ЗАЧЕМ ИНВЕСТИРОВАТЬ В IT-БЕЗОПАСНОСТЬ

Задача, решение, результат

Kaspersky Security для бизнеса.
Время серьезных решений.
kaspersky.ru/business

KASPERSKY lab

КАК БИЗНЕС ВЛИЯЕТ НА IT

1

Трудно переоценить условия работы современных компаний. Для поддержания конкурентоспособности всем им приходится решать похожие задачи: увеличивать гибкость, повышать эффективность и производительность труда. Стремясь достичь этих целей, компании обращаются к IT-специалистам за решениями по оптимизации процессов, внедрением новых систем и технологий, а также за созданием надежной системы защиты постоянно растущего объема корпоративной информации и управления ею.

Вкратце о проблеме

Технологии, используемые сегодня на любом предприятии, часто поражают уровнем своей сложности.

Бизнес в целом все больше зависит от современных технологий и интернета: данные должны передаваться и использоваться все быстрее, становясь при этом доступнее для постоянно растущего круга сотрудников, поставщиков и клиентов.

Мобильность сотрудников — наиболее часто упоминаемая тенденция в развитии бизнеса, которая изменила способ работы и общения для многих из нас.

С точки зрения обеспечения IT-безопасности это означает, что методы и средства защиты, эффективные еще пару лет назад, сегодня уже считаются устаревшими.

В то время как большинство IT-специалистов признают наличие такой тенденции, многие компании не считают нужным инвестировать в создание одновременно надежного и адаптивного подхода к изменчивым потребностям мира бизнеса.

Данное руководство, предлагающее бизнес-аргументы за развитие и улучшение сферы IT-безопасности, составлено с учетом перечисленных проблем.

В руководстве приводятся важные факты, которые помогут сформулировать прочное экономическое обоснование, точно определить потребности бизнеса и защитить его от текущих и будущих угроз.

ЗАЧЕМ ЧИТАТЬ ЭТО РУКОВОДСТВО?

- Ознакомиться с ключевыми фактами и статистикой, которые помогут экономически обосновать необходимость вложений в IT-безопасность.
- Больше узнать о рисках IT-безопасности и способах борьбы с ними.
- Выяснить, как новые интегрированные платформы обеспечения безопасности защищают рабочие места и повышают производительность.
- Узнать, как «Лаборатория Касперского» может устранить слабые места в вашей системе безопасности и уменьшить количество используемых вами инструментов.

ПОЧЕМУ НЕЛЬЗЯ ИСПОЛЬЗОВАТЬ УСТАРЕВШИЕ ТЕХНОЛОГИИ?

2

Мобильные устройства, удаленные сотрудники, съемные носители, приложения сторонних производителей, веб-приложения... Все это повышает производительность. Но в то же время — делает вашу компанию еще более уязвимой.

Традиционные методы защиты больше не работают

Чтобы справиться со всем разнообразием угроз, с которыми может столкнуться ваш бизнес, одних антивирусных программ уже недостаточно.

И дело не только в устаревших технологиях: 58% компаний признают, что их службы IT-безопасности испытывают недостаток ресурсов хотя бы по одному из трех пунктов: персонал, системы или знания[1].

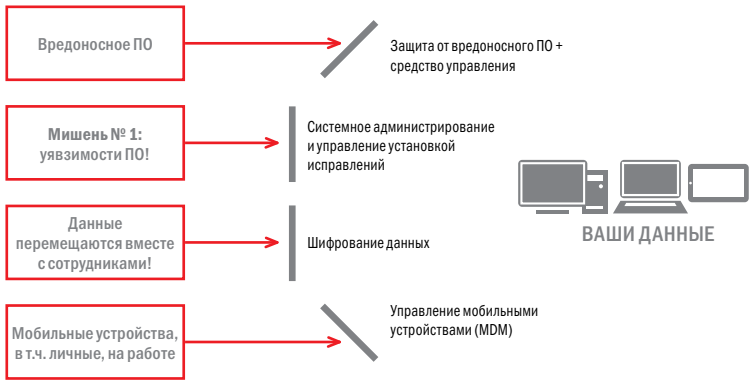
Если вы занимаетесь обеспечением IT-безопасности, то, вероятно, бежите изо всех сил, чтобы просто оставаться на месте. Или безуспешно пытаетесь получить поддержку, необходимую для эффективной борьбы с угрозами. Или привычно жонглируете постоянно растущим набором разрозненных решений (см. рис. 1), каждое из которых имеет собственную консоль, пользовательский интерфейс и требования по обслуживанию. Не говоря уже о проблемах совместимости, которые вам приходится решать.

