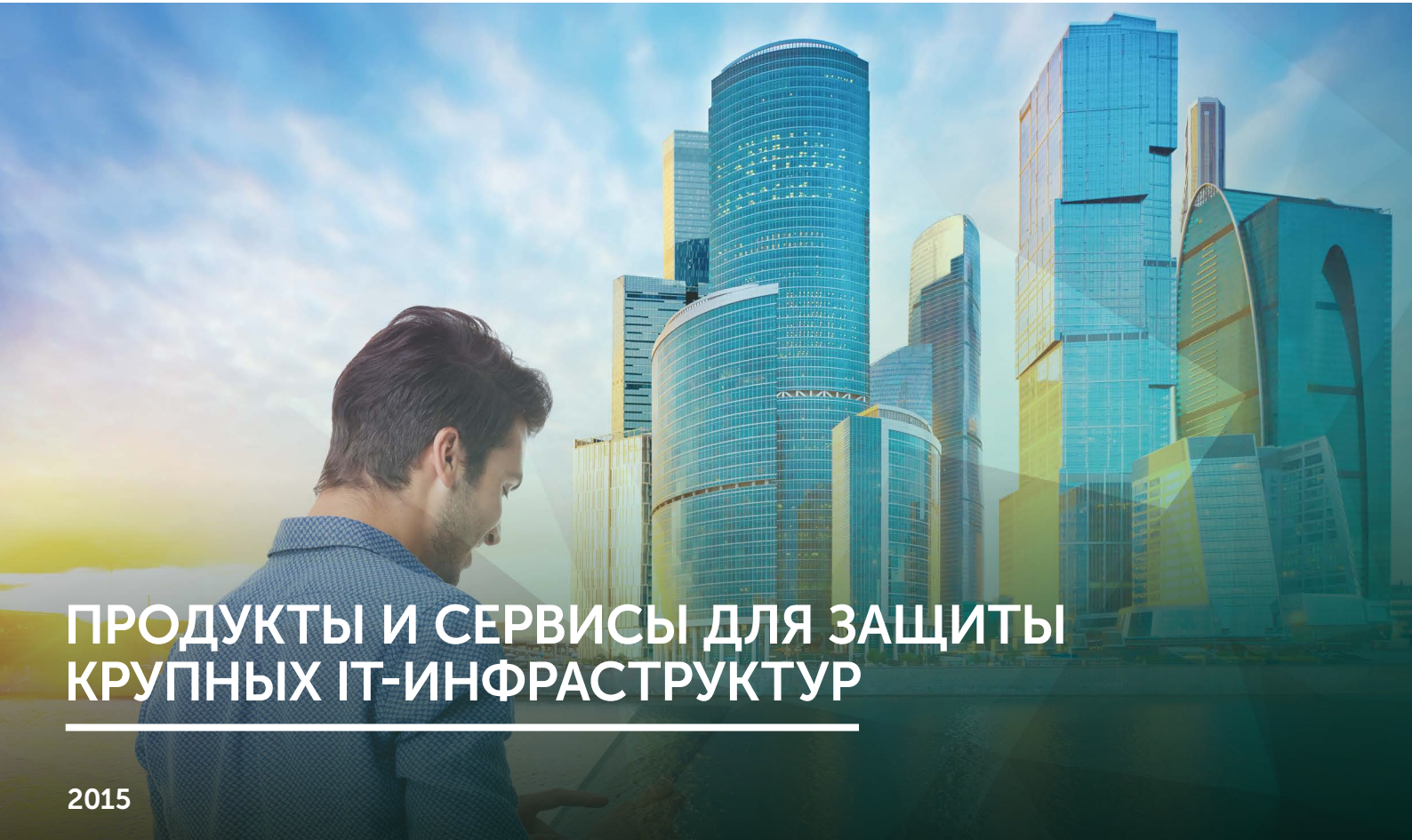
KASPERSKY lab

Стратегические решения в сфере IT-безопасности



ПРОДУКТЫ И СЕРВИСЫ ДЛЯ ЗАЩИТЫ КРУПНЫХ IT-ИНФРАСТРУКТУР

2015

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 несет дополнительные риски для информационной безопасности компаний.

Ежедневно появляются новые угрозы, столкновение с которыми может иметь разрушительные последствия как для организаций и частных лиц, так и для общества в целом. Рост числа комплексных таргетированных атак (APT-угроз, англ. Advanced Persistent Threats) и глобальных кампаний по кибершпионажу ставит под угрозу деятельность критически важных объектов инфраструктуры, финансовых организаций, телекоммуникационных и транспортных предприятий, исследовательских институтов, военных ведомств и правительственных учреждений разных стран.

Кибератаки приводят к серьезным финансовым потерям. Этот тезис уже второй год подряд подтверждается результатами опроса*, совместно проводимого аналитическим агентством B2B International и «Лабораторией Касперского». Согласно данным, полученным от представителей организаций, столкнувшихся с утечкой конфиденциальных данных в результате инцидента информационной безопасности, ущерб от одного подобного инцидента для крупных компаний в среднем составляет около 20 млн. рублей.

