Mobile management (MAM)

• Compliance Auto detect compromised status upon application launch to restrict the use of applications when detected
• Solution should be able to apply per-app VPN for any mobile published application
• Support for Android SafetyNet Attestation to protect sensitive data from malicious attacks
• Solution must be able to provide secure back-end connectivity to internal resources via secure mobile applications such as email and web pages without any VPN or public publication
• Solution must provide a dedicated Mail secure app that includes mail, calendar, and contacts
• Secure Mail client must support mailbox delegate, shared mailboxes, PIM, shared calendars and show live status of the contacts
• Secure Mail client must include Azure RMS Support
• Secure Mail client must contain an embedded attachment viewer for Microsoft and PDF documents
• Solution must provide secure access to back-end SMB CIFS shares via secure mobile application with inherited NTFS permissions
• Solution must provide secure app for web browsing with access to intranet resources
• Solution must provide a secure application to integrate with Notes.
• Solution must provide a secure application to integrate with Tasks.
• Solution must provide a secure collaboration application that integration with Skype, Lync, and Jabber for secure chatting
• Secure apps must provide app-level watermarking
• Solution must provide a secure application for editing Microsoft documents and PDFs 3
• Solution must provide a secure application to collaborate, share, and synchronize content
• Solution must provide a secure application that enables secure container integration with native Microsoft 365 mobile applications
• Solution must provide a secure containerized browser application for Windows 10 and MacOS.

Secure browser for Windows 10 and MacOS should support the following without VPNs or agents:
✓ Authentication on launch
✓ Access to intranet web
✓ Access to mail access
✓ Access to intranet contacts
✓ Access to intranet calendar

Secure Application Container must support
✓ biometric authentication for IOS and Android
✓ screen lock timeout
✓ App Lock timeout
✓ Data leak prevention
✓ Enable/disable FIPS
✓ Restrict screen recording and sharing on iOS, Android and Windows 10

• Integrates with existing on-prem repositories (network shares, WebDAV, SharePoint, CMIS)
• Supports cloud repositories (O365, One Drive, Google Drive, Box)
• Seamlessly integrates with existing content repositories - no need to copy or duplicate existing content
• Content encrypted at rest (FIPS 140-2 AES 256)
• Prevent copy / paste / screenshot / printing
• Content accessibility effective and expiration dates
• Restrict content downloads while roaming, Wi-Fi only connections
• Whitelist or Blacklist file types to determine what can be uploaded or synced
• Desktop synchronization - two-way sync of content rom desktop to device (PC & Mac)
• Outlook Add-In for creating links to documentation in email Share content
with external users
and view with HTML5 content viewer for DLP
• Solution must employ files level security wherever files travel, and wherever they're opened online or offline, internally or externally.