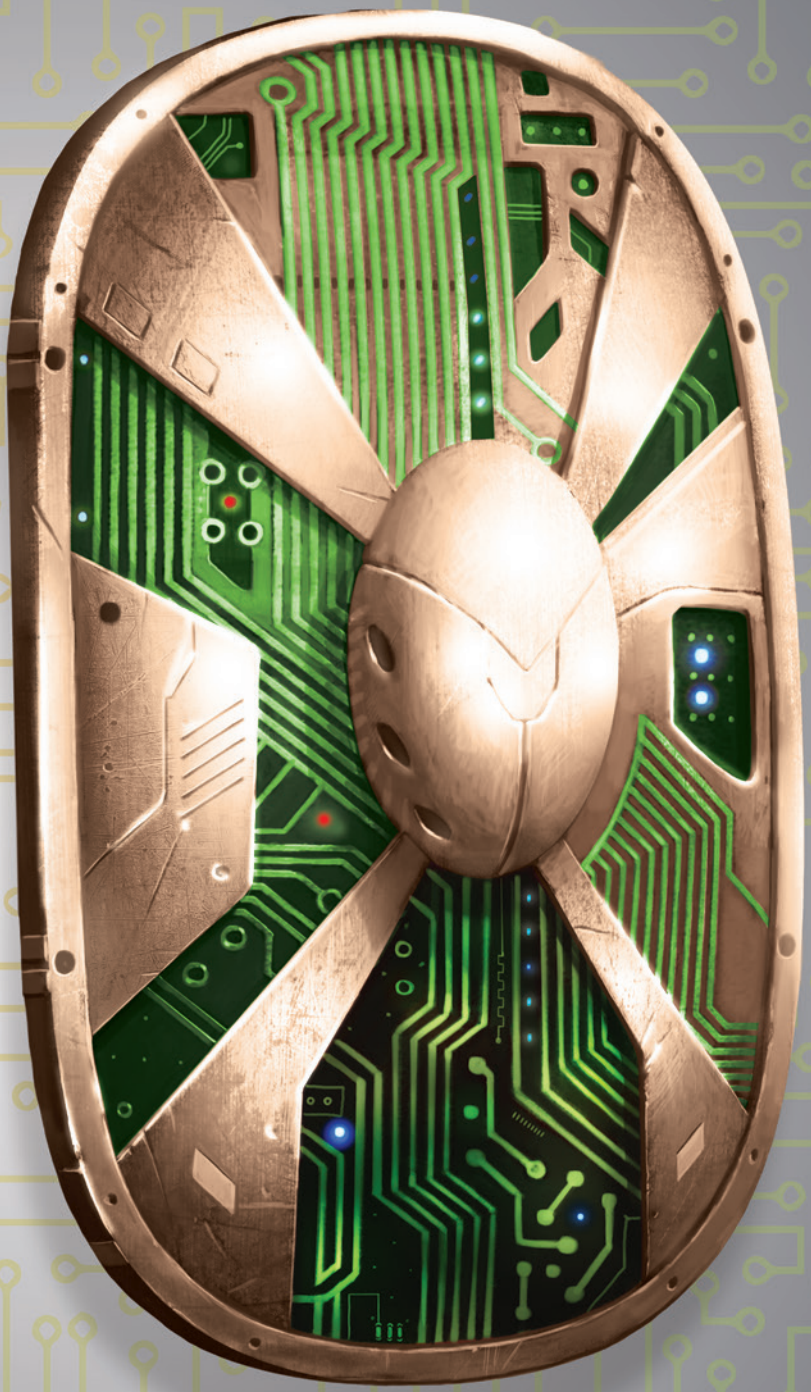
КОД БЕЗОПАСНОСТИ

SECRET MDM

Управление корпоративной мобильностью
и защита данных на мобильных устройствах

ПРЕИМУЩЕСТВА

- КОМПЛЕКСНЫЙ ПОДХОД К РЕШЕНИЮ ЗАДАЧ УПРАВЛЕНИЯ И ЗАЩИТЫ МОБИЛЬНЫХ УСТРОЙСТВ
- УПРАВЛЕНИЕ ДЕСЯТКАМИ ТЫСЯЧ УСТРОЙСТВ ИЗ ЕДИНОЙ КОНСОЛИ
- РАБОТА SECRET MDM НЕ ТРЕБУЕТ ПОСТОЯННОГО ПОДКЛЮЧЕНИЯ УСТРОЙСТВА К ИНТЕРНЕТУ
- ГИБКИЕ ВОЗМОЖНОСТИ РАЗВЕРТЫВАНИЯ: В «ОБЛАКЕ» ИЛИ В СОБСТВЕННОЙ ИНФРАСТРУКТУРЕ
- ГИБКАЯ ПОЛИТИКА ЛИЦЕНЗИРОВАНИЯ: ПО ПОЛЬЗОВАТЕЛЯМ ИЛИ ПО УСТРОЙСТВАМ



ВОЗМОЖНОСТИ

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ (MDM)

- Управление настройками устройств на базе iOS и Android с помощью механизма политик.
- Настройка подключений к точкам доступа Wi-Fi.
- Настройка прокси для выхода в Интернет через Wi-Fi.
- Запрет на подключение к недоверенным точкам доступа и ведение «белого» и «черного» списков Wi-Fi.
- Запрет на использование Wi-Fi, Bluetooth, а также запрет на использование встроенной фотовидеокамеры.
- Управление доступом к серверу корпоративной почты (Exchange).

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ ПРИЛОЖЕНИЙ И ДАННЫХ*

- Создание изолированного контейнера для корпоративных приложений и данных на личных устройствах.
- Изоляция приложений и данных в контейнере от личных приложений на устройстве .
- Прозрачное шифрование данных в контейнере.
- Выборочная очистка данных и приложений в контейнере.
- Блокировка функций «копировать/вставить» между приложениями в контейнере и вне него.

ЦЕНТРАЛИЗОВАННАЯ УСТАНОВКА И РАЗВЕРТЫВАНИЕ

- Регистрация устройств и установка агента управления по сети.
- Сервис регистрации пользователей.
- Инвентаризация конфигурации устройств.
- Инвентаризация приложений и сервисов.
- Получение списка зарегистрированных точек доступа Wi-Fi.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ ПРИЛОЖЕНИЯМИ (MAM)

- Установка приложений из публичных магазинов (Apple AppStore, Google Play Market).
- Распространение приложений из корпоративного магазина приложений или других источников по протоколам http и ftp.
- Ограничение запуска приложений в режиме «белого» (для контейнеров Samsung Knox) или «черного» списка.

МОБИЛЬНАЯ БЕЗОПАСНОСТЬ

- Удаленная блокировка устройства и управление парольной защитой.
- Удаленный сброс или смена пароля блокировки для восстановления доступа к устройству.
- Дистанционная очистка устройства (затирание всех данных).
- Шифрование данных на устройстве (криптоалгоритм AES).
- Обнаружение скомпрометированного устройства (rooting).
- Управление настройками СКЗИ «Континент-АП».
- Криптографически защищенные голосовые звонки (VoIP) и обмен сообщениями (шифрование «end-to-end»).
- Криптографическая защита и шифрование данных в интернет выполняется в соответствии со стандартами ГОСТ 28147–89, ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012.

ДОПОЛНИТЕЛЬНЫЕ КОРПОРАТИВНЫЕ ВОЗМОЖНОСТИ

- Геолокация: определение местоположения устройства по координатам в системе GPS, A-GPS, GLONASS.
- Интеграция с LDAP/Active Directory (импорт пользователей из AD).
- Ведение журналов событий.
- Мониторинг онлайн-активности и состояния защищенности мобильных устройств.
- Рассылка сообщений от администратора.

** Поддерживается управление контейнерами Knox, которые требуют наличия соответствующих лицензий компании Samsung*

СЦЕНАРИИ ПРИМЕНЕНИЯ

УПРАВЛЕНИЕ КОРПОРАТИВНОЙ МОБИЛЬНОСТЬЮ

Результат:

- Сокращены временные и материальные затраты на развертывание и администрирование систем корпоративной мобильности.
- Добавление новых пользователей и исключение устройств из списка контролируемых осуществляется администратором из веб-консоли.

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

Результат:

- Конфиденциальная информация защищена в соответствии с корпоративными политиками безопасности.
- Минимизированы финансовые и репутационные риски утечки конфиденциальной информации с мобильных устройств сотрудников.
- Политики безопасности продолжают действовать даже при отсутствии соединения с MDM-сервером.
- Повышена скорость реакции на инциденты безопасности.

ЗАЩИТА ТЕЛЕФОНИИ И СООБЩЕНИЙ

Результат:

- Минимизированы финансовые и репутационные риски утечки конфиденциальной информации при использовании звонков и сообщений с мобильного устройства.

ЛИЦЕНЗИРОВАНИЕ

ВОЗМОЖНОСТИ	START (БЕСПЛАТНО)	SMART	SECURE PACK
Удаленная настройка сетевых подключений	●	●	●
Управление доступом и парольной защитой	●	●	●
Защита от утечки при утрате устройства	●	●	●
Обнаружение обхода механизмов защиты	●	●	●
Настройка электронной почты (Exchange)		●	●
Управление приложениями		●	●
Контейнеризация корпоративных данных и приложений (требуется дополнительная лицензия Samsung Knox)		●	●
Управление VPN-подключениями			●
Защищенный мессенджер и телефония (beta)			●
Геолокация		●	●
Интеграция с LDAP/AD		●	●
Дистанционная регистрация устройств	●	●	●
Мониторинг и журналирование	●	●	●
Количество подключаемых устройств/пользователей	До 25 устройств	Не ограничено	Не ограничено
Размещение в «облаке»	●	●	
Размещение в собственной инфраструктуре		●	●

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка Secret MDM может осуществляться как напрямую, силами специалистов «Код Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера – партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов – обращается в службу технической поддержки вендора.
Существует несколько пакетов технической поддержки:


Базовый


Стандартный


Расширенный


VIP

КАТАЛОГ УСЛУГ	ПАКЕТ ПОДДЕРЖКИ			
	БАЗОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ	VIP
Доступность услуги	8x5, e-mail, телефон		24x7, e-mail, телефон	
Приоритет	Низкий	Средний	Высокий	Первоочередной
Количество обращений	Не ограничено			
Консультирование по установке и использованию продукта	●	●	●	●
Доступ на форум по продукту и к базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Личный кабинет на веб-портале	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Регистрация обращений на веб-портале		●	●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О КОМПАНИИ «КОД БЕЗОПАСНОСТИ»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный) info@securitycode.ru www.securitycode.ru