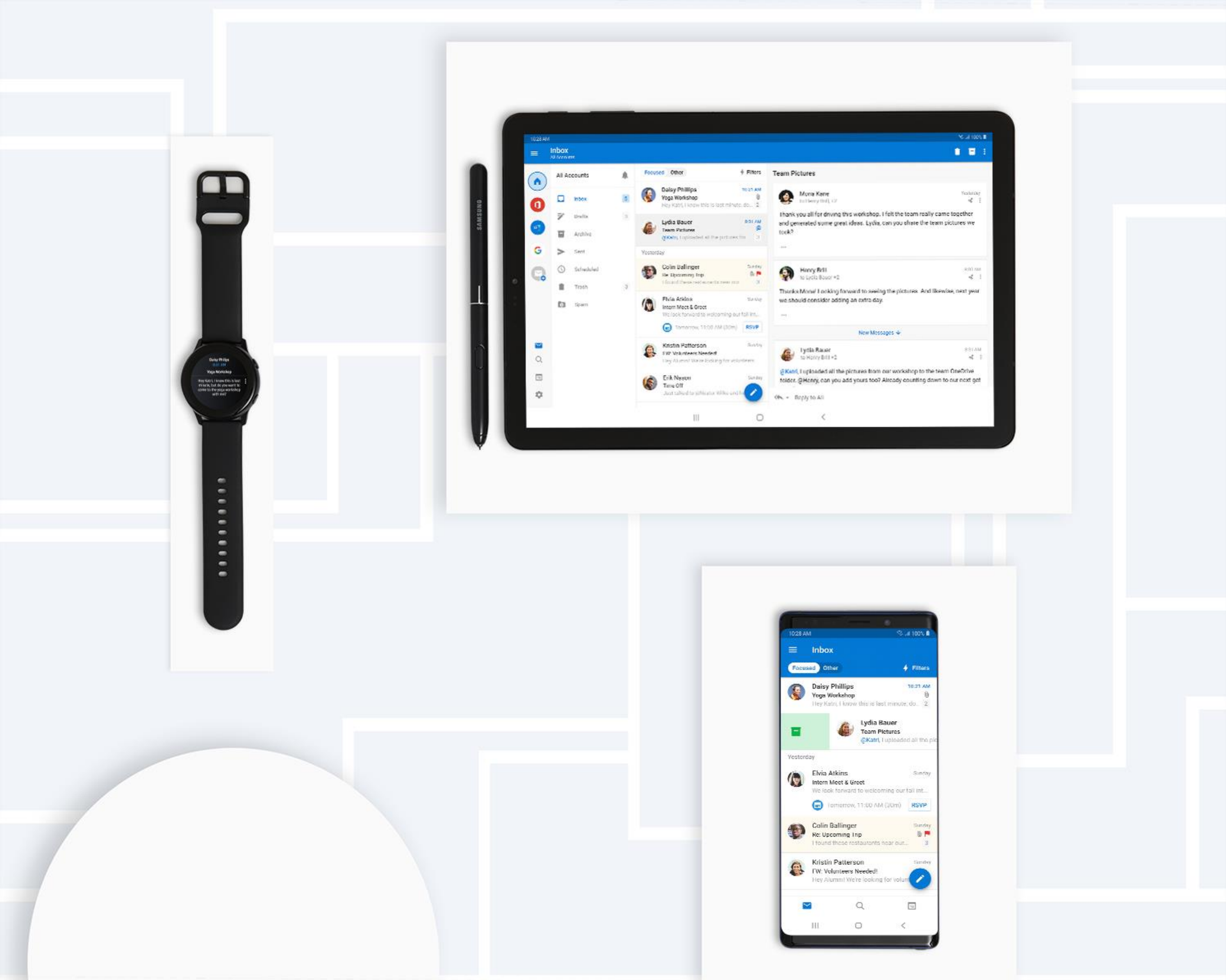
Microsoft

Microsoft 365 Security, Compliance & Identity + Outlook for iOS and Android

A gold standard for secure communications in the enterprise



Protect users on the go

Productivity-on-the-go is the new normal. Your users expect to collaborate and access organizational resources from anywhere, on virtually any device, without impacting their productivity. They schedule meetings from the coffee shop. They communicate with coworkers and friends around the world while standing in line at the grocery. They read email and Word documents on the train to work. The modern workforce's dependency on mobile devices to stay connected and organized has never been stronger. But as the lines between work and personal have blurred, it has also introduced new security risks. The challenge: How do you support employees who want to use their mobile device for both work and personal email and calendar, staying productive and in touch with what's important, while securing corporate data?

