KASPERSKY lab

ЗАЩИТА ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ ЦОД. КАК ЭТО ДЕЛАТЬ ПРАВИЛЬНО

www.kaspersky.ru

ОСНОВНЫЕ ИДЕИ ДОКУМЕНТА

Парадигма построения корпоративных центров обработки данных (ЦОД) серьезно изменилась и становится все более программно-определяемой. Концепции виртуализации вычислительных нагрузок, успешно применяемые на протяжении последних лет, нашли применение и в других индустриях — например, в виртуализации сетевой инфраструктуры. Технологии виртуализации уже давно стали корпоративным стандартом (аналитика 2016 года показывает проникновение технологий виртуализации в корпоративном сегменте на уровне 75%). Цель этого движения — перевести управление корпоративным ЦОД на тот уровень, чтобы идти не от инфраструктуры, а от бизнес-процессов.

Разумеется, учитывая эти изменения, политики защиты корпоративного ЦОД должны быть пересмотрены — они должны обновляться вместе с обновлением технологий ЦОД, и если ИБ «не поспевает» за инфраструктурой или не умеет оперативно адаптироваться к ее изменениям, то это хороший повод задуматься о том, а не стоит ли сменить средства обеспечения защиты вашего ЦОД на специализированные решения.

При этом всегда следует помнить о том, что проект по построению ЦОД начинался с идеи получить эффективную и производительную площадку для реализации бизнес-задач, так что решения по организации ИБ не должны ни в коем случае влиять на производительность систем в корпоративном ЦОД.

«Лаборатория Касперского» предлагает специализированное решение для защиты корпоративных ЦОД от киберугроз. Являясь частью решения, **Kaspersky Security для виртуальных сред и Kaspersky Securtiy для систем хранения данных** изначально проектировались и создавались с упором на то, чтобы интегрироваться с технологиями, используемыми для построения корпоративных ЦОД, и достичь оптимального ресурсопотребления, чтобы минимизировать любое воздействие на производительность систем, составляющих основу корпоративного ЦОД.

ЧТО ТАКОЕ КОРПОРАТИВНЫЙ ЦОД И ПОЧЕМУ ТАК ВАЖНО ЕГО ЗАЩИЩАТЬ?

В современном мире сложно представить предприятие, которому не нужно обрабатывать, хранить и передавать информацию. И сегодня все это обеспечивается корпоративными центрами обработки данных. Сам корпоративный ЦОД может быть частным или публичным, размещен как на территории самого предприятия или вынесен за его пределы. Но в большинстве случаев ЦОД является куда более сложным объектом, так как зачастую объединяет в себе и частную, и публичную, и территориально распределенную инфраструктуру. В любом случае именно современный центр обработки данных выводит работу компании на новый уровень, позволяя инфраструктуре быстрее следовать за изменениями в бизнесе и эффективнее предоставлять ресурсы для возникающих оперативных задач.

Более 75% компаний уже работают с программно-определяемыми ЦОД, при этом доля проникновения виртуализации в них продолжает расти

Но даже учитывая применение современных технологий для построения корпоративных ЦОД, идеология организации их инфраструктуры остается достаточно традиционной:

- **Инфраструктура обработки данных** — предоставляет вычислительные ресурсы для бизнес-приложений.
- **Инфраструктура хранения данных** — отвечает за хранение данных компании.
- **Сетевая инфраструктура** — помогает без проблем организовать всю связь и потоки данных.

