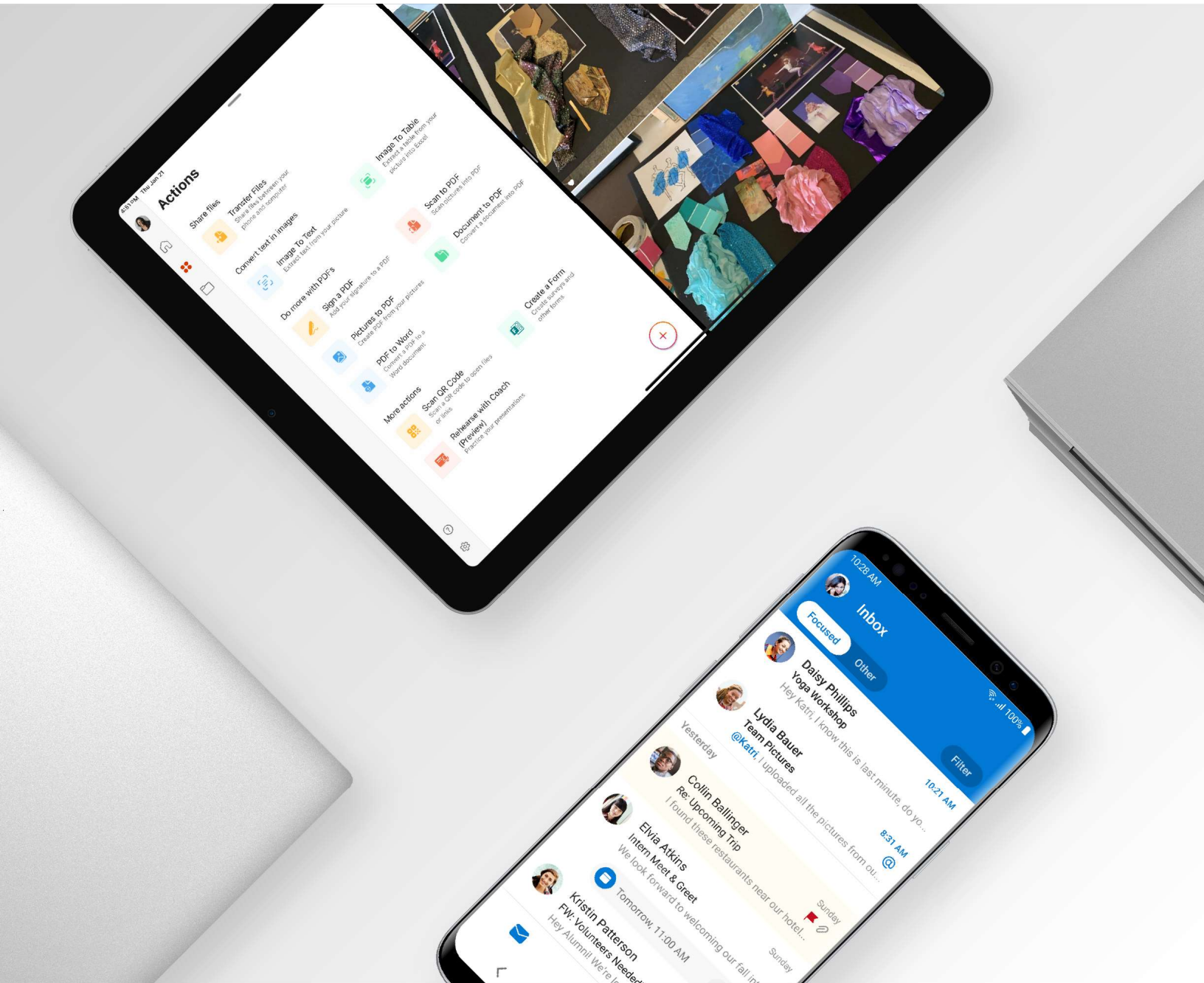
Microsoft

Microsoft 365 mobile apps with Security, Compliance, & Identity

The lowdown of locking down secure mobile productivity



Introduction

Mobile technology has transformed the business landscape. Workers rely on multiple screens to manage work and personal pursuits throughout the day. They are taking Teams calls and web surfing on their phones in the kitchen, reviewing spreadsheets and PowerPoints on tablets at a local cafe, and deftly moving between business and personal projects on their laptops. But as the lines between work and personal use have blurred, new security risks have arisen. The challenge: How can organizations support employees who want to use their mobile devices for both work and personal reasons while securing corporate data?

