CHECK POINT CAPSULE WORKSPACE

FEATURES

- Corporate resource security and access control
- Encryption for data at rest and for data in transit
- Root and jailbreak detection
- Man-in-the-Middle attack detection
- Single Sign-on (SSO) to corp apps
- App wrapping for native mobile apps
- Remote wipe of business data
- Supports iOS and Android devices

BENEFITS

- One-touch, secure access to email, messaging, calendar, contacts, native enterprise apps, and docs
- Secure access to corporate data on any mobile device
- Separate corporate and personal data on mobile devices
- Prevent corporate data loss on mobile devices
- Respect user privacy
- Control costs with low overhead architecture
- Protect against advanced mobile threats

MOBILE SECURITY IS CHALLENGING

Our world is more connected than ever. Instant access to apps and information isn't just a convenience; it's a necessity. Whether a smartphone or tablet is company issued or personally owned, your employees expect it to meet all of their personal and professional needs.

The data accessed and stored on these devices makes them valuable and vulnerable targets for cybercrime, but users won't tolerate a locked-down experience or security that forces them to change. A successful mobile security strategy must balance your organization's requirements with its employee's demand for privacy and a straightforward, familiar user experience.

Protect and manage sensitive mobile data

Check Point Capsule Workspace protects and manages enterprise apps and data on iOS and Android devices without needing to manage Mobile Device Management (MDM) profiles. So no matter which team is responsible for supporting smartphones and tablets, they'll value how Capsule Workspace secures mobile environments with ease – including BYOD.

Capsule Workspace is easy to deploy and manage, helping to reduce the time, effort, and cost of keeping mobile devices and data secure. Once deployed, it creates an AES256-bit encrypted container for enterprise apps and data that puts you in control of the sensitive enterprise information you need to protect. It never touches the personal apps, media, or content, on a device which helps improve end user adoption, even on personally-owned devices.

Users will also appreciate the native experience and one-touch access Capsule Workspace provides to the critical enterprise apps they need to stay in touch on the go. It supports Microsoft Exchange Server and Office 365 email, calendar, and contacts, and includes secure enterprise instant messaging and document access.

Authentication, data protection, and vulnerability mitigation

Capsule Workspace protects your organization's mobile data in several ways. Strong authentication options like Active Directory, LDAP, RADIUS, and RSA SecureID keep access to enterprise apps and data safe. Data stored on devices can be set to expire within a certain timeframe, limiting the amount of locally-accessible data. Enterprise data can also be wiped safely from lost or stolen devices.

January 11, 2017

Capsule Workspace also protects organizations from security risks introduced if a user roots or jailbreaks a device, and from Man-in-the-Middle attacks. If any of these risks are detected, Capsule Workspace blocks access to the container, to internal resources and to any enterprise apps on the device protected by Capsule Workspace app wrapping. For additional security, Capsule Workspace integrates with Check Point Mobile Threat Prevention for advanced mobile threat detection and mitigation capabilities.

Anywhere, anytime access to critical business apps

Capsule Email, Calendar, and Contacts

On-the-go workers want enterprise ready apps that are consumer simple. Capsule Workspace Email, Calendar, and Contacts provide a native experience users expect that syncs automatically with their Exchange or Office 365 account. Perform bulk actions like deleting or archiving messages, manage multiple synced folders, review availability and send meeting invites, and update contacts from anywhere.

Capsule Workspace Messages

Capsule Workspace Messages is an integrated, secure instant messaging feature that uses Exchange to store and retrieve messages between business colleagues. It supports personal and group messaging with internal or external users with push notifications for new messages. Users can send messages, locations, videos, photos, and attack, save and view protected or unprotected documents.

Enterprise Document Access

Enterprise files and documents can be accessed in a secure, controlled way in Capsule Workspace. You can set policies for how users share and if they can open documents from files saved in Workspace using external apps (on Android only). And external files can be brought into Capsule Workspace container by saving them from mail attachments and messages, or from within business apps.

Capsule App Wrapping

Capsule App Wrapping provides an extra layer of encryption and security for native iOS and Android enterprise apps, developed for their own use. It offers different methods to fulfill your app security needs including:

- **Wrapping Engine:** Runs on closed (unsigned) app binary (IPA/APK) files and provides them with security layers that prevent data leakage and a built-in SSL VPN as a Capsule Workspace app.
- **SDK Library (iOS only):** Gives the same abilities as the Wrapping Tool, but also gives developers control over the security features we offer dynamically at development time. It supplies more granular settings for which app parts to protect and how. The developer can choose between Quick Integration and Manual Integration.

Mobile Operating System Support

- Android 4.0 and up and iOS 9.0 and up

Supported Applications in Capsule Workspace

- Email, Calendar, Contacts
- Notes
- Tasks
- Workspace Messenger
- File repository & editing
- Web-based business applications
- Remote desktop (using WebSocket)
- Wrapped native applications

Server Support

- Supported on Exchange server 2007 SP2+, 2010, 2013, and 2016
- Supported on Office 365 Exchange Online
- Based on “Exchange Web Services” protocol
- Support for push email

Security and access

- Username / password (AD/LDAP)
- RADIUS challenge response
- Client certificate
- RSA SecureID
- DynamicID SMS
- 2FA authentication with password (AD/LDAP), RADIUS, Client certificate, RSA SecurID, DynamicID SMS
- App protection
- Root/Jailbreak detection
- MitM protection
- Advanced Threat Protection through Check Point Mobile Threat Prevention integration

Security Gateway and Management Support

- R77.30 and higher

CONTACT US

Worldwide Headquarters | 5 Ha’Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

January 11, 2017