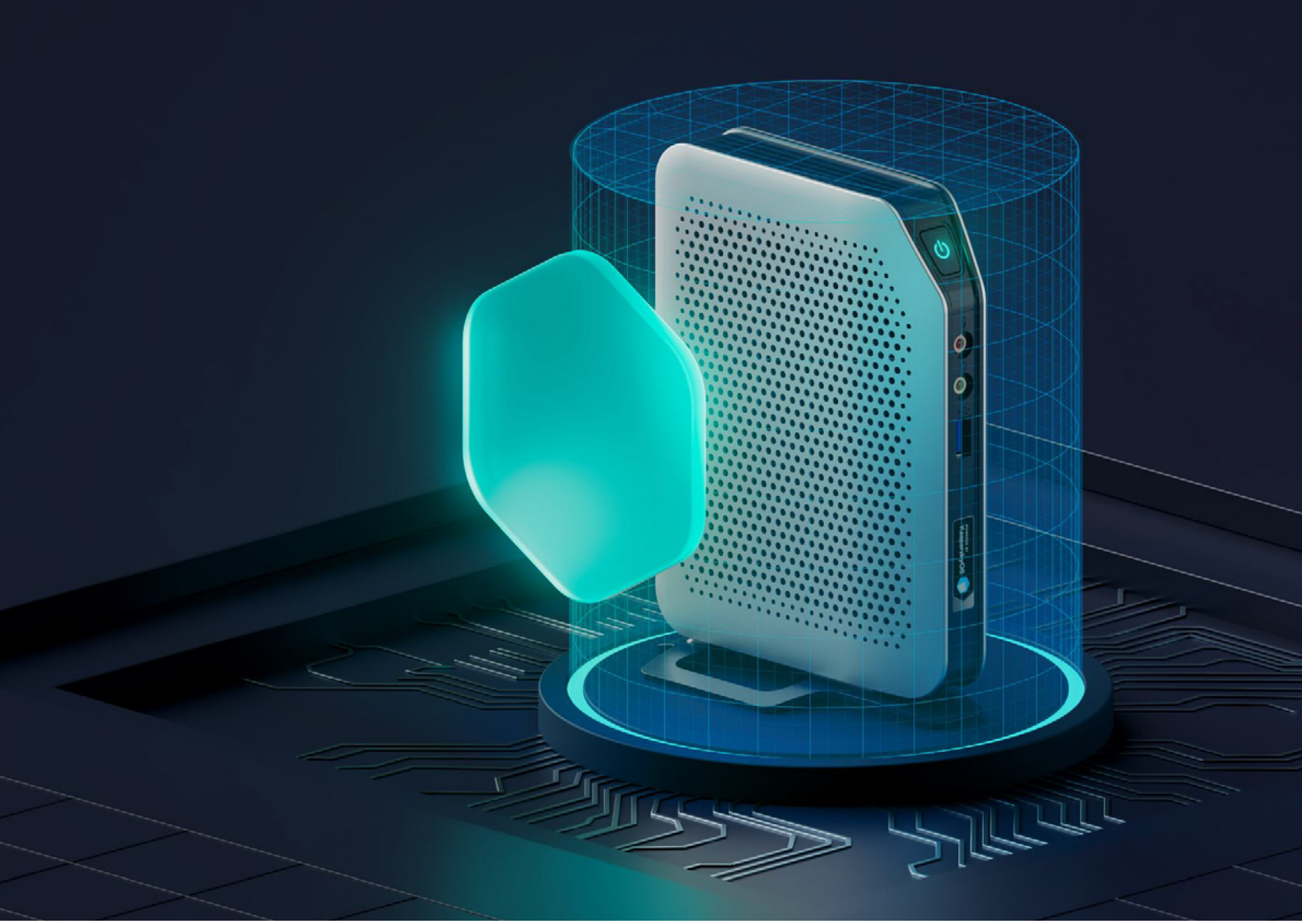


Kaspersky
Thin Client

Кибериммунная,
управляемая
и функциональная
инфраструктура
тонких клиентов

Kaspersky Thin Client

kasperskyOS

kaspersky
cyber
immunity

Создание рабочих мест на базе тонких клиентов — преимущества и вызовы

Современный подход к организации удаленных рабочих мест подразумевает, что на рабочем месте сотрудника находится только монитор, клавиатура и тонкий клиент. Через тонкий клиент пользователь подключается к развернутой на сервере операционной системе, в которой работают только необходимые для бизнеса приложения. Такая концепция имеет 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;
- сниженный риск атак удаленных рабочих мест.

Тонкий клиент может подключаться к:

- терминальному серверу;
- удаленной виртуальной машине;
- VDI инфраструктуре;
- DaaS;
- удаленному физическому ПК/Серверу;
- серверу приложений.

Рабочая станция пользователя — одна из самых распространенных точек проникновения в корпоративную сеть, где хранятся чувствительные данные. Уязвимыми могут быть — наборы сетевых протоколов операционной системы (ОС) тонких клиентов, устройства, подключенные к тонким клиентам, приложения сторонних вендоров и серверы управления тонкими клиентами. Кроме того, имеются бреши в коде протоколов доставки удаленной среды.

Так, по данным ICS CERT «Лаборатории Касперского», в RDP-клиентах (протокол подключения пользователя к удаленному рабочему столу) rdesktop и FreeRDP, которые используются в Windows, Linux и macOS, есть **как минимум** 25 известных уязвимостей.

Возможные угрозы для тонких клиентов

Подмена RDP-сервера

Существует много инструментов (пример) для выполнения атаки Man-in-the-middle на RDP/VNC. Все атаки пользуются чем-то из следующего списка:

- на стороне клиента используется протокол без шифрования (некоторые инсталляции VNC);
- на стороне клиента не проверяется серверный сертификат;
- между клиентом и сервером используется слабое шифрование.

Уязвимости в коде библиотек RDP/VNC

При подключении к вредоносному серверу происходит удаленное исполнение произвольного кода, в контексте пользователя из-под которого запущен RDP/VNC-клиент. Это может использоваться для сбора учетных записей от других систем и продвижения атаки.

Атака на других пользователей тонкого клиента

При совместном использовании устройства, легитимный пользователь может проэксплуатировать уязвимость, повысить привилегии и получить доступ к учетным записям других пользователей.

Атака на сервер управления

При помощи эксплуатации уязвимости сервера управления или при его подмене, злоумышленники могут поменять конфигурацию или обновить прошивку тонких клиентов, которые к нему подключаются. Далее со взломанных устройств можно собрать учетные записи от других систем и использовать их для дальнейшего продвижения атаки

Обязательное условие: управляемость тонких клиентов

Парк оборудования для подключения к инфраструктуре удаленных рабочих мест зачастую бывает разнородный. В одной организации могут использоваться ПК, ноутбуки и тонкие клиенты. С точки зрения затрат на администрирование наиболее оптимально использовать тонкие клиенты, поскольку замена вышедшего из строя устройства или установка нового легко может быть выполнена персоналом, вообще не имеющим специальной подготовки.

Кроме того, тонкие клиенты обладают 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.

При этом полноценное управление большим парком тонких клиентов, их настройка, обновление или аудит — трудоемкий и рискованный процесс. В полной мере достоинства тонких клиентов раскрываются при наличии централизованной системы управления, позволяющей упростить процессы администрирования и поддержки.

