Microsoft

SCC

Endpoint Management with Security Workshop

Overview

Technology needs are evolving in the modern workplace

Old world versus new world

Single corporate-owned device	⇋	Multiple BYOD devices and IoT devices
Business owned	⇋	User and business owned
Corporate network and legacy apps	⇋	Cloud managed and SaaS apps
Manual and reactive	⇋	Automated and proactive
Corporate network and firewall	⇋	Expanding perimeters
Employees	⇋	Employees, partners, customers, bots
Mostly onsite employees	⇋	Remote and hybrid environment

Market trends

The world of hybrid work is evolving…

38%

Of people are already hybrid working

52%

Of people are considering a transition to remote or hybrid work

50%

Of people use a personal device for work

And so are the threats and challenges.

83%

Organizations that have experienced at least 1 firmware attack in the past 2 years

25%

Organizations that identified unauthorized access to sensitive data as a top security threat

921

Passwords attacked every second

65% of security decision-makers report that investing in security increases efficiency: it frees up teams to work on other projects, promotes business continuity, and safely enables end-user productivity.

Microsoft Security Signals Research Learnings Report

People are working in more places, with more flexibility and more devices

SCC

And they want answers to these questions:

How do you secure your endpoint estate?

How do you reduce complexity of IT workloads?

How do you ensure protection, while enabling workforce flexibility and productivity?

Technology must keep us connected and productive while reinforcing our security posture in an increasingly sophisticated and complex world.

Do More With Less using Microsoft 365

SCC

Protect the digital worker

Create a secure, flexible work environment anywhere, while improving endpoint visibility.

Reduce security costs with pre-integrated identity, endpoint management & security solutions to advance zero-trust architecture.

Simplify IT management

Automate system updates to reduce cost and optimize IT administration.

Improve IT efficiencies for new devices, apps, and data management.

Eliminate redundant solutions

Consolidate complex licensing structure.

Eliminate redundant capabilities, while benefiting from seamless, native integration.

Azure AD, Defender for Endpoint, Intune and Windows 11: The value of more

Endpoint Management with Security Workshop Overview

An executive deep dive into remote deployment, management and security of corporate and BYOD devices, identities and data in your organization

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

What we'll do during the workshop

Focus on learning about your priorities, initiatives and key influences in your endpoint management and identity protection strategy

Learn how Microsoft Intune supports managing the entire device lifecycle and how Azure AD and Defender for Endpoint secures your data, identities and devices

Work together on showcasing cloud-based endpoint management and protection in your production environment

Plan next steps on how we can work together

Device lifecycle management with Microsoft Intune

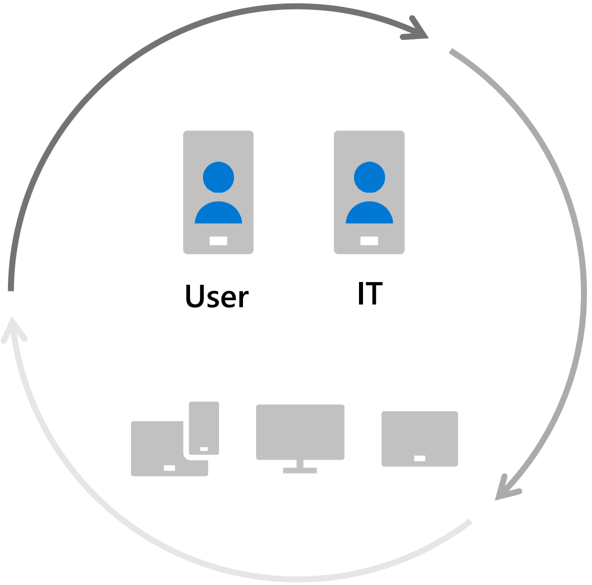
Enroll

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

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

Support and retire

Revoke access to corporate resources

Perform selective wipe

Audit lost and stolen devices

Retire device

Provide remote assistance

Customer benefits of the Endpoint Management with Security Workshop

Today's users are looking for more ways to remain productive while working on any device. 95% of organizations allow personal devices in the workspace while 70 million smartphones are lost every year. With users asking for more ways to work the way that they want, this workshop will show you how to manage and protect both company-owned and user-chosen devices in the cloud and how to secure identities, devices and data in your organization.

