Документ

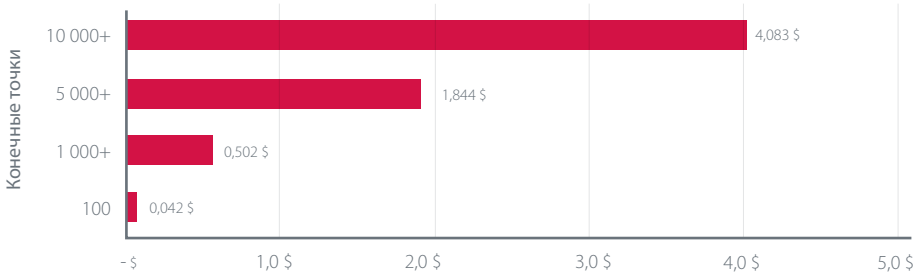
Решение McAfee Total Protection for Endpoint обеспечивает лучшие показатели совокупной стоимости владения по сравнению с Symantec Endpoint Protection

Содержание

Краткая сводка

В данном документе анализируется и сравнивается совокупная стоимость владения (ССВ) корпоративными продуктами McAfee для защиты конечных точек и аналогичными продуктами разработки Symantec. Symantec — это единственный производитель, помимо McAfee, предлагающий комплексный набор продуктов, необходимых для защиты конечных точек на предприятиях различного масштаба — от малого бизнеса до гигантских корпораций. Тем не менее, следует отметить, что подходы к управлению безопасностью конечных точек, выбранные McAfee и Symantec, отличаются фундаментально. В частности, McAfee в рамках своего решения McAfee® ePolicy Orchestrator® (McAfee ePO™) предоставляет общую точку управления, что позволяет пользователям управлять всеми компонентами безопасности конечной точки с единой консоли, работающей на основе веб-приложения. Таким образом минимизируется нагрузка на ИТ-персонал, а эффективность защиты, предоставляемой развернутыми продуктами McAfee, — напротив, максимизируется. В противоположность этому, подход Symantec требует от пользователя, чтобы тот развернул 12 консолей управления, практически не связанных между собой и не имеющих совместимости по интерфейсу пользователя. Приведенный ниже анализ свидетельствует о том, что продукты Symantec требуют больших трудозатрат со стороны ИТ-персонала и, в отсутствие общей точки интеграции, эффективность защиты, предоставляемой Symantec, значительно ниже той, которая обеспечивается McAfee. Различие заключается в основополагающем преимуществе, которое получает McAfee за счет ССВ, в которой учитываются программное обеспечение, оборудование и постоянные расходы на персонал.

Для организаций любого размера компания McAfee предлагает защиту конечных точек, требующую ССВ на 55 % ниже, чем у Symantec, что эквивалентно 155 долларам США на одну конечную точку в год.



Суммарная экономия за три года (в миллионах долларов США)

Введение

В данном документе приводится анализ ССВ, где внимание уделяется семи основным составляющим расходов, перечисленным ниже.

«Когда это возможно, уменьшайте число поставщиков безопасности для конечных точек, покупая наборы вместо отдельных продуктов».

— Питер Ферстброк (Peter Firstbrook)
Gartner Inc.
(2009 г., G00167430)

- Лицензирование требуемых компонентов безопасности конечной точки вместе со всем другим программным обеспечением, связанным с этими компонентами и развертываемым на сервере
- Лицензирование управляющего программного обеспечения или управляющих консолей с целью наиболее эффективного управления каждым компонентом при как можно более низком уровне затрат
- Оборудование, обеспечивающее работу развернутого компонента и управление им
- Требуемое количество управляющих консолей — ССВ возрастает прямо пропорционально количеству управляющих консолей, необходимых для управления всей инфраструктурой защиты конечной точки
- Группа из профессиональных ИТ-специалистов — она нужна для поддержки работы и управления развернутыми компонентами
- Выявление недостатков в функциональности и охвате угроз требует дополнительных затрат по двум причинам: в связи с тем, что недостающие функции все равно необходимо выполнять (возможно вручную), либо вследствие того, что недостаток функциональности приведет к повышению риска нарушения безопасности и последующего «ремонта»
- Оценка общей архитектуры, предложенной каждым из производителей, с точки зрения полного перечня предъявляемых требований по безопасности.

В данном документе мы применяем методологию, учитывающую градацию предприятий, что позволяет нам проанализировать четыре сценария развертывания.

