

Kaspersky Secure Remote Workspace



Кибериммунная,
управляемая и
функциональная
инфраструктура
тонких клиентов

Инфраструктура виртуальных рабочих столов (**Virtual Desktop Infrastructure**, или VDI) подразумевает, что сотрудники получают свои рабочие инструменты, виртуальные ПК, в виде набора программ и данных на удаленном сервере. Подключение к серверу происходит при помощи специальных терминалов – тонких клиентов (ТК). У этой концепции есть множество преимуществ перед традиционными рабочими местами:

- автоматизация процесса создания рабочих мест;
- уход от хранения и обработки данных на устройствах сотрудников;
- быстрое восстановление данных после инцидентов;
- управление удаленными рабочими местами из одной точки;
- пониженный риск атак удаленных рабочих мест.

Тонкие клиенты обладают своими преимуществами перед ПК и ноутбуками:

- отсутствие движущихся частей (вентиляторов и HDD) положительно сказывается на сроке эксплуатации (7-10 лет);
- небольшие габариты и вес, эргономичность и простота обслуживания и эксплуатации;
- низкое энергопотребление и тепловыделение;
- выгодная цена и стоимость владения по сравнению с классическими десктопами и ноутбуками.

В полной мере достоинства тонких клиентов раскрываются при наличии централизованной системы управления, позволяющей упростить процессы настройки, администрирования и поддержки. Также необходимо обеспечить безопасность VDI. Оконечные устройства в составе инфраструктуры могут стать объектом для разного типа кибератак, таких как: перехват нажатий клавиш клавиатуры, заражение с неконтролируемых съемных носителей или использование уязвимостей вовремя не обновленной версии ПО.

Решение **Kaspersky Secure Remote Workspace** позволяет предотвратить потенциальные угрозы. В его состав входят кибериммунные тонкие клиенты на базе безопасной операционной системы KasperskyOS. Такой подход избавляет от необходимости использовать антивирусные средства защиты. Также в состав решения входит инструмент централизованного управления, что упрощает администрирование инфраструктуры ТК.

Kaspersky Secure Remote Workspace – решение для построения управляемой и функциональной инфраструктуры тонких клиентов на базе кибериммунной операционной системы KasperskyOS для защищенного подключения к VDI.

Состав решения



Kaspersky Secure Remote Workspace

Kaspersky Thin Client



Программный продукт на базе операционной системы KasperskyOS, устанавливаемый на аппаратную платформу

Бессрочная лицензия на мажорную версию

Kaspersky Security Center



Единая консоль управления тонкими клиентами и другими продуктами «Лаборатории Касперского»

Бесплатная установка (в случае отсутствия консоли в инфраструктуре)

Kaspersky Security Management Suite



Модуль расширения для организации централизованного администрирования тонких клиентов через единую консоль управления KSC

Лицензия на подключение к KSC. Подписочная модель по количеству устройств на 1, 2 или 3 года

Преимущества Kaspersky Secure Remote Workspace

Защита на уровне ОС

Тонкие клиенты на базе KasperskyOS обладают кибериммунитетом — «врожденной» защищенностью на уровне архитектуры ОС. Это означает, что подавляющее большинство типов кибератак на устройство не смогут повлиять на безопасность инфраструктуры удаленных рабочих столов.

Снижение затрат

Затраты на развертывание и обслуживание инфраструктуры **Kaspersky Thin Client** могут быть меньше, чем при использовании других решений. Работа со знакомым заказчику продуктом **Kaspersky Security Center** не требует обучения и переустановки.

Поддержка популярных носителей ключевой информации и внешних накопителей

Токены PУТОКЕН, SafeNet, JaCarta и проброс USB-накопителей.

Централизованное управление

Централизованный мониторинг и управление всеми событиями инфраструктуры тонких клиентов осуществляются с помощью консоли **Kaspersky Security Center**. Поддерживается управление до 100 000 узлов. При подключении к инфраструктуре новых устройств регистрация и настройка тонких клиентов происходит автоматически.