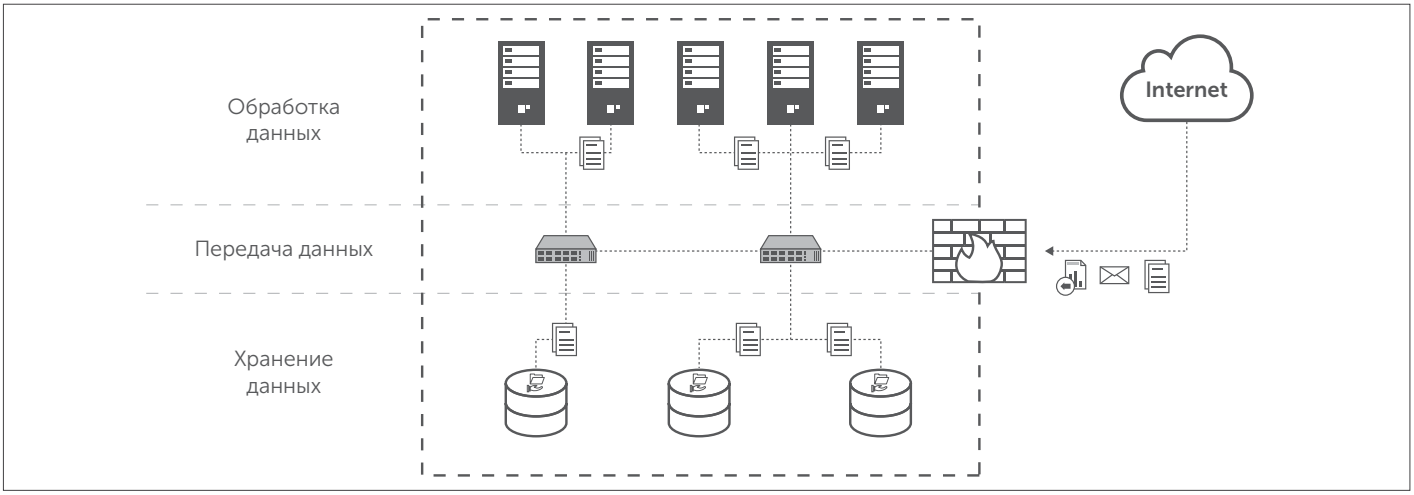


Рис. 1. Верхнеуровневая архитектура центра обработки данных

Все эти компоненты участвуют в обеспечении эффективной работы любого центра обработки данных вне зависимости от того, публичным, частным или гибридным он является.

Сейчас предприятия рассматривают центры обработки данных как инструмент с надежной инфраструктурой и гибко масштабируемыми системами при неизменно высоком уровне производительности и эффективности. При этом организации предъявляют дополнительные требования к центрам обработки данных — им нужно больше ресурсов, больше контроля, больше надежности, больше операционной эффективности и больше безопасности.

Согласно последним исследованиям и опросам, **безопасность инфраструктуры входит в первую тройку аспектов**, наиболее важных как для владельцев центров обработки данных, так и для любых больших предприятий.

Рис. 2. Основные проблемы ЦОД[1]

1 http://www.seagate.com/ru/ru/tech-insights/data-center-management-master-ti/

В то же время в процессе переноса критичных бизнес-систем в корпоративные ЦОД компании все чаще сталкиваются с тем фактом, что существующая концепция организации информационной безопасности должна быть пересмотрена, так как для защиты современного ЦОД она уже не может быть применима.

Суть проблемы кроется в том факте, что технологии, на базе которых строятся современные ЦОД, реализуют новые сценарии взаимодействия пользователей, а также создают дополнительные взаимосвязи между компонентами инфраструктуры.

Парадигма обеспечения безопасности современных ЦОД должна быть пересмотрена с учетом технологий, используемых для их построения

Следует подчеркнуть, что, хотя безопасность становится основным мотивирующим фактором для пересмотра концепции ИБ современных ЦОД, такие вещи, как сохранение производительности систем и удобства управления всей инфраструктурой, все еще остаются важными вопросами для руководителей предприятий.

ЧТО ВАЖНЕЕ ВСЕГО ЗАЩИЩАТЬ В ЦОД

С точки зрения инфраструктуры среда современного центра обработки данных представляет собой довольно простое сочетание нескольких систем.

- **Инфраструктура обработки данных**, построенная с использованием платформы виртуализации, таких как VMware vSphere, Microsoft Hyper-V, Citrix XenServer или KVM, обеспечивающая размещение виртуальных серверов и рабочих станций.
- **Инфраструктура хранения корпоративных данных**, организуемая чаще всего как комбинация файловых серверов и систем хранения данных, подключаемых напрямую в корпоративную сеть.
- **Сетевая инфраструктура**, обеспечивающая потоки данных и взаимодействие между компонентами инфраструктуры ЦОД, в том числе и виртуализированные сети, построенные, например, на базе технологии VMware NSX.

Все эти компоненты участвуют в обеспечении эффективной работы центра обработки данных. И, разумеется, безопасность каждого из них может оказаться под угрозой.

Средства организации безопасности ЦОД должны «знать» технологии, с которыми они работают

Задача «Лаборатории Касперского» — обеспечивать защиту каждого их этих компонентов, с учетом особенностей конкретных технологий, применяемых для построения ЦОД.

ТРАДИЦИОННОЙ ЗАЩИТЕ НЕ МЕСТО В СОВРЕМЕННОМ ЦОД

Иногда традиционные решения, которые повсеместно используются для защиты физических серверов и рабочих станций, также развертываются и на виртуальных машинах. Но при установке традиционного решения для обеспечения безопасности оно начинает потреблять ресурсы, и критические бизнес-приложения получают меньше мощностей, что тормозит их работу. Безусловно, это будет заметно пользователям и будет их раздражать, так как работа становится менее удобной, а скорость выполнения бизнес-задач снижается.

Виртуализация в ЦОД нужна для эффективного использования ресурсов, и решения по ИБ не должны эту идею губить

- В результате каждая виртуальная машина выполняет полезные, но избыточные в рамках хоста виртуализации задачи: локально хранит и обновляет антивирусные базы, самостоятельно проводит проверку на наличие вредоносного ПО и сама себя защищает от сетевых атак.
- Казалось бы, это обеспечивает надежную защиту каждой отдельно взятой виртуальной машины. Но такой подход к защите излишне нагружает каждую отдельно взятую виртуальную машину, что в конечном итоге складывается в **значительную дополнительную нагрузку на хост виртуализации**, снижая при этом эффективность работы всей инфраструктуры и ее пользователей.
- Шквальная загрузка антивирусных баз на виртуальные машины, а также запуск проверки по расписанию очень серьезно нагружают инфраструктуру ЦОД и образуют «**штормы обновлений**» и «**штормы проверок**».
- Выключение на значительное время виртуальной машины с традиционным антивирусом, ведет к устареванию антивирусных баз, что создает «**окно уязвимости**» для проникновения нового вредоносного ПО и будет являться значительной угрозой для безопасности всего корпоративного ЦОД.
- Более того, традиционный подход также бесполезен для защиты сетевых хранилищ данных и файловых серверов, так как с его помощью не удастся обеспечить **безопасность всех операций с файлами** и придется ограничиться только проверкой файлов, загружаемых с СХД на рабочие станции пользователей, что не позволит защитить сетевые папки от **вирусов-шифровальщиков**.

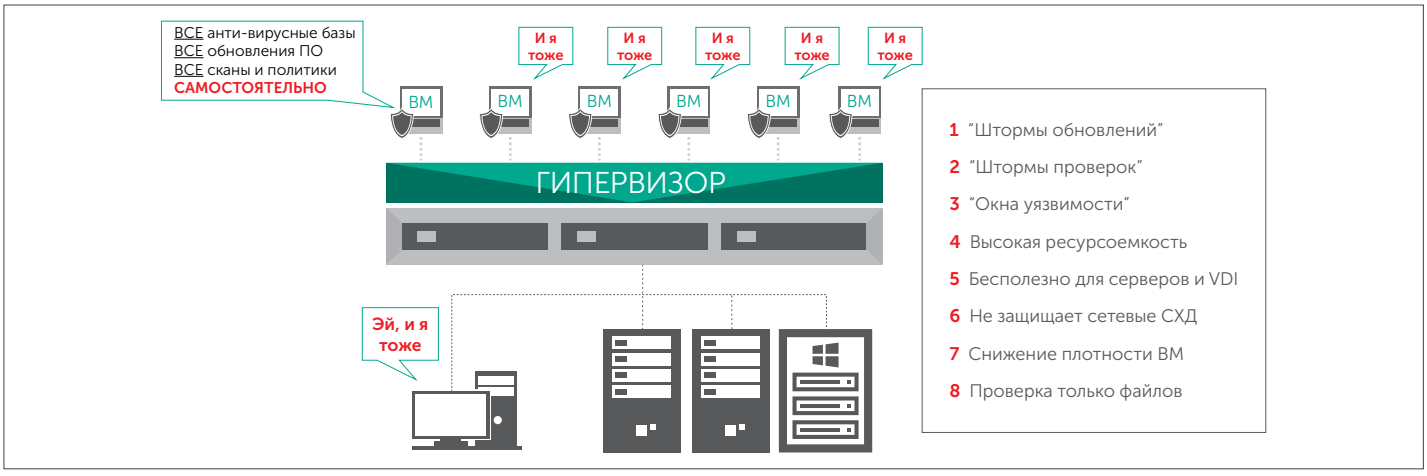


Рис. 3. Минусы традиционных средств обеспечения безопасности

СОВРЕМЕННЫЕ УГРОЗЫ В СОВРЕМЕННЫХ ЦОД

Традиционные решения, установленные для защиты виртуальных инфраструктур, могут разрушить сами инфраструктуры даже без помощи вредоносного ПО, просто серьезно замедляя их работу и не давая IT-системам нормально функционировать, а также создавая неудобства для выполнения бизнес-задач сотрудниками компании.

Исследования передовых компаний из индустрии информационной безопасности, в том числе собственные исследования «Лаборатории Касперского», только подтверждают тот факт, что множество из существующих угроз опасны даже для самых современных ЦОД, если вопросы организации ИБ плохо или совсем не проработаны.

И дело совсем не в том, что технологии современных ЦОД недостаточны для противодействия угрозам. Наоборот, в новых решениях, которые применяются при построении ЦОД, реализуются прекрасные идеи обеспечения защищенности инфраструктуры с использованием, например, политик нулевого доверия на сетевых экранах и методологии микросегментации. Но даже с учетом этого, в обеспечении защиты современных ЦОД от кибератак и вредоносного ПО должны применяться специализированные решения, разработанные специально для виртуальных сред и хранилищ данных и позволяющие обеспечить многоуровневую защиту всего ЦОД.

Вся инфраструктура нуждается в новых способах защиты

Инфраструктуры современных программно-определяемых ЦОД становятся все более сложными, так как они объединяют в себе большое количество систем, ориентированных на выполнение различных бизнес-задач. И чем больше задач, тем больше систем и тем больше многоуровневых связей между системами и их пользователями. Требуется обеспечить надежную защиту всей инфраструктуры без влияния на ее производительность и протекающие в ней бизнес-процессы. Самые совершенные технологии защиты должны работать в нужном месте и в нужное время, вне зависимости от сложности и масштаба инфраструктуры центра обработки данных.

Неконтролируемый рост числа виртуальных машин

В очень крупных инфраструктурах сложно контролировать изменение количества виртуальных машин. Поскольку виртуализация позволяет создавать виртуальные машины на основе шаблонов и клонов, пренебрегать вопросами безопасности недопустимо. Проще говоря, репликация незащищенных или инфицированных виртуальных машин может привести к массовым сбоям и серьезным убыткам для предприятия.

Кибератаки через сети

Большая часть сетевого взаимодействия в виртуализированных инфраструктурах происходит посредством виртуализированных сетей. При этом сетевой трафик и потоки данных редко достигают физического оборудования, установленного для защиты корпоративной сетевой инфраструктуры и ее периметра. Поэтому ни мощные коммутаторы, ни дорогие маршрутизаторы и устройства защиты не обеспечивают полного контроля над виртуализированным центром обработки данных.

Приостановленные виртуальные машины

Каждый раз, когда вы приостанавливаете виртуальную машину или ставите ее на паузу, любое установленное на ней традиционное решение для защиты рабочих мест тут же перестает обновляться. После включения такая виртуальная машина становится слабым звеном цепи информационной безопасности современного ЦОД.

Угроза для «золотых образов» VDI

Виртуализация рабочих столов дает множество преимуществ и повышает эффективность работы. Один «золотой образ» позволяет всего за несколько минут создать сотни виртуализированных рабочих столов. Однако повреждение или заражение «золотого образа» может привести к возникновению сотен опасных виртуальных машин, на которых пользователи могут работать с критическими бизнес-данными.

Хранилища данных под угрозой

Большинство современных сетевых устройств хранения данных (NAS), а также популярные файловые серверы предоставляют расширенные возможности для обеспечения защиты данных. Необходимо дополнительное решение, специально предназначенное для защиты критически важных данных, предпочтительно такое, которое разработано специально для хранилищ данных и не влияет на производительность систем.

Избыточное потребление ресурсов

В основе идеологии построения современных программно-определяемых ЦОД лежит принцип повешения эффективности систем и достижения высокой консолидации вычислительных ресурсов. Установка «тяжелого» решения для защиты создает огромную нагрузку на каждую виртуальную машину и в результате существенно повышает использование ресурсов на хостах виртуализации (гипервизорах). Таким образом, неверно выбранное защитное рещение легко может уничтожить все преимущества, которые бизнес преследовал, начиная проект построения своего собственного современного программно-определяемого ЦОД.

Обобщая вышесказанное, можно смело заявить, что использование старых подходов или недостаточное внимание к организации правильной защиты ЦОД может привести к его выходу из строя и нанести серьезные ущерб бизнесу и репутации.

Многие специалисты по безопасности подтверждают, что описанных выше проблем можно избежать при обеспечении защиты ключевых компонентов (или технологий) программно-определяемого ЦОД — виртуализированной среды обработки и инфраструктуры хранения данных. Более того, для бизнеса крайне важно, чтобы решение для обеспечения безопасности было разработано специально для таких инфраструктур, предусматривало эффективную интеграцию с их основными технологиями и не оказывало отрицательного влияния на работу и производительность систем.

КАК ЗАЩИЩАТЬ КОРПОРАТИВНЫЙ ЦОД

«Лаборатория Касперского» предлагает специализированное решение для защиты современных центров обработки данных, которое обеспечивает защиту и виртуальных сред (виртуализированные серверы и рабочие места), и систем хранения корпоративных данных.

Уникальная архитектура решения разработана с учетом особенностей построения современных ЦОД, минимально воздействует на его производительность и скорость работы систем, тем самым обеспечивая высокую плотность размещения рабочих нагрузок, что увеличивает бизнес-эффективность самого проекта построения корпоративного ЦОД. Важным преимуществом решения является интеграция с технологическими решениями, применяемыми в ЦОД, и централизованное управление из единой консоли — все это помогает администраторам быстрее внедрять политики безопасности.

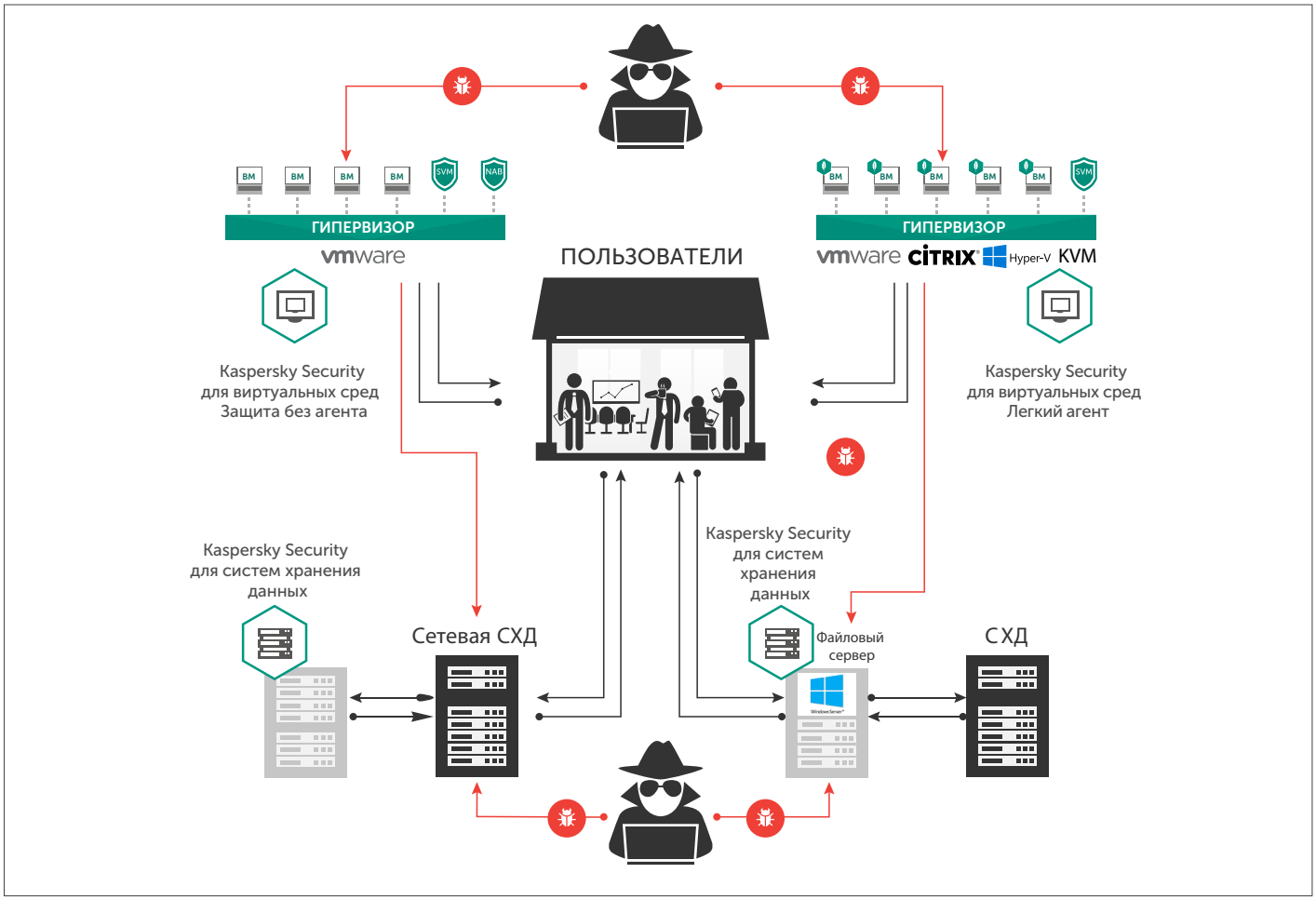


Рис. 4. Архитектура решения Kaspersky Security для виртуальных сред

ИНТЕГРАЦИЯ БЕЗОПАСНОСТИ В ИНФРАСТРУКТУРУ: KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД НА VMWARE VSPHERE И NSX

Платформа VMware vSphere с технологией NSX воспроизводит модель сети на программном уровне, обеспечивая возможность за несколько секунд создать или переконфигурировать сетевую топологию и оперативно внедрить стратегию безопасности ЦОД, основанную на модели нулевого доверия. Совместное решение «Лаборатория Касперского» и VMware делает задачу обеспечения целостной защиты инфраструктуры современного центра обработки данных легко достижимой.

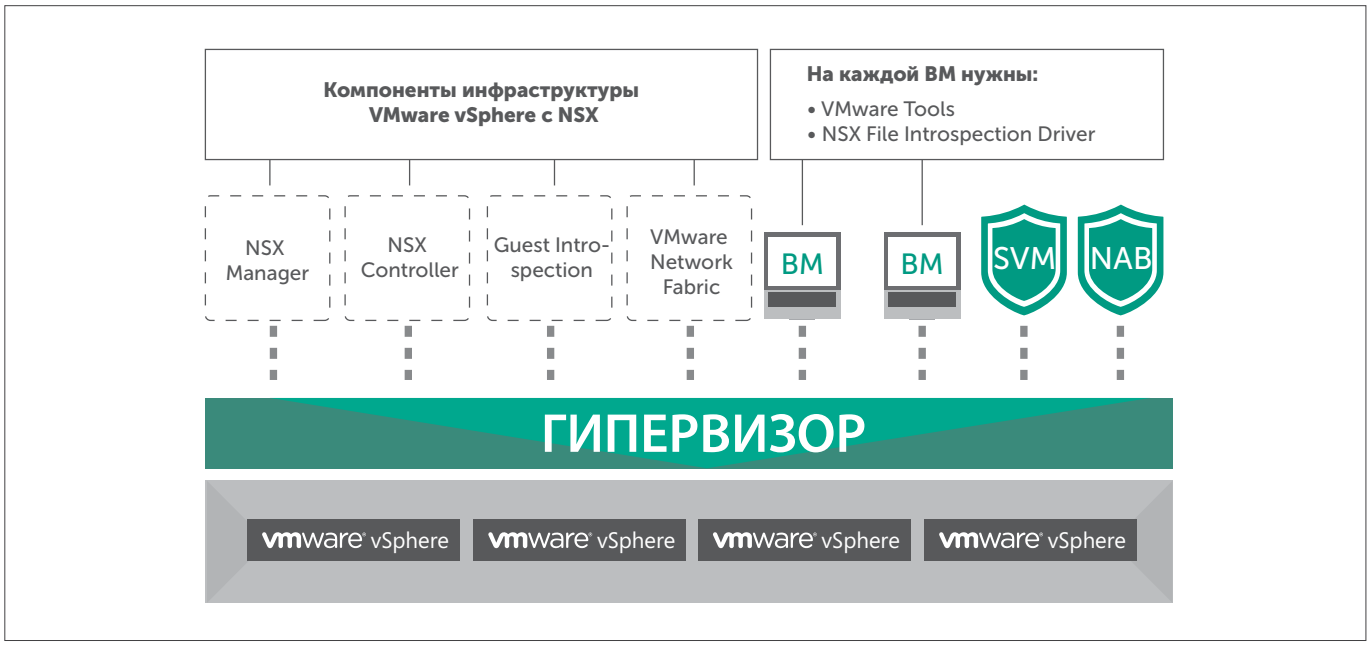
Решение **Kaspersky Security для виртуальных сред Защита без агента** было специально разработано для защиты программно-определяемых ЦОД, построенных на технологиях VMware. Благодаря тому, что не требуется установка никакого дополнительного агента на защищаемые ВМ, а «лишние» для виртуализированной среды процессы вынесены на выделенные устройства защиты, которые обеспечивают проверку файлов и сетевого трафика, воздействие на производительность систем программно-определяемого ЦОД минимально, а каждая ВМ оказывается защищенной сразу же после включения.

