Использование программного обеспечения в качестве услуги для ведения бизнеса и повышения производительности информационных технологий

Для продуктов Google, обеспечивающих безопасность и соблюдение правил

Google™

Корпорация LSI использовала внутреннее программное решение для защиты своего канала электронной почты от нежелательного трафика, но когда объем трафика сообщений резко вырос и замедлил работу пользователей, стало понятно – пришло время перемен. После строгого отбора корпорация LSI выбрала систему Google для обеспечения безопасности и соблюдения правил передачи сообщений, основанную на технологии Postini – и теперь, после трех лет работы и приобретения шести других компаний, данное решение все еще требует лишь минимальной настройки.

Введение

Ведущие ИТ-организации могут повысить свою производительность, применяя методы сотрудничества и передачи информации в режиме реального времени. По мере того как увеличивается количество сотрудников, использующих для передачи важных сообщений электронную почту и Интернет, повышается уязвимость информации, передаваемой по этим каналам; если не принять меры по защите таких каналов, то в организации повышается риск потенциальных нарушений безопасности и соответствия правилам.

Многие ИТ-организации для обеспечения безопасности передачи электронной информации используют специально разработанные устройства или программное обеспечение, однако эти системы первого поколения не отвечают четырем основным требованиям, предъявляемым к подобным решениям (см. рис. 1).

Во-первых, такие решения являются дорогостоящими и имеют значительную скрытую общую стоимость владения. Хотя исходная стоимость открытой лицензии на программное обеспечение кажется приемлемой, сопутствующие затраты на приобретение, установку и текущее обслуживание оборудования могут существенно увеличить общую стоимость владения решением.

Во-вторых, аппаратные и программные решения первого поколения не обеспечивают гибкость, и их модернизация весьма сложна. Каждый раз, когда требуется обновить или изменить политику, связанное с этим время простоя или задержки может представлять риск для безопасности или соответствия правилам. Кроме того, программы обеспечения безопасности, а также оборудование и операционную систему необходимо регулярно модернизировать или обновлять, что связано с незапланированными затратами на управление и доработку, а также создает нежелательные риски для организации.

