Kaspersky Vulnerability Management

Устраняйте слабые места
в инфраструктуре, пока
они не превратились в инциденты

kaspersky

Не каждая уязвимость критична. Но любая может стать точкой входа.

Количество уязвимостей растет быстрее, чем команды успевают их обрабатывать. Новые CVE появляются ежедневно, критичные исправления откладываются на недели, а ручная приоритизация оставляет командам ИБ слишком мало времени для работы с действительно опасными уязвимостями.

Kaspersky Vulnerability Management

Kaspersky Vulnerability Management помогает перейти от разрозненного сканирования к управляемому процессу: с видимостью активов, регулярным поиском уязвимостей, проверкой конфигураций, патч-менеджментом и контролем устранения.

Решение помогает командам видеть реальные риски, быстрее устранять критичные слабые места и снижать нагрузку на специалистов без усложнения инфраструктуры.

До 44% кибератак

начинаются с эксплуатации известных уязвимостей.[1]

Около 50 000 новых CVE

(Common Vulnerabilities and Exposures) было зарегистрировано в 2025 году.[2]

~40–55 дней

составляет среднее время устранения критичных уязвимостей (MTTR — Mean Time To Remediate), что оставляет инфраструктуру открытой для атак.[3]

Найти уязвимости — только начало. **Главное — понять, какие из них создают реальный риск, где они находятся и устранены ли они до того, как ими воспользуются атакующие.**

Видеть активы. Приоритизировать риски. Устранять уязвимости.

1

Уберите слепые зоны в инфраструктуре

Невозможно защитить то, что не видно. Kaspersky Vulnerability Management помогает **обнаруживать устройства, операционные системы и установленное ПО в инфраструктуре**, чтобы команды ИБ и ИТ работали с актуальной картиной активов, а не с устаревшими таблицами и неполными списками.

Решение поддерживает агентную и сетевую инвентаризацию, помогая выявлять как управляемые активы, так и устройства без установленного агента.

2

Расширьте покрытие без усложнения инфраструктуры

Регулярное сканирование помогает **выявлять уязвимости на рабочих станциях, серверах и сетевых устройствах.** Агентный подход использует существующие компоненты Kaspersky Endpoint Security, а безагентное сетевое сканирование позволяет проверять порты и сервисы на активах без установленного агента.

Это помогает расширить покрытие инфраструктуры и снизить риск того, что критичная уязвимость останется вне поля зрения.

[1] «Анатомия ландшафта киберугроз», Глобальный отчет Kaspersky Security Services 2026
[2] https://www.cve.org/About/Metrics
[3] Edgescan Vulnerability Statistics Report 2026

3

Не дайте ошибкам конфигурации стать точкой входа

Ошибки конфигурации часто становятся таким же риском, как и незакрытые CVE. Kaspersky Vulnerability Management **помогает проверять параметры конфигурации** на соответствие требованиям безопасности, регуляторным практикам и внутренним политикам.

Поддержка готовых профилей ФСТЭК и возможность использовать предустановленные профили на основе лучших практик помогают упростить контроль соответствия и подготовку данных для аудита.

4

Устраняйте уязвимости, а не просто фиксируйте их в отчетах

Сканер показывает проблему. Но бизнесу нужен результат — устраненный риск. Kaspersky Vulnerability Management помогает встроить патч-менеджмент **в единый процесс управления уязвимостями** и использовать интеграцию с Kaspersky Security Center Linux для управления обновлениями Windows.

Это сокращает разрыв между обнаружением уязвимости и ее фактическим устранением.

