Endpoint Management Workshop

Microsoft Endpoint Manager Overview

Market trends

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 cloud is everywhere

90 percent
of enterprises anticipate higher cloud usage than before COVID-19

Endpoint threats are increasing

24 percent
of enterprise mobile endpoints were exposed to device threats in 2019

Continuous updates keep you moving forward

1–4 times/month
is the typical update cycle, ensuring both security and your ability to work seamlessly

Cybersecurity breaches are getting smarter

36 billion
records were exposed through cybercrime in 2020

BYOD is now standard

59 percent
of organizations let employees
use their own devices for work

Today's workplace is evolving

4.3 million
people in the US work from home at least half the time

Top endpoint management challenges

Distributed workers

Remote and hybrid work environments

Endpoint diversity

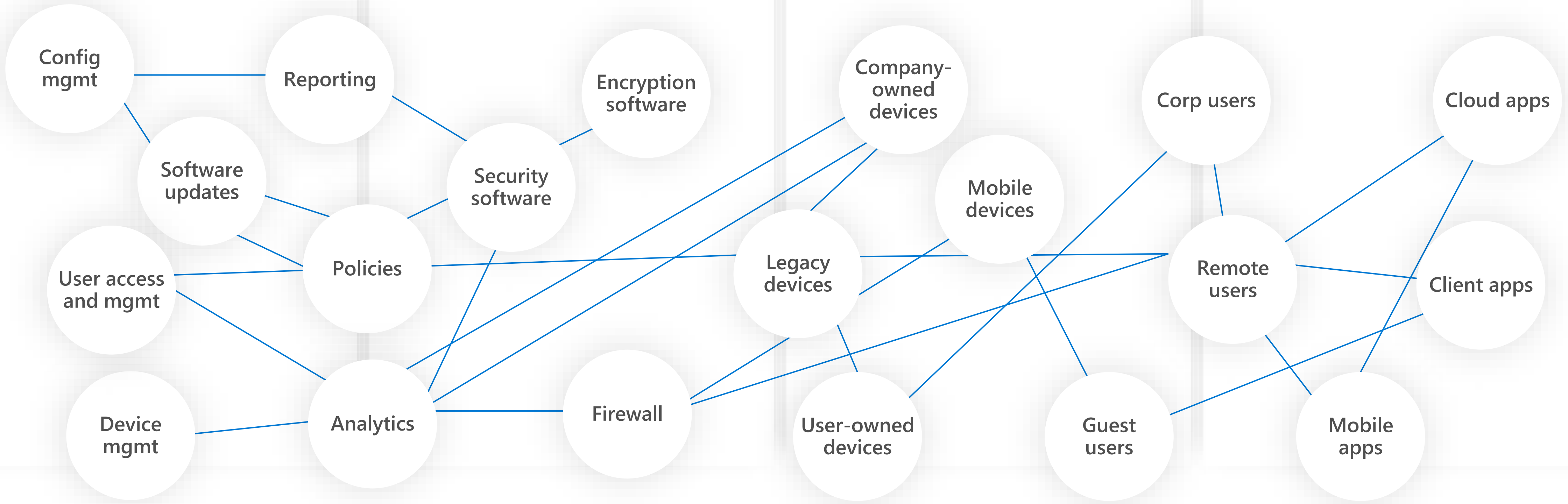
Multiple devices and app platforms

Employee satisfaction

Easy, fast access to company resources

Cybersecurity

Mitigating risk and vulnerabilities



The challenges of endpoint management

Distributed workers

Remote and hybrid work environments

49 million

Remote workers report it takes days—and even weeks—to get issues fixed.

Endpoint diversity

Multiple devices and app platforms

48 percent

IT leaders say ensuring data security is their top challenge in supporting end-user productivity.

Employee satisfaction

Easy, fast access to company resources

44 percent

Remote workers say they have access, but not to everything they need.

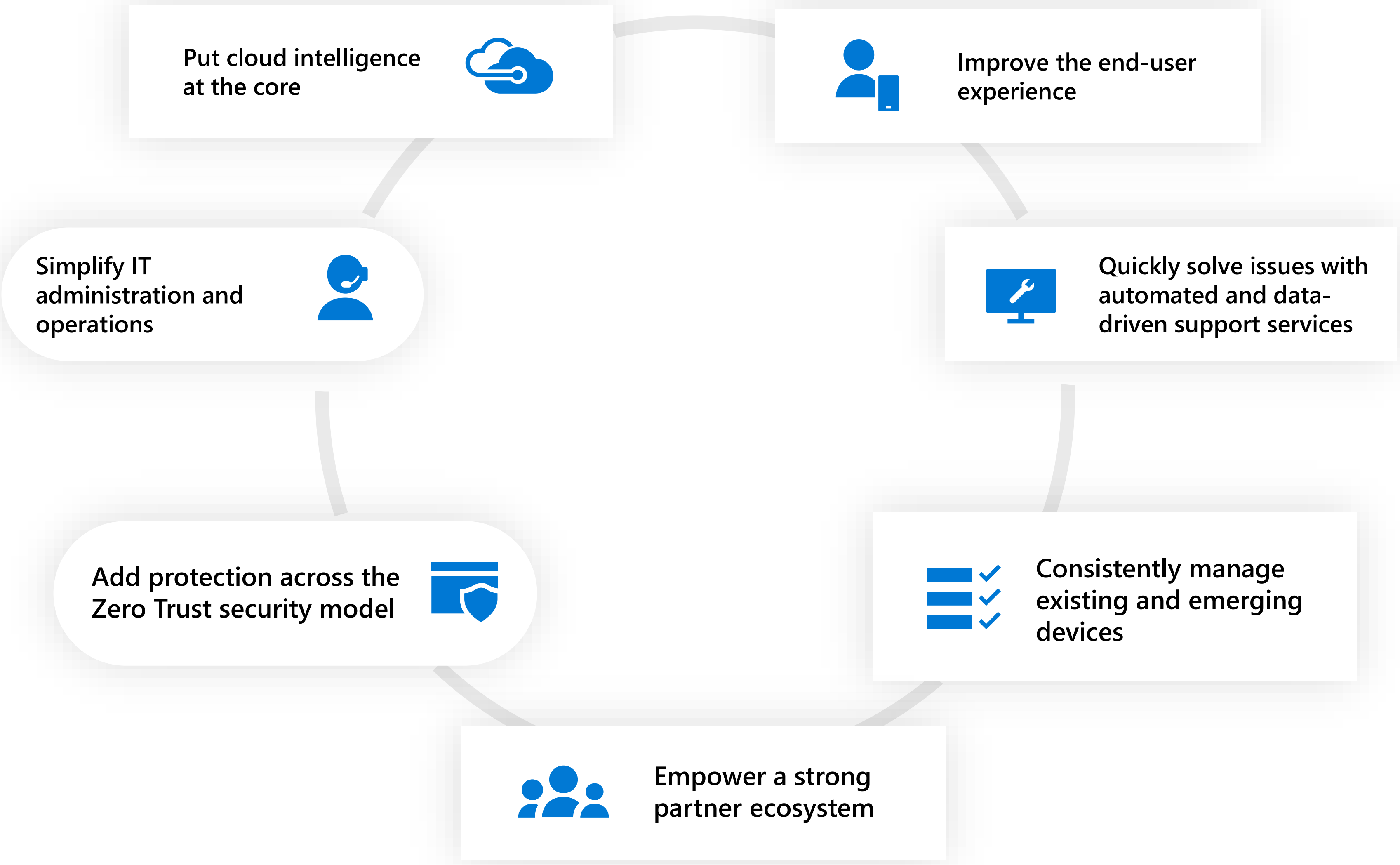
Cybersecurity

Mitigating risk and vulnerabilities

65 percent

Enterprises need to ensure security and compliance across multiple device types.

What do we mean by “modern management”?



Put cloud intelligence at the core

Improve the end-user experience

Quickly solve issues with automated and data-driven support services

Consistently manage existing and emerging devices

Empower a strong partner ecosystem

Add protection across the Zero Trust security model

Simplify IT administration and operations

Microsoft Endpoint Manager

alnafitha IT

Microsoft Endpoint Manager

Endpoint Manager combines the Microsoft Intune and Configuration Manager solutions to provide modern management of endpoints with the protection of a Zero Trust strategy.

Protect apps and devices for a resilient workforce

Maximize digital investment with co-management

Get integrated Conditional Access controls

Use simplified management workflows

Secure managed and unmanaged devices and apps

Unified management

Apps, device controls, and insights are brought together in one cloud-based endpoint management platform.

Built-in protection

IT is empowered to apply the controls needed for a Zero Trust security model and protect their digital estate without getting in the way of user productivity.

Comprehensive scalability

Intuitive management controls, workflows, and analytics ensure healthy and compliant device and app deployments.

Reduced total cost of ownership (TCO)

Microsoft Endpoint Manager

Endpoint Manager combines the Intune and Configuration Manager solutions to provide the modern management of endpoints with the protection of a Zero Trust strategy.

Protect apps and devices for a resilient workforce

Maximize digital investment with co-management

Get integrated Conditional Access controls

Use simplified management workflows

Secure managed and unmanaged devices and apps

What does Microsoft Endpoint Manager enable?

Unified management

Apps, device controls, and insights are brought together in one cloud-based endpoint management platform.

Built-in protection

IT is empowered to apply the controls needed for a Zero Trust security model and protect their digital estate without getting in the way of user productivity.

Comprehensive scalability

Intuitive management controls, workflows, and analytics ensure healthy and compliant device and app deployments.