В этой ситуации крупным корпорациям приходится уделять особое внимание усилению защиты своей IT-инфраструктуры. Кроме того, такие организации традиционно более требовательны к масштабируемости и отказоустойчивости системы защиты, а также заинтересованы в возможностях подписки на дополнительные сервисы. Именно поэтому «Лаборатория Касперскрого» предлагает комплексный стратегический подход к обеспечению информационной безопасности. Защитные решения, разработанные специалистами компании, ориентированы не только на борьбу с существующими угрозами, но и на предотвращение новых, еще не известных угроз. Мы предлагаем как готовые продукты, которые обеспечивают многоуровневую защиту IT-инфраструктуры крупных организаций, так и ряд сервисов, в том числе расширенную техническую поддержку и экспертные сервисы Kaspersky Intelligence Services. Принцип нашей работы прост: лучшая экспертиза в сочетании с лучшими технологиями позволяют обеспечить лучшую защиту корпоративной IT-инфраструктуры.

*kaspersky.ru/IT-risk-report-Russia-2014

Контроль и защита рабочих мест

Корпоративные IT-среды усложняются с каждым днем, в то время как хакеры и киберпреступники используют все более изощренные методы для атак на организации любого размера. При этом крупные компании находятся в зоне наибольшего риска. В отсутствие адекватных мер по обеспечению IT-безопасности и управления ею такие организации могут оказаться не готовы к столкновению с новыми угрозами.

Ключевыми инструментами в построении системы защиты предприятия являются средства контроля и защиты рабочих мест. 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.

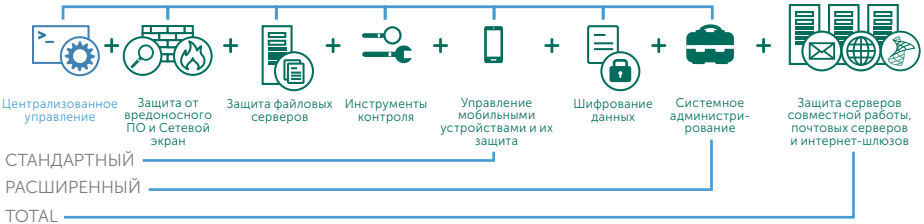
В то время как от известных угроз можно защититься с использованием традиционных сигнатурных методов, неизвестные угрозы требуют применения более совершенных технологий защиты. Одни вредоносные программы полностью блокируют критически важные бизнес-процессы, а другие готовят почву для последующих атак киберпреступников. Даже атаки с использованием сравнительно безобидного кода сказываются на производительности и требуют дополнительных ресурсов для нейтрализации угрозы и устранения последствий атаки. В связи с этим компаниям необходимо уделять особое внимание надежной защите как от известных, так и от неизвестных вредоносных программ.

В случае потери или кражи ноутбука сотрудника ущерб для компании может быть огромным. Помимо того, что бизнес-данные данные могут быть утрачены навсегда, также существует риск нарушения конфиденциальности информации, если доступ к ней получит неавторизованный пользователь.

Еще одной угрозой безопасности корпоративной IT-инфраструктуры являются уязвимости в ПО и операционных системах, которые киберпреступники часто используют для проникновения в сеть атакуемых организаций.

Для защиты и контроля рабочих мест в корпоративной среде «Лаборатория Касперского» предлагает линейку решений Kaspersky Security для бизнеса. Оптимальным образом подобранные инструменты и технологии формируют несколько уровней решения с нарастающим функционалом. Все компоненты разработаны внутри компании на собственной технологической базе и составляют единую платформу для обеспечения безопасности, легко адаптируемую в соответствии с потребностями бизнеса.

УРОВНИ KASPERSKY SECURITY ДЛЯ БИЗНЕСА



Уникальная интегрированная платформа безопасности

- Единая консоль управления
- Единая платформа
- Единая лицензия

СТАНДАРТНЫЙ

Помимо защиты от вредоносного ПО и сетевого экрана, решение «Лаборатории Касперского» уровня СТАНДАРТНЫЙ включает в себя средства для управления мобильными устройствами и защиты их от вредоносных программ, а также инструменты контроля использования веб-ресурсов, устройств и программ на компьютерах сотрудников. Все это позволяет эффективно применять политики, обеспечивающие безопасность важнейших элементов IT-инфраструктуры организации любого размера. На этом уровне решения также предусмотрена защита файловых серверов.

РАСШИРЕННЫЙ

На уровне РАСШИРЕННЫЙ инструменты предыдущего уровня дополнены шифрованием данных и средствами системного администрирования (Kaspersky Systems Management), включая инструменты мониторинга уязвимостей и автоматической установки исправлений программ и ОС.

TOTAL

Kaspersky Total Security для бизнеса — наиболее полнофункциональное решение для построения комплексной системы IT-безопасности, в котором технологии защиты и контроля рабочих мест дополнены средствами защиты почтовых серверов, интернет-шлюзов и серверов совместной работы.

Защита отдельных узлов сети

Все устройства в составе корпоративной сети нуждаются в надежной специализированной защите. Поэтому, помимо решения для контроля и защиты рабочих мест, мы разработали ряд продуктов для обеспечения безопасности отдельных узлов сети: файловых и почтовых серверов, интернет-шлюзов, серверов совместной работы, мобильных устройств, виртуальной инфраструктуры и др.

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 МОБИЛЬНЫХ УСТРОЙСТВ

Kaspersky Security для мобильных устройств обеспечивает безопасность устройства независимо от его местонахождения и позволяет осуществлять мониторинг и контроль смартфонов и планшетов из единого центра с минимальным влиянием на работу пользователей.

ЗАЩИТА ВИРТУАЛЬНЫХ СРЕД

Kaspersky Security для виртуальных сред – это специализированное решение для защиты сред на базе VMware® ESXi™, Citrix® XenServer® и Microsoft Hyper-V®. Гибкие возможности централизованной настройки и администрирования обеспечивают сохранение высокой производительности виртуальной среды.

СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Решение Kaspersky Systems Management обеспечивает централизованное и автоматизированное выполнение задач системного администрирования, таких как мониторинг уязвимостей, установка исправлений и обновлений ПО, учет аппаратного и программного обеспечения, развертывание ОС и приложений и многое другое.

Решения для защиты отдельных узлов сети могут приобретаться в дополнение к другим решениям «Лаборатории Касперского». Управление всеми технологиями безопасности производится из единой консоли администрирования.

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 Linix и Windows®.

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 вредоносных и опасных программ, блокируя даже новейшие известные и потенциальные угрозы.

ЗАЩИТА СЕРВЕРОВ СОВМЕСТНОЙ РАБОТЫ

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

ЗАЩИТА СИСТЕМ ХРАНЕНИЯ ДАННЫХ

Kaspersky Security для систем хранения данных обеспечивает надежную, высокоэффективную и масштабируемую защиту ценной и конфиденциальной корпоративной информации, хранящейся в системах EMC® Isilon™, Celerra® и VNX™, NetApp, Hitachi®, IBM и Oracle®.

Защита мобильных устройств

Некоторые организации предоставляют своим сотрудникам корпоративные смартфоны и планшеты, в то время как другие разрешают использовать для работы личные устройства. В любом случае, мониторинг всех устройств, управление ими и формирование комплексной многоуровневой системы безопасности корпоративной среды становятся сложными и трудоемкими задачами. Кроме того, число вредоносных программ, веб-сайтов и фишинговых атак, нацеленных на мобильные устройства, растет с каждым днем, поэтому защита мобильных устройств сейчас не менее важна, чем защита любых других устройств в составе корпоративной сети.

Сегодня в мире используется более 5 миллиардов смартфонов. Возможности мобильных устройств постоянно растут, что делает их особенно удобными для выполнения широкого круга бизнес-задач. Смартфоны и планшеты стали важным инструментом работы практически для каждой компании, но именно поэтому они все чаще служат мишенью для атак киберпреступников. В то же время, политика использования личных устройств в рабочих целях (Bring Your Own Device, BYOD) расширяет диапазон устройств в составе корпоративной сети, что создает IT-администраторам дополнительные сложности в управлении и контроле IT-инфраструктуры.

ЛИЧНЫЕ УСТРОЙСТВА СОТРУДНИКОВ – РИСК ДЛЯ КОМПАНИИ

В результате использования сотрудниками для работы личных мобильных устройств, на которых хранятся их собственные приложения и данные, а также корпоративные данные и пароли доступа, значительно возрастает риск нарушения IT-безопасности компании. В случае кражи или потери устройства злоумышленники могут получить прямой доступ к корпоративным системам и конфиденциальной бизнес-информации.

ВСЕ ПЛАТФОРМЫ ПОД УГРОЗОЙ

Киберпреступники применяют различные методы и средства для получения несанкционированного доступа к мобильным устройствам, в том числе зараженные приложения, публичные Wi-Fi-сети с недостаточным уровнем безопасности, фишинговые атаки и зараженные текстовые сообщения. Когда пользователь неосмотрительно посещает вредоносный веб-сайт или даже легальный веб-сайт, на который был загружен вредоносный код, он также подвергает риску безопасность своего устройства и хранящихся на нем данных. Перечисленные выше угрозы актуальны для всех популярных мобильных платформ – Android™, iOS® и Windows Phone.

Для обеспечения безопасности мобильных устройств и управления ими «Лаборатория Касперского» предлагает решение Kaspersky Security для мобильных устройств, которое предоставляет не только средства многоуровневой защиты, но и целый ряд функций управления мобильными устройствами (Mobile Device Management, MDM) и приложениями (Mobile Application Management, MAM). Они позволяют значительно сократить время, необходимое для обслуживания мобильных устройств и обеспечения безопасности мобильного доступа к корпоративным системам.

KASPERSKY SECURITY ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

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

Поддерживаемые платформы

- Android
- iOS
- Windows Phone

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ (MDM)

Интеграция со всеми основными платформами для управления мобильными устройствами позволяет осуществлять развертывание и контроль удаленно (Over-the-Air, OTA), что значительно облегчает защиту и управление устройствами на базе Android, iOS и Windows Phone.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ ПРИЛОЖЕНИЯМИ (MAM)

Изолированные контейнеры для приложений и возможность выборочной очистки памяти устройства позволяют разделить корпоративную и личную информацию, хранящуюся на устройстве сотрудника. Сочетание функционала шифрования и защиты от вредоносного ПО в составе Kaspersky Security для мобильных устройств дает возможность обеспечить проактивную защиту мобильного устройства, а не просто изолировать устройство и хранящиеся на нем данные.

* Набор доступных функций зависит от защищаемой платформы

Защита виртуальных сред

Виртуализация должна обеспечивать максимальный возврат инвестиций за счет эффективного использования и консолидации ресурсов корпоративной IT-инфраструктуры. При этом существует ошибочное мнение, что виртуальные машины более устойчивы к вредоносному воздействию по сравнению с физическими машинами. К сожалению, это не так, и все преимущества виртуализации могут быть сведены к минимуму, если виртуальная инфраструктура не обеспечена надлежащей специализированной защитой.

