



CHECK POINT CAPSULE WORKSPACE

FEATURES

- Secure access control for business resources
- Locally stored business data is sandboxed and encrypted
- Integrated encrypted communication for remote access
- Remote wipe of business data
- Detection and prevention of rooted and jailbroken mobile devices
- Single Sign-On (SSO) for ease of use and increased security
- Supported on iOS and Android devices

BENEFITS

- Secure access to business data on any mobile device
- Segregate business data from personal data and applications
- Prevent business data loss from mobile devices
- One-touch secure access to business resources such as email, corporate documents, calendar and more

CHALLENGE

Today we live in a world where we are always connected, from any device, everywhere we go. We check our business email from our personal devices and stay connected with our friends and family from our business devices. Today, all our devices, from corporate issued laptops and mobile phones, to personal smartphones and tablets combine both our business and personal needs.

Due to this shift, the data and applications on our mobile devices have become more vulnerable than ever. Commonly occurring incidents like lost or stolen phones can cause sensitive business data to be compromised. On the other hand, remote wipe of devices by the IT departments can cause loss of valuable personal data.

Organizations are seeking to find a solution that will strike a balance between enabling an increase in employee productivity and ensuring strong data security to support full business continuity.

SOLUTION

Check Point Capsule provides organizations with a better solution to this problem. By providing access to business data from within a secure application, it enables organizations to protect and manage business data on any mobile device.

With Check Point Capsule, employees have secure, one-touch access to corporate email, files, and other corporate assets. By separating business and personal applications, Check Point Capsule ensures that personal applications, media, and content on mobile devices remain private.

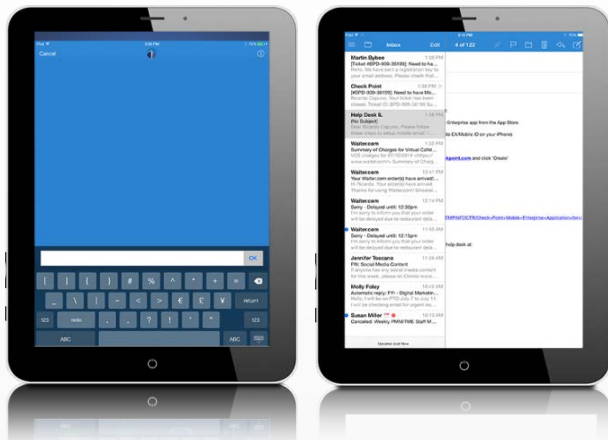
Check Point Capsule enables organizations to strike the perfect balance between supporting easy access on mobile devices for increased employee productivity, and strong data security.

Segregate business and personal data

Check Point Capsule provides a secure environment for authorized users where business data is stored, managed, and encrypted. This enables secure use of business resources on both corporate and personal devices. With Check Point Capsule, personal applications on mobile devices stay personal as business data is separated from personal assets.

Secure and seamless access

Secured through an authenticated and encrypted connection, business resources can be remotely accessed from any iOS or Android device. With a simple touch of a button you have secure access to business resources such as email, calendar, contacts, notes, documents, web applications and remote desktops.



Prevent data loss from mobile devices

Check Point Capsule provides secure access to business applications and data through strong authentication options such as Active Directory, LDAP, RADIUS, and RSA SecureID. Businesses can protect their data in several ways. Data stored on mobile devices can be set to expire within a certain timeframe, limiting the amount of data accessible locally. And, business data can be safely removed from a lost or stolen device.

Check Point Capsule protects organizations from the additional security risks introduced by rooting and jailbreaking by detecting and preventing access from these devices, keeping business data safe.

SPECIFICATIONS

MOBILE OPERATING SYSTEM SUPPORT

- iPhone and iPad—Apple iOS 7.0 and up
- Android 4.0 and up

SUPPORTED APPLICATIONS IN CHECK POINT CHECK POINT CAPSULE WORKSPACE

- Email
- Calendar
- Contacts
- Notes
- File repository
- File editing
- Internal web based business applications
- Remote desktop (using WebSocket)

EMAIL, CALENDAR, CONTACTS, AND NOTES SERVER SUPPORT

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

AUTHENTICATION OPTIONS

- Username / password (AD/LDAP)
- RADIUS challenge response
- Internal CA certificate
- RSA SecureID
- DynamicID SMS
- 2-step authentication

SECURITY GATEWAY AND MANAGEMENT SUPPORT

- R77.10 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