

Microsoft Endpoint Manager 3-Week Workshop

by Exelegant & Microsoft



This provider has demonstrated competency in the following areas

Gold	Communications
Gold	DevOps
Gold	Data Analytics
Gold	Data Platform
Gold	Cloud Productivity
Gold	Security
Gold	Cloud Platform
Gold	Windows and Devices
Gold	Collaboration and Content
Gold	Messaging
Silver	Small and Midmarket Cloud Solutions
Silver	Enterprise Mobility Management
Silver	Application Development
Silver	Project and Portfolio Management
Silver	Datacenter

10 -Time Gold Microsoft Partner



[Visit Website](#)

About us

Exelegant is a cyber security and professional services company where efficiency is standard, and our customers are our partners. Headquartered in Freehold, NJ with supporting offices in Newark, NJ and L'viv Ukraine, Exelegant leverages years of experience to bring about a world-class experience for our clients.

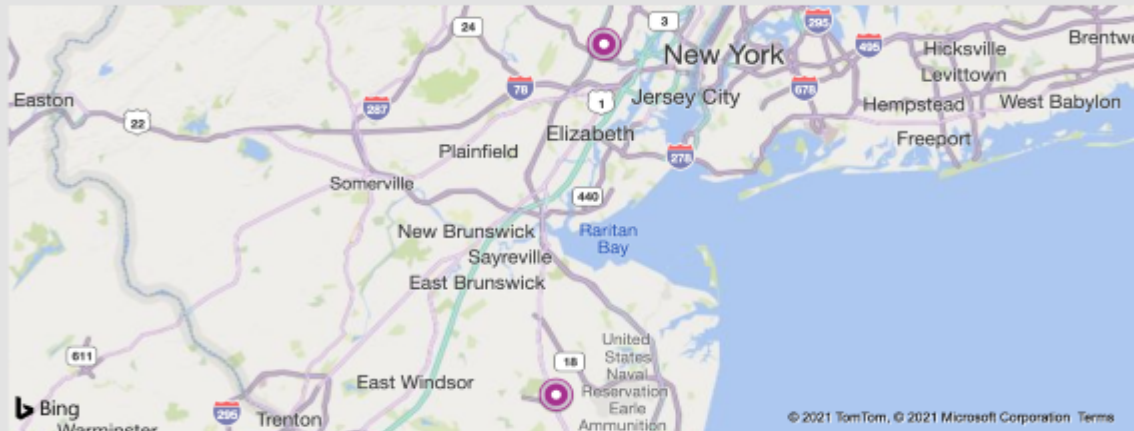
Our specialties include:

[More](#)

Skills and Capabilities

- Advanced Analytics
- Agriculture, Forestry, & Fishing
- Application Integration
- Artificial Intelligence
- Azure
- Azure Security & Operation Management

Top locations



36 W Main Street, Suite 300, Freehold, NJ, US 07728

495 N 13th street, Newark, NJ, US 07107

Clients

What our clients say:

- "Exelegant helped our company migrate from G-Suite to Microsoft Office 365 with zero downtime and zero data loss. During the process, over 3,500 users continued to collaborate and run critical business functions seamlessly."

Robert Florescu, CISO, CityMD

- "Switching to Exelegant has been a major contributing factor to the growth of our group. As a company looking to expand, we really value our employees' time and productivity. Exelegant's IT Support has enabled our business to run as efficiently as possible."

Bruce Lucarelli, CTO, DermOne

- "Exelegant has been with our hospital since we've opened our doors. Their experience in a wide range of projects and solutions, and management of vendors has made a tremendous impact on our efficiency"