Users want—and expect—the ability to access their work and personal data anytime, anywhere, on any device, using the apps they know and love. However, the very features that users love also leave devices vulnerable. An SMS (text) or social media posting may include a legit link—or a phishing lure. A free game download in the app store may be malware in disguise. Attackers use these (and other) schemes to get into the user's device in pursuit of the real target: their corporate network.

Security from the ground up

At Microsoft, we spend more than $1 billion per year on cybersecurity research and development. What differentiates Microsoft from other security companies is our approach. We take a truly holistic approach to the technology that safeguards identities, data, applications, and mobile devices end-to-end. The goal: protect sensitive data no matter where it's created, where it lives, or where it travels.

Microsoft 365 was developed with both the mobile-end user and corporate security experience in mind. This combination of Office 365, Windows, security, endpoint management, and enhanced data management incorporates the mobile apps and solutions that are loved by IT, loved by users, and trusted by all. Workers get one-stop shopping for the apps and tools they already know and use daily, tailored to ensure they feel at home on their preferred iOS and Android devices. IT teams value Microsoft 365 for its deep integration with the Azure ecosystem, familiar toolset, and strong security. Plus, Microsoft security intelligence capabilities can be used to accurately identify and evaluate threats captured from user activity.

In the event a threat is identified, the information is extracted and fed in real-time to Microsoft Security teams who use powerful tools including AI, audits, and ediscovery to investigate compromised accounts and help better understand the scope of a breach. Having this broad view of user activity and potential threats enables risk-based assessments for protecting identities, data, applications, and mobile device end-to-end benefits for all users, and protects SMB and enterprise customers.

In this paper, we'll review the critical components of mobile security—identity, device, and data protection—and discuss how Microsoft 365 can help prevent attackers from breaching the network via mobile device usage.

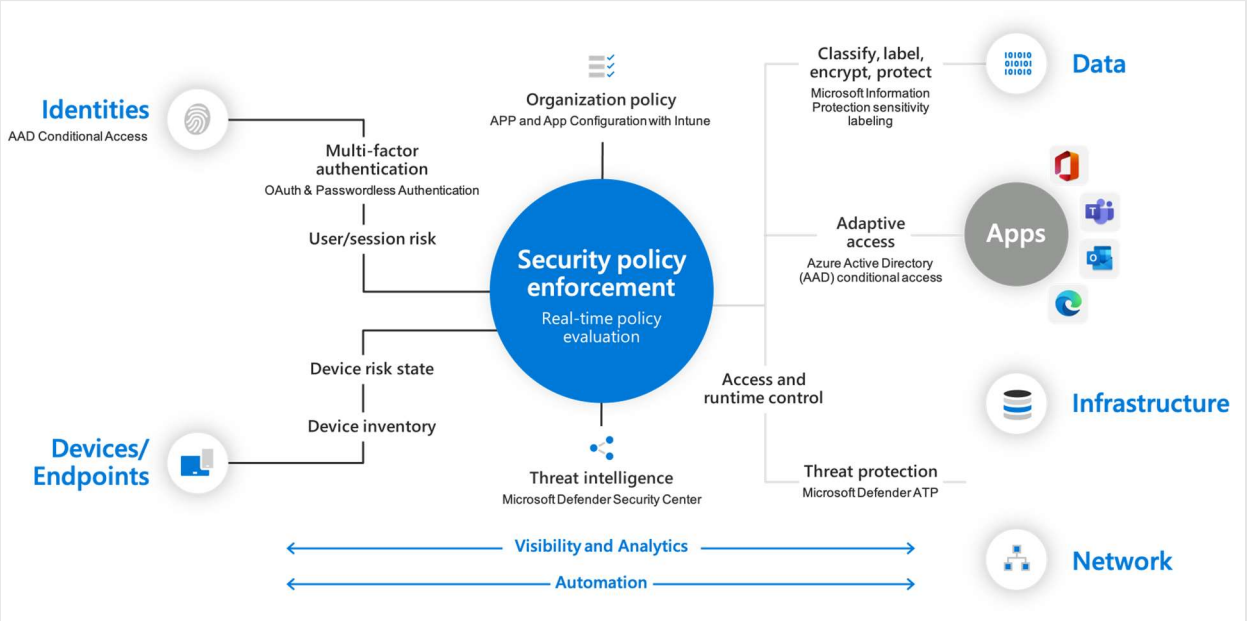


Figure 1: Microsoft Zero Trust architecture

Identity protection

The explosion of iOS and Android devices, apps, and users outside of the corporate network creates identity challenges for today's IT teams. Identity attacks, particularly on mobile devices, are on the rise—yet organizations lack visibility (and control) over their workers' personal devices. The foundation of Microsoft 365 security and compliance is based on user identity; In other words, ensuring that the person accessing corporate data is authorized to do so. Before a user is allowed on the network, they must be authenticated to ensure they are a trusted user. This involves:

- Confirming the user's identity
- Identifying previous network activity (what they have been allowed to do in the past)
- Determining what they've attempted to do (e.g., previous failed authentication attempts)
- Evaluating what they are attempting to do now

Microsoft has been working to develop identity management options that can be plugged into an organization's existing security solution with minimal impact on the end user. In this section, we'll take a brief look at how Microsoft can help organizations manage, strengthen, and simplify users' identity for their mobile workforce.

Implement conditional access policies

Users may try to access corporate resources from anywhere. Therefore, Microsoft recommends moving from a traditional, perimeter-based network defense to an identity-driven security model.

Azure Active Directory Conditional Access policies use a combination of user, location, device, app, and other risk factors to protect Microsoft service endpoints such as Microsoft 365. The policies define which authentication attempts in Azure Active Directory (Azure AD) will be subject to which access controls. For example, organizations can enforce multifactor authentication (MFA) for all users outside the network perimeter or require a password reset if a user's risk level is elevated.

Conditional Access policies also let organizations block email access from undesired apps such as native OS clients, unknown networks, or devices that may be non-compliant with corporate security policies. For example, if a company only allows modern authentication or OAuth, Conditional Access can be used to block Exchange Active Sync (EAS) clients on iOS and Android devices that use basic authentication to access Exchange Online.

Move to passwordless authentication

Passwords have been a staple of identity management for decades—and a common source of vulnerability. End-user fatigue may lead to unsafe practices such as repeating passwords or using ones that are easy to guess. Passwordless authentication methods replace a password requirement with something the user has, plus something they know.

Microsoft offers passwordless authentication options that integrate directly with Azure AD, including the Microsoft Authenticator app. Workers with Android and iOS devices can use biometrics (e.g., their face or thumbprint) to verify their identity through the app. Organizations can also add a secondary verification requirement such as a password, PIN, or time-based, one-time passcode (also known as TOTP or OTP).

As an added benefit, putting workers' identification into Azure AD enables organizations to manage laptop authentication with Windows Hello for Business and FIDO2 security keys (e.g., an external security key or platform key).

Implement endpoint compliance

Organizations are under intense pressure to ensure all mobile devices used to handle company data are secure and compliant. That extends to vendors and service providers hired to assist with projects using their own (or company-owned) mobile devices. Microsoft Endpoint Manager helps organizations modernize IT processes and increase security posture for all devices while utilizing existing technology investment. Endpoint Manager can be used to help onboard PCs, Macs, and mobile devices. Windows Server can be used for security management, device management, and device monitoring on all devices both in the cloud and on-premises. It has built-in integration with Azure Active Directory Conditional Access to verify endpoint compliance status using device, app, and risk-based policies evaluation. The device compliance dashboard helps ensure update readiness, deploying and managing apps, operating system, and software updates, as well as up-to-date security and compliance policies.

For more information

For more information about identity management, please see these resources:

→ Azure Active Directory Universal identity and access management solution

→ Azure Active Directory Identity Protection

→ Identity and device access configurations

→ Endpoint Manager Compliance Policies

Device protection

Personal phones and tablets are more than productivity devices; they entertain, inform, and connect people to each other. Allowing workers to use personal mobile devices and protecting the network are not mutually exclusive goals; with the right apps, both can be achieved. Microsoft provides protection on the mobile apps that users already know and love, including Edge and Office, so workers can enjoy everything mobile has to offer while minimizing their device's vulnerability to attack. In this section, we'll take a brief look at how Microsoft can help ensure workers' devices will be protected.

Deliver protected mobile experiences

Microsoft Endpoint Manager, which includes Microsoft Intune, is a unified endpoint management solution that provides the tools required to securely support employees who want to work on the devices and apps they choose. There are multiple ways of managing mobile devices and apps. These include mobile device management (MDM), which allows configuration and compliance for the entire device and requires device enrollment and mobile application management (MAM), which applies data protection controls on applications to protect the corporate data on personal (non-corporate-owned) or corporate-owned devices.

Intune's MAM solution includes mobile app protection policies (APP) and app configuration settings and may be deployed with or without device enrollment (MDM). The primary difference: MDM ensures the device is managed and compliant, while the APP solution focuses on ensuring compliance with respect to the data. A fuller scope of APP capabilities also includes enabling data transfer, encryption, access, and conditional launch capabilities.

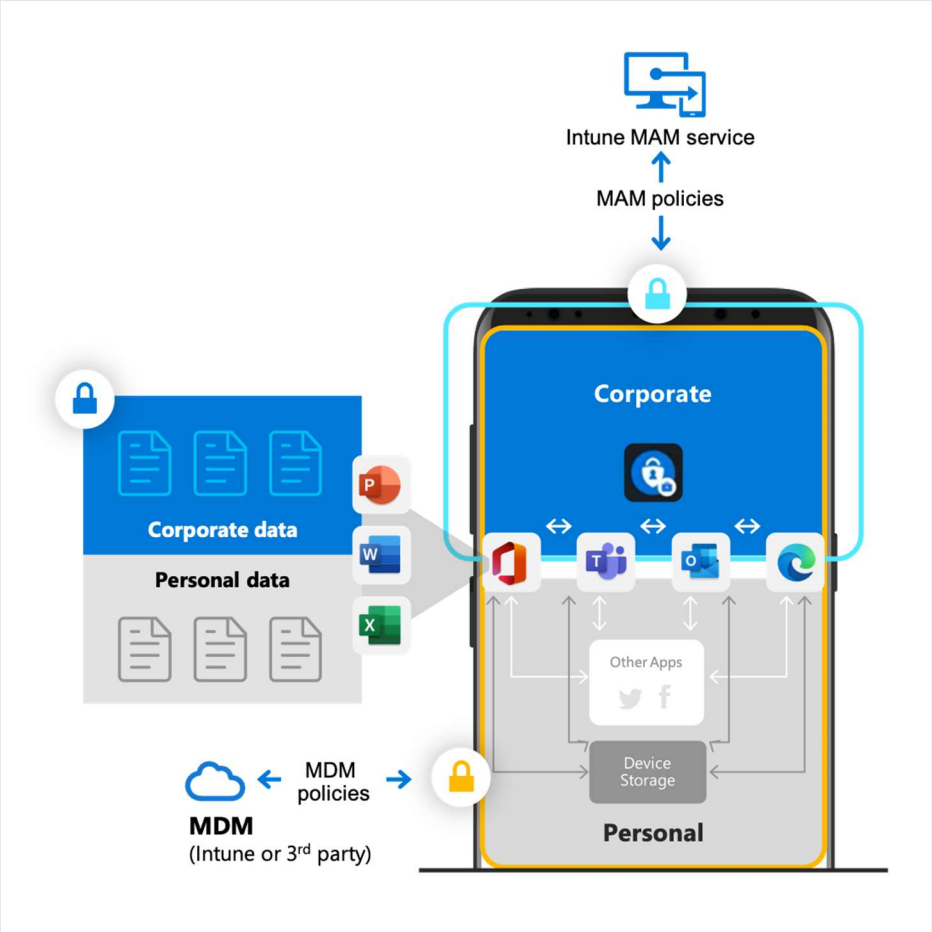


Figure 2: Sample device showing corporate and personal profiles

For Android device users, Intune supports the configuration of Android Enterprise work and personal containers enabling both personal and corporate-owned devices to be configured with a set of features and services that separate personal apps and data from work apps and data. The work profile can be set-up with Intune and Azure Active Directory (using an Active Directory join) with IT administrators making the determinations regarding what apps will be allowed and how they will be configured by way of enrollment options for managing device, data and app security. When work profile authorized apps are configured and installed, they are easily identified by a lock icon such as for Microsoft Authenticator. Note that Intune only manages the corporate apps and data, the user is responsible for managing the personal side of the device and personal profile which are not accessible by corporate IT. Admins should be aware that Android Enterprise devices aren't preconfigured for capabilities such as forcing the user to encrypt so utilizing Conditional Access policies and compliance settings to protect organizational resources is highly recommended.

