

IT-БЕЗОПАСНОСТЬ ИЛИ IT-УПРАВЛЕНИЕ ДЛЯ МАЛЫХ И СРЕДНИХ КОМПАНИЙ?

МОЖНО ЛИ ИМЕТЬ
ОДНО БЕЗ ДРУГОГО?



Угрозы теперь направлены на экономическую выгоду, а не на хаос.

Решения безопасности постоянно развиваются, чтобы идти в ногу с развитием вредоносных программ. Т.к. большинство отраслей находится в тисках технологических преобразований, подпитываемых облаками, мобильностью и в некотором роде Большими данными, эволюция IT-безопасности также реагирует на глубокие перемены.

Индустрия вредоносного ПО уже долгое время обусловлена финансовыми выгодами и уже давно перестала "крутиться" вокруг личного эго программистов, хакеров и пр., как было раньше с вирусами I Love You* и Anna Kournikova, когда угроза привлекала внимание общественности и СМИ.

Как в любой другой отрасли: только появляется возможность заработать, используется все возможности для наживы.

Теперь преследуются финансовые цели: чем дольше угроза незаметна в системе, тем больше выгоды может извлечь владелец этого вредоносного ПО.



Вирус I love you поразил примерно 45 млн. ПК, ущерб составил примерно \$5,5-8,7 млрд. долларов США, расходы на удаление червя составили почти 15 млрд. долларов США.

Однако он не извлекал финансовую выгоду для разработчиков (Wikipedia)



Инвестиции во вредоносное ПО достигли исторических максимумов

Приток инвестиций в разработку вредоносных программ побил все рекорды по созданию угроз: в 2015 году было создано порядка 84 млн угроз (27% от всех угроз за всю историю), в среднем - порядка 230 000 новых угроз ЕЖЕДНЕВНО.

Во главе списка угроз мы все еще можем найти трояны - тип вредоносного ПО, разработанный для использования уязвимостей системы и приложений, которые сами по себе представляют еще одну сторону всей проблемы защиты.



PANDALABS
ЗАРЕГИСТРИРОВАЛА СВЫШЕ

250
МИЛЛИОНОВ

ОБРАЗЦОВ ВРЕДОНОСНЫХ ПРОГРАММ



9 583
КАЖДЫЙ ЧАС



230 000
ВДЕНЬ



84
МИЛЛИОНА

29,48%	США
32,15%	Испания
33,34%	Бразилия
29,03%	Канада
21,34%	Великобритания
20,32%	Швеция
22,78%	Германия
36,01%	Россия
57,24%	Китай
25,34%	Япония

Сегодняшние мобильные и гетерогенные среды создают новые проблемы для управления дополнительными бреши в защите

Т.к. растут расходы на аппаратное и программное обеспечение и зависимости от них (Отчет «State of SMB IT» от Spiceworks), IT-системы становятся более разнородными, распределенными и сложными в управлении. Просто с т.з. объема, IT-специалисты сегодня сталкиваются с проблемами управления разными офисами, операционными системами и многочисленными устройствами у каждого пользователя. Каждое дополнительное устройство добавляет компании эффективность, но также создает дополнительные уязвимости.

Если говорить про мобильные устройства в случае с малыми и средними предприятиями (SMB), то можно увидеть, как эта проблема еще больше усугубляется, что было упомянуто аналитиками Gartner в своем недавнем отчете*. SMB имеют те же проблемы, что и крупные компании, когда пытаются обеспечить их контроль и безопасность.

Все эти сложности напрягают ИТ-отделы до предела и создают дополнительные слабые места в безопасности компании.

Например, одна из проблем в защите этого нового технологического окружения - это ложное чувство безопасности в надежде на то, что некоторые устройства неуязвимы (устройства с MAC или Linux).

"Наибольшая уязвимость Macintosh - это вера среди ее преданных пользователей, что операционная система Apple превосходна, а потому она не уязвима перед вредоносными программами"^{***}. Это заблуждение оставляет "открытую дверь" для угроз (включая угрозы под Windows), которые могут проникать в такие системы беспрепятственно и использовать преимущества таких слабых мест.



*Gartner_March 2014

The Six Pain Points of Managing Mobile Devices for Small or Midsize Businesses.

** Белая книга: Следует ли мне беспокоиться о вирусах на моем MAC?

• По данным AMI, расходы SMB в США и Канаде, связанные с мобильностью, достигнут 71,5 млрд \$ к 2018 г. Например, только среднегодовой темп роста затрат в США и Канаде на планшеты составит 21%.

<http://www.ami-partners.com>

• Gartner: BYOD к 2017 г.
<http://www.gartner.com/newsroom/id/2466615>

• По прогнозу Gartner к 2017 г. половина работодателей будет требовать от сотрудников использовать свои собственные устройства в рабочих целях

Первый шаг в верном направлении: облако, от первых внедрений до стандарта для всей отрасли.

Когда количество угроз бьет все рекорды, производители решений безопасности уже не могут полагаться только на локальные решения, основанные на сигнатурах, для защиты IT-систем своих клиентов. В дополнении к пониженным возможностям обнаружения, т.к. растет число угроз, такие решения тяжелее для сетей.

Производители сейчас смотрят в сторону облаков и огромной вычислительной мощности Больших данных, чтобы реагировать на постоянный огромный рост, перенося рабочие процессы из сети / устройства в облако. Это позволило некоторым производителям решений безопасности получить преимущества при обнаружении угроз, а также позволить компаниям сфокусироваться на своем основном бизнесе, а не на управлении безопасностью. Большой шаг в верном направлении, но, как мы уже говорили, решает проблему частично.

Системные и программные уязвимости сейчас являются причиной большинства заражений до такой степени, что опытные ИТ-руководители знают, что ориентация даже на лучшие антивирусы и файерволы (даже облачные) теперь не всегда помогает для решения постоянно растущей проблемы.

Свыше 90% всех заражений вызваны не закрытыми уязвимостями, особенно в сторонних приложениях (Java, Adobe, Flash и т.д.)



PandaLabs 2015

Большинство локальных решений зависит от обновлений сигнатурных файлов (несколько раз в день или реже), что явно недостаточно при появлении свыше 230 000 угроз в день по данным отчета PandaLabs за 2015.

Наличие облачного решения означает, что вся защита всегда обновлена, при этом не требуется дополнительное аппаратное или программное обеспечение в сети.



Сочетание безопасности и управления.

Т.к. уязвимости в системах и приложениях становятся все более критическими, то происходит вполне логичное сближение функций безопасности устройства и управление им. Безопасность выходит за рамки традиционного подхода "антивирус и фаервол" и охватывает более широкую сферу применения, начиная от видимости устройств и заканчивая внедренными политиками. Такой новый подход следует рассматривать более совершенным для применения ко всем ИТ-системам без исключения.

Еще совсем недавно (эра ПК), когда локальные сети состояли в основном из компьютеров и серверов с Windows за редким исключением, управление большинством аспектов систем и обновлений ПО хоть и было трудоемким, но вполне выполнимым. Теперь же проблема стала более актуальной: IT-менеджеры для снижения общей угрозы безопасности ДОЛЖНЫ быть способны управлять каждым устройством вне зависимости от его местоположения. Они должны гарантировать постоянную видимость устройств, а также следить за тем, что они обновлены, патчи установлены и оптимизированы. И если что-то пойдет не так, то должны быть механизмы, позволяющие реагировать быстро и эффективно.

К сожалению, в современных компаниях даже наличие постоянной видимости устройств в распределенных и гетерогенных окружениях далека от нормы.



По оценкам Microsoft всего 40% предприятий имеют какие-либо заслуживающие доверия средства управления устройствами.

Меньше фрагментарности, проще управление.

Фрагментарность

Фрагментированные среды с огромным числом различных типов устройств части способствуют внедрению отдельных решений для контроля обновления ПО, безопасности, удаленной поддержки, MDM и т.д. Чтобы можно было решить проблему и значительно повысить уровень эффективности работы ИТ-отдела требуется централизованное решение. Все устройства, все ИТ-задачи - все должно быть через единую централизованную консоль, доступную требуемым ИТ-специалистам в любое время из любого места с любого устройства.

Сложность управления

Данная проблема весьма актуальна в тех случаях, когда один пользователь имеет несколько устройств, компания имеет несколько удаленных офисов, практикуется концепция BYOD. Однако решение проблемы с помощью фрагментированных решений только усугубляет ее, т.к. повышается сложность управления с внедрением каждого дополнительного решения.

Выбранное Вами решение должно сразу помогать Вам, быть простым во внедрении, а для управления им не должно требоваться дополнительных знаний. Такое решение должно упрощать сложность управления сегодняшними ИТ-системами.

Вывод

Количество угроз, создающихся для извлечения выгоды, стремительно растет. SMB вынуждены управлять более разнообразными, распределенными и сложными ИТ-системами, которые только увеличивают проблему безопасности.

Это создает дополнительные сложности, а ресурсов при этом зачастую не хватает.

Облако, мобильные технологии и Большие данные являются не только частью этой новой ИТ-реальности, но и неотъемлемой частью защиты и управления ею. Управление устройствами сейчас сближается с безопасностью, чтобы компании могли решать проблемы безопасности в более широком аспекте и более эффективно. Такое сближение для потребностей SMB должно быть централизованным и НЕ сложным.



Вопрос НЕ в том, следует ли управлять каждым устройством и защищать его, а в том - как ЛУЧШЕ это сделать?

Мы обращаем здесь Ваше внимание на фрагментарность решений и сложность управления.





Panda Fusion позволяет упростить и централизовать облачную безопасность, управление и поддержку. Panda Security предлагает полноценный подход в управлении системами для каждого устройства. Вне зависимости от типа устройства (ПК с Windows XP, сервер с Linux, компьютер MAC или планшет / смартфон) и его местонахождения (в локальной сети или за ее пределами) Вы можете управлять, защищать и обслуживать его из единой веб-консоли.

Как Gartner отметил в своем "магическом квадранте" (январь, 2014), «Panda - это [также] первый производитель решений для защиты конечных точек, который полностью охватил облачную поставку сервисов безопасности». Классифицировав в качестве "визионера", Gartner отметил у Panda возможности защиты и способность "ловить современные угрозы" благодаря поведенческому обнаружению и облачной базе знаний Коллективный разум.

В том же отчете Gartner упоминает о сильных сторонах "недавно добавленного решения для удаленного управления системами конечных точек, которое включает функции аудита, конфигурации, управления патчами, внедрения ПО и удаленного контроля".

Централизованный аудит означает, что IT-администраторы имеют постоянную видимость всех своих IT-систем из единой консоли, включая мобильные

устройства и смартфоны. Функции управления патчами и внедрения ПО обеспечивают обновленность и оптимизацию систем, в свою очередь, снижая угрозу атаки через уязвимости.

Незаметная удаленная поддержка дополняет предложение, позволяя IT-специалистам выполнять обширную диагностику проблем и внедрять требуемые решения в фоновом режиме, в то время как пользователь продолжает работать на своем устройстве.

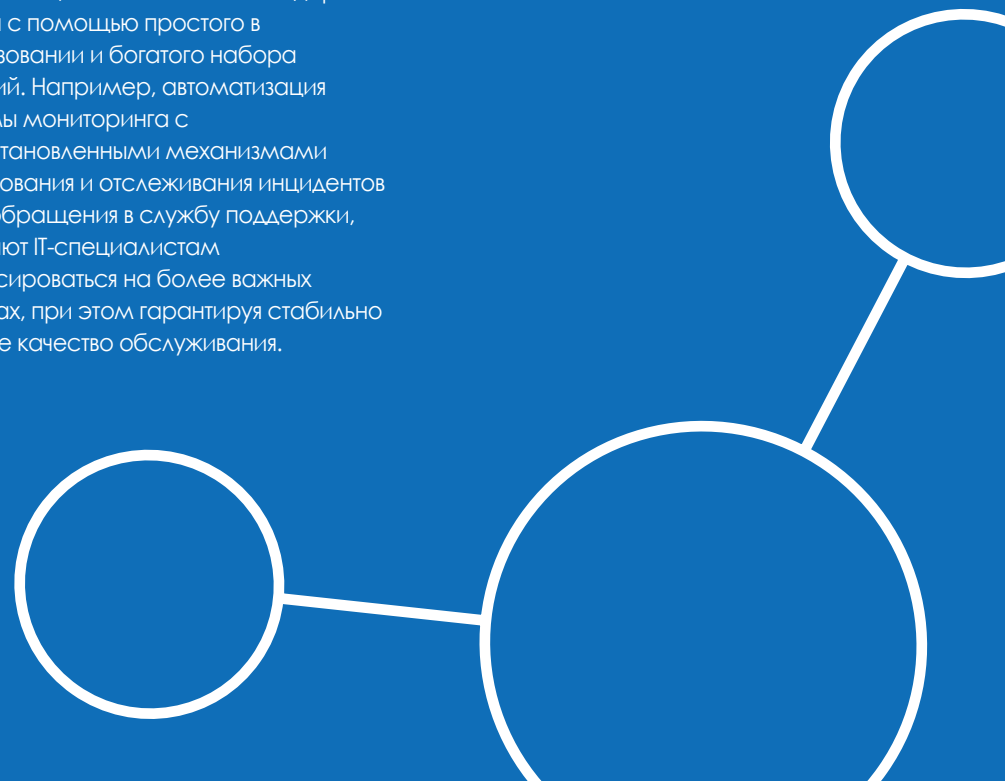
В дополнение к оптимизации и защите всех Ваших устройств, Panda Fusion также позволяет IT-специалистам повысить эффективность работы за счет автоматизации большинства стандартных IT-задач с помощью простого в использовании и богатого набора функций. Например, автоматизация системы мониторинга с предустановленными механизмами реагирования и отслеживания инцидентов через обращения в службу поддержки, позволяют IT-специалистам сфокусироваться на более важных проектах, при этом гарантируя стабильно высокое качество обслуживания.



Узнайте подробнее о Panda Solution

Триал-версия на 30 дней

[Подробнее](#)



Мы делаем все простым

Защитите Ваши устройства, где бы они не находились. Эффективно управляйте ими на всех платформах. Обслуживайте всех пользователей, управляйте инцидентами и решайте проблемы легко и просто.

Объединяем все в единую централизованную консоль.

Единая консоль для решения всех вопросов управления и безопасности.

Доступная из любого месте без VPN.

Не требуется дополнительная IT-инфраструктура, обслуживание систем или инвестиции в инфраструктуру.

