Kaspersky® Security для виртуальных и облачных сред

Передовая защита и контроль гибридной облачной инфраструктуры

Главные сложности перехода на облако:

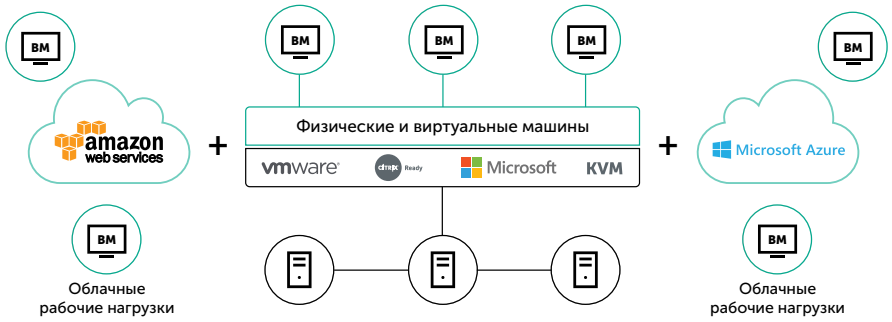
- Растущая сложность инфраструктуры может снизить прозрачность операций.
- Действительно надежная защита возможна только при многоуровневой интеграции.
- Традиционные тяжеловесные защитные продукты отнимают много системных ресурсов.
- Несовместимые средства управления усложняют администрирование.
- Неэффективная организация защиты приводит к такой же неэффективности системных процессов.
- Вредоносное ПО и программы-вымогатели атакуют как виртуальные, так и физические рабочие места.
- Низкий уровень защиты не соответствует нормативным требованиям.
- Реактивная защита не может заменить адаптивную и проактивную системы безопасности.

Преимущества Kaspersky Security для виртуальных облачных сред

- Оптимизация под физические, виртуальные и облачные рабочие нагрузки
- Многоуровневая интегрированная система защиты для любого частного ЦОД
- Гармоничная интеграция гибких и автоматизированных средств безопасности с публичными облаками AWS и Azure
- Полный набор инструментов для соблюдения требований по общей ответственности
- Централизованное управление безопасностью всей гибридной облачной среды корпоративного класса

Сочетание виртуальных и облачных сред разного типа с локальными ресурсами зачастую оказывается экономически оправданным. Однако эта гибридная среда должна соответствовать жестким стандартам безопасности. В противном случае под ударом окажутся ценные данные и непрерывная работа бизнеса.

Решение Kaspersky Security для виртуальных и облачных сред позволяет организовать адаптивную экосистему кибербезопасности с продуманным управлением. Где бы вы ни хранили и обрабатывали критические бизнес-данные – в частном или публичном облаке либо в их сочетании, – сбалансированное сочетание гибких и эффективных средств защиты оградит ваши рабочие нагрузки от самых сложных известных и неизвестных угроз, без ущерба для производительности.



Защита нового поколения для физических, виртуальных и облачных сред

- Запатентованные технологии защищают все рабочие нагрузки вне зависимости от их расположения.
- Многоуровневая постоянная защита в паре с машинным обучением отвечает за безопасность ваших данных, процессов и приложений.

Защита гибридного облака с эффективным использованием ресурсов

- Технологии защиты виртуальных машин на основе легкого агента и без агента позволяют обезопасить программно-определяемые ЦОД без ущерба производительности.
- Интеграция со встроенной системой безопасности публичных и управляемых облачных сред помогает защитить приложения, ОС, пользователей и потоки данных с минимальным расходом ресурсов.
- Объединенное управление физическими и виртуальными ресурсами повышает эффективность администрирования.

Полный контроль гибридной инфраструктуры

- **Унифицированное управление безопасностью** из единой консоли охватывает все корпоративные устройства, включая рабочие места и серверы в офисах, центрах обработки данных и облаке.
- **Гармоничная интеграция с облачными API** публичных облаков AWS и Azure открывает возможности обнаружения инфраструктуры, автоматического развертывания агентов безопасности и управления на основе политик, а также упрощает инвентаризацию и развертывание средств безопасности.
- **Гибкое управление** поддерживает несколько клиентов и контроль учетных записей на основе разрешений, включая при этом все преимущества унифицированного управления из единого сервера.

Унифицированная безопасность

Публичные облачные службы
- Amazon Web Services (AWS)
- Microsoft Azure

Платформы виртуализации
- VMware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM

Среды VDI
- VMware Horizon
- Citrix XenDesktop

Физические серверы
- Windows
- Linux

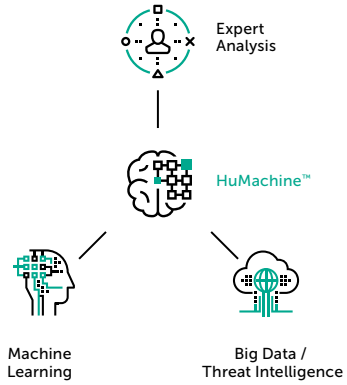
CITRIX Ready · Microsoft Azure · vmware · amazon web services

Защита облачных рабочих нагрузок

- **Контроль программ** позволяет перевести все рабочие нагрузки в гибридном облаке в режим «Запрет по умолчанию», чтобы усилить защиту систем и четко обозначить, где именно могут выполняться разрешенные программы и что им будет доступно.
- **Контроль устройств** отвечает за то, какие виртуализированные устройства могут обращаться к отдельным облачным рабочим нагрузкам, а функция веб-контроля защищает среду от киберугроз из интернета.
- **Сегментация сети** позволяет организовать прозрачную и автоматизированную защиту сетей инфраструктуры гибридного облака, которая проверяет отдельные сети и порты, а также может интегрироваться с программно-определяемыми сетевыми платформами наподобие VMware NSX.
- **Защита уязвимостей** предотвращает использование неисправленных уязвимостей продвинутым вредоносным ПО и угрозами нулевого дня.

Постоянная защита на основе машинного обучения

- **Передовая защита от вредоносного ПО** обеспечивает для каждой облачной рабочей нагрузки автоматическую защиту на уровне файлов при доступе и по требованию в реальном времени.
- **Облачная репутационная база данных** мгновенно обнаруживает новые угрозы и предоставляет автоматические обновления.
- **Защита электронной почты** с модулем Анти-спам отвечает за чистоту почтового трафика в облачных рабочих нагрузках.
- **Защита от интернет-угроз** с модулем Анти-фишинг защищает пользователя от потенциально опасных веб-сайтов и скриптов.
- **Мониторинг целостности файлов** защищает критически важные и системные файлы, а модуль анализа журналов проверяет внутренние файлы журналов, чтобы убедиться в безопасности операций.
- **Модуль анализа поведения** контролирует поведение программ и процессов, защищая от продвинутых киберугроз и бесфайловых вирусов.
- **Защита от эксплойтов** следит за поведением системных операций, процессов и программ, чтобы блокировать продвинутые угрозы и программы-вымогатели.
- **Защита от программ-вымогателей** предотвращает атаки на облачные рабочие нагрузки и их общие папки.
- **Системы обнаружения и предотвращения вторжений** (HIPS и HIDS) обнаруживают и предотвращают сетевые вторжения в облачные активы.



«Лаборатория Касперского»

www.kaspersky.ru

#истиннаябезопасность
#HuMachine