ПОЛНАЯ СТОИМОСТЬ ВЛАДЕНИЯ ENDPOINT PROTECTION

panda

pandasecurity.com

01

Обзор
для руководителя

02

Основные составляющие
полной стоимости владения

03

Расчет полной стоимости
владения и сравнение

01 Обзор для руководителя

В наши дни предприятия любых размеров при ведении бизнес-деятельности все больше зависят от своих ИТ-систем и, как результат, они стали более чувствительны к уязвимостям и другим проблемам ИТ-безопасности. Добавьте еще к этому возросшую мобильность персонала и объективные трудности в управлении удаленными и мобильными устройствами. В итоге мы имеем сценарий, при котором управление операциями безопасности стали более комплексными, дорогостоящими и сложными. Фактически, многие сбои и простои ИТ-систем вызваны человеческими ошибками в силу ручного характера управления традиционными локальными ИТ-решениями.

Ситуацию усугубляет еще и тот факт, что по данным Gartner, малым и средним предприятиям (а в наши дни это большинство предприятий) все сложнее удержать специалистов по ИТ-безопасности.

Для решения этих проблем появляются новые решения класса "ПО как услуга" (SaaS), которые способны заменить или расширить возможности традиционных локальных решений. В частности, SaaS-решения по безопасности конечных точек, такие как Endpoint Protection, могут быть доступны в любое время с любого устройства через любой веб-браузер, обеспечивая простое и понятное управление файерволом и защитой от вредоносных программ.

Потребности компаний, которые способствуют внедрению комбинированной модели

Первое преимущество SaaS-решения типа Panda Endpoint Protection, если сравнивать с традиционной защитой от вредоносных программ для рабочих станций, - это отсутствие первоначальных инвестицийдля его внедрения. Традиционная защита требует инвестиций в локальные "железо" и ПО (административные серверы, репозитории, базы данных), добавляя точки сбоя, уязвимости и соответствующие расходы на обслуживание и апгрейд. SaaS-решение, наоборот, переносит все инфраструктуру управления в инфраструктуру производителя.
В этом плане чем более распределенная средва, тем выше уровень экономии (обычно, каждый офис требует как минимум один сервер при использовании локальных решений).

Рассматривая усредненный случай внедрения антивирусного решения в среднем предприятии, экономия при внедрении SaaS-решения может достигать 50% от всех расходов. Данный документ показывает, как такая экономия возможна.

Второе важное преимущество заключается в том, что у партнеров появляется возможность предоставлять услуги своим клиентам, а многие из них ищут такие возможности, чтобы отчасти компенсировать свои потери от продажи компьютерной техники в последние годы. В случае с Endpoint Protection, партнеры могут использовать специальную "партнерскую" консоль, позволяющую им эффективно управлять решением безопасности своих клиентов через единую веб-консоль, удаленно без дополнительных расходов на ПО и "железо". Таким образом, малые и средние предприятия теперь имеют возможность отдавать функции управления на аутсорсинг таким провайдерам (MSSP).

Наконец, третье преимущество состоит в "природной" способности SaaS-подхода решать вопросы, связанные с мобильным персоналом. Сегодня контроль и управление мобильными сотрудниками с ноутбуками и смартфонами - это источник беспокойства для администраторов. С помощью такого решения как Panda Endpoint Protection администратор (или MSSP) может удаленно контролировать и настраивать антивирус и файервол на ноутбуках и смартфонах вне зависимости от их местоположения или типе Интернет-подключения.

02 Основные составляющие полной стоимости владения

Каковы определяющие расходы, на которые компаниям необходимо обратить внимание при анализе полной стоимости владения?

Капитальные расходы

Традиционные решения безопасности

Переходы на другие решения безопасности, которые могут потребоваться, связаны с дополнительными капитальными расходами.

Аппаратное и программное обеспечение, сетевая инфраструктура, утилиты мониторинга и тестирования, дополнительные принадлежности и другая требуемая инфраструктура являются частью типовых капитальных расходов. Такие расходы - это предварительные финансовые расходы.

SaaS-решения безопасности

С помощью SaaS-решений Вы избавлены от инфраструктурных расходов. "Природа" SaaS - Вы платите за то, что используете. SaaS-модели позволяют говорить о повторяющейся структуре расходов. Вы платите месячную или годовую стоимость сервиса так долго, пока Вы пользуетесь сервисом.

Данная оплата сервиса включает в себя сопровождение, поддержку, обновления и апгрейды программного обеспечения, а также все расходы на аппаратное обеспечение, сетевые инструменты, хранение, базы данных, администрирование и другие расходы, связанные с предоставлением SaaS-сервиса.

Расходы на внедрение

Традиционные решения безопасности

- Расходы на штатный и наемный персонал для интеграции, тестирования, настройки и запуска решений безопасности - это значительные расходы, связанные с развертыванием традиционных решений безопасности.
- Должны быть оценены и при необходимости расширены серверные и сетевые возможности.
- Должны быть проверены и обновлены (если надо) серверное "железо", операционные системы и приложения на совместимость с выбранным решением безопасности.
- Необходимы тестирование и настройка системы для обеспечения требуемой производительности при внедрении решения.
- Требуется обучение ИТ-персонала.
- Внедрение, пилотные проекты и пр. также требуют ИТ-ресурсов.

SaaS-решения безопасности

SaaS-решения безопасности могут быть внедрены намного быстрее и за меньшую стоимость по сравнению с традиционными решениями безопасности.

Очень важно, когда расходы на возможность получения приложения слишком высоки. Но с другой стороны, в силу того, что SaaS-решение безопасности является многопользовательским приложением, существует меньше возможностей для его кастомизации в соответствии с ИТ-архитектурой предприятия.

Текущие затраты на инфраструктуру

Традиционные решения безопасности

- Для текущей эксплуатации часто требуются инструменты сетевого мониторинга и управления, чтобы обеспечить в реальном времени диагностику проблем и реагирование на них.
- Ежегодные контракты на сопровождение и поддержку ПО, системные обновления и апгрейды делают весомый вклад в полную стоимость владения.
- Масштабирование инфраструктуры, несколько резервных систем и дополнительные компоненты увеличивают расходы.
- Ремонт и замена оборудования - это периодические расходы.

SaaS-решения безопасности

Помимо возможных потребностей в дополнительном Интернет-канале, почти нет дополнительных расходов на инфраструктуру, требуемую при масштабировании SaaS-решения безопасности, а в некоторых случаях, как с Panda Endpoint Protection, SaaS-решение безопасности позволяет избавится даже от этих затрат.

Возможно, придется внедрить локальные приложения, позволяющие запустить защиту конечных точек и обеспечить соединение с серверами, размещенными у производителя.

Масштабирование инфраструктуры и расходы, связанные с ее ростом, - это полностью ответственность SaaS-провайдера.