← Reduced TCO →

Unified Management

Extend the benefits of cloud management

Provide business continuity for remote and hybrid workers

Protect devices for all workers

Manage both virtual and physical assets

Unified management

Extend the benefits of cloud management

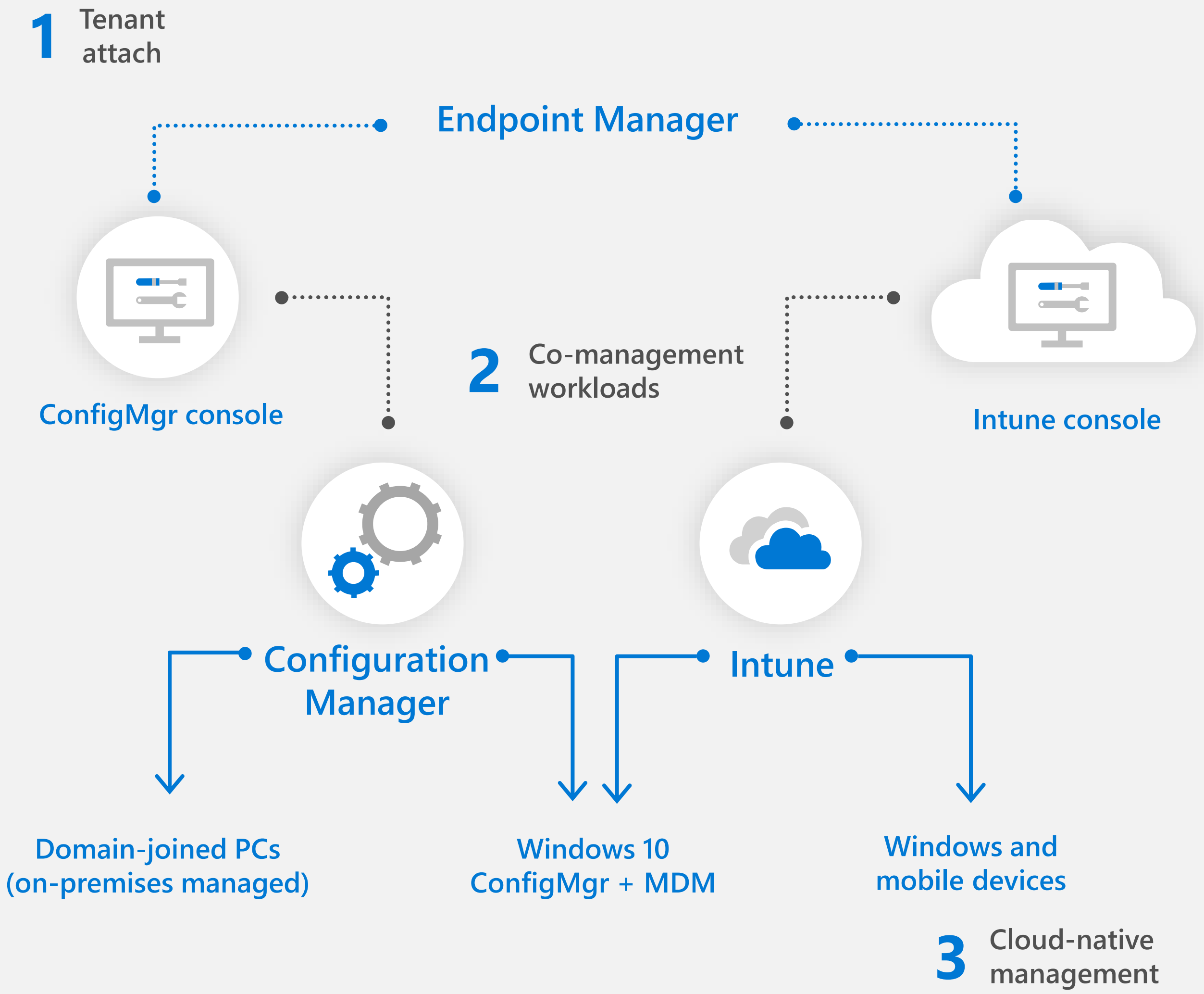
Ability to attach on-premises devices to the cloud with tenant attach

A centralized console to co-manage apps and devices with Windows 10

Centralized visibility across device platforms into device health and compliance

Instant access to Azure Active Directory (Azure AD) across physical and virtual devices

Support for remote actions like restart, remote control, and factory reset


1 Tenant attach
Endpoint Manager
ConfigMgr console
2 Co-management workloads
Intune console
Configuration Manager
Intune
Domain-joined PCs (on-premises managed)
Windows 10 ConfigMgr + MDM
Windows and mobile devices
3 Cloud-native management

Unified management

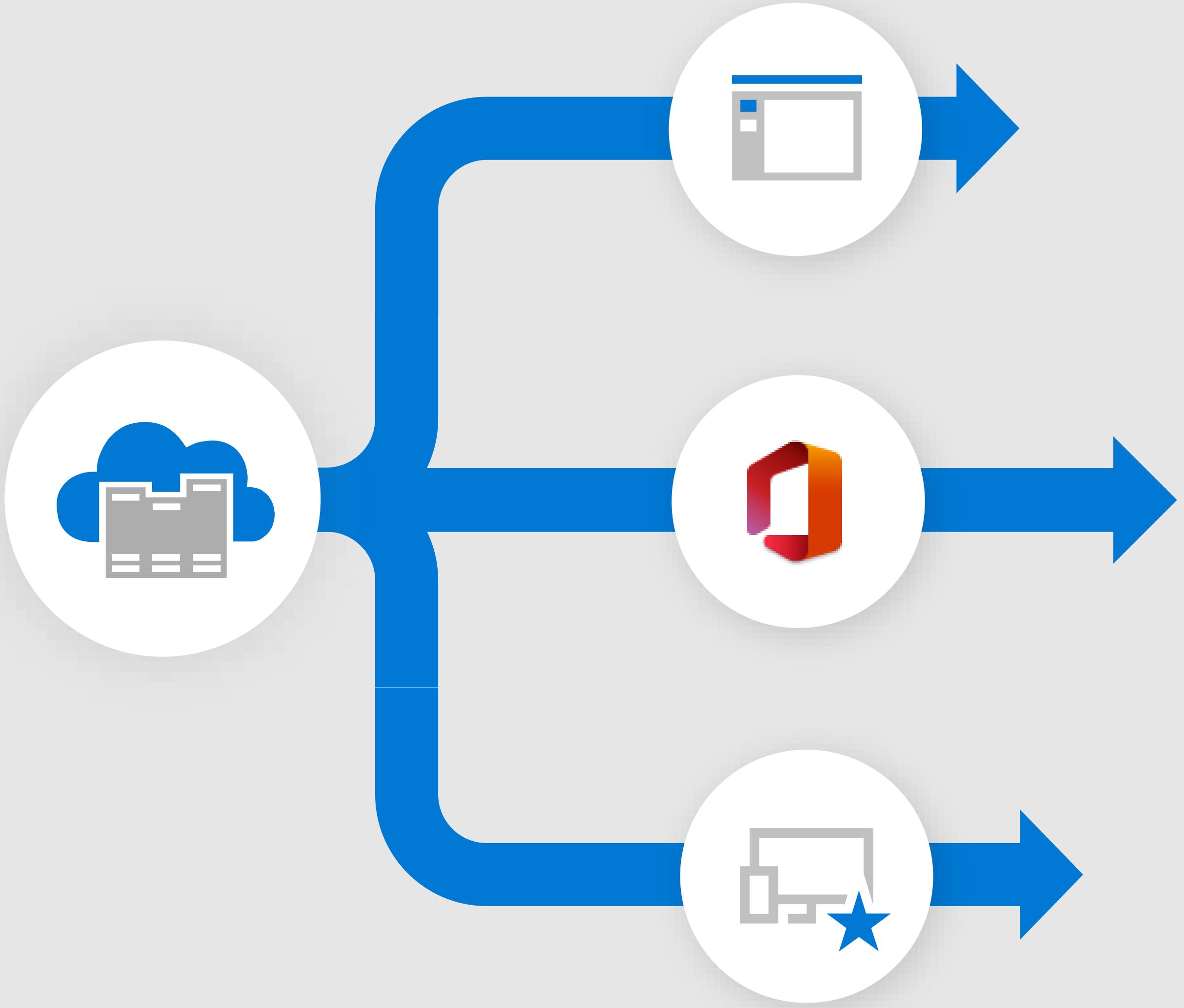
Provide business continuity for remote and hybrid workers

Protection for data on managed and unmanaged devices, whether they’re company-owned or personal

Built-in protection with native integration with Microsoft 365 apps and services

Enterprise-grade remote assistance to quickly resolve end-user issues

Touchless provisioning with Windows Autopilot



Unified management

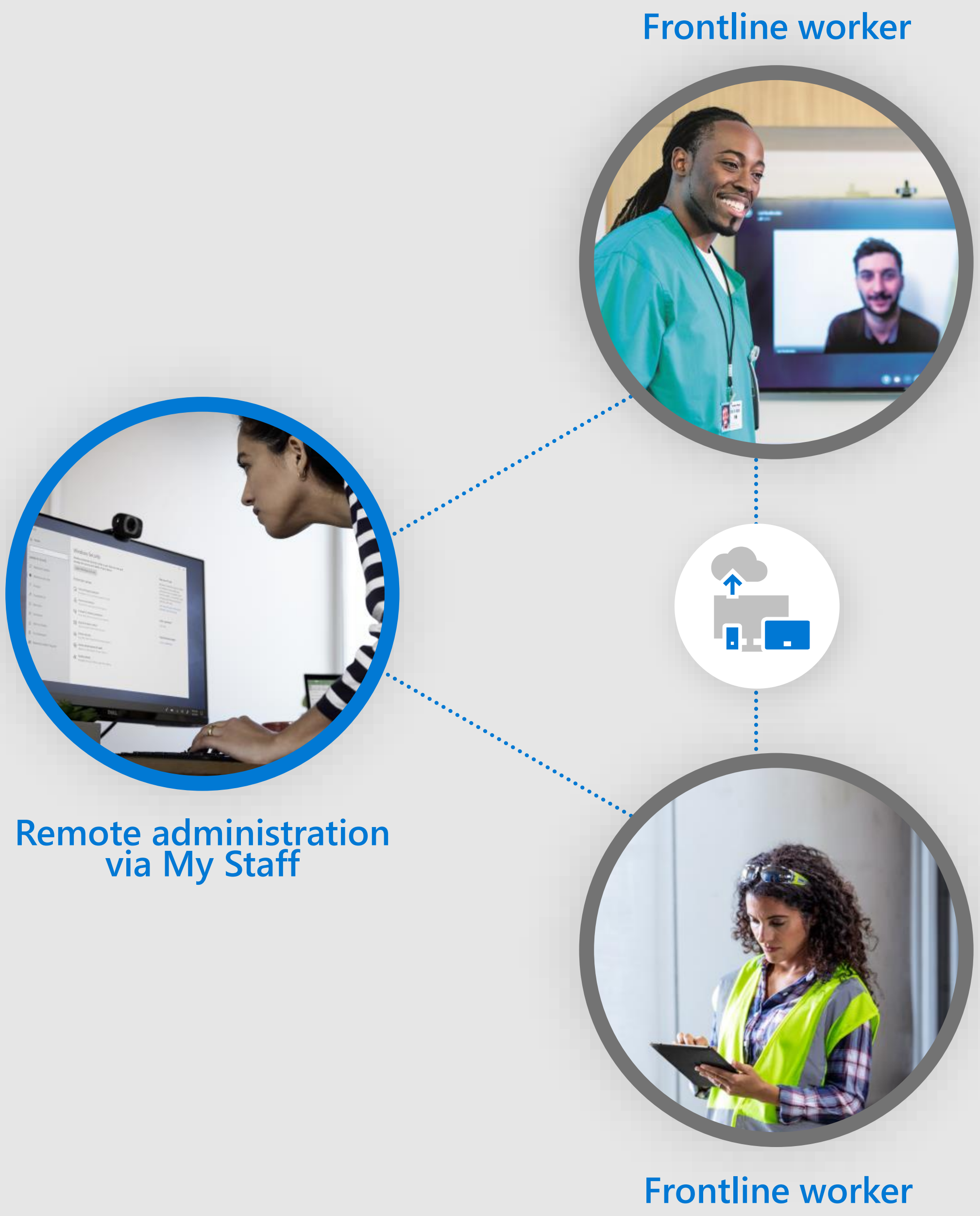
Protect devices for all workers

Shared devices with data removal between users

Simplified experiences with familiar, consistent home screens

Administration permission extended to management at the frontline via My Staff

Reduced helpdesk effort with remote assistance on mobile devices



Frontline worker

Remote administration via My Staff

Frontline worker

Unified management

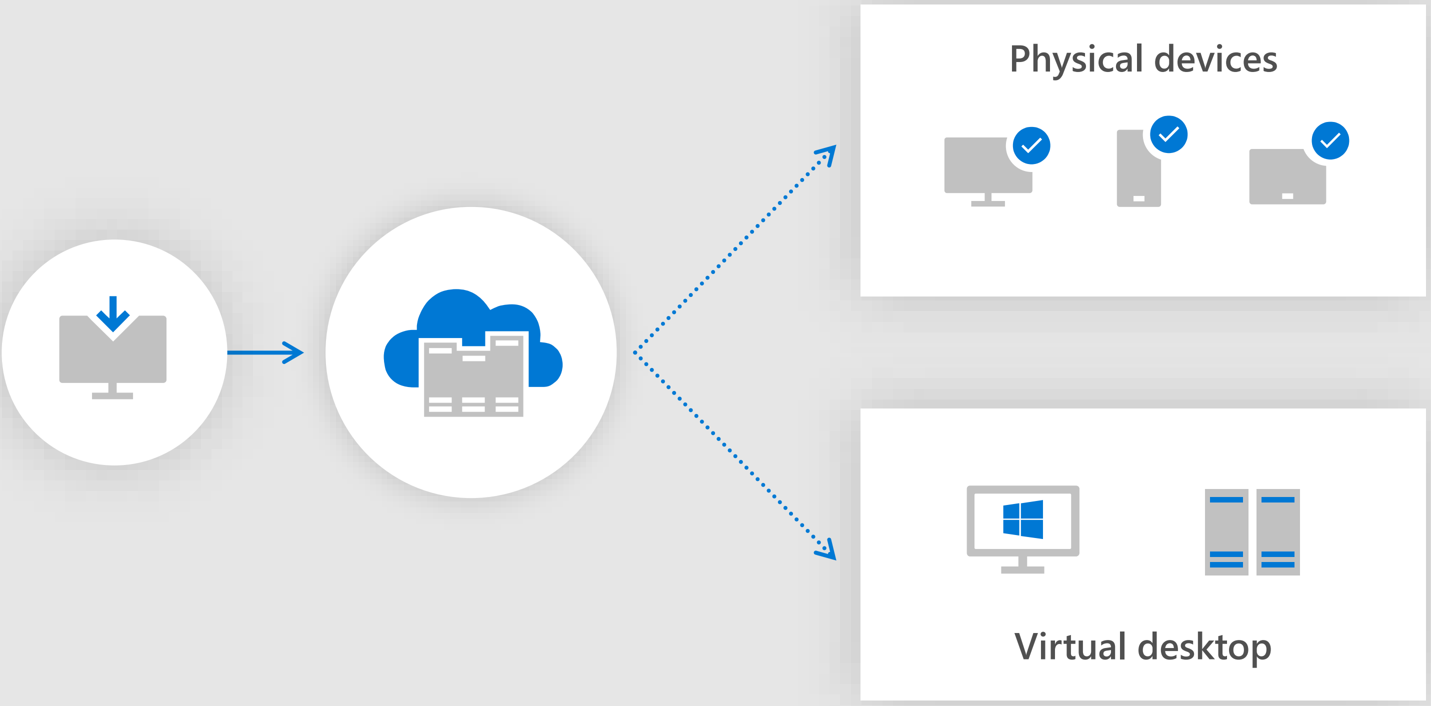
Manage both virtual and physical assets

One tool to manage physical devices and virtual desktops

Integration with Azure Virtual Desktop

Support for a range of virtualization environments, including Windows Server and Microsoft Hyper-V Server

Use of cloud config to easily apply a uniform set of configurations to Windows 10 devices



Built-in protection

- Protect your company data
- Ensure device and app compliance
- Prevent and detect security breaches
- Proactively remediate vulnerabilities

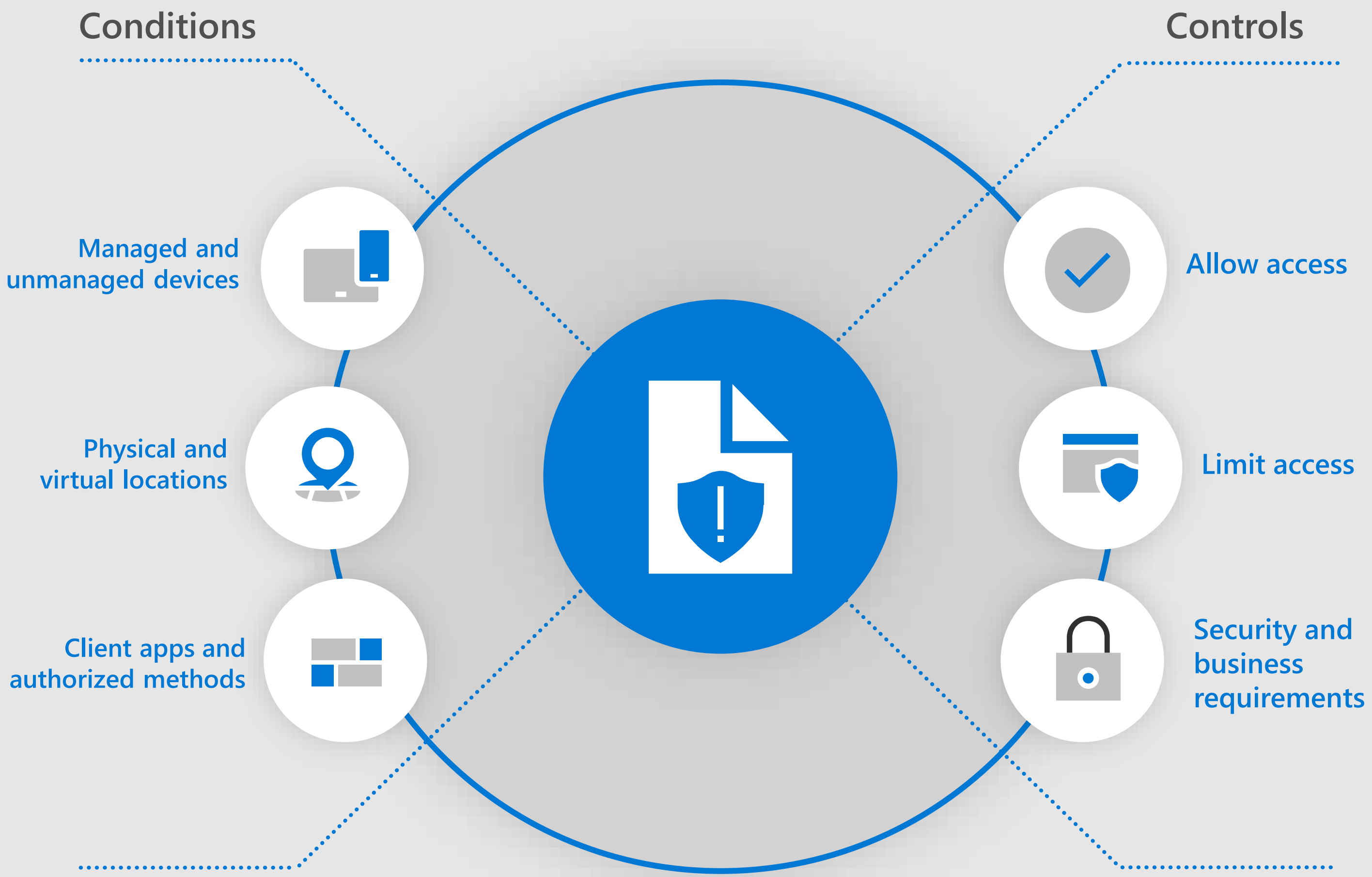
Built-in protection

Protect your company data

Protection for your organization's data, whether it's accessed from managed or unmanaged devices