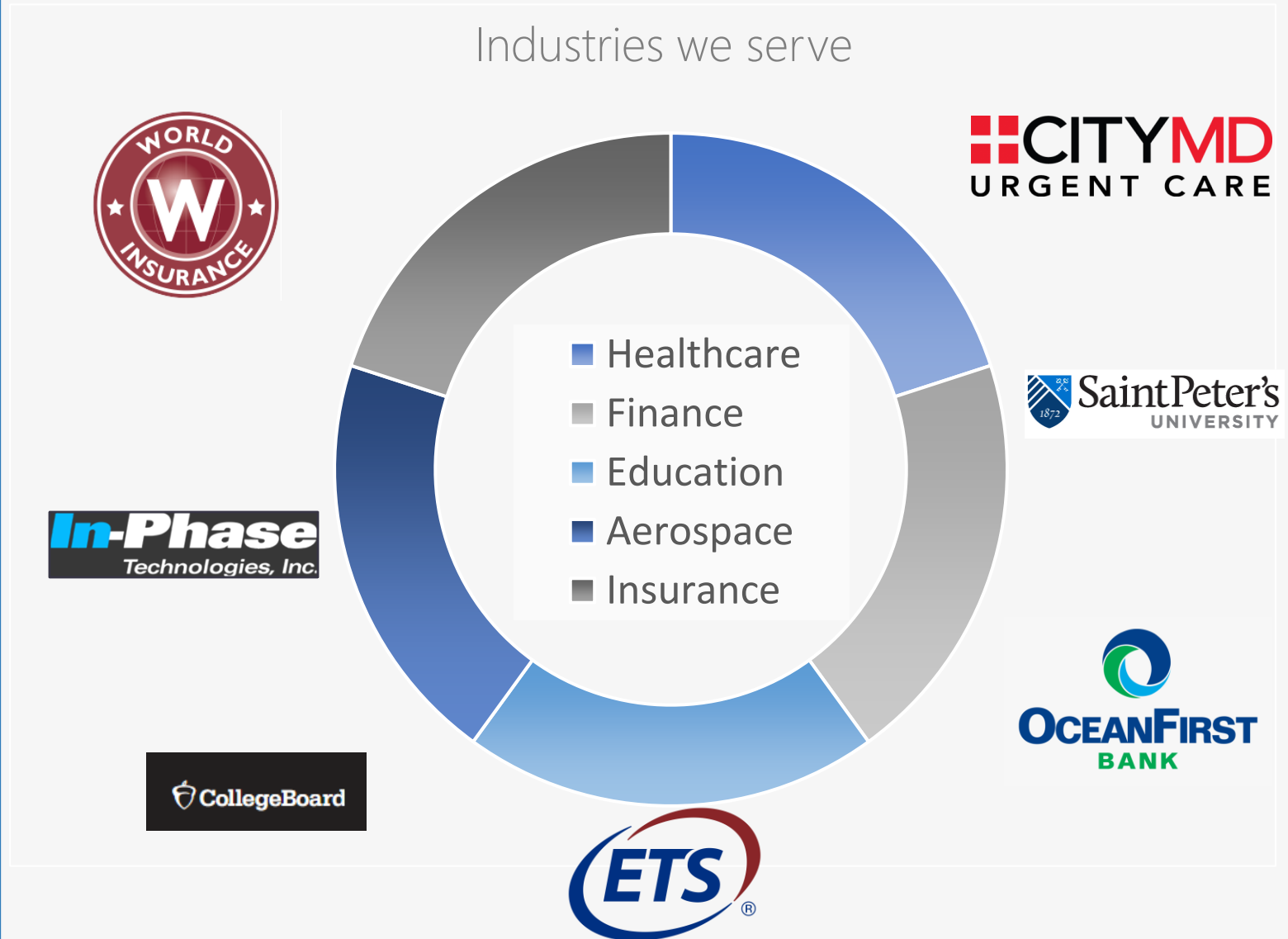
Alexey Gololobov, CFO, Columbus Hospital LTACH

- "Exelegant has become our trusted business partner and completed migration on time, alleviated hosting responsibilities, and gave us capabilities to enable team productivity and data security."

Kevin Hannigan, President, ACC Inc.



