

ZERO TRUST BASELINE SECURITY PILOT

Microsoft Partner



Gold Cloud Platform Gold Data Platform Gold Data Analytics Gold Windows & Devices Gold Data Center Gold Cloud Productivity

Value proposition

Whether users are working remotely or on-site, the Zero Trust Baseline Security Pilot is meant to understand the customer's security goals and develop the foundation of a baseline by securing identities, applications, and devices. The pilot will help customer prepare a successful platform to easily scale the baseline security framework to all users in the enterprise.

Eligible workloads

- Azure Active Directory(SSO, Conditional Access, Identity protection, MFA, SSPR, IGA)
- · Microsoft Endpoint Manager
- · Microsoft 365 E3 or E5

Customer benefits

- Quick assessment on your M365 environment to improve security strategies aligning with zero trust principles.
- Successful platform layout to roll out enterprise-wide business needs surrounding SSO, MFA, BYOD, Remote management of corporate devices etc.
- · Learn how to operationalize and build on Zero trust security principles.
- Customer immersion experience to help test and learn the tools used.
- Discuss and review to embark on a more advanced end-to-end security journey with Invoke

Planning workshop offer*

• Microsoft funding may be available upon request

Invoke scope of delivery

- Invoke engineer would deploy the configurations remotely based on the agreed scope during the assess phase
- The pilot can include up to 600 users.

Timeline – Customer customizable agenda and timeline



Phase 1- Assess

- Create a detailed design for Intune for iOS, Android and Windows device types, Azure AD Conditional Access for Intune enabled Office 365 apps
- Configure Azure AD Conditional Access for Azure AD/Intune integrated applications
- Test the configured services to a limited set of users
- Setup and configuration of the customer infrastructure to support a Zero Touch deployment:
 - → Microsoft Azure Active Directory
 → Microsoft Endpoint Manager



Phase 2 - Execute Identity Strategy

- Review and setup Azure Identity Management
- Connect users, groups, and devices (including federating cloud)
- Standardize and integrate applications with Azure Active Directory
- Review and implement Policies and Access
- Configure logging and reporting to improve visibility
- Manage Entitlements (Azure AD Premium P2)
- Enable Azure AD Hybrid Join or Azure AD Join
- Enable Intune for managing users' mobile devices (EMS)
- Migrate existing identity providers integrated applications to Azure AD
- Knowledge, skill transfer and training



Phase 3 – Execute Endpoint Strategy

- Set up and configure Microsoft Intune Mobile Device Management (MDM)
- Align policies
- Configure monitoring and alerts
 Protect corporate email on managed & unmanaged devices
- Microsoft Endpoint Management review of how devices are enrolled
- Demonstrate and setup/Configure MDM base
- Review & demonstrate enrollment scenarios available for Mobile Devices
- Implement PC Client devices with Microsoft Endpoint Manager
- Potentially Configure and Demonstrate Unenrollment of devices
- Configurations and compliance policies for iOS, Android, Windows & MacOS
- Docs management & operations

Zero Trust Security Baseline Strategy

Execute Identity
Strategy

Execute Endpoint Strategy

Zero Trust Baseline

CONTACT US: InvokeLLC.com | hello@InvokeLLC.com | +1 (713) 909-0411 | 118 Vintage Park Blvd. #W, Houston, TX 77070