Conditions can be defined to gate access to your corporate data based on location, device, user state, and application sensitivity

Every device must meet your security and business requirements before accessing your network


Conditions
Controls
Managed and unmanaged devices
Physical and virtual locations
Client apps and authorized methods
Allow access
Limit access
Security and business requirements

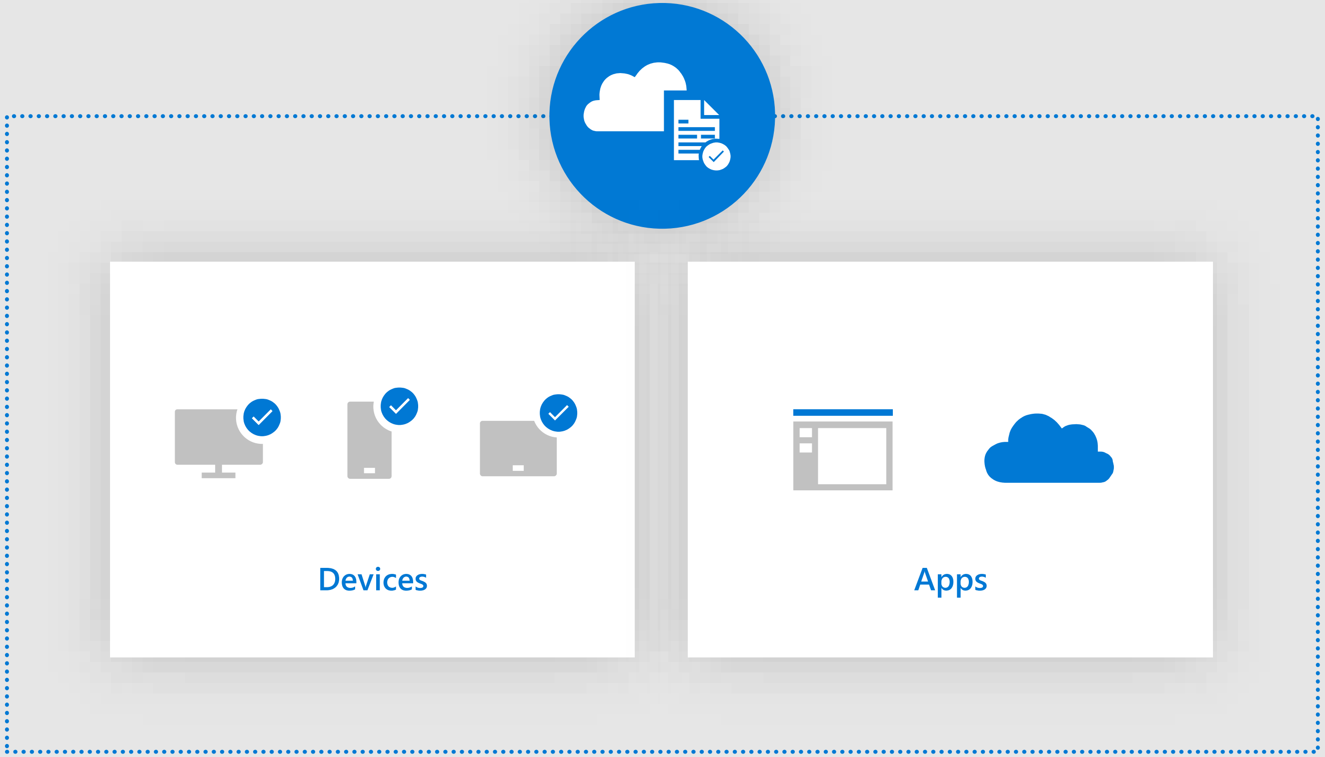
Built-in protection

Ensure device and app compliance

Device compliance policies evaluate devices that don’t comply with rules you specify

Policies with Conditional Access allow or block access to resources

Compliance policies can be deployed according to need:
tenant-wide for all devices or platform-specific for groups of users or devices



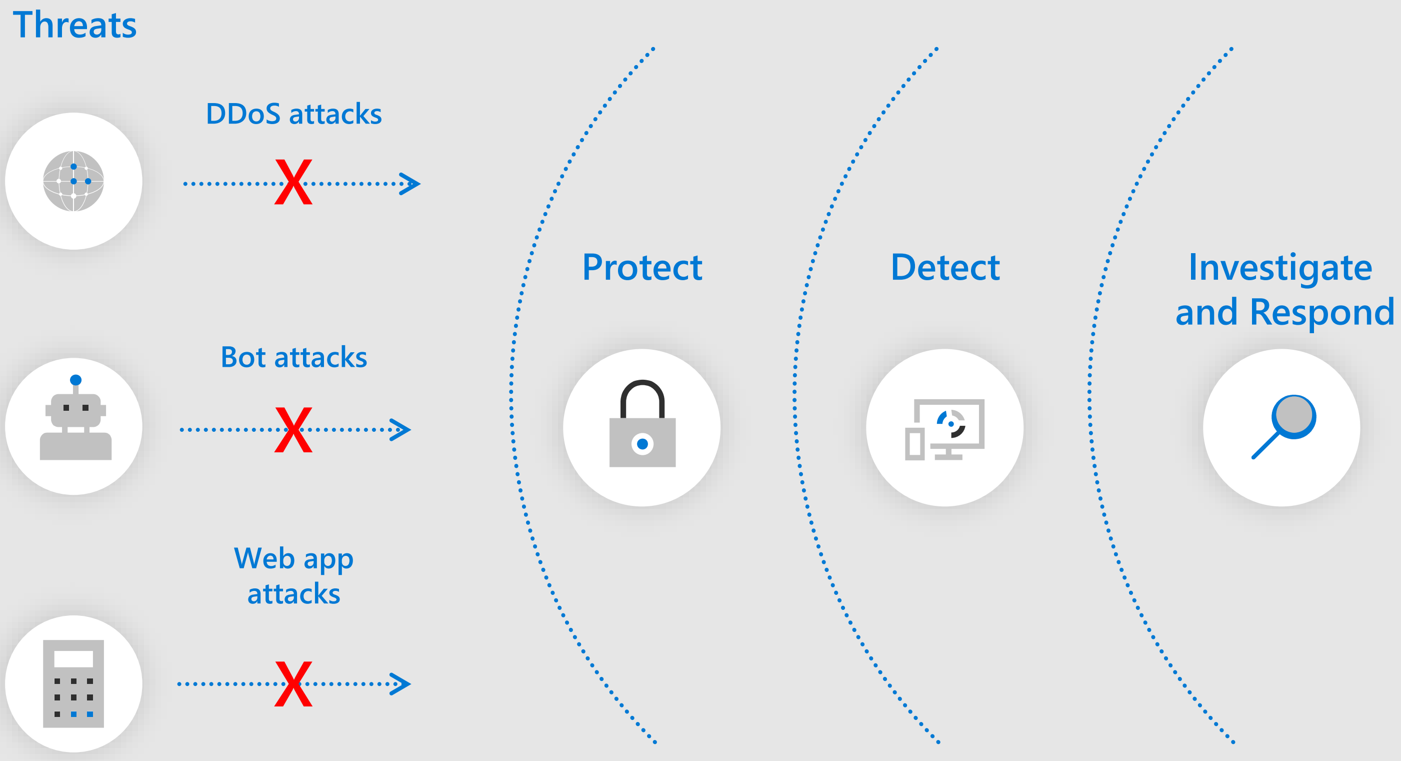
Built-in protection

Prevent and detect security breaches

Integrated security capabilities that detect and respond to vulnerabilities to prevent breaches

Preventative protection, post-breach detection, automated investigation, and rapid response

A foundation of the industry’s deepest insights across devices, identities, and information