- Предприятия малого бизнеса: 100 конечных точек
- Предприятия среднего бизнеса: 1 000 конечных точек
- Корпорация среднего размера: 5 000 конечных точек
- Крупная корпорация: 10 000 конечных точек

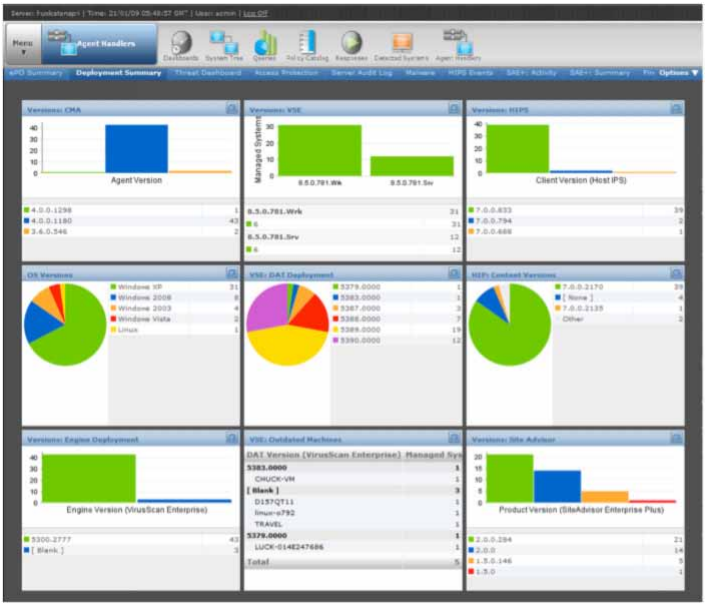
В качестве конечной точки рассматривается компьютер, работающий под управлением операционных систем Microsoft Windows (XP, Vista, Windows 7), Unix, Linux или Apple MacIntosh.

Уровни защиты

Первым шагом в анализе ССВ является определение необходимых уровней защиты, которые должны быть установлены для обеспечения надлежащей безопасности предприятия. Стандартный подход в этой отрасли, применяемый практически всеми предприятиями, начиная от малого бизнеса, состоит в том, что каждая конечная точка должна защищаться, по меньшей мере, антивирусной программой и программой для защиты от нежелательной почты для почтового клиента и персонального компьютера, а также антишпионской программой, межсетевым экраном и программой для безопасной работы в Интернете.

По мере роста масштабов предприятия растет и необходимость в применении дополнительных уровней защиты. Платформа ePO используется во всем мире для управления более чем 60 миллионами корпоративных конечных точек, при этом предприятия вносят дополнительные инвестиции в защиту по мере их роста.

Единая система управления в сравнении с использованием нескольких систем



Платформа McAfee ePO

McAfee ePolicy Orchestrator — это открытая платформа управления безопасностью, являющаяся точкой интеграции для сетевых продуктов McAfee, а также для продуктов, разработанных ее партнерами из McAfee Security Innovation Alliance[1]. Это система, управляющая более чем 60 миллионами конечных точек по всему миру, позволяет администраторам установить связь между конечными точками, данными и сетевой безопасностью посредством общей управляющей консоли, средств для проведения оценки угроз и соответствия нормативным требованиям, а также других инструментов для обеспечения безопасности. Благодаря средствам глобального обзора, которыми обладает консоль McAfee ePO, для групп ИТ-специалистов упрощается задача управления и обмена информацией в процессе обеспечения безопасности. Развертывание и администрирование таких продуктов вместе с подготовкой специалистов существенно упрощаются, а эксплуатационные затраты на управление безопасностью в значительной степени снижаются.

После восьми лет своего развития платформа McAfee ePO на сегодняшний день является лидером в области систем управления безопасностью. Платформа McAfee ePO может масштабироваться от предприятий малого бизнеса до гигантских корпораций. С ее помощью с единого сервера может управляться до 300 000 конечных точек. Она была развернута в организациях, в управлении которых находится более пяти миллионов конечных точек. Консоль McAfee ePO, работающая на основе веб-приложения, дает возможность осуществлять дистанционное управление из любого обозревателя. Кроме того, она позволяет использовать многоуровневые административные роли и очень гибкие в настройке панели управления. В каждой защищаемой конечной точке должен быть развернут единственный агент, который может запускаться и обновляться в любое время, в особенности тогда, когда наблюдается вспышка угроз.

1. В состав McAfee Security Innovation Alliance входит более 80 ведущих производителей в области безопасности. Список партнеров приведен на веб-странице www.mcafee.com/us/partners/security_innovation_alliance.

Symantec SEP 11

В противоположность приведенному выше подходу, для эффективного управления своей инфраструктурой обеспечения безопасности конечных точек Symantec требует увеличения числа управляющих консолей. Ниже приведены примеры.

- Даже предприятие малого бизнеса с конечными точками Apple потребует трех управляющих консолей: **(1)** SEP 11, **(2)** Symantec Administration Console for Macintosh и **(3)** Symantec Web Gateway
- Для предприятий среднего бизнеса количество необходимых управляющих консолей возрастает до шести: добавляются **(4)** консоль Brightmail и **(5)** Symantec Mail Security for Microsoft Exchange (или Domino) для управления серверной частью антивирусной программы и программы защиты от нежелательной почты, а также **(6)** консоль Vontu для управления инфраструктурой предотвращения утечки данных
- Для корпораций среднего размера количество консолей практически удваивается до 11, при этом добавляются **(7)** Symantec Critical System Protection для защиты серверного узла от вторжений и межсетевого экрана, **(8)** консоль Symantec Control Compliance Suite (SCCS) для управления уязвимостями, **(9)** консоль GuardianEdge для управления полнодисковым шифрованием, **(10)** консоль Altiris SecurityExpressions (ASE) для управления распределением агентов и аудитом политик для персональных компьютеров, а также консоль Symantec Brightmail Appliance **(11)** для антивирусной программы, программы защиты от нежелательной почты для шлюзов электронной почты и Интернет, а также для фильтрации URL-адресов/содержимого шлюзов электронной почты и Интернет
- Наконец, пользователи Symantec, пользующиеся более старыми версиями антивирусных программ для ПК, должны будут установить консоль SAV 9 или 10 для управления антивирусной программой более ранней версии, а также консоль SEP 11 — для управления другими, более новыми элементами защиты конечных точек, отсутствующими в старых версиях (потенциально — это двенадцатая консоль).

