



Продвинутая защита
для компаний, использующих
ОС на базе Linux

Решения «Лаборатории Касперского» для Linux

kaspersky активируй
будущее



Kaspersky Endpoint Security for Linux



Linux повсюду

Согласно исследованиям ZDNET, более 90% веб-серверов работают под управлением Linux. Linux также активно используется на персональных компьютерах в организациях, работающих с большими объемами конфиденциальных данных.

[Подробнее](#)

О Linux-системах в двух словах

Первая операционная система с действительно открытым исходным кодом, GNU/Linux (или просто «Linux»), широко применяется в самых разных устройствах — от телефонов и IoT-устройств до обычных персональных компьютеров, серверов и даже суперкомпьютеров. Но Linux — это не какая-то конкретная операционная система, как, например, Windows или MacOS. Она представлена множеством дистрибутивов, предназначенных для выполнения конкретных задач. ОС Linux нечасто встречается в персональных компьютерах. Однако в корпоративной среде она представлена весьма обширно.

Широкое использование и рост популярности привели к тому, что Linux стала крайне привлекательной мишенью для атак. Чтобы быть на шаг впереди, киберпреступники вкладывают все больше средств в поиск новых способов эксплуатации уязвимостей, проникновения и получения контроля над ОС.

Рост угроз для Linux

Тенденция последних лет — активное внедрение систем на базе Linux в рамках импортозамещения, а также значительный рост запросов на защиту отечественных Linux-систем.

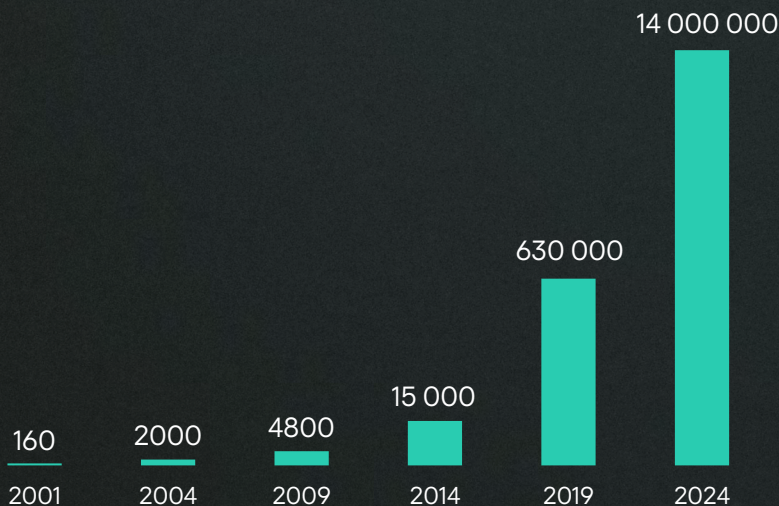
Еще 10-20 лет назад угрозы для Linux встречались относительно редко. Киберпреступники в первую очередь фокусировались на Windows из-за ее большей распространенности на персональных компьютерах.

Сейчас злоумышленники активно разрабатывают вредоносное ПО для Linux, в том числе увеличивается количество вредоносных программ и число продвинутых угроз (APT). Растущее распространение облачных вычислений и технологий контейнеризации еще больше усложняет защиту систем от этих угроз. **Угрозы для ОС Linux перешли из разряда нишевых и редких в разряд изоощренных и распространенных.**

Показатель	Раньше	Сейчас
Количество угроз	Малое	Большое, зачастую со сложными векторами атак
Цели	Серверы, малые среды	Облака, контейнеры, IoT, КИИ, встраиваемые системы
Вредоносное ПО	Простые троянцы, базовые руткит-технологии	APT-угрозы, продвинутые троянцы
APT-группы	Участвуют редко	Часто рассматривают Linux-системы в качестве мишеней
Эксплойты	Пароли по умолчанию, неисправленные уязвимости ядра	Уязвимости нулевого дня, выход за границы контейнера
Защитные меры	Базовый антивирус, ручной аудит	EPP-, EDR-решения, средства защиты для встраиваемых систем и контейнеров



Количество вредоносных файлов для Linux (в нашей коллекции)



Актуальные угрозы



Вымогатели



Майнеры



Уязвимости



Вредоносное ПО с IoT



Целевые атаки

Инцидент с XZ Utils

Атака на цепочку поставок с использованием зараженных троянцами версий 5.6.0 и 5.6.1 архиватора XZ Utils позволила выявить уязвимость CVE-2024-3094, затрагивающую SSH-серверы Linux, а также несколько популярных сборок Linux, выпущенных в марте 2024 года. В перспективе это могло бы стать самой масштабной атакой на экосистему Linux за всю ее историю. А все потому, что целью оказались в первую очередь SSH-серверы — основной инструмент удаленного управления всеми Linux-серверами в интернете.

