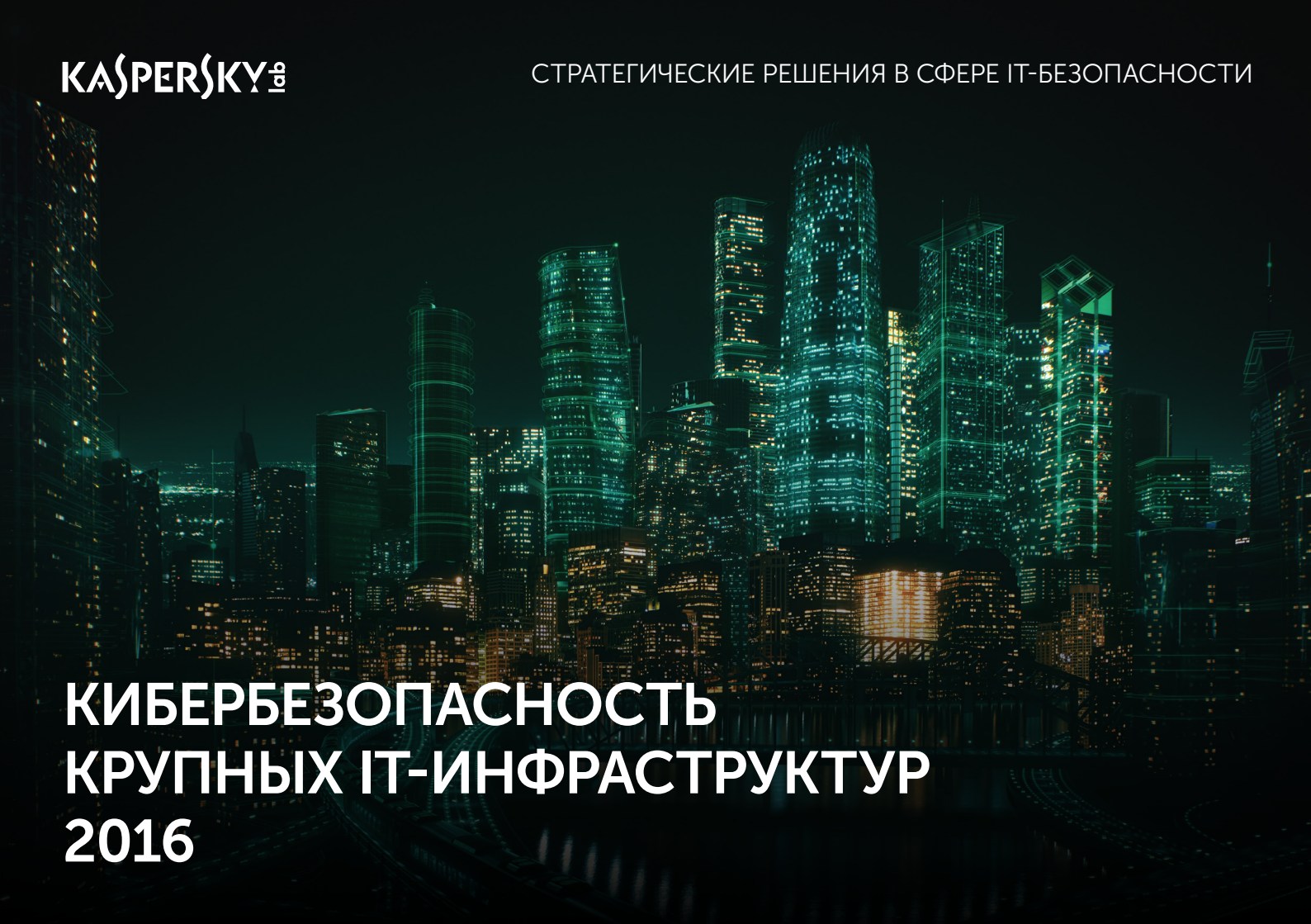
KASPERSKY lab

СТРАТЕГИЧЕСКИЕ РЕШЕНИЯ В СФЕРЕ IT-БЕЗОПАСНОСТИ



КИБЕРБЕЗОПАСНОСТЬ КРУПНЫХ IT-ИНФРАСТРУКТУР 2016

Содержание

ЗАЩИТА IT-ИНФРАСТРУКТУРЫ СЕГОДНЯ — ВАШ ВКЛАД В БЕЗОПАСНОЕ ЗАВТРА

Каждый день миллиарды людей работают с различными данными и передают их через интернет. Обмен информацией между компаниями, их сотрудниками, клиентами и поставщиками происходит непрерывно по всему миру. Это дает бизнесу очевидные преимущества, но одновременно создает дополнительные риски для информационной безопасности компаний.

В ситуации когда ежедневно появляются сотни тысяч новых угроз, растет число целенаправленных атак и глобальных кампаний по кибершпионажу, крупным корпорациям приходится уделять особое внимание усилению системы IT-безопасности. Выбор подходящих решений зависит от сегодняшних и завтрашних рисков, стоящих перед компанией, сложности ее инфраструктуры, уровня требований к защите конфиденциальных данных, необходимости контроля за действиями сотрудников и множества других факторов.

Сегодня, как никогда прежде, крупный бизнес нуждается в защите от киберугроз, которые способны повлиять на критически важные бизнес-процессы, привести к простоям, финансовому и репутационному ущербу. Решения «Лаборатории Касперского» нацелены на борьбу как с существующими, так и ранее неизвестными и сложными угрозами, поэтому оптимально подходят для компаний, нацеленных сохранить непрерывность технологических и бизнес-процессов и предоставлять широкий спектр современных возможностей для сотрудников, клиентов и партнеров.

Принцип нашей работы прост: лучшая экспертиза в сочетании с лучшими технологиями позволяют обеспечить лучшую защиту корпоративной IT-инфраструктуры.

ЗАЩИТА И КОНТРОЛЬ РАБОЧИХ МЕСТ

Защита нового поколения от всех видов киберугроз, нацеленных на устройства сотрудников и пользователей

Хакеры и киберпреступники применяют все более изощренные методы атак против IT-инфраструктур крупных компаний. Без надлежащих средств защиты и управления IT-безопасностью предприятия подвергают себя повышенному риску. При этом большинство кибератак производится при помощи рабочих устройств сотрудников. Надежная защита каждого рабочего места может служить основой для эффективной стратегии в области обеспечения безопасности.

Сегодня рабочее место — это не только стационарный компьютер сотрудника, но и ноутбук, планшет или смартфон, на которых хранятся ценные бизнес-данные и конфиденциальная информация. При таком разнообразии нуждающихся в защите рабочих мест требуется решение, позволяющее централизованно контролировать их безопасность. Оно также должно быть достаточно гибким, чтобы обеспечить поддержку изменений IT-инфраструктуры организации в будущем.

