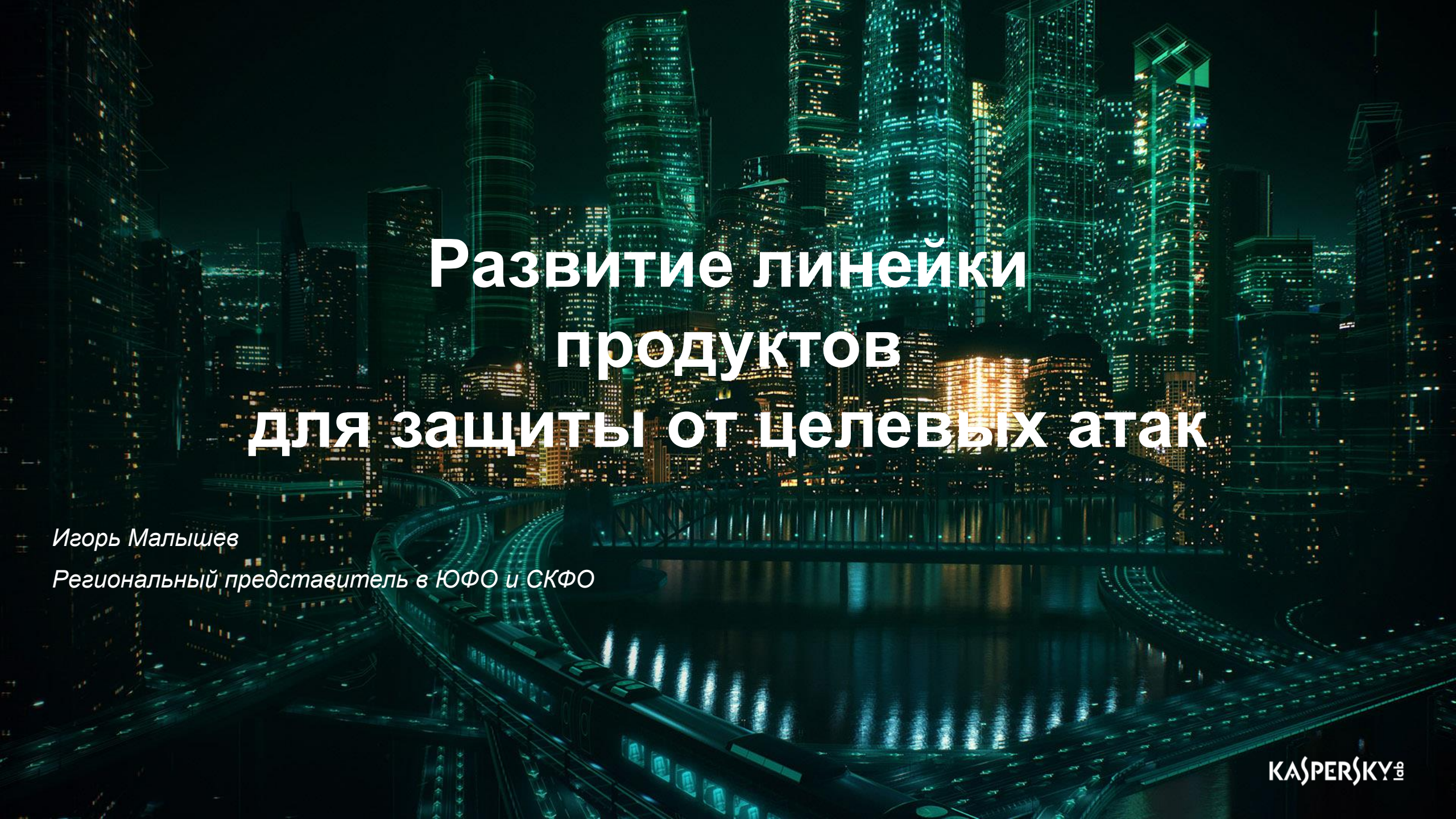


Развитие линейки продуктов для защиты от целевых атак

Игорь Малышев

Региональный представитель в ЮФО и СКФО

KASPERSKY lab

Kaspersky Sandbox

KASPERSKY lab

О чем будем говорить?

- Адресуемые проблемы заказчиков
- Классификация угроз и пути противодействия
- Обоснование преимуществ решения
- Обзор лицензирования решения
- Выводы

Адресуемые проблемы заказчиков

Нехватка специалистов ИБ

Автоматические средства блокировки не справляются со сложными угрозами (APT, zero-day, malware-less…)

