Mobile Device Management (MDM)

Supports all types of endpoints
• Mobile • Tablet iPad • Thick (laptops and desktops) • Thin Clients • IOT • Wearables
Supports all types of ownership models
• BYOD • SOVO • COPE • BYOL
Supports all types of operating systems
• Android • IOS • Chrome OS • Windows 10 • MacOS • BlackBerry

Supports all types of device enrollment
• iOS MDM Controls • IOS user registration • iOS user privacy • Android Enterprise Work and Personal full • Android Enterprise Work and Personal User Privacy • Android Enterprise Workspace Only • Samsung Knox Workspace Only • Samsung Knox Work and Personal • Android User Privacy • Windows 10 MDM controls • macOS MDM controls • BlackBerry Work and Personal * BlackBerry Workspace Only

Solution provides proprietary platform agnostic secure container with ability to secure applications only without UEM agent or device enrollment:

- Password enforcement (complexity and rotation)
- Device Lock and container lock (after a specified period of inactivity)
- Remote Full Device Wipe
- Selective Wipe (eg. only corporate content and applications)
- Certificates (eg. federal information processing standard [FIPS] 140-2) and EAL4+ certified
- Managed Application Data Removal
- Support Windows 10 and MacOS security policies and compliance
- MultiSource Authentication (credentials, certificate-based authentication, pin, and biometric data)
- Enforce compliance security across all types of endpoints and operating systems
- Detect and enforce OS platforms and versions, installed applications, and manipulated data
- Detect iOS jail-broken devices and rooted Android devices
- Filter (restrict) access from noncompliant devices to corporate servers to corporate servers (eg. email)
- Restrict downloadable applications through whitelists and blacklists
- Support for the Apple Device Enrollment Program and the Volume Purchase Program for IOS and MacOS
- Support for integration with Windows Information Protection
- Support for integration with Microsoft Intune App Protection
- Single unified UEM Management Console for MDM, MAM, MCM, IAM and MTD.

• Ability to leverage a centralized UEM instance across multiple separate Exchange and AD forests.
• Capabiliy to delegate policy management (select user / device to policy) and deployment to abusiness unit. (eg. via AD group)
• Microsoft SQL-based configuration/data repository
• Role Based Administration Capability for granular level admin rights.
• Self-service Portal for initial activation/repositioning.
• Self-service troubleshooting capability for end users
• Platform scalability for over 50,000 supported devices
• Users can be activated on UEM with zero-input activation using a QR code for iOS and Android
• Supports Active Directory linked groups for automated user onboarding.
• Solution must be deployable completely on premises
• Containerized applications must use FIPS validated cryptography and Common Criteria EAL 4 +
• Solution must employ end-to-end encryption for data at Rest, data in-Transit, and data in-Use
• Solution must support its own application containerization engine
• Solution should be able to apply mobile security policies on application level
• Solution must be able to secure applications with certificate-based authenticatio

Solution must be able to support application upload via:
• AppStore
• Google Play Store
• Windows Store
• BlackBerry World
• in -House Internal application
• web shortcuts
• Solution must be able Blacklist/Whitelist/ and the group required applications lists
• Secure applications by wrapping post code complies without modifying the source code
• Enforce authentication of the user before using the application (for example, login with corporate credentials)