KASPERSKY SECURITY ДЛЯ БИЗНЕСА

Решение Kaspersky Security для бизнеса обеспечивает комплексную защиту всех рабочих устройств. Оно сочетает сигнатурные и облачные технологии, методы эвристического анализа и инструменты проактивного реагирования для создания многоуровневой системы безопасности рабочих станций и мобильных устройств. Технологии защиты дополняются инструментами контроля рабочего места, которые помогают управлять приложениями, контролировать или запрещать использование съемных устройств и применять политики безопасного доступа к интернету.

УРОВНИ KASPERSKY SECURITY ДЛЯ БИЗНЕСА

СТАНДАРТНЫЙ

- IT-безопасность рабочих станций и файловых серверов
- Инструменты контроля рабочих мест
- Контроль и защита мобильных устройств
- Централизованное управление системой защиты
- Защита от программ-вымогателей

РАСШИРЕНННЫЙ

Инструменты уровня СТАНДАРТНЫЙ, а также:

- Средства системного администрирования
- Мониторинг уязвимостей и установка исправлений
- Защита данных с помощью технологий шифрования
- Контроль запуска приложений на серверах

TOTAL

Инструменты уровня РАСШИРЕННЫЙ, а также:

- Защита почтовых серверов
- Защита серверов совместной работы
- Защита интернет-шлюзов

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ

Расширенные средства управления мобильными устройствами и их защитой

По данным «Лаборатории Касперского», в 2015 году продолжился существенный рост количества мобильных вредоносных программ. Их число составило 884 774 — против 295 539 в 2014 году.

Мобильные устройства сегодня все чаще находятся в зоне риска — им угрожает вредоносное ПО, фишинговые сайты, таргетированные атаки. Это тем более опасно, что планшеты и смартфоны являются важным рабочим инструментом почти для каждой компании и на них хранится важная деловая информация. Чтобы защитить эти данные и контролировать широкий диапазон устройств в рамках IT-инфраструктуры, администраторам нужно единое решение.

ПОЛИТИКА BYOD СОЗДАЕТ ДОПОЛНИТЕЛЬНЫЕ РИСКИ

Политика BYOD (использование личных устройств в рабочих целях) становится все популярнее. На личных мобильных устройствах сотрудников хранятся как собственные приложения и данные, так и корпоративные данные и пароли доступа. Это повышает вероятность появления брешей в системе безопасности. Кроме того, мобильные устройства легко потерять и их легко украсть, благодаря чему злоумышленники могут получить несанкционированный доступ к корпоративным системам и данным.

KASPERSKY SECURITY ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Kaspersky Security для мобильных устройств обеспечивает безопасность устройства сотрудника независимо от его местонахождения. Решение защищает устройства от вредоносного ПО и позволяет осуществлять мониторинг и контроль смартфонов и планшетов в корпоративной сети из единого центра с минимальным влиянием на работу пользователей.

- **Защита мобильных устройств**
  Решение обеспечивает многоуровневую защиту от известных и неизвестных угроз, а также помогает удаленно управлять устройством в случае его потери или кражи.
- **Управление мобильными приложениями (MAM)**
  Технологии контейнеризации отделяют корпоративные данные от персональных, а Контроль приложений помогает определить приложения, которые разрешается использовать в корпоративной сети.
- **Управление мобильными устройствами (MDM)**
  Решение предоставляет доступ к функциям управления мобильными устройствами различных платформ из единого интерфейса. Это экономит время сотрудников IT-служб и упрощает применение единых политик безопасности.

ЗАЩИТА ВИРТУАЛЬНЫХ СРЕД

Эффективная защита основных виртуальных платформ

Сегодня типичная виртуальная среда предприятия включает широкий спектр технологий, многие из которых работают под разными гипервизорами. Эта сложная инфраструктура требует защиты от утечек данных и кибератак, тем более что ущерб в результате атак, затронувших виртуальные среды, как правило, оказывается значительным.

Технологии виртуализации повышают эффективность и производительность IT-инфраструктуры. Однако не стоит забывать, что большинство кибератак, которые нацелены на физические компьютеры, могут поражать и виртуальные машины. Риск для виртуальных сред даже выше, поскольку отслеживать работу и взаимодействие каждого из технологических уровней — не так просто. Кроме того, виртуальные среды имеют больше «поверхностей атаки», что активно используют киберпреступники.

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

Специализированное решение для защиты виртуальной инфраструктуры на базе VMware® vSphere®, Microsoft® Hyper-V®, Citrix® Xen® и KVM и обеспечения ее высокой производительности.

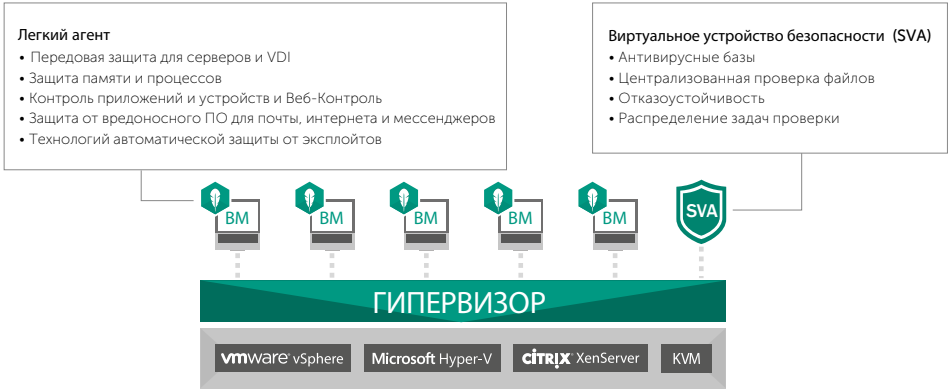
Источник: Исследование рисков IT-безопасности «Лаборатория Касперского» и B2B International 2015

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД — ЭТО:

- Централизованная защита виртуальных машин (ВМ) с помощью виртуального устройства безопасности
- Полноценная защита от вредоносного ПО с использованием облачных технологий
- Персональный сетевой экран и система предотвращения вторжений (HIPS)
- Контроль приложений, веб-ресурсов и периферийных устройств
- Проверка IM-сообщений, почтовый и веб-антивирус
- Централизованное управление через Kaspersky Security Center

Kaspersky Security для виртуальных сред может лицензироваться двумя способами, в зависимости от потребностей компании и особенностей виртуальной инфраструктуры: по количеству виртуальных рабочих станций и серверов или по количеству ядер физических процессоров хост-сервера.

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД
Конфигурация с установкой Легкого агента



ЗАЩИТА БЕЗ УСТАНОВКИ АГЕНТА

- Только для сред VMware
- Защита на уровне файловой системы и корпоративной сети
- Минимальное влияние на производительность
- Минимальные затраты на установку и управление
- Типовое применение: виртуализация серверов с контролируемым подключением к интернету

ЗАЩИТА НА БАЗЕ ЛЕГКОГО АГЕНТА*

- Для сред VMware, Microsoft, Citrix и KVM
- Защита критически важных для бизнеса виртуальных серверов и VDI
- Расширенная защита, в том числе Контроль программ, устройств и Веб-Контроль
- Типовое применение: виртуализация рабочих станций и серверов, выполняющих критически важные задачи

* Для временных ВМ защита осуществляется сразу же после добавления Легкого агента в образ ВМ. Для защиты постоянных ВМ Легкий агент должен быть установлен на каждую виртуальную машину в процессе инсталляции.