Industries we serve



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



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



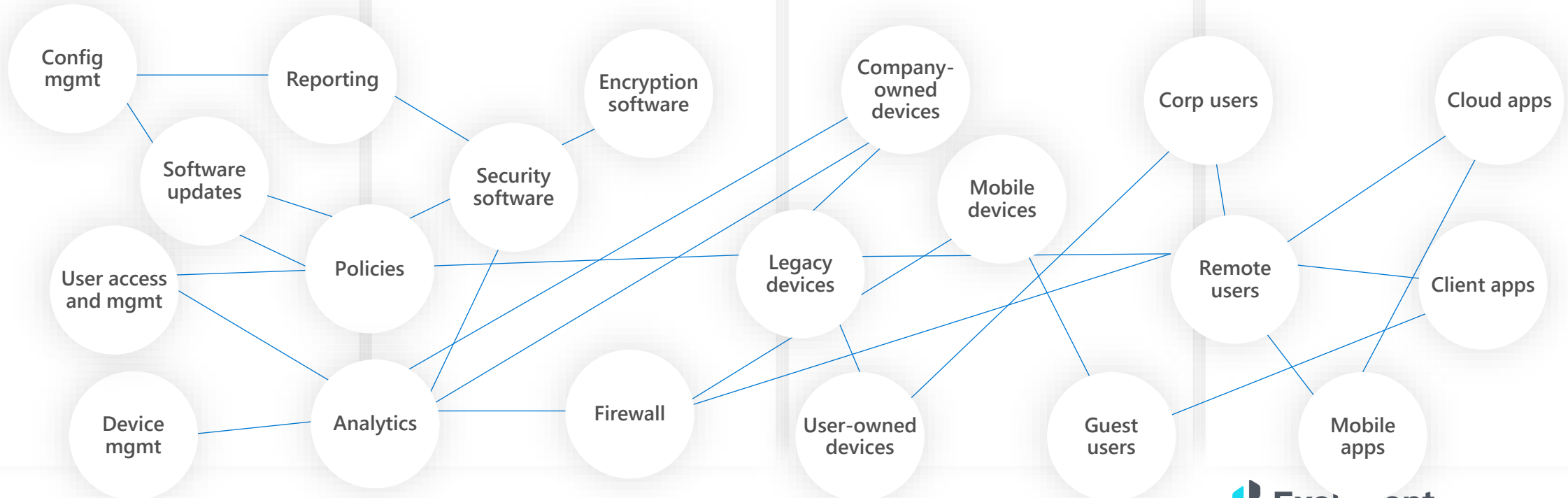
Employee satisfaction

Easy, fast access to company resources



Cybersecurity

Mitigating risk and vulnerabilities



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) →



Unified management

Extend the benefits of cloud management

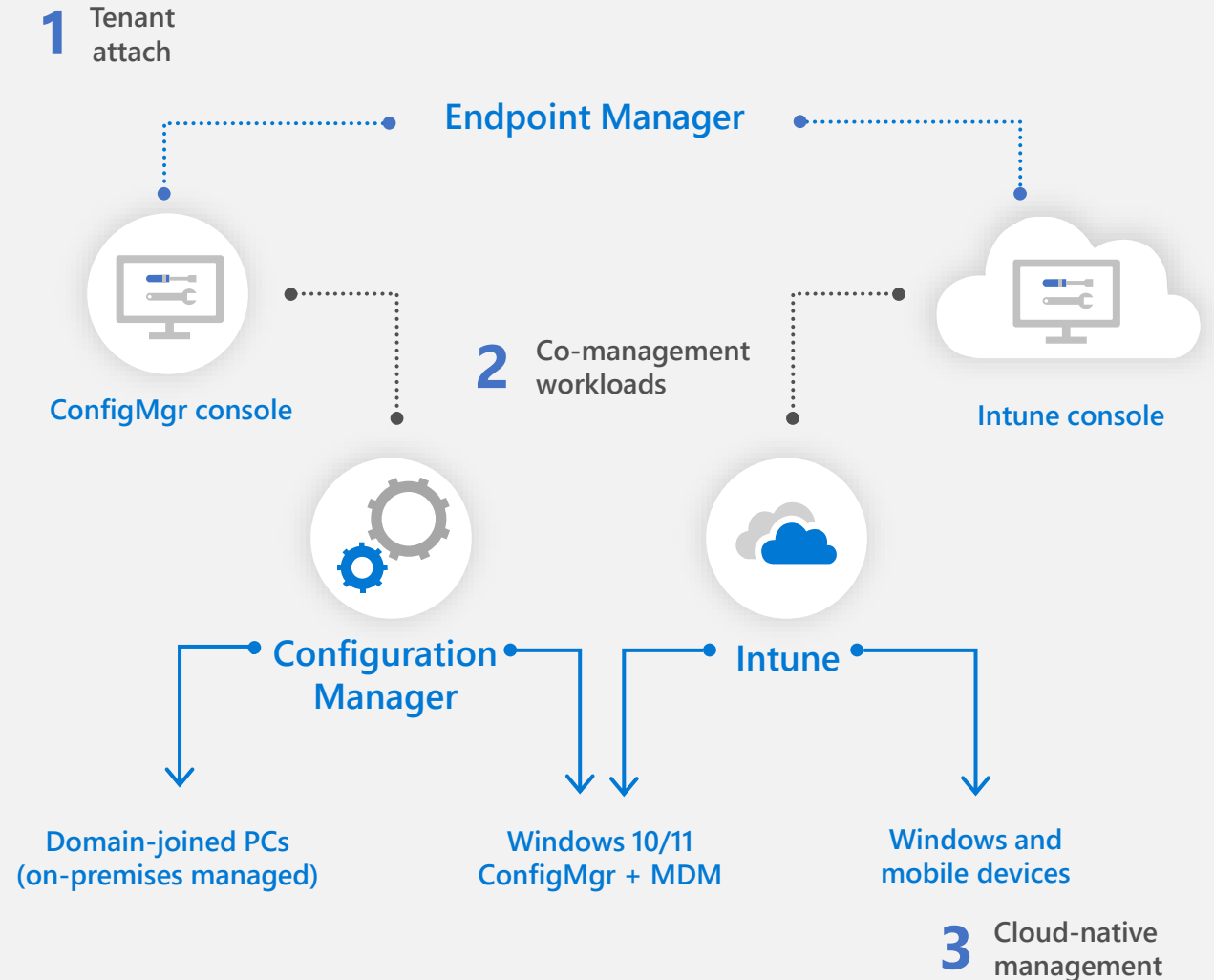
Ability to attach on-premises devices to the cloud with tenant attach

A centralized console to co-manage apps and devices with Windows 10 or Windows 11