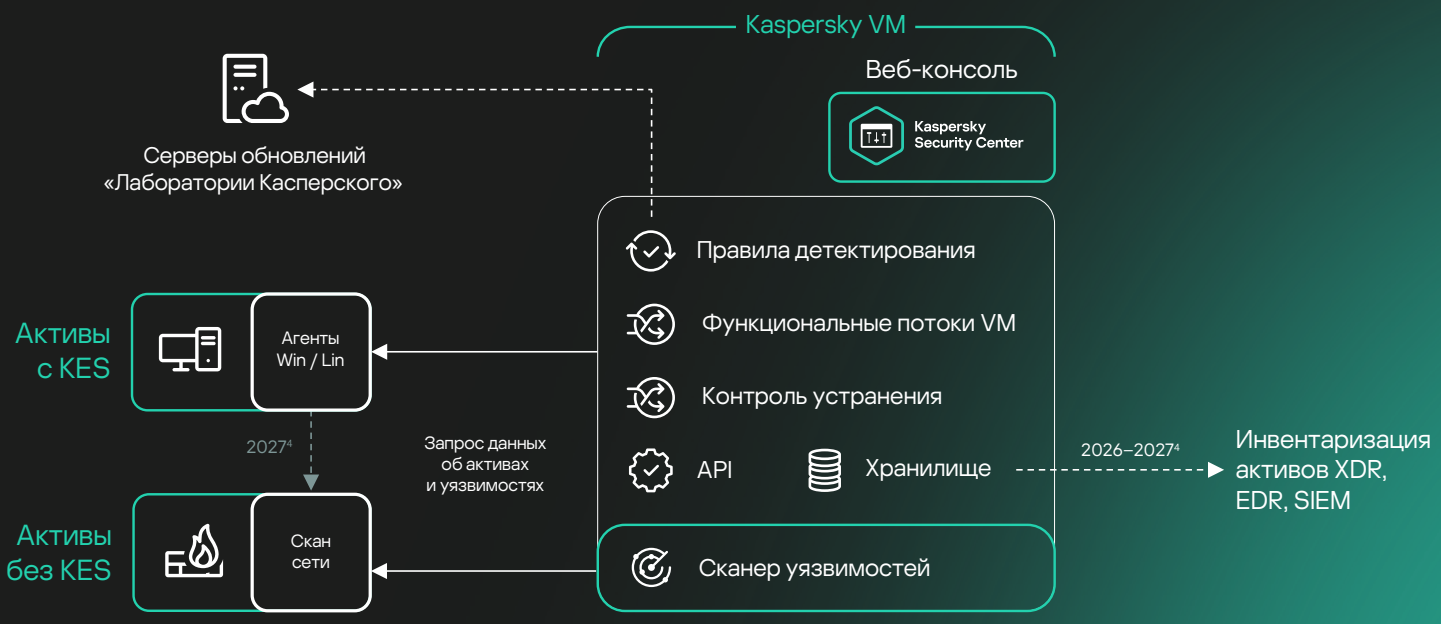
5

Убедитесь, что риск закрыт

После исправления важно подтвердить результат. Решение помогает отслеживать статус устранения уязвимостей: какие риски уже закрыты, какие остаются открытыми и где требуется внимание команд ИБ или ИТ.

Так процесс становится не разовой проверкой, а управляемым циклом: обнаружить, приоритизировать, устранить и подтвердить.

Архитектура и основные компоненты решения



[4] Данный функционал будет доступен не раньше 2027 года

Преимущества для бизнеса

Прозрачность и контроль над активами и уязвимостями организации

Решение помогает поддерживать актуальное представление об инфраструктуре, установленном ПО и связанных с ними уязвимостях.

Ускорение цикла реагирования и сокращение среднего времени устранения уязвимостей

Связка сканирования, патч-менеджмента и контроля устранения помогает быстрее переходить от обнаружения уязвимости к ее закрытию.

Снижение рисков несоответствия регуляторным и отраслевым требованиям

Проверка конфигураций, отчетность и мониторинг устранения помогают подтверждать прогресс по снижению рисков и подготовке к внутренним или внешним проверкам.

Повышение эффективности команд ИБ

Централизованное управление и отчеты уменьшают объем ручной работы и помогают командам ИБ и ИТ фокусироваться на наиболее значимых рисках.

Нативная интеграция с продуктами «Лаборатории Касперского»

Kaspersky Vulnerability Management развивается как часть единой экосистемы решений «Лаборатории Касперского» и позволяет использовать данные об уязвимостях в более широком контексте управления киберрисками.

Возьмите уязвимости под контроль

Узнайте, как Kaspersky Vulnerability Management поможет снизить реальные риски в вашей инфраструктуре.

Kaspersky Vulnerability Management

Подробнее

www.kaspersky.ru

© 2026 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее