**TITLE**

Protect Your Endpoint Environment with Microsoft Endpoint Manager (MEM)

**WHAT IS MEM?**

* Unified platform for endpoint management
* Combines Intune (cloud) + SCCM (on-prem)
* Supports Windows, macOS, iOS, Android
* Enables Zero Trust security model

**WHY PROTECT ENDPOINTS?**

* Endpoints = entry points for cyberattacks
* Risks: malware, phishing, data theft
* Remote/hybrid work → larger attack surface
* Strong endpoint protection = safe organization

**KEY SECURITY FEATURES**

* Device compliance policies
* Conditional access control
* App protection policies (MAM)
* Encryption & threat protection
* Integration with Microsoft Defender (EDR)

**BENEFITS & MONITORING**

* Unified endpoint management
* Improved security and compliance
* Remote management saves time
* Monitoring dashboards → Track device health, app usage, security alerts
* Reporting & audit logs → Analyze and track devices

### ****HOW MEM PROTECTS YOUR ENVIRONMENT****

* Enforces security policies across all devices
* Automates OS & app updates/patching
* Secures company data in apps (BYOD included)
* Provides insights & reports for proactive defense

**SUMMARY**

* **Microsoft Endpoint Manager = Intune + SCCM + Defender**
* Provides **complete endpoint protection & management**
* Key Features:
  + Compliance policies
  + Threat detection
  + Conditional access
  + Device enrollment
  + Encryption & monitoring
* Ensures organizations are **secure, compliant, and productive** in the modern workplace