

Immediate

Enable Security Defaults / MFA. Review Global Admin counts.

30 Days

Configure Defender for Office 365. Enable Audit Logging.

60 Days

Implement Intune Compliance Policies and App Protection.

90 Days

Roll out Sensitivity Labels and DLP policies.

Questions?

Thank you for your attention.

Ready to secure your Microsoft 365 environment?