Kaspersky
Cloud Workload
Security

Ноябрь'24

Kaspersky Cloud Workload Security

kaspersky активируй будущее

>90%

организаций используют тот или иной тип облачных сред*

84%

организаций используют контейнеры в различных средах**

72%

компаний используют гибридные облачные среды***

Согласно оценкам компании Frost & Sullivan, рынок IT-безопасности облачных нагрузок вырастет с $3 млрд долларов США в 2022 году до $9,8 млрд в 2027 году со среднегодовым темпом прироста 26,3%.

Переход в облако: преимущества и риски

Ускорение процессов

Сокращение издержек

Рост производительности

Новые риски безопасности

Миграция в облака и использование технологий контейнеризации являются важным компонентом успешного развития бизнеса любого типа. Это справедливо даже для компаний, работающих в очень регулируемых и закрытых сферах деятельности. Но чем больше рабочих нагрузок переносится в облако, тем более сложной, менее контролируемой и прозрачной становится вся облачная инфраструктура. Этот переход несет в себе новые риски, так как обеспечение кибербезопасности не всегда поспевает за трансформацией бизнеса.

Чтобы обеспечить надежную защиту критически важных для бизнеса сервисов, современные компании обычно применяют гибридный подход, когда локальные инфраструктуры сочетаются в различных комбинациях с частными и публичными облачными инфраструктурами.

При этом гибридные облачные среды отличаются от физических, поэтому традиционные средства киберзащиты, такие как EPP-платформы, совсем не так эффективны. Необходимо, чтобы такие решения действовали в связке со специализированными средствами защиты облачных нагрузок.

Возьмите курс на облачную безопасность

Kaspersky Cloud Workload Security (Kaspersky CWS) — решение для комплексной кибербезопасности облачных инфраструктур и сред разработки. Оно защищает от широкого спектра угроз: от вредоносного ПО и фишинга до контейнеров с наличием уязвимостей в рантайме.

Решение защищает:

- хосты
- виртуальные машины
- компоненты публичных и частных облаков
- контейнеры
- оркестраторы
- другие компоненты гибридной облачной и контейнерной инфраструктуры

Решение гибко лицензируется и готово легко встроиться в вашу систему кибербезопасности. Kaspersky CWS оптимально подходит для компаний с распределенной и сложной IT-инфраструктурой.

* AAG. The Latest Cloud Computing Statistics, 2023
** CNCF. Annual Survey, 2024
*** Flexera. State of the Cloud Report, 2023

Что Kaspersky CWS даёт вашей компании?

Для бизнеса

- Уменьшение затрат
- Снижение рисков
- Ускорение бизнес-процессов
- Повышение эффективности
- Соответствие указу Президента № 250 об импортозамещении

Для ИБ-команд

- Защита облачных рабочих нагрузок, приложений и сервисов
- Повышение прозрачности процессов
- Оптимизация управления рисками
- Поддержка соответствия нормативным требованиям

Для ИТ-команд

- Оптимизация вычислительных ресурсов в гибридных облаках
- Увеличение производительности инфраструктуры
- Повышение прозрачности всей инфраструктуры
- Снижение количества ИТ-инцидентов

Для команд разработки

- Ускорение вывода продукции на рынок
- Прозрачная инвентаризация ресурсов
- Экономия времени благодаря автоматизации
- Повышение надежности приложений и сервисов

Ключевые особенности

Защита, на которую можно положиться

Kaspersky Cloud Workload Security обеспечивает надежную защиту облачных сред и предлагает высококачественную техническую поддержку по принципу «одного окна». Kaspersky CWS интегрируется с другими решениями «Лаборатории Касперского» для всеобъемлющей защиты вашей инфраструктуры

Специализированное решение для защиты облачных рабочих нагрузок

Решение учитывает особенности работы в облачных, виртуальных и контейнерных средах, обеспечивая защиту от специфических для них киберрисков. Kaspersky CWS содержит такие инструменты, как, например, легкий агент для защиты виртуальных сред и VDI, поведенческий анализ контейнеров, и другие

Универсальное решение для разных типов инфраструктуры

Выбирайте только нужные вам возможности по защите всех рабочих нагрузок – физических, виртуальных или контейнерных, независимо от того, где они развернуты (частные, публичные или гибридные облака)

Экономия ресурсов для сложных инфраструктур

Уникальные технологии позволяют сэкономить до 30% виртуальных вычислительных ресурсов при защите частных облаков и избежать снижения производительности кластера

Быстрые и качественные проверки на безопасность

Kaspersky Cloud Workload Security помогает прогнозировать время выхода приложений на рынок за счет автоматизации проверок на соответствие требованиям и нормам безопасности

Соблюдение требований регуляторов

Kaspersky Cloud Workload Security позволяет обеспечивать высокий уровень безопасности и соответствие необходимым нормам и стандартам, благодаря широкому инструментарию проверок, включая аудит на соответствие лучшим практикам и проверки собственного состояния

Компоненты решения

Kaspersky Cloud Workload Security состоит из двух продуктов — Kaspersky Security для виртуальных и облачных сред и Kaspersky Container Security. В будущем в решение будут добавлены функции управления средствами безопасности в облаке (CSPM).

Kaspersky Security для виртуальных и облачных сред

Kaspersky Security для виртуальных и облачных сред защищает гибридную инфраструктуру от широкого спектра кибератак, экономя при этом ресурсы.

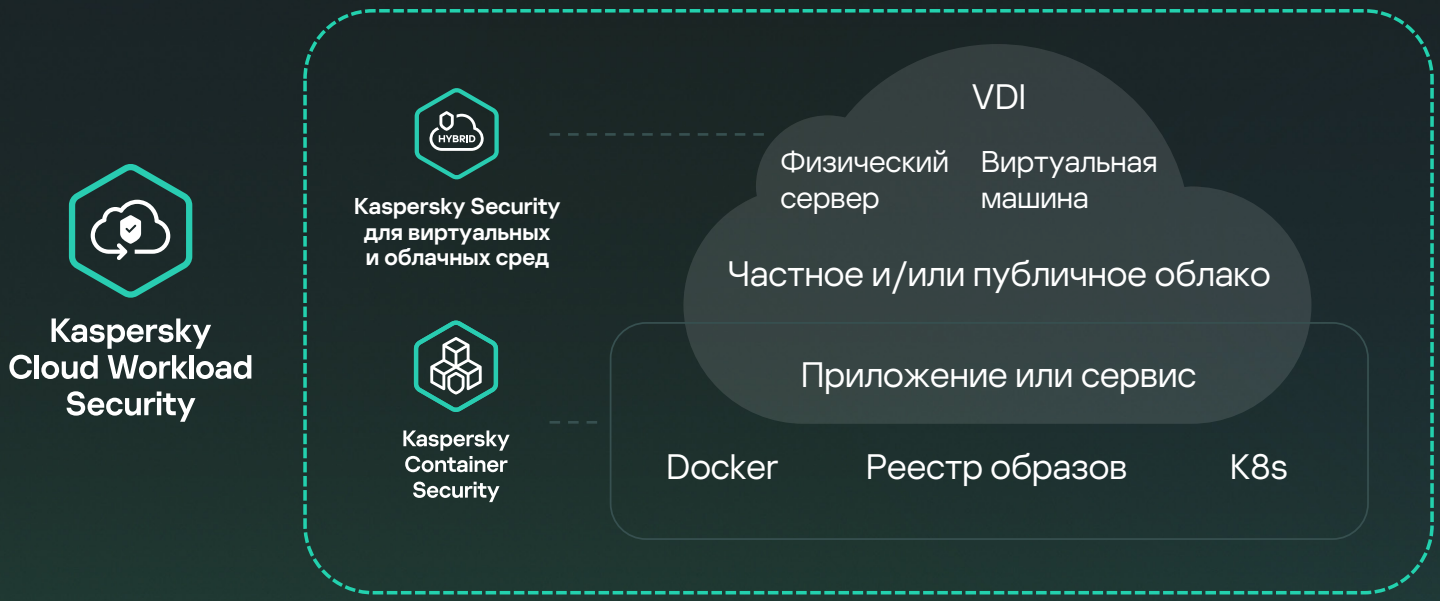
- Многоуровневая защита гибридного облака от киберугроз
- Повышение надежности и устойчивости инфраструктуры
- Широкий набор инструментов для обеспечения соответствия нормативным требованиям
- Визуализация процессов в облаке

Kaspersky Container Security

Kaspersky Container Security комплексно защищает контейнерные приложения на всех этапах их жизненного цикла, от разработки до эксплуатации.

