Функции, доступные на уровнях Standard и Enterprise

Kaspersky Security для виртуальных и облачных сред

kaspersky

С Kaspersky Security для виртуальных и облачных сред ваша миграция в облако пройдет гладко. Доступны два уровня продукта – Standard и Enterprise. Решение уровня Standard снижает риски безопасности, сокращает потребление ресурсов виртуализации и экономит ваше время и деньги, а уровень Enterprise предлагает дополнительные преимущества и сценарии использования в контексте цифровой трансформации. Мы сравнили основные возможности двух уровней, чтобы помочь вам выбрать подходящее решение.

Сравнение уровней

Возможности	Standard	Enterprise
Интеграция с облачными API Решение интегрируется через API с публичными облачными платформами, такими как AWS, Microsoft Azure и Google Cloud.	✓	✓
Защита файлов, процессов и памяти Мы постоянно обновляем технологии, которые защищают от продвинутых угроз и программ-вымогателей вашу гибридную инфраструктуру, в том числе данные и общие папки.	✓	✓
Системы обнаружения и предотвращения вторжений, управление сетевым экраном Система предотвращения вторжений, которая работает совместно с двусторонним сетевым экраном «Лаборатории Касперского», контролирует входящий и исходящий сетевой трафик.	✓	✓
Веб-антивирус, Почтовый антивирус, Анти-Спам, Анти-Фишинг Защита от проникновения через почту и веб-приложения гарантирует безопасную работу виртуальных и удаленных рабочих столов.	✓	✓
Контроль защиты устройств и веб-контроль Компонент определяет, какие виртуализированные устройства могут обращаться к отдельным рабочим нагрузкам в облаке, и контролирует использование веб-ресурсов.	✓	✓
Контроль программ для настольных компьютеров На устройстве можно разрешить запуск только доверенных приложений.	✓	✓
Поведенческий анализ и защита от эксплойтов Мониторинг приложений и процессов защищает системы от продвинутых угроз и эксплойтов, включая бесфайловые и скриптовые зловреды.	✓	✓
Защита общих папок от шифрования Решение защищает важные коммерческие данные от атак программ-вымогателей, блокируя попытки удаленного шифрования и выполняя откат поврежденных файлов к предыдущему состоянию.	✓	✓
Защита контейнеров и интеграция для DevOps Защита интегрируется в процессы CI/CD, не замедляя их, и предотвращает заражение гибридной IT-инфраструктуры через скомпрометированные контейнеры.		✓
Оценка уязвимостей и управление установкой исправлений Решение обеспечивает централизацию базовых функций защиты, конфигурации системы и задач по управлению, таких как проверка на уязвимости, установка исправлений и обновлений, учет ПО и развертывание приложений.		✓
SIEM-коннекторы Интеграция с SIEM-системами позволяет централизованно управлять различными аспектами корпоративной безопасности.		✓
Контроль программ для серверных ОС Все рабочие нагрузки в гибридном облаке можно перевести в режим «Запрет по умолчанию».		✓
Мониторинг целостности файлов (FIM) Отслеживает целостность ключевых компонентов системы.		✓
Анализ журналов Проверка файлов журналов обеспечивает безопасность операций.		✓
IDS/IPS нового поколения для VMware NSX Предлагает расширенные возможности обнаружения подозрительной сетевой активности.		✓

Дополнительные возможности и преимущества уровня Enterprise

Дополнительные сценарии использования

Обеспечение полного соответствия требованиям

Расширенные возможности защиты

Безопасность DevOps	Решение позволяет защитить процессы DevOps и интегрировать проверку репозиториев, образов и контейнеров в процессы CI/CD.
Обеспечение соблюдения требований	Эта функция будет полезна компаниям, действующим в строго регулируемых отраслях, и тем, которые хотят максимально строго соблюдать применимые нормы. Компоненты Контроль программ, Мониторинг целостности файлов и Анализ журналов позволят соблюдать требования безопасности системы и данных, в том числе в соответствии с такими стандартами, как PCI DSS (версия 3.21, № 10.5, 11.5), ISO/IEC 27001 (A10.10.1, A10.10.3, A.12.4.2), FedRAMP (CM-7, RA-5, AU-2, AU-5, AU-6, AU-9), Common Criteria (CC 3.2–3.4, 4.2, 5.1, 5.2, 6.1, 7.2, 7.3).
Экспорт событий в SIEM-систему	Эта функция пригодится компаниям, которые используют SIEM-систему и хотят собирать в ней события систем безопасности виртуальных и облачных рабочих мест.
Режим «Запрет по умолчанию»	Компании, которым требуется более строгая защита, могут ввести режим «Запрет по умолчанию» для всех приложений. Контроль программ в режиме «Запрет по умолчанию» в сочетании с мониторингом целостности файлов обеспечивает всестороннюю безопасность базового уровня.
Сокращение поверхности атаки	Технологии оценки уязвимостей и управления установкой исправлений позволяют уменьшить поверхность атаки и сократить временные затраты на управление программами.
Дополнительная защита сети для VMware NSX	Если компания использует платформу VMware и стремится максимально усилить защиту сети, ей пригодится инструмент IDS/IPS нового поколения для VMware NSX.

Цифровая трансформация без границ

Цифровая трансформация открывает множество возможностей для бизнеса, но на этом пути компанию могут ждать серьезные трудности. Выберите уровень Kaspersky Security для виртуальных и облачных сред, который отвечает вашим потребностям, чтобы переход к новой бизнес-модели был максимально комфортным. Имейте в виду, что уровень Enterprise позволит воспользоваться дополнительными преимуществами цифровой трансформации.

www.kaspersky.ru

www.securelist.ru