

Endpoint Management with Security Workshop

Overview



Agenda

Market trends

Microsoft Security

Microsoft Intune

Windows 11 Enterprise and Intune

Paths to modern management

Device lifecycle

Microsoft 365 business value

Summary

Market trends



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

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



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

Microsoft Security





Security has never
been more critical



Cyber attacks are becoming more frequent and sophisticated

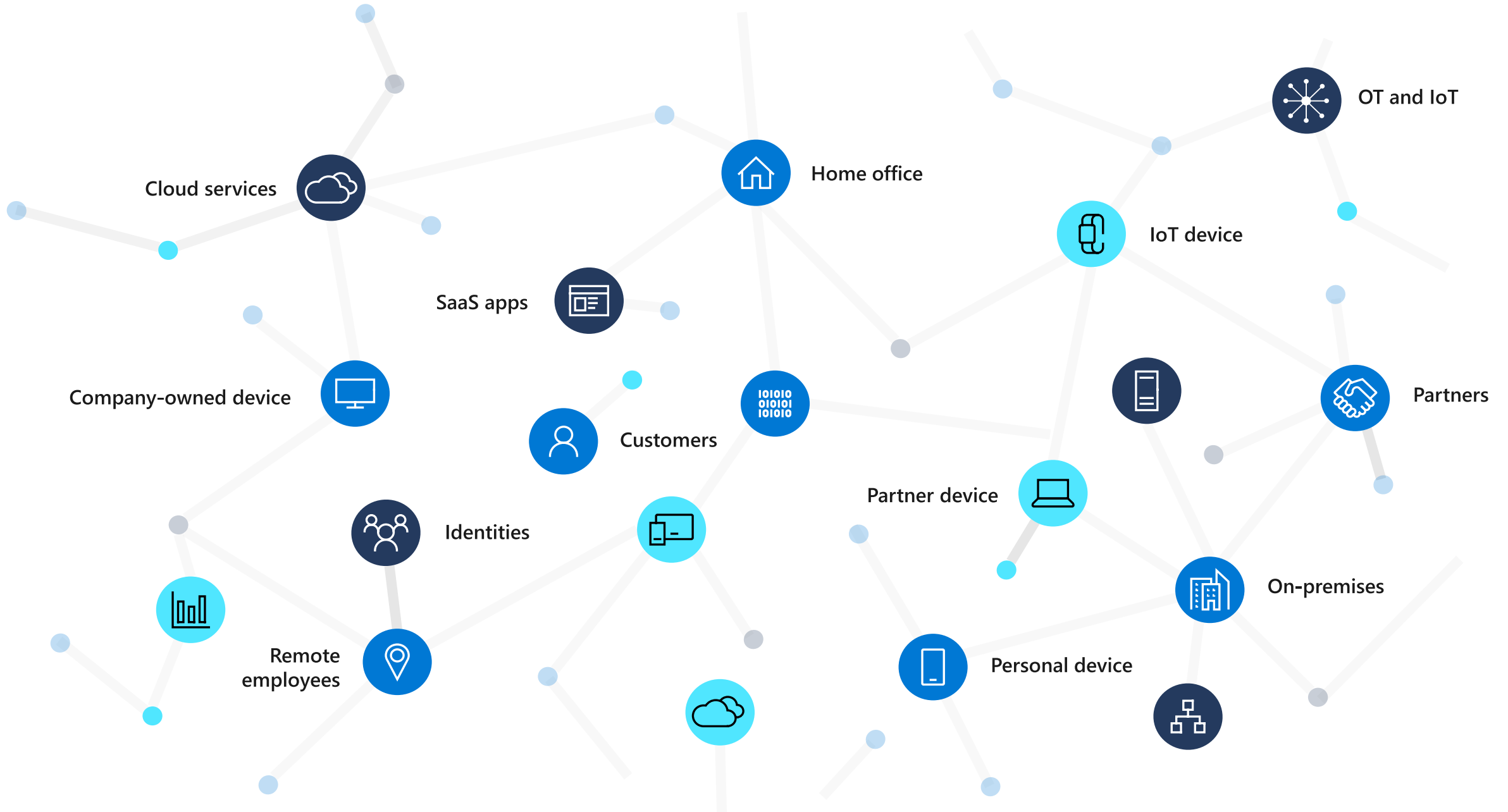
Pressures to address multicloud IT environment

Increasingly demanding regulatory landscape



**The technology
environment has never
been so complex**





Microsoft on the front lines

Protecting

785K

organizations
in 120 countries

Analyzing

43T

threat signals
every day

Tracking

250+

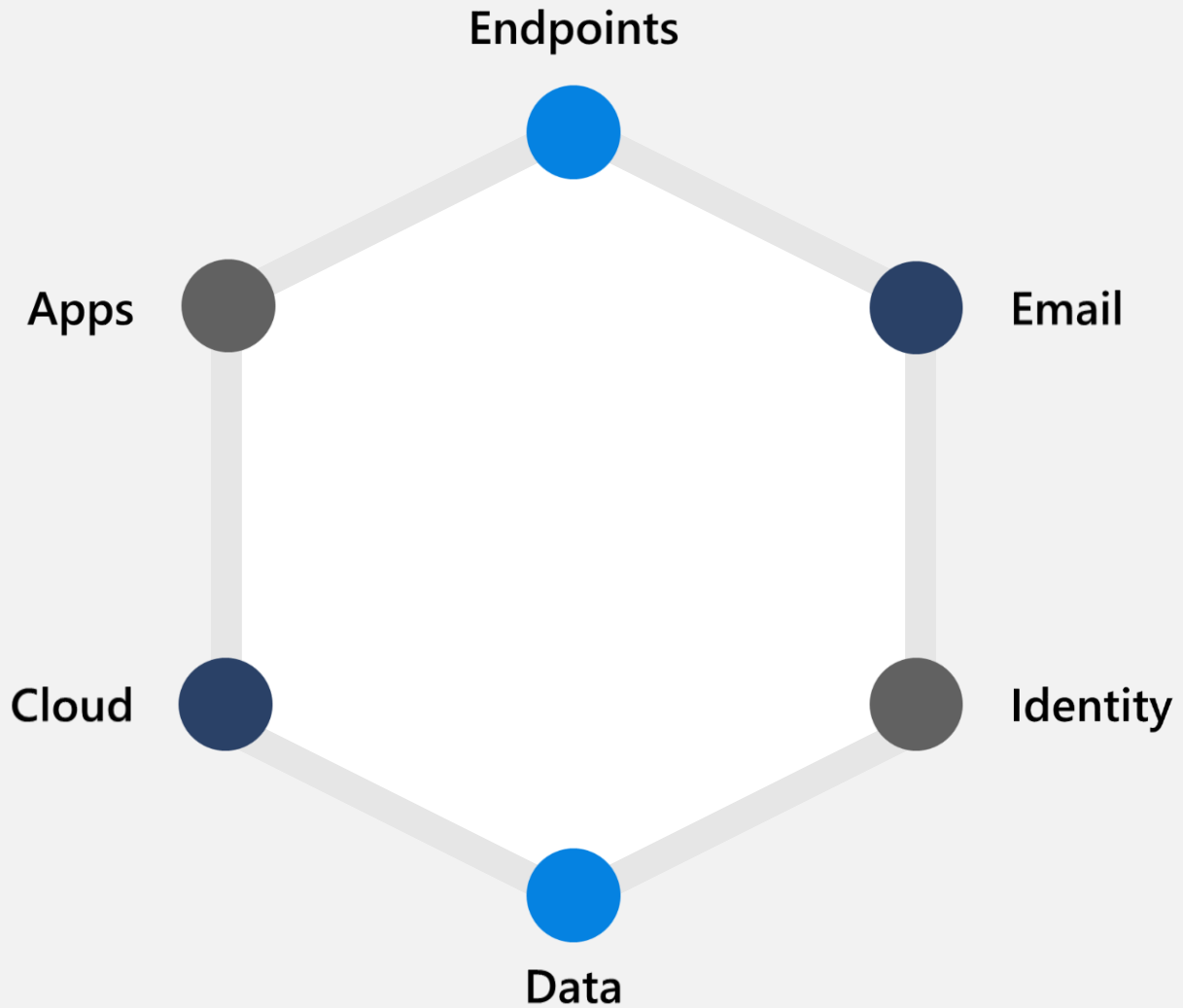
unique nation-states,
cybercriminals, and
other threat actors

Blocked

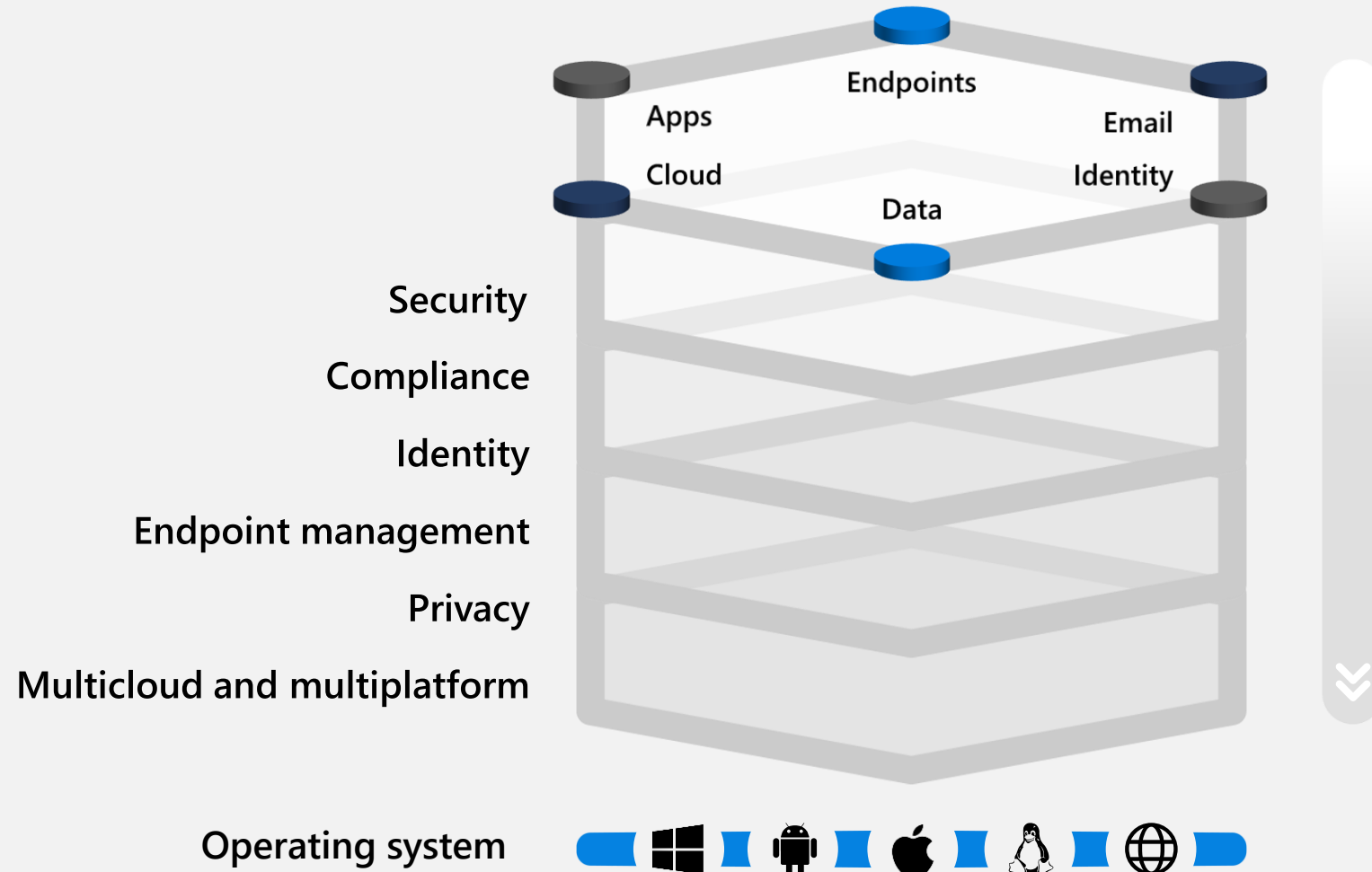
70B

attacks
last year


End-to-end protection



A comprehensive approach to security



CISOs are under pressure to contain costs



Conventional security tools **have not kept pace**

Cost of security breaches **is rising**

Resources are **constrained**

*"Boards are now pushing back for improved understanding of what they have achieved after years of such heavy investment."*¹

Gartner

Paul Proctor
Distinguished VP Analyst, Gartner

Significantly more security decision makers have felt pressure to cut costs within the past 6 months²

82%

feel pressured to lower costs³

#1

priority to reduce cost is improved threat protection

¹ "The Urgency to Treat Cybersecurity as a Business Decision" February, 2020

² March 2022 survey of 501 US Security Decision Makers commissioned by Microsoft from agency, Vital Findings

³ Microsoft Pandemic CISO Survey³ 2020

Microsoft Security
helps you do more
with less

60%

savings by consolidating a
patchwork of vendors for a
comprehensive solution
from Microsoft*

Be more efficient

Unify your tools, consolidate your licenses, and cast aside redundant contracts and consultants.

Be more effective

AI and automation help you detect and respond faster and more accurately to attacks and insider risks.

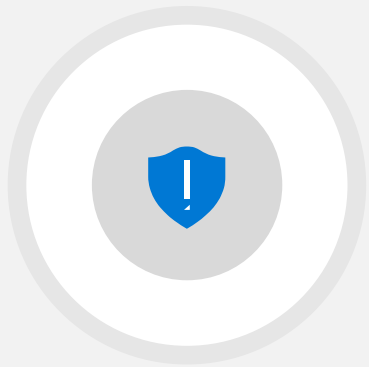
Be more unified

Increase SecOps efficiency with a unified SIEM and XDR experience that improves visibility across identities and endpoints

* Savings based on publicly available [estimated pricing](#) for other vendor solutions and Web Direct/Base Price shown for Microsoft offerings.