This workshop will show you how to leverage intelligent security, risk-based controls, zero-touch provisioning, and advanced analytics to enable cloud management for the devices your users need.

✓ **Learn** how to improve your knowledge of cloud-based device management and security using Microsoft solutions

✓ **Discover and protect** your endpoints by enforcing policies and deploying security tools

✓ **Secure** your identities with multi-factor authentication and conditional access from any device

✓ **Enable** your users to be productive with the applications they need, on the devices they want

Objectives

Discover

Gain visibility into the customer’s endpoint management and security goals and objectives.

Showcase Microsoft Intune, Azure AD and Defender for Endpoint

Present Microsoft Intune, Azure AD and Defender for Endpoint features related to managing the entire device lifecycle and protecting your users, data and devices from anywhere. Enable these features in the customer environment focusing on cloud-only management and protection for selected users and devices.

Define results and next steps

Provide the customer with the results of all activities included in the Endpoint Management with Security Workshop and agree on the next steps that will help the customer to move to a modern management solution based on Microsoft Intune, Azure AD and Microsoft Defender for Endpoint.

Who should attend

IT Management decision makers

C-Suite

Chief Information Security Officer (CISO)

Chief Information Officer (CIO)

Chief Security Officer (CSO)

Endpoint management owners/decision makers

Other roles

IT Security

IT Operations

Security Architect

Security Engineers

Application business owners

Top concerns

Users don’t have the same secure, productive experiences from home as they do from the office.

Modern device management has expanded from desktops and laptops to include all user devices.

Organizations want to ensure that Windows endpoints are up-to-date and secured.

Users want to have access to the latest versions of Office apps on any device.

IT wants to implement policies that enable productivity, but not at the expense of company security.

BYOD is common with remote workers; these devices need to be configured for secure access to prevent data leakage.

Provisioning new devices quickly and managing updates and patches for all devices can be a struggle.

Workshop phases and modules

Endpoint Management with Security Workshop modules

SCC

Assess

- □ Pre-engagement call
- □ Customer questionnaire
- □ Endpoint Management with Security overview
- □ Security posture assessment

Art of the Possible

- □ Secure your identities and devices
- □ Simplify IT management with Intune
- □ Upgrade to Windows 11
- □ Optional modules

Build the Plan

- □ Value Calculator
- □ Results and Next Steps
- □ Reports and Recommendations

Secure your identities and devices

- □ Azure AD overview
- □ Conditional Access
- □ Microsoft Defender for Endpoint
- □ Windows 11 Security
- □ Windows Autopatch overview

Simplify IT management with Intune

- □ Enroll overview & enablement
- □ Configure overview & enablement
- □ Protect overview & enablement
- □ Support & Retire overview & demo

Upgrade to Windows 11

- □ Windows 11 Enterprise overview
- □ Upgrading and deploying Windows 11 Enterprise
- □ Refresh Windows devices

Optional modules

Microsoft Edge

- □ Microsoft Edge

Microsoft Devices

- □ Microsoft Surface
- □ Surface Hub
- □ Microsoft Teams Rooms
- □ HoloLens

Analytics and Reporting

- □ Endpoint analytics
- □ Intune reporting and Graph API

MDM Migration

- □ MDM migration overview

Intune for Education

- □ Intune for Education deployment
- □ School Data Sync deployment

Advanced Management Solutions

- □ Advanced Management Solutions overview

Immersive experiences Endpoint Management | Identity & Security | IT Pro guided hands-on activities

Out of scope

Configuration of Azure Active Directory, Microsoft Intune and Microsoft Defender for Endpoint beyond what's required for showcasing capabilities

Design and planning sessions for any topics

Custom configurations in the production environment

Low-level designs or implementations

Proof of concepts or lab deployments

Customer responsibilities

Access to key participants

Multiple workshops require the attendance of selected members of device management, security or cloud infrastructure teams

Provide stakeholder/sponsor oversight

A stakeholder/sponsor is required to oversee and own the process from the customer side

Access to the tenant

Provide access to the Microsoft 365 tenant to set up scenarios used to showcase the different capabilities