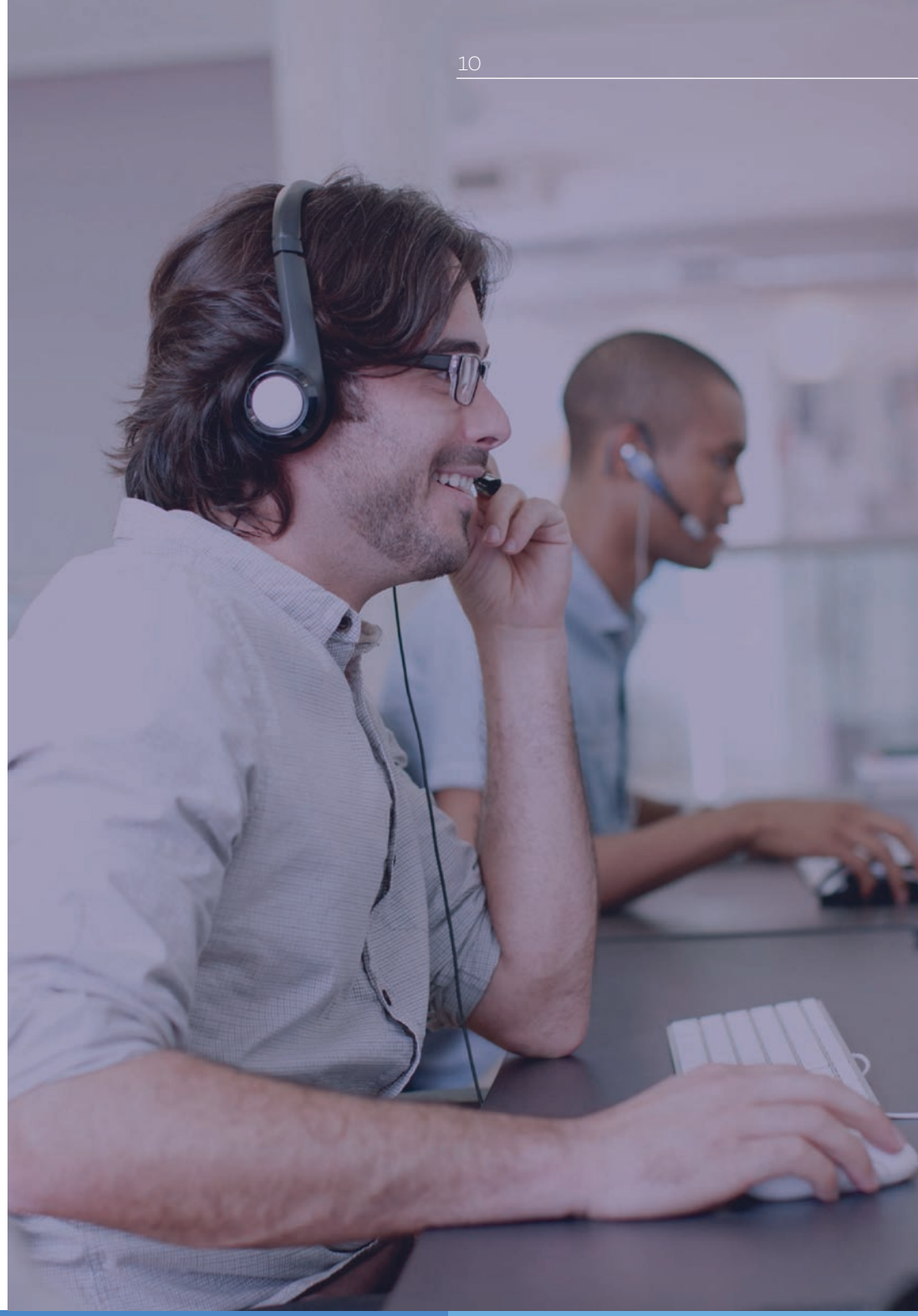
Операционные расходы и поддержка

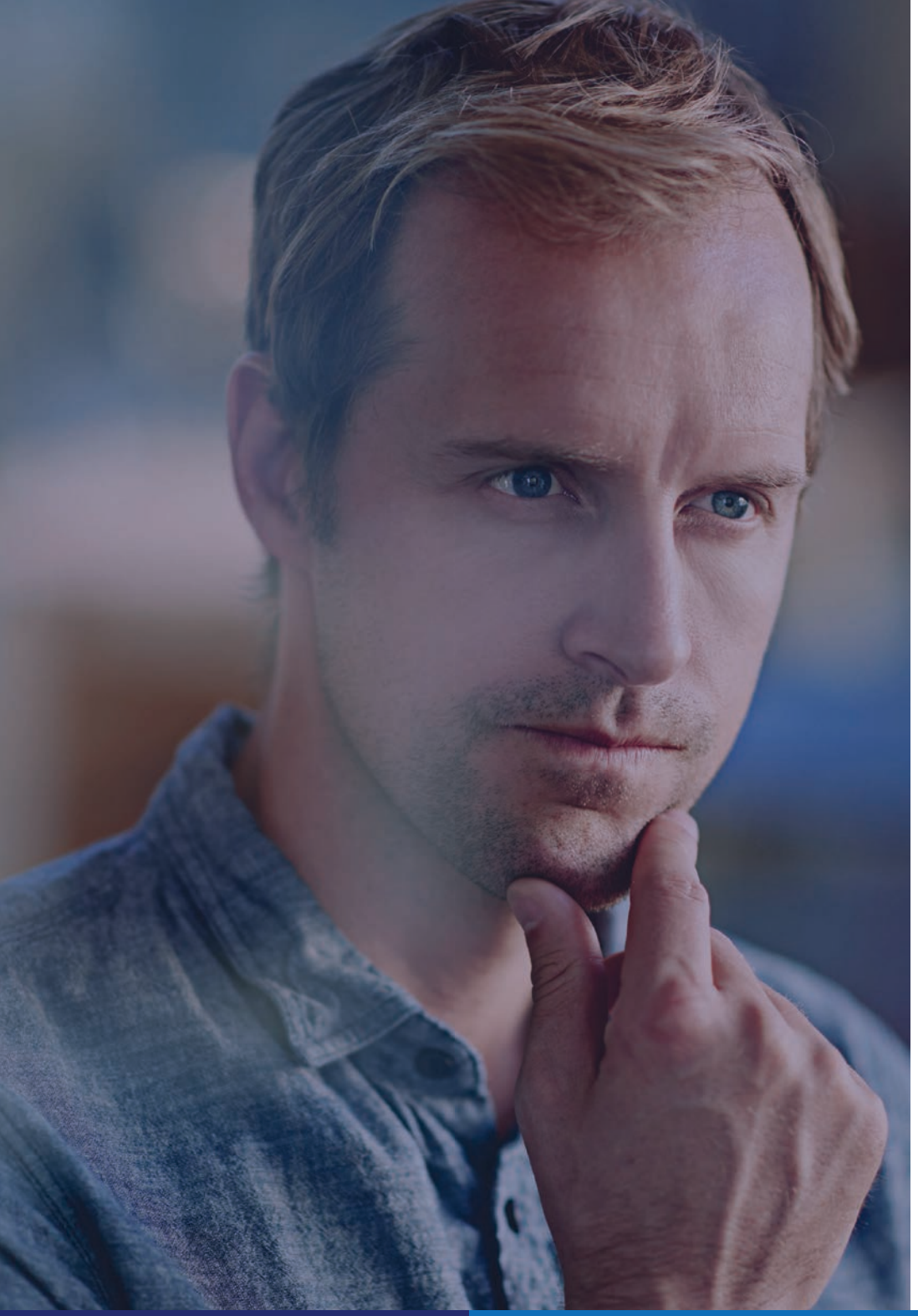
Традиционные решения безопасности

- Необходимо выделять ресурсы на мониторинг, поддержку и обслуживание решения безопасности.
- Если решение новое для компании, то необходимо обучать и сертифицировать существующий персонал и/или набирать новый персонал с или без знания приложения.
- Плюс каждый раз, когда необходимо внедрить патч или апгрейд, требуются дополнительные ИТ-ресурсы.
- Это, как правило, наибольшие скрытые расходы, которые должны учитываться при принятии решения о том, стоит ли покупать новое решение. Если данные расходы оцениваются неверно, то существенно могут измениться и оценки возможного снижения затрат.
- Поддержка - это заключительный и самый важный файктор успеха для успешного внедрения и последующего использования нового решения безопасности: всякий раз, когда есть проблема, она может привести к потери производительности или, в худшем случае, к отказу от использования решения безопасности.

SaaS-решения безопасности

Провайдеры SaaS-решений в конечном итоге ответственны за предоставление решения и работу инфраструктуры, на которой размещено SaaS-решение безопасности.





Нематериальные затраты

Нематериальные затраты труднее измерить, поэтому их труднее включить в анализ полной стоимости владения, но при этом они не становятся менее реальными. Некоторые из них, влияющие на полную стоимость владения:

- **Надежность и доступность**: Сбой в работе означает потерю рабочего времени и возможностей, так что могут потребоваться дополнительные усилия для восстановления работы. Какой уровень сервиса предлагает SaaS-провайдер и как сравнить с уровнем сервиса традиционного решения?
- **Совместимость**: Насколько просто интегрировать решение с другими приложениями?