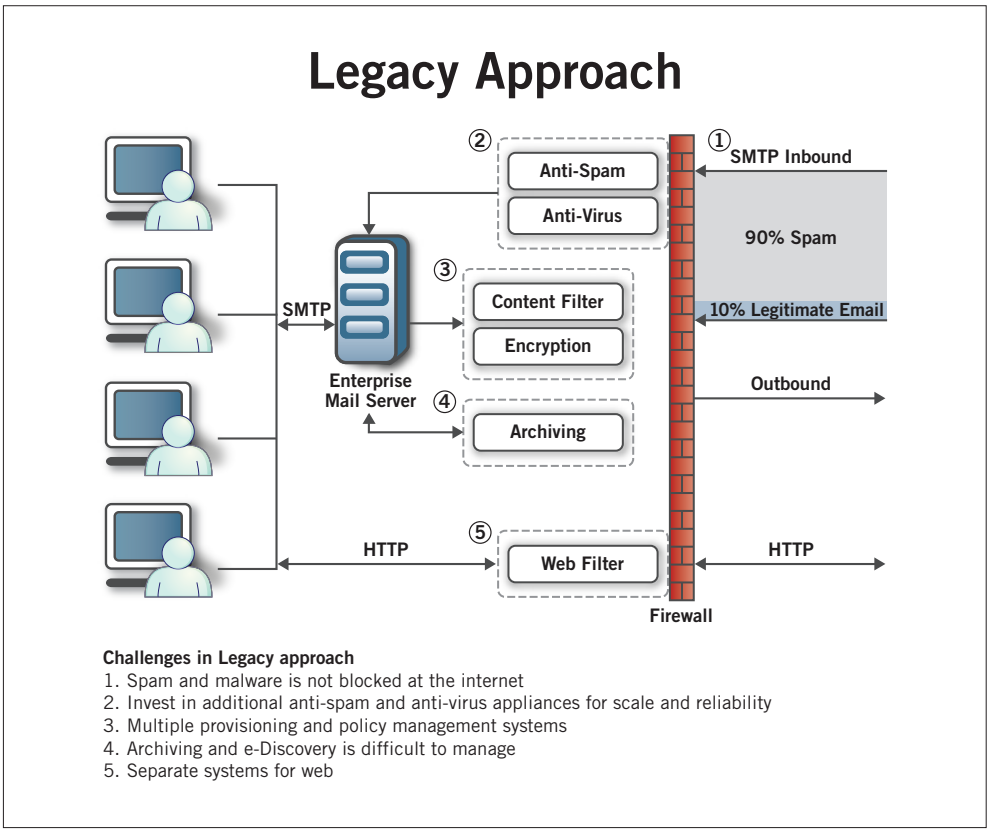

Рисунок 1. Система обеспечения безопасности электронной связи на основе специально разработанных устройств или программного обеспечения, устанавливаемого на оборудовании клиента, обходится дорого, обычно не интегрирована, требует нескольких решений, сложна в управлении и требует обслуживания в пределах брандмауэра.

Бухгалтерская фирма Harb, Levy & Weiland LLP (Сан-Франциско) полностью полагается на продукты Google для обеспечения безопасности и соответствия правилам для повышения производительности более чем 100 своих сотрудников. Отфильтровывая весь нежелательный трафик еще до того, как он дойдет до конечного пользователя, компания Google помогает этой фирме свести к минимуму время, затрачиваемое сотрудниками на очистку входящей почты от спама. Кроме того, для обеспечения конфиденциальности важной информации клиентов во всех электронных сообщениях эта фирма использует службу шифрования сообщений компании Google, основанную на технологии Postini.

В-третьих, этим решениям не хватает встроенной масштабируемости, что приводит к необходимости приобретения дополнительных ресурсов по мере роста организации или даже для обработки информации при периодических пиковых нагрузках. Отсутствие масштабируемости также обусловливает значительные затраты и риски и может отрицательно сказываться на производительности, если при увеличении количества сообщений из-за неэффективности решения будут происходить сбои в их передаче.

Наконец, отдельные решения обычно не интегрированы в общую систему, что создает проблемы с соответствием нормативным требованиям из-за несовместимых, конфликтующих конфигураций и политик. Проблема усложняется при отсутствии единого командного и управляющего интерфейса или консоли управления, в результате чего эти системы первого поколения фактически усложняют ту проблему, которую они должны были бы устранить.

Недавно в качестве альтернативы дорогим, негибким и сложным в использовании решениям на основе программного и аппаратного обеспечения, устанавливаемого у пользователя, появились перспективные решения типа "программное обеспечение как услуга" (Software as a Service, SaaS). Предоставляя программные функции в качестве услуги вместо традиционного подхода с установкой системы на оборудовании пользователя, решения SaaS стали популярной альтернативой для всех типов программного обеспечения, критически важного для бизнеса. Согласно прогнозу компании отраслевого анализа Gartner Group в 2011 г. ожидается более чем двукратное увеличение числа решений SaaS по сравнению с традиционно устанавливаемыми приложениями[1].

Однако не все решения для обеспечения безопасности и соблюдения правил передачи электронной информации, использующие модель SaaS, одинаковы – ИТ-организациям требуется надежный набор критериев для оценки поставщиков решений "по запросу" и выбора решения, наиболее отвечающего требованиям конкретной компании.

В этой статье рассматриваются пять ключевых критериев, которые должны учитывать директора по информационным технологиям при выборе решения "по запросу" для обеспечения безопасности и соблюдения правил передачи информации, чтобы организация обслуживания информационных технологий могла принести большую практическую пользу компании.

Оценка решения "по запросу" для обеспечения безопасности и соблюдения правил передачи информации

При оценке поставщика решений "по запросу" для обеспечения безопасности и соблюдения правил передачи информации ИТ-организации должны рассматривать пять основных вопросов.

1. Эффективность

Высокая эффективность решения для обеспечения безопасности и соблюдения правил передачи информации – решающий фактор при выборе. Организациям необходимо знать, что решение может эволюционировать для удовлетворения изменяющихся потребностей и при этом также эффективно обеспечивать безопасность и соблюдение правил передачи информации. Потенциальный поставщик решения "по запросу" должен дать ответы на следующие вопросы:

- Основано ли решение на использовании платформы, обеспечивающей безопасность и соблюдение правил по всем каналам связи (например, электронная почта и Интернет)?
- Допускает ли решение быстрое и простое добавление новых служб или приложений без перерыва в работе служб?
- Может ли поставщик быстро внести изменения в решение для обеспечения соответствия новым правилам и юридическим стандартам по мере их появления?

