kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Secure Remote Workspace

Комплексный подход к безопасности удаленной работы

Инфраструктура виртуальных рабочих столов (Virtual Desktop Infrastructure, или VDI) дарит множество преимуществ. Она позволяет автоматизировать процесс создания рабочих мест, уйти от хранения и обработки данных на устройствах сотрудников, быстро восстанавливать рабочие станции после инцидентов, из одной точки управлять удаленными рабочими местами и снижать риски атак через них.

Концепция VDI подразумевает, что сотрудники получают свои рабочие инструменты, виртуальные ПК, в виде набора программ и данных на удаленном сервере. Чаще всего для подключения и работы с ними используются специальные терминалы – **тонкие клиенты.** Они значительно снижают риски в области информационной безопасности, так как на рабочих станциях сотрудников не хранится и не обрабатывается информация.

Тонкие клиенты проще в администрировании и управлении по сравнению с традиционными персональными компьютерами. Они упрощают работу корпоративных ИТ-служб: те имеют физический доступ к рабочим столам, находящимся на сервере компании. Оптимальны тонкие клиенты и с точки зрения экономии сил и средств: можно обновлять ПО сразу на всех терминалах из единого центра, а их жизненный цикл гораздо дольше, чем у обычных персональных устройств. К тому же тонкие клиенты предназначены для выполнения конкретных задач, и зачастую их функционал ограничивается программным обеспечением, необходимым для работы. Это препятствует использованию таких терминалов в личных целях сотрудников, а значит, способствует большей результативности и не дает пользоваться сторонними, возможно, недоверенными ресурсами.

При всем своем удобстве, **формат VDI сам по себе не может полноценно обеспечивать безопасность и легкость управления виртуальной инфраструктурой.** Так, в случае компрометации или заражения типовых образов как тонких клиентов, так и виртуальных машин каждый запускаемый образец операционной системы будет представлять угрозу для всей компании. А для того чтобы, например, избежать дублирования виртуальных машин и оптимизировать аудит управления конфигурациями, требуется надежная идентификация всех составляющих VDI.

Kaspersky Secure Remote Workspace – надежное решение для полноценного администрирования инфраструктуры тонких клиентов под управлением KasperskyOS. Оно предоставляет следующие возможности:

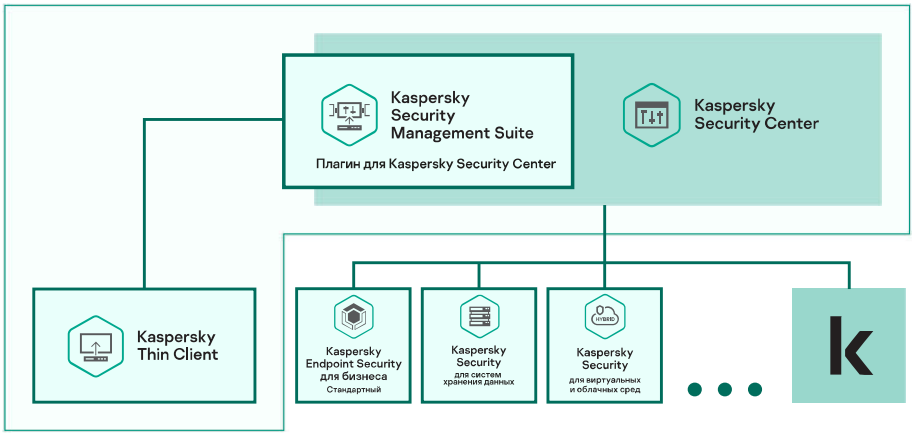
- Удобство и эффективность использования корпоративной инфраструктуры тонких клиентов
- Легкость, гибкость и прозрачность централизованного управления тонкими клиентами
- Снижение затрат на развертывание и обслуживание тонких клиентов
- Совместимость с различными системами виртуализации рабочих столов (Microsoft, Скала)

Решение состоит из трех дополняющих друг друга компонентов.

Kaspersky Thin Client на основе безопасной операционной системы KasperskyOS – продукт, который делает работу с тонкими клиентами комфортной и предсказуемой. На данный момент Kaspersky Thin Client работает на аппаратном тонком клиенте Depo Sky 270.

Продукт **Kaspersky Security Center** – основной инфраструктурный элемент централизованного управления тонкими клиентами. Разработанный для него плагин **Kaspersky Security Management Suite** предоставляет Kaspersky Security Center все необходимые инструменты для настройки и администрирования инфраструктуры тонких клиентов под управлением Kaspersky Thin Client.

Решение Kaspersky Secure Remote Workspace органично встраивается в инфраструктуру используемых продуктов «Лаборатории Касперского»



Продукты «Лаборатории Касперского»

Kaspersky Thin Client

Kaspersky Thin Client

Защита тонких клиентов для безопасной виртуальной инфраструктуры

Продукт **Kaspersky Thin Client** на основе KasperskyOS превращает тонкие клиенты в надежный и легко управляемый элемент корпоративной VDI.

Возможности и преимущества

- Поддержка двухфакторной аутентификации в гостевых операционных системах
- Контроль подключаемых устройств
- Удобный графический интерфейс тонких клиентов
- Централизованное автоматизированное обновление образа ос на тонких клиентах
- Управление сертификатами безопасности

Интеграция с технологическими партнерами

Depo Sky 270	Depo Sky 270 – базовая модель поддерживаемого тонкого клиента
RDP и Скала-Р BPM	Подключение к виртуальным рабочим столам по протоколу Microsoft RDP и к виртуальным машинам в системе виртуализации Скала-Р BPM
РУТОКЕН, SafeNet, JaCarta	Работа с самыми распространенными носителями ключевой информации. Проброс USB-устройств (mass storage, tokens, smart cards)

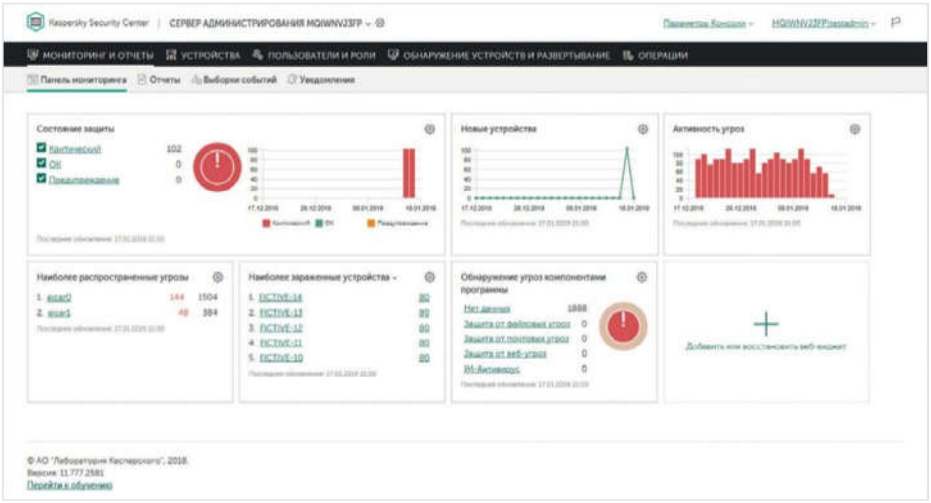
Kaspersky Security Center

Kaspersky Security Center

Централизованное управление и мониторинг тонких клиентов

Продукт **Kaspersky Security Center** в составе решения Kaspersky Secure Remote Workspace — удобная платформа для централизованного администрирования инфраструктуры тонких клиентов на базе Kaspersky Thin Client.

В его составе есть все инструменты и технологии, необходимые для легкого перехода компании на работу с тонкими клиентами, а также для интеграции с другими продуктами «Лаборатории Касперского».



Интерфейс Kaspersky Security Center

Возможности и преимущества

- Мониторинг, конфигурирование и доставка обновлений для тонких клиентов из единого центра
- Автоматическая регистрация и настройка тонких клиентов при подключении к инфраструктуре Kaspersky Secure Remote Workspace
- Централизованное обновление образа на тонком клиенте
- Управление настройками тонкого клиента из Kaspersky Security Center
- Централизованный сбор системных событий с тонких клиентов для аудита и исправления неполадок

Доступ на основе ролей	Каждый администратор может обращаться только к тем инструментам и данным, которые имеют отношение к его служебным обязанностям
Простое масштабирование	Масштабирование без изменения первоначальной настройки: управление до 100 000 узлов с помощью Kaspersky Security Center
Расширяемая архитектура	Управление тонкими клиентами происходит из единой консоли для разных решений «Лаборатории Касперского». Удобное подключение дополнительных решений
Гибкая система отчетности	Настраиваемые отчеты с динамической фильтрацией и сортировкой по любому полю

Kaspersky Security Management Suite

Kaspersky Security Management Suite (плагин)

Инструменты **Kaspersky Security Management Suite** позволяют Kaspersky Security Center управлять Kaspersky Thin Client, обеспечивая полноценное функционирование всего решения Kaspersky Secure Remote Workspace.

Спецификация поддерживаемого аппаратного обеспечения

Depo Sky 270	
Операционная система	KasperskyOS
Процессор	Intel® Celeron® J4005 Processor (4M Cache, up to 2.70 GHz)
RAM	Поддержка памяти DDR4 2400 (2 × SO-DIMM). Максимальный объем памяти 8 ГБ
Жесткий диск	Один встроенный контроллер Serial ATA со скоростью передачи до 6 Гбит/с
Видео и аудио	Интегрированное Intel® UHD Graphics 600. Интегрированный двухканальный звук Realtek® ALC269
Сетевая карта	· Интегрированный гигабитный сетевой контроллер 10/100/1000 Мбит/с · Wi-FI 802.11b/g/n
I/O порты	· Разъемы VGA / HDMI / DP для подключения трех независимых мониторов · Считыватель флеш-карт на лицевой панели (только Win10IoT) · 2 последовательных RS232-порта (1 × 0V/5V/12V, 1 × RS232/RS422/RS485) · 4 порта USB 2.0 на задней панели · 2 порта USB 3.0 на передней панели · Разъем RJ-45 для подключения к локальной сети Ethernet · Разъемы звуковой карты на лицевой панели (Front Speaker/Microphone) · Разъем для подключения Wi-Fi-антенны · Заглушка для подключения второй Wi-Fi антенны · 1 слот M.2 Type M (2280) с поддержкой NVMe и режимов PCIe 3.0 x4, SATA 6 Гбит/с · 1 слот M.2 Type E (2230) с предустановленным Wi-FI-модулем IEEE 802.11 b/g/n
Корпус	· Исполнение: Ultra Slim Form Factor · Размеры корпуса: 165 × 45 × 200 мм (Ш × В × Г) · Размеры коробки: 250 ×137 × 255 мм (Ш × В × Г)
Особенности	· Возможность горизонтальной установки, а также крепления VESA · Внешний безвентиляторный блок питания мощностью 40 Вт · Возможна опциональная установка дополнительной антенны WLAN · В модели отсутствуют вентиляторы, полностью пассивное охлаждение · Kensington Lock · Кронштейн VESA 75/100 мм – для крепления на задней части монитора или на стену

Преимущества Kaspersky Secure Remote Workspace

Продукты в составе Kaspersky Secure Remote Workspace делают простым и безболезненным переход с тяжеловесной, уязвимой и сложной в управлении инфраструктуры локальных рабочих мест на гораздо более подвижную, защищенную и удобную.

С помощью нашего решения вы сможете уверенно пользоваться всеми преимуществами тонких клиентов:

- Одновременное изменение конфигураций на всех терминалах корпоративной VDI
- Быстрое восстановление после системных сбоев
- Экономия ресурсов – долгий жизненный цикл тонких клиентов и простота их замены
- Удобство выполнения однотипных задач администраторов
- Уход от хранения информации на конечных устройствах

Конечно, это далеко не все, чем может быть полезна инфраструктура виртуальных рабочих столов. Какими бы ни были цели компании, внедряющей VDI, решение Kaspersky Secure Remote Workspace поможет легко освоить этот формат работы и получить от него максимум возможностей для успешного ведения бизнеса.

KasperskyOS®

Kaspersky Secure Remote Workspace

Подробнее на os.kaspersky.ru

www.kaspersky.ru