
NT KONF
25. – 27.
SEPTEMBER
2023
PORTOROŽ
NT KONF
NT KONFERENCA

NT KONF

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ

Desetak razloga zašto koristiti Intune za upravljanje uređajima

Tomislav Lulić

World Bank Croatia

Tomislav Lulić

World Bank office in Croatia
IT analyst
Microsoft MVP, MCT

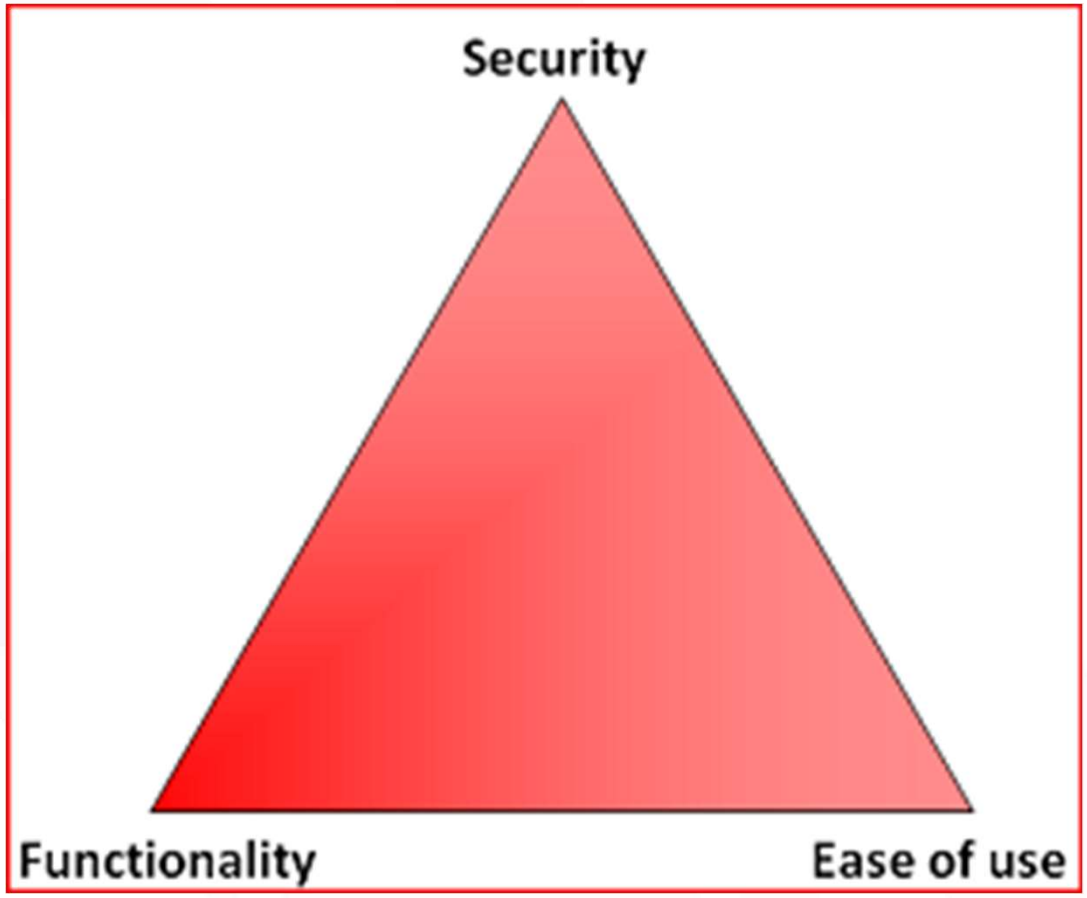
Microsoft® Most Valuable Professional

IT Pro User Group Croatia
MS Community HR

@tlulic
tlulic.wordpress.com
tomislav@tlulic.com
www.linkedin.com/tomislavlulic

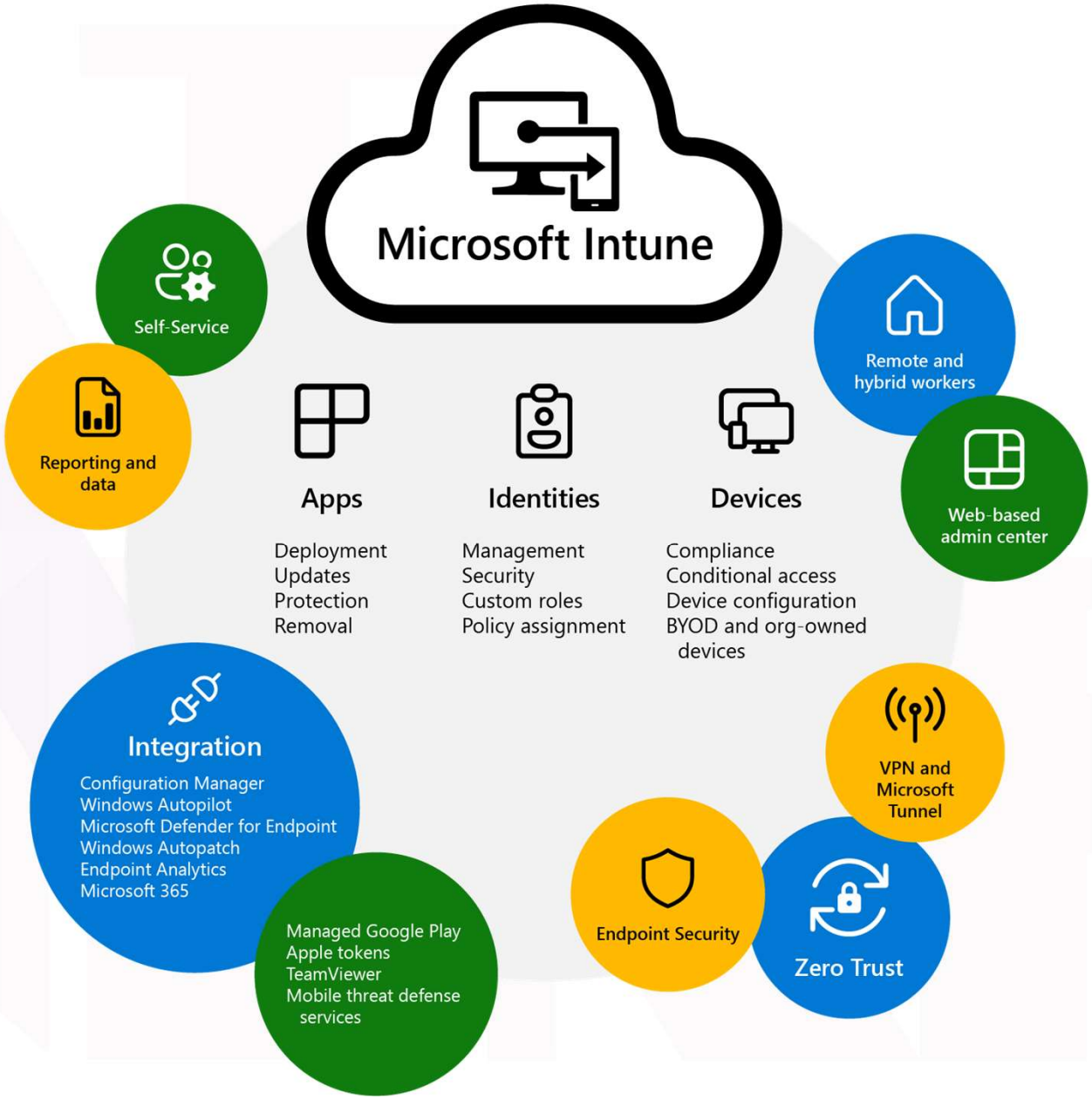
Microsoft Intune

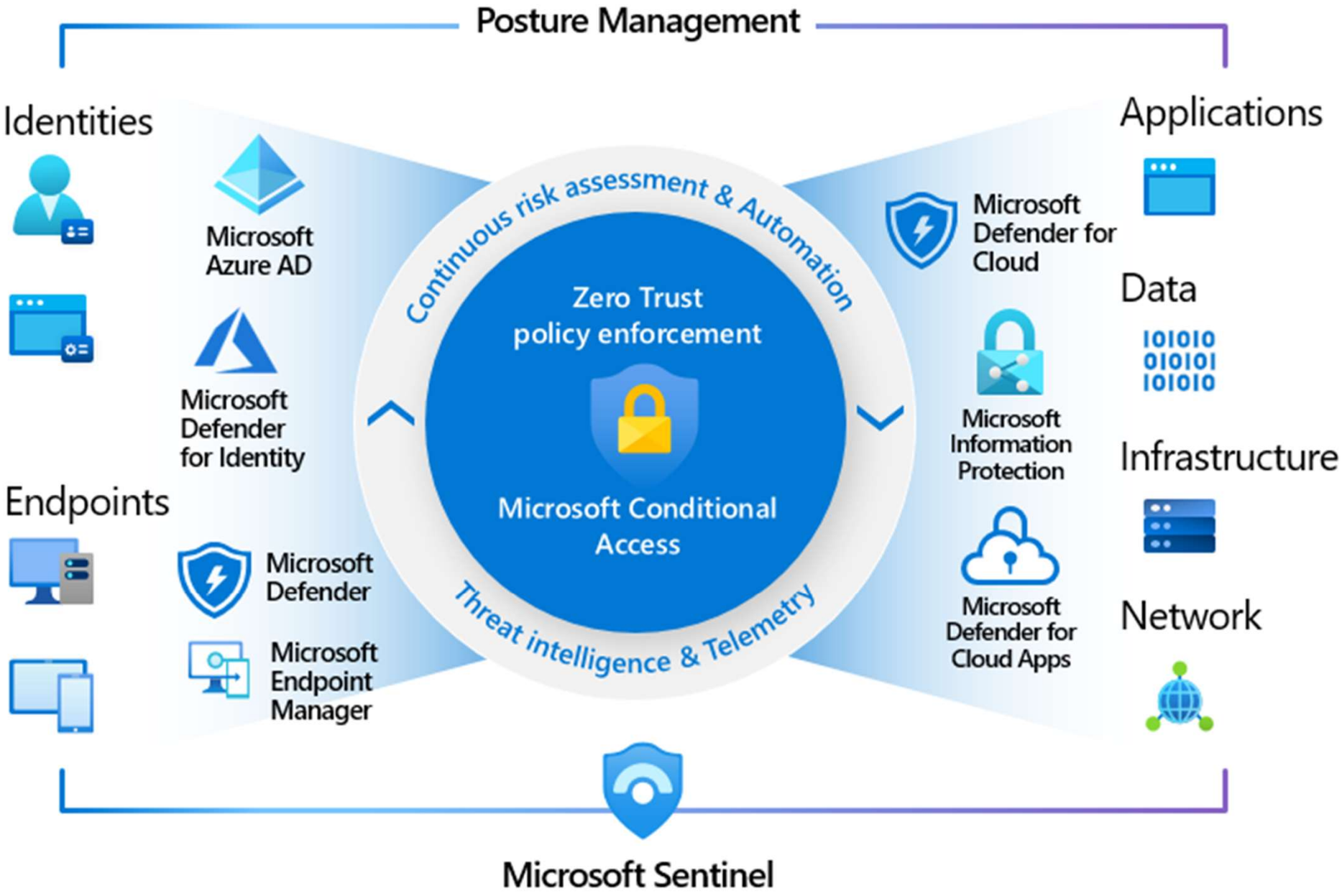
Famous Triangle



What is Intune?

Intune is the cloud-based solution for your mobile/device-management needs




Posture Management
Identities
Microsoft Azure AD
Microsoft Defender for Identity
Endpoints
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Microsoft Conditional Access
Threat intelligence & Telemetry
Applications
Microsoft Defender for Cloud
Data
Microsoft Information Protection
Infrastructure
Microsoft Defender for Cloud Apps
Network
Microsoft Sentinel

Why Zero Trust - Zero Trust priciples

- Verify explicitly
  - Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies
- Use least-priviledge access
  - Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity
- Assume breach
  - Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses

Zero Trust

Identities

- When an identity attempts to access a resource, verify that identity with strong authentication and ensure that requested access is compliant and typical.

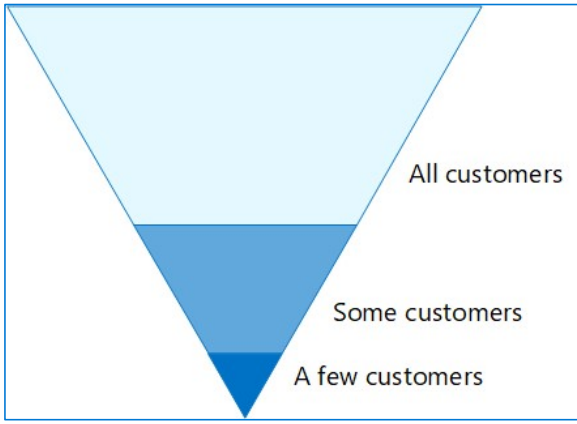
Devices (also called endpoints)

- Monitor and enforce device health and compliance requirements for secure access.

Applications

- Apply controls and technologies to discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control user actions, and validate secure configuration options.

Zero Trust Security with Intune



- Never trust, always verify ☺
- Possible to implement Zero Trust on all platforms
- Every request treated as originates from an untrusted network, regardless of its actual source or network location
- Data and apps remain secure even if a device or user's credential are compromised

User roles for Intune

To create, edit, or assign roles, your account must have one of the following permissions in Azure AD (Entra ID):

- Global Administrator
- Intune Service Administrator (also known as Intune Administrator but not to be confused with the built-in Intune Role Administrator role.)

Admin role	Who should be assigned this role?
Application manager	Assign the Application manager role to users who manage the application lifecycle for mobile apps, configure policy-managed apps, and view device info and configuration profiles.
Help desk operator	Assign the help desk operator role to users who assign apps and policies to users and devices.
Intune role administrator	Assign the Intune role administrator to users who can assign Intune permissions to other admins and can manage custom and built in Intune roles.
Policy and profile manager	Assign the policy and profile manager role to users manage compliance policy, configuration profiles and Apple enrollment.
Read only operator	Assign the read only operator role to users who can only view users, devices, enrollment details and configurations.
School administrator	Assign the school administrator role to users for full access to manage Windows 10-11 and iOS devices, apps, and configurations in Intune for Education.
Cloud PC Administrator	A Cloud PC Administrator has read and write access to all Cloud PC features located within the Cloud PC blade.
Cloud PC Reader	A Cloud PC Reader has read access to all Cloud PC features located within the Cloud PC blade.

1. Centralised Control

- No need for additional infrastructure
- Cloud Based platform
- You can manage all devices
  - PC
  - Mac
  - Mobile devices (Android, iOS)
- Data and Threat protection, Identity management
- Connection to Configuration Manager

2. Detailed reporting and analytics

- To make decisions or actions you need reporting
- Holistic view of device compliance accross tenant
- Usage analytics (devices, apps)
- Monitoring Security incidents
- Helps optimising management strategy

3. Microsoft's Enterprise Mobility + Security suite

- Security and and data control
- Easy BYO device management
- Mobile-device management, apps, identity access management

- VAN

4. Unify access to business apps for employees

- Based on device types (PC, Mac, iPhone, Android)
- Grouping Line of Business (LOB) apps based on app types
- Grouping users and provide access
- Add apps to Microsoft Intune | Microsoft Learn

App types

App types	Installation	Updates
Apps from the store (store apps)	Intune installs the app on the device.	App updates are automatic.
Apps written in-house or as a custom app (line-of-business)	Intune installs the app on the device (you supply the installation file).	You must update the app.
Apps that are built in (built-in apps)	Intune installs the app on the device.	App updates are automatic.
Apps on the web (web link)	Intune creates a shortcut to the web app on the device home screen.	App updates are automatic.
Apps from other Microsoft services	Intune creates a shortcut to the app in the Company Portal. For more information, see App source setting options.	App updates are automatic.

Compatible with all your employees' devices

- Managing devices on one place
- Bulk enrolment
- Setup and add protection policies

5. Admin console for company-assigned Cyber Security requirements

- Security controls and features
- Easy setup and manage cyber security goals
- Controled access managed by approved admins
- All devices are set up with Intune before any work applications, email, files are in use
- Control compliance and actions

6. Easy and reliable control over the security and applications

- Control accross all users and devices
- Easy security update
  - Anti-malware, firewall policies, virus definition
- Limit email (and other apps) access to device, such as a public computers
- BYOD matrix and management

7. No need to deal with individual device setup

- Enables to deploy software accross all enrolled devices
- Configure Windows update for Business
  - Feature update (major, semi-annual updates)
  - Quality update (monthly updates that reduce patching issues)
- Other updates

8. Embrace the Cloud: no on-site maintenance required

- Intune is Cloud based system
- Global accessibility
- Possible Hybrid environment
- Reduced the rist of potential security vunerabilities associated with on-site server
- Single sign-on for iOS and Android platforms

9. Easily deploy software and updates to your business devices

- Again…
  - Mac OS, Android, iOS, Windows suite
- Easy switch from desktop to mobile device without compromising the company's security
- Effortlessly manage software deployment and updates

10. Allow or deny user access - Security management

- Wifi pre-setup
- Certificates
- Business apps
- Conditional access


Thank you!

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