Кибериммунный подход к защите и управляемости инфраструктуры тонких клиентов

Потенциальные угрозы можно предотвратить и защитить инфраструктуру рабочих мест благодаря кибериммунному подходу, который применен в Kaspersky Thin Client. Это специальная версия операционной системы KasperskyOS для тонких клиентов. Исходно безопасная (Secure by Design) операционная система избавляет от необходимости использовать наложенные средства защиты. Входящая в состав решения единая консоль Kaspersky Security Center решает проблемы управляемости и мониторинга инфраструктуры тонких клиентов

Состав решения

Кибериммунный тонкий клиент

Kaspersky Thin Client

Операционная система для тонких клиентов на базе микроядерной KasperskyOS

TONK TN1200

Единая консоль для централизованного управления

Kaspersky Security Center

Единая консоль для централизованного управления продуктами «Лаборатории Касперского»

Kaspersky Security Management Suite

Расширение для Kaspersky Security Center для управления тонкими клиентами

Программное обеспечение внесено в единый реестр российских программ для ЭВМ и баз данных:

КТС №11965 от 29.10.2021

KSMS №11918 от 29.10.2021

Аппаратная платформа тонкого клиента — TONK TN1200 — внесена в реестр Минпромторга РФ на основании заключения № 40608/11. Номер реестровой записи — 1018\1\2023.

Где применяется Kaspersky Thin Client

Решение Kaspersky Thin Client подходит для многих сфер, где используется большое количество рабочих мест со схожими задачами и типовым набором приложений. Для различных вертикалей возможны следующие сценарии применения.

Финансы и страхование

- Локальные офисы финансовых организаций
- Колл-центры
- Служба поддержки пользователей

Энергетика и производство

- Доступ к SCADA/ АСУ ТП системам
- Рабочие станции инженеров

Государственные организации

- Доступ к системам электронного документооборота
- Рабочие места сотрудников МФЦ

Образовательные учреждения

- Учебные классы
- Лабораторные полигоны
- Олимпиады

Здравоохранение

- Приемные отделения
- Информационные табло
- Точки подключения рабочих мест мед. специалистов

Ритейл и складская логистика

- Рабочее место кассира
- Рабочее место оператора колл-центра
- Доступ к системам управления складом (WMS, СУС)

Кибериммунитет

Подход к построению систем с «врожденной» защитой от кибератак.

Кибериммунитет обеспечивается чётким определением целей безопасности, разделением IT-системы на изолированные части, контролем взаимодействий между ними и минимизацией потенциальной поверхности атаки. Критические активы кибериммунной системы остаются устойчивыми даже к неизвестным угрозам без дополнительных средств защиты.

KasperskyOS

Собственная, созданная с нуля, микроядерная операционная система «Лаборатории Касперского», поддерживающая разработку кибериммунных продуктов. В ее основе — лучшие практики разработки специализированных исходно безопасных систем и многолетняя экспертиза «Лаборатории Касперского» в области информационной безопасности.

Кибериммунные тонкие клиенты — безопасность при подключении к удаленным рабочим столам

Kaspersky Thin Client обладает свойством кибериммунности, что означает выполнение следующих требований:

- целостность данных, полученных от пользователя, от сервера централизованного управления Kaspersky Security Center и от серверов брокеров соединения;
- безопасное обновление тонких клиентов;
- конфиденциальность и целостность данных, передаваемых между

Kaspersky Thin Client, удаленным рабочим столом, сервером **Kaspersky Security Center**, сервером логирования и брокером соединения.

Кибериммунные тонкие клиенты — это защищенная «последняя миля» построения надежной ИТ-инфраструктуры для работы с виртуальными рабочими столами.

Централизованное управление инфраструктурой тонких клиентов

Консоль **Kaspersky Security Center**, входящая в состав решения, позволяет управлять тонкими клиентами из единого центра, настраивать их, администрировать, доставлять обновления и собирать системные события. KSC активно используется другими продуктами «Лаборатории Касперского». Благодаря этому интеграция Kaspersky Thin Client в существующую экосистему защиты корпоративных IT-систем может стать максимально бесшовной и не потребует найма дополнительных специалистов.