Бизнес наращивает использование новых технологий, не учитывая связанные с ними аспекты безопасности. Некоторые компании готовы к атакам, но гораздо больше таких, чья наивность притягивает к себе все более изощренных и организованных хакеров, спамеров и разработчиков вредоносного и шпионского ПО.

ЧТО МЫ ИМЕЕМ?

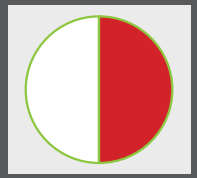
Вы гоняетесь за собственным хвостом: лишь внедрив технологию, вы начинаете думать, как одновременно отреагировать на изменения, оценить риски и защитить свой бизнес.

Рис. 1. Разные решения — разные консоли управления

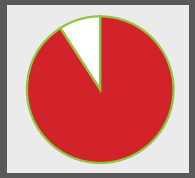


ЗНАЕТЕ ЛИ ВЫ, ЧТО...

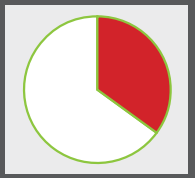
50% ОРГАНИЗАЦИЙ СЧИТАЮТ, ЧТО КИБЕРУГРОЗЫ КРИТИЧЕСКИ ОПАСНЫ ДЛЯ БИЗНЕСА[1]



91% ОРГАНИЗАЦИЙ ПОДВЕРГАЛИСЬ В ПРОШЛОМ ГОДУ ПРЯМОЙ КИБЕРАТАКЕ[1]



35% ОРГАНИЗАЦИЙ СТАЛКИВАЛИСЬ С СЕРЬЕЗНЫМИ ПОТЕРЯМИ ДАННЫХ[1]



1. Источник: «Лаборатория Касперского», Global IT Risk Report, 2012

Как единая платформа для обеспечения безопасности может изменить ситуацию?

Единые платформы для обеспечения безопасности помогут справиться со стоящими перед вами сложными задачами.

Скорее всего, ваша компания уже использует достаточно надежное антивирусное решение, однако этого недостаточно — необходимо уметь бороться не только с вирусами, но и с другими видами угроз. Например, не забывать об установке исправлений для устранения уязвимостей в приложениях, защите данных на ноутбуках или обеспечении безопасности мобильных устройств.

Основная проблема заключается не в отсутствии нужных инструментов, а в том, что каждое отдельное средство увеличивает сложность системы защиты, что сильно помешает, когда вы захотите внедрить свои политики безопасности. А, как известно, сложность — это враг IT-безопасности.

Интеграция инструментов обеспечения безопасности со средствами системного администрирования позволяет использовать единую консоль для удовлетворения растущих потребностей в области обеспечения безопасности.

Такое решение объединяет контроль рабочих мест, шифрование данных и управление мобильными устройствами, а также обеспечивает защиту вашей сети от вредоносного ПО.

Единая платформа для обеспечения безопасности предлагает IT-специалистам простой способ управления затратами, повышения производительности, снижения нагрузки на систему и централизации управления (см. рис. 2).

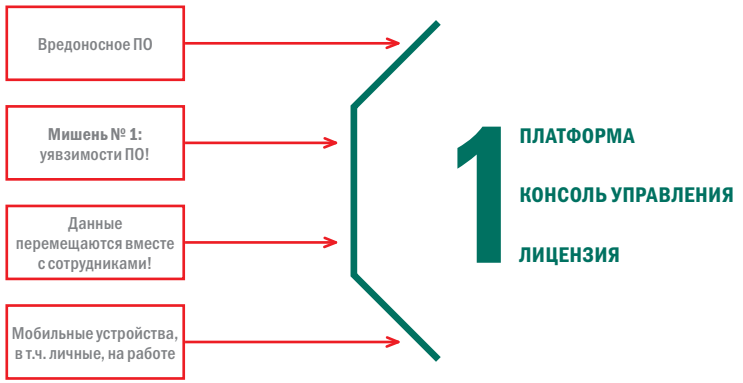
Глубокая интеграция компонентов повышает надежность и стабильность системы.

Важно помнить!