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





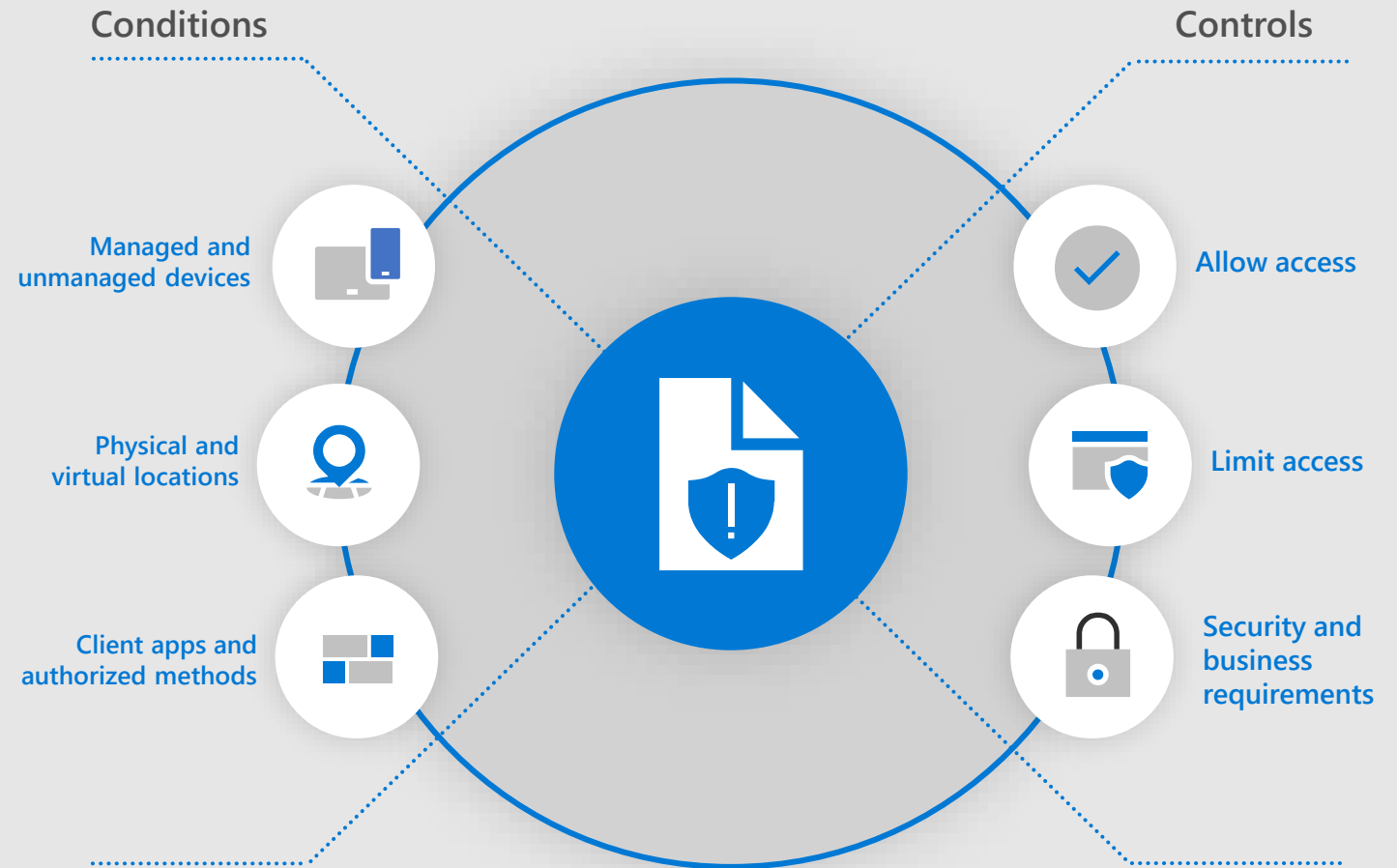
Built-in protection

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



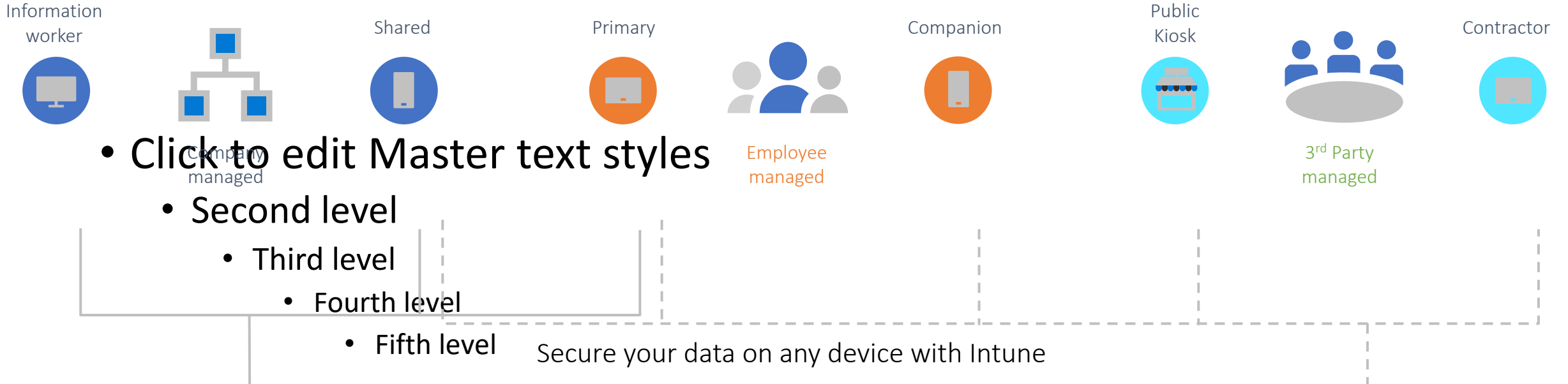
Management Powered by Microsoft 365 Cloud

	 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, iPadOS, 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		✓

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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

In a complex device landscape, you need choices



Intune device management



Enroll devices for management



Provision settings, certs, profiles



Report and measure device compliance



Remove corporate data from devices

Conditional access: Restrict access to managed and compliant devices



Intune app management



Publish mobile apps to users



Configure and update apps



Report app inventory and usage



Secure and remove corporate data within mobile apps

Conditional access: Restrict access to apps with app protection policy

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

Support and retire

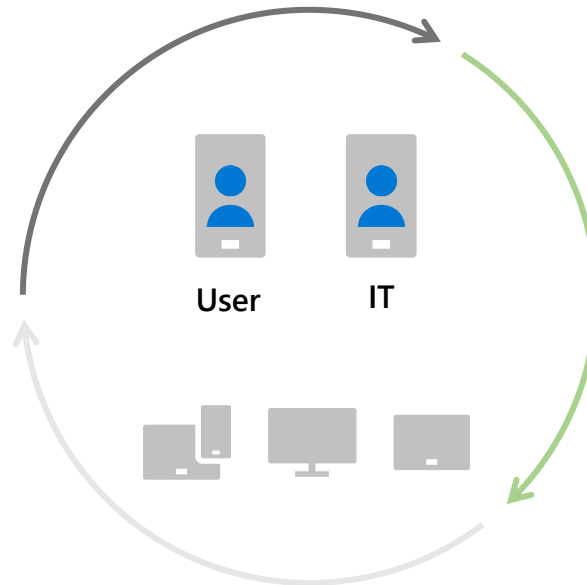
Revoke access to corporate resources

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)

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

Report on device and app compliance



Assess

- Pre-Engagement Call
- Customer Questionnaire
- Microsoft Endpoint Manager Overview
- Manage Your Endpoints



Art of the Possible

- Azure AD
- Microsoft Devices
- Microsoft 365 Apps and Edge
- Analytics and Reporting
- MDM Migration
- Intune for Education
- Modernize Windows



Build the Plan

- Results and Next Steps
- Reports and Recommendations



Optional modules
(at least two modules required)



Azure AD

- Azure AD Overview
- Secure, Seamless Access to all Your Apps with Azure AD



Microsoft Devices

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



Microsoft 365 Apps and Edge

- Microsoft 365 Apps for Enterprise
- Microsoft Edge



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



Modernize Windows

- Windows 11 Enterprise Overview
- Upgrading and deploying Windows 11 Enterprise



Art of the Possible



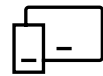
Azure AD

Azure AD Overview presentation

Present a high-level overview of Azure Active Directory and how it helps organizations to secure access to a connected world. The presentation also includes information on identity fundamentals and Azure AD integration scenarios.

Secure, seamless access to all your apps with Azure Active Directory presentation

Present how Azure AD helps to secure and manage your on-premise and cloud applications.



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 Endpoint Manager.





Art of the Possible



Microsoft 365 apps and Edge

Microsoft 365 apps for Enterprise presentation

Present an overview of the Microsoft 365 apps for Enterprise and how to deploy and service the applications.

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 Endpoint Manager.



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 Endpoint Manager reporting features including Intune reports, the Intune Data Warehouse, exporting reports with Microsoft Graph, and creating custom reports with Log Analytics.



Art of the Possible



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 Endpoint Manager.





Art of the Possible



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.



Modernize Windows

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.