Kaspersky® Security для виртуальных и облачных сред

Передовая защита и контроль гибридной облачной инфраструктуры

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

Выберите решение, которое подходит именно вам

В таблице представлено сравнение функциональных возможностей версий Kaspersky Security для виртуальных и облачных сред. Стандартная версия включает в себя все необходимые технологии для защиты гибридной облачной инфраструктуры. Для организаций с повышенными требованиями к безопасности существует версия Enterprise, которая позволяет обеспечить соответствие строгим нормативным и законодательным требованиям.

	Standard	Enterprise
Интеграция с AWS и Azure при помощи API	✓	✓
Мониторинг, отчеты, ролевой доступ, виртуальный сервер администрирования	✓	✓
Защита файлов, памяти и процессов	✓	✓
Защита от эксплойтов, защита от сетевых угроз	✓	✓
Защита общих папок от попыток шифрования (Анти-Криптор)	✓	✓
Управление сетевым экраном	✓	✓
Контроль программ, система предотвращения вторжений для рабочих станций	✓	✓
Контроль устройств для серверов	✓	✓
Веб-антивирус, Почтовый антивирус, Анти-Спам, Анти-Фишинг	✓	✓
Контроль программ (Запрет по умолчанию) для серверов		✓
Передовые сетевые системы IDS/IPS (только в KSV без агента)		✓
Мониторинг целостности файлов		✓
Проверка журналов		✓
Поддержка сложных распределенных сред		✓

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

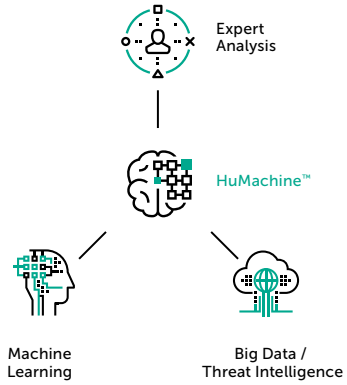
Физические серверы
- Windows
- Linux

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