IRONPORT

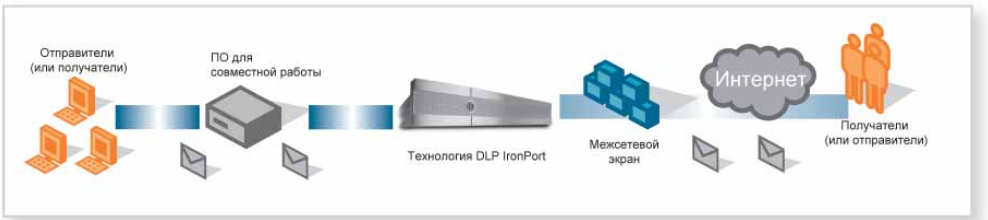
Технология предотвращения утечки данных (DLP)

ИНТЕГРИРОВАННЫЕ ВОЗМОЖНОСТИ DLP ПО СКАНИРОВАНИЮ И ОТРАЖЕНИЮ УГРОЗ ДЛЯ ОРГАНИЗАЦИЙ ЛЮБОГО МАСШТАБА

ОБЩИЕ СВЕДЕНИЯ

Электронная почта стала основным способом связи для организаций любого масштаба. Преднамеренная или случайная утечка конфиденциальной информации может иметь серьезные последствия: нарушение нормативных требований, подрыв доверия клиентов и потеря репутации и ценности бренда. Как следствие, руководители больше чем когда-либо заинтересованы в быстром развертывании решений по защите данных, которое было бы простым в управлении незаметным.

Специалисты компании IronPort® Systems, являющейся лидером в обеспечении безопасности эдектронной почты и Web-трафика, понимают сложность создания решений, предназначенных для одного из самых значительных направлений потери данных: электронных коммуникаций. Технология предотвращения утечки данных IronPort предоставляет корпоративным ИТ-отделам единое, полностью интегрированное решение, которое сочетает традиционные функции защиты электронной почты (например, фильтрация спама и вирусов) с корпоративными функциями, такими как создание политик, сканирование содержимого, шифрование, помещение в карантин и архивирование.



Упрощение процесса предотвращения утечки данных. Компании по всему миру все больше осознают необходимость защиты важных данных. Тогда как для существующих DLP решений требуются дополнительные аппаратные средства и новое программное обеспечение, используемые для настройки решений по мониторингу, заказчики компании IronPort могут добавить возможности DLP простым щелчком мыши. Решение IronPort содержит все компоненты, необходимые ИТ-отделу предприятия для безотлагательного внедрения технологии предотвращения утечки данных.

ИНТЕГРИРОВАННОЕ СКАНИРОВАНИЕ

Из словарей нормативных требований (Compliance Dictionaries) заказчики могут узнать о нормах и стандартах, таких как PCI, HIPAA, GLB, SOX и других. В словарях соответствий IronPort администраторы могут найти предварительно заданный набор ключевых слов и строк, упрощающий защиту от нарушений нормативных требований, предъявляемых к исходящим данным.

«Электронная почта стала фактически системой хранения почти всей корпоративной информации, поэтому защита исходящего потока сообщений приобрела еще более важное значение».

— Брайан Берк (Brian Burke), руководитель отдела исследований продуктов безопасности компании IDC

ИНТЕГРИРОВАННОЕ СКАНИРОВАНИЕ (ПРОДОЛЖЕНИЕ)

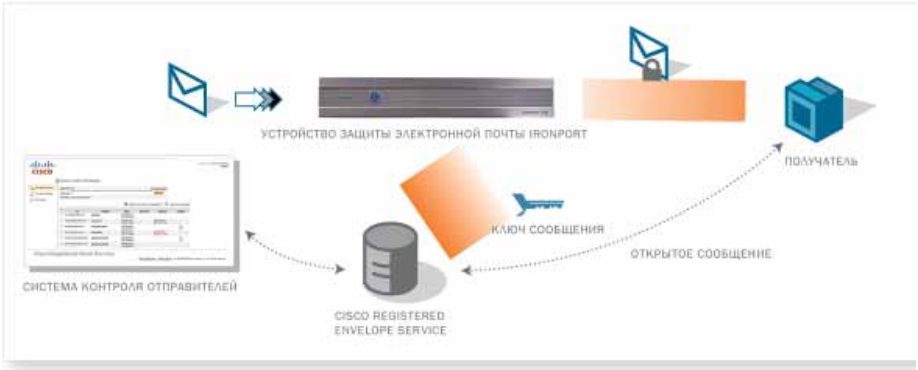
Интеллектуальные идентификаторы (Smart Identifiers) предоставляют администраторам простой способ настройки и поиска шаблонов и строк с важной информацией, которые нарушают требования политик безопасности. Используя удобный и эргономичный интерфейс администраторы могут настроить фильтры для поиска следующей информации:

- номеров кредитных карт,
- номеров карт социального страхования,
- банковских маршрутных номеров ABA,
- номеров ценных бумаг (CUSIP).

Фильтры содержимого и механизм сканирования вложений облегчают создание политик, которые являются уникальными для вашей организации. Механизм сканирования IronPort может обрабатывать более 390 различных типов вложений и производить фильтрацию содержимого для обеспечения соблюдения политик DLP.

ИНТЕГРИРОВАННАЯ ЗАЩИТА

Шифрование является основой эффективного решения DLP. Автоматическое шифрование необходимо как вариант исправления в ситуации, когда информация должна быть передана за пределы организации. При шифровании используется технология IronPort PXE ™, интегрированная непосредственно в устройство IronPort.

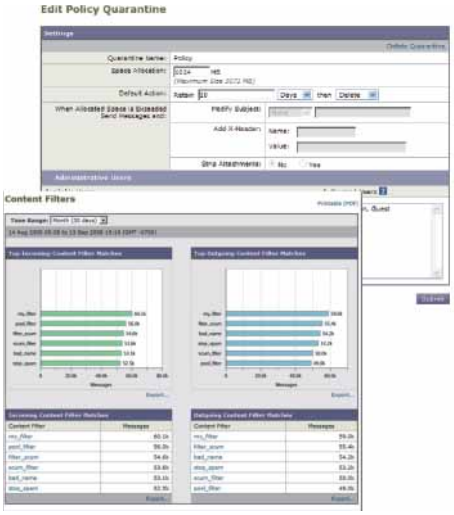


Шифрование в действии: Используя службу Cisco Registered Envelope Service™ (CRES), устройства защиты электронной почты IronPort зашифровывают и расшифровывают сообщения, обеспечивая низкую совокупную стоимость владения и высочайшую доступность сервиса.

Теперь входящая и исходящая почта может быть зашифрована и расшифрована без использования каких-либо дополнительных аппаратных средств, необходимых для безопасной фильтрации, маршрутизации и доставки сообщений. Исходящие сообщения обнаруживаются и автоматически зашифровываются устройством в соответствии с политиками безопасности компании.

ИНТЕГРИРОВАННАЯ ЗАЩИТА

Карантин. Сообщения электронной почты, которые помечены механизмом сканирования содержимого, помещаются в карантин и могут быть просмотрены через web-интерфейс. Для соответствия уникальным политикам организации и нормативным требованиям можно создать несколько управляемых карантинов.



Отчетность по соблюдению нормативных требований позволяет организациям увидеть эффективность их политик DLP. Механизм предоставления отчетности обеспечивает просмотр сработавших правил DLP и сводную ведомость нарушителей политик в реальном времени. Кроме того, создаются отчеты по конкретным пользователям для идентификации, возможного обучения и процесса исправления.

ВАРИАНТЫ РАЗВЕРТЫВАНИЯ

Технология предотвращения утечки данных IronPort полностью интегрирована в следующие устройства:

- устройства *IronPort C-Series*™
- устройства *IronPort X-Series*™
- устройства *IronPort Encryption Appliance*™

РЕЗЮМЕ

Решения IronPort обеспечивают высокопроизводительноое, комплексное предотвращение утечки передаваемых данных, помогая небольшим и крупным предприятиям избегать кражи информации, соблюдать нормативные требования и защищать свой бренд и репутацию. Компания IronPort считает, что всеобъемлющее решение по мониторингу и предотвращению утечки данных во всех каналах связи имеет жизненно важное значение для обеспечения целостности политик организации. Благодаря лидирующей позиции на рынке продуктов защиты от интернет-угроз, а также партнерским отношениям с ведущими в отрасли поставщиками решений DLP, компания IronPort располагает уникальной возможностью, предлагая предприятиям единое решение с массой преимуществ.

КОНТАКТЫ

НАЧАЛО РАБОТЫ С КОМПАНИЕЙ IRONPORT

Продукция IronPort сделает вашу инфраструктуру безопасной, надежной и легко управляемой. Убедиться в ее ценности вам помогут торговые представители, деловые партнеры и специалисты по технической поддержке компании IronPort. Если вы считаете, что лучшие в отрасли продукты IronPort могут принести пользу вашей организации, отправьте сообщение по адресу security-request@cisco.com.

Cisco
Москва, 115054, бизнес-центр "Риверсайд-Тауэрс",
Космодамианская наб., 52, стр. 1, 4-й этаж
ТЕЛ.:+ 7 (495) 961-14-10 ФАКС: + 7 (495) 961-14-69
EMAIL: security-request@cisco.com WEB: www.cisco.ru

ООО "Хедтехнолоджи РУ"
Москва, 105066,
ул. Ольховская 45, стр. 1, оф. 12
ТЕЛ.: + 7 (499) 267-66-10 ФАКС: + 7 (499) 263-05-75
EMAIL: info@headtechnology.ru WEB: www.headtechnology.ru

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

IronPort is now part of Cisco.