Рост количества событий ИБ

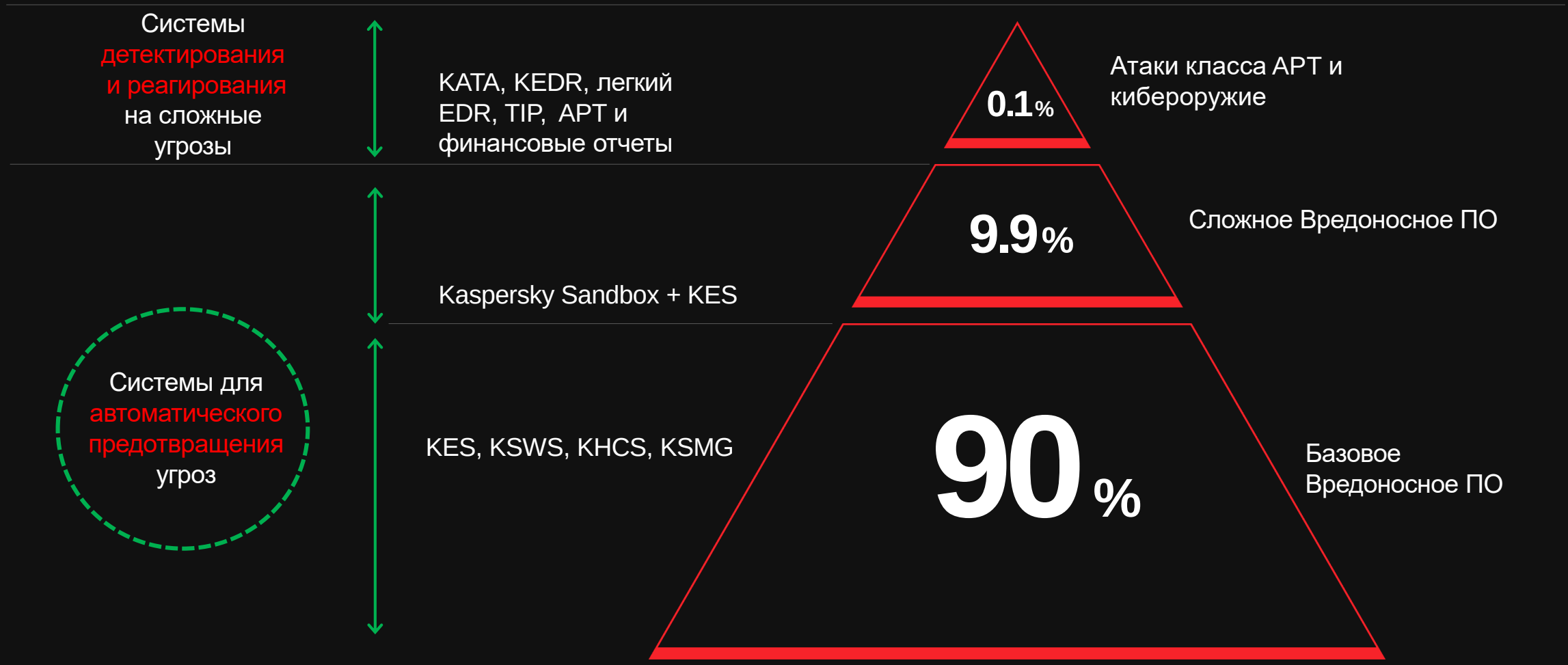
Между KES и KATA/KEDR пропасть, нам нужно промежуточное решение и дешевле

Нехватка бюджета на решения класса ANTI-APT и EDR

Как большой организации защитить маленький офис от сложных угроз?
Тяжелые решения не подходят. Нет ИБ-специалистов на местах, слабые интернет каналы, удаленность офисов…

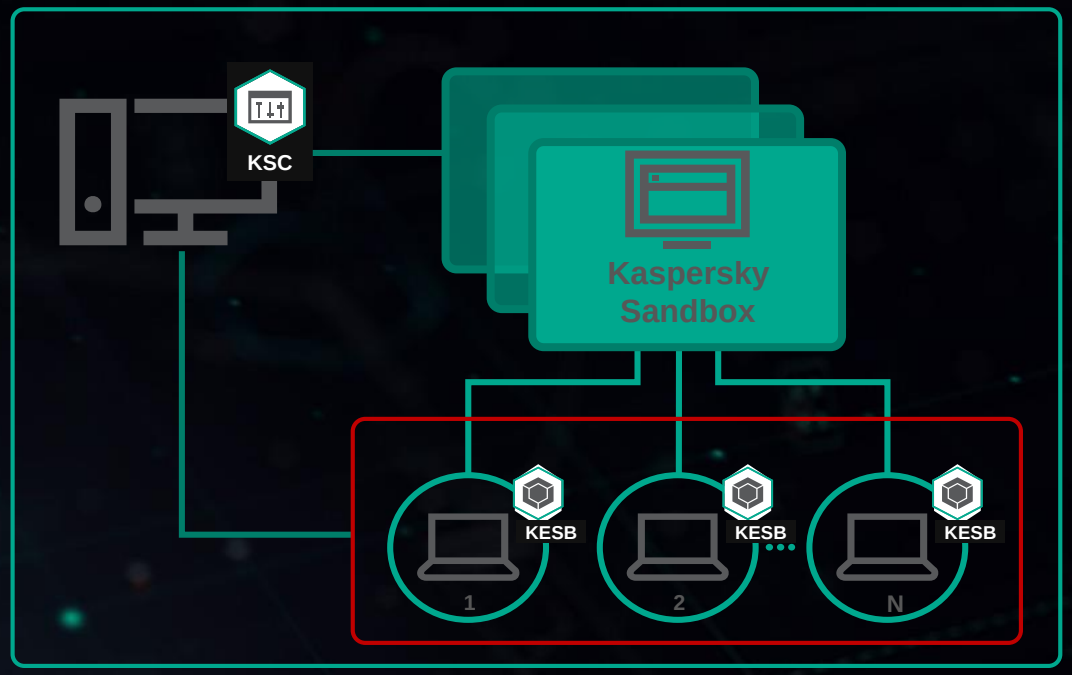
Возложение функций ИБ на IT департамент приводит к рискам возникновения серьезных инцидентов