В итоге становится понятным, каковы возможные варианты выбора: интегрированный комплект McAfee для защиты конечных точек, более экономичный при управлении с единой консоли ePO, или продукты Symantec для обеспечения различных видов безопасности, большинство из которых имеют собственную управляющую консоль и связанную с ней базу данных.

Уровень защиты	McAfee	Symantec
Антивирусная программа для персонального компьютера • Windows • Apple • Linux	ePolicy Orchestrator представляет собой единую консоль управления и общую точку интеграции	SEP 11 • Включена в SEP 11 • Symantec Administration Console for Macintosh • Только с пользовательским интерфейсом в виде командной строки
Текущая версия – 1		Консоль Symantec Antivirus 10
Текущая версия – 2		Консоль Symantec Antivirus 9
Защита от шпионских программ для персонального компьютера		SEP 11
Система предотвращения вторжения на узел и межсетевой экран для персонального компьютера		SEP 11
Безопасность Интернета		Symantec Web Gateway
Защита сервера электронной почты от нежелательной почты и антивирусная программа		Консоль Brightmail + Symantec Mail Security for Microsoft Exchange или Domino
Управление устройствами		SEP 11
Утечка данных		Консоль Vontu
Система предотвращения вторжения на узел и межсетевой экран для сервера		Консоль Critical System Protection
Управление доступом к сети		SEP 11
Аудит политики для персонального компьютера		Консоль Altiris SecurityExpressions (ASE)
Полнодисковое шифрование		Консоль GuardianEdge
Антивирусная программа для шлюзов электронной почты и Интернет		Консоль устройства Консоль Symantec Brightmail Appliance
Фильтрация URL-адресов/содержимого шлюзов электронной почты и Интернет		Консоль устройства Консоль Symantec Brightmail Appliance
Распределение агентов		Консоль ASE
Управление уязвимостью		SCCS
Защита от нежелательной почты для шлюзов электронной почты и Интернет		Консоль Brightmail и Web GW
Исправление		Консоль ASE

Продукты Symantec для обеспечения различных видов безопасности и множество управляющих консолей каждый день требуют сотни раз вручную передавать управление, что связывает ресурсы и привносит повышение уровня рисков без соответствующей необходимости. При использовании защиты Symantec ИТ-подразделение менее эффективно управляет процессом обеспечения безопасности, ему часто недостает универсальной возможности получения информации обо всех системах и сетях, вне зависимости от того, где эти системы расположены.

Не удивительно, что влияние на ССВ дополнительных консолей, обязательных для установки в инфраструктуре Symantec, влекут затраты в различных сферах, и они могут быть значительными.

- Затраты на лицензирование программного обеспечения дополнительных консолей
- Дополнительное оборудование, необходимое для обеспечения работы консолей и поддержка дополнительных баз данных
- Дополнительное обучение для профессиональных ИТ-специалистов и подбор кадров для управления работами при значительном возрастании их сложности
- Снижение эффективности ИТ-специалистов в связи с тем, что консоли Symantec не полностью поддерживают веб-приложения, требуя от ИТ-специалистов для управления каждой консолью использовать ПК со специально установленными клиентами консоли. В кризисные моменты ИТ-администраторы не в состоянии реагировать, используя доступные ПК для диагностики и принятия необходимых мер в реальном времени.
- Администраторы вынуждены вручную устанавливать связь между событиями и отчетами, поступающими с разных консолей. Даже такие простейшие операции как «копирование-вставка» между консолями требуют немалых усилий, а при наличии нескольких консолей можно только представить насколько это становится сложным.
- Отсутствие возможности сгенерировать централизованные отчеты и оповещения об угрозах, собрав их по всей среде обеспечения безопасности предприятия

Наконец, неинтегрированная архитектура Symantec, в которой собраны продукты для обеспечения различных видов безопасности, облегчает задачу нарушения безопасности, поскольку злоумышленники будут атаковать области, где отсутствует взаимодействие между отдельными продуктами в связи с отсутствием общей точки их интеграции, кроме того, при наличии нескольких консолей легче пропустить угрозу. Общеизвестно, что экономические последствия от использованной злоумышленниками уязвимости могут быть глубокими. Затраты могут включать ущерб от простоя бизнеса, прямые штрафы, извещения о санкциях, затраты на PR и кампанию в средствах массовой информации, затраты на ИТ, управление, наем персонала, а также на оплату услуг других профессионалов и судебные тяжбы.