Большинство вредоносных программ, предназначенных для физических компьютеров, могут атаковать и виртуальные машины. При этом риски IT-безопасности в виртуальных средах зачастую значительно выше. Повышая гибкость и эффективность работы IT-инфраструктуры, виртуализация одновременно усложняет ее за счет использования дополнительных технологий. Это повышает уязвимость IT-инфраструктуры и дает киберпреступникам новые возможности для атак на компании.

Для обеспечения безопасности виртуальных IT-инфраструктур «Лаборатория Касперского» предлагает специализированое решение Kaspersky Security для виртуальных сред. Оно обеспечивает высочайший уровень защиты для виртуальных сред на базе VMware ESXi, Microsoft Hyper-V и Citrix Xen®.

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 – это специализированное решение для защиты виртуальной инфраструктуры и обеспечения ее высокой производительности.

Решение «Лаборатории Касперского» предусматривает два типа установки: с использованием Легкого агента на каждой ВМ и без использования агента. Оба варианта предполагают применение виртуального устройства безопасности, которое осуществляет централизованную антивирусную проверку всех виртуальных машин, размещенных на хост-сервере, что обеспечивает эффективную защиту ВМ без дополнительной нагрузки на гипервизор и поддерживает высокую плотность ВМ на хост-сервере.

ЗАЩИТА БЕЗ УСТАНОВКИ АГЕНТА

- Только для сред VMware
- Высокая плотность ВМ
- Защита только ВМ на базе ОС Windows
- Минимальные затраты на установку и управление
- Типовое применение: виртуализация серверов с контролируемым подключением к интернету

ЗАЩИТА НА БАЗЕ ЛЕГКОГО АГЕНТА*

- Для сред VMware, Microsoft и Citrix
- Высокая плотность ВМ
- Защита только ВМ на базе ОС Windows
- Расширенная защита и применение политик
- Типовое применение: виртуализация рабочих станций и серверов, выполняющих критически важные задачи

ГИБКОЕ ЛИЦЕНЗИРОВАНИЕ

Kaspersky Security для виртуальных сред может лицензироваться двумя способами, в зависимости от потребностей компании и особенностей виртуальной инфраструктуры.

- По количеству виртуальных машин:
  – по количеству рабочих станций
  – по количеству серверов
- По количеству ядер физических процессоров хост-сервера

* 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

С каждым днем число кибератак растет, а сами угрозы становятся все более изощренными. Киберпреступники целенаправленно атакуют крупные предприятия и поставщиков услуг. В этой ситуации задача по обеспечению безопасности центра обработки данных (ЦОДа), который служит своеобразным «ядром» предприятия и большинства критически важных бизнес-процессов, и простой которого совершенно недопустим, также усложняется.

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: обеспечивая необходимый уровень безопасности существующей среды сегодня, они должны легко масштабироваться, чтобы поддержать любые ее изменения в будущем. Кроме того, такое решение должно включать специализированные технологии для защиты систем хранения данных и виртуальных сред.

ОПТИМИЗАЦИЯ РАСХОДОВ

Недостаточная интеграция системы безопасности с IT-инфраструктурой или невозможность ее масштабирования могут негативно сказаться 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. Невыполнение этих условий может привести к увеличению расходов, снижая тем самым рентабельность инвестиций (ROI).

МИНИМИЗАЦИЯ НАГРУЗКИ НА IT-СЛУЖБЫ

Помимо сохранения высокого уровня производительности ЦОДа и обеспечения его непрерывной работы, настройка и управление системой защиты не должны отнимать у IT-персонала много времени.

Независимо от конфигурации и назначения используемого в компании центра обработки данных, «Лаборатория Касперского» предлагает комплексное решение для обеспечения безопасности информации и непрерывности бизнес-процессов организации.

Защитное решение «Лаборатории Касперского» учитывает особенности ключевых технологий, используемых при создании ЦОДов, обеспечивая безопасность виртуальных сред VMware, Microsoft и Citrix, а также включает инструменты для защиты систем хранения данных и файловых серверов.

Все компоненты решения легко развертываются и интегрируются с центром обработки данных любой конфигурации, что позволяет экономить время и использовать все преимущества единой платформы безопасности. Управление из единого центра дает возможность применять единую политику безопасности ко всему центру обработки данных, тем самым снижая эксплуатационные расходы.

КОМПЛЕКСНОЕ РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»:

- Защищает ЦОД и ценную информацию от кибератак
- Предоставляет эффективные инструменты для поддержания высокой производительности и непрерывности бизнес-процессов
- Обеспечивает безопасность виртуальной инфраструктуры и сетевых хранилищ
- Администрируется из единой консоли управления

Защита от DDoS-атак

Сегодня DDoS-атака (Distributed-Denial-of-Service) – один из самых распространенных видов кибератак. Ее цель – довести информационную систему предприятия-жертвы (например, веб-сайт или базу данных) до такого состояния, при котором легитимные пользователи не могут получить к ней доступ. Финансовые и репутационные потери организации, которая подверглась атаке такого типа, могут быть очень велики.

ОБЪЕМЫ И СЛОЖНОСТЬ АТАК РАСТУТ

К сожалению, за последние годы затраты на организацию DDoS-атак существенно снизились, а объем таких атак значительно возрос. Вместе с тем, сами атаки стали сложнее и масштабнее: всего за несколько секунд или минут они могут вывести из строя веб-ресурсы предприятия, вызвать перегрузку сети атакуемой организации, остановить ее 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. Устранение последствий успешной DDoS-атаки может обойтись пострадавшему бизнесу очень недешево.