ЗАЩИТА ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Инструменты защиты критически важных участков инфраструктуры центров обработки данных

Непрерывность бизнес-процессов и безопасность данных сегодня являются главными приоритетами для крупных компаний. Во многом они обеспечиваются с помощью надежной защиты центров обработки данных.

ПОЧЕМУ КАЧЕСТВО ЗАЩИТЫ ЦОДОВ ТАК ВАЖНО

Независимо от того, какой центр обработки данных используется в организации — собственный или арендованный, — перед компанией стоит непростая задача по обеспечению безопасности и целостности хранимой на нем информации. Защитные решения для таких систем должны быть гибкими: поддерживая необходимый уровень безопасности существующей среды сегодня, они должны легко масштабироваться, чтобы поддержать любые ее изменения в будущем.

Недостаточная интеграция системы безопасности IT-инфраструктурой или невозможность ее масштабирования негативно сказываются не только на качестве работы ЦОДа, но и на эффективности бизнеса в целом. Кроме того, защитные решения не должны оказывать значительного влияния на производительность IT-систем или затруднять работу пользователей. В противном случае это может привести к увеличению расходов и снижению ROI.

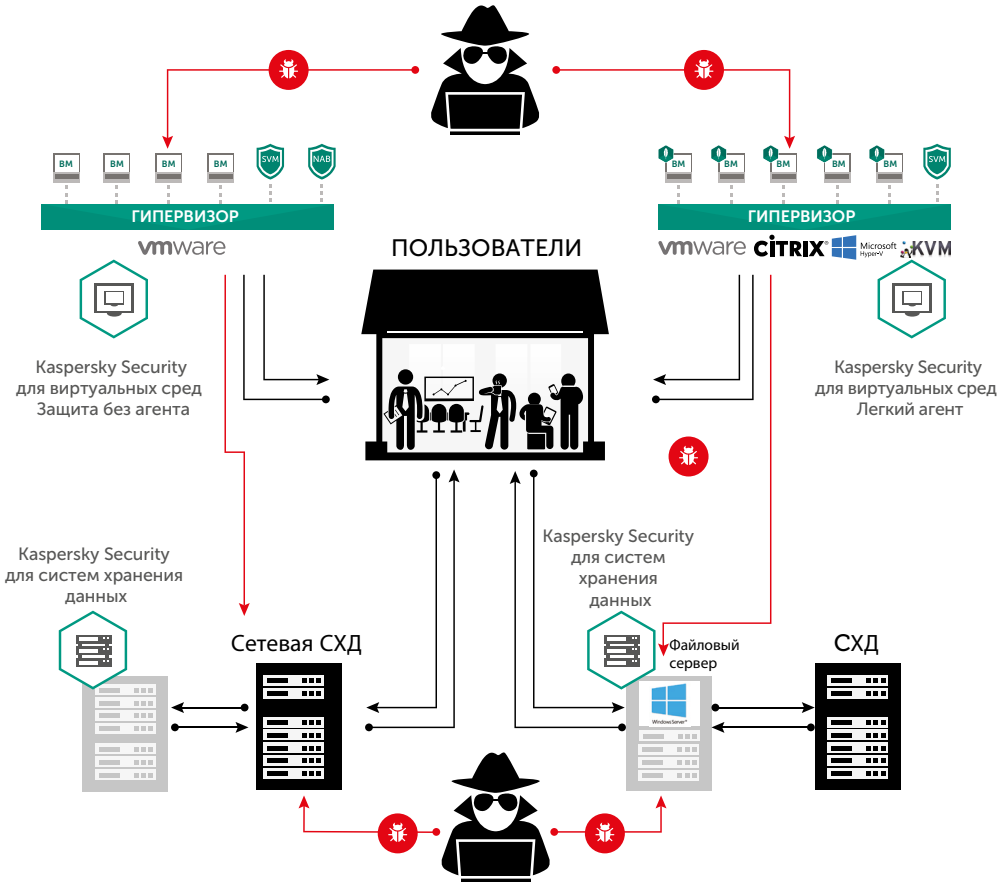
КОМПЛЕКСНОЕ РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»:

- Защищает ЦОД и ценную информацию от кибератак
- Предоставляет эффективные инструменты для поддержания высокой производительности и непрерывности бизнес-процессов
- Просто развертывается и интегрируется с центром обработки данных любой конфигурации
- Обеспечивает безопасность виртуальной инфраструктуры и сетевых хранилищ
- Администрируется из единой консоли управления

ПОДДЕРЖКА ПОПУЛЯРНЫХ ПЛАТФОРМ

Решение «Лаборатории Касперского» специально разработано для защиты ключевых технологий ЦОД. Оно защищает самые распространенные гипервизоры, в том числе VMware, Microsoft, KVM и Citrix, помогая достичь высокой степени плотности виртуальных машин. В дополнение к специальным защитным решениям для виртуальных сред «Лаборатория Касперского» также предоставляет решения для защиты серверов Network Attached Storage (NAS) и файловых серверов.

АРХИТЕКТУРА РЕШЕНИЯ



ЗАЩИТА ОТ DDOS-АТАК

Противодействие DDoS-атакам и обеспечение непрерывной работы бизнеса

Одна DDoS-атака может обернуться многочасовыми сбоями и многомиллионными убытками. При этом стоимость проведения таких атак сегодня может составлять всего несколько тысяч рублей.

DDOS-АТАКИ СТАНОВЯТСЯ СЛОЖНЕЕ

Затраты на проведение DDoS-атак снижаются, а их количество постоянно растет. При этом атаки становятся сложнее и масштабнее: за считанные минуты они могут вывести из строя веб-ресурсы предприятия, вызвать перегрузку сети, остановить ключевые внутренние бизнес-процессы и полностью парализовать онлайн-операции.

Нарушение работы онлайн-сервисов компании, деятельность которой напрямую связана с функционированием веб-сайта или внутренней IT-инфраструктуры, совершенно недопустимо для современного бизнеса. Защита не должна отставать от развития атак, тем более что финансовые и репутационные последствия DDoS-атаки бывают весьма значительными.