- **Гибкость**: Насколько просто кастомизировать приложение в соответствии с потребностями предприятия?
- **Масштабируемость**: По мере роста числа пользователей, ресурсов исходной системы может не хватить, что приведет к задержкам работы сотрудников и потере возможностей. Насколько масштабируемо SaaS-решение и каковы расходы, связанные с масштабируемостью традиционного приложения?
- **Производительность**: Использование и внедрение внутри предприятия сложно предсказать, что усложняет управление производительностью. В итоге: низкая производительность с одной стороны и малоиспользуемая инфраструктура с другой. Этими аспектами намного проще управлять с помощью SaaS-решения по сравнению с традиционным приложением.
- **Потеря возможностей**: Человеческие ресурсы и капитальные затраты, требуемые на внедрение локального решения, могут сократить расходы на другие проекты или временно отложить внедрение новых продуктов и сервисов, что может непосредственно повлиять на развитие компании.

03
Расчет полной стоимости владения и сравнение

Пример 1: один офис с 50 сотрудниками

Первый пример касается среднего предприятия с 50 рабочими станциями и серверами, которые должны быть защищены от вредоносных программ. Представлено сравнение показателей трех традиционных решений безопасности с SaaS-решением Panda Endpoint Protection.

Примерно два человека-дня требуется на внедрение традиционного решения безопасности (установка, интеграция и конфигурация) плюс дополнительно полдня в год на апгрейд. С Panda Endpoint Protection это время сокращено до полдня на настройку решения. С SaaS-решением безопасности регулярное обслуживание сводится только к поддержке конфигурации, т.е. внедрению правил корпоративной безопасности в решение.

Т.к. традиционные решения требует большего внимания со стороны администраторов, то требуется больше времени на мониторинг и дальнейшее обучение. Примерно 6 человеко-дней в год должно быть выделено на обслуживание традиционного решения безопасности. При использовании SaaS-решения безопаности Panda Endpoint Protection, не требуется время на обучение, мониторинг и администрирование сервера и ПО, а потому это время сокращено до 2 человеко-дней в год.

Если мы оценим человеко-день в 400 евро, то становится очевидным, что административные расходы для традиционного решения примерно равны стоимости приобретения.

Впрочем, данный пример не является истинным для подобного сравнения, т.к. SaaS-сервис наподобие Panda Endpoint Protection использует технологию резервирования для обепечения безотказной работы сервиса, в то время как традиционное решение связано с определенными рисками сбоя. Компании, желающие внедрить резервные системы, должны будут инвестировать во вторую машину, что существенно увеличит административные расходы.

Чтобы упростить анализ, мы не рассматриваем преимущества в масштабируемости, гибкости и сокращении потерей возможностей, которые дает SaaS-решение.

Анализ полной стоимости владения для данного примера показывает, что Panda Endpoint Protection обойдется в 4150 евро за один год и 6525 евро за два года. Традиционные решения безопасности потребуют больших расходов в первый год за счет расходов на сервер управления и затрат на обслуживание.

Даже при консервативной оценке расходов, связанных с традиционными решениями безопасности, компании потребуется потратить в первый год 7189 евро за решение А, 7315 евро - за решение Б и 7663 - за решение В.

Двухлетние расходы на Panda Endpoint Protection составят 6525 евро, в то время как расходы на традиционные решения безопасности составят 10853, 10867 и 13797 евро соответственно.

При покупке лицензий на 1 год, Panda Endpoint Protection дешевле примерно на 42%, чем традиционное решение безопасности А, на 43% дешевле решения Б и на 46% дешевле решения В.

При покупке лицензий на 2 года, Panda Endpoint Protection на 40% дешевле традиционных решений А и Б и на 53% дешевле решения В.

Анализ расходов Начальные расходы	Традиционное решение безопасности А	Традиционное решение безопасности Б	Традиционное решение безопасности В	SaaS-решение безопасности Panda Endpoint Protection
Капитальные затраты:				
Расходы на ПО или лицензии	0 €	0 €	0 €	0 €
"Железо" (сервер управления)	1.400 €	1.400 €	1.400 €	0 €
ОС (сервер управления)	250 €	250 €	250 €	0 €
Расходы на внедрение:				
Проектировка и инжиниринг (дней)	1	1	1	0
Проектировка и инжиниринг (расходы)	400 €	400 €	400 €	0 €
Интеграция/внедрение (дней)	1	1	1	1
Интеграция/внедрение (расходы)	400 €	400 €	400 €	200 €
Год1				
Капитальные затраты:				
Расходы на ПО или лицензии	3.203 €	3.218 €	6.147 €	4.725 €
Расходы на внедрение:				
Интеграция/внедрение (дней)	1	1	1	0
Интеграция/внедрение (расходы)	200 €	200 €	200 €	0 €
Текущие расходы на инфраструктуру, операции и поддержку:				
ИТ-персонал (дней)	6	6	6	2
ИТ-персонал (расходы)	2.400 €	2.400 €	2.400 €	800 €
Год2				
Расходы на внедрение:				
Интеграция/внедрение (дней)	0,5	0,5	0,5	0
Интеграция/внедрение (расходы)	200 €	200 €	200 €	0 €
Текущие расходы на инфраструктуру, операции и поддержку:				
ИТ-персонал (дней)	6	6	6	2
ИТ-персонал (расходы)	2.400 €	2.400 €	2.400 €	800 €
Всего расходов (2 года)	10.853 €	10.868 €	13.797 €	6.525 €

Примечание: Анализируемые решения предлагают одинаковые функции безопасности для корпоративных рабочих станций и серверов. Расчеты основаны на потребности в выделенном сервере безопасности, хотя возможно запустить традиционное решение безопасности на суещсвующем сервере. Расходы на серверы управления (аппаратное и программное обеспечение), проектировку, внедрение, текущие операции и поддержку были получены после опроса малых и средних предприятий. Расходы на лицензии были взяты из официальных интернет-магазинов производителей решений, доступных через Интернет по состоянию на февраль 2009 года.