ПРЕДУПРЕЖДЕН – ЗНАЧИТ ВООРУЖЕН

У каждой компании должна быть эффективная стратегия защиты, чтобы применить ее в случае обнаружения DDoS-атаки. Тогда организация сможет незамедлительно заняться устранением ее последствий, чтобы:

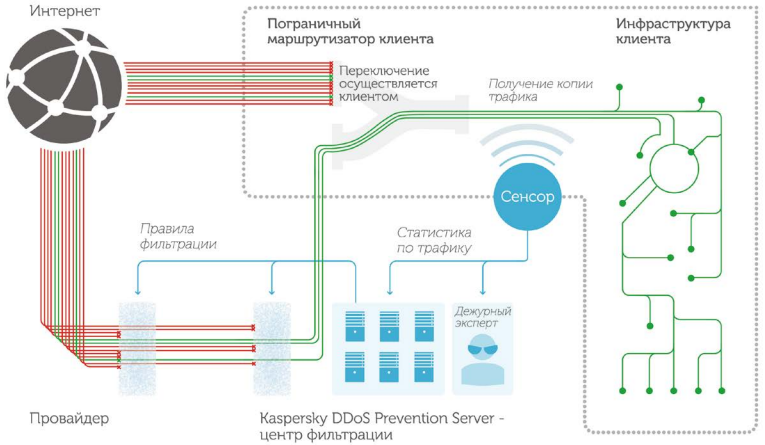
- минимизировать ущерб от простоя инфраструктуры и остановки бизнес-процессов;
- обеспечить клиентам скорейший доступ к онлайн-сервисам;
- не допустить падения продуктивности работы сотрудников.

Для противодействия DDoS-угрозам «Лаборатория Касперского» предлагает решение Kaspersky DDoS Prevention, которое обеспечивает надежную интегрированную защиту от DDoS-атак. Решение включает все необходимое для обеспечения безопасности бизнеса. Система Kaspersky DDoS Prevention осуществляет непрерывный анализ всего онлайн-трафика организации без прямого доступа к передаваемым данным, уведомляет о возможной атаке, а затем принимает перенаправленный трафик, очищает его и доставляет на ресурсы клиента. Это позволяет эффективно защитить бизнес от всех типов DDoS-атак.

KASPERSKY DDOS PREVENTION – ЭТО:

- Специальное приложение-сенсор «Лаборатории Касперского», работающее в составе IT-инфраструктуры клиента
- Распределенная сеть центров очистки трафика
- Поддержка со стороны специалистов центра управления Kaspersky DDoS Prevention и экспертов по защите от DDoS-атак
- Детальный анализ и отчеты по имевшим место атакам
- Личный кабинет клиента на портале Kaspersky DDoS Prevention
- Расширенные аналитические данные о последних DDoS-атаках

Схема работы Kaspersky DDoS Prevention



Защита мобильного и онлайн-банкинга

Банковские онлайн-сервисы всегда под угрозой. На кону – миллиарды рублей, ведь любой инцидент, затрагивающий банк, оборачивается потерей времени и денег, а также подрывает долгосрочные отношения с клиентами. Кроме того, возможности традиционных средств защиты в данном случае сильно ограничены, поскольку главной причиной уязвимости банковских онлайн-сервисов служит человеческий фактор. Чтобы случайная ошибка не привела к серьезным финансовым последствиям, необходима превентивная защита.

Финансовое мошенничество – это серьезная угроза, которая может иметь разрушительные последствия, если вовремя не принять меры. С каждым годом она становится все сложнее, поскольку организованные киберпреступные группировки применяют все более изощренные методы для перехвата финансовых транзакций и кражи денег пользователей.

Для похищения денег через интернет-банки и сайты финансовых услуг киберпреступники используют разнообразные мошеннические схемы. Это может быть как вмешательство в санкционированные транзакции с помощью вредоносного ПО с целью перевода денег на счета злоумышленников, так и сочетание фишинга с приемами социальной инженерии для получения доступа к счетам.

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.

ЗАЧЕМ НУЖНЫ ДОПОЛНИТЕЛЬНЫЕ ТЕХНОЛОГИИ ДЛЯ ЗАЩИТЫ ОТ МОШЕННИЧЕСТВА?

Согласно глобальному обзору рисков IT-безопасности* за 2014 г.:

- 73% компаний учитывают репутацию в области безопасности, выбирая банк для размещения своих средств
- 82% отметили, что могут отказаться от услуг банка, допустившего утечку данных
- Лишь 51% компаний считает, что финансовые организации предпринимают достаточно усилий для защиты конфиденциальной информации

*kaspersky.com/Global-IT-risk-report-2014

Для защиты от финансового мошенничества «Лаборатория Касперского» предлагает решение Kaspersky Fraud Prevention, которое усиливает существующую систему безопасности банка, выводя ее на принципиально новый уровень защиты от мошенничества. Решение обеспечивает безопасность пользователей компьютеров и мобильных устройств. Благодаря защите транзакций клиентов решение Kaspersky Fraud Prevention позволяет повысить уровень лояльности клиентов, что, в свою очередь, способствует успешному внедрению новых сервисов и услуг.

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. Эта информация может снять с банка ответственность за мошенничество, сократив расходы на возмещение ущерба и компенсации.

Преимущества для банка

- Гибко настраиваемая защита
- Экономия средств
- Защита репутации
- Простота установки

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 критической инфраструктуры

Число вредоносных атак на промышленные системы, в том числе на системы управления процессами (ICS-системы) в последнее время значительно возросло. И если раньше физической изоляции между производственными системами и внешними сетями вполне хватало для обеспечения хорошего уровня защиты, то теперь это не так. Одного зараженного USB-накопителя может быть достаточно, чтобы вредоносное ПО преодолело защитный барьер и попало в изолированную сеть.

ICS-системы 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.

Кроме того, такие защитные решения должны отвечать требованиям не только IT-руководства и персонала предприятия, но также полностью соответствовать параметрам, установленным инженерами-технологами и инженерами по организации производства, а также представителями отдела эксплуатации.

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.

Для обеспечения IT-безопасности промышленных систем «Лаборатория Касперского» предлагает решение Kaspersky Industrial Cyber Security, которое защищает инфраструктуру системы управления производственными процессами и поддерживает их бесперебойное выполнение.

Решение Kaspersky Industrial Cyber Security разрабатывалось с учетом ключевых особенностей промышленных сред; особое внимание при этом уделялось обеспечению непрерывности производственных процессов. Решение предназначено для защиты сложных сред, построенных на узкоспециализированных собственных платформах.

Широкие возможности настройки Kaspersky Industrial Cyber Security позволяют сконфигурировать решение в точном соответствии с требованиями конкретной ICS-среды. Подбор оптимальной конфигурации защитных технологий и сервисов осуществляется после полного аудита инфраструктуры экспертами «Лаборатории Касперского».

KASPERSKY INDUSTRIAL CYBER SECURITY:

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

Защита от APT-атак

Комплексные таргетированные угрозы (APT-атаки, Advanced Persistent Threats) получают все более широкое распространение. При этом одна подобная атака, если ее вовремя не обнаружить, может причинить компании ущерб, исчисляемый миллионами долларов. В связи со сложностью и большой продолжительностью подобных атак традиционных решений для защиты рабочих мест для эффективной борьбы с ними уже недостаточно. Для обеспечения безопасности предприятий необходимо специализированное решение, основанное на анализе актуальных угроз.

В последние годы стоимость разработки APT-атак значительно снизилась. В связи с этим число киберпреступников, считающих экономически выгодным атаковать предприятия и организации, значительно возросло. В то же время технологии и сценарии проведения APT-атак стали намного сложнее: сначала киберпреступники собирают максимум информации об IT-инфраструктуре предприятия-жертвы, в том числе о предпринимаемых мерах безопасности. Эти сведения позволяют им определить слабые места и бреши в системе защиты, которые затем используются во время атаки.

Обычное решение для обеспечения IT-безопасности, установленное в корпоративной сети, может успешно заблокировать ту или иную вредоносную программу. Однако, если она была компонентом APT-атаки, это не остановит киберпреступников, которые продолжат искать другие пути для заражения IT-инфраструктуры организации. Возможность вовремя определить, что вредоносная программа или ее часть являются звеньями целевой атаки, позволяет свести к минимуму возможный ущерб.

Комплексная природа APT-атак значительно усложняет задачу защиты от них. Для выяснения, подвергается ли организация такой атаке, требуется непрерывный анализ данных. Однако даже крупные международные компании не могут себе позволить содержать специализированный отдел, отслеживающий и анализирующий актуальные угрозы в глобальном масштабе.

Широкие возможности и многоуровневая стратегия «Лаборатории Касперского» помогают успешно бороться с APT-атаками, нацеленными на предприятия и организации. Решения и экспертиза «Лаборатории Касперского» позволяют эффективно обнаруживать и анализировать APT-угрозы, а также оперативно блокировать их, минимизируя наносимый ими ущерб.

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

Потенциальный ущерб от атаки можно значительно снизить за счет своевременного обнаружения и устранения уязвимостей в ОС и установленных программах. Решения «Лаборатории Касперского» включают инновационные технологии, которые по функционалу и возможностям значительно превосходят базовое антивирусное программное обеспечение. В дополнение к системе мониторинга уязвимостей и средствам установки исправлений ПО и операционных систем, они включают технологию автоматической защиты от эксплойтов (Automatic Exploit Prevention), которая контролирует работу приложений, наиболее часто подвергающихся атакам хакеров. Контроль программ и динамические белые списки позволяют обеспечить выполнение в корпоративной сети только разрешенного безопасного ПО.

ОБЫЧНОЕ ВРЕДОНОСНОЕ ПО ИЛИ ЧАСТЬ APT-АТАКИ?

Чем раньше компания определит, что подвергается APT-атаке, тем быстрее она сможет ее блокировать, минимизировать связанные с ней затраты и вернуться к нормальной работе. Использование распределенной архитектуры датчиков внутри корпоративной сети позволяет определить, является ли обнаруженное вредоносное ПО частью APT-атаки или нет.

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ

Для тех компаний, которые подверглись атаке, «Лаборатория Касперского» предлагает ряд сервисов по анализу компьютерных инцидентов, которые включают все стадии расследования инцидента, в том числе разработку рекомендаций по мерам, необходимым для укрепления системы IT-безопасности предприятия.

Расширенная техническая поддержка

Поскольку IT-системы служат фундаментом важнейших бизнес-процессов любой организации, перебои в их работе недопустимы. Если онлайн-ресурс компании в течение какого-то времени недоступен клиентам, или из-за перебоев в работе корпоративной сети сотрудники не могут выполнять свои повседневные задачи, серьезно страдают и производительность труда, и деловая репутация компании, и доходность бизнеса.

Когда инцидент безопасности приводит к простою IT-систем, последствия могут затронуть все аспекты деятельности компании и стать причиной ряда серьезных проблем:

- Невозможность осуществления продаж ведет к снижению прибыли
- Невыполнение соглашений об уровне обслуживания может стать причиной судебных исков со стороны клиентов
- Нарушение договоренностей может повлечь за собой ухудшение взаимоотношений с поставщиками и проблемы в цепи поставок
- Остановка внутренних бизнес-процессов приводит к снижению производительности бизнеса в целом
- В случае задержек ключевых платежей возрастает вероятность штрафов и комиссий
- Может быть нанесен серьезный ущерб репутации и имиджу компании
- Неизбежны прямые финансовые затраты на устранение IT-инцидента

РАСШИРЕННАЯ ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Периоды простоя, вызванные сбоями в работе IT-инфраструктуры предприятия, дорого обходятся бизнесу. Премиальная техническая поддержка, предоставляемая «Лабораторией Касперского» в рамках пакетов услуг Enterprise и Business, дает возможность минимизировать ущерб от компьютерных инцидентов и сбоев в работе системы обеспечения IT-безопасности организации. Обширные знания и богатый экспертный опыт специалистов «Лаборатории Касперского» позволяют в каждом случае максимально быстро и эффективно вернуть работу предприятия в обычное русло.

Расширенная техническая поддержка

Чтобы помочь компании-клиенту обеспечить непрерывность своих бизнес-процессов, минимизировать количество инцидентов безопасности и сбоев в работе IT-инфраструктуры, «Лаборатория Касперского» предлагает ряд профессиональных сервисов, а также набор программ расширенной технической поддержки.

С каждой компанией-клиентом работает персональный технический менеджер. Он принимает сообщение об имеющейся проблеме и передает ее на рассмотрение выделенной группе экспертов (технических специалистов и аналитиков) «Лаборатории Касперского», для которой ее решение является приоритетной задачей.

ПРОФЕССИОНАЛЬНЫЕ УСЛУГИ

Специалисты «Лаборатории Касперского» готовы оперативно провести установку и обновление решений компании в рамках следующих сервисов:

- **Установка и обновление версий:** проектирование, развертывание, настройка и обновление решений «Лаборатории Касперского» для бизнеса
- **Обучение** IT-специалистов компании-клиента 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 IT-инфраструктуры компании-клиента с предоставлением подробного отчета и рекомендаций

Экспертиза в области кибербезопасности

Новые киберугрозы появляются каждый день. Они действуют под разными масками и используют для атак множество различных векторов. Единого решения, которое бы обеспечило всеобъемлющую защиту, не существует. Однако даже в нашем мире «больших данных», чтобы успешно бороться против новейших угроз, крайне важно знать, откуда ожидать нападения.

Специалисты по информационной безопасности несут ответственность за защиту организации от актуальных угроз и за предупреждение угроз, которые возникнут в ближайшие годы. Это требует не просто обеспечения ежедневной защиты от уже известных угроз, но стратегического анализа угроз и знания перспектив их развития. Очень немногие компании имеют ресурсы для разработки необходимых для этого структур своими силами.

«Лаборатория Касперского» – это ценный бизнес-партнер, всегда готовый поделиться с вашими специалистами новейшей информацией об актуальных угрозах, используя для этого различные каналы. Широкий спектр способов доставки информации помогает вашей службе IT-безопасности быть во всеоружии и эффективно защищать организацию от любых интернет-угроз.

Даже если ваша организация не работает с защитными продуктами «Лаборатории Касперского», вы можете использовать все преимущества наших экспертных сервисов.

ОБУЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

В рамках этой инновационной образовательной программы «Лаборатория Касперского» делится своими экспертными знаниями и опытом в сфере информационной безопасности, а также уникальными данными о киберугрозах. Обучение сотрудников и развитие у них навыков применения передовых технологий IT-безопасности – один из ключевых элементов эффективной корпоративной стратегии, направленной на защиту от угроз и минимизацию последствий кибератак.

ДАННЫЕ ОБ УГРОЗАХ

Предоставление новейших данных о киберугрозах из облачного сервиса Kaspersky Security Network с целью заблаговременного предупреждения о них государственных учреждений, поставщиков сервисов киберзащиты и телекоммуникационных операторов. Эти данные помогают им усилить меры безопасности путем блокирования вредоносного ПО на инфраструктурном уровне.

МОНИТОРИНГ БОТНЕТОВ

Позволяет поставщикам сервисов киберзащиты и финансовым организациям отслеживать активность ботнетов, направленную на пользователей конкретных онлайн-сервисов, и своевременно блокировать соответствующие атаки.

АНАЛИТИЧЕСКИЕ ОТЧЕТЫ

В рамках подписки поставщики сервисов киберзащиты и финансовые организации получают подробную информацию о тенденциях в области развития киберугроз, в том числе характерных для того или иного региона. Информация подготавливается на основе аналитических данных, предоставляемых командой Глобального исследовательско-аналитического центра «Лаборатории Касперского», а также получаемых из других внутренних источников компании.

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Ведущие эксперты в сфере анализа вредоносного ПО в сотрудничестве со специалистами, имеющими большой опыт работы в правоохранительных органах, оказывают помощь в расследовании инцидентов в сфере IT-безопасности, а также помогают компании-клиенту сформировать собственную стратегию защиты, предоставляя углубленный анализ угроз, актуальных для данной организации.

«Лаборатория Касперского» обеспечивает лучшую защиту*

Продукты и технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч организаций по всему миру. На сегодняшний день в компании работают более 3000 высококвалифицированных специалистов, треть из которых занимается исследованиями и разработкой.

Наиболее ценный актив компании – обширный экспертный опыт, накопленный за годы борьбы с киберугрозами. Благодаря своей уникальной экспертизе «Лаборатория Касперского» по праву считается одним из лидеров в отрасли информационной безопасности, предоставляя своим клиентам передовые решения для защиты от всех типов кибератак.

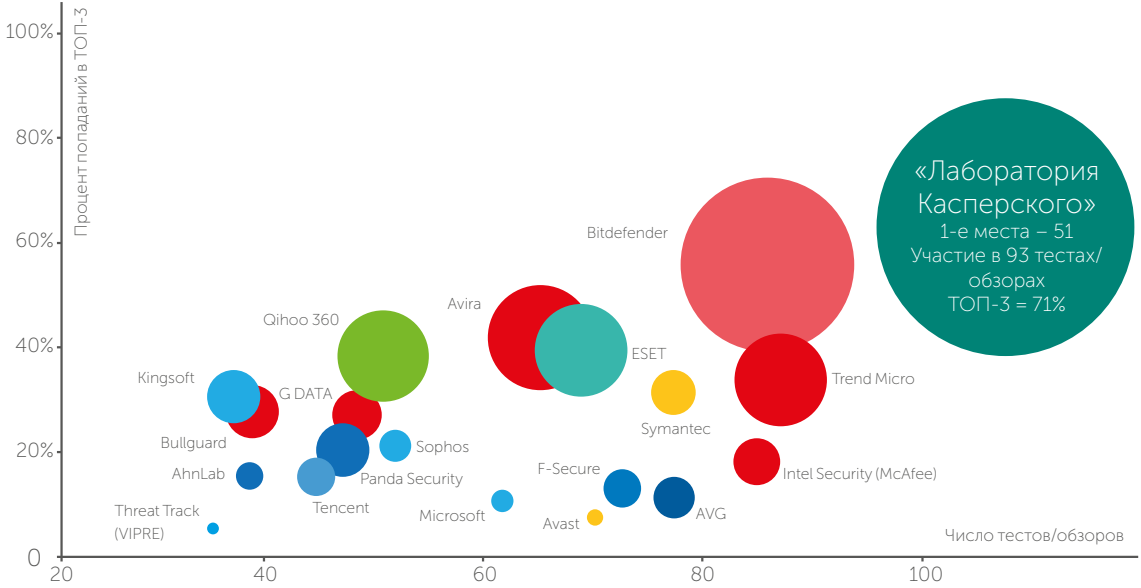
Глобальный центр исследований и анализа угроз (GReAT) «Лаборатории Касперского» был создан в 2008 году для расследования инцидентов безопасности, изучения угроз и развития инноваций. Сегодня это международная команда ведущих экспертов в области IT-безопасности, работающих во всех регионах присутствия компании и активно участвующих в расследовании киберинцидентов. Специалисты GReAT обнаружили и проанализировали такие сложные угрозы, как Flame, Gauss, miniFlame, Red October, NetTraveler, Icefog, The Mask, Darkhotel, Regin и др.

Защитные решения «Лаборатории Касперского» ориентированы не только на борьбу с существующими угрозами, но и на предотвращение новых, еще не известных угроз. Они отвечают всем основным требованиям, предъявляемым к средствам для обеспечения информационной безопасности, включая высочайший уровень защиты, адаптируемость к меняющимся условиям, масштабируемость, совместимость с различными платформами, высокую производительность, отказоустойчивость и удобство использования.

Эффективность продуктов «Лаборатории Касперского» регулярно подтверждается результатами независимых тестов. В 2014 году компания заняла первое место среди производителей защитных решений по показателю TOP-3. По итогам 93 различных испытаний, проведенных авторитетными тестовыми организациями разных стран, решения «Лаборатории Касперского» вошли в тройку лидеров в 71% случаев и 51 раз занимали первое место. Это неоспоримое доказательство того, что «Лаборатория Каперского» предоставляет лучшую в отрасли защиту.

«Лаборатория Касперского» обеспечивает лучшую защиту

В 2014 году продукты «Лаборатории Касперского» для защиты рабочих мест и мобильных устройств приняли участие в 93 независимых тестах и обзорах. В 51 случае они заняли первое место и 66 раз вошли в тройку лучших (ТОП-3).



* Примечание:

- Включает тесты продуктов для бизнеса, домашних пользователей и мобильных приложений за 2014 год
- В обзор включены тесты, проведенные следующими независимыми организациями и изданиями: тестовые лаборатории AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs; Virus Bulletin
- Диаметр круга соответствует числу занятых первых мест

Подробнее: kaspersky.ru/top3

О «Лаборатории Касперского»

«Лаборатория Касперского» – крупнейшая в мире частная компания, работающая в сфере информационной безопасности, и один из наиболее быстро развивающихся вендоров защитных решений. Компания входит в четверку ведущих мировых производителей решений для обеспечения IT-безопасности пользователей конечных устройств (IDC, 2014). С 1997 года «Лаборатория Касперского» создает инновационные и эффективные защитные решения и сервисы для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. «Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира; ее технологии защищают более 400 миллионов пользователей по всему миру. Более подробная информация доступна на сайте www.kaspersky.ru.

АО «Лаборатория Касперского»
www.kaspersky.ru

Решения для бизнеса:
www.kaspersky.ru/corporate

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