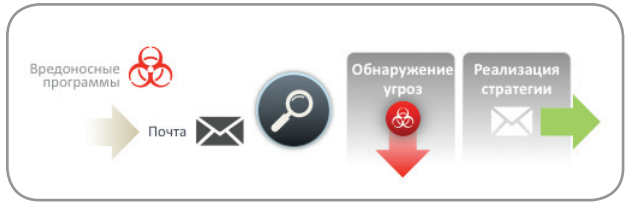
Cisco Email Security

В чем состоит ценность Cisco Email Security?

Электронная почта исключительно важна в современном бизнесе, и задержка с ее доставкой или взлом могут серьезно отразиться на результатах деятельности в целом. В Cisco® Email Security заложены возможности шифрования и система предотвращения потери данных (DLP), основанная на создании стратегий и анализе контента. Благодаря этому компании получают возможность распознавать угрозы и управлять рисками, связанными как с исходящей, так и с входящей почтой, а следовательно, без опасности для себя ускорять бизнес-процессы и создавать более продуктивную среду для пользователей. Это передовое решение, как и все продукты компании Cisco в сфере безопасности, реализуется через облачную службу Cisco Security Intelligence Operations (SIO), призванную отражать угрозы.

Рис. 1. Cisco Email Security: отражение изощренных угроз путем предотвращения потери данных (DLP) и шифрования



Какие проблемы помогает решать Cisco Email Security?

С одной стороны, электронная почта жизненно необходима для ведения бизнеса; с другой стороны, из-за нее на организацию постоянно обрушивается поток стремительно меняющихся и усложняющихся угроз, например целенаправленные атаки (в том числе направленный фишинг и изощренные APT-атаки). Системы электронной почты с трудом справляются с новой архитектурой, проблемами информационной безопасности и такими мобильными тенденциями, как использование личных устройств на рабочем месте. Поэтому исходящий трафик организации все чаще становится ее слабым местом из-за сложностей с обеспечением следования стратегиям использования электронной почты на смартфонах и прочих личных мобильных устройствах.

Благодаря Cisco Email Security организация получает простой, но в то же время мощный инструмент для постоянного отслеживания угроз, осуществления политики допустимого использования и предотвращения потери данных (DLP). Cisco Email Security реализуется в нескольких форм-факторах, начиная от отдельных устройств и заканчивая облачной технологией, и обеспечивает безопасность мобильных пользователей, пользователей личных устройств на рабочем месте и пользователей, подключенных по IP версии 6. Благодаря этому Cisco Email Security помогает организациям предвосхищать изменения на рынке и дает им гибкость, необходимую для защиты пользователей, вне зависимости от того, где они находятся и как просматривают свою электроную почту.

Лучшая система обеспечения безопасности входящей и исходящей почты

В основе Cisco Email Security лежит та же самая технология, которая защищает более 20% крупнейших предприятий мира, восемь из 10 крупнейших интернет-провайдеров и 50% компаний, входящих в список Fortune 1000. Независимо от метода развертывания, Cisco Email Security предлагает не имеющую аналогов защиту от угроз, содержащихся как во входящем, так и в исходящем трафике.

Не имеющая аналогов защита от вредоносных программ

Cisco Email Security использует информацию, собранную службой Cisco SIO, которая просматривает 35% мирового трафика электронной почты и 75 Тб интернет-данных в день.

Рис. 2. Архитектура отражения атак нулевого дня с помощью Cisco Security Intelligence Operations

В Cisco Email Security используются фильтры Cisco Outbreak Filters – инновационное решение, обеспечивающее защиту электронной почты от трудно распознаваемых угроз нового поколения. Компания Cisco предлагает первый в отрасли специально разработанный механизм блокирования целенаправленных атак, в котором используются три основных элемента: эвристика целенаправленных атак, динамический карантин и облачное сетевое перенаправление.

Фильтры Cisco Outbreak Filters сканируют URL-ссылки, вставленные в электронную почту, еще до того, как она попадает к пользователю, таким образом снижая ущерб от инфицированных ссылок. Cisco Outbreak Filters эффективно предотвращают заражение тогда, когда новая угроза уже возникла, но подписи вредоносных программ пока не выявлены, что ограждает организацию от потенциальных потерь и уничтожения данных.

В рамках Cisco Email Security предлагается целый ряд модулей, разработанных компаниями Sophos, McAfee и Cloudmark для поиска и удаления вредоносных программ и спама. Для повышения защиты от вредоносных программ администраторы могут запускать все эти модули сканирования, причем практически без потерь для производительности системы.