Outlook for iOS and Android empowers work and personal productivity on the move while providing companies access to the tools to help keep them secure. Whether your employees work from a personal device or a company-provided one, you can use capabilities built natively into Outlook for iOS and Android, plus solutions provided by Microsoft 365, to safeguard them and your organization's digital information. Device enrollment is not required for most scenarios, so you can support bring-you-own-device (BYOD) practices.

Microsoft 365 Security, Compliance and Identity solutions and Outlook mobile provide the following solutions to help you meet internal security needs and external compliance requirements:

- Identity and access management to help you secure your identities
- Unified endpoint management to deliver protected experiences on any device
- Information protection to protect your sensitive information in transit and at rest
- Threat protection to detect and investigate advanced threats, compromised identities, and malicious actions

In the following pages we provide an overview of how each of these key elements work with Outlook for iOS and Android. From real-time control over access to Exchange mailboxes, to policies that govern how data can flow between apps, to sensitivity labeling and protection templates, we provide tools to help you better protect your organization and improve productivity. Together, these capabilities establish Outlook mobile as a gold standard for communications and personal productivity in the enterprise.

Security from the ground up

At Microsoft, we spend over $1B every year on cybersecurity research and development. What makes Microsoft so different from other cloud providers—and even other security providers—is our people and our cloud intelligence. We have over 3,500 security professionals protecting our customers, and we derive intelligence from trillions of threat signals from around the globe. We can help you make smarter decisions and remediate faster.

We take a truly holistic approach to the technology that safeguards identities, data, applications, and devices across on-premises, cloud, and mobile end-to-end. The goal is to protect your sensitive data, no matter where it's created, where it lives, or where it travels. To defend Outlook, we run Exchange Online on Windows 2019 Server Core to reduce attack surface area. We automate deployment and management to remove errors, and we continuously run attack simulations to probe for weaknesses. We even think about how to protect your data from our own engineers. If a service engineer needs personal identifying information (PII) access to debug your issue, they must request just-in-time, limited access that is approved through a management chain with business justification. Once access is granted, it will only last long enough for the engineer to do their job. You can insert yourself into that process, too. In Exchange Online, our engineers have no standing admin access to any of our systems. This is all independently audited, so you don't have to take our word for it.

We protect your server data, while respecting geographic specific restrictions, by maintaining multiple copies of your data across multiple worldwide datacenters with server and database redundancy. We have built incredibly sophisticated management systems to manage our infrastructure and operate a DevOps model. Our engineering team have a real sense of ownership and pride in the code that runs on thousands of servers.

Protection built into Outlook

Outlook for iOS and Android is built on the Microsoft cloud utilizing the native Microsoft sync technology for data synchronization, connecting directly to the Exchange Online back end.

This means that all Office 365 Enterprise, Government, Business, and Education accounts are supported natively, and mailbox data is not cached outside of Office 365. Data simply stays in its current Exchange Online mailbox. Your email is protected by TLS-secured connections between Office 365 and the Outlook app. This architecture respects locality and regionality promises for data to stay in the region in which the tenant is located. It also means that customers with the highest level of security requirements, such as the Department of Defense, can trust Outlook mobile for their email and calendar needs.