- Интеграция в процесс разработки
- Защита оркестратора
- Проверка на соблюдение требований регуляторов
- Визуализация и инвентаризация ресурсов кластера

Архитектура решения



Система управления состоянием безопасности облака (CSPM) (в перспективе)

Совместимость

Kaspersky Security для виртуальных и облачных сред

Публичные облачные платформы

AWS, Microsoft Azure, Google Cloud, Yandex Cloud, а также возможность интеграции с другими публичными облачными службами и MSP-провайдерами.

aws
Yandex Cloud
Google Cloud
Microsoft Azure

Платформы виртуализации

На базе VMware, KVM, RHEL и других

vmware
Red Hat Enterprise Linux
KVM

Инфраструктура виртуальных рабочих столов (VDI)

VMware Horizon, Termidesk VDI, Citrix Virtual Apps and Desktops

vmware
TERMIDESK
citrix

Kaspersky Container Security

Оркестраторы

Kubernetes, OpenShift, Deckhouse

kubernetes
OPENSHIFT
Deckhouse Kubernetes Platform

Реестры образов

Docker hub, Harbor, jFrog, Nexus

dockerhub
HARBOR
JFrog
nexus repository

Платформы CI/CD

Jenkins, TeamCity, GitLab, CircleCI

Jenkins
TeamCity
GitLab
circleci

Лицензирование

Kaspersky Cloud Workload Security состоит из двух продуктов с отдельным лицензированием для каждого из них. Это дает возможность использовать только нужные вам возможности обеих продуктов.

Kaspersky Security для виртуальных и облачных сред

Standard

Фундаментальная защита гибридных облачных сред

Kaspersky Security для виртуальных и облачных сред

Enterprise

Всобъемлющая защита гибридных облачных сред и соблюдение требований регуляторов

Kaspersky Container Security

Standard

Безопасность образов

Kaspersky Container Security

Advanced

Защита в рантайме и соответствие требованиям регуляторов

Примеры вариантов лицензирования

Примеры сочетания продуктов		Kaspersky Security для виртуальных и облачных сред		Kaspersky Container Security	
Уровень защиты		**Standard**	**Enterprise**	**Standard**	**Advanced**
		Фундаментальная защита гибридных сред	Standard + Всеобъемлющая защита гибридных облачных сред и соответствие требованиям	Безопасность образов контейнеров	Standard + Защита в среде выполнения и соответствие требованиям
Вариант 1	Базовая защита ВМ	•	•		
	Защита образов контейнеров			•	•
Вариант 2	Базовая защита ВМ	•	•		
	Защита контейнеров в среде выполнения				•
Вариант 3	Продвинутая защита ВМ		•		
	Защита образов контейнеров			•	•
Вариант 4	Продвинутая защита ВМ		•		
	Защита контейнеров в среде выполнения				•

Преимущества для бизнеса

Сокращение затрат

- Выбирайте и используйте только те возможности, которые необходимы
- Сокращение потребления ресурсов с помощью специальных функций и технологий

Снижение рисков

- Обширный набор функций защиты для мультиоблачных и контейнерных сред
- Соблюдение требований регуляторов для облачных сред и DevOps

Ускорение бизнес-процессов

- Автоматизация проверок безопасности
- Предсказуемое время выпуска приложений на рынок

Увеличение эффективности

- Подход Shift-left
- Полный обзор происходящего в гибридных облачных и контейнерных средах

Почему Kaspersky:

Глобальный охват и международное признание

Доказанная эффективность технологий

Прозрачность и соответствие стандартам

Опыт и знания мирового уровня

Высокий статус в индустрии ИБ

>25 лет безупречной работы

Kaspersky Cloud Workload Security

Узнайте больше

www.kaspersky.ru

#kaspersky
#активируйбудущее