Существует большая разница между просто интеграцией различных инструментов и использованием единой платформы. Степень интеграции также может быть различной. Между тем для многих слово «интеграция» стало просто синонимом «совместимости».

Отличие единой платформы в том, что преимущества всех из входящих в нее компонентов дополняют друг друга. Благодаря этому возможности комплексного решения значительно шире, чем возможности набора различных инструментов, которые могут быть недостаточно совместимы между собой.

Рис. 2. Единая платформа для обеспечения безопасности



ПРЕИМУЩЕСТВА ЕДИНОЙ ПЛАТФОРМЫ

- Позволяет легко и просто оценить риски для всех систем и устройств.
- Дает возможность последовательно применять политики.
- Приводит систему безопасности в соответствие с общими целями компании.
- Таким образом, вы сможете снизить риск потери данных, упростить структуру обеспечения безопасности, сократить вложения и при этом соблюсти все требования бизнеса.

МОБИЛЬНОСТЬ, ИСПОЛЬЗОВАНИЕ ЛИЧНЫХ УСТРОЙСТВ: КАКОВЫ РИСКИ?

4

Итак, каковы фактические риски? Переизбыток технологий, ограниченность ресурсов и слабое понимание многих проблем безопасности — лишь вершина айсберга...

Мобильность, разнообразие мобильных устройств и приложений

«Умные» устройства повышают производительность, но они же приносят и новые угрозы.

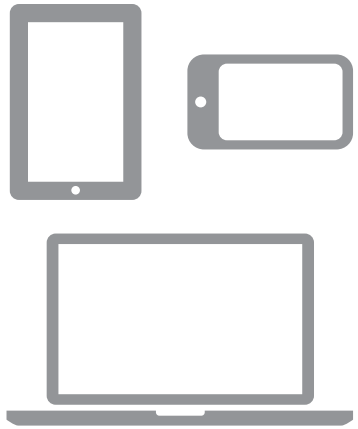
Сегодня среднестатистический сотрудник, работающий с данными, использует три устройства. Это значит, что компаниям приходится выделять больше ресурсов для решения задач контроля и управления, растут риски утраты данных и количество атак вредоносного ПО, увеличивается сложность систем.

Сотрудники приносят личные устройства на работу независимо от того, разрешено это или нет, и часто оставляют их без присмотра вместе с находящимися на них конфиденциальными данными компании.

Использование личных устройств особенно популярно среди руководителей разного уровня, так что ответственному лицу приходится разбираться не только с блокировкой потерянных устройств, но и с недовольством сотрудников, привыкших получать доступ к корпоративной сети и данным компании. Все это может привести к тому, что IT-департамент утратит контроль над ситуацией.

44% компаний во всем мире позволяют сотрудникам бесконтрольно подключать к сети и корпоративным ресурсам свои ноутбуки, а 33% — также и смартфоны[2].

В марте 2012 года «Лаборатория Касперского» в сотрудничестве с аналитиками Bathwick Group провела глобальное исследование «Безопасность на фоне меняющихся технологий», которое продемонстрировало, что источником наибольшего беспокойства IT-специалистов во всем мире является мобильность (см. рис. 3).



РЕЗЮМЕ

- Использование личных устройств на работе увеличивает сложность системы: в среднем каждый сотрудник использует по три устройства.
- 44% компаний разрешают сотрудникам бесконтрольный доступ к сети и корпоративным ресурсам с личных ноутбуков.
- Мобильность в настоящее время вызывает наибольшее беспокойство среди IT-специалистов всего мира.

Рис. 3. Какие факторы, действующие в вашей организации, создают наибольшие проблемы в области безопасности?[2]

2. Источник: «Лаборатория Касперского», Global IT Risk Report, 2012

5

Вместо борьбы с использованием личных устройств на работе следует искать способы управлять ими.

Благодаря сотрудникам, использующим на работе собственные устройства, компании повышают эффективность, рентабельность и гибкость бизнеса. Однако системные администраторы знают, что не все так просто.

Преимущества для бизнеса могут быстро обернуться проблемами в сфере IT-безопасности — потерей данных, сложностями с управлением устройствами, многочисленными платформами и различными приложениями. Вскоре использование личных устройств и мобильность уже не покажутся такой уж хорошей идеей.

Кроме того, не стоит забывать и о постоянном росте числа киберугроз, ориентированных на мобильные устройства и их приложения.

