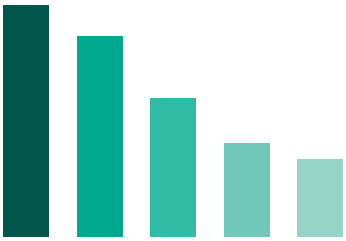
Надежная облачная защита и высокая производительность для вашей гибридной инфраструктуры

Kaspersky Security для виртуальных и облачных сред

kaspersky



Безопасность 81%

Управление затратами на облако 79%

Корпоративное управление и соответствие требованиям 75%

Управление несколькими облаками 72%

Миграция в облако 71%

Основные проблемы использования облачных сред, с которыми сталкиваются все организации[2]

89%

компаний используют решения VDI[1]

55%

корпоративных рабочих нагрузок планируется перенести в облако в течение 12 месяцев[2]

Как достичь максимальной эффективности бизнеса в ходе цифровой трансформации?

Повсеместная цифровая трансформация современного бизнеса требует скорейшего освоения облачных технологий. Они помогают компаниям повышать гибкость, адаптироваться к региональным стандартам и потребностям рынка, совершенствовать продукты и услуги, оптимизировать операции и улучшать качество обслуживания клиентов. Трансформация открывает для бизнеса много бесспорных преимуществ, но у этой медали есть и обратная сторона: повышается сложность инфраструктуры, а вместе с ней и риски безопасности; компаниям приходится пересматривать принципы корпоративного управления, расширять штат специалистов, оптимизировать производительность, выполнять новые требования и нести дополнительные расходы.

Сложности работы с разными типами рабочих нагрузок

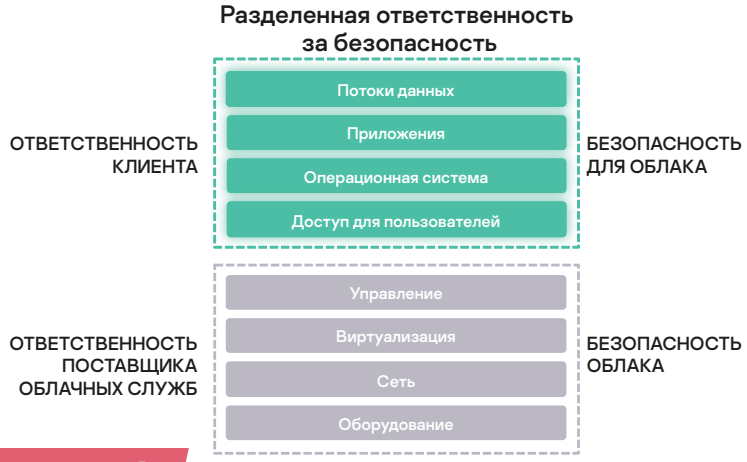
Гибридные инфраструктуры поддерживают широкий спектр рабочих нагрузок: на физических серверах или виртуальных машинах, в частном или публичном облаке и даже в мультиоблачных средах. Решать задачи, связанные с контролем рисков безопасности, корпоративным управлением, соблюдением нормативных требований и распределением бюджета на обслуживание инфраструктуры, приходится всем организациям. Однако необходимость управлять различными типами рабочих нагрузок создает дополнительные сложности.

Виртуализация без ущерба для производительности

Виртуальные серверы и инфраструктуры виртуальных рабочих столов (VDI) используются компаниями из любых отраслей, независимо от их размера и региона деятельности. Виртуализированная инфраструктура позволяет использовать имеющиеся физические ресурсы гораздо эффективнее, чем локальная. Однако, чтобы сохранить ее производительность, требуется защитное решение, разработанное специально для виртуальных сред. Эффективные инструменты для защиты виртуальных сред должны обеспечивать централизованное управление задачами безопасности, использовать все доступные данные без создания лишних копий, сбалансированно распределять нагрузку между виртуальными машинами и задействовать все возможности платформы виртуализации, чтобы обеспечить максимальную защиту систем с минимальным влиянием на их производительность.

Разделение ответственности при защите рабочих нагрузок в облаке

Все больше компаний переносят рабочие процессы в публичное облако и часто пользуются услугами сразу нескольких (в среднем двух) поставщиков облачных служб. Облачные технологии обеспечивают высокую масштабируемость и производительность и используются бизнесом для вычислений, обработки и анализа данных и выполнения других задач. С переходом в облако вам не придется беспокоиться об обслуживании инфраструктуры – она будет развернута на стороннем оборудовании. Обслуживание сети и виртуальных компонентов и управление ими тоже переходит в зону ответственности поставщика облачных служб. Это очень удобно. Но передав ответственность за свою инфраструктуру, вы теряете и контроль над ней. При этом вы все еще отвечаете за другие аспекты вашей виртуализированной среды, о которых мы расскажем ниже, и должны позаботиться об их безопасности.



[1] Внутреннее исследование «Лаборатории Касперского», 2021 г.

[2] Отчет Flexera State of the Cloud, 2021 г.

53%

организаций используют контейнеры Docker[3]

51%

организаций пользуются предложением AWS «Контейнеры как услуга»[3]

«Решение обеспечивает безопасность виртуальных и облачных сред, не снижая производительности системы и не отвлекая пользователей».

Из отзывов на сайте Gartner

Особые требования к средам DevOps

Если раньше разработчики выпускали новые сборки ежегодно или раз в полгода, то теперь они делают это ежедневно или даже ежечасно. Именно поэтому при разработке ПО особое внимание уделяется обеспечению процессов непрерывной интеграции и доставки (CI/CD). Это автоматизированные операции, которые помогают компаниям улучшить ключевые показатели. Контейнеры играют ключевую роль в DevOps-процессах, поскольку ускоряют разработку и позволяют выполнять масштабные развертывания. Внедрение методов DevOps обычно становится возможным благодаря использованию общедоступных облачных платформ. При этом основной целью является сокращение сроков выпуска продукта за счет увеличения скорости и гибкости разработки. Поэтому интеграция решений безопасности не должна нарушать процессы разработки и функционирование облачных приложений.

Облачная защита для поддержания оптимальной производительности гибридных инфраструктур

Kaspersky Security для виртуальных и облачных сред позволяет решить эти задачи, обеспечивая высококачественную защиту на любой платформе и не ограничивая возможности виртуализации и облачных технологий. Где бы вы ни развернули рабочие нагрузки – на физических серверах или виртуальных машинах, в частном, публичном или гибридном облаке, – наши защитные технологии обеспечат полную безопасность вашей инфраструктуры с минимальной нагрузкой на систему.

- Легкие агенты, оптимизированные для работы с каждой ОС, позволяют снизить потребление ресурсов виртуализации на 30%, высвобождая мощности для выполнения других бизнес-операций. Благодаря оптимизации, например использованию общего кеша, в котором хранится информация о проверках файлов, приложение сокращает объем обрабатываемых данных и количество выполняемых действий, значительно уменьшая число операций ввода-вывода в секунду и затрачиваемых циклов ЦП, потребность в памяти и дисковом пространстве, и снижает общую нагрузку на вашу IT-инфраструктуру. Это позволяет достичь высоких коэффициентов консолидации и увеличить рентабельность вложений в проекты виртуализации.

- Наше решение совместимо с разными платформами – оно защищает рабочие нагрузки в Windows и Linux и интегрируется с платформами AWS, Microsoft Azure и Google Cloud через API. Это позволяет четко разделить зоны ответственности в области безопасности между вашей компанией и поставщиком облачных служб. Интеграция с облачными службами через API обеспечивает автоматизацию и гибкие возможности администрирования. Информация обо всех экземплярах виртуальных машин, запущенных под разными учетными записями, которая доступна через консоль управления, поможет вам при развертывании защитных агентов и настройке политик безопасности для них. По мере развертывания новых облачных экземпляров Kaspersky Security для виртуальных и облачных сред автоматически подстраивается под растущие нагрузки. Применяя политики управления API и автоматического масштабирования, вы сможете защитить каждый новый экземпляр, который добавляется к группе, в соответствии с корпоративной политикой безопасности.

- Kaspersky Security для виртуальных и облачных сред позволяет реализовать концепцию «безопасность как код» – вы сможете не только защищать память хоста с помощью контейнеризации, создавать задачи для контейнеров, проверять образы и реализовывать интерфейсы через скрипты, но и интегрировать задачи безопасности в цепочки CI/CD, не мешая процессу разработки, что очень важно для DevOps-инженеров. Решение обеспечивает безопасность в контейнерах Docker и Windows, не позволяя злоумышленникам использовать вредоносные компоненты контейнеров для атак на инфраструктуру компании.

[3] Отчет Flexera State of the Cloud, 2021 г.

64%

организаций более всего опасаются потери или утечки данных при работе в облачных средах[4]

«Не нужно устанавливать дополнительные антивирусные программы или агенты».

