kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Sandbox

Расширенные возможности для защиты от неизвестных и маскирующихся киберугроз – без привлечения экспертов по IT-безопасности

Сегодня продвинутые кибератаки способны полностью парализовать работу предприятий и нанести ощутимый финансовый и репутационный ущерб. Кража денежных средств и конфиденциальной информации, утеря доверия клиентов из-за недоступности сервисов и другие негативные последствия угроз существенно влияют на стабильность и успешное развитие бизнеса. Сегодня для предотвращения изощренных кибератак недостаточно использовать только традиционные решения, направленные на защиту периметра сети (межсетевые экраны, почтовые и веб-шлюзы, прокси-серверы), а также рабочих станций и серверов (антивирусы и платформы для защиты рабочих мест с базовым функционалом). Современные компании все чаще рассматривают вариант приобретения специализированных средств обнаружения, расследования и реагирования на сложные инциденты.

Кому подходит Kaspersky Sandbox:

- Компаниям, у которых нет специализированного ИБ-отдела
- Небольшим компаниям, которые не готовы выделять дополнительные ресурсы на IT-безопасность
- Крупным организациям с географически распределенной инфраструктурой, не имеющим специалистов по IT-безопасности в филиалах
- Компаниям, которым важно, чтобы штатные ИБ-аналитики были полностью сосредоточены на критичных задачах

Kaspersky Sandbox: эффективное и доступное решение для противодействия сложным угрозам

Вот уже более двадцати лет «Лаборатория Касперского» создает защитные технологии для крупных и малых компаний из разных отраслей и с разным уровнем зрелости ИБ-процессов. Благодаря исследованиям, постоянному развитию и достижениям в области активного поиска угроз, расследования инцидентов и реагирования на них, «Лаборатория Касперского» сохраняет ведущие позиции в борьбе с киберпреступностью.

«Лаборатория Касперского» предлагает ряд продуктов и сервисов для противодействия сложным угрозам:

- Kaspersky Anti Targeted Attack — для обнаружения и расследования изощренных угроз и целевых атак на уровне сети.
- Kaspersky Endpoint Detection and Response — для обнаружения, расследования и устранения сложных киберугроз, направленных на рабочие места и серверы.
- Kaspersky Threat Intelligence Portal – портал, обеспечивающий доступ к облачной песочнице, аналитическим отчетам об APT-атаках и другим сервисам информирования об угрозах.

Чтобы эффективно использовать эти продукты и сервисы, компаниям необходим специализированный, хорошо подготовленный ИБ-отдел. Однако дефицит специалистов, обладающих нужной квалификацией, и, как следствие, высокая стоимость их услуг становятся стоп-фактором для приобретения продуктов, направленных на борьбу со сложными угрозами. Даже если такие специалисты у компании есть, они загружены текущими задачами и высвободить их ресурсы не так просто. Это приводит к незащищенности компаний от сложных угроз.

Решение Kaspersky Sandbox основано на запатентованной технологии* и помогает организациям противостоять комплексным угрозам, способным обходить используемую защиту рабочих мест. Kaspersky Sandbox расширяет возможности Kaspersky Security для бизнеса и позволяет компаниям повысить уровень защищенности рабочих станций и серверов от неизвестного вредоносного ПО, вирусов-шифровальщиков, эксплойтов нулевого дня и других угроз, и все это — без привлечения ИБ-аналитиков.

Это значит, что компаниям больше не придется нанимать или привлекать высокооплачиваемых специалистов. А крупные предприятия с распределенными сетями смогут оптимизировать расходы на защиту удаленных объектов и уменьшить нагрузку на штатных ИБ-аналитиков.

* Номер патента — US 10339301B2

Поставка и развертывание
Решение Kaspersky Sandbox поставляется в виде ISO-образа с предварительно настроенной операционной системой CentOS 7 и всеми необходимыми защитными компонентами. Его можно развернуть как на физическом сервере, так и на виртуальных серверах на базе VMware ESXi.

Интеграция
- SIEM-системы могут получать информацию об угрозах, обнаруженных Kaspersky Sandbox. Она отправляется через Kaspersky Security Center в общем потоке событий.
- В Kaspersky Sandbox реализован API для интеграции с другими решениями. Он позволяет отправлять файлы в Kaspersky Sandbox для сканирования и запрашивать данные об их репутации.

Масштабирование
В базовой конфигурации решение поддерживает до 1000 защищенных рабочих мест и легко масштабируется, обеспечивая непрерывную защиту крупных инфраструктур.

Кластеризация
Несколько серверов можно объединить в кластер для увеличения производительности и повышения доступности.

Как работает Kaspersky Sandbox

В основе Kaspersky Sandbox — экспертные знания в области противостояния сложным угрозам и APT-атакам. Решение тесно интегрировано с Kaspersky Security для бизнеса и тоже управляется через консоль Kaspersky Security Center.