Анализ совокупной стоимости владения

Приведенные ниже финансовые результаты были рассчитаны с использованием информации, полученной на веб-сайте компании Symantec и из ее публикаций. Помимо этого мы использовали технологическую и бизнес-модель, разработанную компанией Forrester Research Inc. и предоставленную McAfee на исключительной основе. Компания Forrester считает этот анализ репрезентативным в плане преимуществ, которые могут быть получены компаниями, установившими ePO вместе с решениями McAfee для защиты конечных точек. В Приложении приведена более подробная информация о методе вычисления и методологии Forrester для расчета общего экономического эффекта.

Предприятия малого бизнеса (100 конечных точек): ССВ снижается на 35 % при использовании решений McAfee

Для любых предприятий малого бизнеса, имеющих в своем распоряжении до 250 конечных точек, McAfee предлагает Total Protection Service — решение на основе программного обеспечения как услуги (SaaS, software-as-a-service) в противоположность решениям, предоставляемым на месте. Его администрирование осуществляется полностью через Интернет и не требует на месте использования ни программного обеспечения, ни оборудования для управления. Управление пользователями — упрощенное и не требует привлечения ИТ-специалистов. Руководитель офиса может просто разослать всем пользователям URL-адрес, который они будут в дальнейшем использовать для установки решения. McAfee Total Protection Service имеет в своем составе централизованный межсетевой экран ПК, антишпионскую программу, интегрированную антивирусную программу для персональных компьютеров и файлового сервера, усовершенствованную защиту сервера электронной почты, а также защиту обозревателя в реальном времени.

У Symantec нет предложения, сравнимого с McAfee Total Protection Service. Взамен этого они предлагают услугу, называемую Symantec Managed Security Services, которая может использоваться для управления инфраструктурой безопасности пользователя. В отличие от услуги SaaS, основанной на веб-приложении, как например, Total Protection Service, Symantec Managed Security Services разворачивает в конечных точках пользователя SEP 11, после чего удаленно управляет развертыванием. В результате, Symantec Managed Security Services требует такого же оборудования и консолей на месте развертывания как и в случае применения решения уровня предприятия, предлагая лишь дополнительную услугу по управлению.

Предлагая услугу SaaS, McAfee обеспечивает меньшую ССВ по сравнению с решением Managed Security Services от Symantec. За три года McAfee снижает ССВ на 35 % за счет экономии почти 35 000 долларов США, что эквивалентно экономии более чем 115 долларов США на каждой конечной точке в год.

	Год 1	Затраты за три года
Symantec — удаленное управление SEP 11		
Лицензия на SEP 11 для конечной точки	4,000 $	8,500 $
Managed Security Services (и оплата за установку)	13,350 $	22,700 $
Аппаратное обеспечение	15,000 $	19,500 $
ИТ-персонал	15,850 $	48,500 $
Итого, затраты по Symantec	48,200 $	99,200 $
McAfee SaaS		
Лицензия на Total Protection Service для конечной точки (и услуга установки)	11,150 $	16,150 $
ИТ-персонал	15,850 $	48,500 $
Итого, затраты по McAfee	27,000 $	$64,650 $

Предприятия среднего бизнеса (1 000 конечных точек): ССВ снижается на 53 % при использовании решений McAfee

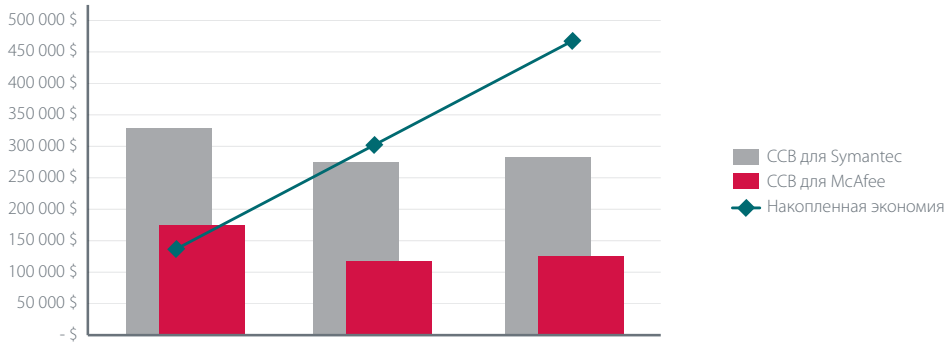
Большинство предприятий среднего бизнеса предпочитают переместить защиту конечных точек внутрь собственного периметра и осуществлять ее на собственном оборудовании. Для управления данными решениями они также пользуются услугами собственных ИТ-специалистов.

Для поддержки предприятий среднего бизнеса Symantec требует четыре управляющие консоли: SEP 11 и Symantec Administration Console for Macintosh вместе с консолью Symantec Mail Security for Microsoft Exchange/ Domino для управления антивирусной программой и защитой от нежелательной почты на серверной стороне, а также консоль Vontu для управления инфраструктурой предотвращения утечки данных.

