

# Контроль и защита физической и виртуальной инфраструктуры из единой консоли



**Kaspersky  
Endpoint Security**  
для бизнеса  
Универсальный

В эпоху цифровой трансформации организации начинают активно использовать виртуальные платформы. Это дает бизнесу массу новых возможностей, но одновременно с этим серьезно усложняет задачу реализации единой стратегии информационной безопасности.

Kaspersky Endpoint Security для бизнеса Универсальный объединяет в одном продукте все необходимые функции управления и контроля для всех типов рабочих мест – как виртуальных и физических. Это снижает нагрузку на администраторов и позволяет повысить общий уровень безопасности компании.

## Основные преимущества

### Почему Kaspersky Security для бизнеса Универсальный

- Одна лицензия для защиты виртуальных и физических рабочих мест и серверов
- Заслужившие признание технологии предотвращения угроз
- Централизованное управление безопасностью
- Снижение нагрузки на ИБ-службы за счет увеличения уровня отраженных угроз
- Обеспечение соответствия регуляторным нормам
- Интегрированные шифрование и патч-менеджмент
- Поддержка всех популярных платформ виртуализации
- Простая интеграция с SIEM-системами

### Экономия ресурсов за счет унифицированного управления всеми ресурсами

Администраторы управляют защитой виртуальных и рабочих мест из единой консоли Kaspersky Security Center, что упрощает внедрение единообразных политик во всей инфраструктуре. Разграничение прав доступа администраторов, централизованная установка ПО, автоматизированные средства поиска уязвимостей – эти и другие возможности позволяют экономить ресурсы, оптимально распределять обязанности и поддерживать стабильно высокий уровень безопасности всех видов рабочих станций и серверов.

### Специализированная защита виртуальных платформ

Традиционные защитные решения не предназначены для виртуальных платформ. Они потребляют много ресурсов и критически важные бизнес-приложения начинают работать медленнее. Запатентованная технология легкого агента позволяет обеспечить защиту без воздействия на производительность, а также ускорить возврат инвестиций за счет повышения плотности виртуальных машин.

### Технологии защиты, признанные экспертами

В основе продуктов «Лаборатории Касперского» лежит сочетание опыта экспертов и технологий машинного обучения, что помогает эффективно противодействовать самым изощренным угрозам. Продукты «Лаборатории Касперского» регулярно участвуют и побеждают в независимых тестированиях – в 2018 году они заняли 73 первых мест в 88 тестах.

## Kaspersky Endpoint Security для бизнеса Универсальный –

это решение, которое в рамках одной лицензии объединяет защиту физических и виртуальных рабочих мест и серверов. Оно упрощает цифровую трансформацию компании, экономит ресурсы и позволяет эффективно и в полной мере обеспечивать проведение адаптивной стратегии обеспечения безопасности.

### Поддерживаемые платформы

#### Платформы виртуализации

- VMware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM
- Huawei FusionSphere

#### Физические серверы

- Windows
- Linux

#### Рабочие станции

- Windows
- Linux
- Mac

#### Мобильные устройства

- Android
- iOS

### Приложения в составе продукта

[Kaspersky Endpoint Security для Windows](#)

[Kaspersky Endpoint Security для Linux](#)

[Kaspersky Endpoint Security для Mac](#)

[Kaspersky Security для Windows Server](#)

[Kaspersky Security для мобильных устройств](#)

[Kaspersky Security Center](#)

[Kaspersky Security для виртуальных сред Легкий агент](#)

# Основные функции защиты и управления

## Единая консоль управления

Kaspersky Security Center – гибкая и полнофункциональная консоль управления, которая позволяет управлять системой безопасности, контролировать все виды устройств, получать наглядные отчеты и распределять обязанности.

## Мощные инструменты контроля

Кроме автоматизированных средств предотвращения угроз, продукт содержит мощные инструменты контроля, которые снижают вероятность заражения. В частности, контроль программ помогает снизить угрозы на этапе запуска той или иной программ, а сценарий «Запрет по умолчанию» серьезно снижает поверхность потенциальной атаки.

## Легкий агент

В отличие от традиционных решений, требующих установки полноценного тяжелого агента на каждую виртуальную машину, Легкий агент требует установки решения только на выделенное устройство безопасности (SVM) на каждом виртуальном хосте. После этого на виртуальной машине нужно развернуть лишь небольшое ПО – Легкий агент. При этом выделенное устройство безопасности выполняет централизованную проверку виртуальных машин.

## Защита от шифровальщиков

Средства защиты от шифровальщиков обеспечивают защиту от любых попыток шифрования критических данных помогают откатывать зараженные файлы к исходному состоянию, а также позволяют заблокировать удаленную атаку шифровальщика.

## Система предотвращения вторжений на уровне хоста (HIPS)

На основе данных Kaspersky Security Network образуется четыре стандартные группы доверенных программ, а HIPS распределяет программы по этим группам. Самые доверенные из них заносятся в белый список и запускаются без ограничений. Остальные имеют ограниченные привилегии и лимитированный доступ к критическим сетевым ресурсам.

## Защита от веб-угроз

Этот компонент защищает данные, которые поступают на компьютер и отправляются с него, устанавливает принадлежность URL-адресов к вредоносным или фишинговым веб-адресам, а также проверяет HTTPS-трафик, чтобы своевременно пресечь действия агентов ботнетов, дропперов, вирусов-вымогателей и т. д.

[www.kaspersky.ru](http://www.kaspersky.ru)