Операционные системы iOS и OS X компании Apple, а также семейство Android от Google сегодня собирают не меньший урожай вирусов, чем Windows. Во втором квартале 2012 года количество троянов, нацеленных на платформу Android, почти утроилось по сравнению с тем же периодом 2011 года[3] (см. рис. 4).

Тенденция к росту сохранится, так как простота, с которой можно украсть или перехватить данные с мобильного устройства делового человека, делает мобильную связь крайне привлекательной областью для киберпреступников.

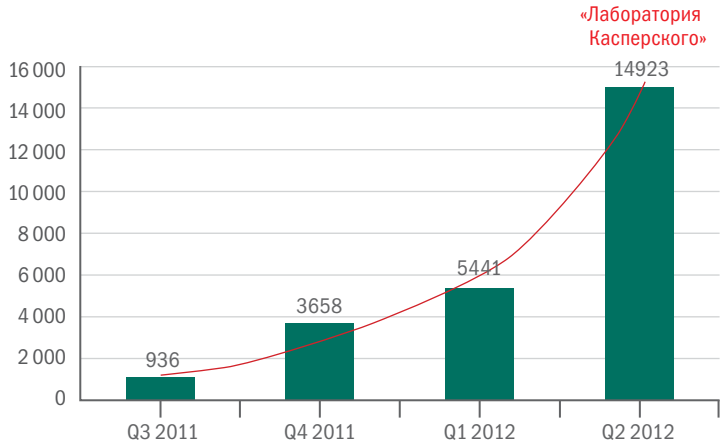
«Использование личных устройств на работе — один из самых серьезных рисков для IT-безопасности. Присутствие в сети личных устройств ставит дополнительные задачи при построении системы защиты. Необходимо целиком и полностью разделять использование устройства в личных и рабочих целях».

Роул Шоуэнберг (Roel Schouwenberg),
эксперт «Лаборатории Касперского»

ЕСТЬ НАД ЧЕМ ПОДУМАТЬ

- Как защитить рабочую информацию на устройстве пользователя, не отказываясь от использования на работе личных устройств, позволяющих экономить на оборудовании?
- Как гарантировать, что выбор приложений сотрудниками не приведет к появлению вредоносных программ в сети?
- Как достичь равновесия между ключевыми требованиями бизнеса и задачами обеспечения безопасности?

Рис. 4. Количество обнаруженных модификаций вредоносного ПО для Android OS



3. Источник: securelist.ru

▶ ШИФРОВАНИЕ: НАСКОЛЬКО ВЫ ДОРОЖИТЕ ДАННЫМИ?

6

IT-специалисты часто сталкиваются со случаями потери устройств. Конечно, их огорчают затраты на приобретение нового оборудования взамен утраченного. Но это лишь вершина айсберга. Куда болезненней проблема защиты конфиденциальной информации, оказавшейся на потерянном устройстве.

Добавьте к этому постоянно растущие правительственные штрафы, ущерб репутации компании и потерю лояльных клиентов — и станет ясно, что цена утечки данных значительно превышает стоимость замены оборудования.

Чтобы лучше понять истинную ценность надежной защиты, давайте рассмотрим простой пример: ноутбук, потерянный в аэропорту. Заодно упомянем и риски, связанные с этой ситуацией.

Только в Соединенных Штатах каждую неделю в аэропортах теряется 12 тысяч ноутбуков[4]. В год это составляет 624 тысячи, причем только стоимость оборудования оценивается в 987 млн долларов. И это – данные лишь по одной стране. Представьте, какими могут быть цифры для всего мира — а это ведь еще не полная картина[4].

Вместе с тем существуют и более значительные финансовые потери, неочевидные на первый взгляд, — это стоимость утечки данных.

Стоимость утечки данных при этом оценивается в 25 млрд долларов убытков в год.

И это только в одной стране! Что же тогда творится в мире?

При этом 85% опрошенных клиентов заявили, что откажутся от дальнейшего сотрудничества с компанией, которая потеряла их данные, а 47% — готовы подать на такую компанию в суд[4].

Шифрование привыкли считать сложным и дорогим процессом, хоть это уже давно не так: 43% крупных предприятий шифруют все свои данные, а 36% компаний малого бизнеса шифруют конфиденциальные данные[4].

Это известно всем, но не будет лишним повторить: посторонние пользователи и преступники не в состоянии прочитать зашифрованные данные.
Шифрование — важнейший компонент единой платформы защиты рабочих мест.