Provide necessary devices and accounts

Provide a list of users who will test the implemented features

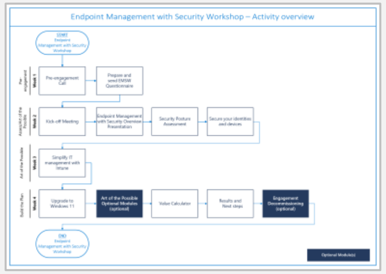
Provide an appropriate number of Windows 10/11, iOS/iPadOS (optional), Android (optional) or macOS (optional) devices

Provide, if required, Apple Business Manager (optional) or Google Play account (optional)

Endpoint Management with Security Workshop

Readiness Content

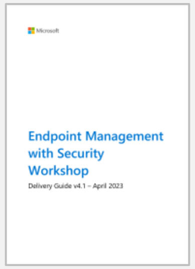
Workshop flow illustrations



Endpoint Management with Security Workshop – Activity overview

START
Endpoint Management with Security Workshop
Pre-engagement
Week 1
Pre-engagement Call
Prepare and send EMSW Questionnaire
Assess/Art of the Possible
Week 2
Kick-off Meeting
Endpoint Management with Security Overview Presentation
Security Posture Assessment
Secure your identities and devices
Art of the Possible
Week 3
Simplify IT management with Intune
Build the Plan
Week 4
Upgrade to Windows 11
Art of the Possible Optional Modules (optional)
Value Calculator
Results and Next steps
Engagement Decommissioning (optional)
END
Endpoint Management with Security Workshop
Optional Module(s)

Delivery guide



Microsoft

Endpoint Management with Security Workshop

Delivery Guide v4.1 – April 2023

Sales and marketing content

Program Overview

Customer benefits of the Endpoint Management with Security Workshop

Today's users are looking for more ways to remain productive while working on any device. 95% of organizations allow personal devices in the workspace while 70 million smartphones are lost every year. With users asking for more ways to work the way that they want, this workshop will show you how to manage and protect both company-owned and user-chosen devices in the cloud and how to secure identities, devices and data in your organization.

This workshop will show you how to leverage intelligent security, risk-based controls, zero-touch provisioning, and advanced analytics to enable cloud management for the devices your users need.

✓ Learn how to improve your knowledge of cloud-based device management and security using Microsoft solutions

✓ Discover and protect your endpoints by enforcing policies and deploying security tools

✓ Secure your identities with multi-factor authentication and conditional access from any device

✓ Enable your users to be productive with the applications they need, on the devices they want

Customer flyer

Microsoft

Manage and protect your devices, your apps, and your users

Endpoint Management with Security Workshop

Workshop highlights

Enable users to be productive, on any device, without compromising IT security

Why you should attend

E-mail template

Microsoft

Endpoint Management with Security Workshop

Dear <customer name>

If you're among the 95% of organizations that allow personal devices in the workplace, you may be concerned about the extra risks they create. And for good reason: over 70 million smartphones are lost every year!

<Partner name> is pleased to offer you a **Microsoft Endpoint Management with Security Workshop**, allowing you to experience the power of modern device management and security within your own environment. The workshop will be customized to meet your organization's specific needs.

Let us show you how to leverage intelligent security, risk-based controls, zero-touch provisioning, advanced analytics, and deep integration to the Microsoft products you already use.

- Learn how to build management policies that **protect your users, company data, and devices**
- **Gain insights about your users' endpoints and their compliance** with your IT policies
- Determine the **best way to give your users access to the apps they need** on the devices of their choosing

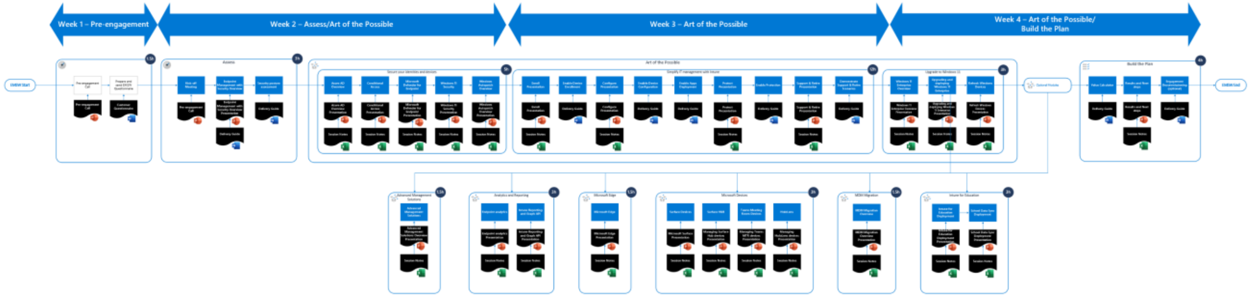
Get in touch with us today for more details and to schedule your workshop.

Best regards,

Contact Name
Contact phone #, contact email address

Partner landing page URL

Workshop Content



Week 1 – Pre-engagement
Week 2 – Assess/Art of the Possible
Week 3 – Art of the Possible
Week 4 – Art of the Possible/ Build the Plan

aka.ms/EndpointMgmtWithSecurityWorkshop/Download

Assess

Assess

Kick-off meeting

Introduce the Endpoint Management with Security Workshop engagement, discuss the upcoming activities, align expectations and establish timelines.

Microsoft Endpoint Management with Security Overview

Provide a high-level overview of the capabilities of Azure AD, Microsoft Intune and Microsoft Defender for Endpoint with a focus on security, flexible management, and deep Microsoft 365 integration.

Security posture assessment

Perform a security assessment using Microsoft Secure Score, analyzing and prioritizing recommendations to improve your security posture.

Art of the Possible

Art of the Possible

Choose your own adventure!

The Art of the Possible phase includes three required modules:

- Secure your identities and devices
- Simplify IT management with Intune
- Upgrade to Windows 11

On top of that, you can choose any of the optional modules for delivery based on your company interest.

Secure your identities and devices

- ❑ Azure AD overview
- ❑ Conditional Access
- ❑ Microsoft Defender for Endpoint
- ❑ Windows 11 Security
- ❑ Windows Autopatch overview

Simplify IT management with Intune

- ❑ Enroll overview & enablement
- ❑ Configure overview & enablement
- ❑ Protect overview & enablement
- ❑ Support & Retire overview & demo

Upgrade to Windows 11

- ❑ Windows 11 Enterprise overview
- ❑ Upgrading and deploying Windows 11 Enterprise
- ❑ Refresh Windows devices

Optional modules

Microsoft Edge

- ❑ Microsoft Edge

Microsoft Devices

- ❑ Microsoft Surface
- ❑ Surface Hub
- ❑ Microsoft Teams Rooms
- ❑ HoloLens

Analytics and Reporting

- ❑ Endpoint analytics
- ❑ Intune reporting and Graph API

MDM Migration

- ❑ MDM migration overview

Intune for Education

- ❑ Intune for Education deployment
- ❑ School Data Sync deployment

Advanced Management Solutions

- ❑ Advanced Management Solutions overview

Art of the Possible

Secure your identities and devices

Azure AD Overview presentation

Present how Azure AD helps to secure adaptive access, how it provides seamless user experiences, how it secures access to all your applications and how it automates identity governance.

Conditional Access presentation

Present how Azure AD Conditional Access brings signals together, to make decisions, and enforce organizational policies.

Microsoft Defender for Endpoint presentation

Present Microsoft Defender for Endpoint, an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Windows 11 Security presentation

Present Windows 11 Security, built with zero-trust principles at the core to safeguard data and access anywhere, keeping you protected and productive.

Windows Autopatch Overview presentation

Present a technical overview of Windows Autopatch including: its Quality Update release process, how to work with the solution, how to register devices and how to use the Windows Autopatch reports.

Art of the Possible

Simplify IT management with Intune

Enroll Presentation

Present a high-level overview of the device enrollment methods and tenant setup options in Microsoft Intune.

Enable Device Enrollment

Enable Microsoft Intune in the production tenant, setting up device enrollment, and enrolling selected devices.

Configure Presentation

Present a high-level overview of the device configuration options and the app deployment methods in Microsoft Intune.

Enable Device Configuration

Create device configuration profiles for the different in-scope device platforms in the production tenant and apply them to selected devices.

Enable Apps Deployment

Deploy the Microsoft 365 apps and Microsoft recommended apps to the Microsoft Intune managed devices in the production tenant.

Protect Presentation

Present key account and device security features in Microsoft 365 and how they can be enabled or managed with Microsoft Intune.

Assess

Simplify IT management with Intune (continued)

Enable Protection

Enable identity and device security features with Microsoft Intune, Azure Active Directory and Microsoft Defender for Endpoint.

Support and Retire Presentation

Present a high-level overview of the troubleshooting and support features, the remote assistance options and the endpoint analytics features in Microsoft Intune.

Demonstrate Support and Retire

Demonstrate how help desk associates can use the troubleshooting and support features in Microsoft Intune to help users with their managed devices and to get insights and analytics on their end user experience.

Art of the Possible

Upgrade to Windows 11

Windows 11 Enterprise Overview presentation

Present an introduction to Windows 11 Enterprise, designed for hybrid work with a focus on productivity, collaboration, security and consistency.

Upgrading and deploying Windows 11 Enterprise presentation

Present what's new with Windows 11, deployment considerations and prerequisites and how to go modern for deployment.

Refresh Windows Devices presentation

Present how modern Windows devices can help deliver the best Windows 11 experience.

Art of the Possible

Optional Modules

Microsoft Edge

Microsoft Edge presentation
Present an overview of Microsoft Edge, how it helps to secure access to your applications and corporate resources with zero trust, and how to deploy and manage the browser with Microsoft Intune.

Analytics and Reporting

Endpoint Analytics presentation
Present a detailed overview of Endpoint Analytics and its features.

Intune Reporting and Graph API presentation
Present a detailed overview of the Microsoft Intune reporting features including Intune reports, the Intune Data Warehouse, exporting reports with Microsoft Graph, and creating custom reports with Log Analytics.

Microsoft Devices

Microsoft Surface presentation
Present an overview of Microsoft Surface and the Modern Workplace. Learn about modern management and zero-touch deployment of Surface devices.

Managing Surface Hub devices presentation
Present Surface Hub 2S management options and cloud-based management.

Managing Teams MTR devices presentation
Present cloud-based management options for Android MTR devices.

Managing HoloLens devices presentation
Present an overview of how to manage HoloLens 2 with Microsoft Intune.

Art of the Possible

Optional Modules (continued)

Intune for Education

Intune for Education Deployment presentation
Present an overview of how to setup and configure Intune for Education, how to control updates, manage applications and how to setup school PCs.

School Data Sync Deployment presentation
Present an overview of what School Data Sync does and how to configure a sync profile.

MDM Migration

MDM Migration Overview presentation
A presentation that can be used to assess the customer's current MDM solution and to discuss high-level steps to migrate to Microsoft Intune.

Advanced Management Solutions

Advanced Management Solutions Overview presentation
Present an overview of the advanced endpoint management and security capabilities in Microsoft Intune which includes Remote Help, Microsoft Tunnel for Mobile Application Management, Specialized devices management and Advanced endpoint analytics.

Build the Plan

Build the plan

Value Calculator

Use the Value Calculator to calculate and present the ROI your organization can achieve by adopting the Microsoft solutions covered in this workshop

Results and Next Steps

Present workshop outcomes, strategic and technical next steps and agreed follow-up engagements