Protection aligned to what's ahead

Solutions to support your digital journey



**Defend against
threats with SIEM
plus XDR**



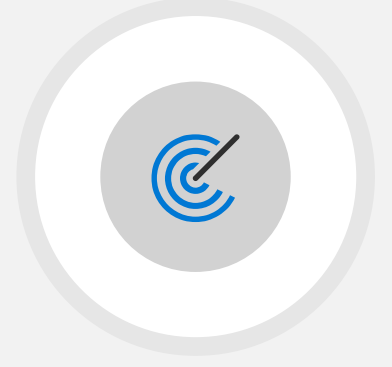
**Secure
multicloud
environments**



**Secure identities
and access**



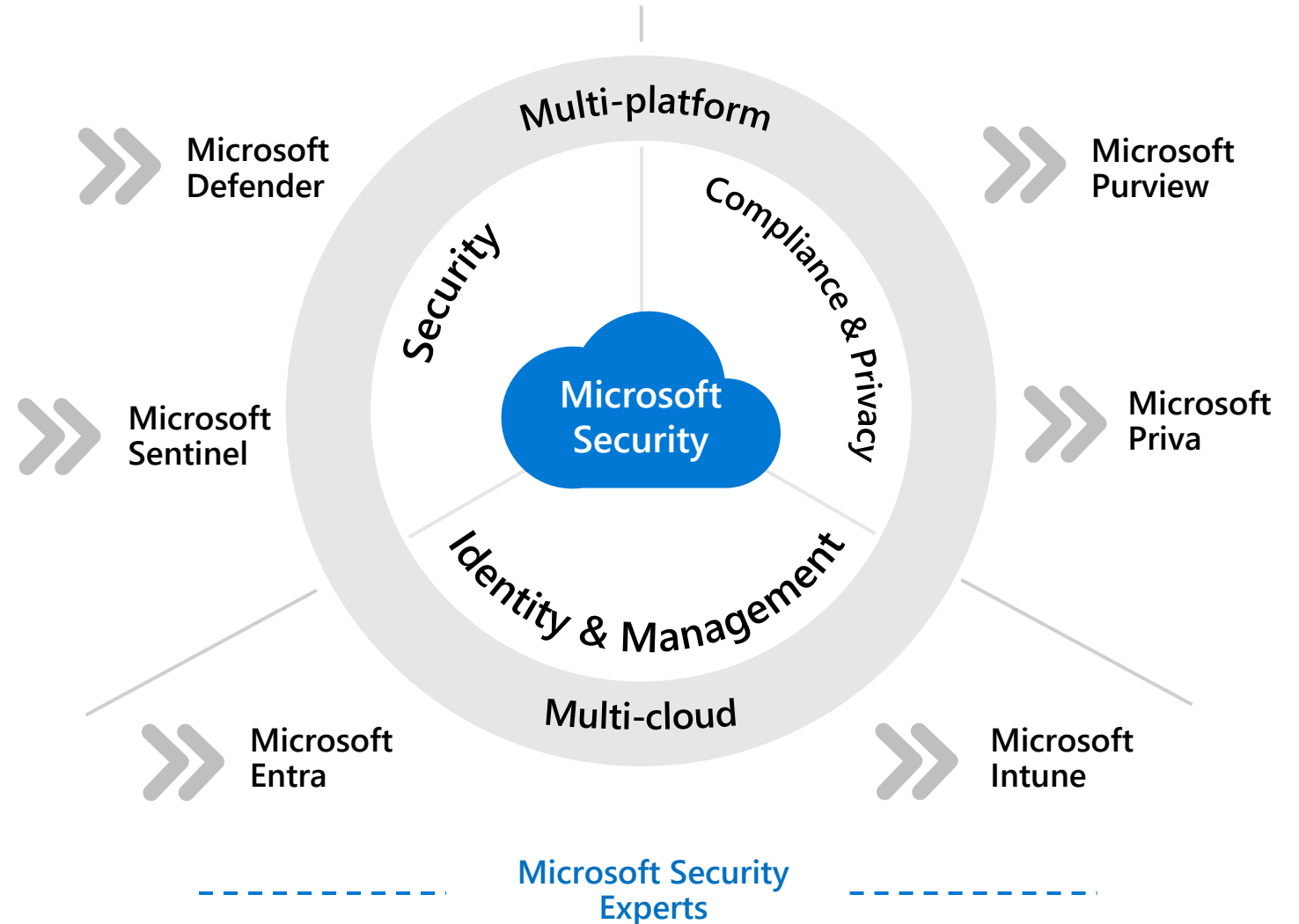
**Protect and
govern sensitive
data**



**Mitigate
compliance and
privacy risk**

Portfolio overview

Six product families integrating over 50 product categories



Azure Active Directory



Microsoft Azure Active Directory

Secure access for a connected world



Secure adaptive
access



Seamless user
experiences



Unified identity
management



Simplified access
governance



Azure AD Multi-factor authentication

Verify user identities with strong authentication



Azure AD supports a broad range of multi-factor authentication options

Including passwordless technology



Microsoft Authenticator



Windows Hello



FIDO2 Security key



Biometrics



Push Notification



Soft Tokens OTP



Hard Tokens OTP



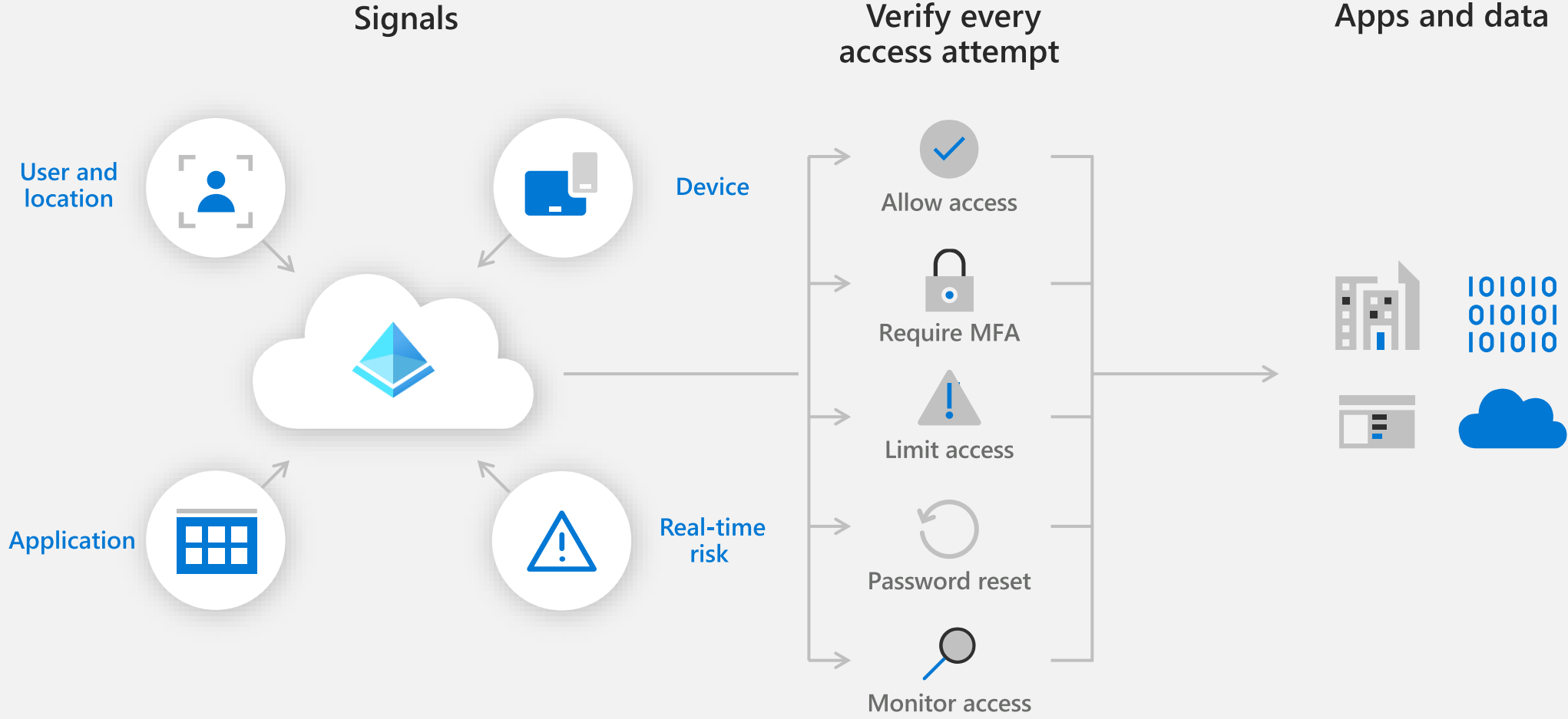
SMS, Voice



Multi-factor authentication prevents 99.9% of identity attacks

Protect identities with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies



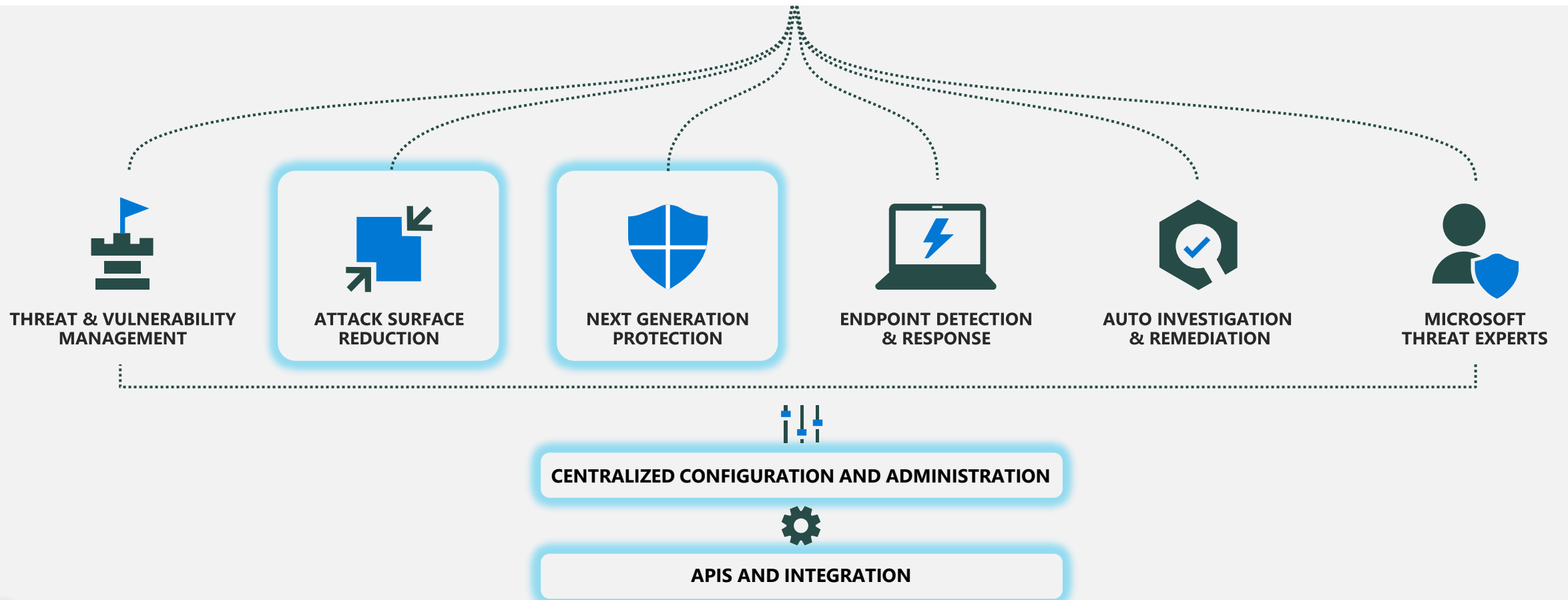
Microsoft Defender for Endpoint





Microsoft Defender for Endpoint

Threats are no match.