Пример 2: три офиса с 50 сотрудниками

Разница между локальными традиционными решениями безопасносит и SaaS-решением безопасности Panda Endpoint Protection становится более заметной, когда мы рассматриваем компанию с несколькими офисами. Если представить, что вышеупомянутые 50 сотрудников распределены между тремя офисами компании, то каждый офис требует отдельного сервера управления, который необходимо установить и обслуживать.

Хотя, конечно, можно установить менее мощные серверы в каждый офис по сравнению с тем, что был установлен в примере 1, но все равно полные расходы на приобретение значительно возрастут.

Административные расходы также намного выше для компаний с распределенной структурой и офисами. Т.к. многие административные задачи могут выполняться централизованно для всех офисов, расходы не увеличиваются пропорционально количеству инсталляций. Расходы на поддержку и издержки, понесенные в силу потери производительности, остаются прежними, т.к. эти факторы во многом зависят от количества сотрудников и типа решения.

Стоимость внедрения локального традиционного решения безопасности в компании с тремя офисами примерно на 50% выше, чем поддержка такого же количества пользователей в одном офисе. С Panda Endpoint Protection количество офисов не влияет на расходы, т.к. они основаны исключительно на количестве пользователей. Административные расходы также остаются такими же, т.к. сервис может полностью централизованно управляться из единого офиса.

Даже при консервативной оценке расходов, связанных с традиционными решениями безопасности, компании потребуется потратить в первый год 9774 евро за решение А, 9900 евро - за решение Б и 10248 - за решение В.

Двухлетние расходы на Panda Endpoint Protection составят 6525 евро, в то время как расходы на традиционные решения безопасности составят 14703, 14717 и 17647 евро соответственно.

При покупке лицензий на 1 год, Panda Endpoint Protection дешевле примерно на 65%, чем традиционное решение безопасности А, на 66% дешевле решения Б и на 67% дешевле решения В.

При покупке лицензий на 2 года, Panda Endpoint Protection на 55% дешевле традиционных решений А и Б и на 63% дешевле решения В.

Анализ расходов Начальные расходы	Традиционное решение безопасности А	Традиционное решение безопасности Б	Традиционное решение безопасности В	SaaS-решение безопасности Panda Endpoint Protection
Капитальные затраты:				
Расходы на ПО или лицензии	0 €	0 €	0 €	0 €
"Железо" (сервер управления)	2.250 €	2.250 €	2.250 €	0 €
ОС (сервер управления)	250 €	250 €	250 €	0 €
Расходы на внедрение:				
Проектировка и инжиниринг (дней)	2	2	2	0
Проектировка и инжиниринг (расходы)	600 €	600 €	600 €	0 €
Интеграция/внедрение (дней)	2	2	2	1
Интеграция/внедрение (расходы)	600 €	600 €	600 €	200 €
Год 1				
Капитальные затраты:				
Расходы на ПО или лицензии	3.203 €	3.218 €	6.147 €	4.725 €
Расходы на внедрение:				
Интеграция/внедрение (дней)	0,8	0,8	0,8	0
Интеграция/внедрение (расходы)	300 €	300 €	300 €	0 €
Текущие расходы на инфраструктуру, операции и поддержку:				
ИТ-персонал (дней)	9	9	9	2
ИТ-персонал (расходы)	3.600 €	3.600 €	3.600 €	800 €
Год 2				
Расходы на внедрение:				
Интеграция/внедрение (дней)	0,8	0,8	0,8	0
Интеграция/внедрение (расходы)	300 €	300 €	300 €	0 €
Текущие расходы на инфраструктуру, операции и поддержку:				
ИТ-персонал (дней)	9	9	9	2
ИТ-персонал (расходы)	3.600 €	3.600 €	3.600 €	800 €
Всего расходов (2 года)	**14.703 €**	**14.718 €**	**17.647 €**	**6.525 €**

Примечание: Анализируемые решения предлагают одинаковые функции безопасности для корпоративных рабочих станций и серверов. Расчеты основаны на потребности в выделенном сервере безопасности, хотя возможно запустить традиционное решение безопасности на суещсвующем сервере. Расходы на серверы управления (аппаратное и программное обеспечение), проектировку, внедрение, текущие операции и поддержку были получены после опроса малых и средних предприятий. Расходы на лицензии были взяты из официальных интернет-магазинов производителей решений, доступных через Интернет по состоянию на февраль 2009 года.


panda