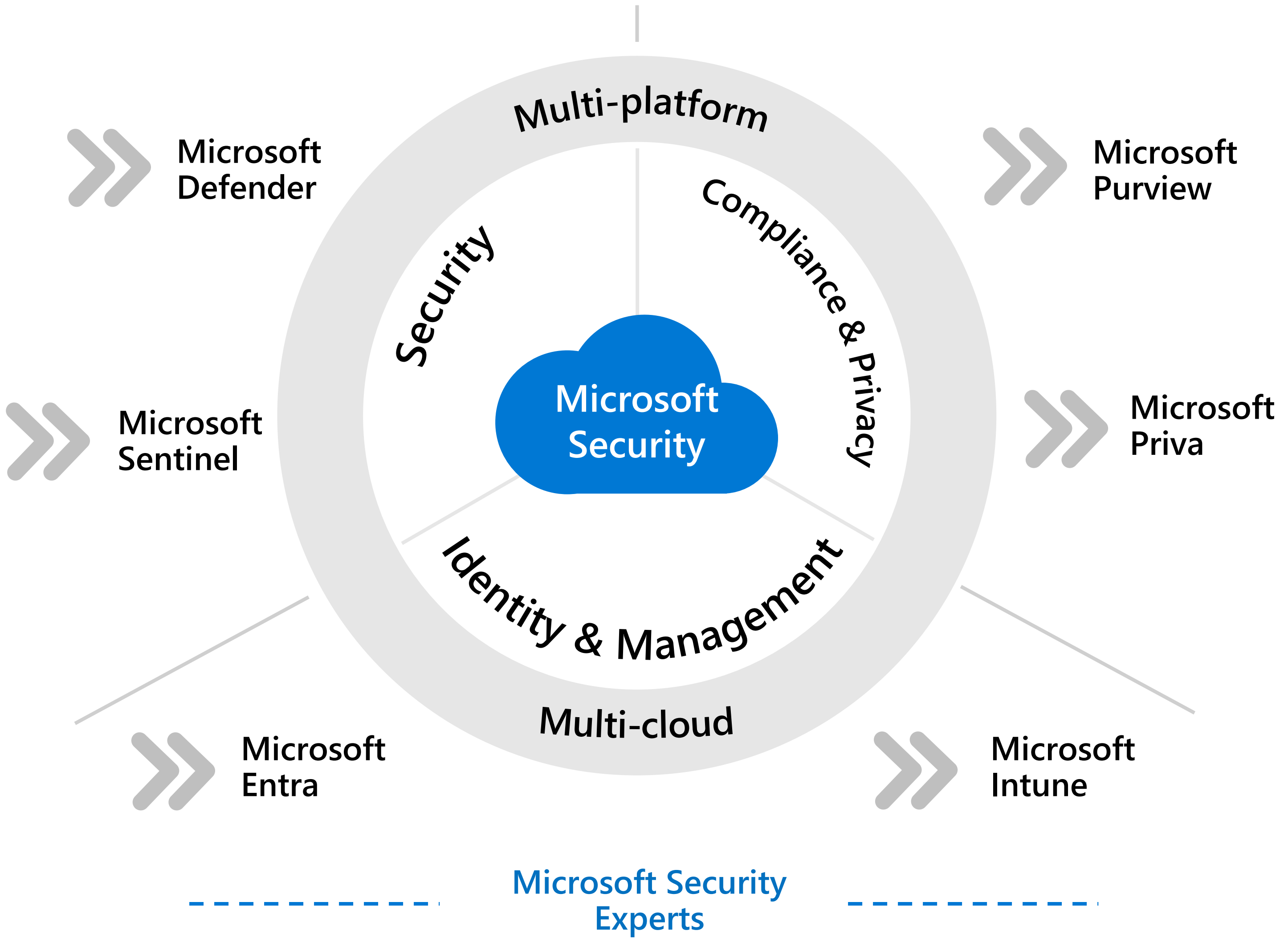
Reports and Recommendations

Optionally, document findings and recommendations in a report

Call to action

Microsoft Security Portfolio overview

Six product families integrating over 50 product categories



A unified solution to manage endpoints anywhere

Simplify management

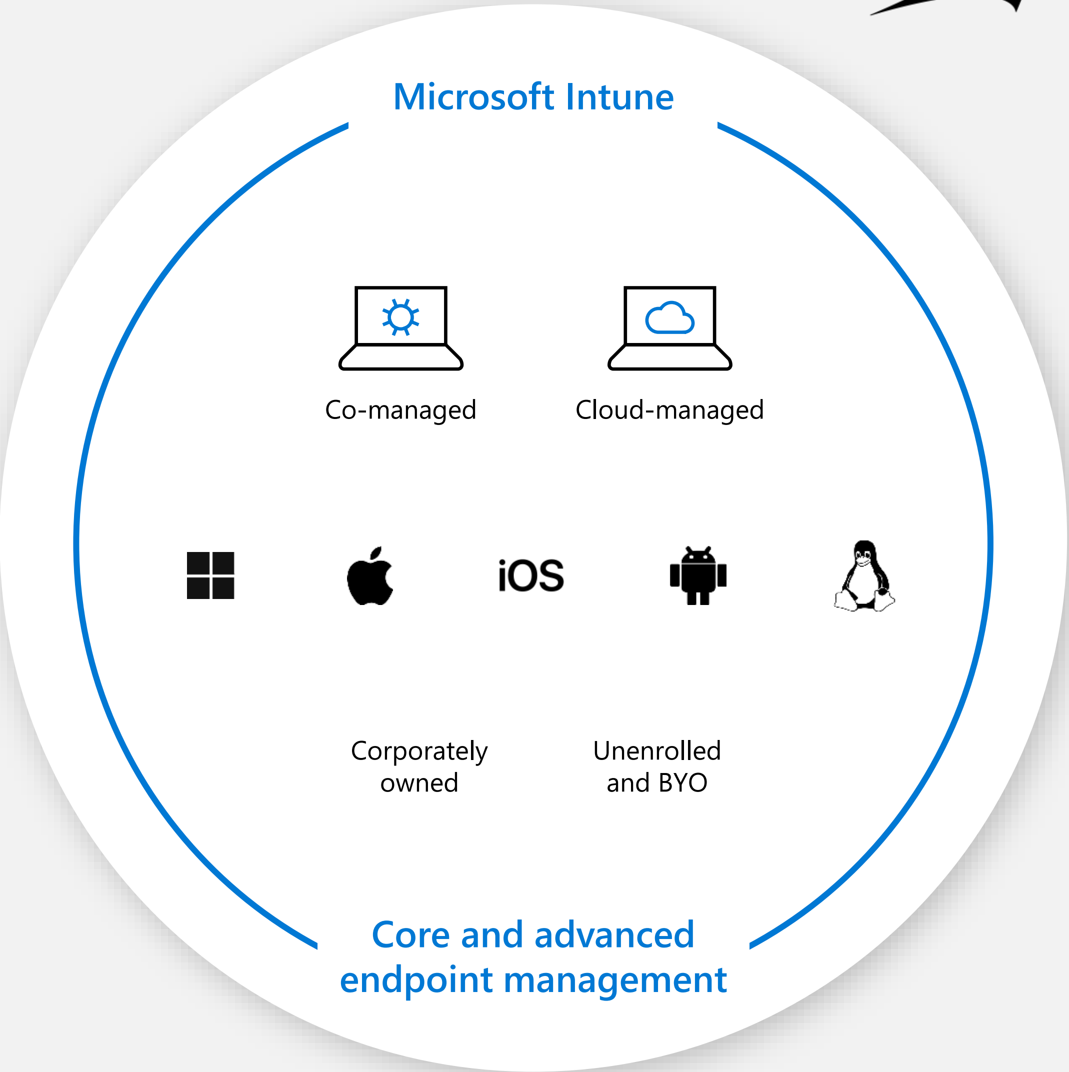
Enable the shift to cloud management, leveraging rich insights on endpoint analytics and cloud-based deployment.

Protect hybrid workforces

Protect users, apps, and data across all devices with Defender for Endpoint.

Power better user experiences

Enable users with device and application management for iOS, macOS, Linux, and Android.



Windows 11 Enterprise is built to protect your hybrid workforce

Protect the digital worker

Security by default

Windows, Microsoft Intune and Azure AD can reduce the data breach risk

+

Simplify IT management

Proactive remediation and automation from a single source

Improve operational efficiency with Windows Enterprise and Intune

+

Power better experiences

Protected and productive without downtime

Increase in end-user productivity and give IT more time for other projects

TCO and cost savings benefits from Microsoft 365 E3

Total Economic Impact study Windows 11 Enterprise	aka.ms/Windows11EconomicValue
Total Economic Impact study Microsoft Intune	aka.ms/IntuneEconomicValue
Total Economic Impact study Microsoft 365 E3	aka.ms/Microsoft365EconomicValue

Strategies for cost savings

Reduced support needs

Significantly reduce the total ticket queue for IT teams and enable them to manage endpoints remotely to continually lower the number of support requests.

Improved security

Reduce the burden of managing multiple tools so security teams can improve security posture and lower the threat of security incidents.

Redeployed IT time

Enable faster and smoother remote device provisioning and upgrades so that IT teams can spend less time monitoring and facilitating planned updates and reconfigurations.

Enhanced end-user experience

Improve flexibility and productivity by allowing employees to use their smartphones to access corporate applications.

Retired endpoint management tools

Move to the cloud and retire former solutions to save licensing fee costs as well as hardware and maintenance costs.

Microsoft

Thank you.