[1] Report Highlight for Dataquest Insight: SaaS Demand Set to Outpace Enterprise Application Software Market Growth (Основные положения отчета для Dataquest Insight: спрос на решения SaaS опережает рост рынка программных приложений для предприятий), Sharon A. Mertz, Gartner, Inc, August 17, 2007

Служба вывоза и утилизации отходов Norcal Waste (Калифорния) предоставила 2100 своим сотрудникам доступ к интернет-приложениям с помощью клиент-терминалов, подключенных к центральному прокси-серверу. Перейдя с внутренней системы на службы Google для организаций, основанные на технологиях Postini, компания Norcal Waste теперь защищает свою сеть от интернет-угроз, не снижая эффективность работы своих пользователей и не загружая свой небольшой ИТ-персонал задачами по обслуживанию.

- Может ли поставщик быстро адаптироваться к изменяющимся требованиям к безопасности и обеспечивать защиту, сводящую к минимуму риск для клиентов?
- Как давно данный поставщик предоставляет надежные и высококачественные решения SaaS?

2. Гибкость

При выборе поставщика решения "по запросу" для обеспечения безопасности и соблюдения правил передачи информации важно помнить, что одно и то же решение не может подходить всем. Организации должны искать легко администрируемые и управляемые решения, соответствующие их конкретным требованиям и позволяющие техническому персоналу сфокусировать свои усилия на производительных операциях, непосредственно связанных с основной деятельностью компании. Вот некоторые вопросы, которые следует задать поставщику решения:

- Как осуществляется управление аналогичными наборами правил для электронной почты и веб-содержания?
- Можно ли использовать одни и те же настройки политики или требуется создать специальный профиль для каждого набора правил?
- Как быстро вводятся в действие срочные изменения в наборы правил, связанные с появлением новых угроз безопасности или нормативных требований? Время ожидания – это минуты или часы?
- Могут ли различные отделы внутри организации создавать свои собственные требования к безопасности и соблюдению правил, не нарушая при этом процесс передачи сообщений?
- Какой уровень структуризации используется для отслеживания сообщений и расследования нарушений?

3. Простота развертывания и использования

К числу важнейших характеристик решения для обеспечения безопасности и соблюдения правил передачи информации относятся простота развертывания и использования. Чем сложнее решение с точки зрения развертывания и использования, тем оно менее безопасно – и тем меньше вероятность, что решение обеспечит соответствие организации текущим нормативным требованиям. Следует обратить внимание на следующие основные вопросы:

- Сколько времени требуется для установки и запуска системы?
- Насколько сложен процесс настройки и периодического изменения конфигурации системы?
- Насколько сильно система вмешивается в обработку электронной корреспонденции? Требуется ли запись на диск (что вносит задержку и увеличивает угрозу безопасности) или используется более рациональный метод обработки сообщений?
- Могут ли сотрудники самостоятельно выполнять типовые задачи (например, настройку фильтров) через порталы самообслуживания или требуется помощь администратора?
- Сколько места займет решение в вычислительном центре?
- Потребуется ли дополнительное оборудование или персонал для запуска или для управления решением?

4. Низкая общая стоимость владения

К сожалению, у некоторых поставщиков начальная стоимость решения для обеспечения безопасности и соблюдения правил передачи информации может быть лишь "верхушкой айсберга". Организациям следует быть внимательными и выбирать решение "по запросу", которое обеспечивает низкие как исходные, так и последующие накапливающиеся затраты. Вот некоторые вопросы, на которые должен ответить поставщик:

Учитывая постоянные и устанавливаемые юридические требования и правовые нормы, более 2500 сотрудников фирмы Analysts International предоставляют местным властям и властям штата консультационные услуги по широкому кругу вопросов (от автомобилей до медицины). Фирма обратилась в компанию Google не только для защиты электронной почты, но и для архивирования всех почтовых и мгновенных сообщений. Почему? Потому что продукты Google для обеспечения безопасности и соблюдения правил экономически привлекательны со всех точек зрения – эффективность, затраты и поддержка – и освобождают ИТ-персонал фирмы от значительной нагрузки по поддержке и обслуживанию большой базы пользователей.

- Сколько времени требуется для развертывания решения?
- Какие ресурсы требуются для развертывания решения?
- Выполняется ли внедрение решения самим поставщиком или заказчику нужно будет нанимать экспертов для работы на своем объекте?
- Требует ли решение каких-либо капиталовложений на дополнительное оборудование, программное обеспечение или ресурсы?
- Каковы предварительные расходы на решение? Существуют ли какие-либо скрытые или последующие затраты?
- Как быстро решение начнет приносить пользу организации?
- Насколько предсказуемы затраты на расширение услуги в случае развития компании или изменения ее потребностей?

5. Масштабируемость и надежность

В современной быстро развивающейся бизнес-среде масштабируемость и надежность приобретают первостепенное значение. Решение, обеспечивающее безопасность и соблюдение правил передачи информации, должно быть масштабируемым, чтобы эффективно работать при любых обстоятельствах и постоянно приносить пользу организации. При выборе поставщика решения SaaS ключевыми являются следующие критерии:

- Работает ли поставщик на глобальном уровне, чтобы обеспечить масштабирование по мере роста вашей компании?
- Предусмотрена ли поставщиком физическая защита своего объекта?
- Какова общая архитектура рабочей сети? Одиночный сайт с резервированием или кластер? Почему была выбрана архитектура данного типа?
- Как обеспечиваются целостность систем и конфиденциальность данных?
- Как будет осуществляться масштабирование рабочей сети для последующего роста потребностей? Предусмотрена ли стратегия роста?
- Какой тип задержки передачи сообщений может быть обусловлен самим решением?
- Как обеспечивается обработка отказов и резервирование?

Решения "по запросу" для обеспечения безопасности и соблюдения правил передачи информации, которые не соответствуют этим пяти критериям, фактически вводят в заблуждение организацию, которая приобрела подобную услугу. Почему? Потому что они не помогают компании ни улучшить работу и производительность информационных технологий, ни увеличить доход.

Платформа – решение "по запросу" для обеспечения безопасности и соблюдения правил

Компания Google является поставщиком наиболее эффективных решений "по запросу", соответствующих всем пяти критериям эффективности решения для обеспечения безопасности и соблюдения правил передачи информации.

1. Эффективность

Платформа Google для обеспечения безопасности и соблюдения правил, созданная на основе технологий Postini, ежедневно обрабатывает больше сообщений, чем какой-либо другой из предлагаемых в настоящее время продуктов для обеспечения безопасности и соблюдения правил передачи электронной информации. Такой объем сообщений позволяет компании Google создавать современную и самую точную интеллектуальную систему обработки существующих в Интернете угроз и очень эффективно применять эту интеллектуальную систему для обработки сообщений, проходящих

Когда предоставление собственного хостинга электронной почты и услуг службы доставки стало невозможным из-за стремительного роста объемов спама, расположенная в Канаде розничная торговая компания Dazzl обратилась в компанию Google. Избавившись от затрат на оборудование для обеспечения растущих мощностей, а также от проблем с временем работы и задержкой доставки, компания Dazzl после ввода в эксплуатацию системы безопасности Google почти сразу же добилась значительного роста производительности персонала, так как сотрудники смогли уделять больше внимания клиентам и приносить доход, а не тратить время на обслуживание собственного решения для обеспечения безопасности электронной почты.

по сети Google, в режиме реального времени. Например, когда Google обнаруживает вирус с началом атаки по расписанию, передаваемый отправителем клиенту, по всей сети рассылается предупреждение, выполняется обновление и сеть защищается в режиме реального времени, обеспечивая опережающую защиту от злоумышленников. Благодаря этому так называемому "сетевому эффекту" система защиты от вирусов компании Google более эффективна, чем традиционные брандмауэры или антивирусное программное обеспечение, требующее обновления баз данных или отключения для изменения конфигурации.

Обработка каждого канала связи в продуктах Google состоит из четырех этапов (см. рис. 2).

Обработка сообщений – система ежедневно принимает более двух миллиардов запросов на передачу сообщений и обрабатывает их в соответствии с репутацией и частотой обращений запрашивающего сервера.

Анализ данных сообщений – на основе эвристических и постоянно обновляемых алгоритмов система Google оценивает содержание на предмет наличия подозрительных объектов или известных аномалий, включая вложения и файлы ZIP.

Система политик – на основе характера коммуникации система выбирает определенные настройки для конкретного сообщения, помещая его в карантин для просмотра, отказывая в доставке, архивируя или даже шифруя это сообщение.

Распределение – система направляет электронные сообщения в соответствии с правилами, требуемыми политикой. Дополнительно система может приостанавливать передачу сообщений при недоступности принимающего сервера (вследствие технического обслуживания, неожиданной аварии или стихийного бедствия).

Во время всего процесса обработки перед выполнением любых действий запись сообщений на диск не производится (кроме случая архивирования), все необходимые операции выполняются в памяти. Это не только ускоряет доставку сообщений, но и устраняет риски, связанные с несанкционированным доступом к диску.

2. Гибкость

Продукты Google для обеспечения безопасности и соблюдения правил обладают гибкостью, необходимой для удовлетворения конкретных требований и потребностей каждой организации (см. рис. 3). Административный веб-интерфейс позволяет администраторам быстро

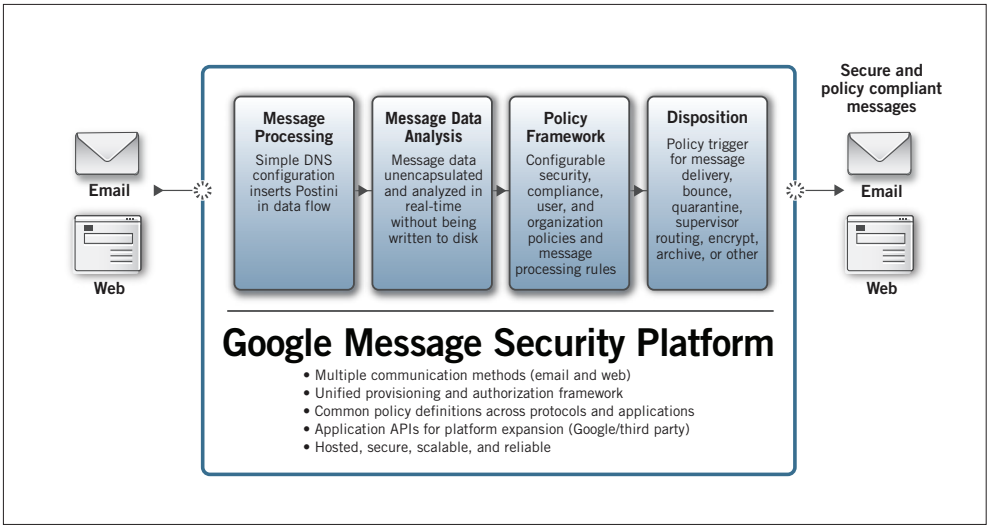

Рисунок 2. Платформа SaaS компании Google предоставляет эффективные продукты для обеспечения безопасности и соблюдения правил.

и просто создавать, изменять и реализовывать политики в соответствии с изменяющимися условиями ведения бизнеса и применяемыми правовыми нормами. Изменения обновляются и распространяются в режиме реального времени, сокращая риски нарушения безопасности или соответствия правилам. При этом политики можно применять централизовано для всех каналов во всей организации, гарантируя согласованное обеспечение безопасности и соблюдения правил.

Другим важным свойством, влияющим на сложность администрирования и управления решением для обеспечения безопасности и соблюдения правил передачи информации, является структуризация и гибкость управления политиками. Другими словами, насколько узкой может быть область применения определенного правила к потоку сообщений? В продуктах Google для обеспечения безопасности и соответствия правилам политики могут быть определены на уровнях пользователя, роли, группы, отдела, подразделения и организации, обеспечивая высокую гибкость структуризации. Платформа предоставляет организациям подробные и настраиваемые наборы правил, которые можно легко изменять в режиме реального времени.

3. Простота развертывания и использования

Созданное на основе платформы решение "по запросу" для обеспечения безопасности и соблюдения правил передачи информации является простым в развертывании и использовании. Благодаря патентованной технологии обработки в режиме реального времени, система выполняет оценку содержания сообщений и вложений незаметно – без записи на диск, которая может стать причиной снижения производительности и создать риск нарушения безопасности – и определяет способы обработки для обеспечения безопасности и соответствия правилам на основе уникальной комбинации интеллектуальной оценки угроз, эвристического анализа, интеллектуальной оценки соединения и бизнес-политик.

Используемый компанией Google уникальный подход, основанный на процессах, выполняемых в режиме реального времени, гарантирует, что задержки в обработке не будут мешать передаче корректных сообщений и что ни одно из сообщений не будет потеряно. Преимущество для пользователей состоит в "прозрачности" платформы, которая обрабатывает и моментально доставляет сообщения, соответствующие требованиям безопасности, с нулевой задержкой. Соединения с IP-адресов, демонстрирующих злонамеренное поведение или распространяющих спам, разъединяются, а сообщения, в которых обнаружен спам, фишинг или вредоносные вирусы, блокируются. Сообщения с подозрительным или несоответствующим правилам содержанием помещаются системой Google в карантин и сохраняются для просмотра пользователем.

4. Низкая общая стоимость владения

Используя платформу Google, организации могут внедрить решение для обеспечения безопасности и соблюдения правил за несколько дней или часов, а не ждать недели или даже месяцы. Не надо выбирать и закупать оборудование, не надо устанавливать программное обеспечение – следовательно, не надо беспокоиться об интеграции с существующей инфраструктурой или о значительных затратах на бригады квалифицированных технических специалистов для развертывания и обслуживания решения. Решение Google "по запросу" для обеспечения

безопасности и соблюдения правил передачи информации характеризуется одним из самых низких уровней эксплуатационных, финансовых и накладных затрат на информационные технологии, обеспечивая быструю окупаемость средств, вложенных клиентами в платформу Postini (см. рис. 4).

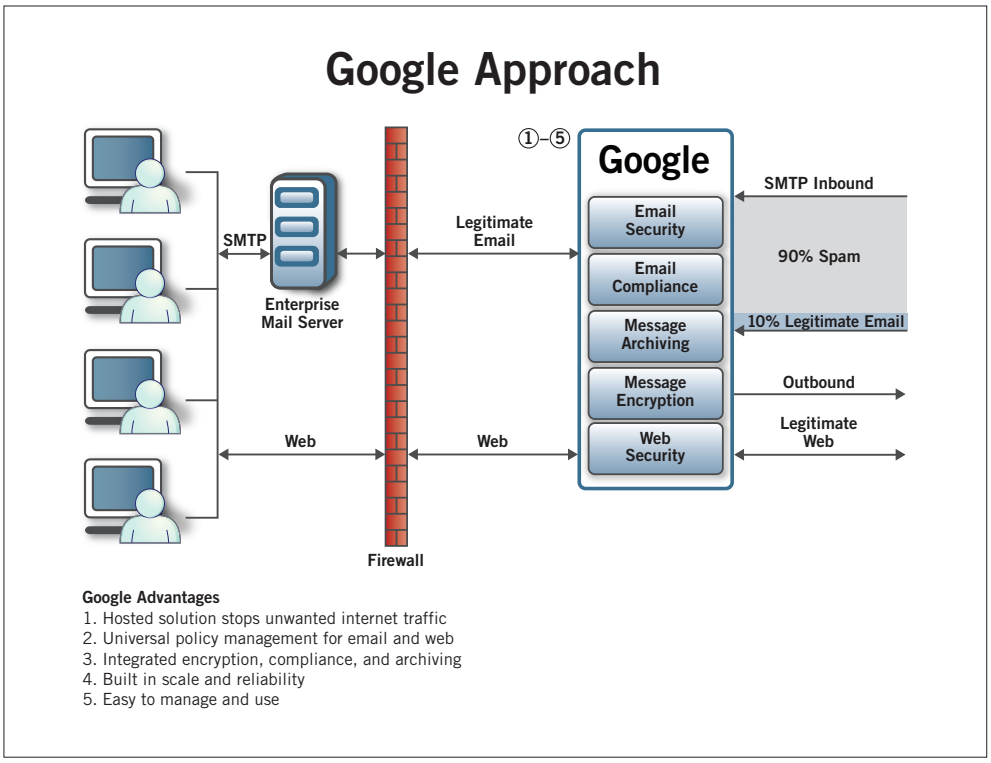

Рисунок 3. Решение "по запросу" компании Google останавливает нежелательный интернет-трафик еще до его прохождения через брандмауэр предприятия.

ПОДРОБНЕЕ

www.google.com/a/security

5. Масштабируемость и надежность

Построенная на основе передовой глобальной инфраструктуры, охватывающей 14 различных вычислительных центров, эффективно и надежно обрабатывающих сообщения, данная сеть служб обеспечивает масштабируемую работу и поддержку, круглосуточно контролируемую на предмет непредвиденных неполадок в системе или угроз. Благодаря глобальной инфраструктуре, сеть служб может легко справиться с дополнительной нагрузкой для клиентов в связи с требованиями роста или временными пиками сетевого трафика, гарантируя, что перегрузка сети или ограничения для соединений не повлияют на продуктивность работы компаний-клиентов.

Сеть обладает не только масштабируемостью, но и высокой надежностью, обеспечивая немедленное переключение на резервный ресурс в случае аварии с гарантированным уровнем обслуживания обработки электронной почты, равным 99,999%. Надежность сети прошла независимую оценку в соответствии с принятой в отрасли практикой. Кроме того, каждый год эксплуатационный персонал сети проводит строгую аудиторскую проверку SAS 70 типа II всех вычислительных центров компании. В настоящее время продукты Google для обеспечения безопасности и соблюдения правил – единственное решение "по запросу", получившее почетный знак WebTrust за соответствие жестким стандартам, определенным в рекомендациях SAS 70.

Заключение

Не все продукты "по запросу" для обеспечения безопасности и соблюдения правил передачи информации равноценны. На самом деле многие из них далеки от соответствия пяти основным критериям, позволяющим клиентам повысить продуктивность своих компаний и ИТ-пользователей, одновременно обеспечивая безопасность и соблюдение правил для всех каналов передачи электронной информации.

Продукты Google для обеспечения безопасности и соблюдения правил передачи сообщений уникальны с точки зрения соответствия пяти критериям эффективной стратегии "по запросу" для обеспечения безопасности и соблюдения правил передачи информации. Предлагая простоту использования, гибкие администрирование и управление, высокую эффективность, низкую общую стоимость владения, а также высокие масштабируемость и надежность, Google помогает своим клиентам не только улучшить производительность своей компании и ИТ-сотрудников, но и повысить доходы от основной деятельности.

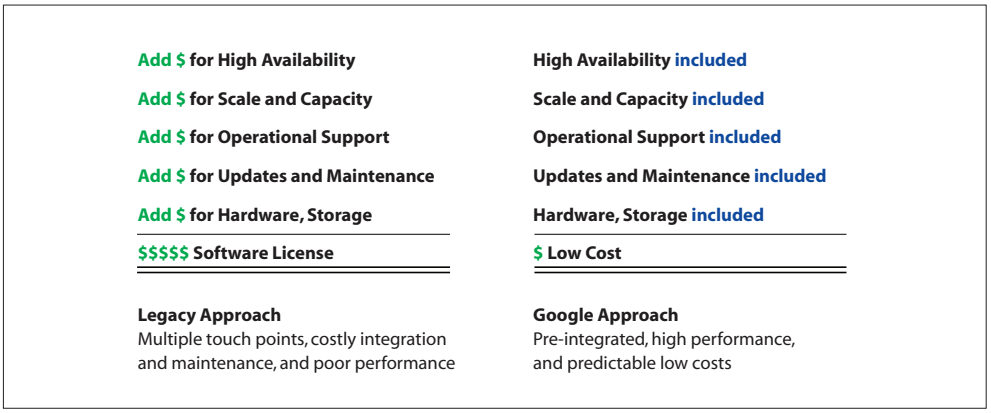

Рисунок 4. Продукты Google отличаются простотой внедрения, масштабируемостью, простотой обслуживания и высокой производительностью при низких затратах.