«Распространение шифрования прямо связано с растущим пониманием того, что всегда сотрудники, которые работают в любое время, в любом месте и с любого устройства, подвергают незашифрованные данные беспрецедентному риску».

Дэвид Эмм (David Emm),
эксперт «Лаборатории Касперского»

Рис. 5

4. Источники: WMBF News, октябрь 2012 г. Исследование Newspoll, ноябрь 2011 г. Исследование Ponemon Institute «Стоимость ноутбука» (The cost of a laptop), апрель 2009 г. Отчет “Лаборатории Касперского” Global IT Risk Report, 2012

ЗАЩИТА РАБОЧЕГО МЕСТА: ВОЗМОЖНЫЕ ВАРИАНТЫ

7

Вариант 1. Только антивирус

Мощная и современная антивирусная программа играет центральную роль в обеспечении IT-безопасности. Но одного этого недостаточно, чтобы защитить бизнес от целевых атак, использующих, помимо вирусов, другие методы, например фишинг или социальную инженерию. Антивирус не поможет вам справиться со всеми и полностью обеспечить безопасность.

Вариант 2. Покупка универсального пакетного решения

Некоторые решения по обеспечению безопасности предлагают множество функций: шифрование, антивирус, мониторинг уязвимостей. Казалось бы, что еще нужно для полной безопасности? Но что делать, если одни функции вам нужны, а другие — нет? Что если сегодня вы прекрасно обходитесь без, предположим, управления мобильными устройствами, но знаете, что в будущем году организация планирует разрешить использование личных устройств на работе, — можно ли добавить этот компонент потом, чтобы не платить за лишние функции?

Знаете ли вы, куда на самом деле вкладываете деньги? Решения могут поставляться в одной упаковке, но в действительности многие из них представляют собой скомпонованные средства, приобретенные у других компаний. Они не всегда так хорошо совместимы, как кажется на первый взгляд, и в случае неполадок причинят проблем больше, чем решат.

Вариант 3. Выбор нескольких решений от разных поставщиков и отладка их совместной работы

На рынке представлено много качественных решений. Проблема в том, как заставить их работать вместе. Даже при удачном выборе программ перед вами все равно встанут проблемы совместимости разных агентов и консолей с разными планами обслуживания и разными типами отчетов.

Вы не сможете полностью использовать весь потенциал отдельных решений — хотя бы из-за того, что они не были предназначены для совместной работы.

Сложность — враг IT-безопасности. Обзор всей системы обеспечения безопасности в едином окне не только высвобождает время для выполнения других задач, но и дает более полное представление о текущих — и будущих — потребностях безопасности.

ЗА И ПРОТИВ

Пакет «все в одном»

За. Кажется менее сложным, требует меньшего количества лицензий, дешевле, чем покупка отдельных приложений.

Против. Часто компоненты разрабатываются различными компаниями, в результате чего отсутствует полноценная интеграция.

Против. Поскольку решение разработано «на все случаи жизни», часто приходится платить за ненужные пока функции. В особенности это касается версий для малого бизнеса — часто они представляют собой просто небрежно урезанные корпоративные версии, не соответствующие требованиям компаний другого масштаба.

Решения разных производителей

За. Можно выбрать именно то, что нужно, и именно тогда, когда нужно.

Против. Возможны проблемы при интеграции с другими решениями. Такой подход увеличивает сложность IT-среды и уменьшает наглядность.

Против. Работа с разными решениями отнимает больше времени.

РЕЗЮМЕ

- Для полной защиты бизнеса возможностей средств борьбы с вредоносным ПО уже недостаточно.
- В пакетных решениях часто недостает полноценной интеграции.
- Лучшие из комплексных решений работают хорошо, но дорого стоят и требуют постоянного выделения внутренних ресурсов.

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

8

«Затыкание дыр» — не самый эффективный способ обеспечить безопасность. Придерживаясь системного подхода, вы сможете гораздо надежнее защитить свои данные.

Линейка продуктов Kaspersky Security для бизнеса предлагает стандартные модули, из которых вы сможете выстроить эффективную систему защиты корпоративной сети, полностью соответствующую потребностям вашего бизнеса.

КОНТРОЛЬ И ЗАЩИТА В ЛЮБЫХ ОБСТОЯТЕЛЬСТВАХ

Представьте, что вся IT-среда компании — от сети до устройств, центра обработки данных и рабочих мест — перед вами как на ладони.