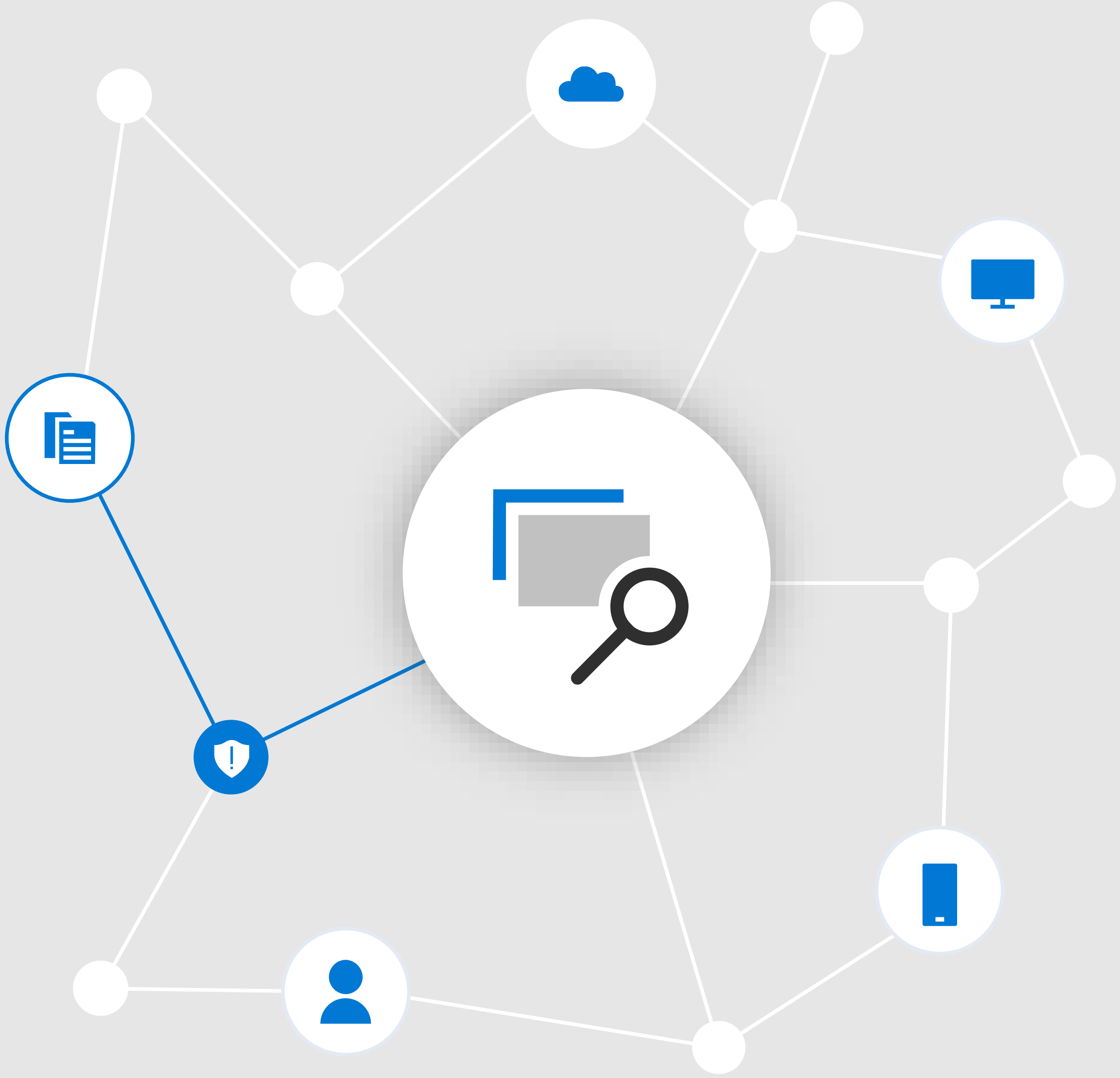
Built-in protection

Proactively remediate vulnerabilities

Identify, assess, and remediate endpoint weaknesses with vulnerability management capabilities

Discover vulnerabilities and misconfigurations in real time with sensors, without the need for agents or periodic scans

Monitor the status and progress of remediation activities across the organization in real time



Comprehensive scalability

- Deploy with zero touch
- Simplify and speed deployments
- Manage digital estate health
- Automate updates

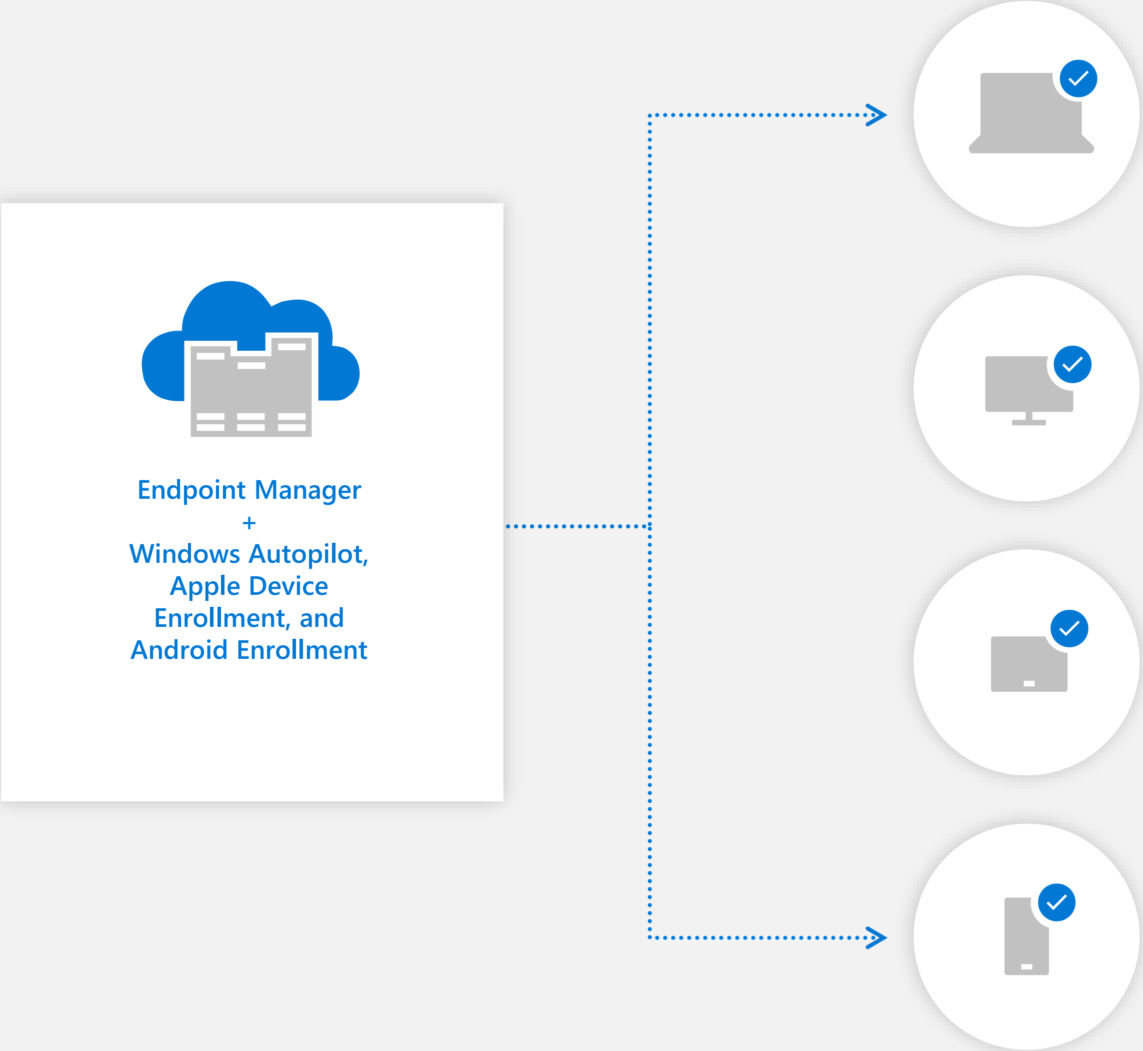
Comprehensive scalability

Deploy with zero touch

Direct device shipments to users' homes without pre-configuration steps

Remote deployment and configuration of devices through a zero-touch process, right out of the box

Support for zero-touch provisioning with Windows Autopilot, Apple Device Enrollment, and Android Enrollment


Endpoint Manager
+
Windows Autopilot, Apple Device Enrollment, and Android Enrollment

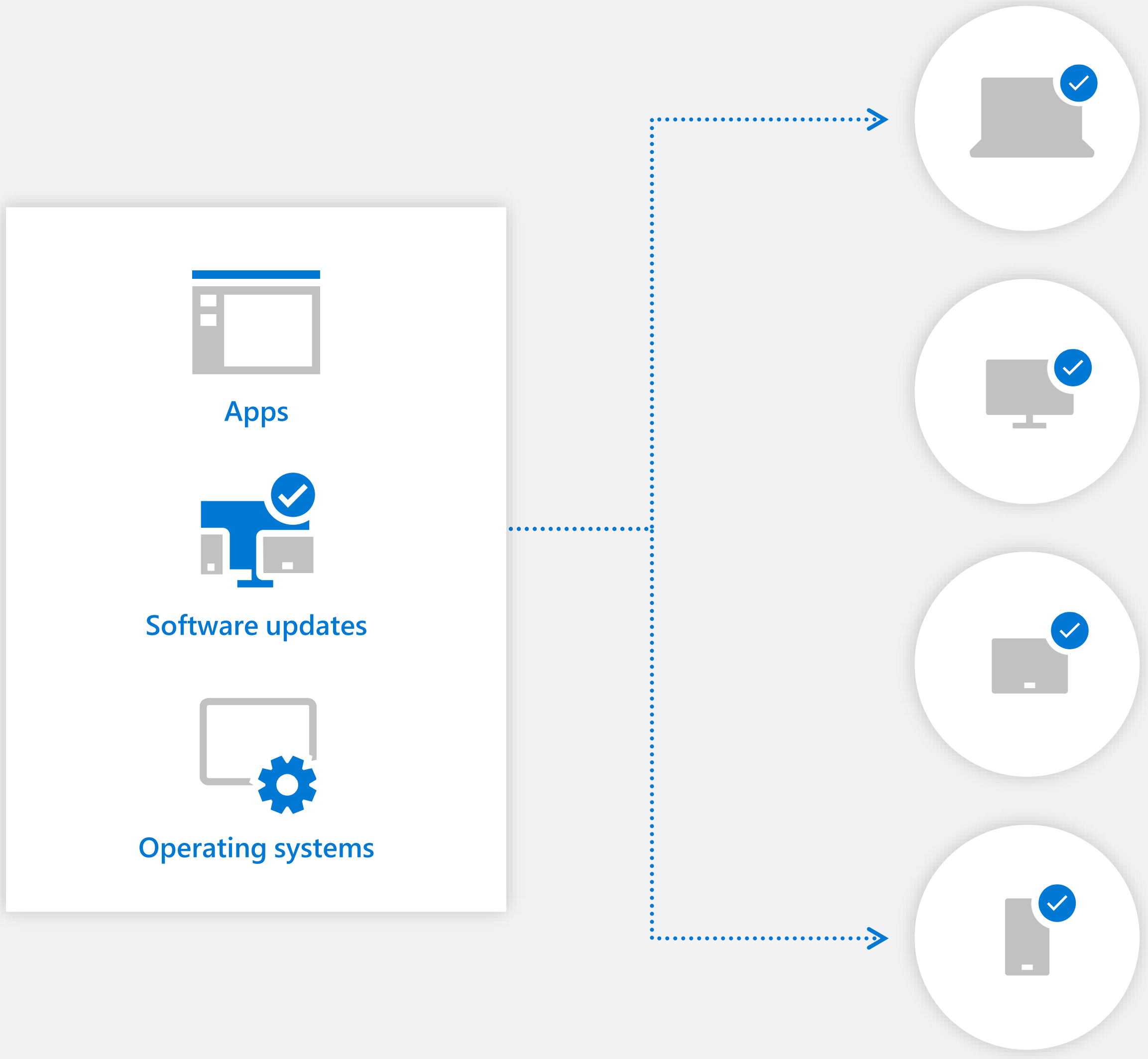
Comprehensive scalability

Simplify and speed deployments

A comprehensive tool for mobile device management (MDM) and mobile application management (MAM) for your apps and devices