Комфортная миграция и обновление

Контроль безопасности осуществляется через привычную администратору консоль управления **Kaspersky Security Center**, что упрощает переход с традиционных рабочих станций на тонкие клиенты. В случае обновления состава ПО в корпоративном образе **Kaspersky Thin Client** производится централизованное автоматизированное обновление на всех тонких клиентах.

Соответствие нормативам

Продукты в составе решения соответствуют приказу Минкомсвязи России о преимущественном использовании отечественного ПО*.

* Компоненты решения Kaspersky Secure Remote Workspace внесены в единый реестр российских программ для ЭВМ и баз данных: Kaspersky Thin Client — под номером 244652 от 20.08.2021 Kaspersky Security Management Suite — под номером 244657 от 16.08.2021



Kaspersky Security Center: централизованное управление и мониторинг

Контроль и обзорность всей инфраструктуры

Удаленное централизованное администрирование с помощью консоли **Kaspersky Security Center** решает проблемы управляемости и мониторинга инфраструктуры тонких клиентов.

Гибкие отчеты и уведомления

Настраиваемые отчеты с фильтрацией и сортировкой по любому полю. Оповещения об инцидентах через различные каналы, удобные администратору (SMS, email, push и т.д.)

Легкая миграция

Не требуется получать компетенции по новому продукту — при использовании KSC, миграция на тонкие клиенты не вызывает сложностей

Kaspersky Thin Client под контролем ИБ

Тонкие клиенты не пропадают из фокуса внимания ИБ-специалистов

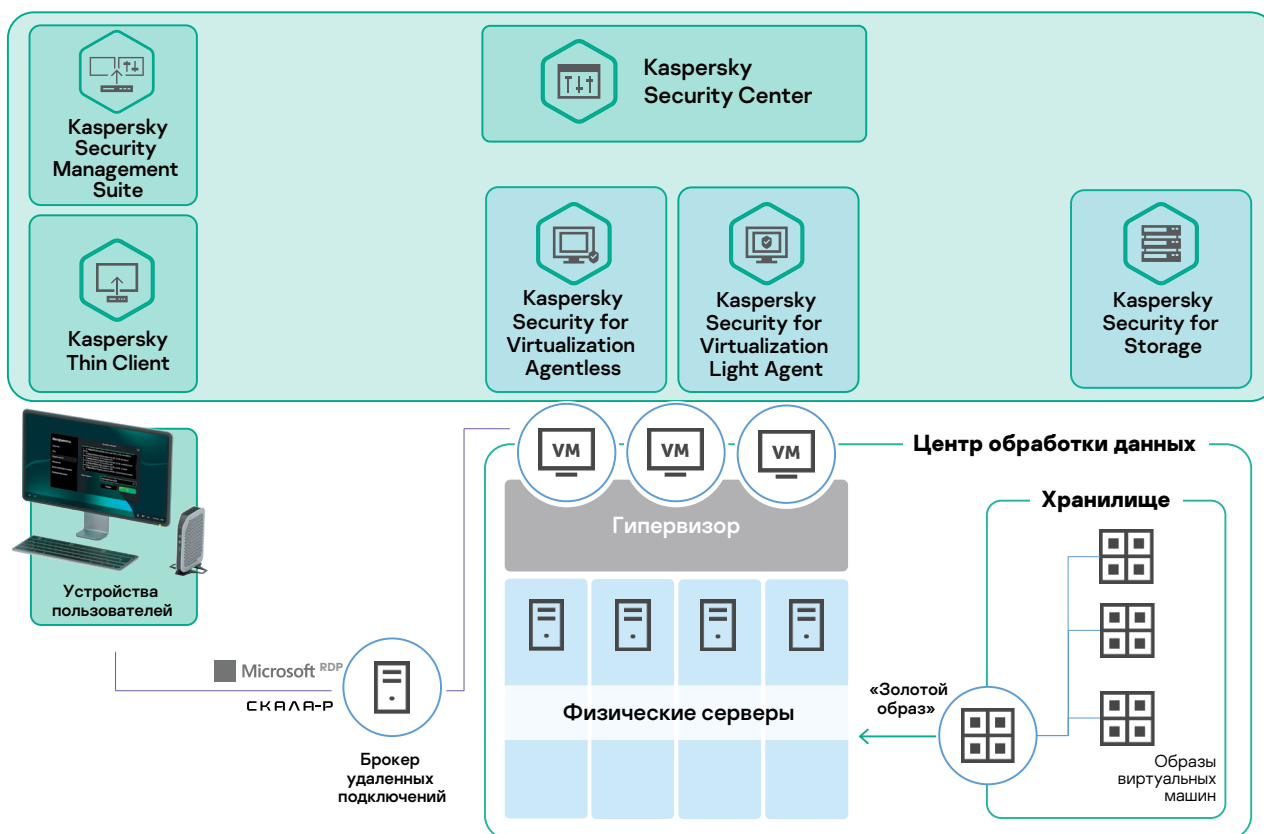


Kaspersky Thin Client: технические характеристики

Аппаратная платформа	TONK TN 1200
Операционная система	KasperskyOS
Процессор	Intel® Celeron® 4125 Gemini Lake Refresh Quad-Core 2.0 ГГц (4М L2 кэш, до 2,7 ГГц)
Память	4 ГБ DDR4 (максимальный объем 8 ГБ, DDR4/LPDDR4)
Флеш-накопитель	64 ГБ, M.2 (2242) SSD
Видео	Intel® UHD Graphics 600, до 1920 x 1080
Сеть	1 x порт LAN (RJ-45) 10/100/1000 для подключения к локальной сети
Интерфейсы периферии	<ul style="list-style-type: none">• 1 x DP• 1 x HDMI• 4 x USB 2.0• 2 x USB 3.0
Габаритные размеры и вес	<ul style="list-style-type: none">• Размер устройства: 131 мм x 31,5 мм x 167 мм• Вес нетто: 0,55 кг• Упаковка: 488 мм x 256 мм x 108 мм
Особенности	<ul style="list-style-type: none">• Входное напряжение постоянного тока: от универсального (110-230 В) адаптера переменного тока 12 В 3 А• Потребляемая мощность: не более 30 Вт• VESA-mount, горизонтальная или вертикальная установка• Kensington Lock• Безвентиляторное охлаждение путем естественной конвекции воздуха

Роль Kaspersky Secure Remote Workspace в комплексной защите VDI продуктами «Лаборатории Касперского»

Kaspersky Secure Remote Workspace является частью комплексного проекта по организации VDI. Решение работает совместно с классическими антивирусными средствами защиты виртуальных и облачных сред, а также систем хранения данных. Все эти продукты также управляются с помощью **Kaspersky Security Center**.



KasperskyOS: принципиально новый подход к кибербезопасности IT-продуктов

KasperskyOS – собственная операционная система «Лаборатории Касперского», платформа для разработки кибериммунных IT-продуктов. Ее исходная безопасность заложена в архитектуре и философии: запускаться и работать может только то, что напрямую разрешено администраторами системы и разработчиками приложений. Уже на этапе проектирования IT-продукта на базе KasperskyOS задаются политики безопасности, которые описывают каждое разрешенное действие. Любое действие, не разрешенное политикой безопасности напрямую, будет заблокировано еще до выполнения. Продукты на базе KasperskyOS востребованы в отраслях с повышенными требованиями к кибербезопасности, надежности и предсказуемости работы IT-систем – от промышленного интернета вещей до транспорта, умных городов и промышленности.

os.kaspersky.ru
www.kaspersky.ru

© 2022 АО «Лаборатория Касперского»
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью их
правообладателей.

 **KasperskyOS**