Microsoft Defender for Endpoint Plan 1 capabilities

Attack Surface Reduction

Eliminate risks by reducing the surface area of attack



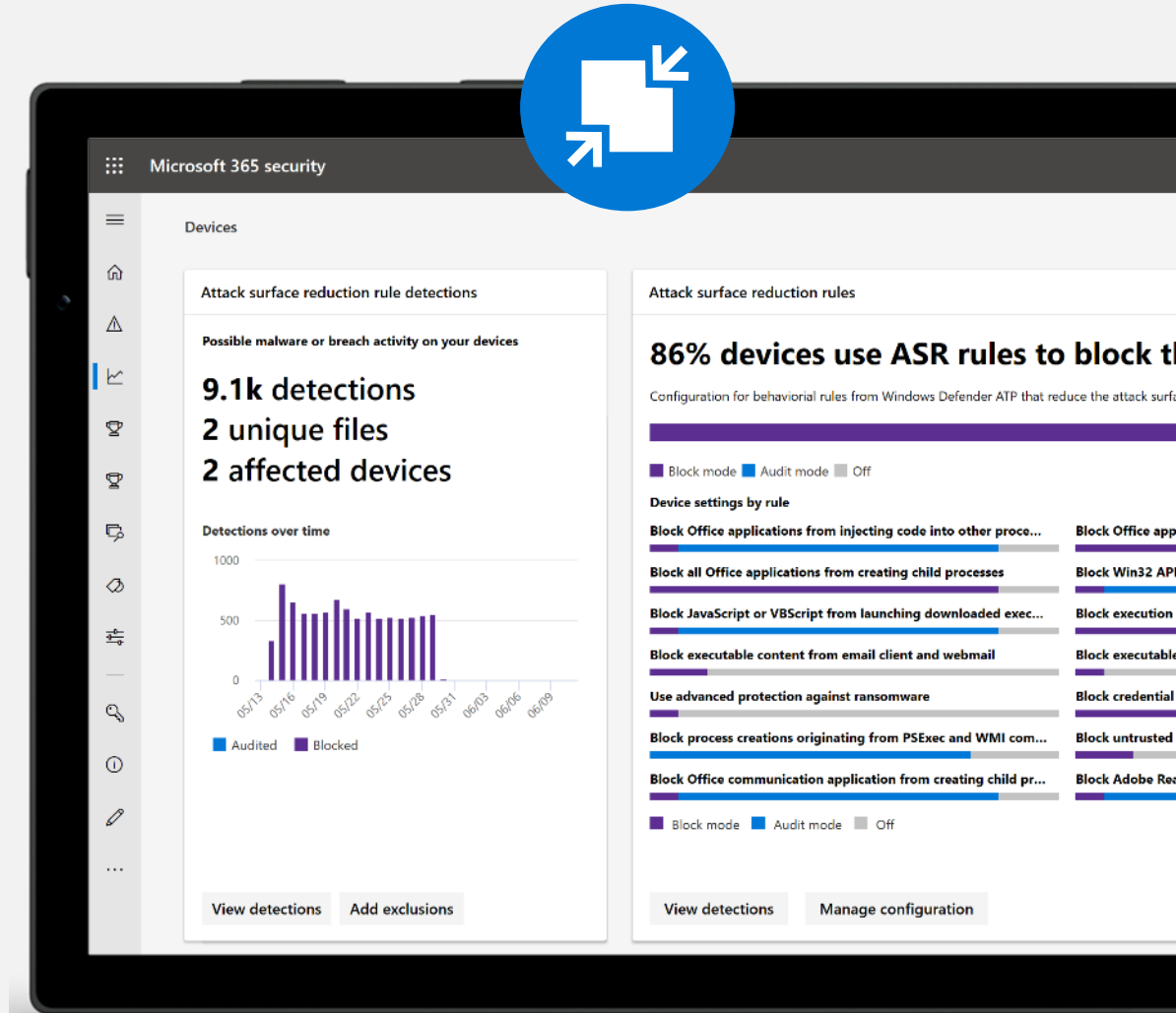
System hardening without disruption



Customization that fits your organization



Visualize the impact and simply turn it on



Next Generation Protection

Blocks and tackles sophisticated threats and malware



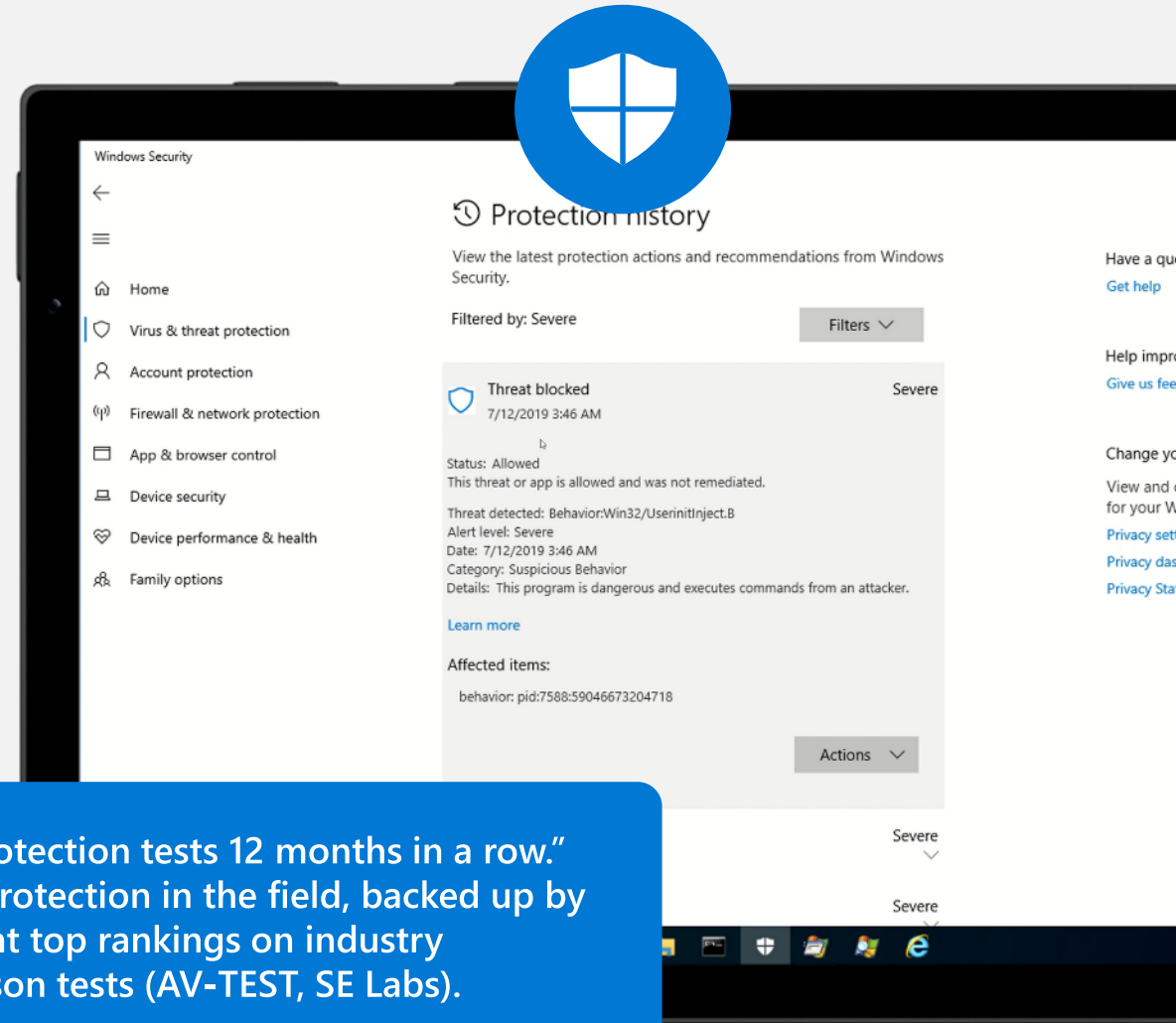
Behavioral based real-time protection



Blocks file-based and fileless malware

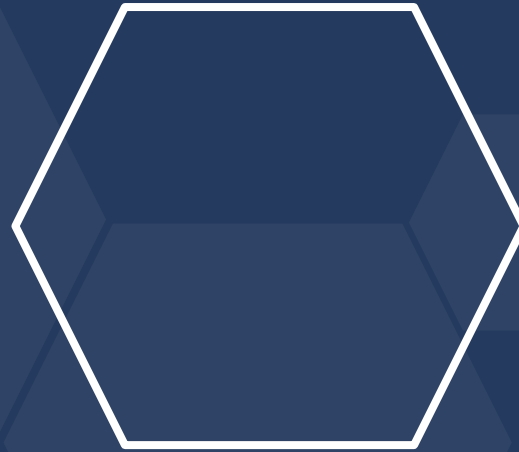


Stops malicious activity from trusted and untrusted applications



“Aced protection tests 12 months in a row.”
Proven protection in the field, backed up by
consistent top rankings on industry
comparison tests (AV-TEST, SE Labs).

Windows 11 Security

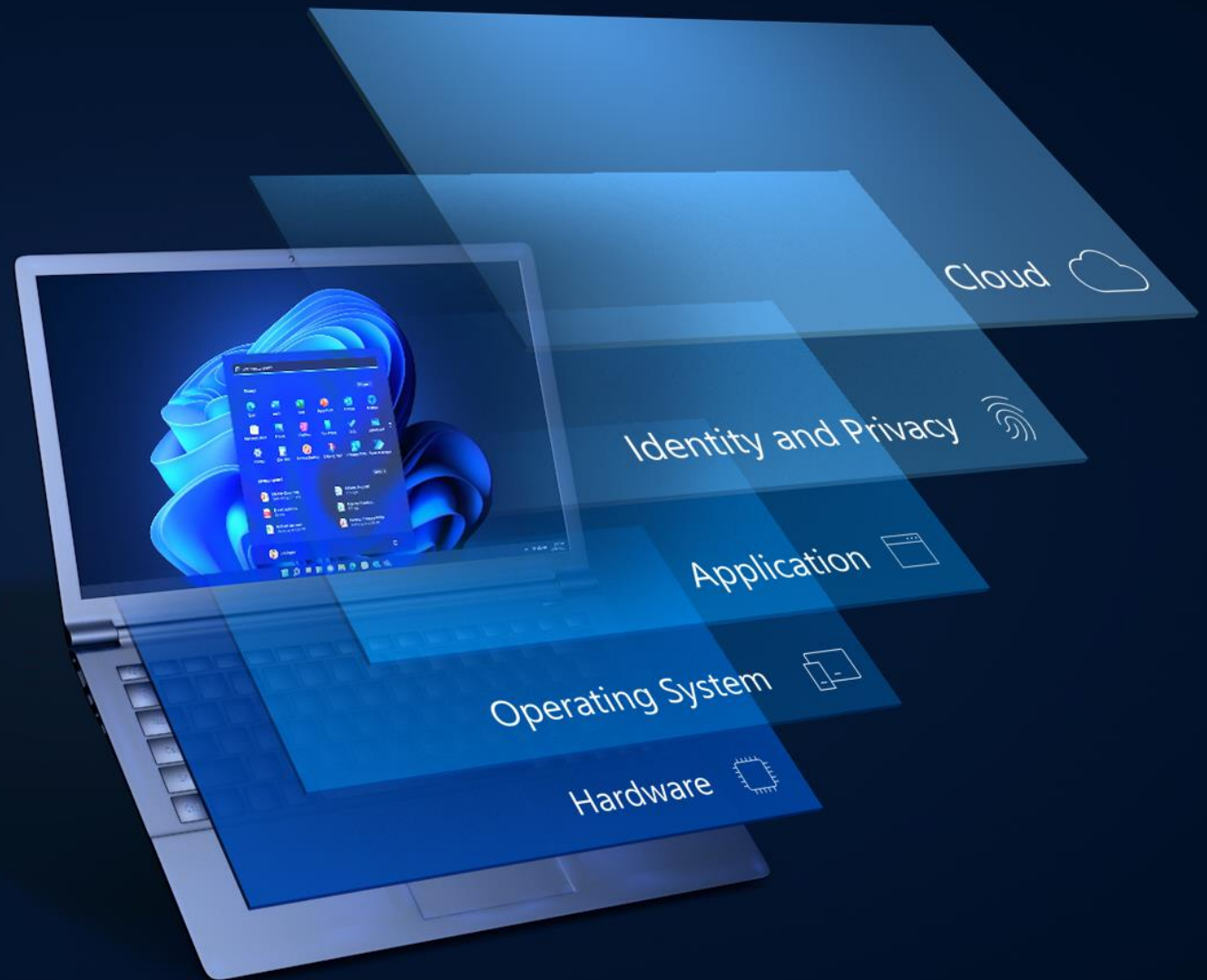


Windows 11 - Security by default

Windows 11 delivers powerful protection from chip to cloud

In Windows 11, hardware and software security work together to help keep users, data, and devices protected.

- Protects against threats by separating hardware from software with **hardware root-of-trust**, for powerful security from the start
- **Protect the OS against unauthorized access** to critical data
- Delivers **robust application security** and prevents access to unverified code
- **Protects user identities** with passwordless security
- **Extends security to the cloud** to help protect devices, data, apps, and identities from anywhere



Microsoft Intune



Microsoft Intune

A unified solution to manage endpoints anywhere

SIMPLIFY ENDPOINT MANAGEMENT



PROTECT A HYBRID WORKFORCE



POWER BETTER USER EXPERIENCES



Imagine if...

...you could **simplify your IT processes** and reduce complexity and costs

SIMPLIFY ENDPOINT MANAGEMENT



Today

The future powered by Microsoft Intune.

Multiple tools
Limited resources for IT
Limited cross visibility

Management and security tools in a single solution

Complete visibility and actionable data

Manage any device, regardless of ownership

Increase IT efficiency and reduce cost



Manage cross-platform endpoints

Day-in-the-life scenario

SIMPLIFY ENDPOINT MANAGEMENT



Paul needs to support workers' device preferences.



Paul realizes he can manage most devices and majority of OSs within Intune.



He can also use Intune for devices on premises and BYO.



Paul saves time and money with a single solution for most endpoints.

Unified management saves time and resources

SIMPLIFY ENDPOINT MANAGEMENT

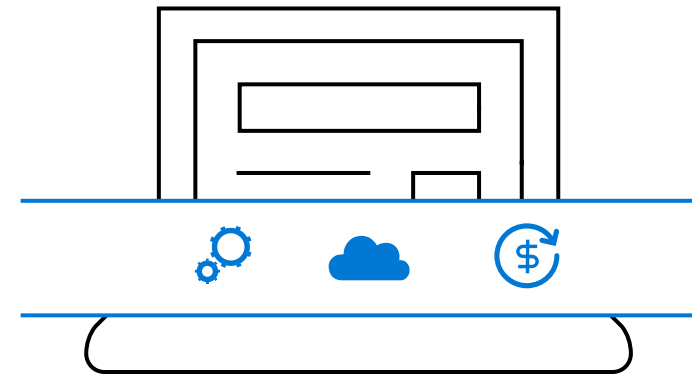


Centrally manage on-premises and cloud-based endpoints.

Empower advanced endpoint management and security tools from a single, cloud-powered solution.

Reduce costs across hardware, licensing, maintenance.

Reduced IT time frees up more than \$479,000 in human capital to apply to under-resourced projects.*



**"The Total Economic Impact™ Of Microsoft Endpoint Manager,"
commissioned by Microsoft, Forrester Consulting, April 2021.