БОРЬБА С DDOS-АТАКАМИ НА ДВУХ ФРОНТАХ

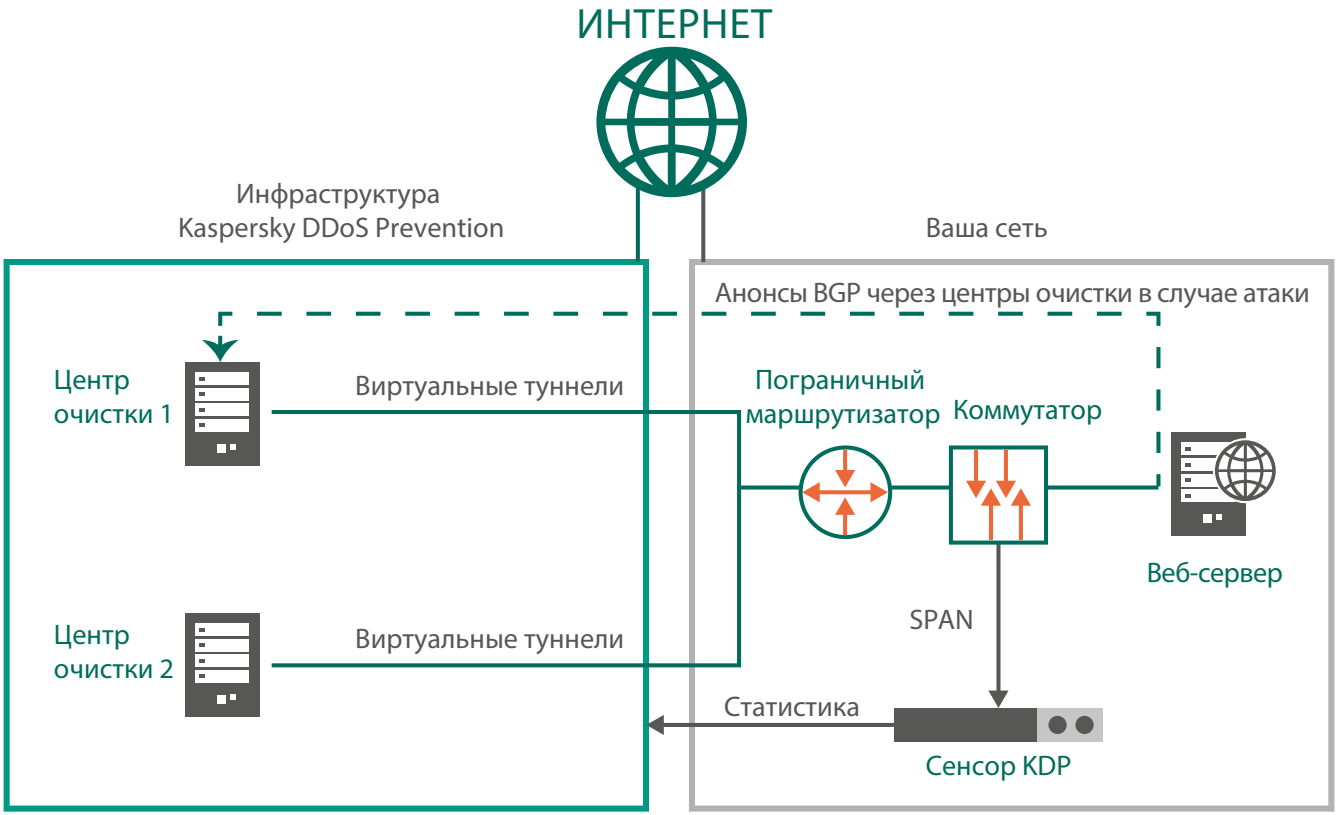
Решение Kaspersky DDoS Prevention способно распознавать атаки предельно быстро и борется с ними на двух фронтах: через систему мониторинга DDoS Intelligence и с помощью специальной защитной инфраструктуры «Лаборатории Касперского». Кроме того, в «Лаборатории Касперского» работает группа экспертов, которая использует передовые методы, чтобы следить за новейшими DDoS-угрозами и определять угрозы как можно раньше.

KASPERSKY DDOS PREVENTION:

- круглосуточно анализирует интернет-трафик;
- предупреждает о возможной атаке;
- перенаправляет трафик на центр очистки;
- возвращает очищенный трафик в вашу сеть.

После того как атака будет отражена, «Лаборатория Касперского» предоставит подробный отчет с полной информацией об инциденте, указанием длительности атаки и результате работы Kaspersky DDoS Prevention.

АРХИТЕКТУРА KASPERSKY DDOS PREVENTION



ЗАЩИТА МОБИЛЬНОГО И ОНЛАЙН-БАНКИНГА

Снижение риска мошенничества при совершении финансовых операций

Клиенты все реже посещают отделения банков и предпочитают совершать банковские операции, используя компьютер и телефон. Разумеется, эту тенденцию заметили многие финансовые организации — они активно запускают мобильные приложения и разрабатывают онлайн-сервисы. Это привлекает не только новую аудиторию, но и киберпреступников.

АТАКИ НА СЧЕТА И ТРАНЗАКЦИИ

Для похищения денег через интернет-банки и сайты финансовых услуг киберпреступники применяют разнообразные схемы.

К основным угрозам относятся:

- захват банковского счета — кража учетных данных пользователя и последующий перевод финансовых средств с этого счета;
- вмешательство в транзакции — изменение параметров транзакции или создание новой транзакции от имени пользователя.

ОШИБКИ КЛИЕНТОВ БЬЮТ ПО РЕПУТАЦИИ БАНКА

Суровая действительность: клиенты банков порой ведут себя легкомысленно, когда дело касается безопасности их компьютеров и мобильных устройств.

При этом ошибки клиентов часто оказываются проблемой банка. Когда клиенты становятся жертвой онлайн-мошенничества, они винят в этом банк, поэтому из-за ошибок клиентов сильнее всего страдает репутация бизнеса.

KASPERSKY FRAUD PREVENTION

Kaspersky Fraud Prevention не просто устраняет последствия мошеннического инцидента, но дает организациям возможность принять превентивные меры, чтобы не позволить злоумышленникам добиться своей цели. Платформа активно блокирует попытки киберпреступников похитить данные пользователей, устраняя угрозу мошенничества до того, как она получит реальное воплощение. Консоль решения также позволяет сотрудникам банка, отвечающим за борьбу с мошенничеством, собрать точные сведения о каждом инциденте, в том числе учетные данные, использованные для доступа к счету.

Kaspersky Fraud Prevention усиливает существующую систему безопасности банка, выводя ее на принципиально новый уровень.

Kaspersky Fraud Prevention Clientless Engine

Технологии на стороне сервера, защищающие клиентов. Вне зависимости от устройства и платформы, используемых клиентом, решение предотвращает доступ зараженных устройств к вашим системам.

Kaspersky Fraud Prevention Mobile SDK

Защищает приложения мобильного банкинга и онлайн-платежей на устройствах на базе Android™, iOS® и Windows® Phone®. Обеспечивает безопасность передачи данных учетной записи пользователя и коммуникаций клиента с банком.

Kaspersky Fraud Prevention for Endpoints

Работает на компьютерах под управлением Windows и Mac OS® X, защищая от вредоносного ПО и онлайн-атак и делая безопасными банковские операции.

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»:

- Защищает системы мобильного и онлайн-банкинга
- Эффективно противодействует основным видам атак на клиентов
- Обеспечивает безопасность компьютеров Windows и Mac®
- Включает средства защиты пользовательских мобильных устройств
- Интегрируется в сеть банка без нарушения существующих бизнес-процессов
- Легко администрируется из единой консоли управления

ЗАЩИТА БАНКОМАТОВ И POS-СИСТЕМ

Специализированная защита для встроенных систем

Банкоматы и POS-системы привлекают киберпреступников тем, что они непосредственно связаны с финансовыми транзакциями, выдачей наличных денег и считыванием данных банковских карт. Защитить встроенные системы особенно трудно: обычно они распределены географически, сложны в управлении и редко обновляются. Таким устройствам требуется направленная защита высочайшего уровня.