Kaspersky Security для бизнеса запрашивает данные о подозрительном объекте из общего оперативного кеша вердиктов на сервере Kaspersky Sandbox. Если объект уже проверялся, Kaspersky Security для бизнеса получает вердикт и реализует один или несколько вариантов реагирования, таких как:

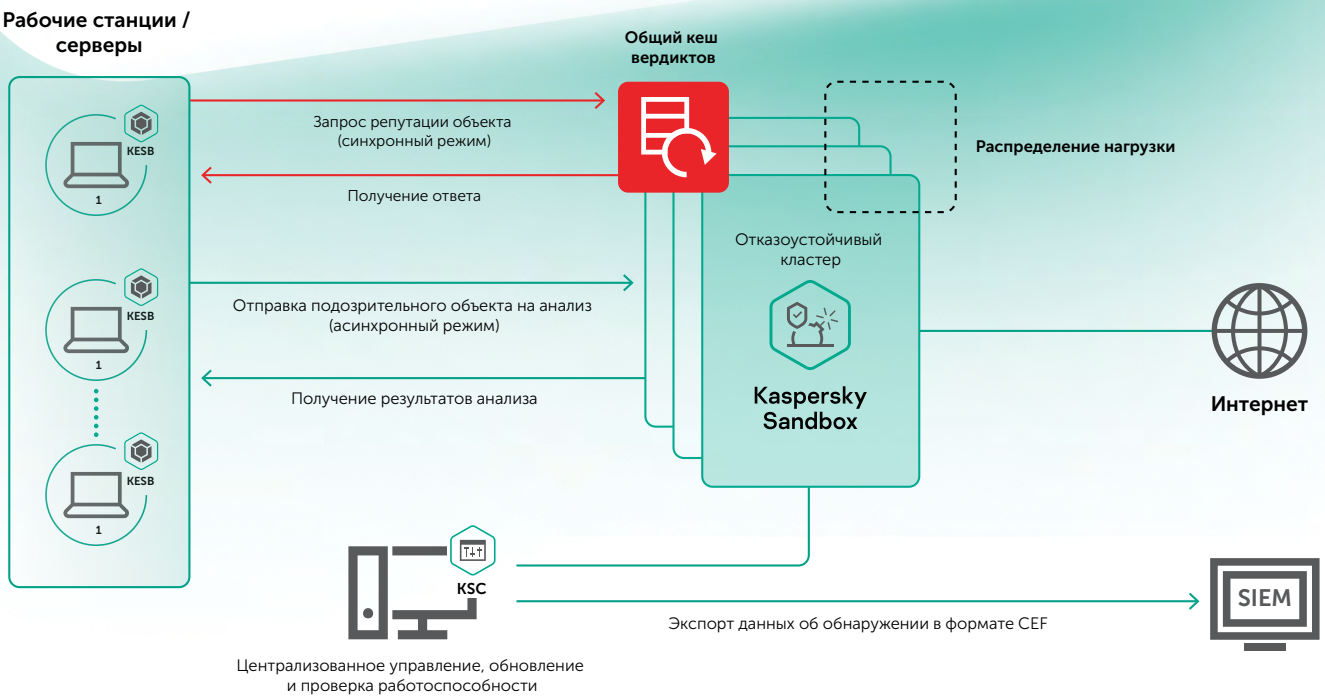
- Удаление и отправка на карантин
- Уведомление пользователя
- Проверка критических областей
- Поиск обнаруженного объекта на других машинах в защищаемой сети

Если вердикт не удается получить из кеша, Kaspersky Security для бизнеса отправляет подозрительный файл в Kaspersky Sandbox и ожидает ответа. Kaspersky Sandbox получает запрос на проверку файла и запускает его в изолированной среде.

Объект сканируется на виртуальной машине, оснащенной инструментами для эмуляции типичной рабочей среды (операционной системы с приложениями). Чтобы определить, является ли объект вредоносным, проводится поведенческий анализ, сбор и обработка артефактов. Если объект совершает вредоносные действия, Kaspersky Sandbox классифицирует его как вредоносное ПО. Таким образом, в ходе анализа в песочнице файлу присваивается вердикт.

Этот вердикт в режиме реального времени отправляется в общий оперативный кеш вердиктов. После этого другие хосты, на которых установлено решение Kaspersky Security для бизнеса, могут быстро получать данные о репутации файла, не проводя его повторный анализ. В результате обеспечивается быстрая обработка подозрительных объектов, снижается нагрузка на серверы Kaspersky Sandbox и повышается скорость и эффективность реагирования на угрозы.

Kaspersky Sandbox – важное дополнение к Kaspersky Security для бизнеса. Оно автоматически блокирует продвинутые, неизвестные и сложные угрозы без привлечения дополнительных ресурсов и позволяет ИБ-аналитикам сосредоточиться на других важных задачах.



www.kaspersky.ru