Top 10 Security Deployment Actions with Microsoft 365
Take these actions to strengthen security across your users, devices, apps, and data.

1. Identify users
   - Deploy Azure Active Directory and connect to your on-premises directories. Create a single, common identity for each user to provide managed, secure access to all corporate resources.
   - Read the blog >

2. Manage authentication and safeguard access
   - Enable Single Sign-On (SSO) in Azure Active Directory to manage authentication across devices, cloud apps, and on-premises apps. Then set up Multi-Factor Authentication to authenticate user sign-ons through a mobile app, phone call, or SMS.
   - Read the blog >

3. Protect your identities
   - Define security policies to protect individual user identities against account compromise in real time with Azure Active Directory Identity Protection. Manage, control, and monitor privileged access permissions to protect your organization with Azure AD Privileged Identity Management.
   - Read the blog >

4. Set conditional access policies
   - Restrict or block user access based on risk, location, device information, apps, and other user behaviors with Conditional Access.
   - Read the blog >

5. Set up Mobile Device Management
   - Deploy Intune to manage and secure company and employee-owned devices (BYOD).
   - Read the blog >

6. Manage mobile apps
   - Deploy Intune App protection policies on all devices in Intune to control how data is used in mobile apps.
   - Read the blog >

7. Discover Shadow IT
   - Discover apps in use, assess risk, identify vulnerabilities, and take action with Microsoft Cloud App Security.
   - Read the blog >

8. Protect your documents and email
   - Configure Azure Information Protection policies to classify, label, and encrypt documents and email. Then configure Office Advanced Threat Protection to protect your email against all known and unknown malicious links and malware.
   - Read the blog >

9. Protect your OS
   - Microsoft Defender Advanced Threat Protection is built into Windows 10 and provides instant detection and blocking of new and emerging threats.
   - Read the blog >

10. Detect and investigate security incidents
    - Use Azure Advanced Threat Protection to detect suspicious user activity in real time.
    - Read the blog >

Assess & Plan
- Assess your current environment using Microsoft Secure Score, and then plan for success by signing into FastTrack.

Prepare & Educate
- Assemble your core Computer Security Incident Response Team and educate your employees on their role in protecting company assets against security threats.

Monitor & Manage
- Log into the Office 365 Admin Center to access the Office 365 Security + Compliance Center in order to monitor and manage security privacy, compliance controls, and devices.

Learn more at www.microsoft.com/security