McAfee осуществляет поддержку предприятий среднего бизнеса с помощью программного обеспечения Total Protection for Endpoint и ePO. Администраторы ePO пользуются единственной консолью, а эффективность интегрированной платформы управления становится очевидной, когда дело доходит до сдерживания и противодействия вирусным эпидемиям, в противоположность подходу, заключающемуся в слежении за деятельностью и управлении конечными точками с нескольких консолей. Подход McAfee заслужил у пользователей высокую оценку, поскольку простои в период вирусной эпидемии могут оказаться очень дорогостоящими для бизнеса. Ключевым преимуществом интегрированного управления является способность полностью просматривать состояние безопасности организации с единой интегрированной точки обзора. Ценность такого инструмента очевидна — предприятия улучшают управление своими инструментами и политиками обеспечения безопасности и имеют возможность реагировать на возникающие вопросы, прежде чем они станут проблемой. Проактивная безопасность, останавливающая проблемы на подходе, всегда эффективнее, чем подход, предполагающий реагирование на возникшую эпидемию.

Сравнивая административные затраты по обоим решениям с использованием программы расчета окупаемости инвестиций от Forrester, получаем, что за три года решение McAfee обеспечивает на 53 % более низкую ССВ по сравнению с Symantec, и это дает экономию в размере 465 000 долларов США, эквивалентную ежегодной экономии 155 долларов США на каждой конечной точке.

Сравнение ССВ для числа конечных точек более 1 000



	Год 1	Год 2	Год 3
ССВ для Symantec	332 500 $	275 000 $	277 500 $
ССВ для McAfee	182 500 $	117 500 $	120 000 $
Накопленная экономия	150 000 $	307 500 $	465 000 $
Чистая приведенная стоимость экономии (i = 14 %)	131 579 $	252 770 $	369 078 $

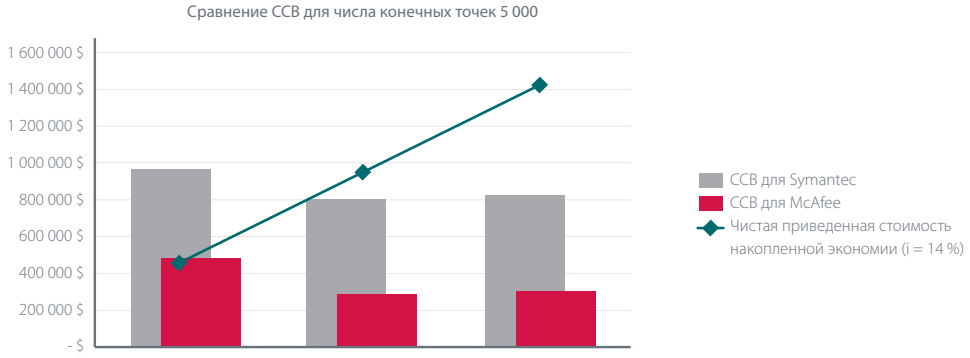
Корпорации среднего размера (5 000 конечных точек): ССВ снижается на 55 % при использовании решений McAfee

Корпорации среднего размера обычно предпочитают развертывать решения по защите конечных точек внутри собственного периметра, на собственном оборудовании, под управлением собственных ИТ-специалистов.

Для поддержки корпораций среднего размера Symantec требует восемь управляющих консолей: SEP 11, Symantec Administration Console for Macintosh, Symantec Mail Security for Microsoft Exchange/Domino, Vontu, SCCS, GuardianEdge, ASE и Symantec Brightmail Appliance. Многие корпорации среднего размера также сталкиваются с потребностью продолжить использование консоли SAV 10/9, поскольку им необходимо сохранить старые версии программ Symantec для защиты конечных точек.

McAfee осуществляет поддержку корпораций среднего размера с помощью Total Protection for Endpoint и консоли ePO, установленной на единственном физическом сервере.

Используя программу расчета окупаемости инвестиций от Forrester, получаем, что при выборе McAfee Total Protection for Endpoint за три года обеспечивается на 55 % более низкая ССВ и экономия в размере более 1 400 000 долларов США по сравнению с использованием решений от Symantec, что эквивалентно ежегодной экономии в размере 95 долларов США на каждой конечной точке.



