Когда среднестатистическому пользователю требуется новая защита для своего компьютера, он просит не “пакет интернет—безопасности”, а “антивирусный продукт”. Это вызывает у работников индустрии безопасности такое расстройство желудка, что в мире не хватит средств, чтобы облегчить все страдания. Но это никогда не изменится. Когда обычные потребители задумываются о защите своих компьютеров, они могут думать о множестве разных вещей, в зависимости от степени их технической подготовленности. Например:

• Защита от вредоносного программного обеспечения (включая шпионское и рекламное ПО), независимо от того, скачали ли они его или подверглись атаке.

• Фильтрация спама (хотя пользователи также ожидают, что это сделает их почтовый клиент).

• Защита от фишинга (они также могут ожидать этого от своих браузеров).

• Защита личных данных — они не имеют в виду какую-либо конкретную технологию, они просто считают, что их продукт для обеспечения безопасности должен решать эту проблему.

• Родительский контроль, который поможет удержать их детей от просмотра сайтов с неприемлемым контентом.

• Рейтинги веб-сайтов, показывающие, какие сайты могут нанести вред компьютерам пользователей при просмотре.

• Персональные брандмауэры, которые блокируют исходящий трафик.

• Предотвращение вторжений на хост, которая отслеживает поведение программ во время их запуска и, как мы надеемся, блокирует вредоносные программы в самый последний момент, когда AV выходит из строя. Этот подход, основанный на технологиях, является одним из способов взглянуть на вещи, но среднестатистическому потребителю нет дела до технологий. На самом деле, большинство из этих технологий являются большой проблемой для обычного человека (и не без оснований). Нет, потребителей волнуют их проблемы, а не блестящие технологические игрушки (приношу извинения тем из нас, кто по праву гордится своими крутыми технологиями). Какие проблемы видят потребители?

1. Люди крадут их личную информацию. Люди, несомненно, заботятся о своих финансах, своей личности и так далее.

2. Плохие люди уничтожают их вещи. Возможно, они боятся потерять свои личные файлы или беспокоятся о том, что плохие вещи могут привести к непригодности их компьютеров (раньше это было гораздо более серьезной проблемой, чем сейчас, когда плохие вещи так стараются не замечать). Люди обычно рассматривают решения для резервного копирования как решение этой проблемы (хотя они надеются, что их AV-сервер в первую очередь не позволит им в этом нуждаться). Это разумно, тем более что резервное копирование также решает другую проблему, связанную с отказом жесткого диска (разрушительную, но не вредоносную).

3. Спам, спам и еще раз спам. Мне кажется, что большинство потребителей будут принимать все, что они получают здесь бесплатно, и, вероятно, готовы мириться с любыми средствами защиты от спама, которые входят в их почтовый фильтр. Люди предпочли бы покупать как можно меньше товаров. В идеале им не нужно было бы ничего покупать, но некоторые люди этого не делают (например, когда Apple убеждает их, что в этом нет необходимости).

При взгляде на мир, ориентированном на конкретные проблемы, люди будут навешивать ярлыки на решения проблем, вот почему маркетинг называет их решениями, а не

технологиями. Что касается проблемы № 1 (и, в некоторой степени, № 2), то люди отождествляют себя с AV. Это связано с тем, что массы были осведомлены о рисках, связанных с подключением к Интернету, более десяти лет назад, когда эти риски назывались вирусами. Сейчас у нас есть десятки запутанных терминов для обозначения существующих рисков, включая:

• Вирусы

• Черви

• Трояны

• Шпионское ПО

• Рекламное ПО

• Руткиты

• Эксплойты

• Уязвимости

• Вредоносное ПО

• Боты/ботнеты-сети

В течение примерно двух минут индустрия безопасности полагала, что защита от шпионских программ будет иметь большое значение, главным образом потому, что она увидела некоторые технические отличия в новых вредоносных программах и выпустила отдельные продукты, которые продавались некоторое время. И некоторые люди в корпоративном мире понимали техническую разницу и хотели быть защищенными. Некоторые потребители подумали: “лучше перестраховаться, чем потом сожалеть”, но большинство людей просто хотят быть защищенными от своих проблем, не заботясь о технологиях. Они бы разозлились на своих поставщиков, если бы возникла какая-то угроза, от которой поставщик мог бы их защитить, но не защитил.

И кто бы захотел купить по одному из следующих средств: AV, anti-spyware, anti-trojan, anti-adware, anti-rootkit, anti-exploit и anti-bot? Даже если все они будут продаваться по той же конечной цене, что и универсальный продукт, никто на самом деле не захочет иметь дело с такой сложностью.

Все, чего хотят люди, - это довериться одному поставщику, который защитит их, и купить, самое большее, один продукт, который решит то, что они считают проблемой. Все эти технические проблемы — кого это волнует? Есть только одна реальная проблема; позвольте одному продукту решить ее. В любом случае, если есть компании, пытающиеся вывести на рынок несколько продуктов, в то время как какая-то другая компания с аналогичной репутацией пытается продать один продукт, чтобы сделать то же самое, что происходит в голове клиента? Вот что я бы подумал: очевидно, что две компании, которым я доверяю, скорее всего, будут в равной степени на высоте положения.

Если кто-то продает мне несколько продуктов, это, вероятно, отнимает много денег, и, возможно, мне следует обратиться к другому специалисту. По сути, потребители ожидают, что при покупке “антивирусной” защиты они получат полную защиту от вредоносных программ.

Этот термин убивает людей в отрасли, особенно гиков, потому что в продуктах содержится гораздо больше, чем просто “антивирусная” защита, хотя из названия это звучит иначе. Но все в мире потребителей привыкли к тому, что “антивирус” - это то, что их защищает, не заботясь о техническом ответе на вопрос “Что такое вирус?” И, как вы знаете, клиент всегда прав.

Поэтому, на мой взгляд, наиболее правильным ответом на вопрос “Что такое вирус?” будет “Все вредоносное, что запускается на вашем компьютере”, потому что именно такое определение есть у 99% людей в мире. Маркетологам эта истина тоже не нравится. Все они пытаются позиционировать свои средства защиты как “средства обеспечения безопасности в Интернете”. Если присмотреться повнимательнее, то основная идея, лежащая в основе пакета Internet security suite, заключается в том, что “это защищает вас лучше, чем просто AV”. Обычно это происходит потому, что поставщик предоставляет все необходимые инструменты, которые могут не понадобиться пользователю, например, средства защиты от спама, средства защиты от детей и так далее. Защита должна быть примерно одинаковой. Не все потребители считают, что она одинакова. Потребители, как правило, делятся на два лагеря:

• Те, кто считает, что единственная “достаточно хорошая” защита - это самая дорогая версия.

• Те, кто считает, что базовая версия “достаточно хороша”, иначе это не было бы предложением, а все остальное - просто навороты.

Очень редко люди действительно вникают в детали, чтобы понять, что они покупают. Для них это все “антивирус”, а не интернет-безопасность. В результате, даже когда компании предлагают четыре разных комплекта по четырем разным ценам, почти каждый клиент выберет либо самый дешевый, либо самый дорогой.

Люди понимают, что вы имеете в виду, когда говорите “интернет-безопасность”, но они рассматривают это как более общий термин, который может применяться ко всей отрасли и к любому продукту, который в ней выпускается. Они понимают, что продуктов может быть больше. Возможно, они слышали о брандмауэрах. Они знают о борьбе со спамом. И так далее. Но когда придет время искать программное обеспечение, которое защитит их компьютеры от этого дерьма, они будут думать: “Какой антивирус мне купить?” Это категория, независимо от того, какая технология используется. Каждые несколько лет кто-нибудь будет заявлять, что “AV мертв” и что за их новой технологией будущее.

Неправильный. Ориентируйтесь на продукт, а не на технологию. Специалисты по безопасности считают, что “эта старая технология - отстой”, и считают “антивирус” старой технологией. Однако потребители думают об этом совсем не так. Они не разбираются в технологии, поэтому все это должно быть доступно. Просто, как и во многих других областях, технологии совершенствуются с течением времени. Если вы попытаетесь переименовать электромобиль под каким-нибудь совершенно новым названием, люди пожмут плечами и назовут его автомобилем, или же они будут сбиты с толку тем, зачем им нужна эта новинка, когда у них уже есть автомобиль.

Слушайте внимательно, все вы, маркетологи (и все вы, венчурные капиталисты), которые считают вашу технологию безопасности потрясающей: чтобы изменить название, вы должны аргументировать, почему эта технология решает проблему, которую не решала AV. Если это просто улучшит решение той же проблемы, вы никогда не заставите людей понять, почему ваш новый термин имеет к ним отношение, и, следовательно, он потерпит неудачу. Вам гораздо лучше позиционировать себя как “лучшего рекламиста”, а затем четко сказать, почему вы лучше. Например, когда мой последний стартап был поглощен McAfee, мы собирались выйти на рынок с предложением по защите прав потребителей. Мы назвали его AV, и это было лучше,

потому что:

• Наш платный AV-продукт поставляется с гарантией отсутствия вирусов — мы бесплатно очистим ваш компьютер, если вы все-таки будете заражены.

• Наш AV—продукт обеспечивает защиту от новых угроз - в среднем на 30 дней быстрее, чем любой другой.

• Наш AV- продукт работал быстро и не замедлял работу вашего компьютера, как это делают большинство других AV-решений.

• Наш AV- продукт был дешевле, чем у основных производителей.

Все это очень хорошо. Если вы подумаете об этом, то можете сделать вывод, что наша технология должна быть намного лучше, чем “традиционная” AV. Но что, если мы решим изобрести для этого новый термин, например, систему предотвращения вторжений в сообщество (термин, используемый другим небольшим поставщиком)?

Что происходит в головах потребителей? Во-первых, они бы спросили: “Что это за чертовщина и зачем мне это нужно?” Ответ таков: “Мы похожи на AV, но лучше".

Теперь компании, занимающей такое положение, придется потратить много времени на разъяснение людям, почему это не AV, заменяет ли это AV или нет (или у них должно быть и то, и другое). Это создаст путаницу, и люди не будут слишком стараться преодолеть эту путаницу, если она не получит широкого распространения. Они считают, что если им нужно купить ваш продукт, а они в нем не разбираются, они просто подождут, пока он зарекомендует себя. “Но подождите!” - может сказать специалист по маркетингу. “Наше решение лучше!”

Если вы сможете помочь людям разобраться в путанице, связанной с позиционированием компании в отношении AV, не заявляя, что решаете какие-либо новые проблемы (а только утверждая, что решаете старую проблему лучше), вероятно, все равно будет много скептицизма. “Действительно ли это может заменить AV? Держу пари, что это невозможно.

Либо это слишком новое решение, чтобы хорошо работать, либо оно не справляется с поставленной задачей; в противном случае, почему бы не всем им пользоваться? Даже если вы утверждаете, что у вас “AV следующего поколения”, вам все равно придется убеждать людей в преимуществах вашего решения. Но, по крайней мере, вы не начинаете с того, что вводите клиентов в заблуждение.

Короче говоря, индустрия безопасности должна сделать себе одолжение и перестать придираться к терминологии. Используйте термин “антивирус”. Кого волнует, насколько он точен с технической точки зрения? Клиент всегда прав.