KASPERSKY EMBEDDED SYSTEMS SECURITY

«Лаборатория Касперского» создала решение Kaspersky Embedded Systems Security для защиты банкоматов, кассовых систем и киосков самообслуживания. Оно создано с учетом актуальных угроз, функционала устройств, особенностей операционных систем, соединений и архитектуры встроенных систем.

НИЗКИЕ ТРЕБОВАНИЯ К АППАРАТНЫМ РЕСУРСАМ

Решение «Лаборатории Касперского» рассчитано на полноценную работу на низкопроизводительных аппаратных платформах, которыми оборудованы большинство банкоматов и POS-систем. Системные требования к оборудованию минимальны. При использовании режима проверки по требованию решение обращается к аппаратным ресурсам только во время проверок на вирусы.

ПОДДЕРЖКА WINDOWS XP

Около 90% банкоматов по-прежнему используют ОС семейства Windows XP, поддержка которого прекращена производителем. Решение Kaspersky Embedded Systems Security оптимизировано для полнофункциональной работы на платформе Windows XP, так же как и на ОС Windows 7, Windows 2009 и Windows 10 IoT.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ PCI DSS

Согласно требованиям PCI DSS, все системы, которые работают с банковскими картами, должны быть снабжены регулярно обновляемым антивирусом. Kaspersky Embedded Systems Security полностью соответствует этим требованиям.

АРХИТЕКТУРА РЕШЕНИЯ

СЦЕНАРИЙ «ЗАПРЕТ ПО УМОЛЧАНИЮ»

При использовании этого сценария в системе исполняются только те файлы, драйверы и библиотеки, которые явно разрешены администратором. Это позволяет защититься от комплексных атак.

КОНТРОЛЬ УСТРОЙСТВ

Функция контроля устройств позволяет контролировать доступ к системе USB-носителей — один из основных путей проникновения во встроенные системы.

ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Стратегический подход к кибербезопасности промышленных сред

Число вредоносных атак на промышленные системы, в том числе на автоматизированные системы управления технологическими процессами (АСУ ТП) в последнее время значительно возросло. Одного зараженного USB-накопителя может быть достаточно, чтобы вредоносное ПО распространилось по всей индустриальной сети.

Системы АСУ ТП требуют совершенно иного подхода к IT-безопасности по сравнению с классической офисной IT-инфраструктурой. В корпоративных средах основное внимание уделяется сохранности конфиденциальных данных, а бесперебойная работа не настолько важна, как для систем управления производственными процессами, где цена минуты простоя, как и любой другой ошибки, очень велика. Поэтому в обеспечении безопасности производственных процессов действует противоположный подход, при котором основной задачей является поддержание их непрерывности и оперативное устранение любых сбоев.

Еще одно отличие заключается в используемых технологиях. Большинство корпоративных сетей строятся на базе «классических» ОС и программ, в то время как промышленные системы, как правило, отличаются исключительной сложностью и задействуют узкоспециализированные технологии, что требует от системы безопасности дополнительной гибкости.

При разработке решения для защиты промышленных предприятий «Лаборатория Касперского» сделала акцент на обеспечении непрерывности технологических процессов. В основе подхода лежат многолетняя экспертиза в области кибербезопасности, глубокое понимание природы уязвимостей информационных систем и тесное сотрудничество с международными и российскими регуляторами в области требований к защите.

Решение Kaspersky Industrial CyberSecurity создано специально для защиты сложных промышленных сред, отличается высокой гибкостью и настраивается в соответствии с потребностями вашего предприятия.

KASPERSKY INDUSTRIAL CYBERSECURITY

- Защищает производственные предприятия от киберугроз
- Обеспечивает безопасность промышленных сред и непрерывность производственных процессов
- Минимизирует время простоев и задержки технологических процессов

СТРУКТУРА KASPERSKY INDUSTRIAL CYBERSECURITY

KASPERSKY INDUSTRIAL CYBERSECURITY

ТЕХНОЛОГИИ

- УСТРАНЕНИЕ УЯЗВИМОСТЕЙ
- ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО
- КОНТРОЛЬ ЦЕЛОСТНОСТИ
- ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
- СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ
- ИНТЕГРАЦИЯ С ДРУГИМИ СИСТЕМАМИ
- РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

УСЛУГИ

ОБУЧЕНИЕ И АНАЛИТИКА

- ТРЕНИНГИ ПО КИБЕРБЕЗОПАСНОСТИ
- АНАЛИТИЧЕСКИЕ ОТЧЕТЫ
- ИГРЫ-СИМУЛЯЦИИ

ЭКСПЕРТНЫЕ СЕРВИСЫ

- ОЦЕНКА ЗАЩИЩЕННОСТИ ОТ КИБЕРУГРОЗ
- ИНТЕГРАЦИЯ РЕШЕНИЯ
- СОПРОВОЖДЕНИЕ
- РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

ЗАЩИТА ОТ ЦЕЛЕВЫХ АТАК

Набор специализированных технологий и услуг для противодействия комплексным целевым атакам

Целенаправленные атаки относятся к самым опасным угрозам для бизнеса. С каждым годом их число растет, а методы злоумышленников — совершенствуются. Сегодня, чтобы успешно противостоять целевым атакам, нужны не отдельные инструменты и сервисы, а комплексная стратегия защиты, способная адаптироваться к постоянно меняющемуся характеру угроз.

KASPERSKY ANTI TARGETED ATTACK PLATFORM

Решение Kaspersky Anti Targeted Attack Platform соединяет новейшие технологии, специализированные услуги и глобальную аналитику для борьбы с целевыми атаками на всех этапах их реализации.

- Противодействие: блокирование сложных угроз и сокращение риска целевых атак
- Обнаружение: постоянный мониторинг активностей, которые сигнализируют о наличии атаки
- Реагирование: помощь в устранении атаки и расследовании причин ее возникновения
- Прогнозирование: укрепление мер безопасности и устранение уязвимостей инфраструктуры

СИСТЕМНЫЙ ПОДХОД

Особенность целевых атак заключается в том, что они тщательно готовятся и управляются вручную на всех этапах реализации. Злоумышленники похищают ценные данные, и нарушают бизнес-процессы, но остаются незамеченными в течение долгого времени — вплоть до нескольких лет. При этом цена проведения целевых атак постоянно снижается, поэтому их жертвой может стать практически любая компания. Чтобы выявить существующую и предупредить будущую целевую атаку, недостаточно иметь в арсенале отдельные превентивные технологии, — требуются способность определять нормальное поведение системы и пользователей, а также постоянный анализ всех действий.

ЭКСПЕРТИЗА МИРОВОГО УРОВНЯ

Чтобы противостоять целевым атакам, также крайне необходимы большой опыт их выявления и постоянное изучение механизмов их распространения. В основе Kaspersky Anti Targeted Attack Platform лежат глубокая экспертиза и инновационные технологии, благодаря которым были выявлены десятки крупнейших целенаправленных атак общемирового масштаба — Darkhotel, Carbanak и многие другие.

ОБУЧЕНИЕ СПЕЦИАЛИСТОВ

Чтобы технологии противодействия целевым атакам сочетались с эффективными мерами безопасности внутри компании, «Лаборатория Касперского» предлагает тренинги для специалистов по ИБ, в том числе по реагированию на инциденты и полноценному расследованию целевых атак.

ГИБКИЙ КОНТРОЛЬ СЕТЕВОЙ АКТИВНОСТИ

Выделенные сенсоры сети и рабочих станций позволяют расположить точки контроля в разных участках сети и быстро обнаружить комплексные угрозы, которым подвержена ваша инфраструктура.

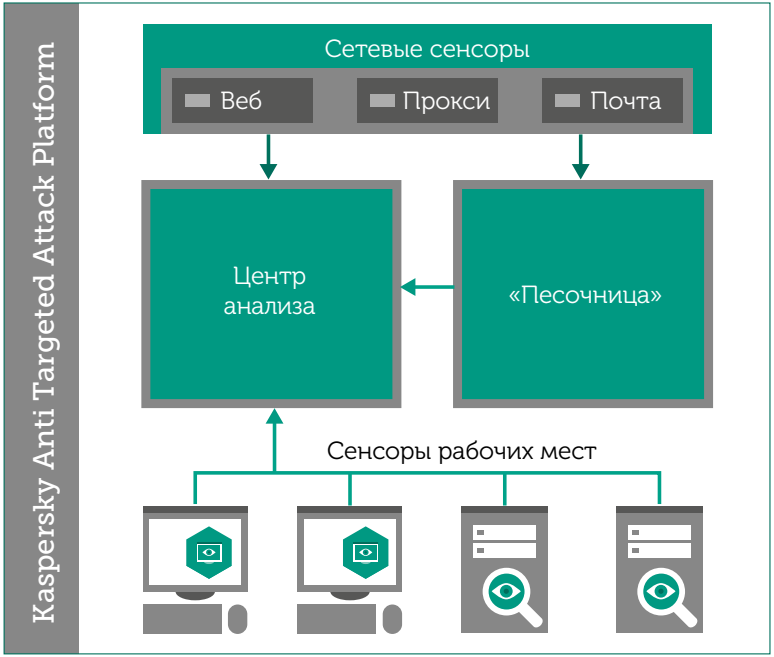
АНАЛИЗ ПОВЕДЕНИЯ ОБЪЕКТОВ

Подозрительные объекты, обнаруженные в почтовых вложениях или интернет-трафике, передаются сенсорами в песочницу — изолированную виртуальную среду. После этого каждый объект анализируется на предмет вредоносной активности, что позволяет выявлять атаку на ранней стадии.

АНАЛИЗ АНОМАЛИЙ

Анализатор целевых атак получает информацию от сетевых сенсоров, сенсоров рабочих станций и серверов для создания типовых шаблонов поведения программ. В дальнейшем на основе отклонений от этих шаблонов определяется, является ли активность потенциально частью целевой атаки, и, если является, немедленно информирует о ней специалистов по безопасности.

АРХИТЕКТУРА РЕШЕНИЯ



ЭКСПЕРТИЗА В ОБЛАСТИ БЕЗОПАСНОСТИ

Широкий спектр экспертных сервисов для повышения уровня безопасности вашего бизнеса

Для повышения эффективности системы кибербезопасности вашей компании «Лаборатория Касперского» предлагает набор сервисов для специалистов в области IT-безопасности, основанный на уникальном опыте и знаниях экспертов «Лаборатории Касперского».

СЕРВИСЫ ИНФОРМИРОВАНИЯ ОБ УГРОЗАХ

Потоки данных об актуальных угрозах, обновляемые в режиме реального времени, позволяют усилить ваше SIEM-решение и получить более широкие возможности в области расследования инцидентов.

Аналитические отчеты об угрозах класса APT позволяют применять проактивный подход к защите благодаря эксклюзивному доступу к подробным описаниям крупных кампаний кибершпионажа. Подписка на отчеты включает в том числе доступ к соответствующим индикаторам компрометации (indicators of compromise, IOC). Индикаторы передаются в формате, распознаваемом устройствами безопасности, позволяя таким образом обнаружить и устранить угрозы до того, как они нанесли ощутимый вред.

Специализированные аналитические отчеты показывают существующие и потенциальные возможности для атак на вашу организацию. Среди прочего, отчеты содержат сведения о критически важных ресурсах компании на периметре сети, об утечках конфиденциальной информации и о векторах атаки, представляющих особый интерес для разработчиков вредоносного ПО и киберпреступников.

ЭКСПЕРТНЫЕ СЕРВИСЫ

Тестирование на проникновение позволяет выявить наиболее уязвимые элементы IT-инфраструктуры, избежать финансового, операционного и репутационного ущерба, связанного с кибератаками за счет своевременного устранения уязвимостей, а также обеспечить выполнение требований государственных, отраслевых и корпоративных стандартов (таких как PCI DSS).

Анализ защищенности приложений позволяет обнаружить уязвимости в приложениях любого типа, от крупных облачных сервисов, ERP-решений, систем дистанционного банковского обслуживания (ДБО) и других бизнес-приложений до встроенных приложений и решений для различных мобильных платформ (iOS, Android и др.).

Расследование инцидентов и анализ вредоносного ПО позволяет воссоздать детальную картину инцидента информационной безопасности. «Лаборатория Касперского» предоставляет подробный отчет, содержащий, в частности, рекомендации по устранению последствий инцидента.

ПРОГРАММА ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ

Повышение культуры кибербезопасности в форме интерактивных тренингов

Программа Kaspersky CyberSecurity Awareness помогает создавать и развивать культуру кибербезопасности с помощью набора тренингов по повышению осведомленности. Тренинги проводятся в тесном сотрудничестве со службой IT-безопасности и отделом по работе с персоналом. Они включают элементы игры и предназначены для сотрудников всех уровней, не обладающих специальными знаниями в области IT-безопасности.

СТРУКТУРА ТРЕНИНГОВ:

ЭФФЕКТ ОТ ПРОГРАММЫ:

- Сокращение числа инцидентов до 90%
- Уменьшение рисков кибербезопасности на 50–60% в денежном выражении
- Вероятность применения полученных знаний в повседневной работе — до 93%
- Более чем 30-кратная окупаемость вложений (ROI)
- Включение в процесс руководителей организации благодаря переводу требований кибербезопасности на понятный язык
- Измеримые результаты программы осведомленности

ЛОКАЛЬНАЯ РЕПУТАЦИОННАЯ БАЗА

Решение проблемы кибербезопасности в изолированных сетях без передачи данных за пределы локальной сети

Сегодня ключевым фактором обеспечения безопасности является время реакции: оно должно быть минимальным. Даже малейший простой может иметь серьезные последствия для крупных предприятий и организаций. При этом нормативные требования, внутренние политики конфиденциальности и отраслевая специфика серьезно влияют на оперативность и качество решения вопросов кибербезопасности.

Для решения проблемы кибербезопасности в изолированных сетях и сетях со строгими ограничениями доступности извне «Лаборатория Касперского» предлагает предприятиям локальную репутационную базу Kaspersky Private Security Network. Она соответствует жестким требованиям к системе защиты и обладает всеми преимуществами облачной сети безопасности, но без передачи данных за пределы локальной сети.

СВЕДЕНИЯ ОБ УГРОЗАХ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Созданная «Лабораторией Касперского» глобальная система сведений об угрозах предоставляет в режиме реального времени всю информацию, необходимую для защиты от киберугроз и расследования возможных инцидентов.

БЫСТРОЕ ОБНАРУЖЕНИЕ УГРОЗ

Традиционным решениям требуется до четырех часов, чтобы обнаружить и заблокировать новое вредоносное ПО. С Kaspersky Private Security Network это происходит меньше чем за минуту — без передачи каких-либо данных за пределы локальной сети вашей компании.

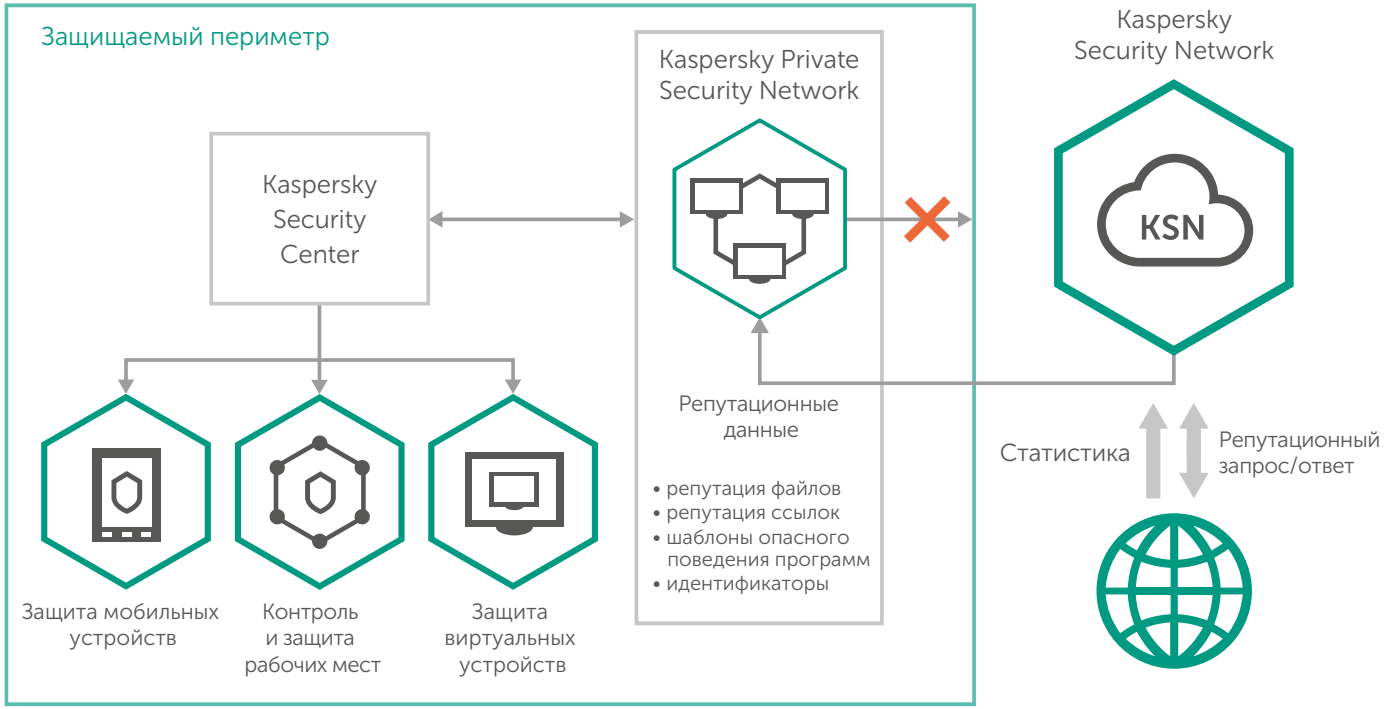
ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ

Передовая облачная система сведений об угрозах позволяет немедленно реагировать на угрозы в рамках контролируемой локальной сети предприятия.

ПРЕИМУЩЕСТВА KASPERSKY PRIVATE SECURITY NETWORK

- Уникальные сведения о новейших и наиболее сложных атаках, предоставляемые в рамках контролируемой среды вашей локальной сети
- Адаптация решения к условиям изолированной сети
- Гибкие возможности развертывания и тестовый режим
- Соответствие требованиям к обеспечению безопасности и защите конфиденциальных данных
- Высокий уровень защиты благодаря быстрой реакции на угрозы и минимизации ложных срабатываний

Решение Kaspersky Private Security Network можно установить в центре обработки данных организации, и его работу будут полностью контролировать IT-специалисты вашего предприятия. При этом вы не подвергаете риску сохранность конфиденциальных данных и не нарушаете требования IT-безопасности для изолированных сетей.



ЗАЩИТА ОТДЕЛЬНЫХ УЗЛОВ СЕТИ

Специализированные решения для обеспечения безопасности отдельных компонентов сети

Все устройства в составе корпоративной сети нуждаются в надежной специализированной защите. Поэтому, помимо решения для контроля и защиты рабочих мест, «Лаборатория Касперского» разработала продукты для обеспечения безопасности отдельных узлов сети. Они могут быть установлены в дополнение к продуктам Kaspersky Endpoint Security для бизнеса или как отдельное решение.

ЗАЩИТА ПОЧТОВЫХ СЕРВЕРОВ

Kaspersky Security для почтовых серверов обеспечивает защиту почтового трафика от спама, фишинговых ссылок и вредоносного ПО. Решение поддерживает популярные почтовые платформы Microsoft Exchange, Linux® Mail Server и IBM® Lotus® Domino®. Кроме того, для почтовых платформ Microsoft Exchange реализован модуль контроля над распространением конфиденциальной информации.

ЗАЩИТА ИНТЕРНЕТ-ШЛЮЗОВ

Kaspersky Security для интернет-шлюзов проверяет трафик HTTP, HTTPS и FTP в режиме реального времени и обеспечивает всестороннюю защиту интернет-шлюзов от известных и вновь возникающих угроз.

ЗАЩИТА ФАЙЛОВЫХ СЕРВЕРОВ

Kaspersky Security для файловых серверов — это эффективное, надежное и масштабируемое решение для защиты файловых хранилищ с общим доступом, не оказывающее заметного влияния на производительность системы. Решение обеспечивает защиту от вредоносного ПО для серверов на базе Linux и Windows.

ЗАЩИТА СЕРВЕРОВ СОВМЕСТНОЙ РАБОТЫ

Kaspersky Security для серверов совместной работы обеспечивает максимальный уровень безопасности серверов SharePoint®, а также их пользователей. Эффективные технологии защиты от вредоносных атак и утечки конфиденциальных данных в этом решении сочетаются с простотой управления и удобством использования.

РАСШИРЕННАЯ ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Реакция на критически важные события в режиме 24x7 и прямой доступ к техническим специалистам

Премиальные программы поддержки идеально подходят крупным компаниям, для которых исключительно важна непрерывность бизнес-процессов. Решение вашей проблемы становится приоритетной задачей для экспертов «Лаборатории Касперского».

ПРОГРАММЫ ПРЕМИАЛЬНОЙ ПОДДЕРЖКИ

	MSA Business	MSA Enterprise
	Решение для компаний, которым требуется реакция на критически важные события в режиме 24x7 и прямой доступ к техническим специалистам	Решение для компаний со сложной инфраструктурой, которым требуется персонализированная и проактивная защита
24x7x365	✓	✓
Выделенная телефонная линия	✓	✓
Время реакции на критические инциденты	4 часа	30 минут
Персональный технический менеджер		✓
Регулярные отчеты о статусе решения проблемы		✓

ПРОФЕССИОНАЛЬНЫЕ УСЛУГИ

Применяя передовой опыт и собственные эффективные методики, наши эксперты окажут поддержку во всех аспектах развертывания, настройки и обновления продуктов «Лаборатории Касперского» в вашей IT-инфраструктуре:

- **Проектирование и установка** решений «Лаборатории Касперского» для бизнеса.
- **Обучение IT-специалистов** для более эффективного использования защитных технологий «Лаборатории Касперского» с учетом особенностей IT-инфраструктуры компании.
- **Проверка состояния системы защиты** с целью оптимизации работы решения для обеспечения IT-безопасности в условиях существующей инфраструктуры с предоставлением подробного отчета и рекомендаций.

О «ЛАБОРАТОРИИ КАСПЕРСКОГО»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и опыт компании лежат в основе защитных решений и сервисов, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и пользователей во всем мире.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для широкого круга пользователей. «Лаборатория Касперского» защищает домашних пользователей, небольшие компании, предприятия среднего бизнеса и крупные корпорации от всевозможных киберугроз, предлагая всем при этом удобные инструменты для управления системой безопасности.

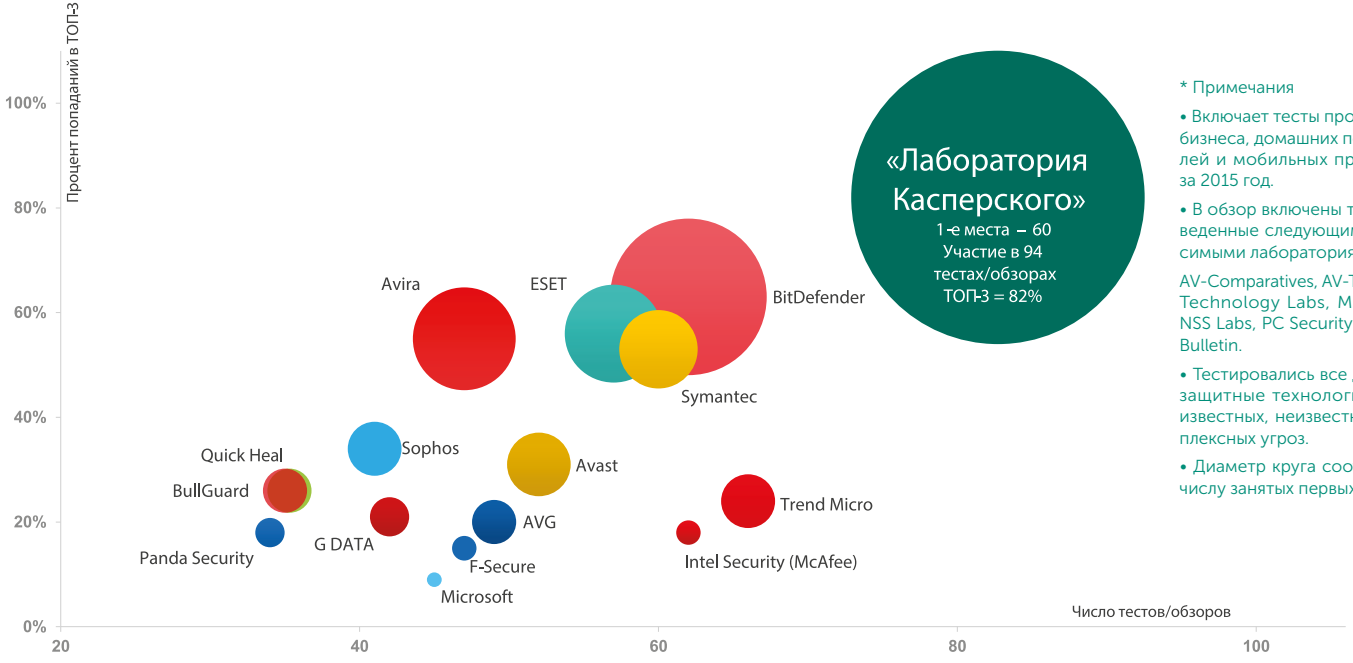
«Лаборатория Касперского» понимает потребности небольших компаний и предлагает им многоуровневые решения, эффективные и простые в управлении. Компания также отвечает всем запросам крупных предприятий, предоставляя им комплексную платформу, которая защищает от всех типов киберугроз, обнаруживает самые сложные атаки, реагирует на любые инциденты и предвидит развитие угроз. Кроме того, компания предлагает набор специализированных решений, которые защищают все узлы корпоративной сети, включая мобильные устройства, а также способны обеспечить безопасность центров обработки данных и индустриальных сред.

Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов, помогая сохранить то, что для них важно.

Более подробная информация доступна на *www.kaspersky.ru*.

БОЛЬШЕ ТЕСТОВ. БОЛЬШЕ НАГРАД. БОЛЬШЕ ЗАЩИТЫ*

В 2015 году продукты «Лаборатории Касперского» приняли участие в 94 независимых тестах и обзорах. В 60 случаях они заняли первое место и 77 раз вошли в тройку лучших (ТОП-3).



* Примечания

- Включает тесты продуктов для бизнеса, домашних пользователей и мобильных приложений за 2015 год.
- В обзор включены тесты, проведенные следующими независимыми лабораториями:

AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, Virus Bulletin.

- Тестировались все доступные защитные технологии против известных, неизвестных и комплексных угроз.
- Диаметр круга соответствует числу занятых первых мест

Подробнее: kaspersky.ru/top3

АО «Лаборатория Касперского»
www.kaspersky.ru

Решения для крупного бизнеса:
www.kaspersky.ru/enterprise

+7 (495) 737-34-12
sales@kaspersky.com