[Подробнее](#)

Защита сред Linux

«Все обойдется», «я не интересен как мишень», — именно на такое отношение потенциальных жертв и делают ставку киберпреступники. В условиях быстро меняющегося ландшафта угроз важно пересматривать системы безопасности всех сред Linux и вносить в них изменения по мере необходимости.

В отличие от большинства поставщиков продуктов в области кибербезопасности, «Лаборатория Касперского» уже давно предлагает решения для защиты Linux. Мы прекрасно осознаем, что фраза «сравнительно безопасно» никогда не значила «достаточно безопасно» и что сейчас, когда Linux находится в зоне повышенного внимания со стороны злоумышленников и хактивистов, наличие надежной и интеллектуальной защиты является критически важным фактором.

Решения «Лаборатории Касперского» для систем на базе Linux обеспечивают комплексную защиту и разработаны с учетом уникальных задач и требований таких сред. Наши решения предлагают **следующие возможности:**

1

Обнаружение на основе статического анализа с применением ИИ

2

Обнаружение на основе данных о поведении, с использованием ИИ-технологий

3

Обнаружение комплексных атак с помощью кросс-продуктовых сценариев

4

Укрепление системы (system hardening)

5

Обнаружение сетевых угроз

6

Мгновенная доставка информации о новых угрозах из облака

Решения «Лаборатории Касперского» для Linux

Решения по защите периметра



Kaspersky
Security
для бизнеса

В релизе 12.3 Kaspersky Endpoint Security доступна технология Universal Linux Kernel Module (ULKM). Ознакомиться с ней подробнее можно в конце даташита

Kaspersky Security для бизнеса является совместимой с Linux линейкой решений для защиты рабочих мест на основе передовых EPP-технологий «Лаборатории Касперского», блокирующих большинство массовых угроз в автоматизированном режиме и собирающих информацию со всех конечных устройств.

В рамках линейки Kaspersky Security для бизнеса работает **Kaspersky Endpoint Security для Linux** — приложение, которое устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации и находящиеся под управлением операционных систем Linux. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами.

Kaspersky EDR для бизнеса Оптимальный — один из уровней Kaspersky Security для бизнеса — объединяет новейшие технологии защиты рабочих мест и гибкие инструменты контроля с базовыми технологиями EDR, что позволяет своевременно реагировать на современные угрозы в автоматическом или полуавтоматическом режиме. Благодаря управлению всеми функциями из единой консоли и автоматизированным инструментам, решение повышает прозрачность инфраструктуры и экономит время администраторов. Начиная с версии Kaspersky EDR для бизнеса Оптимальный 3.0, базовые функции EDR стали доступны не только для Windows, но и для Linux.

Управление защитой



Kaspersky
Security Center

Консоль Kaspersky Security Center Linux (KSC для Linux) предназначена для развертывания и управления защитой устройств с операционной системой Linux. Kaspersky Security Center Linux позволяет вам устанавливать программы безопасности «Лаборатории Касперского» на устройства в корпоративной сети, удаленно запускать задачи проверки и обновления, регулировать политики безопасности управляемых программ. Она обеспечивает защиту всей корпоративной среды, включая облачные, физические и виртуальные машины, а также мобильные устройства. В частности, вы можете управлять защитой устройств Android- и iOS, доступной в **решении Kaspersky Secure Mobility Management**, из веб-консоли Kaspersky Security Center для Linux.

Продвинутые решения



**Kaspersky
Anti Targeted
Attack**

Kaspersky Anti Targeted Attack представляет платформу для анализа сетевого трафика и комплексной защиты от сложных угроз и целевых атак. Решение позволяет контролировать точки входа потенциальных угроз (сеть, веб-трафик, электронная почта) и предоставляет возможность проверять потенциально вредоносные объекты в песочнице. Kaspersky Anti Targeted Attack Platform поддерживает операционную систему Astra Linux.



**Kaspersky
EDR Expert**

Kaspersky EDR Expert является мощной системой информационной безопасности, которая предоставляет специалистам ИБ полную картину событий в инфраструктуре рабочих мест и серверов и обеспечивает их эффективную защиту от сложных угроз и АPT-атак. Благодаря интеграции с работающим на Linux агентом Kaspersky Endpoint Security, обеспечивается высокая детализация при отслеживании событий и обеспечение эффективного сдерживания угроз.

Решения для центров мониторинга и реагирования (SOC)



**Kaspersky
Unified Monitoring
and Analysis Platform**

Kaspersky Unified Monitoring and Analysis Platform (KUMA) — высокопроизводительное решение класса SIEM российского производства, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и своевременной их нейтрализации. Решение совместимо с ОС Linux.



