Microsoft Enterprise Mobility

Architecture matters. That's why our enterprise mobility solutions are designed to run in the cloud and work with your existing on-premises infrastructure.

Our cloud-first approach to managing a mobile enterprise is the fastest, most cost effective way to meet new business challenges and accommodate new devices, new apps, and new hires—without worrying about scale, maintenance, or updates.

Why you'll love it

It protects Office better
It's the only solution designed to protect your Microsoft Office email, files, and apps

It saves you money
Up to 50% less than the cost of buying standalone solutions from other vendors

It just works
Simple to set up, always up to date, and connects to your existing on-premises resources

It's integrated
One identity platform protects them all—users, devices, apps, and data

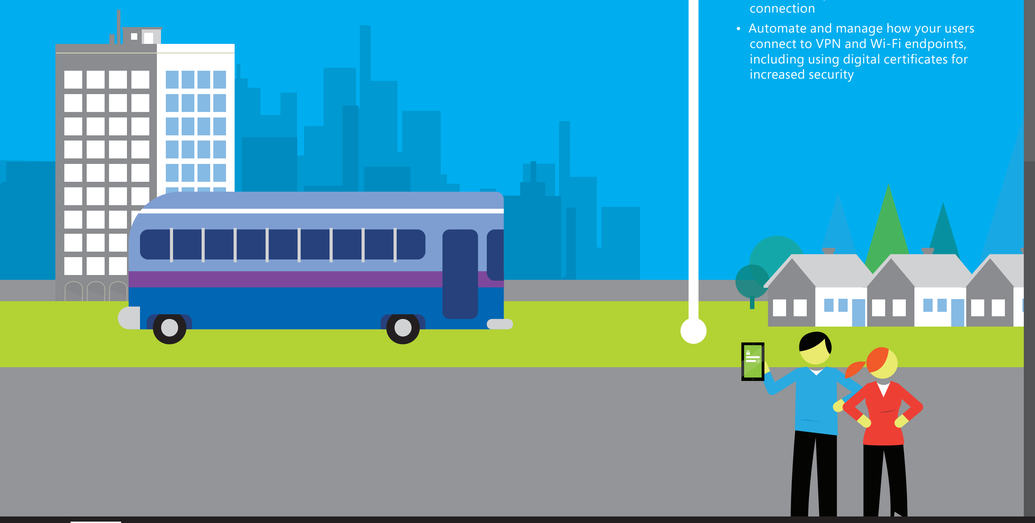
It's comprehensive
Data protection support for Android, iOS, Mac OS, Windows, and Windows mobile devices, including over 2,500 popular SaaS apps

Identify security risks
Identify breaches and threats using behavioral analysis to provide clear, actionable reports

Work anywhere

Your users want to work from home, on the road, or wherever the mood strikes. Give them the tools they need to be productive and safely access corporate resources from anywhere—using any device.

- We support Android, iOS, Mac OS, Windows, and Windows mobile devices
- Our datacenters are deployed globally and are always available
- No matter where your users work or live, they have "local" access to their productivity, identity, and management services—anywhere there's an Internet connection
- Automate and manage how your users connect to VPN and Wi-Fi endpoints, including using digital certificates for increased security



Cloud

SAAS APPS

Deploy native public and internal LOB apps

Enforce app restrictions with Mobile Application Manager

SHAREPOINT EXCHANGE

OFFICE 365

Conditional access

Integration with Office 365

MICROSOFT INTUNE

Mobile Device Management

Mobile Application Management

AZURE REMOTEAPP

AZURE RIGHTS MANAGEMENT

MULTI-FACTOR AUTHENTICATION

AZURE ACTIVE DIRECTORY

AZURE ACTIVE DIRECTORY APPLICATION PROXY

Email protection using Azure RMS

Protection embedded in document

AZURE RMS PROTECTED DOCUMENT

Conditional access

FIREWALL

AZURE ACTIVE DIRECTORY CONNECT

EXCHANGE

Integration with System Center Configuration Manager

WEB APPLICATION PROXY

REMOTE DESKTOP SERVICES

RIGHTS MANAGEMENT CONNECTOR

Document protected on-premises

Leverages Azure RMS templates

ON-PREMISES DIRECTORY SERVICES

WORKSTATION CLIENTS

SYSTEM CENTER CONFIGURATION MANAGER

DESKTOP VIRTUALIZATION

EXCHANGE

WORKSTATION CLIENT

ATA Gateway

ATA Center

Detect threats with Behavioral Analytics

Recommendations for investigation and remediation for suspicious activities

Reduce false positives

Identity

Single sign-on to thousands of popular, preintegrated SaaS apps, such as Salesforce, Concur, and Office 365. Single sign-on and directory synchronization extend your directory services to the cloud and provide your users with a high-fidelity authentication experience.

- Multi-factor authentication offers better security of your corporate resources by requiring additional verification from users beyond their usernames and passwords
- Users access both cloud and on-premises resources with their existing on-premises credentials
- Self-service management features allow users to reset passwords, lock, or wipe their mobile devices

Devices

Connect your existing on-premises resources, such as Microsoft Exchange and SharePoint servers, to leverage the power of cloud services.

- Tight integration of Intune and System Center Configuration Manager helps you virtually manage devices and PCs from a single management console
- Conditional email access to your mailboxes hosted on Exchange Server or Exchange Online, as well as access to SharePoint Online
- Mobile Application Management separates your corporate apps and data from users' personal apps and data and enforces security policies on corporate resources

Apps

Stream applications from on-premises or the cloud to keep users productive anywhere, on any device, and your company data more secure.

- Session-based desktops and Azure RemoteApp offer a scalable platform that delivers your corporate applications simply and cost effectively
- Users install Microsoft Remote Desktop clients and run personal virtual desktops and apps on their laptops, tablets, or phones and stay productive on the go
- Pooled virtual desktops on Azure scale up or down to meet dynamic business needs

Security

Deploy and configure access to corporate resources across your on-premises environment and cloud applications while helping to protect corporate data. You remain in control of your data, even when it is shared with others.

- Encryption policy at the file level follows documents inside and outside of your organization
- Collaborate more securely by protecting any file type on any device platform using Azure Rights Management
- Safely share files in email or use your favorite cloud storage service, such as Microsoft OneDrive or Dropbox

On-premises

Like it? Get it.
www.microsoft.com/ems

© 2015 Microsoft Corporation. All rights reserved.

Version 2.0 Created by the Enterprise Mobility Team Email: EMSPoster@microsoft.com

Microsoft