Полная наглядность — это то, что позволяет предотвращать угрозы, гибко и быстро реагировать на появление вредоносных программ и постоянно удовлетворять меняющиеся потребности бизнеса, будь то поддержка мобильных устройств или управление гостевым доступом в сеть.

Отсутствие «прикрученных» функций. Главное отличие — наш уникальный подход. Все используемые в продуктах «Лаборатории Касперского» ключевые технологии, функциональные компоненты и модули разрабатываются внутри компании на собственной технологической базе. Благодаря этому растет эффективность, снижается нагрузка на систему и повышается стабильность работы приложений. А управление всеми функциями защиты при этом осуществляется из единой консоли администрирования.

Единая, полностью интегрированная платформа «Лаборатории Касперского» позволяет использовать общность рутинных функций системного управления и основных потребностей в сфере обеспечения информационной безопасности.

Рис. 6

Kaspersky Security для бизнеса

Все управление из единой консоли Kaspersky Security Center

Рис. 7

ВЫВОДЫ

- Решение Kaspersky Security для бизнеса предлагает первую полноценную платформу обеспечения безопасности, созданную с нуля.
- С такой платформой системные администраторы в организациях любого размера смогут без труда контролировать и защищать свои системы через , используя при этом единую консоль управления.
- Защитите данные компании независимо от их местонахождения и без дополнительных затрат.
- Интуитивно понятный интерфейс и технология, простая в использовании, развертывании и управлении.
- Уменьшите риски для бизнеса и обеспечьте максимальную эффективность работы.
- Масштабируемое модульное решение, способное расти вместе с бизнесом и гибко реагировать на изменения.

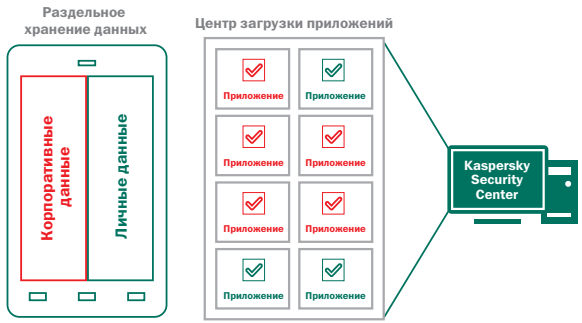
Kaspersky Security для бизнеса. Время серьезных решений.

Рис. 8. Защита от вредоносного ПО

Отправной точкой платформы является признанная во всем мире технология «Лаборатории Касперского» для защиты от вредоносного ПО. Эта технология состоит из нескольких сканирующих модулей, защиты с использованием «облака» и мощного сетевого экрана. Для централизованного управления служит Kaspersky Security Center. При добавлении новых функций доступ к новым средствам управления будет осуществляться из той же консоли.

Рис. 9. Управление мобильными устройствами

Централизованный контроль, управление и защита мобильных устройств и съемных носителей, принадлежащих компании или сотрудникам. Поддержите инициативу сотрудников по использованию на работе личных устройств, применяя контейнеры, дистанционное удаление данных, шифрование и другие функции защиты от кражи ценной информации.



- Раздельное хранение корпоративных данных
- Шифрование
- Выборочное удаление

Рис. 10. Шифрование

Централизованное управление сценариями полного шифрования диска и шифрования отдельных файлов и папок. Управляйте автоматическим принудительным применением политик, соответствующих вашим уникальным потребностям, из единой консоли.

Рис. 11. Средства системного администрирования

Автоматизируйте и приоритизируйте управление установкой исправлений, мониторинг уязвимостей, создание образов, составление отчетов и другие рутинные задачи администрирования. Соедините потребности рутинного администрирования с требованиями обеспечения информационной безопасности, чтобы улучшить защиту, уменьшить нагрузку на систему и выделить время для других задач.

РЕШЕНИЕ «ЛАБОРАТОРИИ КАСПЕРСКОГО»: ПРЕИМУЩЕСТВА ДЛЯ БИЗНЕСА

10

Какой бы пугающей ни казалась общая ситуация с угрозами и рисками, подход к решению этих проблем ясен. Очевидна и выгода, которую он может принести организации.