Кибериммунитет на практике: Kaspersky Thin Client в сравнении с обычными тонкими клиентами

Преимущества кибериммунного подхода

Кибериммунный тонкий клиент не подвержен данной уязвимости, так как перед подключением по протоколу RDP обязательно установление TLS-соединения, в ходе которого происходит авторизация удаленного сервера. Установлением соединения занимается TLS Terminator – компонент с малой поверхностью атаки, который нельзя выключить, изменить или обойти, поскольку это гарантировано дизайном операционной системы.

1. Атака на протоколы RDP/VNC

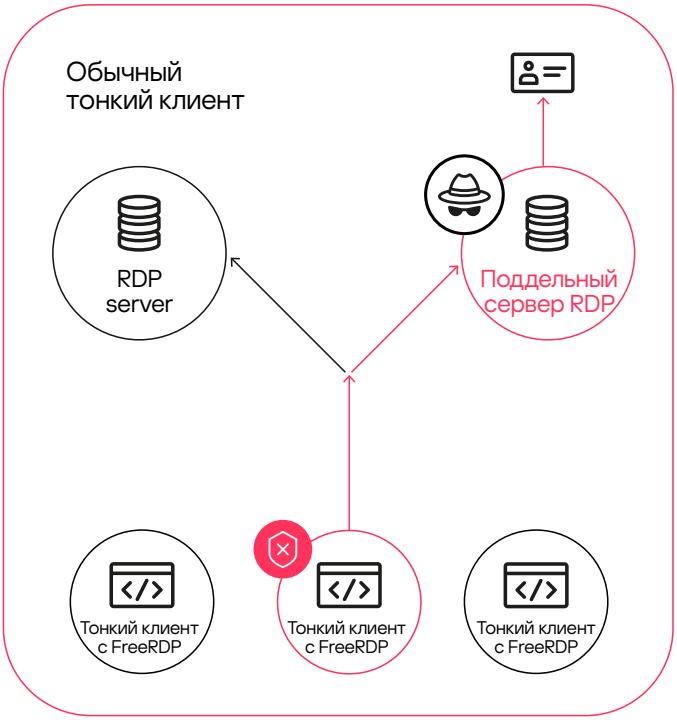
Злоумышленник получает доступ во внутреннюю сеть организации и проводит атаку типа Man-in-the-middle (например, при помощи ARP Spoofing).

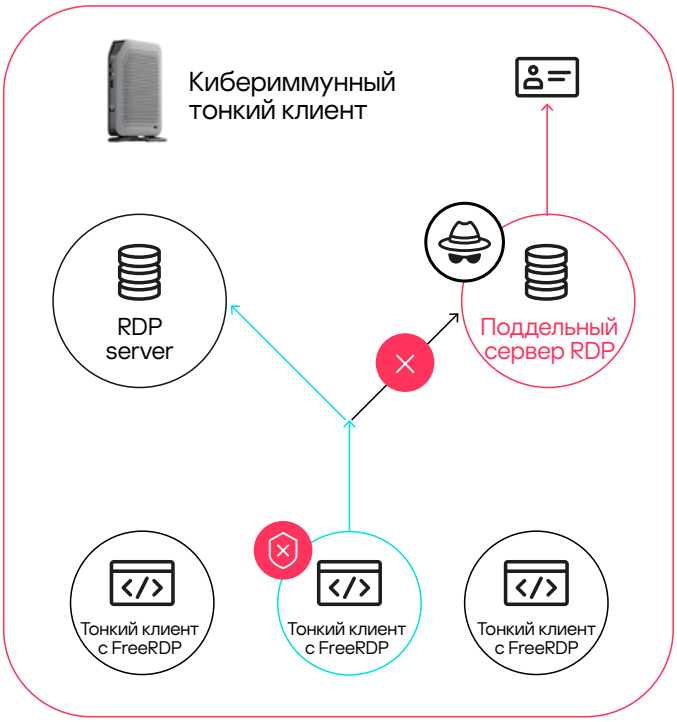
Жертва подключается к подменному RDP/VNC-серверу, и злоумышленник перехватывает учетные данные жертвы.

Далее злоумышленник может использовать эти данные для подключения к легитимному серверу для дальнейшего продвижения атаки (Lateral Movement).

CVE-2005-1794

Уязвимость в Microsoft Terminal Server, которая позволяет злоумышленнику успешно произвести Man-in-the-middle атаку.





Преимущества кибериммунного подхода

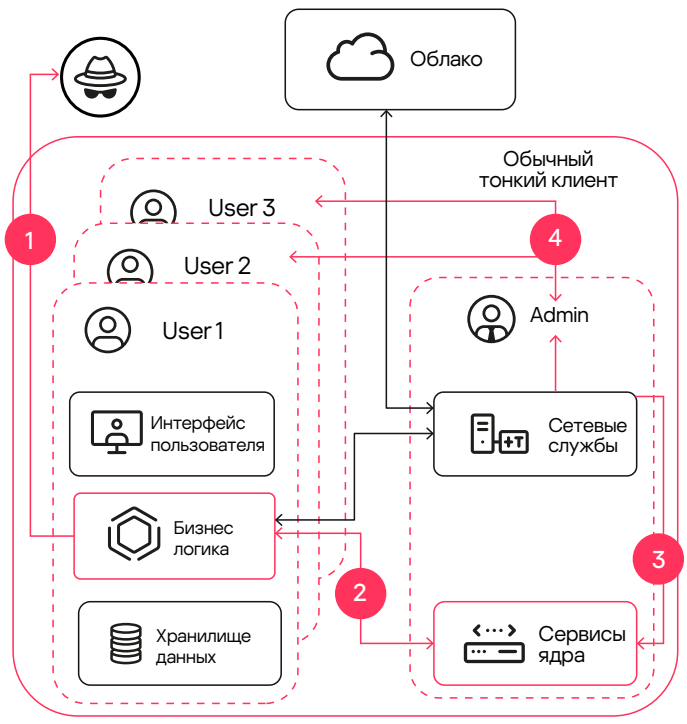
В кибериммунном тонком клиенте отсутствует понятие пользователей. Системные функции, отвечающие за администрирование, вынесены в отдельные, изолированные компоненты. Повышение привилегий в кибериммунном тонком клиенте в принципе невозможно даже в случае успешной атаки на один из компонентов.

2. Атака на других пользователей совместно используемого тонкого клиента

Легитимный пользователь тонкого клиента эксплуатирует уязвимость повышения привилегий, повышается до администратора/root и использует привилегированный доступ для кражи учетных записей других пользователей данного тонкого клиента.

CVE-2016-2246

Локальный пользователь может использовать виртуальную клавиатуру для повышения привилегий.



Преимущества кибериммунного подхода

Администрирование кибериммунного тонкого клиента осуществляется через сервер KSC. Подключение к нему происходит аналогично подключению к удаленному RDP-серверу — с обязательным использованием TLS-соединения. В случае, если злоумышленник развернет собственный сервер KSC, его сертификат будет отсутствовать в доверенном хранилище сертификатов тонкого клиента и подключение по TLS вызовет ошибку.

3. Атака на сервер управления тонкими клиентами

Злоумышленник получает доступ во внутреннюю сеть организации и проводит атаку типа Man-in-the-middle. Жертва подключается к подменному серверу управления и злоумышленник меняет конфигурацию устройства.

Цель атаки — закрепиться на компьютере жертвы для дальнейшего сбора информации и продвижения атаки.

Злоумышленник при помощи эксплуатации уязвимости в сервере управления меняет конфигурацию тонких клиентов или обновляет прошивку.