**Kaspersky
Symphony
XDR**

Kaspersky Symphony XDR — комплексное решение, защищающее ИТ-инфраструктуру от широкого спектра киберугроз, в том числе наиболее скрытных, которые сложно обнаружить с помощью решений класса EPP. Решение обеспечивает полную видимость, корреляцию и автоматизацию, используя широкий спектр инструментов реагирования и источников данных, включая активы конечных точек, данные сети и облачного окружения. Symphony XDR может управляться с Linux-устройств, а также защищать их.

Специализированные решения



**Kaspersky
Embedded Systems
Security**

В решении Kaspersky Embedded Systems Security реализован многоуровневый подход, который обеспечивает эффективную защиту для Linux с учетом специфики использования конкретных типов встраиваемых систем. Риск прямых атак на установленные в общественных местах устройства со встраиваемыми системами снижается благодаря эффективным механизмам автоматической защиты на уровне приложения и контролю целостности файлов.



**Kaspersky
Industrial CyberSecurity
for Nodes**

Kaspersky Industrial CyberSecurity for Linux Nodes осуществляет защиту устройств под управлением операционных систем Linux от вредоносного программного обеспечения для компьютеров с встроенной CS EDR функциональностью. Приложение можно интегрировать с решением Kaspersky Managed Detection and Response (MDR), что обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию, а также с Kaspersky Industrial CyberSecurity for Networks.

Решения по защите инфраструктуры



**Kaspersky
Security для
почтовых серверов**

Kaspersky Security для Linux Mail Server обеспечивает надежную защиту почтовых систем на базе Linux с помощью облачных технологий. Для защиты электронной почты и вложений используются элементы ИИ, эмуляционная песочница и облачная репутационная система. При этом достигается высокая точность и минимальное количество ложных срабатываний.



**Kaspersky
Security для виртуальных
и облачных сред**

Kaspersky Security для виртуальных и облачных сред обеспечивает защиту для DevOps, позволяя интегрировать систему безопасности в платформы CI/CD и контейнеры, а также сканировать образы на предмет атак на цепочки поставок. Где бы вы ни развернули рабочие нагрузки — на физических или виртуальных серверах, в частном, публичном или гибридном облаке, — Kaspersky Security для виртуальных и облачных сред обеспечивает безопасность вашей гибридной инфраструктуры.



**Kaspersky
Container
Security**

Kaspersky Container Security — решение, обеспечивающее безопасность сред, использующих контейнеризацию на всех этапах жизненного цикла: от разработки до эксплуатации. Kaspersky Container Security позволяет защитить бизнес-процессы организации, соответствовать стандартам и нормам безопасности, а также реализовать принцип безопасной разработки ПО (DevSecOps). Решение поддерживает отечественные ОС на базе Linux: Astra Linux и RedOS.

Технология ULKM в KES для Linux 12.3

Linux представляет собой не единую систему, а множество семейств дистрибутивов. С одной стороны, это позволяет конечным пользователям выбирать дистрибутив Linux под решение конкретных задач, но, с другой стороны, приводит к отсутствию единого механизма мониторинга событий безопасности.

В зависимости от дистрибутива и его версии различные возможности мониторинга имеют следующие особенности:

1

Доступны только с относительно новых версий ядра

2

Не предоставляют достаточного уровня детализации событий

3

Не предусматривают одновременного конфигурирования и использования двумя и более потребителями

4

Не предоставляют возможности синхронной обработки событий

5

При активном использовании могут оказывать серьезное влияние на производительность всей системы

Технология Universal Linux Kernel Module (ULKM) решает эти проблемы и в разы уменьшает влияние на производительность системы. Это значительно снижает влияние продукта на быстродействие высоконагруженных серверов и повышает защищенность системы за счёт расширенных возможностей по мониторингу угроз.

Технология автоматической защиты от эксплойтов (АЕР)

является одной из важнейших компонент системы детектирования угроз на основе поведения, созданной в «Лаборатории Касперского». АЕР разработана для борьбы с вредоносными программами, эксплуатирующими уязвимости программного обеспечения. Она обеспечивает дополнительный уровень защиты для наиболее часто атакуемых программ и технологий путём эффективного и неинтрузивного выявления и блокирования как известных, так и неизвестных эксплойтов.

Благодаря ULKM осуществляется **защита от эксплуатации уязвимостей** (входит в ТОП3 угроз для Linux), прикрывая один из основных векторов атаки и достигая паритета с KES for Windows в этом отношении.

АЕР включает защитные механизмы против большинства методов атак на Linux, которые применяются в эксплойтах, например, **Dynamic Linker Hijacking, Reflective Code Loading, Heap Spray Allocation, Stack Pivot** и другие.

[Подробнее](#)



Kaspersky Endpoint Security for Linux

Подробнее

www.kaspersky.ru

© 2025 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.

#kaspersky
#активируйбудущее