Классификация угроз и пути противодействия



kaspersky

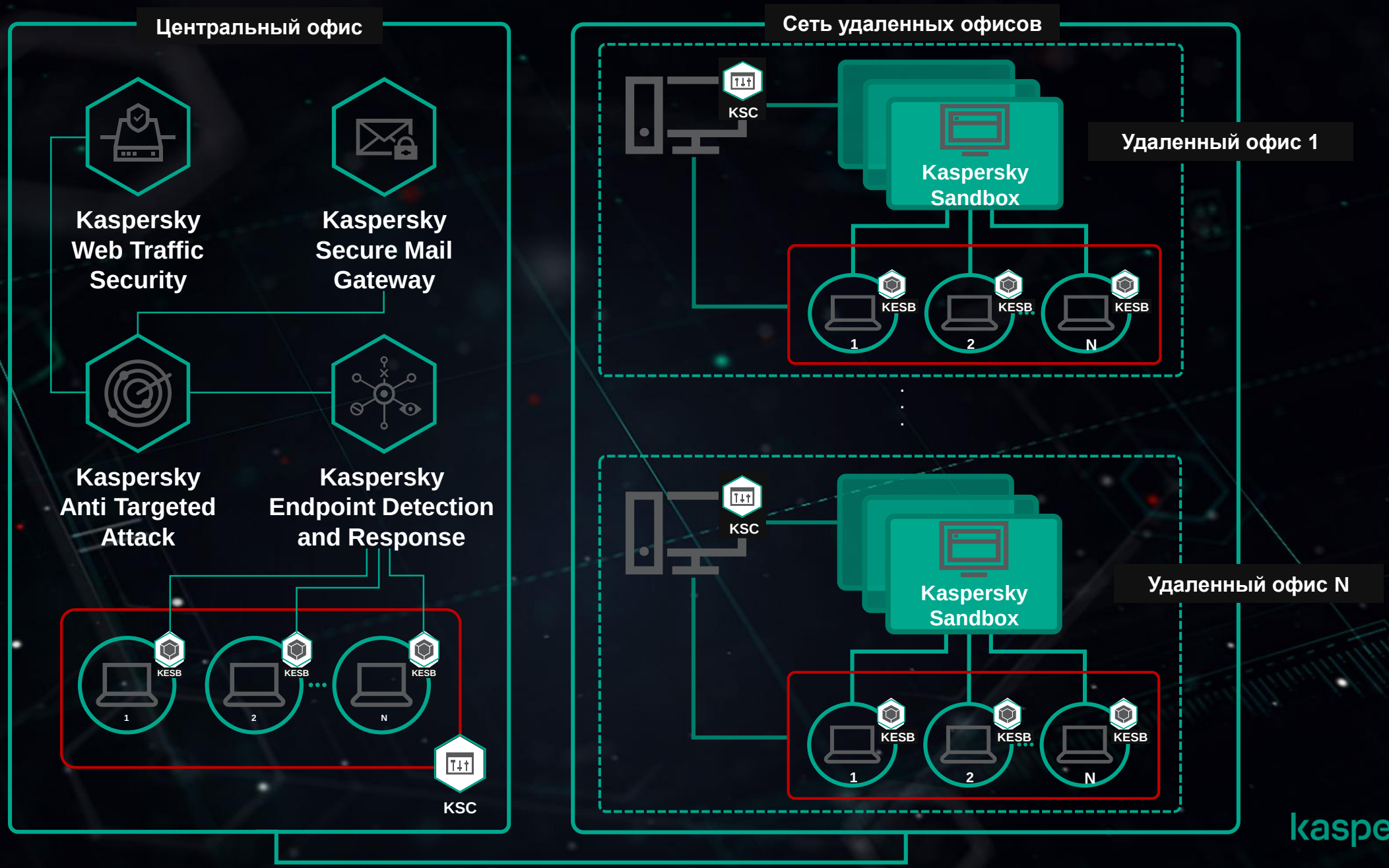
Обоснование преимуществ решения



- Расширение функциональности KES по выявлению и блокировке сложных угроз, таких как:
  - ранее неизвестное вредоносное ПО
  - новые вирусы-вымогатели и шифровальщики
  - эксплойты нулевого дня и др.
- Идеальное решение для организаций в которых функции ИБ возложены на IT департамент
- Автоматизированное реагирование на выявленные угрозы путем сканирования хостов сети и блокировки выявленных вредоносных объектов
- Возможности кластеризации и отказоустойчивости решения, как для средних, так и для крупных организаций
- Опция по виртуализации решения на основе Vmware ESXi
- Лицензии Microsoft включены в стоимость решения
- Экономия трудозатрат штатных ИБ-аналитиков для решения тех задач, которые действительно требуют их внимания
- Бюджетное решение для организаций, не имеющих возможности приобрести продукты класса KATA/KEDR
- Удобство в использовании для крупных организаций с территориально распределенной инфраструктурой без наличия ИБ-специалистов на местах

kaspersky

Преимущества для компаний с распределенной инфраструктурой



kaspersky

KES + Sandbox. Как это работает?

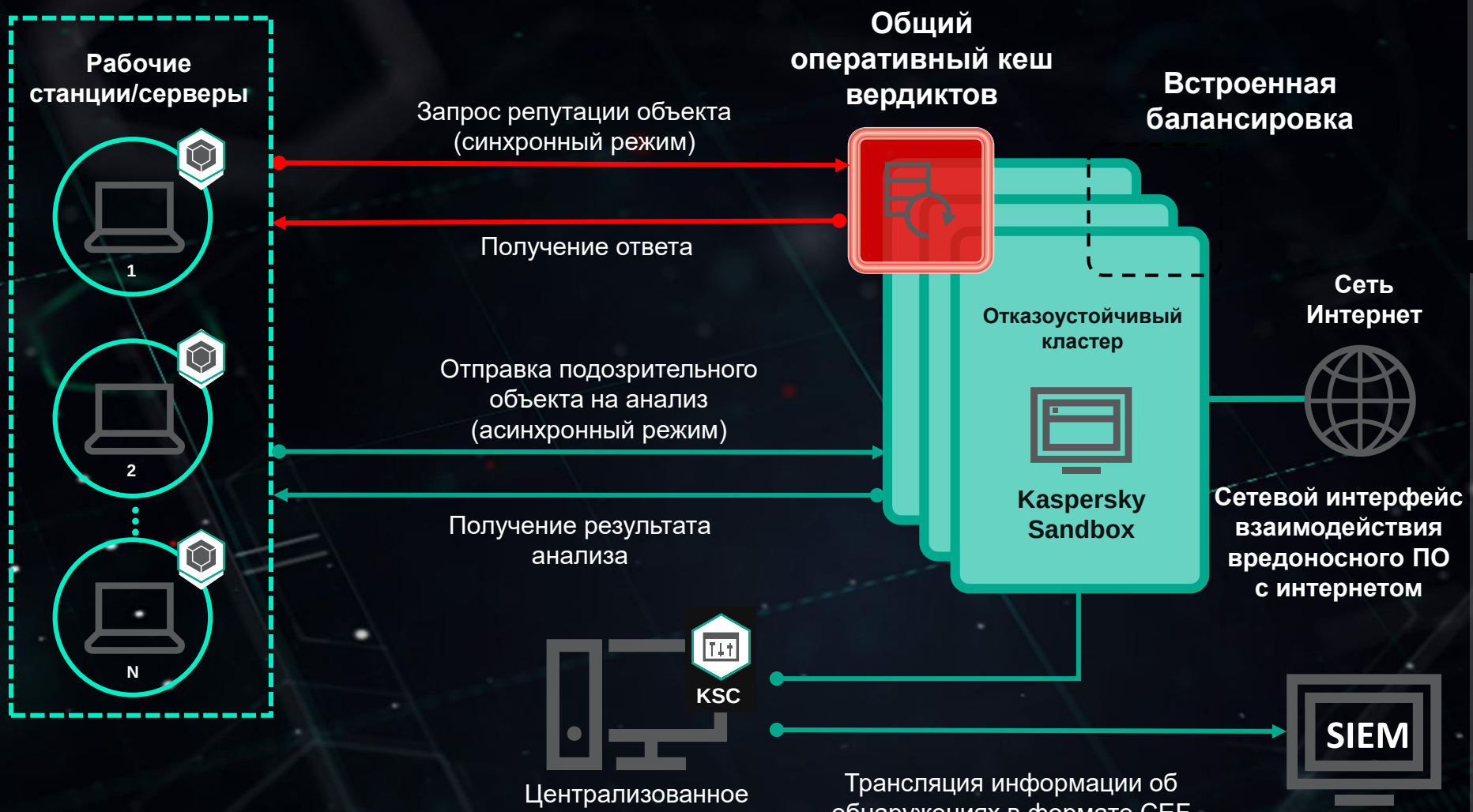
Основная ценность продукта - это создание дополнительного уровня защиты от продвинутых угроз без необходимости расширения штата сотрудников IS или наличия SOC

Основные характеристики:

- Поставка в виде Software appliance
- Управление и мониторинг в Kaspersky Security Center
- Автоматизированные сценарии обнаружения и реагирования с KES for Windows
- Отчетность о работе технологии в Kaspersky Security Center:
  - Информация об обнаружениях в SSB
  - Статистика работы технологии
  - Состояние технологии
- Поддержка кластерной конфигурации SSB серверов: масштабирование и отказоустойчивость

kaspersky

Простота и универсальность архитектуры Kaspersky Sandbox



Проверка объектов в 2 режимах позволяет:

- оперативно обрабатывать подозрительные файлы
- снизить нагрузку на серверы Kaspersky Sandbox
- повысить скорость и эффективность реагирования на угрозы.

Доступность открытого API позволяет:

- Провести интеграцию песочницы с другими продуктами ЛК, например Веб и Почтовыми шлюзами
- Системным интеграторам использовать продукт в составе комплексных решений
- HW и SW вендоры могут использовать Sandbox SDK для интеграции функционала решения в своих продуктах

kaspersky

Обзор лицензирования решения

Продукт Kaspersky Sandbox лицензируется как software appliance с поддержкой, кратной 1000 пользователей KES. Ниже приводится предварительная информация о стоимости решения для продажи конечным пользователям на территории Российской Федерации.

Кол-во SW appliance	**1**	**2-4**	**5-9 ***	**10+ ****
Цена, руб / год	2 300 000	2 200 000	2 100 000	2 000 000

* Необходимые для Kaspersky Sandbox физические и виртуальные серверы не входят в поставку и приобретаются отдельно.
** Для поддержки 5 000 и 10 000 узлов существуют отдельные конфигурации аппаратного обеспечения.

- Лицензии Microsoft включены в стоимость решения

Выводы

1. Kaspersky Sandbox – это необходимое дополнение к KES, которое позволяет автоматически блокировать и реагировать на сложные угрозы без привлечения дополнительных ресурсов и экономить время существующих ИБ-специалистов, находящихся в штате организации.

2. Kaspersky Sandbox идеально подходит для:
   - компаний, где роль ИБ выполняют IT-инженеры,
   - крупных организаций с территориально распределенной инфраструктурой и наличием небольших офисов без квалифицированных ИБ-специалистов на местах.

kaspersky


Kaspersky Web Traffic Security
KASPERSKY lab

Основные возможности

- Защита нового поколения от вредоносных программ и фишинга в режиме реального времени и по запросу
- Фильтрация содержимого для блокирования подозрительных файлов и предотвращения утечки данных
- Масштабируемость
- Защита от угроз «нулевого часа»
- Интеграция с Kaspersky Security Network
- Поддержка Microsoft Active Directory
- Ролевой доступ для администрирования и доступа к интернету
- Рабочие области для создания политик по подразделениям компании
- Контроль использования веб-ресурсов
- Блокирование программ шифровальщиков при попытке проникновения в сеть
- Мониторинг доступа в сеть, возможность расследования инцидентов

Подробнее - https://www.kaspersky.ru/small-to-medium-business-security/proxy-web-traffic

kaspersky

Коротко о том, что нового в KWTS 6.1:

- В составе решения: прокси-сервер и средства защиты веб-трафика

- Обновленные правила обработки трафика

- Ролевой доступ пользователей к отдельным рабочим областям для передачи управления локальным группам администраторов

- Управление параметрами прокси-сервера через веб-интерфейс, включая настройку расшифровки SSL-трафика

- Возможность настройки страницы блокирования по рабочим областям

Поставляется в виде виртуального устройства (допускается установка на физический и виртуальный сервер)

Интеграция с Kaspersky Anti Targeted Attack Platform

kaspersky

KasperskyOS for Thin Client

KASPERSKY lab

История KasperskyOS

kaspersky

Основные принципы реализации

Микроядро собственной разработки (не LINUX)

KasperskyOS построена на микроядре, которое контролирует взаимодействие между любыми компонентами ОС, приложениями и устройствами. Компактность позволяет использовать его на различных платформах.

Безопасность как часть архитектуры ОС

Система не общего, а специального назначения обеспечивает применение тонких политик безопасности к каждому критичному приложению на уровне ядра.

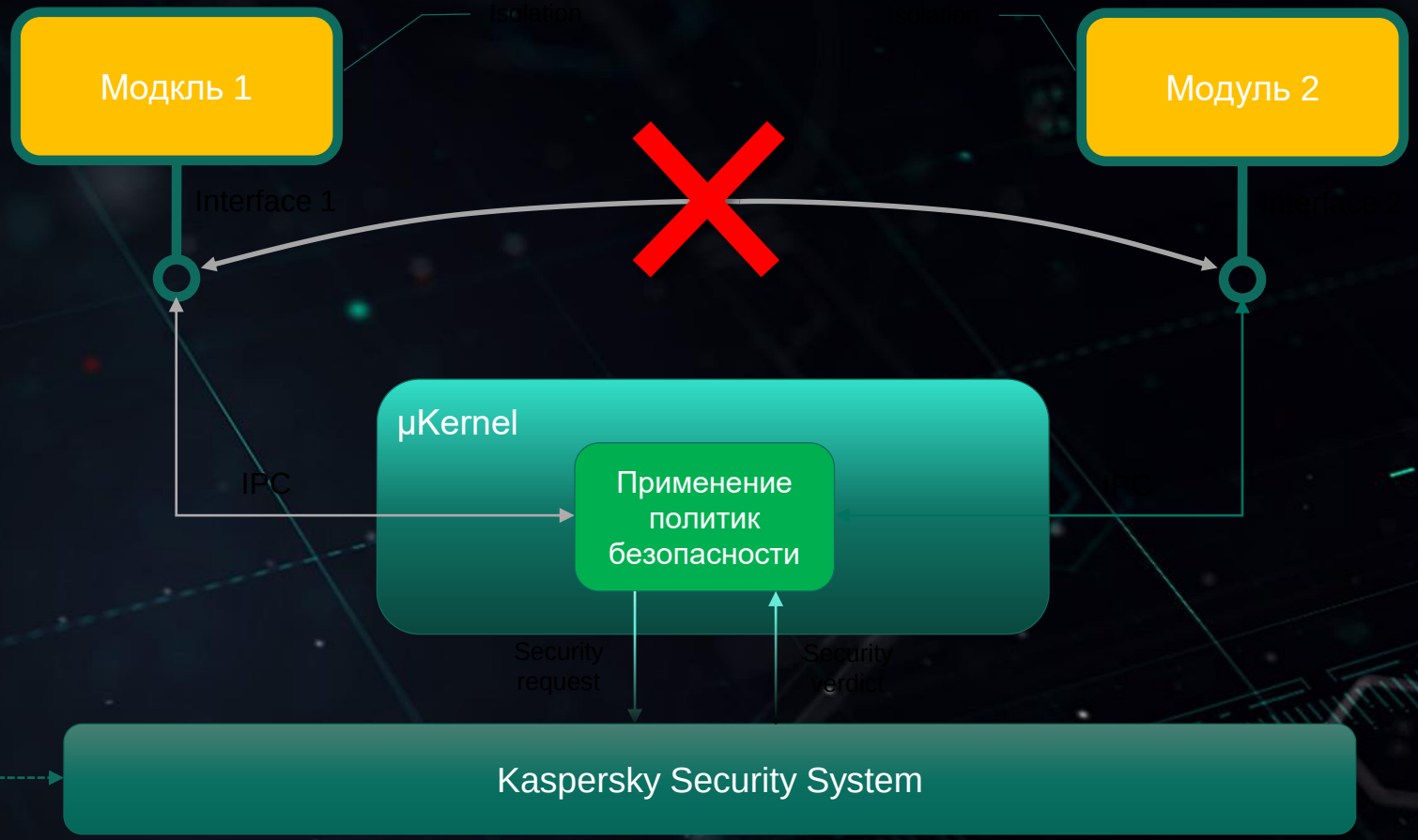
Модульность и неизбыточность кода

Компонентная архитектура приложений упрощает разработку решений. Благодаря модульному подходу оптимизируется размер доверенной кодовой базы.

kaspersky

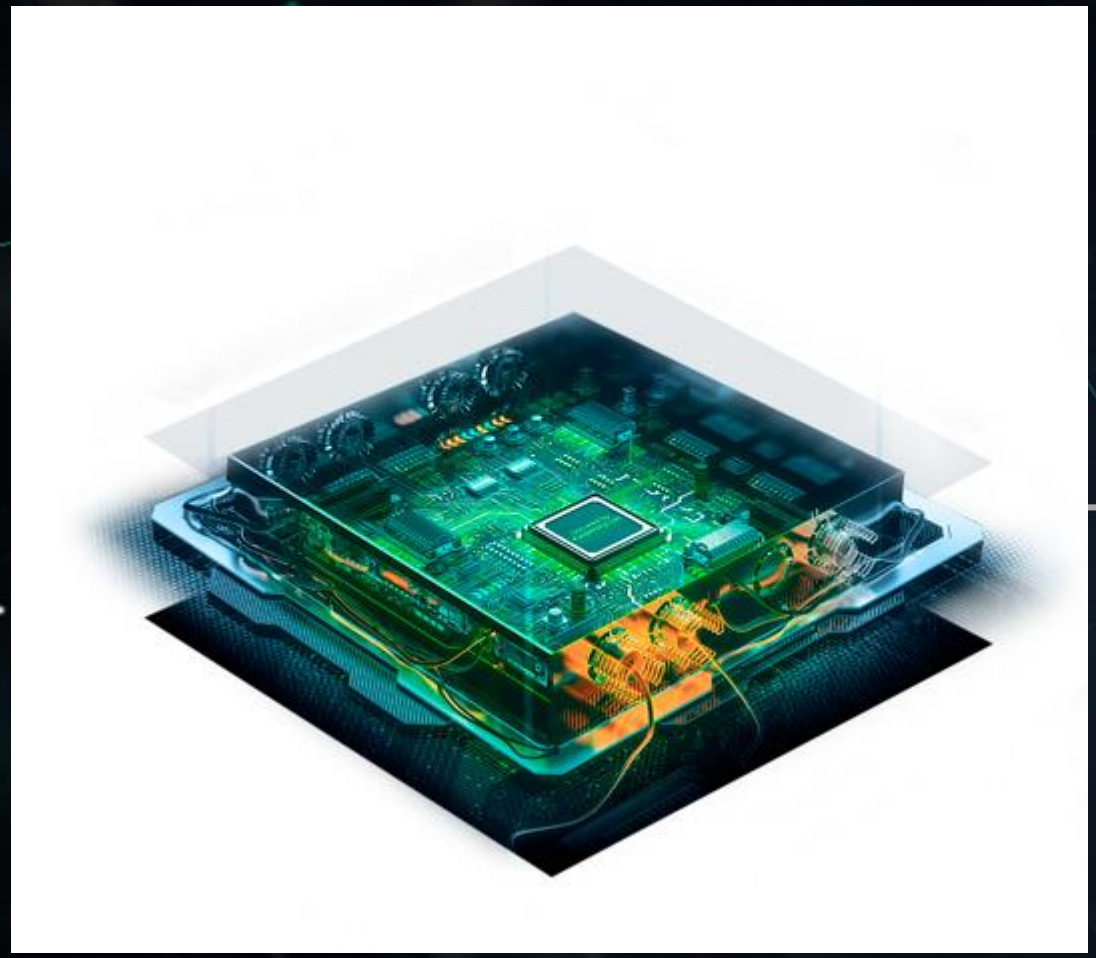
Основные принципы безопасности KasperskyOS

- **Собственное микроядро**
- Строгая изоляция
- Явно определенные типизированные интерфейсы
- Статическая конфигурация безопасности
- Полное посредничество
- Запрет по умолчанию
- Драйверы пользовательского пространства



kaspersky

KasperskyOS – операционная система с функциями безопасности на уровне ядра



Networking
Коммутаторы, маршрутизаторы, Wi-Fi, МЭ

IoT
Умные города, IoT и SCADA, PLC, IIoT

Transportation
Автомобили, автобусы, поезда

Desktop & Mobile
Встроенные системы, пользовательские устройства

kaspersky

Зачем нужен тонкий клиент?

Он заменяет системный блок сотрудника

В нем нет вентиляторов, активного охлаждения. Срок его службы до 10 лет. По производительности он слабее настольного компьютера, поэтому он…

Подключается к удаленному рабочему столу

Это может быть удаленный ПК, терминальный сеанс подключения или виртуальное рабочее место, запущенное в инфраструктуре VDI (Virtual Desktop Infrastructure). Непосредственная работа ведется на удаленном ПК или сервере, и поэтому…

Затраты на обслуживание и поддержку рабочих мест сотрудников снижаются в разы

Помимо этого растет уровень обеспечения безопасности. Ведь сотрудник не хранит никаких данных и не запускает сами бизнес-приложения на своем тонком клиенте.

Основные особенности версии 1.0

Подключение к VDI и терминальным серверам

по протоколу Microsoft RDP и через российскую систему виртуализации Скала-Р

Kaspersky Security Center

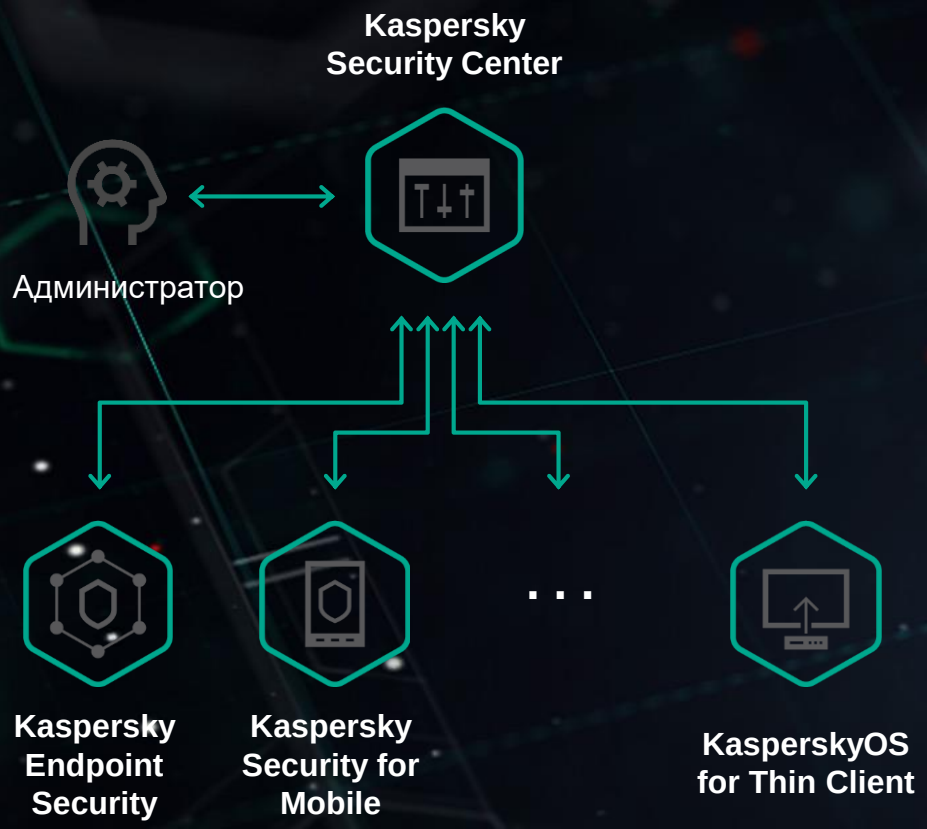
надежный инструмент централизованного управления и настройки тонких клиентов

KasperskyOS

обеспечивает безопасность инфраструктуры тонких клиентов на уровне ядра операционной системы

kaspersky

Централизованное управление инфраструктурой



Kaspersky Security Center

Корпоративная консоль управления KSC получит новый модуль для решения нового спектра задач по управлению тонкими клиентами :

- аутентификация тонких клиентов при подключении в корпоративную сеть
- централизованная настройка тонких клиентов через политики,
- удобное и надежное обновление тонких клиентов без создания критической нагрузки на сеть

Безопасность

На тонком клиенте будет работать только то программное обеспечение, которое подготовлено и разрешено к использованию ИТ и ИБ службами. Тонкие клиенты с KasperskyOS for Thin Client – доверенные и безопасные элементы IT инфраструктуры вне зависимости от ее масштаба.

kaspersky

Интеграция с технологическими партнерами

Depo Sky 270

Тонкий клиент производства компании Depo Computers – первый среди поддерживаемых операционной системой KasperskyOS
https://www.depo.ru/catalog/kompyutery/tonkie-klienty-depo-sky/depo-sky-270/

Скала-Р

RDP и **Скала-Р**

На старте мы поддерживаем работу не только со «стандартным» RDP, но и отечественной системой виртуализации Скала-Р BPM производства компании IBS, нашего технологического партнера. Важно, что система Скала-Р уже интегрирована с продуктом KSV. Список поддерживаемых подключений будет расти от версии к версии.

РУТОКЕН

Поддержка двухфакторной аутентификации – одно из основных требований бизнеса к тонкому клиенту. В версии продукта 1.0 мы реализуем работу с ключевыми носителями РУТОКЕН компании Актив.

kaspersky

12 000 рублей

Именно столько, в среднем, составляет трехлетняя стоимость владения российской операционной системой для тонкого клиента. За эти деньги клиент обычно получает операционную систему и базовую поддержку.

Больше функционала за те же деньги

При сопоставимой стоимости владения операционной системой вместе с KasperskyOS for Thin Client заказчик получает в свое распоряжение консоль и механизмы централизованного управления тонкими клиентами, аналогов которым у российских производителей нет – ни по надежности, ни по функционалу, ни по уровню клиентского доверия.

kaspersky

Лицензирование

KasperskyOS for Thin Client 1.0 состоит из:

1. Лицензии KOS4TC v1.0

Бессрочная лицензия на использование операционной системы KasperskyOS for Thin Client версии 1.0 и других минорных обновлений 1.x .

2. Клиентской лицензии модуля централизованного управления тонкими клиентами для KSC

Годовая лицензия на подключение тонкого клиента под управлением KasperskyOS for Thin Client к модулю централизованного управления тонкими клиентами KSC.

Конечное решение – полноценный VDI проект, собирает системный интегратор.

kaspersky

Этапы развития

Проведено внутреннее тестирование продукта

Полсотни сотрудников Kaspersky в августе-сентябре 2019 работают с тонкими клиентами Depo Sky 270 под управлением **KasperskyOS for Thin Client**. Собрана обратная связь, скорректирован roadmap разработки.

Март 2020: версия 1.0

Выпуск коммерческой версия **KasperskyOS for Thin Client 1.0**. Проведение пилотов.

Q4 2020: релиз версии 2.0

По итогам пилотирования, использования и продаж версии 1.0 будет дополнен существующий перечень требований к версии 2.0. Ее выпуск планируется на конец 2020 года. Вы тоже можете повлиять на то, какой будет **KasperskyOS for Thin Client v 2.0.**

kaspersky

Ценность KasperskyOS for Thin Client

Помогаем перейти на инфраструктуру тонких клиентов

Для перехода на тонкие клиенты на отечественной ОС нет необходимости искать дополнительных администраторов, разрабатывать скрипты и строить процессы поддержки тонких клиентов «на коленке». Все необходимое уже будет в KSC.

Минкомсвязь России:

- *Приказ № 335 от 04.07.2018*
- *Приказ № 486 от 18.04.2019*

Снижение рисков кибератак на тонкие клиенты

Linux давно известен киберпреступникам. Можно максимально усложнить им задачу и упростить модель угроз за счет использования KasperskyOS for Thin Client с нашим качеством безопасной разработки и со встроенными на уровне ядра механизмами безопасности.

Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю *bdu.fstec.ru/vul*

Более 350 уязвимостей в Astra Linux.

Тонкие клиенты на действительно российской операционной системе, а не на Linux

На рынке появляется операционная система, разработка которой с нуля велась в России. Не обязательно выбирать переименованный Linux для того, чтобы соответствовать требованиям организаций и регуляторов..

Приказ Минкомсвязи России от *18.06.2019 №335*

Операционная система KasperskyOS в Едином реестре российских программ для электронных вычислительных машин и баз данных

kaspersky

Планирование пилота

1. **Нужно определиться со средой виртуализации и протоколами для пилота.**
   В Q2-Q3 2020 мы поддержим работу с Microsoft RDP и системой виртуализации Скала-Р BPM
2. **Выделить пилотную зону до 20 типовых рабочих мест.**
   Типов сотрудников может быть несколько, например офис-менеджеры, разработчики, продавцы, юристы.
3. **Выбрать две недели, в которые будет проводиться пилот.**
   Этого времени достаточно для того, чтобы оценить характеристики решения и эффективно собрать обратную связь от пользователей и поддержки.
4. **Согласовать проведение пилота между ИТ и ИБ службой.**
   Добавление новых устройств в корпоративную сеть – процесс, требующий вовлечения обоих сторон. Для того, чтобы стартовать и завершить пилот вовремя, все должно быть готово и согласовано заранее.

Со стороны Лаборатории Касперского в начале 2020 года будет предоставлена предлагаемая программа пилотирования и рекомендации по подготовке и проведению пилотного проекта.

kaspersky

Вопросы?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab