CTI.RU

CTI COMMUNICATIONS TECHNOLOGY INNOVATIONS

ЦИФРОВОЕ РАБОЧЕЕ МЕСТО

Мобильность как бизнес-преимущество:

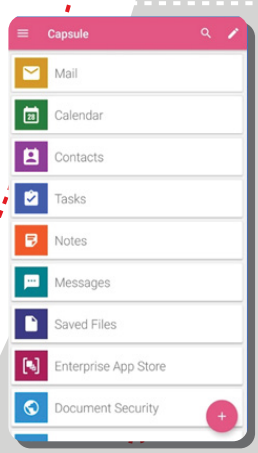
- удобно
- эффективно
- безопасно

Быстрота принятия решений и оперативность позволяют побеждать в конкурентной борьбе. Чтобы обеспечить высокий уровень мобильности необходимо предоставить доступ к корпоративной почте, документам и ресурсам компании со всех устройств — телефона, планшета и ноутбука.

Бизнесу необходимо обеспечить комплексную защиту всех мобильных устройств, которые используют сотрудники для работы. Это позволит предотвращать продвинутые кибератаки, поможет противостоять как внешним, так и внутренним угрозам, а также обеспечит защищенный доступ в корпоративную сеть. Часть используемых сотрудником устройств могут быть не корпоративными, тогда помимо защиты важно сохранить приватность частной информации (концепция BYOD — Bring Your Own Device).

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Capsule создает безопасную бизнес-среду и отделяет корпоративные данные и приложения от персональных. Это позволяет сотрудникам безопасно работать с бизнес-приложениями через простой пользовательский интерфейс, который обеспечивает доступ к корпоративной почте, файлам, каталогам, контактам и календарю в одно касание и не влияет на личные данные пользователя.



Check Point Capsule представляет собой безопасный контейнер защищенный паролем, шифрующий данные в контейнере и ограничивающий доступ, даже если устройство будет взломано.

- Защищенная область на устройствах iOS и Android
- Интеграция с корпоративными приложениями
- Разделение рабочей и личной информации
- Неприкосновенность частной жизни
- Очистка только корпоративной информации в случае кражи устройства или взлома
- Решение поддерживает электронную почту, календарь и контакты Microsoft Exchange Server и Office 365, а также обеспечивает безопасный обмен мгновенными сообщениями внутри компании и доступ к корпоративным документам

Capsule Workspace прост в развертывании и управлении, что позволяет сократить время, рабочие активности и стоимость защиты мобильных устройств и данных. После развертывания создается зашифрованный контейнер для корпоративных приложений и данных с использованием алгоритма шифрования AES-256, позволяющий контролировать конфиденциальную корпоративную информацию, которая должна находиться под защитой. Контейнер не влияет на работу личных приложений, мультимедийных данных и контента на устройстве, позволяя адаптировать работу конечного пользователя даже на личных устройствах.

Пользователям также понравится удобная работа в Capsule Workspace и доступ в одно касание к критически важным корпоративным приложениям, что позволит всегда быть на связи — даже удаленно.

ФУНКЦИИ

- Безопасность и контроль доступа к корпоративным ресурсам
- Шифрование данных при хранении и передаче
- Обнаружение root и jailbreak-атак
- Обнаружение MITM-атак
- Технология единого входа (SSO) в корпоративные приложения
- Полная очистка нативных мобильных приложений
- Удаление корпоративных данных
- Поддержка устройств под управлением iOS и Android

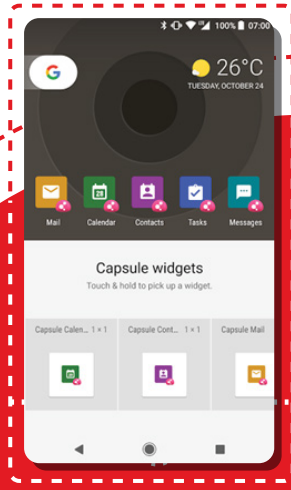
ПРЕИМУЩЕСТВА

- Безопасный доступ к электронной почте, обмен сообщениями, работе с календарем и контактами, защита нативных корпоративных приложений и документов и безопасный доступ к корпоративным данным с любых мобильных устройств
- Разделение данных на мобильных устройствах на корпоративные и личные
- Предотвращение потерь корпоративных данных на мобильных устройствах
- Поддержка приватности пользователя
- Контроль затрат на архитектуру
- Защита от комплексных мобильных угроз

АВТОРИЗАЦИЯ, ЗАЩИТА ДАННЫХ И МИНИМИЗАЦИЯ РИСКОВ УЯЗВИМОСТЕЙ

Capsule Workspace защищает мобильные данные вашей компании с помощью комплекса мер. Продвинутые опции авторизации Active Directory, LDAP, RADIUS и RSA SecureID обеспечивают безопасный доступ к корпоративным приложениям и данным. Пользователи могут установить точный срок хранения данных на устройствах и ограничение на количество данных в локальном доступе, а также удалять корпоративные данные с устройств в случае их потери или кражи.

Capsule Workspace защищает компании от рисков безопасности при root, jailbreak или MITM-атаках на устройства пользователя. При обнаружении рисков Capsule Workspace блокирует доступ к контейнеру, внутренним ресурсам и любым корпоративным приложениям на устройстве под защитой Capsule Workspace. Для обеспечения повышенного уровня безопасности Capsule Workspace интегрируется с Check Point Mobile Threat Prevention для продвинутой защиты мобильных устройств и минимизации негативных последствий.



КРУГЛОСУТОЧНЫЙ УДАЛЕННЫЙ ДОСТУП К КОРПОРАТИВНЫМ ПРИЛОЖЕНИЯМ

Электронная почта, календарь и контакты

Для работы мобильных сотрудников необходимы простые в использовании специализированные бизнес-приложения. Электронная почта, календарь и контакты в рамках Capsule Workspace просты и удобны в работе, автоматически синхронизируются с аккаунтами Exchange или Office 365, и позволяют удалять и архивировать сообщения, управлять набором синхронизированных папок, просматривать статусы доступности сотрудников, отправлять приглашения на совещания и обновлять контакты удаленно.

БЕЗОПАСНАЯ КОММУНИКАЦИЯ

Capsule Workspace Messages — интегрированная безопасная среда с использованием Exchange для хранения и обмена сообщениями между сотрудниками. Доступны персональные сообщения и коммуникация в группах внутренних и внешних пользователей, а также push-уведомления о новых сообщениях. Пользователи могут обмениваться сообщениями, локациями, видео и фотографиями, а также сохранять и просматривать защищенные или незащищенные документы.

ДОСТУП К КОРПОРАТИВНЫМ ДОКУМЕНТАМ

Capsule Workspace обеспечивает безопасный контролируемый просмотр корпоративных файлов и документов. Компания может установить политики для обмена документами между пользователями и открытия файлов, хранящихся на Workspace, через внешние приложения (только для Android). Внешние файлы можно помещать в контейнер Capsule Workspace, сохраняя их без почтовых вложений и сообщений.

Capsule App Wrapping (установка приложения в контейнер)

Capsule App Wrapping – дополнительный уровень безопасности для шифрования нативных iOS и Android-приложений, разработанных для собственного использования, с набором различных методов защиты:

- **Адаптации установки:** запускается в закрытых (неподписанных) бинарных (IPA/APK) файлах приложения, обеспечивая высокий уровень защиты и предотвращая утечку данных со встроенным SSL VPN – приложением Capsule Workspace.
- **SDK-Библиотека (только для iOS):** в дополнение к возможностям, аналогичным Wrapping Tool, разработчикам доступна возможность контроля функций безопасности, предлагаемых в ходе разработки. Более детальные настройки и тип защиты для разных элементов приложений позволяют разработчикам выбирать между опциями быстрой интеграции (Quick Integration) и ручной интеграции (Manual Integration).

Поддержка ОС для мобильных устройств Android 4.0 и выше / iOS 9.0 и выше

Приложения, поддерживаемые Capsule Workspace

- Электронная почта календарь и контакты
- Заметки
- Задачи
- Мессенджер рабочего пространства
- Хранилище файлов и редактирование документов
- Корпоративные онлайн-приложения
- Удаленный рабочий стол (с WebSocket)
- Нативные приложения

Безопасный доступ

- Логин / пароль (AD/LDAP)
- RADIUS challenge response
- Сертификат клиента
- RSA SecureID
- Динамическая SMS-идентификация
- 2FA-авторизация с паролем
- AD/LDAP, RADIUS, сертификат клиента, RSA Secure ID, Динамическая SMS-идентификация
- Защита приложений
- Детектирование Root/Jailbreak-атак
- Защита от MITM-атак
- Продвинутая защита от угроз Check Point Mobile
- Prevention integration

г. Москва, ул. Кржижановского, д. 29, корпус 1 (5-й этаж). +7.495.784.73.13 CTI.RU