Ensure a secure, robust and effective strategy for managing sensitive data on clinicians' personal and corporate devices

with Microsoft Endpoint Manager

The proliferation of devices connecting to corporate networks continues to accelerate across all industries and Healthcare is no exception. More and more, the need to simultaneously support mobility while reducing risk challenges IT teams.

With the unique needs of Healthcare organizations in mind, is important to ask:

- Are you doing enough to protect sensitive data and meet HIPAA and HITECH regulations?
- Are organizational policies seamless enough for busy clinicians and staff to deliver excellent patient care?

Protecting your organization while meeting the needs of busy healthcare professionals and providers is a balancing act. ATSG's Endpoint Management Proof of Concept for Healthcare is designed to show you that it is possible to adhere to corporate policy while eliminating barriers to providing excellent patient care.

ATSG's Endpoint Management Proof of Concept

ATSG has deployed Microsoft Endpoint Manager on over 250,000 of our Healthcare clients' devices, allowing organizations to secure data on clinicians' BYO devices and manage company-owned devices while mitigating risk, removing barriers to embracing digital transformation and eliminating obstacles to providing excellent patient care.

Suitable for managing iOS, Android, Windows 10, and MacOS devices, this structured engagement includes Assessment, Design, Build and Pilot phases with deliverables noted for each phase, including regular project status reports and knowledge transfer.

Assessment	Design	Build	Pilot
• Define business & technical requirements • Document Active Directory & Licensing • Workstation, Mobile Device & Application Discovery • Identify applicable software updates, Security (AV/malware protection) solutions, Identity solutions & current deployment models	• Design device enrollment process (Azure AD Registered/Azure AD Join/Hybrid Azure AD Join) • Design compliance policies, configuration profiles, conditional access policies & endpoint security policies • Define Windows 10 Security baselines • GPO to configuration profiles strategy • Define Azure AD User & Device Groups • Endpoint security AV, disk encryption & Firewall • Autopilot deployment profiles	• Configure Intune MDM • Configure Device Enrollment • Configure up to (2) Compliance Policies, Conditional Access Policies, Device Configuration Policies, Endpoint Security Policies, Windows 10 update rings, feature updates and quality updates & Windows Autopilot deployment profiles • Configure up to (4) Azure AD User and Device Groups & Applications	• Enrollment of Pilot Devices • Deploy up to (2) apps, device configuration and compliance policies to pilot devices • Monitor the success of the Pilot • Create action plan to remediate issues • Validate Intune policies on devices • Validate Autopilot process on pilot devices • Validate findings, present analysis, and develop next steps

Upon the conclusion of the engagement, ATSG will ensure you have a secure, robust, and effective configuration of Microsoft Endpoint Manager's UEM and Autopilot functions that will significantly enhance your device management, deployment, and security, capabilities

www.ATSG.net

ATSG
One Penn Plaza
New York, NY 10119