THE PARTNER MASTERS

Endpoint Management with Security Workshop

After the workshop, you'll…

Improve your knowledge of cloud-based device management and security using Microsoft solutions

Have a better understanding of Microsoft Intune, Azure AD and Microsoft Defender for Endpoint capabilities

Accelerate your endpoint management and identity protection journey with Microsoft

Have defined next steps based on your needs and objectives

THE PARTNER MASTERS

Endpoint Management with Security Workshop overview

Designed as a four-day engagement, the Endpoint Management with Security Workshop enables partners to lead customer conversations around modernizing their endpoint management and security capabilities by leveraging Microsoft 365. By making use of **Microsoft Intune, Intune with Tenant Attach, Azure Active Directory, Defender for Endpoint, Autopilot,** and **Endpoint analytics**, this workshop gives customers visibility into their IT estate and will help define clear next steps and the best ways to manage and secure endpoints at the enterprise level.

Audience

Customers

Senior BDMs concerned with device lifecycle management, endpoint management, security and TDMs

Partner participants

Consultants, Solution Architects

Workshop

Assess

Pre-engagement and assessment

Pre-Engagement Call – define scope and gather information on current endpoint management and security estate

Identify executive sponsors and business stakeholders

Pre-engagement questionnaire

Present Endpoint Management with Security Overview

Security posture assessment

Art of the Possible

Choose your own adventure

Required modules:

Secure your identities and devices

Simplify IT management with Intune

Upgrade to Windows 11

Optional modules: Microsoft Edge, Analytics and Reporting, Microsoft Devices, Intune for Education, MDM Migration and Advanced Management Solutions

Build the Plan

Create a strategy

Use the Value Calculator to show the ROI that your customer can achieve by adopting Microsoft 365 solutions

Develop deployment plans based on key results and recommendations

Define next steps

Device lifecycle management with Microsoft Intune

Enroll

Provide specific enrollment methods for iOS/iPadOS, Android, Windows, macOS and Linux

Provide a self-service company portal for users to enroll BYOD devices

Deliver custom terms and conditions at enrollment

Zero-touch provisioning with automated enrollment options for corporate devices

Configure

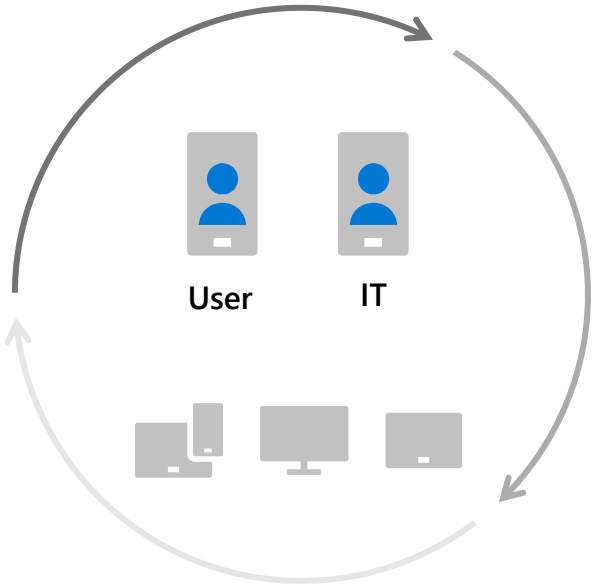
Deploy certificates, email, VPN, and Wi-Fi profiles

Deploy device security policy settings

Install mandatory apps

Deploy device restriction policies

Deploy device feature settings



Support and retire

Revoke access to corporate resources

Perform selective wipe

Audit lost and stolen devices

Retire device

Provide remote assistance

Protect

Restrict access to corporate resources if policies are violated (e.g., jailbroken device) with Conditional Access

Protect corporate data by restricting actions such as copy/cut/paste/save outside of managed app ecosystem

Protect devices from security threats with Microsoft Defender for Endpoint

Report on device and app compliance