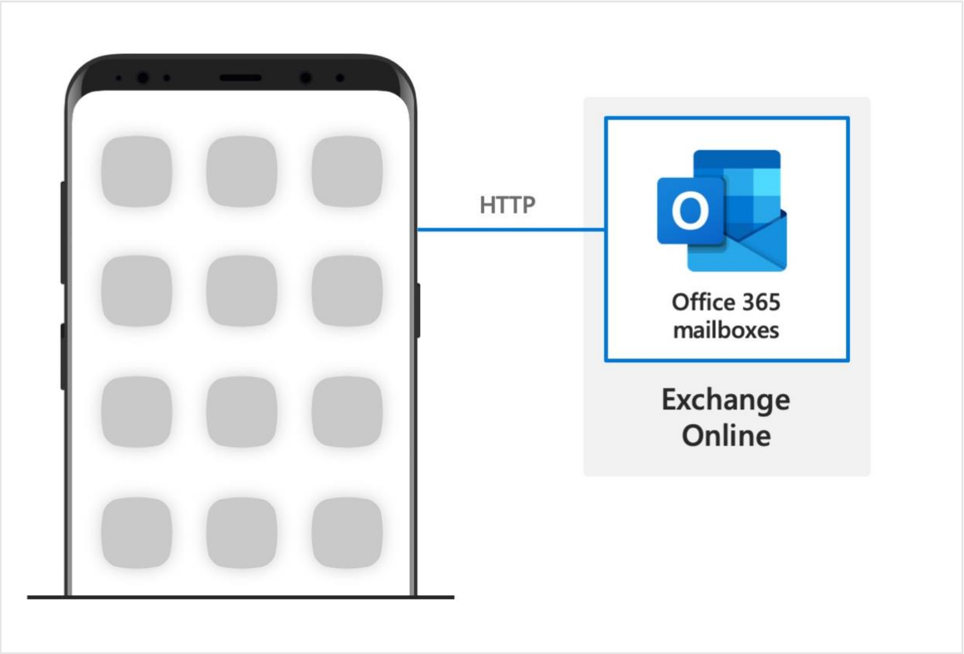


Figure 1: Outlook for iOS and Android connects directly with Exchange

Secure and manage your identities

With users accessing your resources from anywhere, it's critical to move from a traditional, perimeter-based network defense to an identity-drive security model. Integrated with Office 365, Azure Active Directory (Azure AD) is a universal identity and access management solution that simplifies user access and helps you protect and govern your users. Users easily sign in, using a single identity, to Outlook, Office 365, and thousands of on-premises cloud apps. You can safeguard their credentials by enforcing strong authentication and conditional access policies. Azure AD also provides tools to ensure that the right people have the right access to the right resources.

To give your users easy access to your cloud apps, Azure AD supports a broad variety of authentication protocols, including legacy authentication. However, legacy protocols don't support multi-factor authentication (MFA). MFA requires at least two forms of authentication, such as a 6-digit PIN plus a known mobile device. We recommend that all our customers implement MFA to address identity theft. You can use Azure AD to block clients that leverage legacy authentication from connecting to Exchange Online. This is an important part of improving tenant protection.

Outlook mobile and Azure AD use modern authentication (OAuth) which simplifies the initial account set up for users when they first install Outlook for iOS or Android. It also protects their user credentials. At sign-in, users authenticate directly against the identity platform and receive an access token in return. This grants Outlook for iOS and

Android access to the user's mailbox or files. At no time does the service have access to the user's password in any form.

Azure AD Conditional Access policies use a combination of user, location, device, app, and other risk factors to protect Microsoft service endpoints, like Office 365. The policies define which authentication attempts in Azure AD will be subject to which access controls. For example, you can enforce MFA for all users outside your network perimeter or you can require a password reset if a user risk level is elevated.

Conditional Access policies also let you 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 your company only allows 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.

Deliver protected mobile experiences

Microsoft Intune (Intune) is a unified endpoint management solution that gives you tools to securely support employees who want to work on the devices and apps they choose. It provides two means for managing mobile devices and apps, mobile device management (MDM) and mobile application management (MAM). MDM and MAM are not mutually exclusive of each other—they can be used together or separately.

MDM requires device enrollment, which enables inventory (e.g., apps installed), configuration (e.g., provisioning, certificates, profiles, etc.), reporting, device compliance measurement, and wipe capabilities in the event corporate data needs to be removed from the device.

MAM solutions enable app publishing, app inventory/usage, app management, data protection within the app, and the ability to remove corporate data from the apps. The primary difference between MDM and MAM is that MDM ensures the device is managed and compliant, while MAM solutions focus on ensuring compliance with respect to the data. Intune's MAM solution includes app protection policies and app configuration settings.

Companies can use app protection policies with or without MDM. For example, consider an employee that uses both a phone issued by the company, and their own personal tablet. The company phone is enrolled in MDM and protected by app protection policies while the personal device is protected by app protection policies only.

The below illustration shows the layers of protection that MDM and app protection policies offer together.

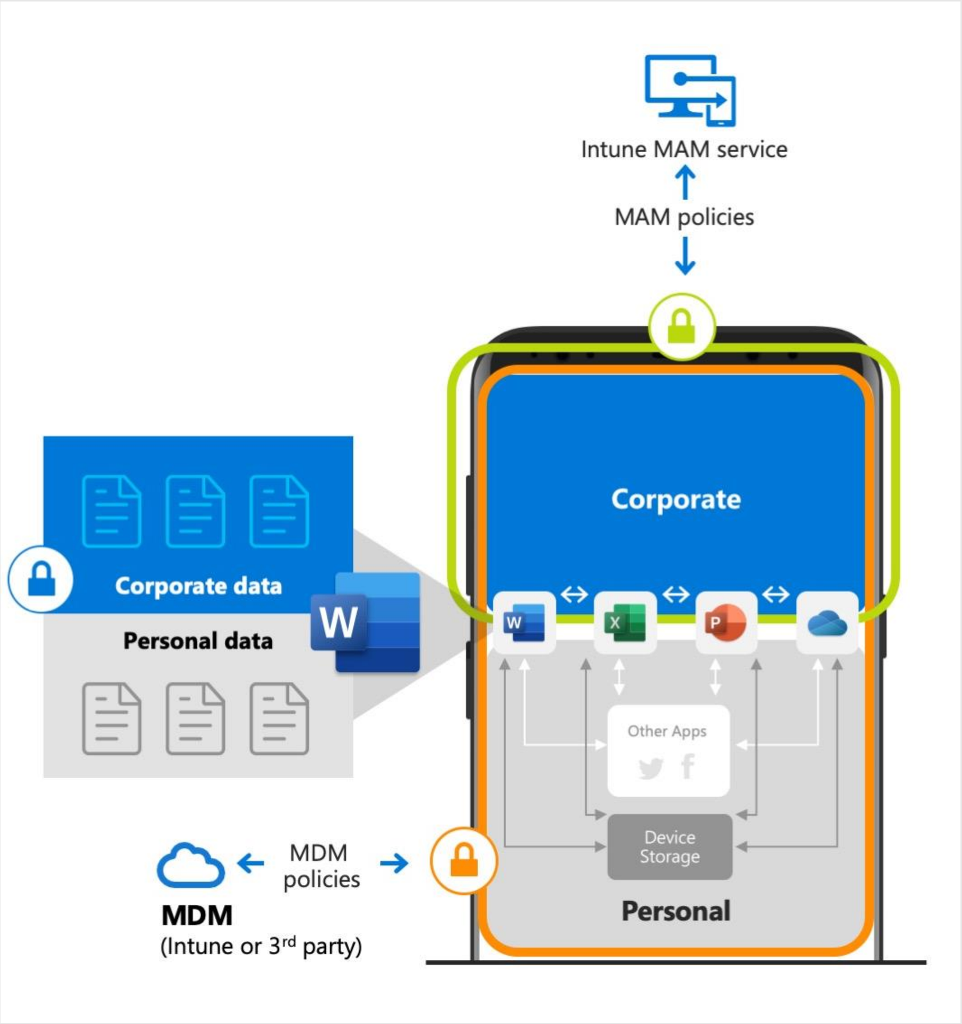


Figure 2: MDM and MAM can be used together or separately

The MDM solution adds value by providing the following:

- Enrolls the device
- Preinstalls apps to the device
- Provides ongoing device compliance and management

The app protection policies add value by providing the following:

- Help protect company data from leaking to consumer apps and services
- Apply restrictions like save-as, clipboard, or PIN to client apps
- Wipe company data when needed from apps without removing those apps from the device

The following diagram illustrates how the data protection policies work at the app level without MDM.

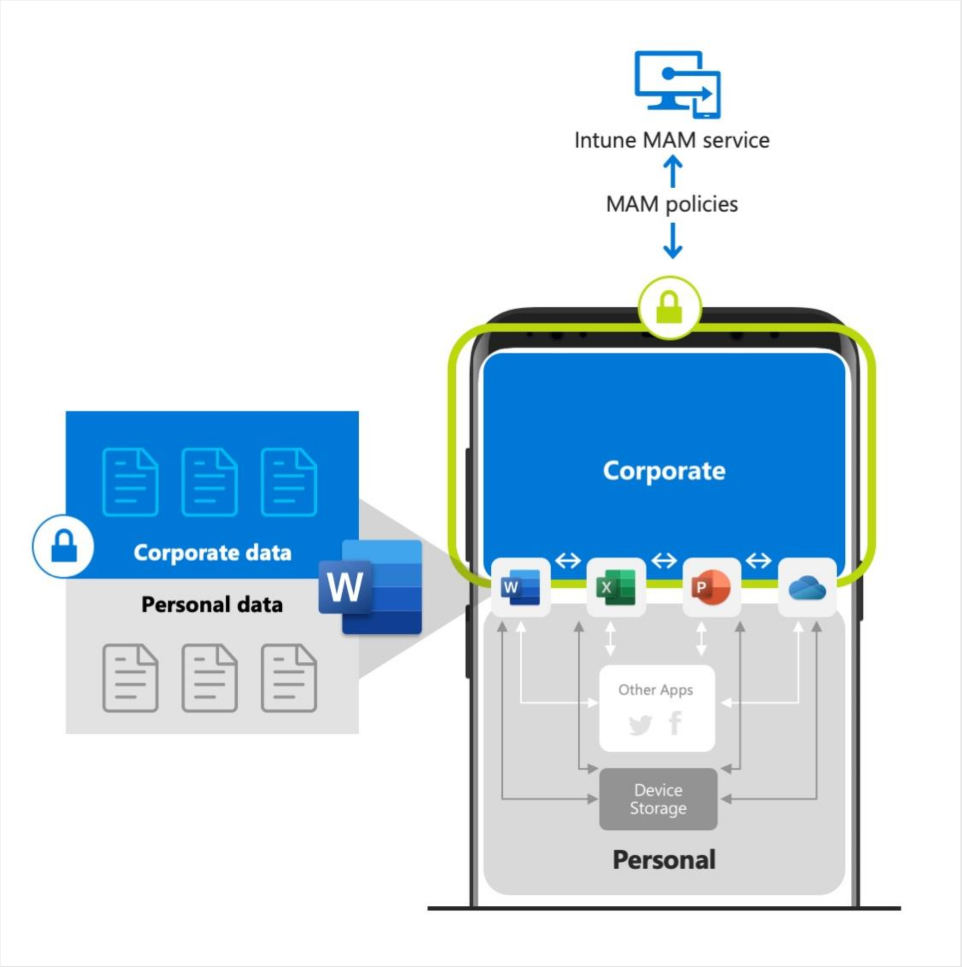


Figure 3: App protection policies provide app level protection

For BYOD devices not enrolled in any MDM solution, app protection policies can help protect company data at the app level. However, there are some limitations to be aware of, such as:

- You can't deploy apps to the device. The end user has to get the apps from the store.
- You can't provision certificate profiles on these devices.
- You can't provision company Wi-Fi and VPN settings on these devices.

Safeguard data, with or without mobile enrollment

Intune app protection policies help ensure an organization's data remains safe or contained in a managed app. The policy is applied to the identity and any content associated with that identity within the targeted app. The targeted app is commonly referred to as a managed app, which is nothing more than an app that has integrated the Intune SDK and supports the app protection policy framework, such as Outlook for iOS and Android. User productivity isn't affected, and app protection policies don't apply when using the app in a personal context. The policies are applied only in a work context, which gives IT the ability to protect company data without touching personal data. App protection policies ensure that the app-layer protections are in place.

There are three categories of policy settings: conditional launch, access requirements, and data protection. For example, with conditional launch you can define what happens if the user jailbreaks or roots the device by blocking access or wiping the data; with access requirements, you can require a PIN to access the work data; and with data protection, you control the sharing of the work data between the managed apps, like Outlook mobile, and non-managed personal apps. You can also define whether the work data can be saved to other storage locations.

In the case of Outlook mobile, with the built in SDK, app protection policies can be applied so that administrators can block users from copying and pasting or saving files and data from their company (email) account to personal storage location. Further, they can prevent users from creating a calendar event in their Office 365 and then switch it to personal calendar, or block users from sending company email and data from a personal account.

Because mobile app management doesn't require device management, you can protect company data on both managed and unmanaged devices. The management is centered on the user identity, which removes the requirement for device management.

App configuration for Outlook mobile

Outlook for iOS and Android offers administrators the ability to customize the default configuration for several in-app settings. This capability is offered for both MDM enrolled devices and for devices that are not enrolled if Outlook for iOS and Android has an Intune app protection policy applied. Block external images is just one app configuration setting that can be set by administrators and pushed to Outlook for iOS and Android. We also give control to administrators through Intune app protection policies to configure the on/off state for saving contacts, iOS biometrics options such as Touch ID/Face ID and the external recipient MailTip.

Users are also made aware of what is protected through subtle user interface clues to provide a greater sense of security. For example, Outlook mobile provides warnings or tips in the app if recipients in the email address are external to their organization. When composing or replying to a message with external recipients using Outlook for iOS and Android, the external recipient email address is highlighted in the address list as well as in the body of the message if @mentioned. A small notice label is visible in the message header during the compose or reply process and is not visible by the external recipients once sent. You can also manage advanced configurations, such as notifications, contact sync, and wearables.

These configurations policies can be set, either at initial onboarding or anytime administrators want to standardize the Outlook mobile experience for their users. Many settings such as Focused Inbox can also be managed by administrators or adjusted by the user.

Govern and protect your sensitive emails

Microsoft Information Protection solutions help you better protect your sensitive information across devices, apps, cloud services, and on-premises. Microsoft Information Protection provides a consistent and comprehensive approach to discovering, classifying, labeling, and protecting sensitive data to help you meet the internal and external requirements to which you are subject. Outlook for iOS and Android supports the ability for users to classify and easily apply sensitivity labels to email based on the policies defined by your organization or required by regulators. The built-in labeling experiences are integrated directly—there's no need for any special plugins or add-ins.

Since the experience is consistent across Office apps, it's easy and familiar for users to apply sensitivity labels while working in Outlook mobile. Users can help manage and control information, without inhibiting productivity. Based on the label policies defined by the organization, the appropriate controls and restrictions are enforced on sensitive emails. For example, you can configure higher sensitivity levels to enforce protection settings such as encryption and rights restrictions, and lower sensitivity settings to display visual markings (i.e. headers), or no protection at all.

For example, if one of your employees uses Outlook mobile to send secret company information to a coworker, the user can select the sensitivity label, "Highly Confidential," for the email. Based on the company's label policies, this can apply encryption and rights restrictions to the email as the message moves though the Exchange Online transport system. In this example the policies prevent external users from reading the messages.

→ You can learn more about sensitivity labeling in our documentation.

Detect and investigate advanced threats

Email continues to be a primary attack vector for compromises. Phishing and other email-based threats increase in both volume and sophistication every year. Office 365 Advanced Threat Protection (Office 365 ATP) helps protect against sophisticated threats hidden in email attachments and links.

Email and documents that pass through Office 365 are detonated and assessed for validity. Detonation is a machine automated scan of the message and attachments, where items that have known attacks are blocked, and items that have suspicious elements are moved to the user's Junk Mail folder. This redirection means that while the message gets delivered (in case it's not actually malicious) the user must take an active action to retrieve the message. However, they don't need to log a ticket with support. The company is protected from unsafe emails, without disrupting user productivity.

Outlook is designed to give users time back

Mobile workers spend an increasing amount of time working on their phones, and mobile devices are now an integral part of business. People depend on their phones to help them work, and they also use mobile tools to manage their personal lives. Security is vital, but protection policies won't work if they slow users down. To safeguard your organization, you must provide easy-to-use tools that unlock productivity, while applying strong security controls.

Outlook mobile is designed with security as a principle, not a nice-to-have. We know that experiences that do not put users at the center will lead to non-secure work arounds. All our experiences, even the security ones, are crafted with care. We created Outlook with a simple and powerful design that drives productivity. It was designed with the goal of helping users get things done in under 22 seconds so they can focus on what's important.

Outlook supports multiple accounts to allow users to manage all their commitments and keep life organized. They can access emails and integrated calendars across both work and personal accounts—all from one location. Built-in integration with Office 365 provides access to familiar tools on the go. By leveraging services such as the Office Graph, Outlook surfaces information to users that connect them to the people that help them get things done and stay on top of their work and personal life.