Proactive visibility and control

SIMPLIFY ENDPOINT MANAGEMENT



Microsoft Endpoint Manager admin center

Home > Devices

Devices | All devices

Search (Ctrl+F) Refresh Filter Columns Export Bulk Device Actions

Overview

All devices

Monitor

By platform

- Windows
- iOS/iPadOS
- macOS
- Android

Device enrollment

- Enroll devices

Provisioning

- Windows 365

Policy

- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Group Policy analytics (preview)
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later (preview)
- Quality updates for Windows 10 and later (preview)

Showing 1 to 25 of 31 records

Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compliance ↑↓	OS	OS version ↑↓	Last check-in ↑↓
3637440b0711fe54_Andr...	Intune	Corporate	Not Evaluated	Android (dedicated)	11	12/14/2021, 3:01:15
3c35b1d4ad08698c_Andr...	Intune	Corporate	Compliant	Android (dedicated)	12	12/17/2021, 4:29:05
APRILMVEERA	Co-managed	Corporate	Not Compliant	Windows	10.0.22000.613	5/3/2022, 11:55:02
Amos's MacBook Air	Intune	Corporate	Compliant	macOS	12.4 (21F79)	6/26/2022, 9:41:31
DESKTOP-1SIBSSS	Intune	Corporate	Compliant	Windows	0.0.0.0	7/15/2022, 6:50:46
DESKTOP-1APLG0A	Intune	Corporate	Compliant	Windows	0.0.0.0	7/21/2022, 3:29:16
DESKTOP-4EJBDCH	Intune	Corporate	Not Compliant	Windows	10.0.22000.556	4/21/2022, 6:36:09
DESKTOP-4FR2MTA	Intune	Corporate	Compliant	Windows	10.0.22000.556	7/19/2022, 11:57:05
DESKTOP-81524SR	Intune	Corporate	Not Compliant	Windows	10.0.19043.1706	6/15/2022, 11:16:47
DESKTOP-AK4B5MQ	Intune	Corporate	Not Compliant	Windows	10.0.19044.1645	6/6/2022, 9:27:45 A
DESKTOP-BLOIABO	Intune	Corporate	Compliant	Windows	0.0.0.0	7/15/2022, 4:49:50
DESKTOP-GUIU10V	Co-managed	Corporate	Not Compliant	Windows	10.0.22453.1000	10/26/2021, 7:46:04
DESKTOP-LN3FBE3	Intune	Corporate	Compliant	Windows	10.0.19044.1766	7/22/2022, 12:08:00
EPZ000005	Co-managed	Corporate	Not Compliant	Windows	10.0.19043.1083	11/4/2021, 10:22:58
EPZ978257	Intune	Corporate	Compliant	Windows	10.0.22000.556	7/19/2022, 12:06:03
EPZCM01	ConfigMgr	Corporate	See ConfigMgr	Windows	10.0.17763.3046	
EPZDC01	ConfigMgr	Corporate	See ConfigMgr	Windows	10.0.17763.2237	
EPZWIN0001	ConfigMgr	Corporate	See ConfigMgr	Windows	10.0.19041.1288	
R61498535	Co-managed	Corporate	See ConfigMgr	Windows	10.0.22598.200	5/25/2022, 7:19:03

Know the health, compliance, and security status of any device.

Secure access to cloud and on-prem apps.

Proactively manage updates, patching, and policy across platforms and apps.

Imagine if...

...you could protect hybrid workers with integrated management and security

PROTECT A HYBRID WORKFORCE



Today

The future powered by Microsoft Intune.

Growing attack surfaces
Frequency of security breaches
Complex corporate devices, BYOD, shared devices

Data protection regardless of enrollment



Risk-based policies for conditional access



Controls to enable threat protection across platforms



Integrated endpoint security and compliance for Zero Trust



Securing people and devices

Day-in-the-life scenario

PROTECT A HYBRID WORKFORCE



Tony | IT manager

Patti | Security manager

Both Tony and Patti care about endpoint performance.

Patti can deploy and adjust **security configurations**.

Transparency gives Tony the ability to avoid security configuration conflicts with **device configurations**.

Tony and Patti collaborate to ensure endpoint security.



Endpoint security is integral to a Zero Trust approach

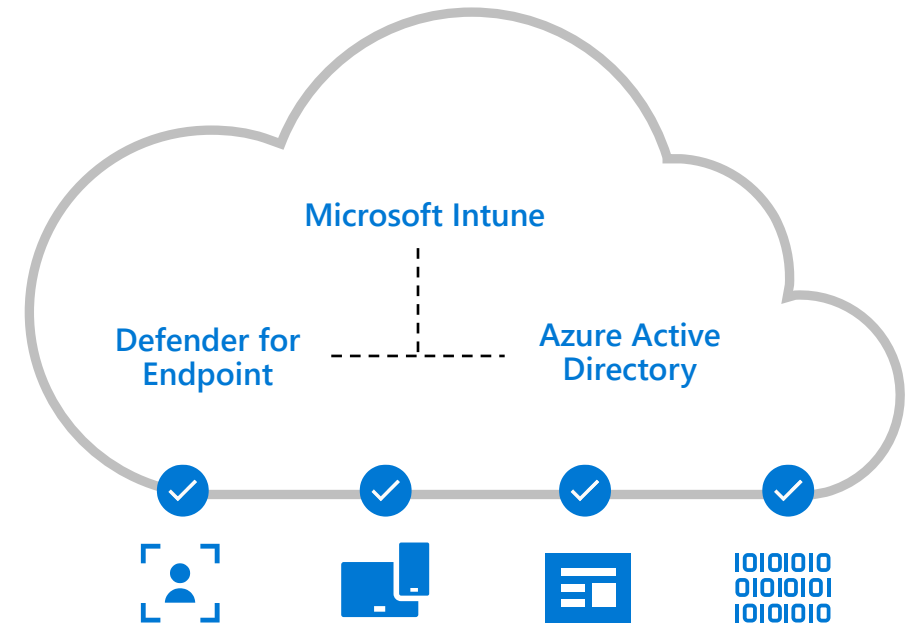
PROTECT A HYBRID WORKFORCE



Verify user identities with strong authentication methods.

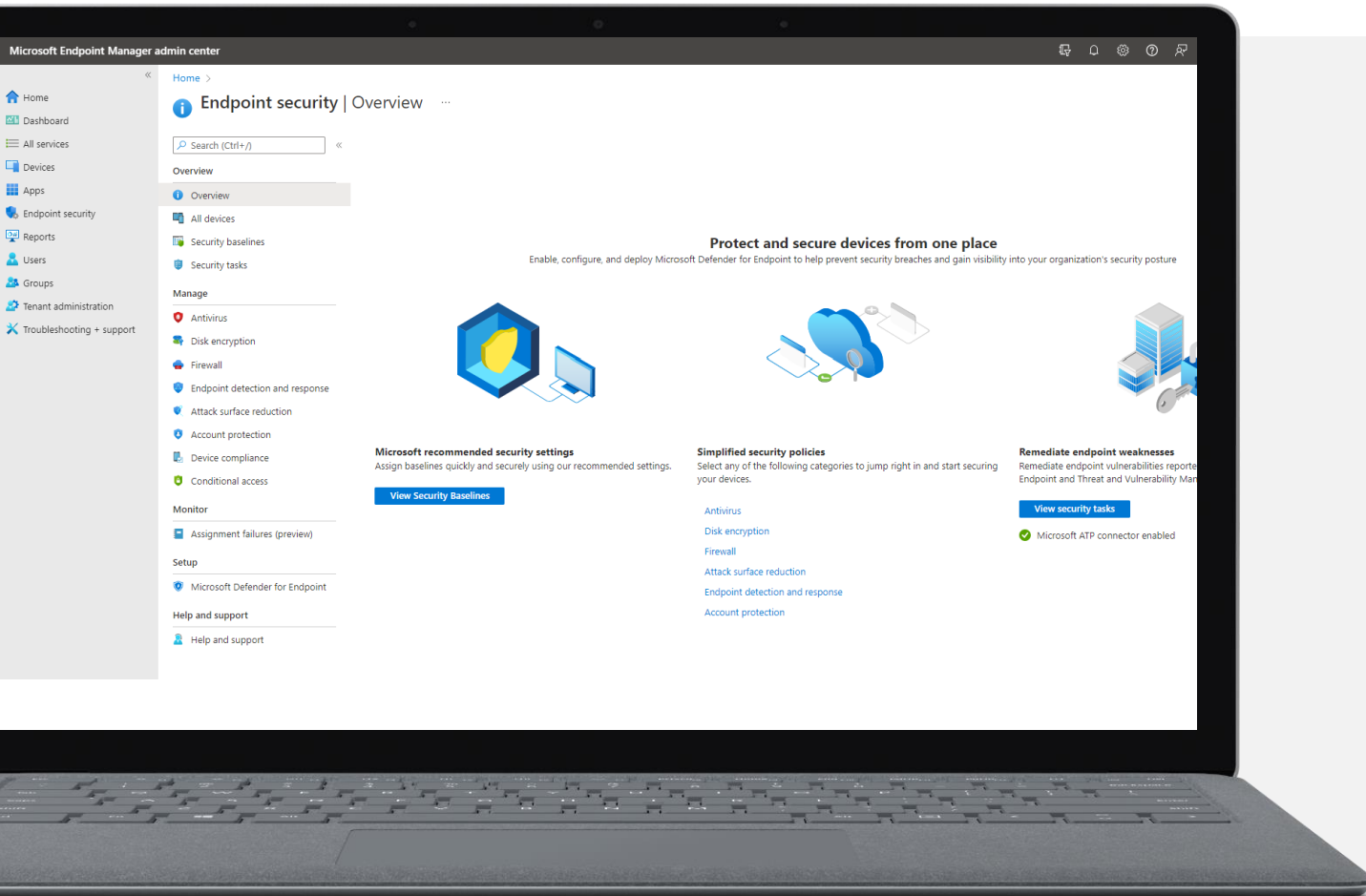
Allow only verified apps and devices access to cloud and on-prem resources.

Reduce risk with data protection on all devices regardless of ownership



Proactive detection and response

PROTECT A HYBRID WORKFORCE



Improved security adds **\$1.2 million** to the bottom line.*

Automatically investigate alerts, remediating threats faster.

Stop malicious activity from trusted and untrusted applications.

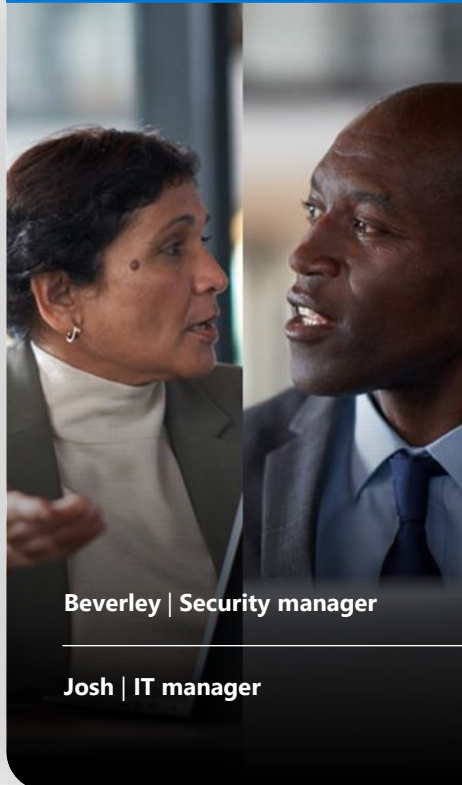
Revoke access to exploited resources in near real time.

*"The Total Economic Impact™ Of Microsoft Endpoint Manager," commissioned by Microsoft, Forrester Consulting, April 2021.

Improve security with automatic updates

Day-in-the-life scenario

PROTECT A HYBRID WORKFORCE



Beverley | Security manager

Josh | IT manager

Beverley wants to understand how device update compliance impacts their security posture.



Josh must evaluate updates and schedule the rollout process in addition to addressing competing priorities.



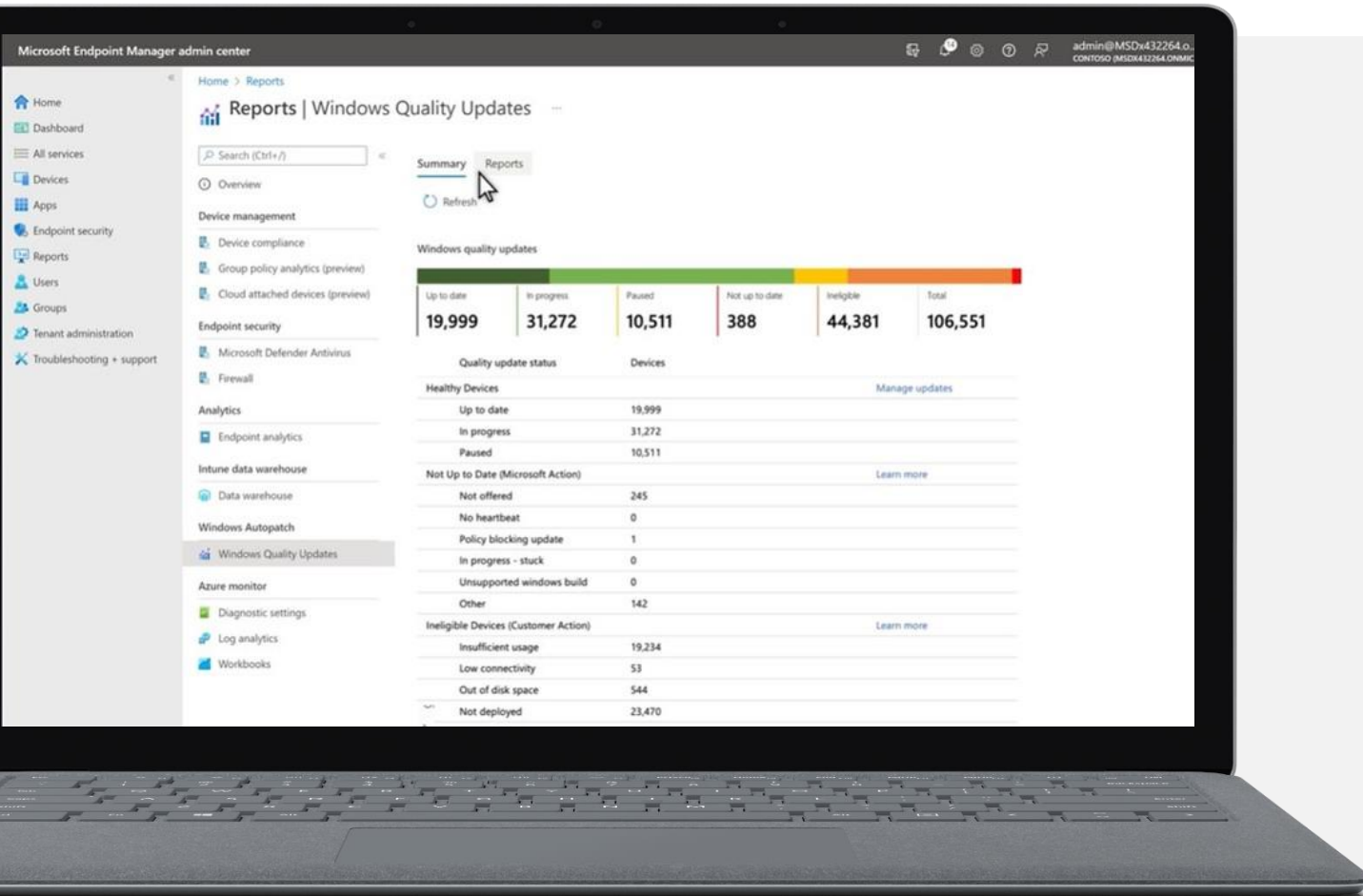
With **Windows Autopatch**, Josh can delegate updating to Microsoft.



Beverley gets detailed compliance reports – and Josh's team has increased capacity to address other needs.

Keep current, stay secure

PROTECT A HYBRID WORKFORCE



Automated updating gives time back to IT admins and peace of mind to security teams

Trust Microsoft to manage updates for Windows and Microsoft 365

Harden your posture against exploits and ransomware

Transparency and reporting keep you in control

Microsoft leverages insights to proactively address challenges and limit interruptions

Imagine if...

...you could **empower end-user needs**, no matter the workplace, no matter the endpoint

POWER BETTER USER EXPERIENCES



Today

The future powered by Microsoft Intune.

Fragmented technology experience

Access challenges

Devices not customized for roles and needs

Insights and proactive recommendations



Windows experiences: native, virtual Cloud PC, or BYOD



Integrated protection across virtually all endpoints



Zero-touch deployments and frictionless access



Support Frontline Workers with remote troubleshooting

Day-in-the-life scenario

POWER BETTER USER EXPERIENCES



Miguel, a member of the helpdesk team, needs to troubleshoot application access for one of the branch employees.



Miguel initiates a [Remote Help*](#) session from within [Microsoft Intune](#).



He can see the employee's environment and perform remote troubleshooting actions.






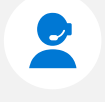



Miguel's remote access is verified in the background by [Microsoft Intune](#) and [Azure Active Directory](#), limiting security risks.

*Remote Help service is a premium add-on feature

Start with remote help

Bring together mission-critical management and security tools into a single, cloud-powered solution.

-  Secure, **cloud-based**, helpdesk-to-user connections for Windows desktops, no matter where they are
-  **Role based access control** that allows administrators to configure who can help whom and with what permissions (view only, full control or elevate)
-  Helpers can use their credentials within User Access Control prompts to complete actions that require **administrative rights**
-  Device **compliance warnings** to alert helpers if user's device is out of compliance, informed by Microsoft 365 integration
-  Session **reporting** that indicates who helped whom, when and on what device
-  Build trust between helpdesk and sharer before connections are made by showing **Azure AD profile** picture, company, name, title, and verified domain to each other
-  Centralized experience in Endpoint Manager admin center helps get you started for **a trial or to purchase additional licenses**



Streamline endpoint experiences for remote and temporary workforces

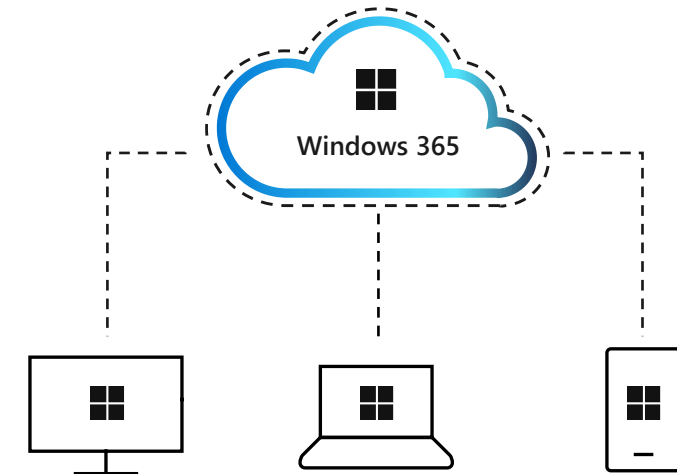
POWER BETTER USER EXPERIENCES



Zero-touch deployment provides employees ready-to-use, secured devices.

Automation enables IT to set up the process and scale to distributed workforce.

Provide virtual or cloud-delivered endpoint experiences to rapidly onboard workers using their own devices.

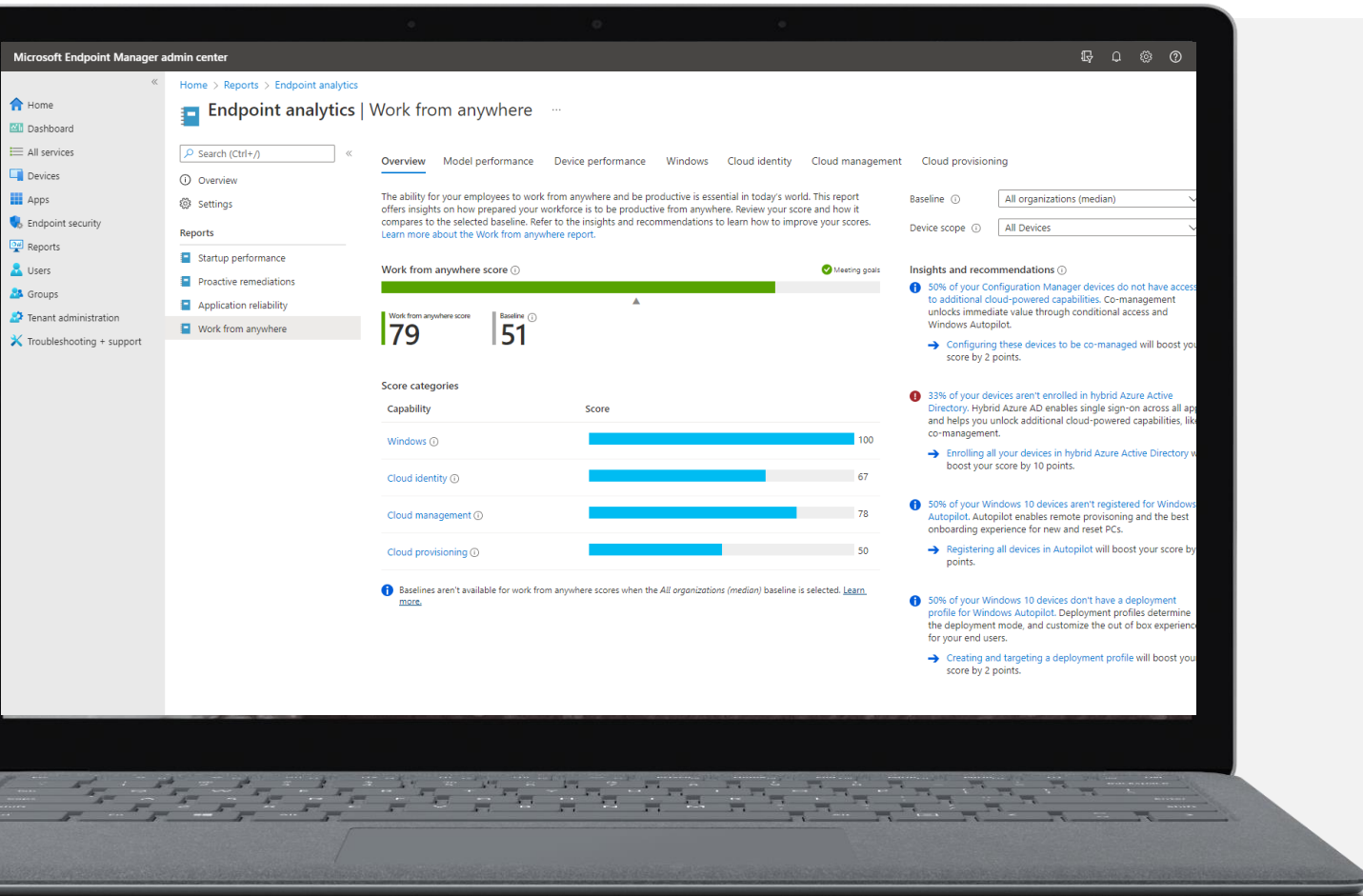


80% deployment time saved with Microsoft Intune.*

*"The Total Economic Impact™ Of Microsoft Endpoint Manager," a commissioned study conducted by Forrester Consulting, April 2021. Forrester based all savings estimates on the composite organizations developed for its TEI studies.

Proactively manage the quality of user experiences

POWER BETTER USER EXPERIENCES



Use app and device health scores to improve the everyday experiences of end users with Endpoint analytics.

Remediate issues before they impact end users and provide Remote Help* for live troubleshooting.

Provide unobtrusive application protection with unified mobile application management.

*Remote Help service is a premium add-on feature

Windows 11 and Intune



Cut cost and complexity with Windows 11 Enterprise and Microsoft Intune



Protect the digital worker

Cloud managed security built into **Windows 11 Enterprise**



Simplify IT management

Proactive remediation and automation in **Microsoft Intune**

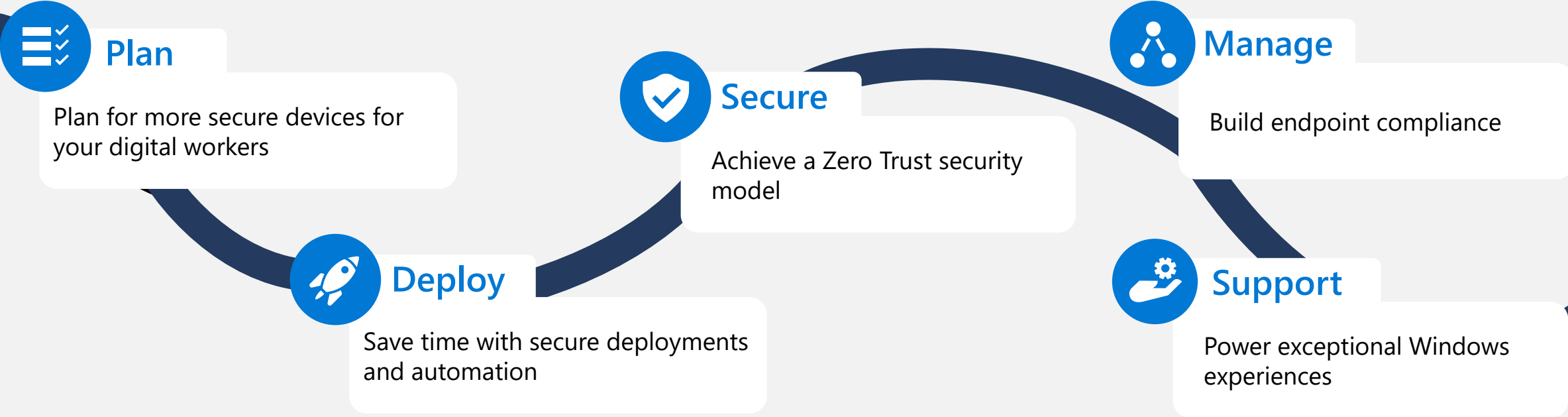


Power better experiences

Creating essential productive and **protected experiences**

Taking the path to reduced TCO

Simple and Safe: The path forward



Windows 11 Enterprise
Microsoft Intune

Modernize your endpoint estate

A plan for better device security

PLAN



What you can do

Have complete visibility

Create inventory

New Windows 11 devices

Always secure by default

How you can do it

Endpoint analytics Upgrade Readiness

Update compatibility reports

Windows 11 hardware requirements

Choose [Secure Core PCs](#) with Pluton

Why it matters

"86% of Security Decision Makers agree outdated PC hardware leaves organizations more vulnerable."

Security Decision Maker Study

Zero touch deployments for new PC

Save time with secure deployments and automation

DEPLOY



What you can do

Rapidly onboard digital workers

Ship new devices to employees anywhere

Simplify authentication and automate MDM enrollment

Local upgrade to Enterprise edition

Ensures app & user data are availability

How you can do it

Zero Touch deployment with **Windows Autopilot**

MFA based on **Azure AD** with **Windows Hello for Business**

Automated **Windows Enterprise activation**

Deploy **targeted apps** for instant productivity

Why it matters

"Device deployment and provisioning using Autopilot, including document migration, saves several hours per device implementation, adding up to a three-year PV of \$102,000 or \$137 in time savings per deployment."

-Forrester TEI study Windows Pro devices

A non-intrusive and reliable upgrade experience

Automation save time and increases protection

DEPLOY



What you can do

Upgrade eligible Windows 10 devices

Repurpose older Windows 10 devices to maximize existing investments

Identify app and compatibility status, including browser-based apps

How you can do it

Windows Update for Business deployment service to targets

Cloud provision Windows 365 on ineligible devices

App compatibility with upgrade readiness reporting

Setup Microsoft Edge in IE mode

Why it matters

"We have received positive feedback from people who have upgraded [to Windows 11]. It was a simple upgrade, a smooth and unintrusive process."

-Technical lead, insurance company

Endpoint analytics

DEPLOY



Microsoft Endpoint Manager admin center

Home > Reports > Endpoint analytics

Endpoint analytics | Work from anywhere

Search (Ctrl+/)

Overview **Windows** Cloud identity Cloud management Cloud provisioning

Overview
Settings

Reports

- Startup performance
- Proactive remediations
- Application reliability
- Work from anywhere**

Refresh Export Columns

Search by device name, manufacturer, model or OS version Device scope: All Devices

Showing 0 to 0 of 0 records < Previous Page 0 of 0 Next >

Add filter

Device name ↑↓	Managed by ↑↓	Manufacturer ↑↓	Model ↑↓	OS version ↑↓	Windows 11 readiness sta... ↑↓	Windows 11 readiness reason
Adele Vance	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19041.1288	Capable	TPM, CPU family
Alex Wilber	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19042.1526	Not capable	CPU family
Debra Berger	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19041.1288	Capable	TPM, CPU family
Diego Siciliani	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19042.1526	Not capable	CPU family
Grady Archie	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.22000.493	Upgraded	--
Invin Sayers	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19041.1288	Capable	TPM, CPU family
Isaiah Langer	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19042.1526	Not capable	CPU family
Johanna Lorenz	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.22000.493	Upgraded	--
Joni Sherman	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19041.1288	Capable	TPM, CPU family
Lee Gu	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19042.1526	Not capable	CPU family
Lidia Holloway	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.22000.493	Upgraded	--
Lynne Robbins	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19041.1288	Capable	TPM, CPU family
Megan Bowen	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.19042.1526	Capable	CPU family
Miriam Graham	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.22000.493	Upgraded	--
Nestor Wilke	Contoso Electronics	Microsoft Corporation	Surface Pro 3	10.0.22000.493	Upgraded	--

Reduce security risks

Achieve a Zero Trust security model

SECURE



What you can do

Verify user identities

Require strong authentication methods

Secure devices with tailored baselines

Encrypt all local data storage.

Prevent unknow apps from running

How you can do it

Simplify MFA & SSO with **Windows Hello for Business**

Enable SmartScreen **advanced Phishing protection**

Configuration Lock prevents changes

Application Guard protects from malware and **Application Control** only allows trusted apps

Set **BitLocker** and key escrow

Why it matters

"Windows 11 has advanced encryption and data protection capabilities. They have added robust network and system security control sets and safeguards that would at least prevent a large number of viruses and malware that we see."

-CISO, IT services

Reduce risks with managed security

Achieve a Zero Trust security model

SECURE



What you can do

Modernize endpoint security configuration in the cloud

Ensure least privilege access

Reduce risk of breach

Manage BYO scenarios with policies that protect company data

How you can do it

Migrate **Group Policy Objects** to the cloud for management consistency.

Set Azure AD *risk-based* **Conditional Access** to control access to resources and enforce *app-based* conditions with **Edge** and LOB apps

Use **Risk Scores** to resolve endpoint issues and help unify IT and security teams

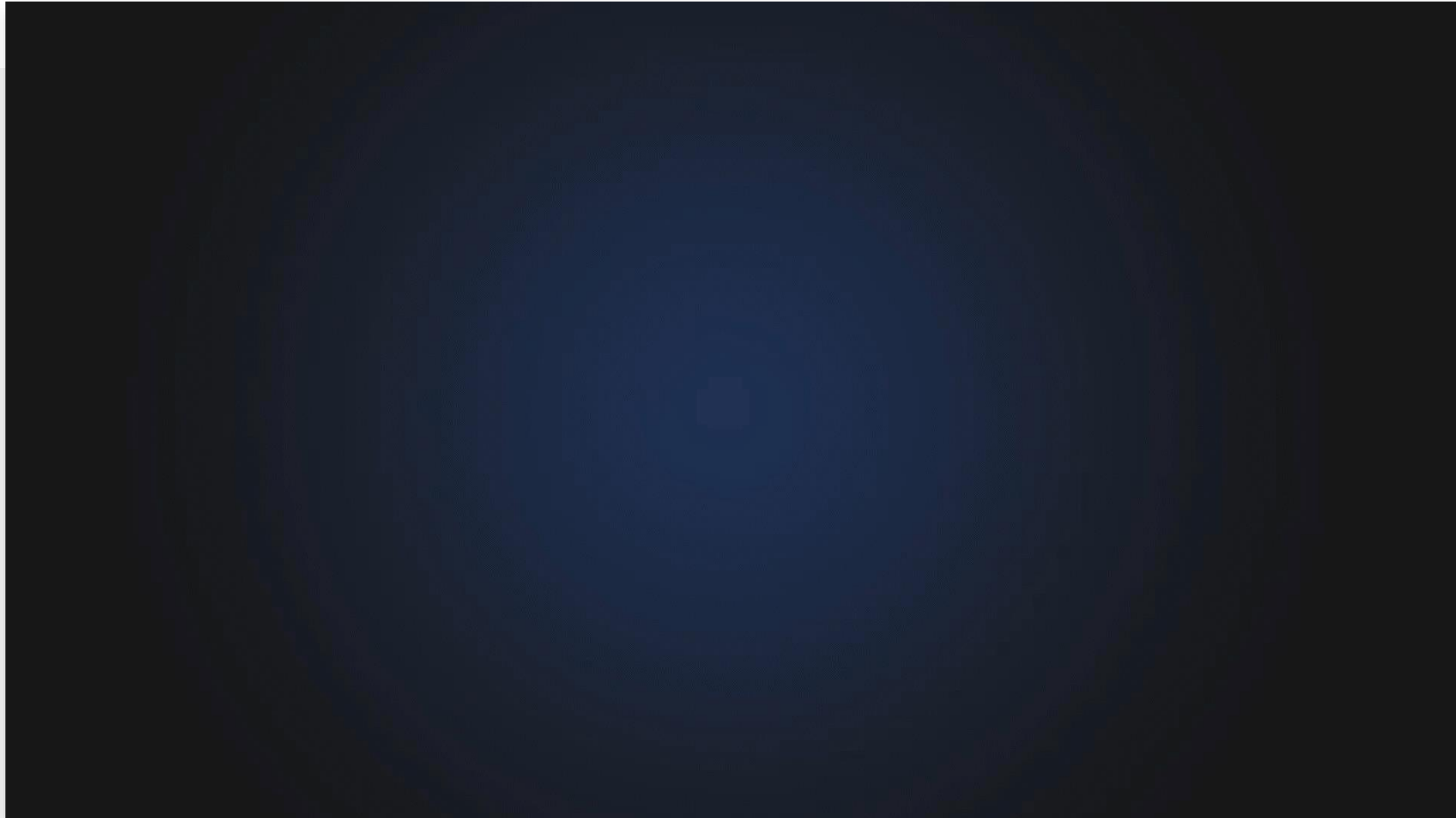
Why it matters

"Microsoft Intune is the center of our endpoint protection strategy. It sets initial configuration through baselines and policy to harden our Windows and iOS devices. That way, we can disable access for devices that do not pass compliance policy."

-Head of Productivity and Endpoint Engineering

Security baseline

SECURE



Automatic and managed updates close security gaps

Enforce endpoint compliance

MANAGE



What you can do

Modernize endpoint security configuration in the cloud

Ensure least privilege access

Reduce risk of breach

Manage BYO scenarios with policies that protect company data

How you can do it

Let Microsoft automate updates with **Windows Autopatch**

Control quality, driver, and feature updates with **Windows Update for Business deployment service**.

Tailor with **custom compliance** policies

See endpoints that don't meet policies with **Endpoint analytics**

Why it matters

"Its simplicity is what makes it so great."

- One of our early enterprise Autopatch customers summed it up in one sentence:

Windows Autopatch

SUPPORT



The screenshot shows the Microsoft Endpoint Manager admin center interface. The top navigation bar includes the user name 'Connie Wilson' and the organization 'CONTOSO'. The left sidebar contains a navigation menu with categories like 'Home', 'Dashboard', 'All services', 'Devices', 'Apps', 'Endpoint security', 'Reports', 'Users', 'Groups', 'Tenant administration', and 'Troubleshooting + support'. The 'Tenant administration' category is expanded, showing a list of sub-items including 'Tenant status', 'Microsoft Tunnel Gateway', 'Connectors and tokens', 'Filters (preview)', 'Roles', 'Azure AD Privileged Identity Management', 'Diagnostics settings', 'Workbooks', 'Audit logs', 'Device diagnostics', 'End user experiences', 'Customization', 'Custom notifications', 'Terms and conditions', and 'Windows Autopatch'. The 'Windows Autopatch' section is selected, and the 'Tenant enrollment' sub-item is highlighted.

Home > Tenant administration > Tenant admin | Tenant enrollment

Welcome to Windows Autopatch

Windows Autopatch is a monthly subscription service to manage all updates for Windows 10 and Windows 11 environments, Windows 365 clients, Microsoft 365 apps, Microsoft Teams, and Microsoft Edge. For technical information, [learn more about Microsoft Autopatch](#). If you're unfamiliar with Windows Autopatch, [learn more about the service generally](#).

To enroll your tenant, start with the readiness assessment tool

The readiness assessment tool checks certain details of your Intune and Azure AD settings to ensure they're ready for the best experience when you enroll in Windows Autopatch. Run this tool whenever you want to confirm you've taken care of any reported issues.

We'll give you a list of things you need to do before enrolling in the tool, [learn more about our prerequisites](#). You must be signed in as at least Intune admin to run this tool. Some checks require additional permissions. [Learn more about these checks](#), permissions, and data storage. Once the tool shows you're ready, you can enroll your tenant into the service. You will not need to run the tool again. You must be a Global Administrator to enroll into the service.

This tool collects, assesses, and stores data in the service to perform the assessment. We do not collect or store personal data, nor share your data with other services. However, we do collect system metadata and organizational information to complete this assessment. We retain data for 12 months after you last use this tool to provide and improve the service. After 12 months, we retain it in de-identified form without company name. You can choose to delete the data we collect. [Learn more about the checks](#) and review the [privacy statement](#).

Select check box to allow Microsoft to assess and store results for the readiness assessment, and then select **Agree**.

Agree

Proactively manage worker experiences and support costs

SUPPORT



Power exceptional Windows experiences

What you can do

Get ahead of issues with device health and performance monitoring

Optimize productivity: update off hours

Onboard flex workers on personal or partner devices

Reduce cost of maintaining on premises print servers

Mitigate the need for additional training and support

How you can do it

Endpoint analytics with **proactive remediation**

Reduce vulnerability with **Windows Autopatch** or **WUfBds**

Provision Windows 11 with **Cloud PC** for contractors and temp workers

Move print to the cloud with **Universal Print**

Deliver **organizational messages** within the Windows experience

Why it matters

"Windows 11 is that extra step in productivity that I didn't know I was missing. It's smarter, faster, and didn't break a thing."

-Comvalius, IT Infrastructure Specialist, Invendows B.V (Nextxpert)

Secure the digital workforce with Windows 11 Enterprise and Intune



Protect the digital worker

Zero Trust security built-in

Windows, Microsoft Intune and Azure AD can reduce the data breach risk by 45% and overall IAM security management costs by 50%.



Simplify IT management

Proactive remediation and automation from a single source

Improved security adds \$1.2 million to the bottom line.

The Total Economic Impact™ Of Microsoft Endpoint Manager," commissioned by Microsoft, Forrester Consulting, April 2021



Power better experiences

Protected and productive without downtime

Windows customers can obtain between 109% and 394% projected return on investment.

"The Total Economic Impact™ Of Windows 11," commissioned by Microsoft, Forrester Consulting, July 2022



TCO and cost savings benefits from Microsoft 365 E3



Enterprise Mobility and Security powered by Microsoft 365

Solution	Feature/capability description	Microsoft 365 Business Premium	Microsoft 365 F1/F3/E3	Microsoft 365 E5
Identity and Access Management	Simplified access management and security: Centrally manage single sign-on across devices, your datacenter, and the cloud.	●	●	●
	Multi-factor authentication: Strengthen sign-in authentication with verification options, including phone calls, text messages, or mobile app notifications, and use security monitoring to identify inconsistencies	●	●	●
	Conditional access: Define policies that provide contextual controls at the user, location, device, and app levels to allow, block, or challenge user access.	●	●	●
	Risk-based conditional access: Protect apps and critical data in real time using machine learning and the Microsoft Intelligent Security Graph to block access when risk is detected.			●
	Advanced security reporting: Monitor suspicious activity with reporting, auditing, and alerts, and mitigate potential security issues using focused recommendations.		●	●
	Privileged identity management: Provide timely, on-demand administrative access to online services with access-related reporting and alerts.			●
	Windows Server Client Access License (CAL)¹: Provide each user access to server functions from multiple devices for a single fee.		●	●
Managed Mobile Productivity	Mobile device management: Enroll corporate and personal devices to provision settings, enforce compliance, and protect your corporate data.	●	●	●
	Mobile application management: Publish, configure, and update mobile apps on enrolled and unenrolled devices, and secure or remove app-associated corporate data.	●	●	●
	Advanced Microsoft Office 365 data protection: Extend management and security capabilities across users, devices, apps, and data, while preserving a rich, productive end-user experience.	●	●	●
	Integrated PC management: Centralize management of PCs, laptops, and mobile devices from a single administrative console, and produce detailed hardware and software configuration reporting	●	●	●
	Integrated on-premises management: Extend your on-premises management to the cloud from a single console with Microsoft System Center Configuration Manager and Microsoft System Center Endpoint Protection integration for enhanced PC, Mac, Unix/Linux server, and mobile device administration.	●	●	●
Information Protection	Persistent data protection: Encrypt sensitive data and define usage rights for persistent protection regardless of where data is stored or shared.	●	●	●
	Document tracking and revocation: Monitor activities on shared data and revoke access in case of unexpected events.	●	●	●
	Intelligent data classification and labeling: Configure policies to automatically classify and label data based on sensitivity and then apply persistent protection			●
	Encryption key management per regulatory needs: Choose default key management options or deploy and manage your own keys to comply with regulations.			●
Identity-driven Security	Microsoft Advanced Threat Analytics: Detect abnormal behavior in on-premises systems and identify advanced targeted attacks and insider threats before they cause damage.		●	●
	Microsoft Cloud App Security: Gain visibility, control, and protection for your cloud-based apps, while identifying threats, abnormal usage, and other cloud security issues.			●
	Microsoft Defender for Identity²: Detect and investigate advanced attacks and suspicious behaviors on-premises and in the cloud.			●

¹Customers purchasing Windows Server CAL agreements, System Center Configuration Manager, System Center Endpoint Protection, Microsoft Active Directory Rights Management Services CALs via the Microsoft Enterprise Volume Licensing agreements may purchase the Enterprise Mobility + Security Add-on offer

²Microsoft Defender for Identity previously known as Azure Advanced Threat Protection

Paths to modern management



What do we mean by "modern management"?



Customer journey

Limited or no existing management tools

➤ Go directly to the cloud with Microsoft Intune

Existing cloud management

➤ Move additional endpoints and workloads to cloud management

Primarily on-prem management + some cloud

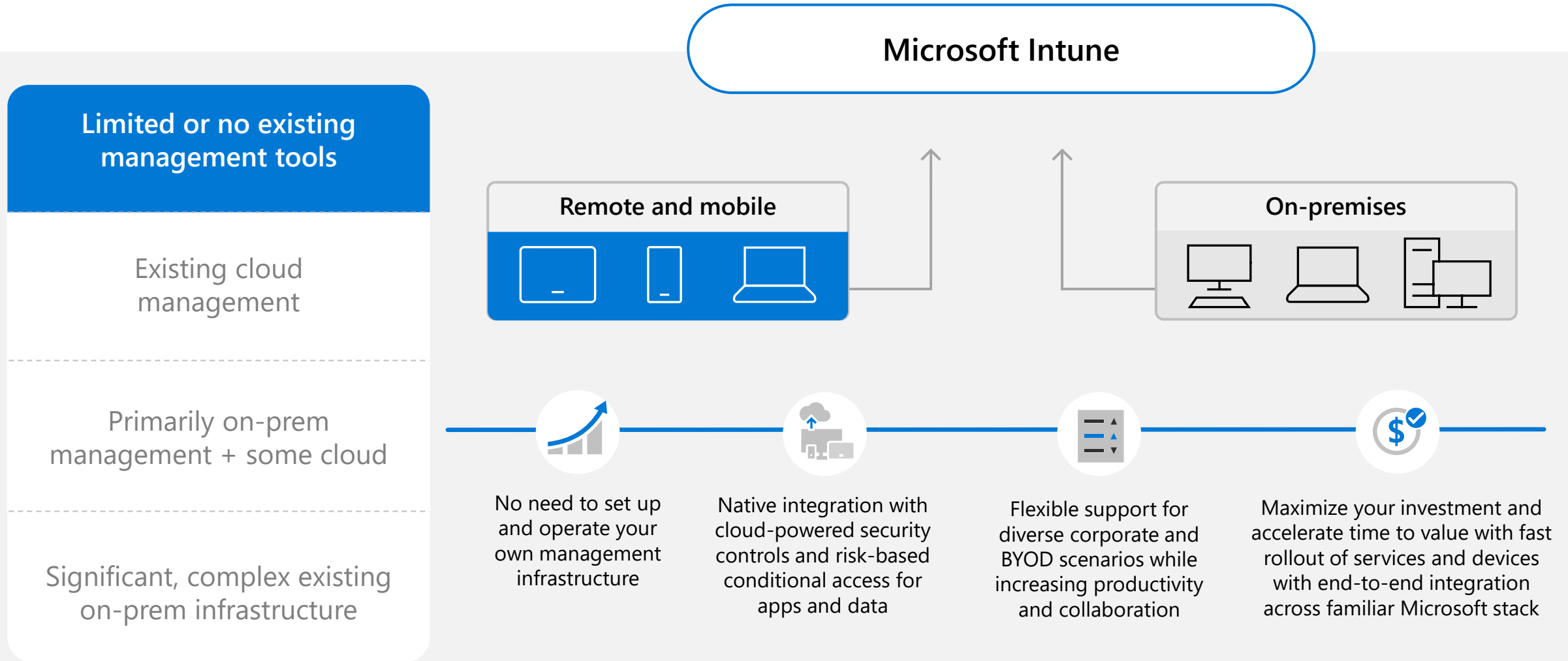
➤ Enroll your Configuration Manager devices into Intune for additional cloud value through co-management

Significant, complex existing on-prem infrastructure

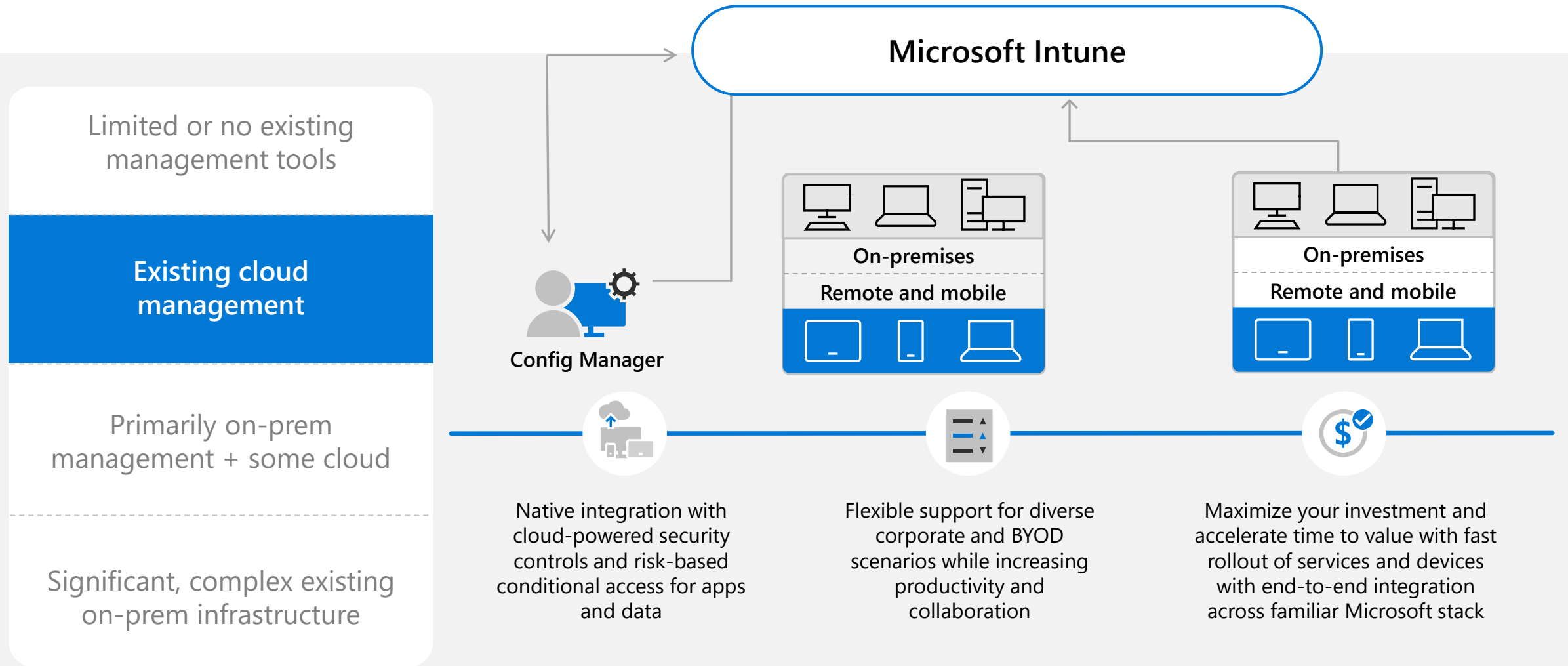
➤ Connect your Configuration Manager site to Intune for instant cloud value (tenant attach)

Modern management

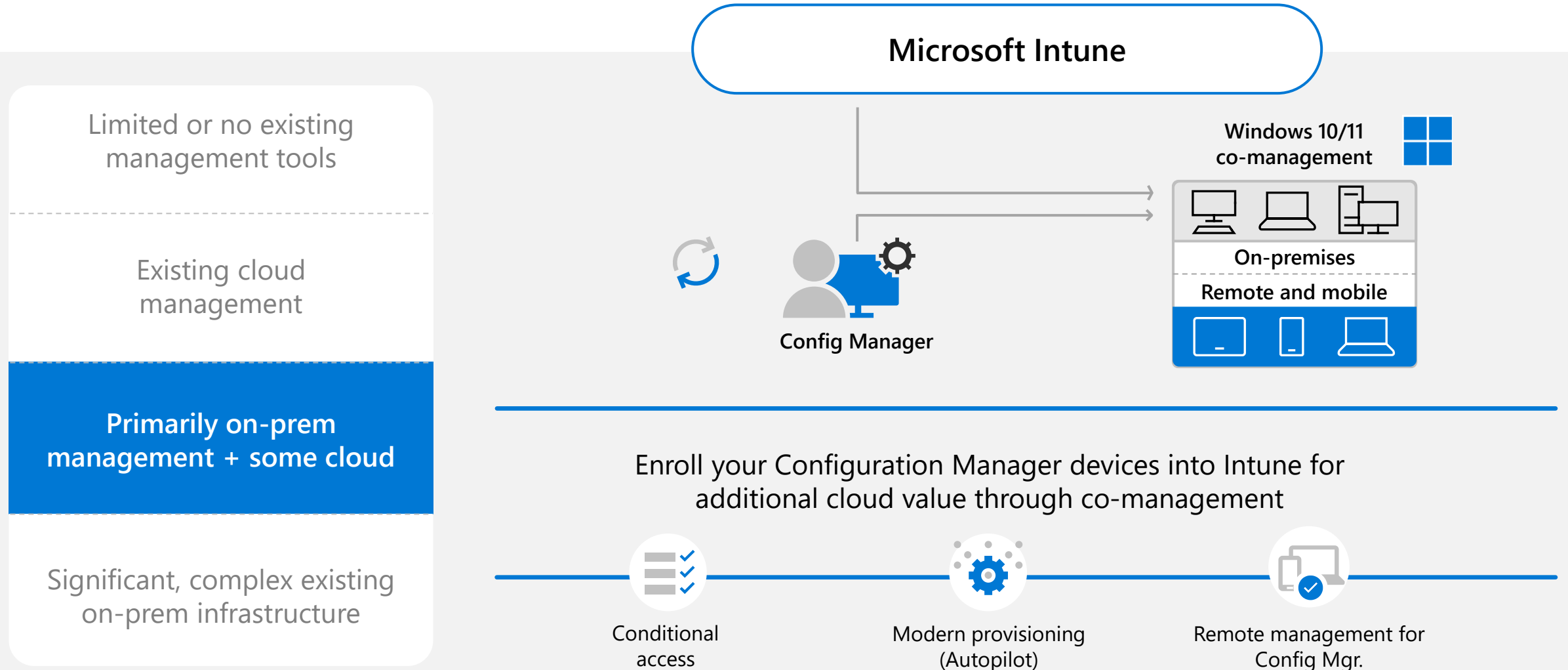
Paths to modern management



Paths to modern management



Paths to modern management



Paths to modern management

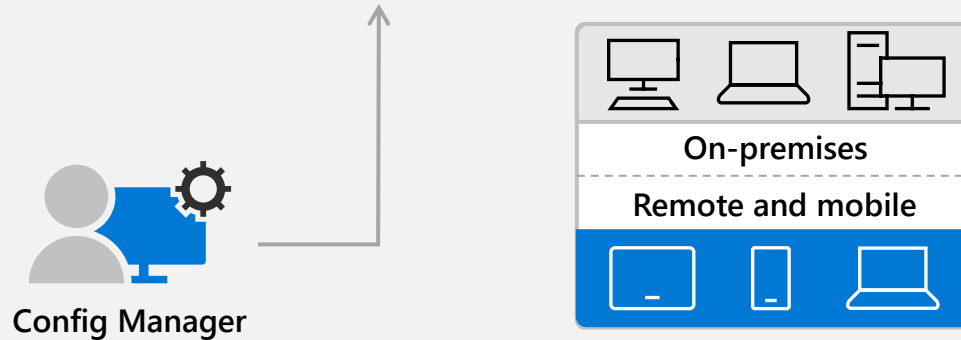
Limited or no existing management tools

Existing cloud management




Primarily on-prem management + some cloud

Significant, complex existing on-prem infrastructure

Microsoft Intune



Connect your Configuration Manager site to Intune for instant cloud value

-  Web-based admin for Config Manager
-  Unified helpdesk and troubleshooting
-  Cloud intelligence drives management

Device lifecycle



Manage the entire device lifecycle 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

Support and retire

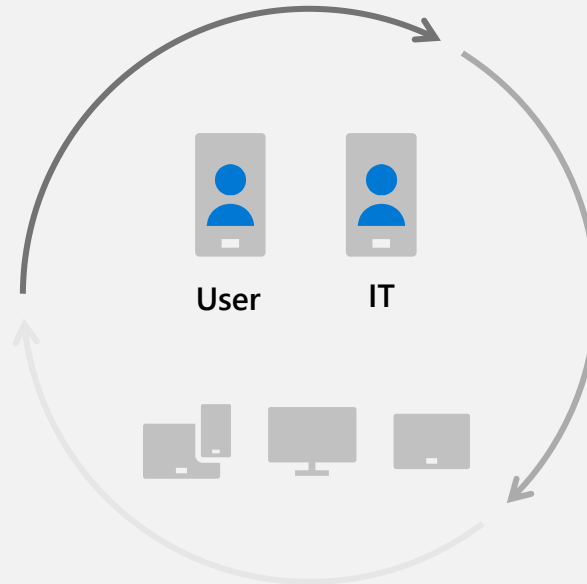
Revoke access to corporate resources

Perform selective wipe

Audit lost and stolen devices

Retire device

Provide remote assistance



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

Microsoft 365 business value

Cloud management



Secure the digital workforce with Windows 11 Enterprise and Intune



Protect the digital worker

Zero Trust security built-in

Windows, Microsoft Intune and Azure AD can reduce the data breach risk by 45% and overall IAM security management costs by 50%.



Simplify IT management

Proactive remediation and automation from a single source

Improved security adds \$1.2 million to the bottom line.

The Total Economic Impact™ Of Microsoft Endpoint Manager," commissioned by Microsoft, Forrester Consulting, April 2021



Power better experiences

Protected and productive without downtime

Windows customers can obtain between 109% and 394% projected return on investment.

"The Total Economic Impact™ Of Windows 11," commissioned by Microsoft, Forrester Consulting, July 2022



TCO and cost savings benefits from Microsoft 365 E3



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.

Improved security



Improved security adds
\$1.2 million to the bottom line.*

“I think from the security standpoint, the integration with the Microsoft platform saves effort on integrating other solutions. Here you have it from one vendor in one platform, and this is a big benefit.”

—
Head of mobile device
management, pharmaceuticals

*The Total Economic Impact™ of Microsoft Endpoint Manager, commissioned by Microsoft, April 2021

Ref.	Metric	Calc.	Year 1	Year 2	Year 3
A1	Average out-of-pocket cost of security breach (scaled to composite)	Forrester study	\$1,210,548	\$1,210,548	\$1,210,548
A2	Hours of lost productivity per affected employee		3.6	3.6	3.6
A3	Average number of affected employees	20,000*10%	2,000	2,000	2,000
A4	Average fully burdened hourly wage	\$50,000+35% benefits/ 2,080 hours	\$32.45	\$32.45	\$32.45
A5	Cost of lost productivity per breach	A2*A3*A4	\$233,640	\$233,640	\$233,640
A6	Average frequency of data breach	Forrester study	2.5	2.5	2.5
A7	Total expected data breach costs	(A1+A5)*A6	\$3,610,470	\$3,610,470	\$3,610,470
A8	Incremental reduction in breaches due to full security stack	Forrester study	4%	4%	4%
A9	Portion attributable to Endpoint Manager	Interviews	20%	20%	20%
A10	Data breach costs avoided	A7*A8*A9	\$28,884	\$28,884	\$28,884
A11	FTEs dedicated to managing security environment	Assumption	20	20	20
A12	Average fully burdened security team salary	\$100,000+35% benefits multiplier	\$135,000	\$135,000	\$135,000
A13	Reduction in time required to manage environment due to Endpoint Manager		20%	20%	20%
A14	Savings from improved security management	A11*A12*A13	\$540,000	\$540,000	\$540,000
At	Improved security	A10 + A14	\$568,884	\$568,884	\$568,884
	Risk adjustment	↓15%			
Atr	Improved security (risk-adjusted)		\$483,551	\$483,551	\$483,551

Three-year total: \$1,450,654

Three-year present value: \$1,202,521

Redeployed IT time



Redeployed IT time frees up more than **\$479,000** in human capital to apply to under-resourced projects.*

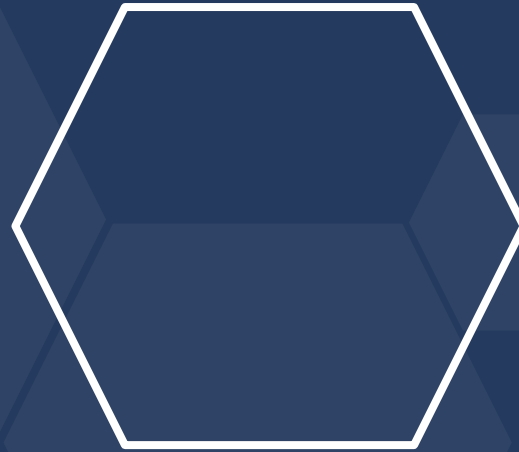
“Whenever there was an upgrade to do, there was a significant risk. If the update failed, that would cause issues across the company. With things being cloud-based now, I don’t have to do upgrades. It’s a real benefit for me.”

—
Head of mobile services, healthcare

*The Total Economic Impact™ of Microsoft Endpoint Manager, commissioned by Microsoft, April 2021

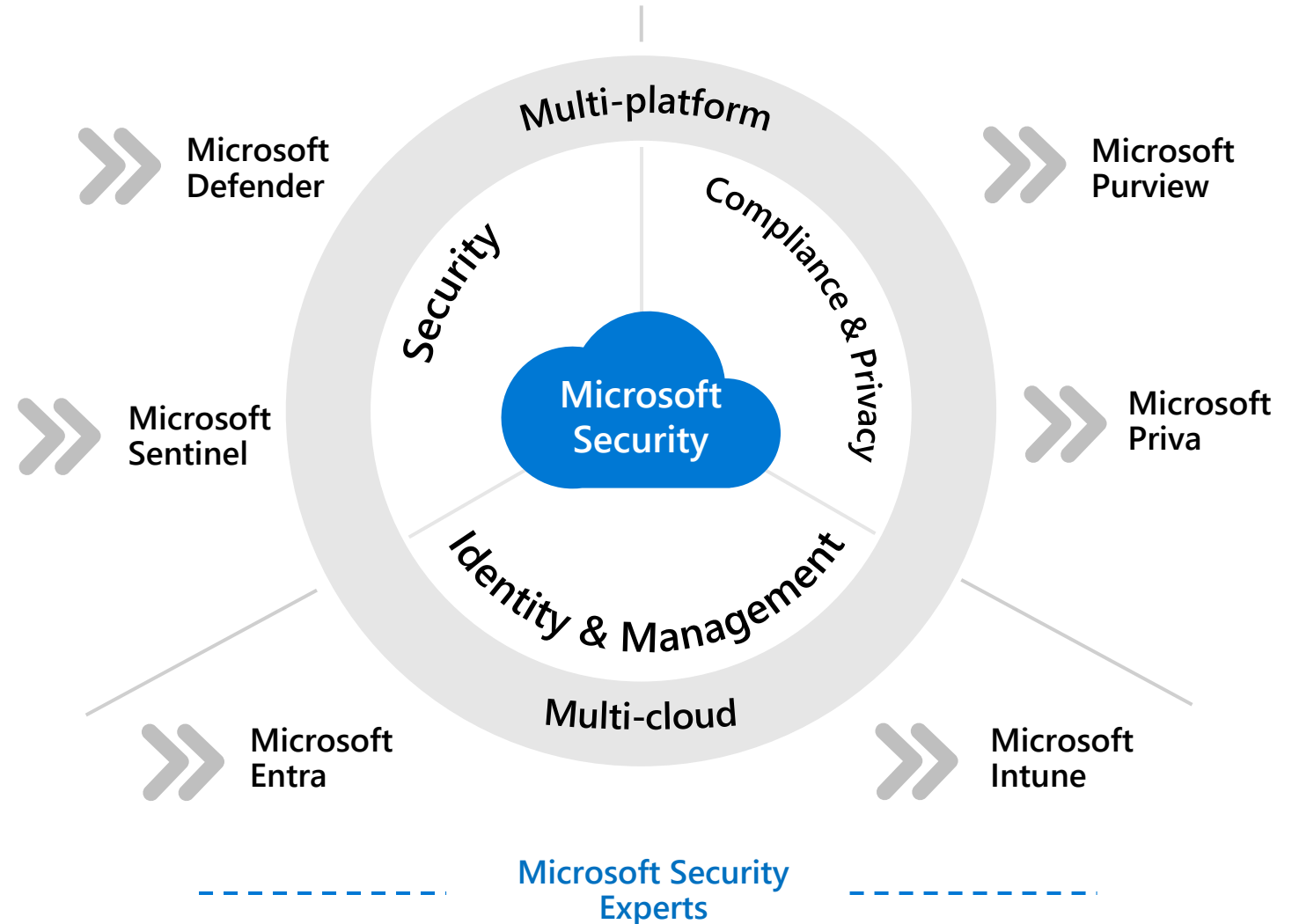
Ref.	Metric	Calc.	Year 1	Year 2	Year 3
D1	IT hours updating/maintaining endpoints before Endpoint Manager	3 per computer; 0.5 per mobile	3,000	18,000	33,000
D2	IT hours updating/maintaining endpoints with Endpoint Manager	0.5 per computer; 0.25 per mobile	1,500	4,000	6,500
D3	Percent of updating hours recaptured		50%	50%	50%
D4	Total IT hours redeployed on configuring/updating devices	$(D1-D2)*D3$	750	7,000	13,250
D5	Fully burdened hourly salary of IT team members	$\$50,000+35\%$ benefits/ 2,080 hours	\$32.45	\$32.45	\$32.45
Dt	Redeployed IT time	$D4*D5$	\$24,338	\$227,150	\$429,963
	Risk adjustment	↓10%			
Dtr	Redeployed IT time (risk-adjusted)		\$21,904	\$204,435	\$386,967
Three-year total: \$613,306			Three-year present value: \$479,601		

Summary



Microsoft Security Portfolio overview

Six product families integrating over 50 product categories



A unified solution to manage endpoints anywhere

Simplify management

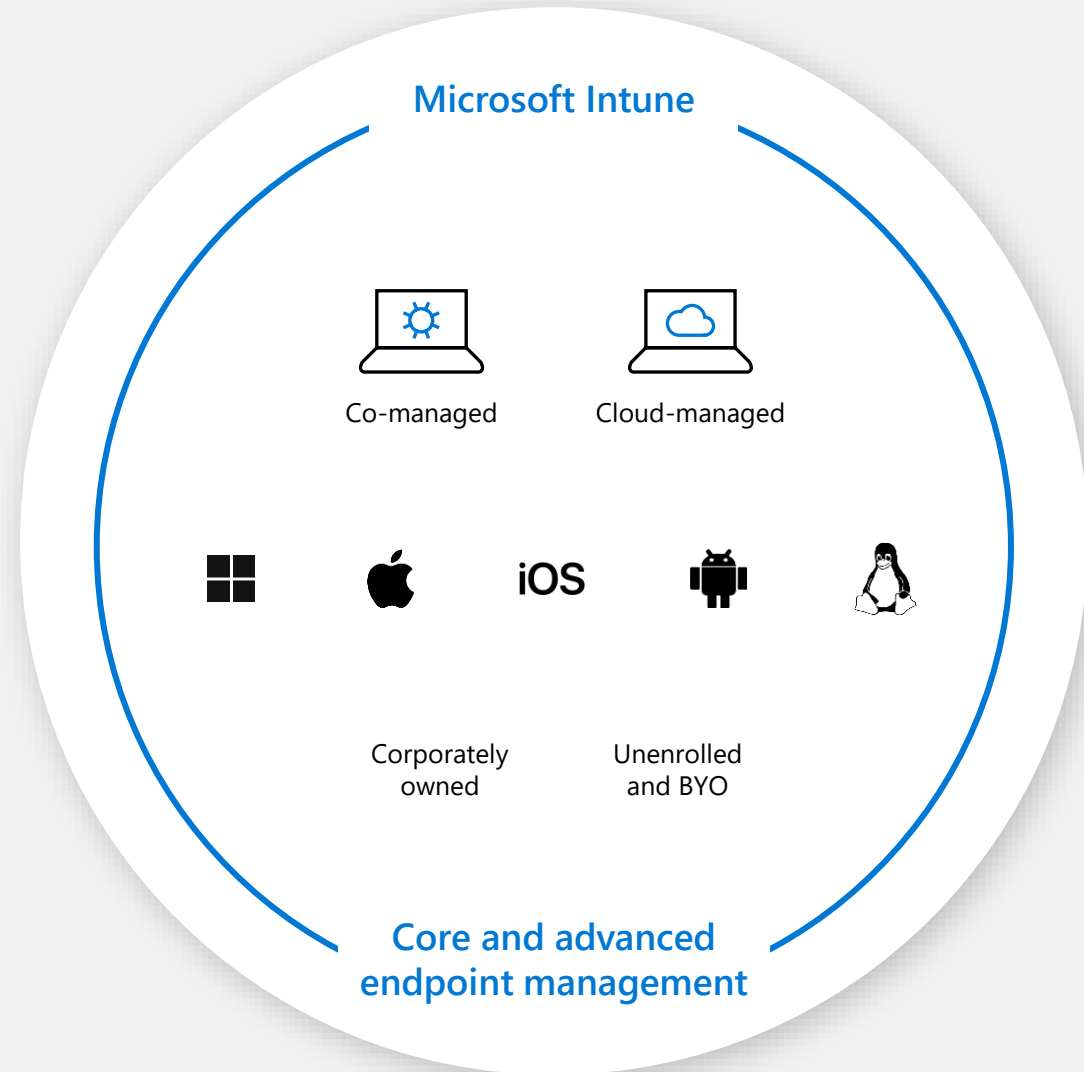
Enable the shift to cloud management, leveraging rich insights on endpoint analytics and cloud-based deployment.

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

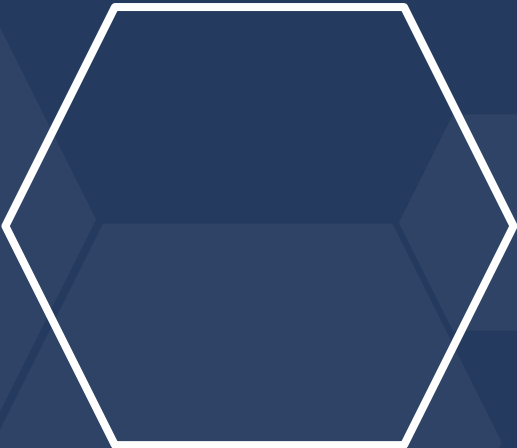
Total Economic Impact study Microsoft Intune

aka.ms/IntuneEconomicValue

Total Economic Impact study Microsoft 365 E3

aka.ms/Microsoft365EconomicValue

Next steps



Next steps

1. Continue with the Security posture assessment activity
2. ...



Thank you.