Гибкость развертывания: от устройства до облачной технологии

Для организаций, которые не могут себе позволить физически хранить конфиденциальную информацию вне своих стен и для которых особенно актуален вопрос о сохранении производительности систем, компания Cisco предлагает специализированные, простые в управлении устройства Cisco Email Security Appliances, которые легко подобрать согласно размеру организации и интегрировать в вашу среду.

Таблица 1. Устройства компании Cisco, подобранные согласно нужному вам размеру

Модели	Cisco X1070	Cisco C670	Cisco C370	Cisco C170
Число пользователей (почтовых ящиков)*	<20 000	10 000+	<10 000	<2000
Кластеризация	Да	Да	Да	Да

*Для определения соответствующей численности обратитесь к специалисту компании Cisco по обеспечению безопасности контента. Он поможет вам учесть пиковые потоки почты и средний объем одного сообщения, чтобы выбранное решение соответствовало вашим текущим и будущим потребностям.

Для организаций, которые хотели бы сократить объем сохраняемых данных, и общую стоимость владения, компания Cisco предлагает облачную инфраструктуру с гибкой моделью развертывания - для обеспечения безопасности электронной почты в любое время и в любом месте. Облачная инфраструктура компании Cisco выстроена на основе бесперебойно работающих, высокопроизводительных центров обработки данных, расположенных по всему миру. Такая инфраструктура уже продемонстрировала свою надежность и способность обеспечивать безопасность и доступ к данным без необходимости использования оборудования, установленного у клиента.

Обеспечение безопасности в соответствии с вашими нуждами

Cisco Email Security – комплексное решение для всесторонней защиты от угроз, включая шифрование и высокоточное предотвращение потери данных (DLP); оно реализуется в нескольких форм-факторах и позволяет управлять входящей и исходящей почтой предприятия, а также формировать отчеты по ней. В Cisco Email Security, наряду с передовыми, высокоэффективными методами поиска вирусов, применяются также традиционные методы борьбы со спамом и инновационные контекстно-зависимые технологии обнаружения всего многообразия известных и новых угроз, связанных с электронной почтой.

Таблица 2. Гибкие варианты подписки на программное обеспечение для защиты входящей и исходящей почты

Варианты подписки на программное обеспечение	Описание
Cisco Email Security Inbound	Защита почтовых ящиков организации от спама, вирусов и целенаправленных атак. **(Outbreak Filters + Antivirus + Antispam)**
Cisco Email Security Outbound	Простые в использовании решения в области шифрования и предотвращения потери данных (DLP) для обеспечения информационной безопасности. **(Data Loss Prevention + Encryption)**
Cisco Email Security Premium	Сочетание защиты входящей и исходящей электронной почты, обеспечивающее ее полную безопасность. **(Inbound + Outbound)**

Cisco Email Security дает организации возможность без опасений ускорять свои бизнес-процессы и создавать более продуктивную среду для пользователей. Общение между пользователями происходит быстрее, а обмен информацией – безопаснее, что благоприятствует сотрудничеству и инновациям.

Как по максимуму использовать возможности вашей сети Cisco

Лучший способ повысить отдачу от инвестиций в оборудование Cisco для центров обработки данных, сетей и филиалов – сделать безопасность составным элементом сетевой архитектуры. Если электронная почта стала неотъемлемой частью вашей деятельности, необходимо гарантировать ее безопасность. Cisco Email Security – эта лучшая в своем классе защита от самых разных угроз, встречающихся в электронной почте. Консалтинговая компания Gartner в своем докладе поместила компанию Cisco в число лидеров в категории Secure Email Gateway.

Почему Cisco?

Сегодня проблема безопасности сетей стоит так остро, как никогда ранее. В обстановке постоянных угроз и рисков обеспечение безопасности необходимо для бесперебойного ведения бизнеса, защиты ценной информации, поддержания репутации бренда и внедрения новых технологий. Безопасная сеть – залог мобильности ваших сотрудников и их защищенного доступа к нужной им информации. Это также облегчает ведение бизнеса с клиентами и партнерами.

Никакая другая организация не понимает проблему сетевой безопасности так хорошо, как компания Cisco. Наше лидерство на рынке, наш многолетний опыт работы и непревзойденная компетентность в сфере предотвращения угроз и защиты от них делают нас именно тем поставщиком инновационных решений для обеспечения безопасности, который вам нужен.

Где можно получить дополнительную информацию?

Лучший способ разобраться в преимуществах продуктов Cisco Email Security – это участие в программе испытаний перед покупкой (Try and Buy). Для получения оценки полнофункционального решения, которое вы сможете на протяжении 30 дней бесплатно тестировать в своей сети, перейдите по адресу: http://www.cisco.com/go/esa.

Cisco Email Security: наиболее часто задаваемые вопросы

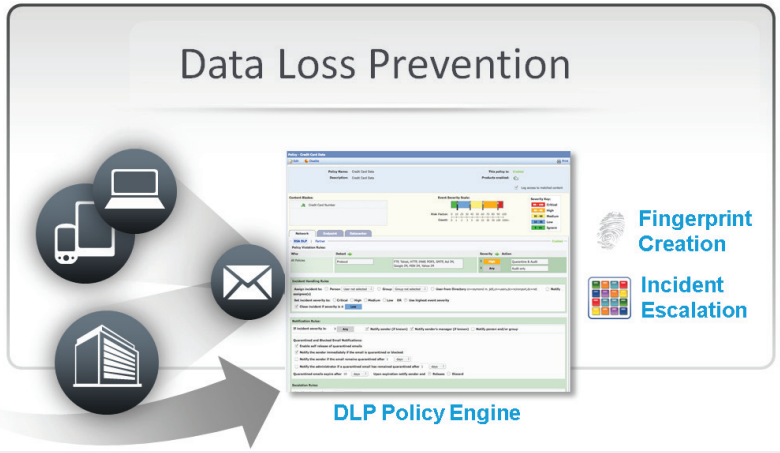
В. Доступны ли в Cisco Email Security функции формирования отчетов и отслеживания сообщений?

О. Да. На устройствах Cisco Content Security Management Appliance централизованно формируются отчеты и собираются данные о выполнении, благодаря чему можно отслеживать сообщения через единый интерфейс управления устройствами обеспечения безопасности электронной почты и сетевой безопасности.

В. Как устроена система предотвращения потери данных (DLP)?

О. DLP-фильтры упрощают применение стратегии управления информацией в исходящей электронной почте, делая ее частью общей DLP-архитектуры, разработанной компанией RSA. Компания Cisco в сотрудничестве с такими партнерами, как RSA, работает над созданием ведущей DLP-экосистемы, которая установит общую для разных предприятий классификацию и платформу управления стратегиями. С 2009 года компания Cisco внедряет в свои продукты для обеспечения безопасности электронной почты технологию предотвращения потери данных (DLP), разработанную компанией RSA. Предлагаемое в результате решение представляет собой комплекс всесторонних защитных мер, соответствует требованиям регулирующих органов по всему миру и обладает высочайшей в своем классе точностью при выборе мер для защиты любых данных (включая универсальное шифрование сообщений).

Рис. 3. Последовательное внедрение политики предотвращения потери данных (DLP) в электронной почте



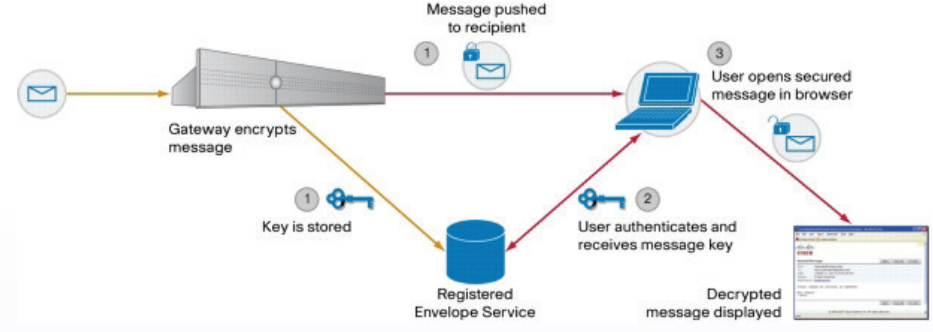
В. Как устроена служба Cisco Registered Envelope Service?

О. Служба зарегистрированных цифровых конвертов (Cisco Registered Envelope Service, CRES) помогает компаниям обезопасить свою электронную почту. Эта служба позволяет организациям отправлять зашифрованные сообщения в зарегистрированных «конвертах» — зашифрованных электронных сообщениях, которые также могут быть защищены паролем.

В. Как работает технология Cisco Business-Class Email?

О. Business-Class Email — это бесплатное мобильное приложение, которое клиент может загрузить на свой смартфон и пользоваться через него пакетом Cisco Email Security Outbound с услугами шифрования. Клиентам обеспечивается межабонентское шифрование вплоть до папки входящих сообщений на их мобильных телефонах. Благодаря Cisco Business-Class Email пользователи без малейших сложностей отправляют и получают защищенные сообщения, не сталкиваясь ни с проблемами шифрования, ни с проблемами управления ключами. Кроме того, отправитель получает дополнительные рычаги управления своими сообщениями, в частности: уведомление о прочтении сообщения, отзыв сообщения, настройка срока действия сообщения, настройки возможности ответа на сообщение или его дальнейшей пересылки.

Рис. 4. Схема работы Cisco Encryption Business-Class Email



C45-715283-00 09/12