Из отзывов на сайте Gartner

Стремительный рост рисков безопасности

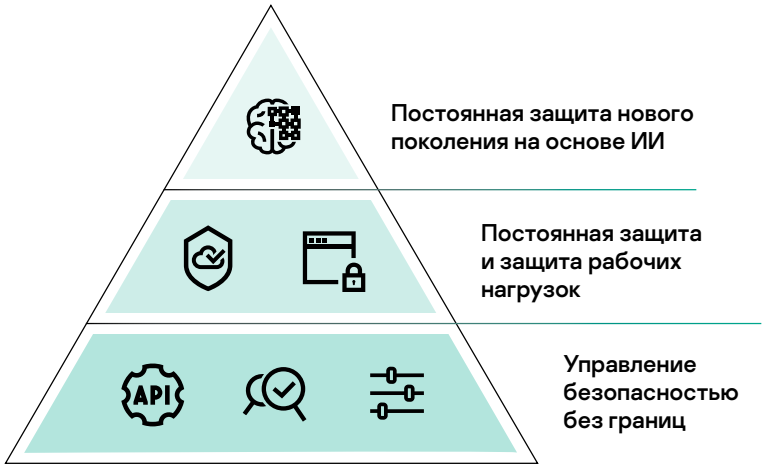
Злоумышленники не упускают возможности нажиться на цифровой трансформации бизнеса. Неправильная конфигурация, отсутствие прозрачности, утрата контроля над отдельными частями инфраструктуры во время миграции в облако делают компании уязвимыми к разнообразным угрозам – от утечки данных до атаки шифровальщиков. Киберпреступники не отстают от потенциальных жертв и тоже осваивают облачные среды: в последнее время число фишинговых атак на облачные ресурсы возросло вдвое[5]. У злоумышленников даже появились специальные инструменты для поиска неправильных настроек.

Защитить гибридную инфраструктуру от постоянно эволюционирующих угроз крайне важно. Но во что это обойдется? Грубые вмешательства системы безопасности в процесс разработки и развертывания недопустимы, а IT-специалисты и службы безопасности не должны тратить рабочее время на обработку ложных срабатываний и событий с низким уровнем риска. Нужно подобрать решение, которое безупречно интегрируется в вашу IT-инфраструктуру и избавит ваших сотрудников от рутинных защитных задач.

Лучшая защита для гибридных сред

Во всех решениях и сервисах «Лаборатории Касперского» используются передовые технологии, которые обеспечат полную безопасность ваших данных, общих папок и всей гибридной инфраструктуры.

- Технологии многоуровневой защиты проактивно противодействуют большинству атак, в том числе вредоносному ПО, фишингу и другим угрозам.
- Алгоритмы машинного обучения и богатый опыт наших экспертов обеспечивают высокий уровень обнаружения угроз при минимальном количестве ложных срабатываний.
- Аналитические данные об угрозах поступают в режиме реального времени и позволяют защитить инфраструктуру от новейших эксплойтов.



Решение не только обнаруживает и предотвращает сетевые вторжения в облачные активы, но и откатывает любые несанкционированные изменения облачных рабочих нагрузок в случае необходимости. Контроль программ позволяет перевести все рабочие нагрузки в гибридном облаке в режим «Запрет по умолчанию», чтобы усилить защиту системы: выполняться смогут только доверенные приложения.

Kaspersky Security для виртуальных и облачных сред также защищает важные коммерческие данные от атак программ-вымогателей, блокируя попытки удаленного шифрования и выполняя откат поврежденных файлов к предыдущему состоянию.

[4] Statista, 2021 г.
[5] Kaspersky Security Bulletin, 2021

44%

компаний столкнулись со значительным ростом затрат на обеспечение безопасности[6]

Баланс между гибкостью, стоимостью и возможностями управления

Облачные среды повышают эффективность операций, позволяя использовать гибкие методологии разработки и обеспечивая эластичность потребляемых ресурсов. Но такая инфраструктура становится более сложной, а в связи с коротким жизненным циклом рабочих нагрузок и недостаточной прозрачностью требуются дополнительные инструменты для ее администрирования. Поэтому важно найти баланс между повышенной эффективностью, которую предлагают облачные технологии, и затратами на администрирование более сложной гибридной инфраструктуры и ее защиту.

«Несколько защитных решений доступны по одной лицензии».

Из отзывов на сайте Amazon

Комфортный переход в облако и удобное администрирование без лишних затрат

Мы знаем, насколько эти аспекты перехода в облако важны для бизнеса, поэтому предлагаем решение с гибким лицензированием и удобными инструментами управления, которое не создает излишней нагрузки на системные ресурсы и корпоративный бюджет.

- Наша гибкая модель лицензирования позволяет разумно распорядиться бюджетом, выбрав только те функции, которые вам необходимы. Вам доступны два уровня защиты и разные объекты лицензирования – компьютеры, серверы и процессоры. Типы лицензий можно комбинировать. Мы также предлагаем возможности пользоваться уже приобретенными лицензиями и оплачивать сервис по факту использования.
- Единая облачная консоль упрощает контроль безопасности вашей инфраструктуры и уменьшает нагрузку на IT-специалистов, позволяя централизованно управлять всеми рабочими нагрузками.
- Удобная инвентаризация облачной инфраструктуры и автоматизированное развертывание средств безопасности в удаленном режиме еще больше повышают удобство управления и обеспечивают максимальную прозрачность.

45%

организаций не прошли аудит облачной инфраструктуры[7]

Соответствие требованиям при работе в облачной среде

Каждая организация должна выполнять как корпоративные стандарты, так и внешние нормативные требования, например GDPR. Ответственность за безопасность облачных сред делят IT-отдел, ИБ-отдел, DevOps (при наличии) и аналитик соответствия, который отвечает за готовность компании к аудитам облачной инфраструктуры. Защитное решение должно обеспечивать соответствие всем новым требованиям по мере их появления и способствовать успешному прохождению аудита.

«Решение предлагает полностью автоматизированную защиту».

Из отзывов на сайте Amazon

Соответствие требованиям в строго регулируемых отраслях

Kaspersky Security для виртуальных и облачных сред не только обеспечивает соответствие требованиям к безопасности, но и максимально автоматизирует связанные с этим рутинные операции.

- В решении используются адаптивные и комплексные технологии, непрерывно обеспечивающие полное соответствие нормативным требованиям, – от усиления защиты систем и самозащиты агентов до оценки уязвимостей и автоматизированного управления установкой исправлений.
- Широкий набор функций позволяет выполнять все нормативные требования и управлять рисками в полном соответствии с действующим законодательством.

[6] Внутреннее исследование «Лаборатории Касперского», 2021 г.

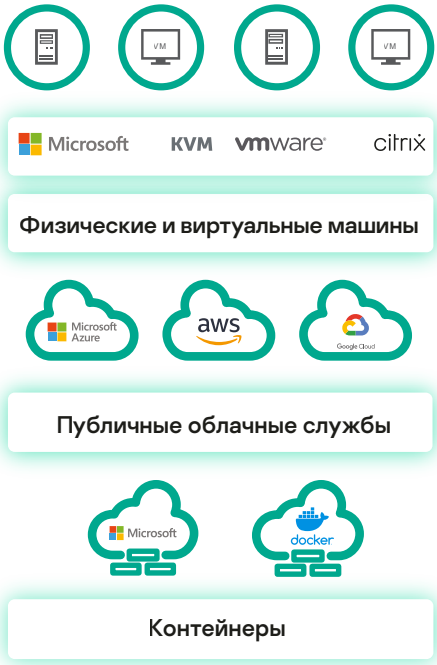
[7] Отчет Fugue The State of Cloud Security, 2021 г.

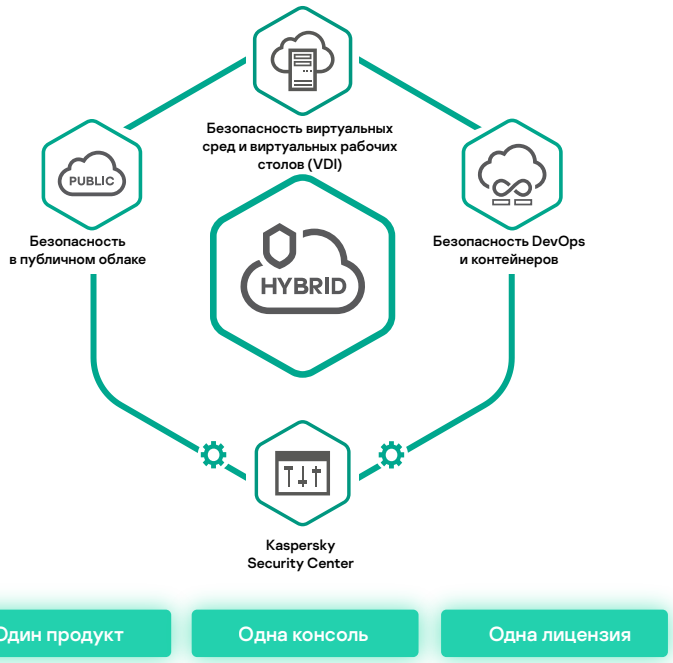
Узнайте больше о Kaspersky Security для виртуальных и облачных сред

На сайт

Цифровая трансформация в центре внимания

Цифровая трансформация открывает множество возможностей как для бизнеса, так и для злоумышленников. Kaspersky Security для виртуальных и облачных сред не просто снижает риски безопасности – это решение экономит ваше время, системные ресурсы и бюджет, делая переход в облако максимально эффективным. Для удовлетворения всех ваших потребностей в облачной безопасности вам нужен всего один продукт, для защиты всех рабочих нагрузок – одна лицензия, а для управления гибридной инфраструктурой – одна консоль. Мы позаботимся о вашей безопасности, а вы сможете сосредоточиться на других важных аспектах цифровой трансформации.





Если вы хотите узнать больше о том, как обеспечить надежную защиту гибридной среды, обратитесь к представителю «Лаборатории Касперского» или перейдите на наш сайт.

www.kaspersky.ru
www.securelist.ru