TECHIMPACT®

Microsoft Intune Overview

FRANCIS JOHNSON

Chief Technology Officer

I manage all aspects of technology services including our Managed IT Support and Cybersecurity services, and technical projects. Our team works with nonprofits across the country to implement on-premises and cloud infrastructure, improve security and provide mobile working opportunities.

francis@techimpact.org

TECHIMPACT®

CYBERSECURITY AWARENESS MONTH

DATA BREACH STATISTICS

Data breach costs averaged $4.88 million

Data breach costs for the healthcare industry averaged $9.77 million, by far the costliest industry

35% of breaches involved shadow data

42% of breaches were detected by internal teams and tools

Initial Attack Vectors:

- Stolen or compromised credentials (16%)
- Phishing (15%)
- Cloud misconfiguration (12%)

Source: IBM and Ponemon Institute 2024 Cost of Data Breach Study

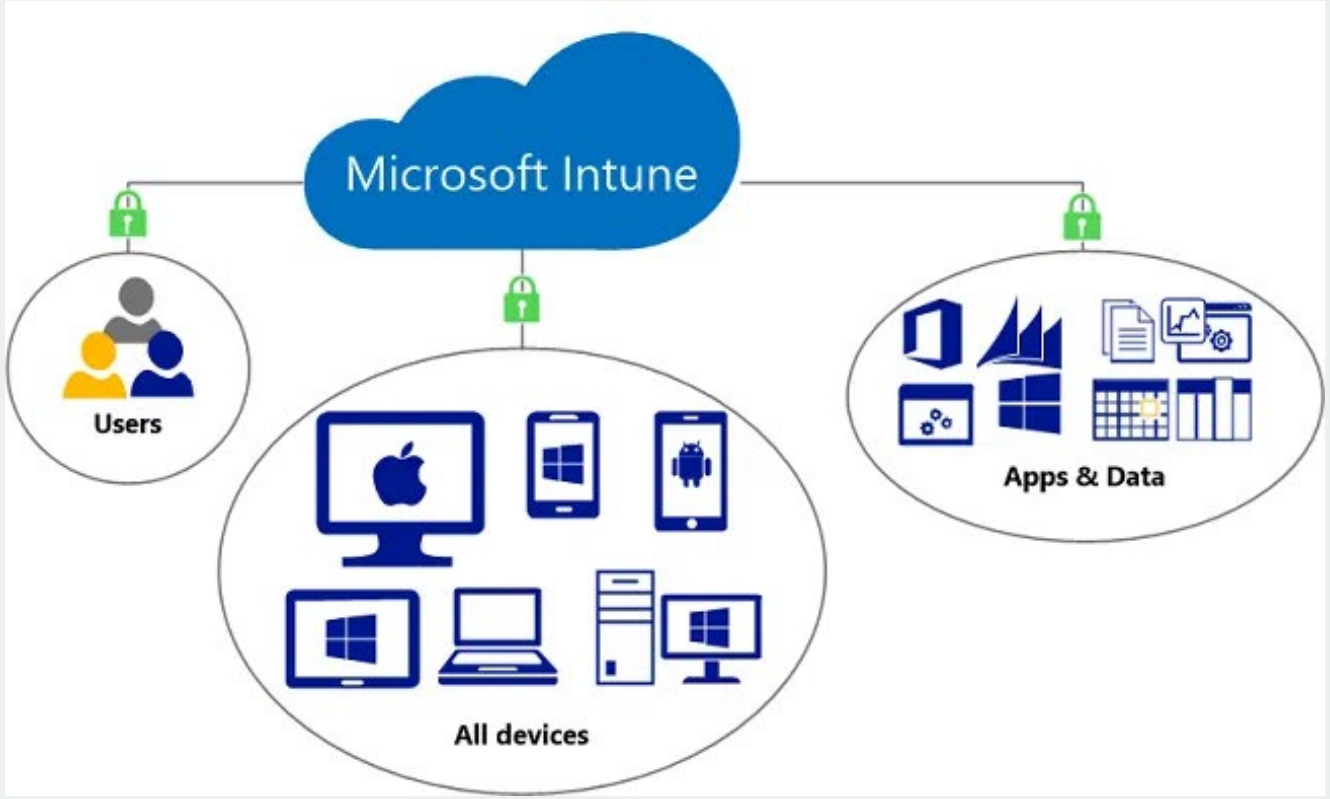
COST OF A DATA BREACH: ACTUAL COSTS

- System recovery
- Data restoration
- Legal guidance
- Crisis management
- Regulatory fines
- Breach notification
- Forensics
- Credit monitoring

Source: IBM and Ponemon Institute 2024 Cost of Data Breach Study

MICROSFT INTUNE DEFINED

MICROSOFT INTUNE EXPLAINED



Intune is Microsoft's cloud-based Endpoint Management platform designed to mitigate the security risks of endpoints (organizational and BYOD devices) in an environment.

Image Credit: Microsoft

WHAT CAN WE DO IN MICROSOFT INTUNE

Protect data on the devices

Restrict and control the applications

Control and manage access to organization data

Use Autopilot to **automate** the setup of new Windows computers

Manage software installations and updates

Wipe and delete sensitive data from a device if it becomes lost or stolen

Enforce software update policies for your organization’s devices

MICROSOFT INTUNE FEATURES

Mobile Device Management

- Enroll ***organization-owned devices***
- Enforce policies on ***organization-owned devices***
- Push applications on ***organization-owned devices***
- Control access to data on ***organization-owned devices***
- Wipe organization data (remotely) off ***organization-owned devices***

Mobile Applications Management

- Allow ***personal devices*** to securely access org data and apps
- Force authentication and re-authentication on ***personal devices***
- Wipe organization app data (remotely) off ***personal devices***

Mobile Device Management

TECHIMPACT®

Mobile Device Management

Mobile Device Management

- Enroll ***organization-owned devices***
- Enforce policies on ***organization-owned devices***
- Push applications on ***organization-owned devices***
- Control access to data on ***organization-owned devices***
- Wipe organization data (remotely) off ***organization-owned devices***

MDM

Mobile Device Management

Complete Control of Device

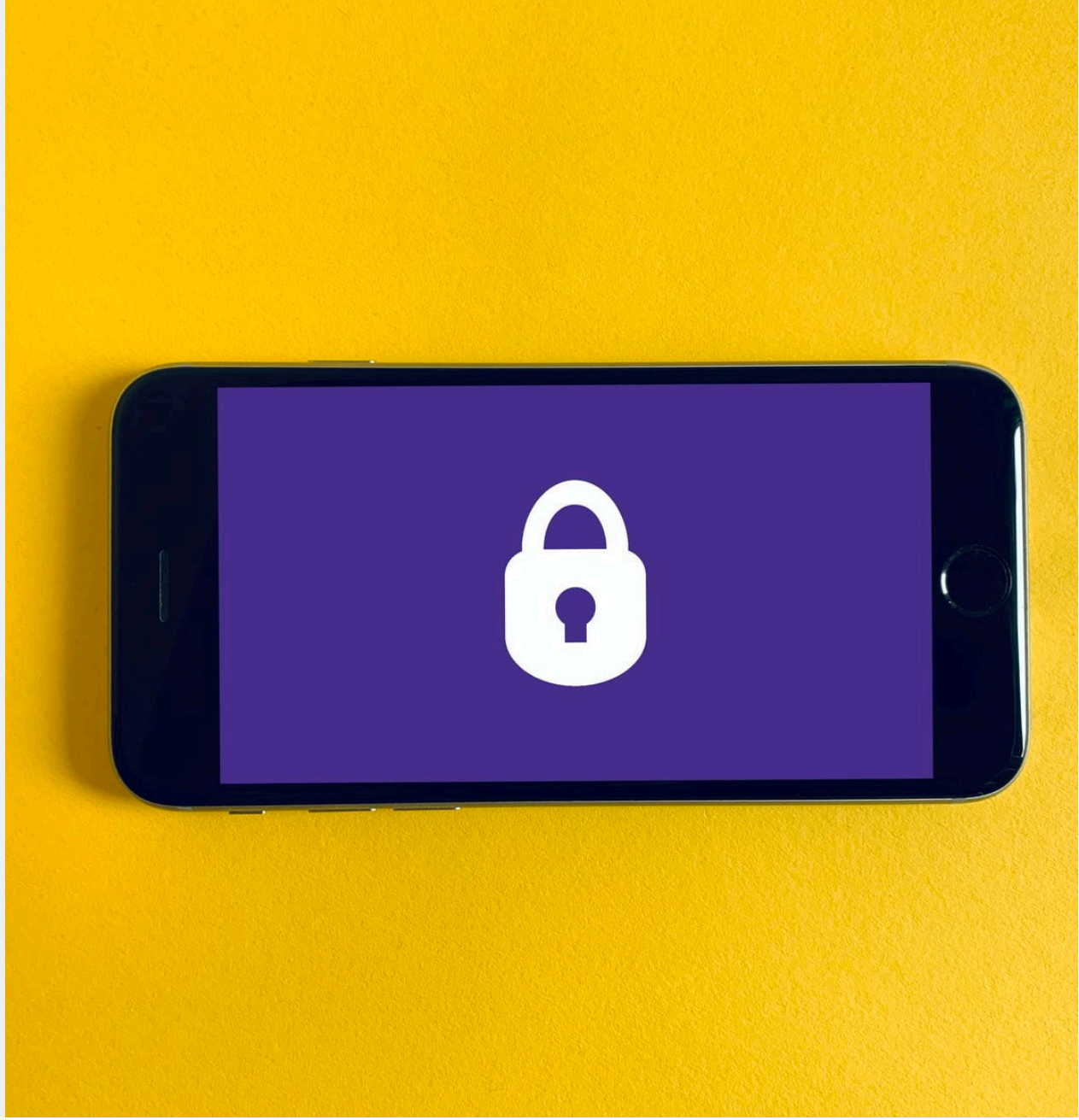
- Best suited for organization-owned devices
- Security parameters:
  - Require Minimum OS and Version
  - Require Multi-Factor Authentication
  - Remote Wipe & Password Reset
  - Require Disk Encryption
  - Require AV and AM

MDM: MOBILE DEVICE MANAGEMENT

When devices are enrolled with Intune, you can create policies that configure the entire device itself.

Best suited for organization-owned devices

- Install and remove software
- Remote Wipe & Factory Reset
- Apply software update policies
- Block user access to various features and settings of the device



DEVICE ENROLLMENT

Enrollment is the process of connecting devices to Intune

Intune needs to know what devices are to be managed – this process is through Enrollment

Each device must be enrolled individually either by the end-user or an administrator

POLICIES

Compliance Policies

Intune compliance policies are sets of rules and conditions used to evaluate the configuration of managed devices. These policies help secure organizational data and resources from devices that don't meet the configuration requirements. Managed devices must satisfy the conditions set in the policies to be considered compliant by Intune

Configuration Policies

Intune configuration policies are used to set configurations for Windows devices. These policies are designed to enhance the security of devices and align them with recommended security baselines. Some of the configurations included are BitLocker Disk Encryption, local admin control, Windows operating system software updates, and automatic stale/offline device cleanup

CONDITIONAL ACCESS POLICIES

Conditional Access Policies

Conditional Access policies are important for keeping your organization's data secure. They enforce restrictions on who can access your organization's data and how they can access and interact with it. Consider the three levels of protection: what devices can access data, what applications can access data, and what users can do with the data.

WINDOWS AUTOPILOT

WHAT IS AUTOPILOT?

Windows Autopilot is designed to simplify the lifecycle of Windows devices for initial deployment through the eventual end of life. It includes four types of Autopilot modes: Self-Deploying Mode, White Glove, Autopilot for Existing devices, and User Driven Mode.

Windows Autopilot can be used to deploy Windows PCs or HoloLens 2 devices. It can also be used to reset, repurpose, and recover devices. This solution enables an IT team (or individual) to achieve these goals with little to no infrastructure to manage, with a straightforward process.

WINDOWS AUTOPILOT BENEFITS

- Reduces the IT team's overall cost and time for deploying, managing, and retiring devices.
- Standardizes OS image profiles on org devices.
- Streamlines enrollment of devices in Intune.
- Allows for self-deployment of devices – extremely beneficial for orgs with remote workers.
- Provides greater security and compliance.

AUTOPILOT REQUIREMENTS

Software Requirements:

Windows 10 or 11

Licensing Requirements:

Microsoft 365 Business Premium subscription

Microsoft 365 F1 or F3 subscription

Microsoft 365 Academic A1, A3, or A5 subscription

Microsoft 365 Enterprise E3 or E5 subscription

Enterprise Mobility + Security E3 or E5 subscription

Configuration Requirements:

Microsoft Entra automatic enrollment

Allow users to join devices to Microsoft Entra ID

Mobile Application Management

TECHIMPACT®

Mobile Application Management

- Allow ***personal devices*** to securely access org data and apps
- Force authentication and re-authentication on ***personal devices***
- Wipe organization app data (remotely) off ***personal devices***

MAM

Mobile Application Management

Control Of Applications Only

- Best suited for Bring Your Own Device policies
- Can apply security settings to applications:
  - Restrict actions
  - Set authentication policies
  - Selective wiping of organizational data

MAM: MOBILE APPLICATION MANAGEMENT

MAM policies enforce access controls and data protection for the apps that your staff use to access Microsoft 365.

Examples:

- Restrict Copy/Paste to personal apps
- Require a PIN to access the apps (Outlook, SharePoint, OneDrive, etc.)
- Prevent data from backing up to iCloud and Google services.
- Block printing from the M365 apps

- Devices do not need to be enrolled with Intune to apply these policies. Perfect for protecting your organization's data on personally-owned devices!

TECHIMPACT®

POLICIES

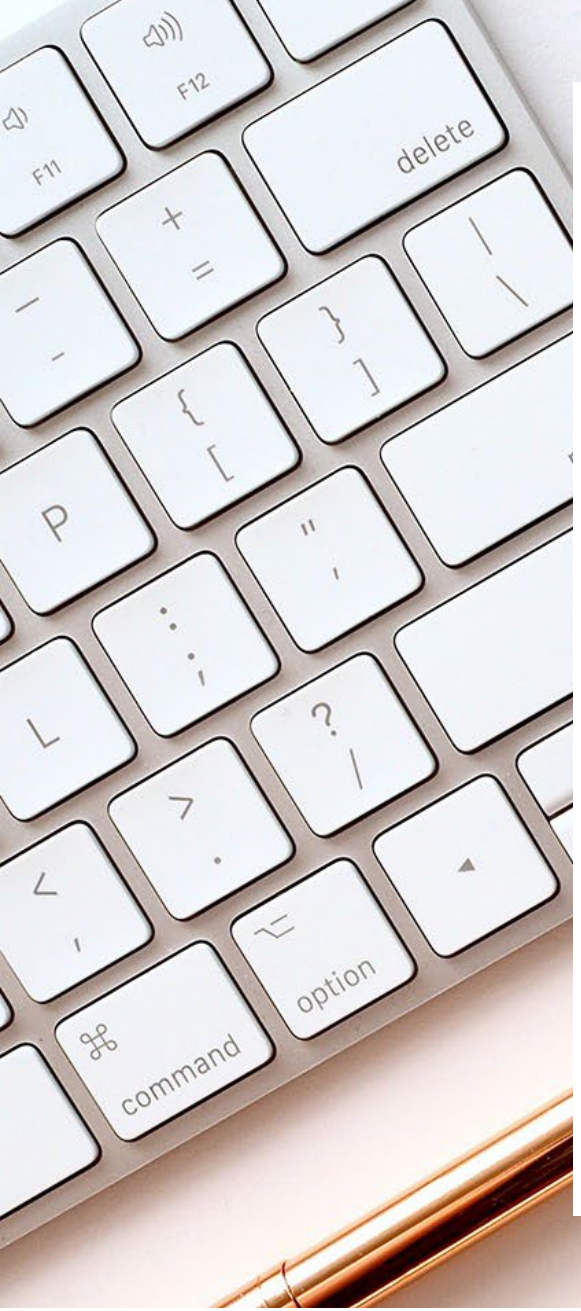
Application Protection Policies

Intune app protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. These policies allow you to control how data is accessed and shared by apps on mobile devices

Applications Configuration Policies

Intune app configuration policies are used to assign configuration settings to apps, ensuring that these settings are automatically applied when the app is installed on end-users' devices. This helps eliminate app setup problems and provides consistency across an enterprise.

REQUIREMENTS



LICENCES RECOMMENDATION FOR MICROSOFT INTUNE

You will need enough licenses of one of these subscriptions to assign to each user account

Recommended Licenses:

Microsoft 365 E3

Microsoft 365 E5

Microsoft 365 Business Premium

Enterprise Mobility + Security E3

Enterprise Mobility + Security E5

Standalone Licenses:

Microsoft Intune Plan 1

Microsoft Intune Plan 2

Microsoft Intune Suite

SUPPORTED PLATFORMS

- ❑ Apple iOS/iPadOS
- ❑ Apple MacOS
- ❑ Windows 10
- ❑ Windows 11
- ❑ Linux
- ❑ Chrome OS

ADDITONAL FEATURES

Microsoft Intune Suite

Microsoft Intune Plan 1

$8.00

A cloud-based unified endpoint management solution included with subscriptions to Microsoft 365 E3, E5, F1, and F3, Enterprise Mobility + Security E3 and E5, and Business Premium plans, including versions of these suites that do not include Microsoft Teams.

Microsoft Intune Plan 2

$4.00

An add-on to Microsoft Intune Plan 1 that offers advanced endpoint management capabilities. Microsoft Intune Plan 2 is included in Microsoft Intune Suite.

Microsoft Intune Suite

$10.00

An add-on to Microsoft Intune Plan 1 that unifies mission-critical advanced endpoint management and security solutions.[1]

Microsoft Intune Suite

The Microsoft Intune Suite includes:

- Endpoint Privilege Management*
- Enterprise App Management*
- Advanced Analytics*
- Remote Help*
- Microsoft Tunnel for Mobile Applications
- Microsoft Cloud PKI*
- Firmware-over-the-air update
- Specialized devices management

*** Can be added to Microsoft Intune Plan 1**

NEXT STEPS

How to be Prepared for an Intune Project

1. Licenses must be purchased and assigned to all users.
2. Org devices will be required to be joined to Microsoft Entra ID.
3. Data Protection on Personal Mobile Devices.
    - Staff must manually install the Intune Company Portal App on Android and the Microsoft Authenticator App on iPhone/iPad.
4. Collect and provide the serial numbers for all org owned iPhone and iPad devices.

Important Notes:

Devices cannot be enrolled in another MDM: Devices must be unenrolled from the previous MDM before they can be enrolled with Intune.

Personal devices will not be enrolled with Intune. Only application protection policies will be enforced (MAM).

If you already have Intune deployed Consider Microsoft Intune Suite

The Microsoft Intune Suite includes:

- Endpoint Privilege Management*
- Enterprise App Management*
- Advanced Analytics*
- Remote Help*
- Microsoft Tunnel for Mobile Applications
- Microsoft Cloud PKI*
- Firmware-over-the-air update
- Specialized devices management

*** Can be added to Microsoft Intune Plan 1**

THANK YOU

Francis Johnson: francis@techimpact.org