В сравнении с традиционными решениями, Kaspersky Security для виртуальных сред Защита без агента потребляет на 40% меньше памяти ВМ и на 80% меньше дискового пространства. Результат – эффективная и безопасная работа бизнес-систем

Решение взаимодействует с инфраструктурой VMware через специализированный API, что позволяет не только обеспечивать защиту каждой виртуальной машины от зловредного ПО, обнаруживать и блокировать сетевые угрозы, но также глубоко интегрироваться с процессами, происходящими внутри самой инфраструктуры.

- **Автоматическое развертывание** в разы упрощает работу ИТ- и ИБ-персонала, позволяя полностью автоматизировать развертывание устройств защиты на гипервизоры, основываясь на политиках безопасности, определенных для каждой ВМ.
- **Тесная интеграция с политиками безопасности** означает, что каждая ВМ теперь получает именно тот функционал защиты, что был предписан корпоративной политикой ИБ.
- **Интеграция с метками безопасности** расширяет границы «общения» инфраструктуры и средств обеспечения ее защиты, чтобы ЦОД мог автоматически и в режиме реального времени реагировать на инциденты ИБ, принимая управленческие решения и перенастраивая топологию сети программно-определяемого ЦОД за считанные секунды.
- **Проверка включенных и выключенных виртуальных машин** также выполняется без агента, поэтому весь корпоративный ЦОД находится под защитой в режиме 24x7.

Архитектура решения изначально создавалась, чтобы минимально воздействовать на работу критически важных серверов и при этом обеспечивать передовые методы защиты.



ПАТЕНТОВАННАЯ ТЕХНОЛОГИЯ ЛЕГКОГО АГЕНТА

Некоторые виртуальные среды, размещаемые в корпоративных ЦОД, не могут похвастаться наличием интеграционных протоколов, позволяющих связать саму инфраструктуру и решение по обеспечению ее защиты, но обеспечивать безопасность такие сред также крайне важно.

Более того, инфраструктуры виртуализированных рабочих столов (VDI, Virtual Desktop Infrastructure) требуют наличия технологий, которые обеспечат каждого пользователя надежной защитой все зависимости от уровня его осведомленности о современных угрозах и методах из профилактики и предотвращения.

Легкий агент контролирует запуск программ и защищает виртуальные рабочие места от вирусов-шифровальщиков и прочих угроз

Kaspersky Security для виртуальных сред Легкий Агент наследует принципы решения без агента, но обеспечивает дополнительные уровни защиты. Решение поддерживает наиболее популярные платформы виртуализации, в том числе VMware vSphere, Microsoft Hyper-V, Citrix XenServer и KVM, а также позволяет каждому виртуализированному рабочему месту получить сбалансированную комбинацию совершенно новых средств защиты и технологий сохранения производительности VDI-платформ, таких как VMware Horizon и Citrix XenDesktop.

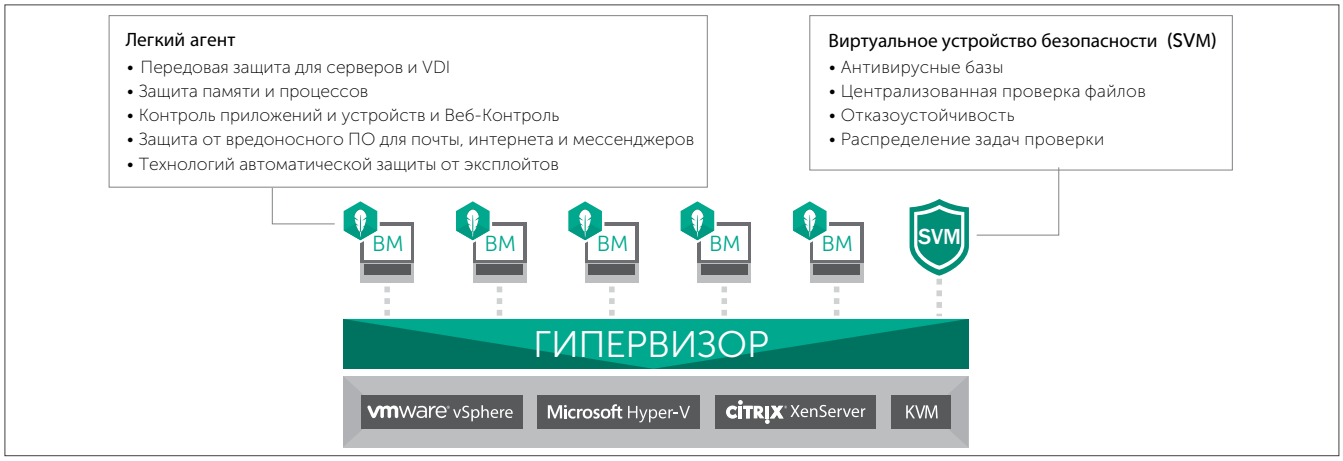


Рис. 6. Принципы работы Легкого агента

Выделенное виртуальное устройство безопасности (SVM, Security Virtual Machine) осуществляет централизованную проверку всех ВМ. В то же время Легкий агент, который устанавливается на каждой ВМ, позволяет выполнять не только проверку файлов, но и сканировать память и процессы. Развертывание Легкого агента на VDI-машины позволяет активировать расширенные функции безопасности, в том числе Контроль запуска приложений, Контроль устройств, URL-контроль, а также эвристические модули анализа трафика электронной почты и интернета. Более того, патентованные технологии защиты, заложенные в основу Легкого агента, позволяют защищать виртуальные рабочие места от сложных атак, в том числе от вирусов-шифровальщиков.

ЗАЩИТА КОРПОРАТИВНЫХ ХРАНИЛИЩ ДАННЫХ В ЦОД

Какими бы совершенными ни были уровни защиты конечных узлов – виртуализированных серверов или рабочих станций – вопросы защиты данных, которые в огромном объеме размещаются в современных корпоративных ЦОД, также должны решаться с применением специализированных средств защиты.

«Лаборатория Касперского» предлагает **Kaspersky Securtiy для систем хранения данных**, которое интегрируется с множеством сетевых СХД корпоративного уровня по протоколам ICAP и RPC, обеспечивая высокоэффективную и масштабируемую защиту каждой файловой операции.

Решение для защиты СХД работает не только с сетевыми СХД, но также защищает файловые серверы

Архитектура решения в сочетании с производительным ядром позволяет свести к нулю потенциальные риски заражения важных корпоративных файлов вредоносным ПО. Не имеет значения, какой пользователь какую файловую активность ведет – все операции будут обработаны антивирусным движком **Kaspersky Securtiy для систем хранения данных**.

Мощное антивирусное ядро, разработанное «Лабораторией Касперского», проверяет каждый файл при его запуске или изменении на наличие всех видов вредоносного ПО, в том числе вирусов, червей и троянцев. Расширенный эвристический анализ позволяет успешно выявлять даже новые и неизвестные угрозы.

В решении реализована гибкая настройка сканирования, которая позволяет создавать так называемые «доверенные зоны», которые могут быть исключены из проверки, наряду с определенными форматами файлов и процессами, такими как резервное копирование.

ЗАЩИТА СОВРЕМЕННЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Традиционные решения, установленные для защиты виртуальных инфраструктур, могут разрушить саму инфраструктуру даже без помощи вредоносного ПО, просто серьезно замедляя ее работу и не давая IT-системам нормально функционировать, а также создавая препятствия для выполнения бизнес-задач.

Учитывая это обстоятельство, в обеспечении защиты современных ЦОД от кибератак и вредоносного ПО должны применяться специализированные решения, разработанные специально для виртуальных сред и хранилищ данных и позволяющие обеспечить многоуровневую защиту всего ЦОД.

«Лаборатория Касперского» предлагает специализированное решение для защиты корпоративных ЦОД от киберугроз. Являясь частью решения, Kaspersky Security для виртуальных сред и Kaspersky Securtiy для систем хранения данных изначально проектировались и создавались с упором на дальнейшую интеграцию с технологиями ЦОД.

Решение обеспечивает защиту каждого компонента программно-определяемого центра обработки данных. При этом сохраняется максимальная эффективность работы систем. Решение поддерживает все ведущие платформы виртуализации, включая VMware vSphere и NSX, Microsoft Hyper-V, Citrix XenServer и KVM.

Решения для защиты крупного бизнеса: kaspersky.ru/enterprise

KASPERSKY lab