> "Some serious effort has gone into the design of Outlook for Android and iOS, with event pages showing locations, attendees, and all the other key information in a refreshingly simple and smart way."
>
> **Gizmodo**

Our user centric design approach extends to the security and compliance experiences on Outlook mobile. Azure AD integration makes sign-in fast and simple, reducing user frustration. For companies that allow both personal and work accounts on the same device, we provide capabilities and protection policies that help separate and manage company data while respecting personal privacy concerns.

Many security features are invisible to users. For example, if a user adds a link to an email in Outlook mobile via the OneDrive integration, the sharing permissions established by administrators at the tenant level are applied by default. When saving an email attachment to the cloud or locally on the mobile device, Outlook mobile respects the policies that define safe locations and blocks others. Users don't have to wonder if they are compliant when they share content through Outlook.

Outlook mobile and Microsoft 365 empower employees to stay connected and organized on the go. At the same time, it provides advanced protection against threats and keeps them in compliance with your organization's policies. Often, users don't even notice the security controls. You gain peace of mind, and users can quickly get back to living their lives outside their inbox.

Preparing for tomorrow's challenges

As the mobile and security landscape evolves, we will continue to enhance Outlook for iOS and Android and Microsoft 365 security and compliance solutions. Despite the full portfolio of capabilities we've built into Outlook mobile, we know we're not done. Our product roadmap is informed by customer feedback. We also anticipate what tools you will need to address the ever-changing conditions of our global environment and regulations.

These are just a few security and compliance capabilities that are being planned for Outlook for iOS and Android:

- Notification protection: Administrators will be able to set app protection policies that require sensitive data be hidden in email and calendar notifications. This way, if a mobile device is left unattended or exposed inadvertently, sensitive information won't be visible until the authorized user unlocks the device. This policy will be managed through app protection policies and won't require device enrollment.
- We are working on updating the user experience in Outlook for iOS and Android to further delineate experiences between work and personal accounts and contacts. For example, when you are addressing work related emails, we can suggest your work contacts and hide your personal ones by default. We will also provide visual cues for events and meetings that are set from a personal account to help protect user privacy and further secure company data.
- User will be able to report emails suspected of phishing or spam directly from the app

- We recognize the need to enable Office 365 Data Loss Prevention (DLP) to block sharing of sensitive information in Outlook mobile. To help prevent oversharing of information both inside and external to your company domain, we are exploring the option of adding DLP policies to email in Exchange Online to automatically inspect the content of emails and attachments. If sensitive data is detected—based on your organization's policies—the email would be blocked and/or a notification sent indicating that there has been a policy violation. For example, you could set credit card information as sensitive information. If a user uses Outlook mobile to send an important email to a vendor and includes a credit card number in the email, this information would be detected by DLP policies, and the email blocked while in transit. Both the sender and your IT administrator would receive a notification that the email was not delivered due to policy. Security admins would have flexibility to define the types of data to detect, the target users or groups, and the enforcement actions to apply.
- We are working on adding a QR code to Outlook on the web, Outlook for Windows, and Outlook for Mac for users who are not using Outlook mobile as their secure mobile email and calendar app. This code could ease deployment of Outlook mobile for administrators by simplifying the app download, account authentication, and sign-in process for Outlook for iOS and Android on unenrolled devices.
- Microsoft recently introduced a new program in the security and compliance center called Secure Score. Secure Score gives you visibility into potential vulnerabilities in your environment across a multitude of controls. We are working toward adding controls to this program that address the security and compliance requirements for mobile email and calendaring.
- Office 365 Message Encryption enables users to apply protection templates to sensitive emails. This includes encryption, identity, and authorization policies to help secure your email on Outlook for Windows, Outlook for Mac, and Outlook on the web. We are evaluating customer feedback to determine whether to also add Message Encryption to Outlook for iOS and Android.

We aim to give Microsoft customers a deeper understanding of how Outlook for iOS and Android with Microsoft security and compliance solutions can mitigate against risks. With a complete suite of solutions, increased visibility, and tools to identify the areas of risk associated with providing access to unsecure mobile email and calendar apps, we are confident customers will realize that Outlook mobile is safe for the modern workplace, designed to unleash productivity, and is a gold standard for secure communications in the enterprise.