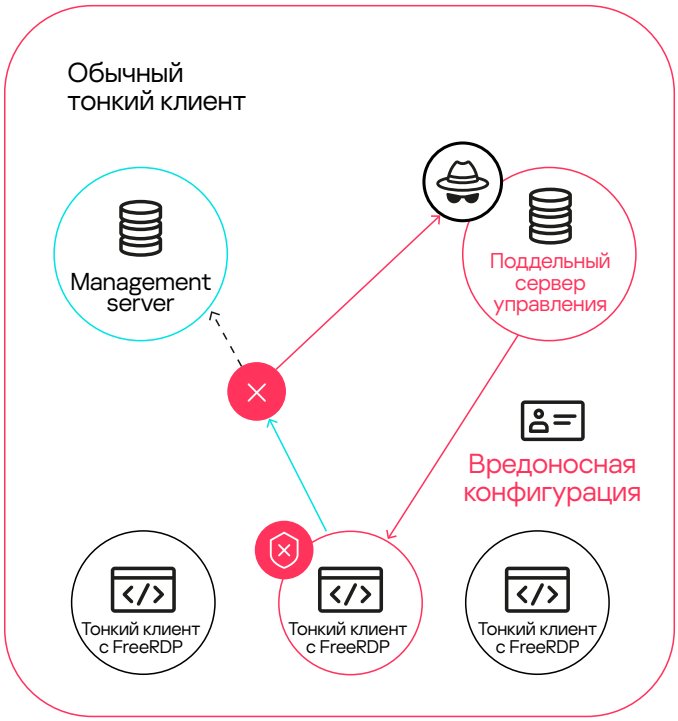
Далее он со всех модифицированных тонких клиентов учетные записи от других систем и использует их для дальнейшего продвижения атаки.

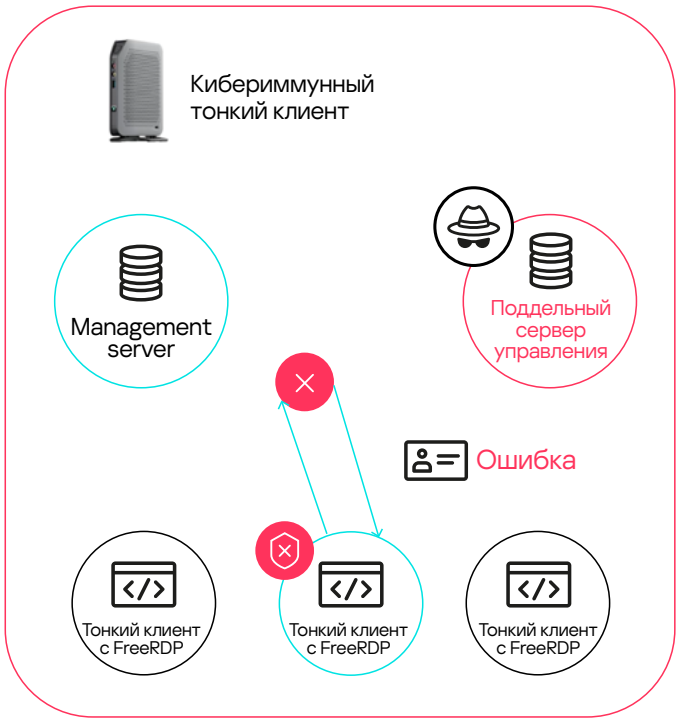
CVE-2021-21532

Данная уязвимость позволяет провести MITM-атаку между тонким клиентом под управлением ОС с монолитным ядром и сервером управления, и поменять конфигурацию устройства.

CVE-2020-29492

FTP-сервер, используемый для обновления прошивки устройств под управлением ОС с монолитным ядром, позволяет пользователю anonymous отредактировать ini-файл. Это может привести к исполнению произвольного кода как на самом тонком клиенте, так и на машине, к которой этот тонкий клиент подключается.





Роль Kaspersky Thin Client в комплексной защите инфраструктуры рабочих мест продуктами «Лаборатории Касперского»

Дополнительная информация

Узнайте больше о возможностях Kaspersky Thin Client и успешных проектах с его использованием и отправьте заявку на консультацию экспертов:

os.kaspersky.ru/solutions/kaspersky-thin-client

Мы предлагаем комплексный подход к кибербезопасности рабочих мест с помощью нескольких продуктов.

Организация киберимунного рабочего места

Kaspersky Thin Client на основе микроядерной KaspeskyOS обеспечивает защищенное и доверенное подключение к удаленным рабочим столам.

Защита виртуальных и облачных инфраструктур

Kaspersky Security для виртуальных и облачных инфраструктур — интегрированное решение для комплексной защиты виртуальных машин от различных типов информационных угроз, сетевых и мошеннических атак.

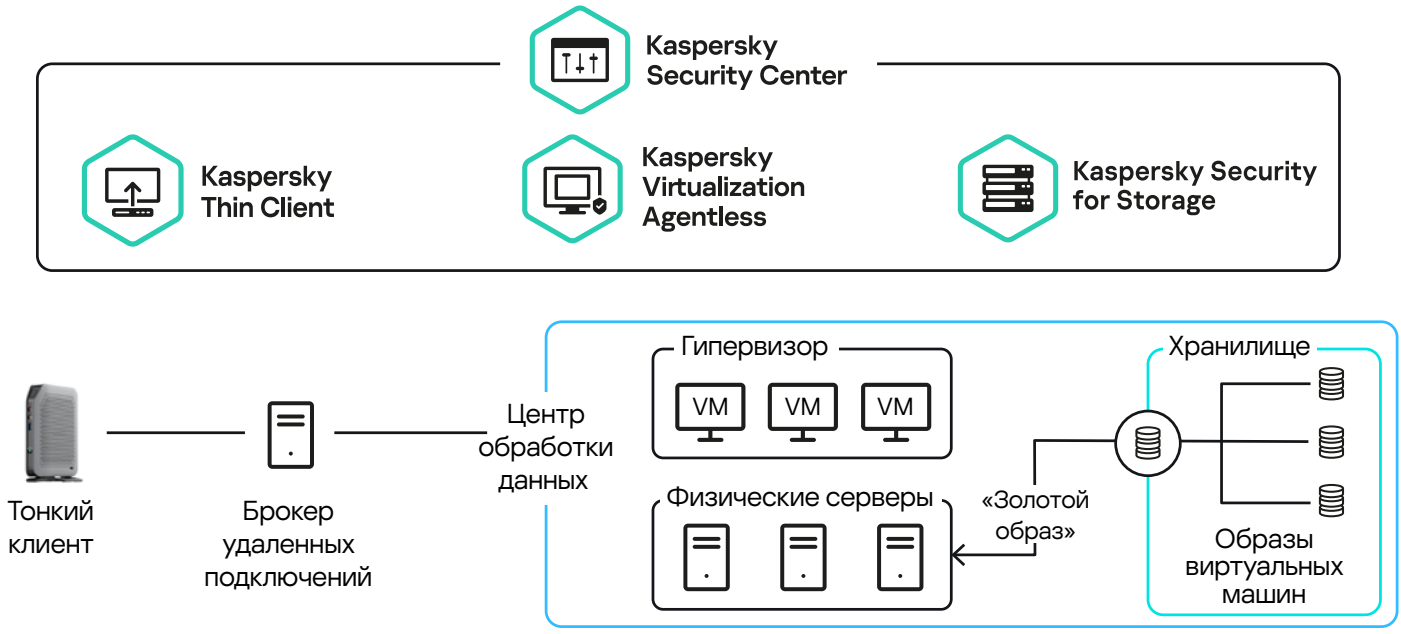
Защита удаленных рабочих мест

Kaspersky Endpoint Security обеспечивает комплексную защиту компьютера от различных типов угроз, сетевых и мошеннических атак.

Централизованное управление

Kaspersky Security Center – единая консоль для централизованного управления всеми продуктами «Лаборатории Касперского».

Все эти продукты также управляются с помощью **Kaspersky Security Center.**



kasperskyOS

kaspersky cyber immunity

os.kaspersky.ru
www.kaspersky.ru