	Год 1	Год 2	Год 3
ССВ для Symantec	960 000 $	800 000 $	807 500 $
ССВ для McAfee	497 500 $	322 500 $	325 000 $
Накопленная экономия	462 500 $	940 000 $	1 422 500 $
Чистая приведенная стоимость экономии (i = 14 %)	405 702 $	773 122 $	1 098 796 $

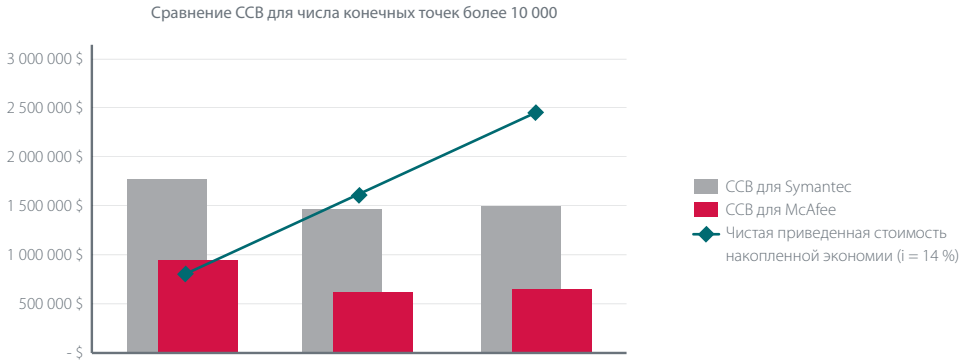
Крупные корпорации (10 000 конечных точек): ССВ снижается на 53 % при использовании решений McAfee

Крупные корпорации также развертывают на местах решения по защите конечных точек и также используют своих собственных ИТ-специалистов для управления этими решениями.

Для поддержки крупных корпораций Symantec требует восемь управляющих консолей: для SEP 11, Symantec Administration Console for Macintosh, Symantec Mail Security for Microsoft Exchange/Domino, Vontu, SCCS, GuardianEdge, ASE и Symantec Brightmail Appliance. Многие крупные корпорации также сталкиваются с потребностью продолжить использование консоли SAV 10/9, поскольку многие из ранее установленных решений требуют старых версий программ Symantec для защиты конечных точек.

McAfee же осуществляет поддержку крупных корпораций с помощью Total Protection for Endpoint и консоли ePO, установленной на единственном физическом сервере.

Используя программу расчета окупаемости инвестиций от Forrester, получаем, что при выборе McAfee Total Protection for Endpoint за три года обеспечивается на 53 % более низкая ССВ и экономия в размере почти 2 500 000 долларов США по сравнению с использованием решений от Symantec, что эквивалентно ежегодной экономии в размере 82 доллара США на каждой конечной точке.



	Год 1	Год 2	Год 3
ССВ для Symantec	1 762 500 $	1 460 000 $	1 475 000 $
ССВ для McAfee	970 000 $	625 000 $	630 000 $
Накопленная экономия	792 500 $	1 627 500 $	2 472 500 $
Чистая приведенная стоимость экономии (i = 14 %)	695 175 $	1 337 681 $	1 908 032 $

Другие элементы полного анализа совокупной стоимости владения

Имеется ряд других важных вопросов, которые может задать любой ИТ-специалист, выбирающий между McAfee и Symantec. Они затрагивают те параметры, которые могут повлиять на окончательное значение ССВ, но обычно не рассматриваются в процессе анализа. В частности, речь идет о следующем.

- Имеются ли пробелы в полноте охвата или в функциональных возможностях линейки продукции, влекущие за собой дополнительную ССВ?
- Располагает ли производитель архитектурой безопасности, которая будет действительно эффективной во всем спектре требований к безопасности вашей организации, а не только в отношении конечных точек, например, будет ли обеспечен переход к этой архитектуре в случае, если со временем вы решите обновить инфраструктуру безопасности?
- Внедрен ли производителем стандарт открытой платформы управления, обеспечивающий техническую интеграцию с другими ведущими производителями ИТ, как например, предоставление общей точки интеграции и управления для каждого элемента ИТ-инфраструктуры, в том числе и для конечных точек?

Пробелы в полноте охвата и функциональных возможностях

У программного продукта Symantec имеются значительные пробелы в полноте охвата и функциональных возможностях, требующие от ИТ-специалистов выполнения значительного объема дополнительной ручной работы; такие пробелы ведут также к повышению риска нарушения безопасности и последующего «ремонта».

Это можно проиллюстрировать одним примером. Продукт Symantec для предотвращения вторжений на узел (IPS) для персональных компьютеров характеризуется отсутствием защиты от общего переполнения буфера — это функция, которой он обязан обладать, чтобы иметь возможность перехватывать вирусы нулевого дня. В продукте Symantec используются сигнатуры межсетевого экрана для обеспечения защиты от переполнения буфера, что позволяет злоумышленникам использовать различные старые и хорошо известные методы для обхода такой защиты. Например, было показано, что простое изменение в размере пакета вредоносной программы делает такую защиту неэффективной. В результате, пользователи Symantec подвержены воздействию вредоносных программ нулевого дня, которые могут вызвать нарушение безопасности, чего не скажешь о пользователях McAfee. Нарушения безопасности влекут за собой тяжелые финансовые последствия для ИТ, связанные с затратами на восстановление.