Ability to deploy apps, software updates, and operating systems for desktops, servers, and laptops from on-premises or the cloud

Remote deployment and management of Microsoft Office, including updates and settings



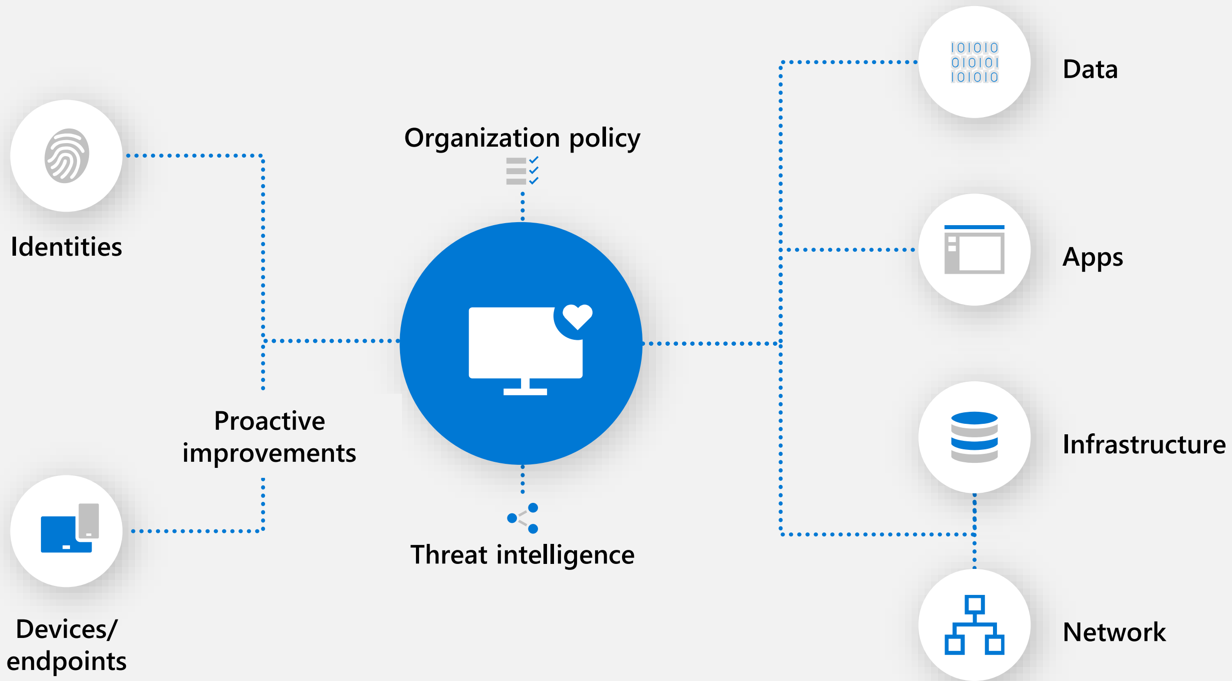
Comprehensive scalability

Manage digital estate health

User experience insights that help improve user productivity and reduce IT support costs

User impact assessment of configuration changes, allowing you to optimize the end-user experience

Ability to proactively make improvements to devices by identifying policies or hardware issues that may be slowing them down



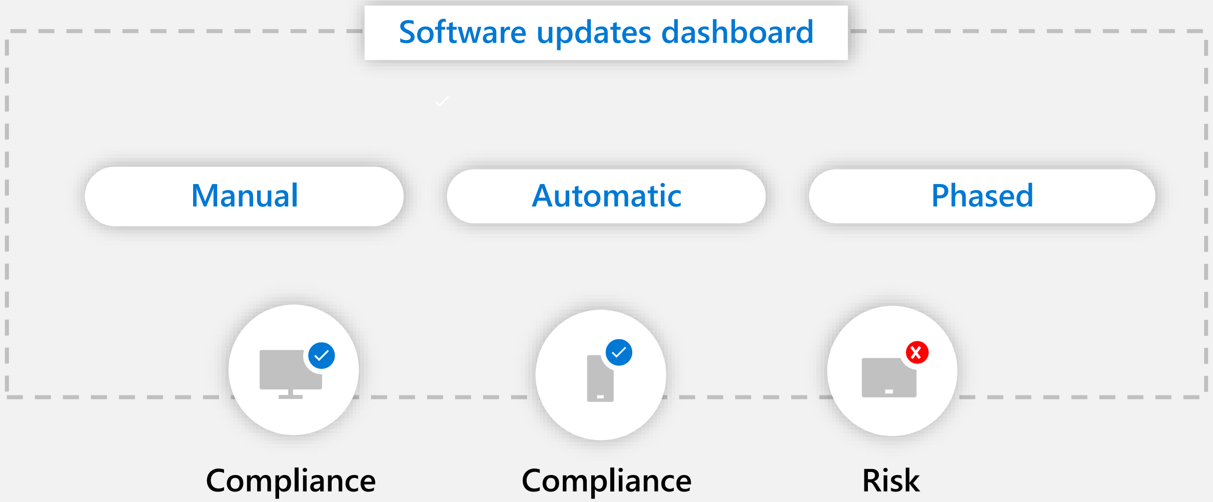
Comprehensive scalability

Automate updates

Set of tools and resources to help manage the complexities of tracking and applying updates to client devices

Ability to easily manage the software update process with manual, automatic, and phased deployment scenarios

Software updates dashboard to view compliance status and quickly analyze data to determine which devices are at risk



Management Powered by Microsoft 365 Cloud

	On-premises	Cloud attached
Traditional OS Deployment	✓	✓
Win32 app management	✓	✓
Configuration and GPO	✓	✓
BitLocker Management	✓	✓
Hardware and software inventory	✓	✓
Update management	✓	✓
Unified Endpoint Management – Windows, iOS, macOS, Android		✓
Modern access control – Compliance, Conditional Access		✓
Modern provisioning – Autopilot, DEP, Zero Touch, KME		✓
Modern security – Hello, Attestation, ATP, Secure Score		✓
Modern policy – Security Baselines, Admin Templates, Guided Deployments		✓
Modern app management – M365 Enterprise apps, Stores, SaaS, VPP		✓
Full M365 integration – Analytics, Graph, Console, RBAC, Audit		✓

The path to Zero Trust with Unified Endpoint Management

alnafitha IT

Enforce Zero Trust security controls with Endpoint Manager

Architecture	What you are trying to achieve	Endpoint Manager features	What you can do in Endpoint Manager
Identities	Protect identities against compromise and secure access to resources	Azure AD	Give users, devices, and apps the right access to the right resources through identity services: • Single sign-on • Conditional Access • Multi-factor authentication
Endpoints	Secure endpoints and allow only compliant and trusted apps and devices to access data	Device management, MDM, Microsoft Defender for Endpoint	Apply security policies for comprehensive endpoint protection: • Antivirus • Disk encryption • Firewall • Endpoint detection and response • Attack surface reduction • Account protection
Applications	Ensure applications are available, visible, and secured	App Protection Policies, App Configuration Policies	Ensure your organization's data remains safe—whether or not it's contained in managed apps—by applying app protection policies that restrict access and give control to your IT department
Data	Protect sensitive data wherever it lives or travels	Disk Encryption Device Policies	Enable built-in encryption for devices running Windows 10 and manage recovery keys Define data loss prevention (DLP) controls to prevent accidental leaks of sensitive corporate data
Infrastructure	Harden defenses and detect and respond to threats in real time	Conditional Access Threat and Vulnerability Management	Define compliance policies for device-based Conditional Access to evaluate the compliance status of the devices Discover vulnerabilities and misconfigurations in real time with built-in Defender for Endpoint sensors
Network	Remove implicit trust from the network and prevent lateral movement	Network Protection Policies Network Access Control, Virtual Private Networks	Protect users from accessing phishing scams, exploit-hosting sites, and malicious content on the internet Check device enrollment and compliance and give users secure remote access to the network

Enforce Zero Trust security controls with Endpoint Manager

Zero Trust controls

Identities

Protect identities against compromise and secure access to resources

Endpoints

Allow only compliant and trusted apps and devices to access data

Enforce with Endpoint Manager

Azure AD

Ensure users, devices, and apps have the right access to the right resources through identity services:

- Single sign-on
- Conditional Access
- Multi-factor authentication

Device management, MDM, and Defender for Endpoint

Apply endpoint security policies for comprehensive endpoint protection:

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection

Enforce Zero Trust security controls with Endpoint Manager

Zero Trust controls

Applications

Ensure applications are available, visible, and secured

Enforce with Endpoint Manager

App protection policies and app configuration policies

Ensure your organization's data remains safe—whether it's contained in managed apps or not—by applying app protection policies that restrict access and give control to your IT department

Data

Protect sensitive data wherever it lives or travels

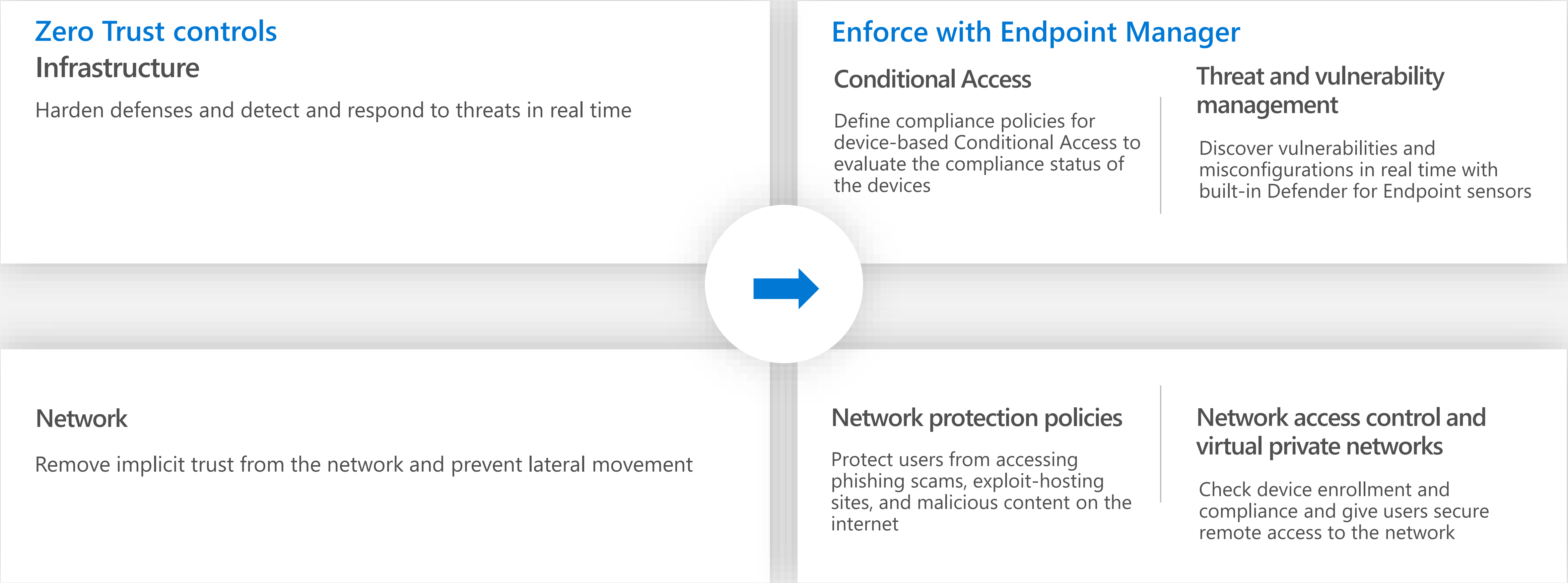
Disk encryption

Enable built-in encryption for devices running Windows 10 and manage recovery keys

Device policies

Define DLP controls to prevent accidental leaks of sensitive corporate data

Enforce Zero Trust security controls with Endpoint Manager



Zero Trust controls

Infrastructure

Harden defenses and detect and respond to threats in real time

Network

Remove implicit trust from the network and prevent lateral movement

Enforce with Endpoint Manager

Conditional Access

Define compliance policies for device-based Conditional Access to evaluate the compliance status of the devices

Threat and vulnerability management

Discover vulnerabilities and misconfigurations in real time with built-in Defender for Endpoint sensors

Network protection policies

Protect users from accessing phishing scams, exploit-hosting sites, and malicious content on the internet

Network access control and virtual private networks

Check device enrollment and compliance and give users secure remote access to the network

Paths to modern management

alnafitha IT

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

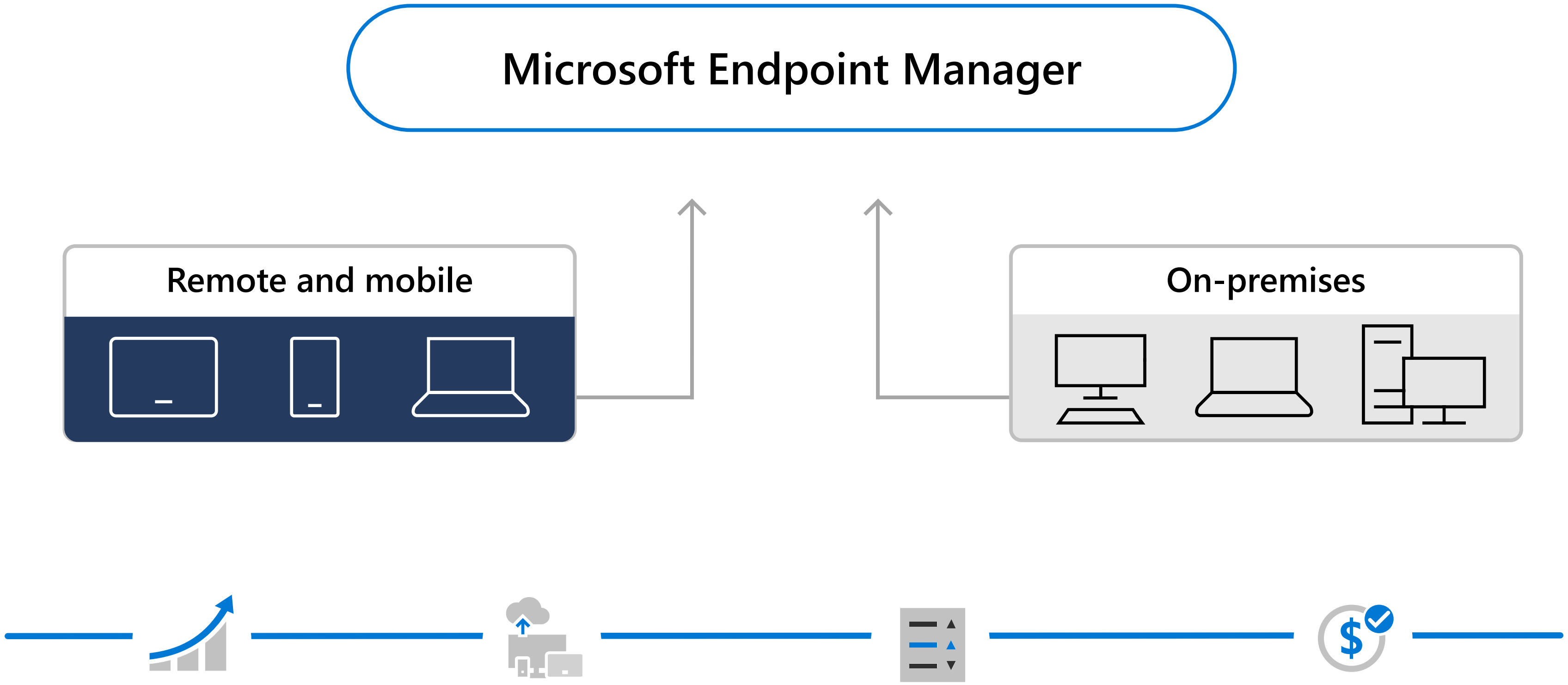
Paths to modern management

Limited or no existing management tools

Existing cloud management

Primarily on-prem management + some cloud

Significant, complex existing on-prem infrastructure



Microsoft Endpoint Manager

Remote and mobile

On-premises

No need to set up and operate your own management infrastructure

Native integration with cloud-powered security controls and risk-based conditional access for apps and data

Flexible support for diverse corporate and BYOD scenarios while increasing productivity and collaboration

Maximize your investment and accelerate time to value with fast rollout of services and devices with end-to-end integration across familiar Microsoft stack

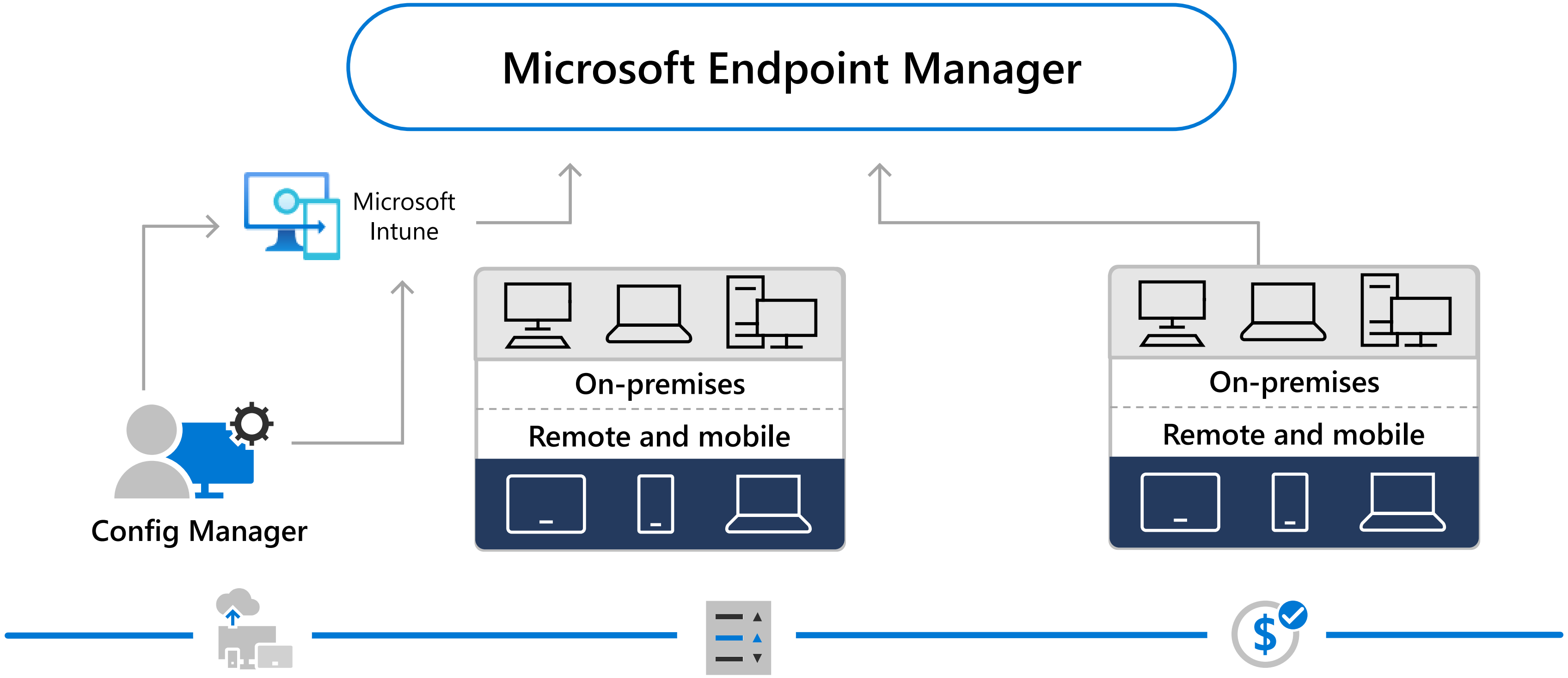
Paths to modern management

Limited or no existing management tools

Existing cloud management

Primarily on-prem management + some cloud

Significant, complex existing on-prem infrastructure



Native integration with cloud-powered security controls and risk-based conditional access for apps and data

Flexible support for diverse corporate and BYOD scenarios while increasing productivity and collaboration

Maximize your investment and accelerate time to value with fast rollout of services and devices with end-to-end integration across familiar Microsoft stack

Paths to modern management

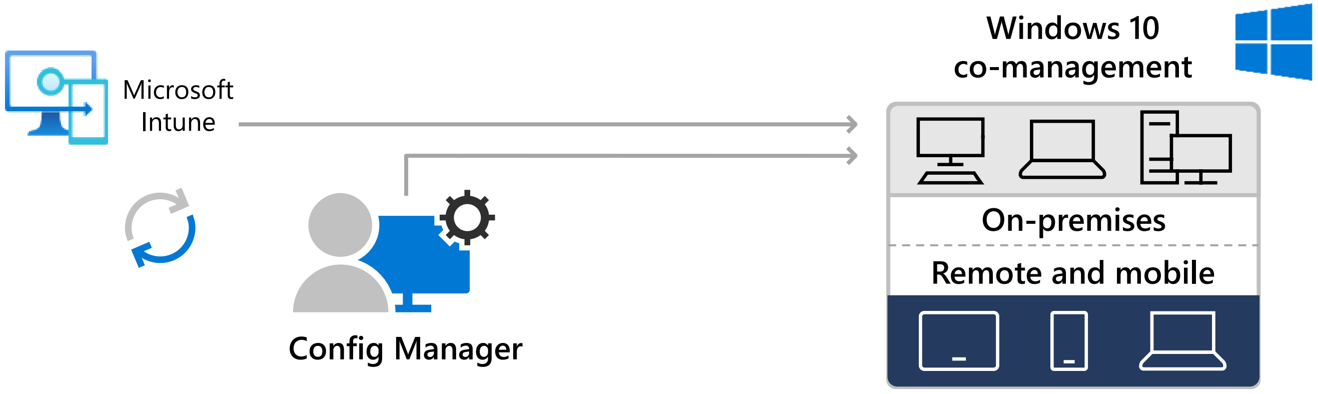
Limited or no existing management tools

Existing cloud management

Primarily on-prem management + some cloud

Significant, complex existing on-prem infrastructure

Microsoft Endpoint Manager



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

Conditional access

Modern provisioning (Autopilot)

Remote management for Config Mgr.

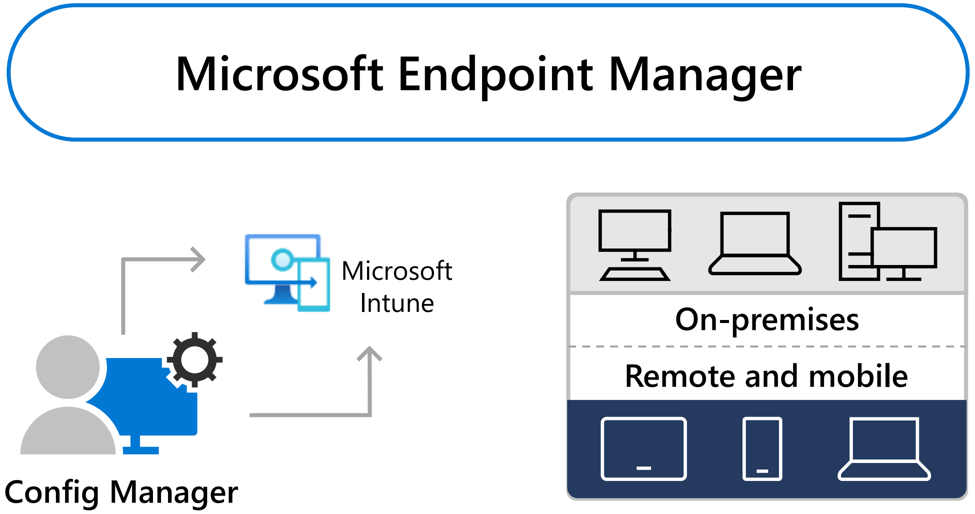
Paths to modern management

Limited or no existing management tools

Existing cloud management

Primarily on-prem management + some cloud

Significant, complex existing on-prem infrastructure



Microsoft Endpoint Manager

Config Manager

Microsoft Intune

On-premises

Remote and mobile

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

Microsoft Endpoint Manager powered by Microsoft 365

Suite	Microsoft solution	Feature/capability description	O365 E3	O365 E5	M365 E3	M365 E5
Office 365	Microsoft 365 apps for enterprise	View, create, and edit documents in Office client, web, and mobile apps	X	X	X	X
	Collaboration and messaging	Teams, OneDrive, and Exchange Online	X	X	X	X
	Portals, video streaming, and social	SharePoint, Stream, forms, and Yammer	X	X	X	X
	Team and task organization	Planner, forms, to do, and delve	X	X	X	X
	Process automation	Power Apps, Power Automate, and forms	X	X	X	X
	Core security and compliance	Exchange Online Protection, e-Discovery, Data loss prevention	X	X	X	X
	Advanced security and compliance	Anti-phishing, Safe Links, Threat Intelligence, Automated Data Classification		X		X
	Advanced e-discovery	Preserve, collect, review, analyze, and export content end-to-end		X		X
	Advanced data analytics	Power BI Pro		X		X
	Advanced communications	Enterprise Voice/Phone System and PSTN Audio Conferencing		X		X
Enterprise Mobility & Security (EMS)	Core identity and device mgmt	AAD Plan 1 (SSO, MFA, CA, SSPR) and Intune			X	X
	Information protection	Data classification, file encryption, document tracking/revocation			X	X
	Threat analytics	Identify suspicious activities and advanced attacks via user behavior analytics			X	X
	Windows Server and System Center	On-prem Windows Server, Config Manager, and Endpoint Protection			X	X
	Microsoft Cloud App Security	Insights into user behavior w/in cloud apps being used on the network				X
	Advanced Identity and Info Protection	AAD Plan 2 (PIM and risk-based CA) and automated data classification				X
	Microsoft Defender for Identity	Detect advanced attacks and investigate suspicious behaviors on-prem/cloud				X
Windows	Windows 10 Enterprise/E3	Windows Defender Security, Managed UX, and Desktop Analytics			X	X
	Azure Virtual Desktop	Desktop and App Virtualization Service Hosted in Azure			X	X
	Microsoft Defender for Endpoint	Behavior-based, attack detection, forensic investigation, threat mitigation				X

Device lifecycle

alnafitha IT

Manage the entire device lifecycle with Microsoft Endpoint Manager

Enroll

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

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

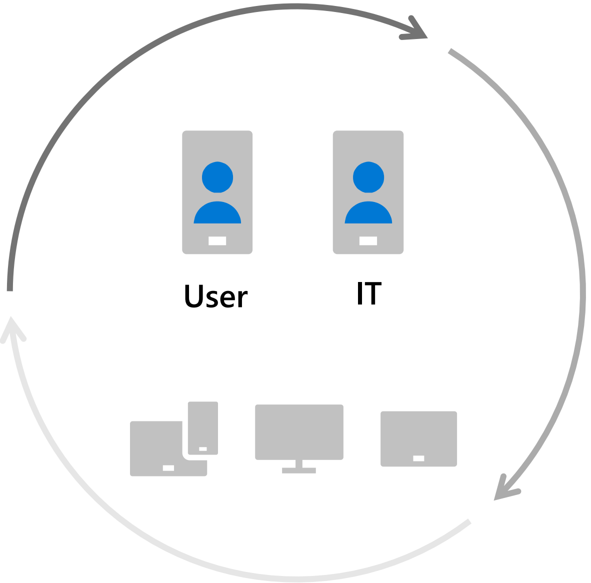
Deploy certificates, email, VPN, and Wi-Fi profiles

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)

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

Report on device and app compliance

Microsoft 365 business value

Cloud management

alnafitha IT

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

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

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

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

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**		

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

Microsoft

Thank you.

alnafitha IT