Высокий уровень обнаружения означает снижение риска для бизнеса

Исключительно высокий уровень обнаружения угроз, характерный для решений «Лаборатории Касперского» позволяет сократить риск потери корпоративных данных. Инцидентов с вредоносными программами станет меньше, а данные будут надежнее защищены как от внутренних, так и от внешних рисков.

Скажите «да» мобильности сотрудников

Дорогу новым технологиям и способам работы! Благодаря функциям управления мобильными устройствами, реализованными в продуктах «Лаборатории Касперского», вы сможете поддержать инициативу по использованию сотрудниками личных устройств и мобильной связи в рабочих целях, не подвергая свой бизнес дополнительному риску.

Повышенная производительность

Интегрированная система безопасности уменьшает нагрузку на ресурсы: для постоянного мониторинга, настройки, поддержки и составления отчетов теперь требуется меньше персонала. Анализировать отчеты и другие сведения в рамках единого интегрированного решения намного проще, чем пытаться разобраться в информации из нескольких, не слишком совместимых между собой, систем.

Лучшая наглядность означает лучшее управление

Единая консоль управления позволяет получить полное представление о виртуальных, физических и мобильных рабочих местах. Как только в сети появляется новое устройство, вы получаете соответствующее уведомление и система автоматически применяет ваши политики.

РЕЗЮМЕ

- Высокий уровень обнаружения означает уменьшение риска для бизнеса.
- Обеспечение безопасности деловой информации.
- Скажите «да» мобильности сотрудников.
- Повышенная производительность и лучшее понимание ситуации.
- Улучшенная наглядность означает улучшенное управление.

Рекомендации «Лаборатории Касперского» для составления надежного экономического обоснования инвестиций в IT-безопасность.

1

Опишите риски, но не фокусируйтесь на страхе, неуверенности и сомнениях

Статистика роста рисков в области IT-безопасности очень убедительна: она демонстрирует тенденцию к увеличению как количества угроз, так и их сложности (возрастает скорость распространения, увеличивается число целевых атак, усложняется вредоносное ПО). Однако одного этого мало, чтобы экономически обосновать ваше предложение. К тому же традиция играть на страхе при продаже своих решений слишком распространена в IT-индустрии. Циничные финансовые директора и руководители не раз слышали «все эти страшные истории» и обычно считают их просто маркетинговым ходом.

2

Позиционируйте систему обеспечения IT-безопасности как источник возможностей, а не ограничений

Значительно эффективнее фокусироваться на том, как система IT-безопасности поддерживает бизнес. Правильная организация и контроль безопасности позволяют бизнесу без риска внедрять новые технологии и методы работы.

3

Мобильность и использование личных устройств на работе имеют критическое значение для бизнеса — покажите, что система IT-безопасности должна быть составляющей этих практик

Из предыдущего пункта логически вытекает, что мобильность и использование сотрудниками личных устройств на работе — важные области с точки зрения повышения производительности бизнеса. И именно в этих областях IT-безопасность имеет очень большое значение. Ведь у сотрудников (среди которых много руководителей) при себе окажутся конфиденциальные или ценные данные компании, и обеспечить безопасность этих данных значительно важнее, чем защитить само устройство. Таким образом, шифрование данных и мобильное управление устройствами становятся обязательными инструментами мобильного бизнеса.

4

Преимущества единых платформ — эффективность и производительность, поэтому проанализируйте отдачу от инвестиций

Унифицированные платформы позволяют централизованно контролировать и защищать рабочие места. Это значит, что вы сможете тратить меньше времени на мониторинг и управление IT-безопасностью, а изменения, обновления и исправления можно будет применять непосредственно, а не через множество различных систем. Такую экономию времени нельзя недооценивать, и самый простой анализ позволит вам получить красноречивые цифры, которые можно будет включить в экономическое обоснование. Высокая совокупная цена нескольких систем также имеет значение, но стоимость рабочего времени — более существенный фактор, и руководители, ориентированные на производительность, отнесутся к нему со вниманием.

О «ЛАБОРАТОРИИ КАСПЕРСКОГО»

«Лаборатория Касперского» входит в число крупнейших мировых производителей решений для обеспечения информационной безопасности. Компания предоставляет организациям решения для обеспечения максимального уровня IT-безопасности, сочетающие мощную защиту от вредоносного программного обеспечения, гибкие инструменты управления, технологии шифрования и средства системного администрирования.

Подробнее: www.kaspersky.ru

KASPERSKY lab