Система предотвращения вторжений на узел для персональных компьютеров	McAfee	Symantec
Бихевиористическая защита	X	X
Защита оперативной памяти	X	
Общее переполнение буфера	X	
Защита приложения	X	X
Режим обучения	X	X
Атаки в Интернете	X	X
Система предотвращения вторжений, интегрированная с антивирусом	X	X

В дополнение к сказанному можно отметить: несмотря на то, что компания Symantec предоставляет антивирусные программы для конечных точек Apple и Linux, у нее отсутствует унифицированная управляющая консоль для таких конечных точек. В результате, ИТ-администраторам приходится управлять индивидуально каждой конечной точкой, в том числе установкой антивирусной программы и обновлением соответствующей базы данных на каждом компьютере. При рыночной доле Apple, составляющей 8 % ПК и имеющемся росте этого показателя, доле Linux в 5 % и также имеющемся росте, этот процесс ложится тяжким бременем на ИТ-специалистов и вызывает повышение ССВ.

Оптимизированная архитектура безопасности McAfee
Оптимизированная архитектура безопасности McAfee предоставляет целостную и эффективную инфраструктуру обеспечения безопасности.

Синхронизация элементов позволяет оптимизировать безопасность

Начиная с единственного набора решений для обеспечения безопасности, McAfee создает многоуровневую архитектуру для защиты вашего бизнеса.

McAfee дает возможность пользователям прогнозировать и анализировать угрозы в реальном времени, используя для этого возможности McAfee Labs®. Переход от реагирования на угрозы к оптимизированному состоянию может произойти лишь в том случае, если организация не ощущает на себе постоянное воздействие атак. С известными угрозами можно справиться, однако, согласно последним сообщениям, в мире полным ходом и с угрожающей скоростью идет разработка новых и все более опасных эксплойтов. Осознание всей картины угроз является крайне важным для перехода от реагирования на угрозы к упреждающим действиям.

Обеспечение соответствия нормативным требованиям интегрируется в корпоративный процесс обеспечения безопасности. Не важно, ставится ли задача внутреннего аудита безопасности или обеспечения соответствия требованиям внешних стандартов, ИТ-подразделения в любом случае тратят огромное количество времени на сбор сведений и подготовку отчетов для того, чтобы подтвердить реализацию соответствующих мер безопасности. Эти трудоемкие процессы зачастую проводятся вручную и находятся за рамками обычного рабочего процесса ИТ-служб.

Платформа McAfee ePolicy Orchestrator — это мировой лидер среди платформ централизованного управления безопасностью. Отдельные продукты для обеспечения различных видов безопасности и раздельные управляющие консоли каждый день требуют сотни раз вручную передавать управление, что связывает ресурсы и привносит повышение уровня рисков без соответствующей необходимости. Для эффективного управления процессами безопасности ИТ-подразделению необходим контроль в масштабе всего предприятия над всеми системами и сетями, независимо от их места расположения.

McAfee ePolicy Orchestrator представляет собой открытую платформу управления безопасностью и точку интеграции для системы McAfee и ее продуктов сетевой безопасности, а также для продуктов, разработанных партнерами по McAfee Security Innovation Alliance. Благодаря средствам глобального обзора, которыми обладает консоль McAfee ePO, для групп ИТ-специалистов упрощается задача управления и обмена информацией в процессе обеспечения безопасности. Развертывание и администрирование таких продуктов вместе с подготовкой специалистов

существенно упрощаются, а эксплуатационные затраты на управление безопасностью в значительной степени снижаются. Благодаря возможности видеть полную картину событий, предприятия любого размера могут быстро и обоснованно принимать необходимые решения.

Краткие выводы

Мы будем рады, если любая организация, рассматривающая возможность покупки решения для безопасности конечных точек с целью замены используемой или установки дополнительной защиты, проведет тщательный сравнительный анализ ССВ при использовании решений от McAfee и от Symantec. Решение компании Symantec следовать подходу, предполагающему развертывание точечных продуктов с использованием компонентов защиты конечных точек в качестве самостоятельных продуктов, каждый из которых имеет собственную управляющую консоль, а также собственное ядро для применения политики и получения отчетности, оборачивается для организаций всех размеров значительно большей ССВ, чем при развертывании решения от McAfee. Несомненно, оптимизированная архитектура безопасности, предлагаемая компанией McAfee, и единая платформа управления ePolicy Orchestrator обеспечивают тесно интегрированные высокоэффективные решения при самой низкой стоимости. Мы уверены, что после выполнения собственного анализа вы придете к таким же выводам.

Приложение

Теоретические основы методологии расчета окупаемости инвестиций

Сравнение было проведено на основе результатов, полученных при использовании определенных сочетаний аппаратного и программного обеспечения, а также ограниченного набора оговоренных условий. Представленные результаты отражают примерные эксплуатационные характеристики продуктов McAfee в соответствии с результатами измерений, проведенных в процессе испытаний. Любые различия в аппаратном или программном обеспечении, а также в конфигурации, информации относительно затрат, влияние человеческого фактора — все это может вызвать изменение эксплуатационных характеристик. Информация, содержащаяся в настоящем документе, предоставляется исключительно в ознакомительных целях и предназначена для клиентов компании McAfee. Содержащаяся в настоящем документе информация может быть изменена без предварительного уведомления и предоставляется «как есть» без каких-либо гарантий точности и применимости данной информации к каким-либо конкретным ситуациям или обстоятельствам. Forrester не рекламирует McAfee и ее продукцию.