Companies can use app protection policies with or without MDM. For example, consider an employee who uses both a company-issued phone and their own personal tablet for work. The corporate asset (phone) would be enrolled in MDM and protected by app protection policies. The

personal device (tablet) would be protected solely by app protection policies. On either device, the employee would login to access work data using the same Azure AD credentials and the right set of policies will be applied based on IT configuration.

Endpoint protection for mobile device users

Microsoft Defender ATP helps protect personal devices against malware and phishing attacks by blocking unsafe connections, scanning for malware, and blocking access to sensitive data on both enrolled and unenrolled devices. In addition, it offers a unified security experience through the Microsoft Defender Security Center, where security teams can get a centralized view of alerts, incidents, and the additional context required to remediate threats across all endpoints. It is now available for both Android and iOS devices.

Implement best practices

It is critical that all companies, vendors, and service providers clearly define and enforce device policies for enrolled devices or workers who opt to use personal devices for work. Organizations can use Microsoft Defender ATP to configure anti-phishing policies to protect devices. This policy also includes anti-impersonation settings to protect users and domains. Organizations can also use the spoof intelligence policy to allow (or block) specific spoofed internal and external email senders.

For more information

For more information, please see these resources:

→ Enforce Compliance for Microsoft Defender for Endpoint with Conditional Access in Intune

→ Microsoft Endpoint Manager

→ Android Enterprise Security Configuration Framework

Data protection

Despite efforts to educate and inform, people can (and do) still make mistakes. Organizations can't stop users from surfing the web, texting, or downloading apps. However, it is possible to prevent those bad decisions from becoming a data leak. In this section, we'll take a brief look at how Microsoft can help ensure organizational data will be safe on workers' personal devices.

Implement app protection policies

Workers are multitasking on their devices, managing work, conducting personal business, and enjoying leisure activities. Microsoft recommends implementing Intune app protection policies (APP) to help ensure employees can use their preferred devices to stay productive while preventing accidental (or intentional) data loss. Intune APPs can be used to restrict access to company resources for enrolled—and unenrolled—devices accessing the network. From the end user perspective, they keep using the protected apps just as they always did, comfortable in the knowledge that their data is safe from leaving the corporate environment.

Protect documents in the cloud

Workers may need to share files with clients or vendors outside of the network. OneDrive for Business can help protect data outside the firewall by requiring a password to access a shared link. This prevents unauthorized users from accessing the file in the event the link is intercepted or forwarded. If Microsoft detects a ransomware attack, the OneDrive user will receive an email or notification.

Add protection through data compliance

Microsoft Information Protection (MIP) for Microsoft 365 helps organizations better protect sensitive information across devices, apps, cloud services, and on-premises. MIP provides a consistent and comprehensive approach to discovering, classifying, labeling, and protecting sensitive data to help prevent accidental sharing of sensitive data. The built-in labeling experiences are integrated directly—there's no need for any special plugins or add-ins. And as the experience is consistent across Office apps, it's easy and familiar for users to apply sensitivity labels while working in Microsoft 365 on the Android or iOS device.

For more information

For more information about data protection and classification functionality, please see these resources:

→ Microsoft Information Protection (MIP)

→ Information Protection and Governance

→ Microsoft Intune App lifecycle

→ APP data protection framework

→ Intune App Protection Policies (APP)

→ App Protection Policies for unmanaged devices (iOS, Android)

In conclusion

Personal device use is here to stay—and so are mobile-centric attacks. Combatting these attacks requires planning and vigilance. Organizations can help protect their network by tailoring a security plan that incorporates identity management, device management, and data protection and utilizes the Microsoft apps that are loved by IT, loved by users, and trusted by all.

January 2021