KASPERSKY lab

РЕШЕНИЯ НОВОГО ПОКОЛЕНИЯ ДЛЯ ЗАЩИТЫ БИЗНЕСА

Как сравнить разные решения и выбрать именно то, что нужно вашей компании

www.kaspersky.ru

Когда вы выбираете новую стратегию IT-безопасности, которая помогла бы защитить ваш бизнес от актуальных угроз, вы сталкиваетесь с трудными вопросами.

Как разобраться, какие технологии надежно защитят ваш бизнес и при этом не ударят по продуктивности? Какие решения и какая стратегия обеспечения безопасности лучше всего подходят именно для вас?

Здесь, как и при принятии других важных решений, прежде всего нужно отделить факты от рекламы и понять, кто действительно может выполнить свои обещания.

БУДУЩЕЕ БИЗНЕСА ЗАВИСИТ ОТ IT-БЕЗОПАСНОСТИ

Вредоносных программ, атак и киберпреступлений становится все больше, и они становятся все сложнее, а значит, растет и риск, которому подвергается ваш бизнес. Поэтому сейчас как никогда важно выбрать самое надежное защитное решение.

При этом на кону стоит не просто часть вашего бюджета на IT. Неудачный выбор защитного решения может вызвать далеко идущие последствия:

- Программы-вымогатели могут зашифровать важную бизнес-информацию, что парализует работу компании.
- Утечка конфиденциальной информации может испортить отношения с клиентами и помешать вам заключить сделку.
- Утечка информации о ваших продуктах и другой интеллектуальной собственности может лишить вас заработанных честным трудом конкурентных преимуществ.

Опрос 5500 компаний из 26 стран показал, что:

- **90% компаний сталкивались с инцидентами безопасности**
- **46% потеряли важную информацию в результате этих инцидентов**

Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского» и B2B International, 2015 год

ПОЧЕМУ КОМПАНИИ ПО-ПРЕЖНЕМУ УЯЗВИМЫ?

На рынке уже много лет существуют решения, обеспечивающие IT-безопасность для бизнеса. Почему же компании по-прежнему становятся жертвами киберпреступников?

Киберпреступники давно поняли, сколько они могут заработать на успешных атаках на бизнес, поэтому тратят все больше времени и сил, чтобы продумать новые хитроумные атаки. Киберпреступность никуда не исчезнет — она слишком выгодна. Преступники и дальше будут стараться обойти защитные решения.

Но многие из компаний, ставших жертвами киберпреступников, сами им помогают.

ОШИБКИ КОМПАНИЙ

Многие организации считают, что они никогда не станут целью киберпреступников, и даже не пытаются защититься от атак. Однако сегодня целью атаки может стать любая компания, не обязательно крупная.

Любому бизнесу есть что защищать — например, информацию о клиентах и сотрудниках, бизнес-идею или стратегический план развития. Все это преступники могут попытаться перепродать вашим конкурентам. И это не говоря о денежных средствах, которые особо привлекательны для преступников...

Некоторые компании, понимая это, выстраивают эшелонированную оборону против отдельных видов атак, но забывают о других атаках и остаются против них беззащитными.

Другие же полностью полагаются на революционное решение, которое обещает стать настоящей панацеей... но почему-то не выполняет своих обещаний. К сожалению, некоторые компании готовы игнорировать факты и верить утверждениям, которые имеют мало отношения к реальности. Почему же так получается?

НЕЛЬЗЯ РЕШИТЬ ПРОБЛЕМУ РАЗ И НАВСЕГДА

Любое новое решение, которое обещает компании один ответ на все проблемы IT-безопасности, не требуя при этом регулярных обновлений и знаний сотрудников о киберугрозах — это именно то, о чем многие мечтают.

К сожалению, такое волшебное решение никогда не появится.

Но когда предприниматель видит громкие заявления о новом защитном решении, им могут завладеть эмоции. Особенно часто эмоциям поддаются компании, недавно пострадавшие от инцидента безопасности и спешащие выбрать новую стратегию. В этой спешке они не всегда выделяют достаточно времени и сил на сравнение предложений разных поставщиков.

Единственный способ создать надежное защитное решение — постоянно собирать и анализировать данные об угрозах. Однако для этого нужна большая команда экспертов по безопасности и аналитиков, работающая по всему миру. Очень немногие производители могут позволить себе такие инвестиции.

Те производители, которые готовы вкладываться в глобальную систему сбора данных, также тратят значительные средства на то, чтобы понять, в каком направлении злоумышленники будут развивать свои инструменты, чтобы заранее подготовить защиту от новых типов атак.

«Новое поколение» — это, конечно, звучит гордо, но на самом деле все куда проще. Компании, которые предлагают бизнесу действительно надежную защиту, понимают: все дело в постоянных исследованиях и аналитике угроз. Да, это долго, сложно, дорого и требует знаний, но волшебной альтернативы не существует.

ЛАНДШАФТ УГРОЗ ОПРЕДЕЛЯЕТ СТРАТЕГИЮ БЕЗОПАСНОСТИ

Компании должны быть защищены от всех IT-угроз:

- известных
- неизвестных
- сложных

Типы угроз разнообразны, а значит, ваша защита также должна быть многоуровневой.

Нельзя предсказать, с какими атаками столкнется ваша система, — поэтому если вы положитесь на решение нового поколения, которое хорошо отражает только один тип угроз, то окажетесь в очень уязвимом положении.

Киберпреступники постоянно стараются перехитрить разработчиков решений для обеспечения IT-безопасности, поэтому полагаться на один уровень защиты — это ошибка. Несколько уровней защиты, частично дублирующих функции друг друга, — это намного лучше: даже если преступник преодолеет один уровень, то его встретит новый слой защиты.

ПОЛИТИКА БЕЗОПАСНОСТИ ЗАВИСИТ ОТ РЕСУРСОВ

Любая компания не хочет тратить слишком много времени на управление безопасностью. И прежде всего, массу времени экономит решение, которое использует единую интегрированную консоль, из которой можно управлять решениями безопасности на всех узлах, в том числе на мобильных устройствах и серверах.

Вы можете выбрать решение, которое использует локальную инфраструктуру, либо решение с облачной консолью, для которой не нужен отдельный сервер. Большинство локальных решений безопасности предлагают очень гибкие настройки, но чтобы их установить и поддерживать их нужны время и силы.

Напротив, некоторые облачные решения могут серьезно упростить управление безопасностью. Такие решения идеально подходят для компаний с маленькими IT-командами или для компаний, которые хотят полностью поручить управление безопасностью стороннему консультанту.

Решения с облачной консолью имеют целый ряд преимуществ:

- Консоль работает из облака, поэтому вам не придется покупать, устанавливать и поддерживать локальный сервер для управления безопасностью.
- Начать работу можно намного быстрее.
- На управление безопасностью требуется намного меньше времени и сил.
- В консоль можно зайти с любого устройства, у которого есть доступ к интернету.

МИФЫ О «НОВОМ ПОКОЛЕНИИ» СРЕДСТВ ЗАЩИТЫ

Давайте обсудим то, что производители обычно говорят о защитных решениях «нового поколения».

Миф 1: Традиционный антивирус больше не нужен

Это, пожалуй, самый главный миф об IT-безопасности. Антивирус, основанный на сигнатурном методе, не защитит компанию от неизвестных и сложных угроз, но это все равно очень важная часть многоуровневой защиты и очень эффективный способ блокировки вредоносных программ. Более того, лучшие из современных решений используют облачные технологии, чтобы быстрее обновлять сигнатуры, — поэтому пользователи сразу получают защиту от новейших угроз.

Слишком многие компании узнали на личном опыте, что игнорирование этого важного слоя IT-безопасности может дорого им обойтись: «универсальные решения» могут оказаться не слишком универсальными или заблокировать полезное приложение, нужное для работы.

Миф 2:
Обновления защитных решений парализуют работу IT

Мы помним, какой была IT-безопасность раньше: антивирусы обновлялись очень медленно и парализовывали работу. Но с тех пор многое изменилось.

К счастью, сегодня существует множество решений, специально разработанных так, чтобы как можно меньше влиять на производительность, несмотря на регулярные обновления. Многие приложения также обновляют отдельно разные уровни защиты, что делает их еще надежнее.

Миф 3:
Редко обновляемые решения тоже дают высокий уровень защиты

Некоторые разработчики пытаются превратить тот факт, что они относительно редко обновляют свои решения, в преимущество: ведь это якобы позволяет сэкономить ресурсы. К сожалению, безопасность — это не то, на чем стоит экономить трафик в корпоративной сети, а редкие обновления — не очень хорошая идея.

Своевременные обновления сигнатур, которые блокируют известные угрозы, и эвристических моделей для борьбы с неизвестными угрозами необходимы для надежной защиты ваших устройств. Более того, регулярные обновления также позволяют свести к минимуму число ложных срабатываний антивируса, что также экономит ваше время и ресурсы.

Обновления просто не должны влиять на продуктивность компьютера.

Миф 4:
Новое поколение — это революция!

В таких важных вопросах значение имеют только реальные результаты решения и эффективность его работы в прошлом. Тщательно проверяйте, что скрывается под названием «новое поколение».

БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ КОТОРОЙ ДОКАЗАНА

Технологии «Лаборатории Касперского» которые сочетают машинное обучение и экспертные данные мирового уровня, справедливо могут отнесены к решениям нового поколения. Но мы так работаем уже много лет — потому что хотим достичь хороших результатов, а не для того, чтобы делать громкие заявления.

Лучше всего о качестве решений говорят результаты независимых тестов.

Уже три года подряд продукты «Лаборатории Касперского» участвуют в рекордном числе тестов и получают рекордное число наград. Решения компании завоевали больше первых мест и больше мест в тройке лучших, чем решения других разработчиков.

МНОГОУРОВНЕВАЯ ЗАЩИТА ВСЕЙ IT-ИНФРАСТРУКТУРЫ

Секрет надежности решений «Лаборатории Касперского» — в многоуровневом подходе к защите. В решениях используется сигнатурный метод, эвристический анализ, проактивная защита, автоматическая защита от эксплойтов и многие другие передовые технологии.

А благодаря тому, что решения получают данные об угрозах из облачной сети Kaspersky Security Network, они быстрее реагируют на новые опасности.

Кроме того, у продуктов «Лаборатории Касперского» высокий уровень обнаружения угроз сочетается с низким числом ложных срабатываний.

«Лаборатория Касперского» предлагает ряд комплексных решений для защиты бизнеса, которые могут защитить все виды устройств — компьютеры, ноутбуки, серверы, смартфоны и планшеты. У компании также есть решения для защиты отдельных узлов сети: для систем хранения данных, виртуальных сред, почтовых серверов и т. д.

В независимых испытаниях на число ложных срабатываний технологии «Лаборатории Касперского» показали идеальный результат: 0 ложных срабатываний.

Испытания были проведены в январе и феврале 2016 года институтом AV-TEST.

ВЫБЕРИТЕ РЕШЕНИЕ ДЛЯ СВОЕГО БИЗНЕСА

Решение **Kaspersky Endpoint Security Cloud** создано специально для компаний малого и среднего бизнеса. Оно идеально подходит организациям, у которых работает либо немногочисленная штатная IT-команда, либо ее нет вообще.

Основные преимущества решения:

- Защита компьютеров, ноутбуков и файловых серверов на платформе Windows и мобильных устройств на Android™ и iOS®*

- Удобное управление через облачную консоль, которая:
  – Экономит ваше время и деньги — не нужно устанавливать отдельный сервер
  – Упрощает развертывание — установка консоли не требуется
  – Интуитивно понятна — не требуется специальных знаний

  Подробнее: www.litek.ru/kes-cloud

Kaspersky Security для бизнеса предлагает гибкую настройку для более крупных или более требовательных к безопасности компаний. Это решение поддерживает более широкое число платформ:

- Компьютеры и ноутбуки — Windows®, Mac® и Linux®
- Файловые серверы — Windows, Linux и FreeBSD®
- Мобильные устройства — Android, iOS и Windows Phone®

Подробнее: www.litek.ru/kes-business

*Набор доступных функций зависит от защищаемой платформы

ВАШ СЛЕДУЮЩИЙ ШАГ

Когда продавец в следующий раз предложит вам решение безопасности нового поколения, обязательно спросите его о результатах независимых испытаний, чтобы проверить, насколько хорошо продукт работает на самом деле.

Как показали себя в независимых испытаниях продукты «Лаборатории Касперского», вы уже знаете. Вы можете бесплатно оценить преимущества облачного решения и понять, насколько оно подходит вашей компании.

Попробуйте Kaspersky Endpoint Security Cloud бесплатно в течение 30 дней:

www.litek.ru/kes-cloud

ВАШ ПАРТНЕР

ЛИТЕК | Лицензионное программное обеспечение для вашей информационной безопасности

+7 (343) 219-73-53
+7 (343) 350-78-76
adm@litek.ru

- Антивирусная защита
- Информационная безопасность
- Лицензирование ПО
- Техническая поддержка

www.litek.ru

Почему нам можно доверять?

БЫСТРОТА

Готовы отвечать на ваши вопросы в кратчайшие сроки

ЛИЦЕНЗИРОВАНИЕ

Поможем разобраться в тонкостях лицензирования

ТЕХПОДДЕРЖКА

Бесплатная техническая поддержка от наших специалистов

Решения для защиты бизнеса www.litek.ru/kes-business

KASPERSKY lab