Помимо использования результатов из базы знаний Forrester Research, в процессе разработки данной модели были опрошены различные заинтересованные лица от компании McAfee, и их отчеты, содержащие информацию о впечатлениях, которыми поделились покупатели, подтвердили приведенные здесь данные. Этот инструмент был разработан для применения в виде книги Microsoft Excel 2003/2007, работающей под управлением операционной системы Microsoft Vista. Несмотря на то, что создавалась точная и отражающая реальность модель, McAfee и Forrester Research не берут на себя никаких юридических обязательств за какие-либо решения, принятые на основе приведенной информации. Данный инструмент предоставляется «как есть», и компании Forrester и McAfee не дают никаких гарантий. Подробная информация о методике Forrester Total Economic Impact изложена на веб-сайте http://www.forrester.com/TEI.

Сокращенную версию программы расчета можно получить по адресу http://www.mcafee.com/us/enterprise/products/tools/ad/roi.

Предположения относительно продукта и консоли Symantec

Для анализа ССВ, приведенного в настоящем документе, использовалась следующая конфигурация продукта и консоли Symantec.

Уровни защиты Symantec	Консоли	101	1 001	5 001	10 001
Антивирусная программа для персонального компьютера • Windows • Apple • Linux	SEP 11 • Symantec Administration Console for Macintosh • Только с пользовательским интерфейсом в виде командной строки	SEP 11	SEP 11	SEP 11	SEP 11
Защита от шпионских программ для персонального компьютера	SEP 11				
Система предотвращения вторжения на узел и межсетевой экран для персонального компьютера	SEP 11				

Уровни защиты Symantec	Консоли	101	1 001	5 001	10 001
Безопасность Интернета	Web Gateway Console	Консоль Symantec Web Gateway			
Защита сервера электронной почты от нежелательной почты и антивирусная программа	Консоль Brightmail		Консоль Brightmail + Symantec Mail Security for Exchange or Notes		
Управление устройствами	SEP 11		SEP 11		
Утеря данных	Консоль Vontu		Vontu		
Система предотвращения вторжения на узел и межсетевой экран для сервера	Консоль Critical System Protection			Critical System Protection	
Управление доступом к сети	SEP 11			SEP 11	
Аудит политики для персонального компьютера	Консоль Altiris SecurityExpressions (ASE)			Altiris SecurityExpressions	
Полнодисковое шифрование	Консоль GuardianEdge			GuardianEdge	
Антивирусная программа для шлюзов электронной почты и Интернет	Дополнительная консоль			Symantec Brightmail Appliance	
Фильтрация URL-адресов/ содержимого шлюзов электронной почты и Интернет	Консоль продуктовой линейки 8300			Symantec Brightmail Appliance	
Распределение агентов	Консоль ASE			Altiris SecurityExpressions	
Управление уязвимостью	SCCS			Symantec Control Compliance Suite (SCCS)	
Защита от нежелательной почты для шлюзов электронной почты и Интернет	Консоли Brightmail и Web GW				Brightmail
Исправление	Консоль ASE				Altiris Security-Expressions

Анализ ССВ проведен также с учетом перечисленных ниже предположений.

- Цена на приобретение решений Symantec для более чем 1 000 конечных точек приведена с учетом стандартной для данной отрасли скидки
- Для цены на Symantec Data Loss Prevention (DLP), зависящей от функциональных возможностей, была принята конфигурация только с функцией Vontu Endpoint Prevent. Цена DLP должна возрасти в два-три раза, если включить шесть дополнительных продуктов Vontu DLP от Symantec (Endpoint Discover, Network Discover, Network Prevent (Email), Network Prevent (Web), Network Protect и Network Monitor).
- Как для McAfee, так и для Symantec в цену покупки включались по одному выделенному серверу на консоль по цене 5 000 долларов США за сервер
- Для развертывания 100 узлов предполагалось привлечение одинаковых ИТ-ресурсов как в McAfee, так и в Symantec, несмотря на то, что сами работы могут быть различными при выполнении каждого из двух развертываний
- И для McAfee, и для Symantec ежегодные затраты на одну полную штатную единицу ИТ-персонала были приняты в размере 79 290 долларов США при ежегодном их двухпроцентном увеличении.

О компании McAfee

Компания McAfee, Inc., штаб-квартира которой расположена в г. Санта-Клара, является крупнейшей в мире компанией, специализирующейся на технологиях безопасности. Она предоставляет проверенные упреждающие решения и службы, которые обеспечивают безопасность систем и сетей по всему миру, позволяя пользователям безопасно работать и совершать покупки. Обладая уникальным опытом в области безопасности и стремясь к инновациям, McAfee предлагает решения, которые позволяют индивидуальным пользователям, компаниям, общественным организациям и поставщикам услуг Интернета соответствовать нормативам, защищать данные, предотвращать нарушение работы, определять уязвимости, а также постоянно наблюдать за уровнем собственной безопасности и повышать его. www.McAfee.ru.

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru