

Защита от внутренних и внешних угроз информационной безопасности с помощью InfoWatch Traffic Monitor и Blue Coat ProxySG

При построении систем защиты информационных активов компании важно сочетать традиционно-актуальные средства защиты от внешних угроз и технологии, позволяющие контролировать распространение конфиденциальных данных. Последняя задача сегодня становится все более актуальной, так как ее решение не только минимизирует риски, которые возникают в связи с умышленной или случайной утечкой информации, но и позволяет государственным и частным компаниям и организациям соответствовать требованиям федерального закона № 152-ФЗ «О персональных данных»

Комплексное решение для обеспечения информационной безопасности

Чтобы обеспечить безопасность информационных активов бизнеса от внешних и внутренних угроз, компании InfoWatch и Blue Coat представляют совместное решение – InfoWatch Traffic Monitor и Blue Coat ProxySG.

Решение включает в себя средства мониторинга и фильтрации данных, передаваемых за пределы компании по электронной почте, через веб или интернет-пейджеры, печать или сменные носители и позволяет контролировать зашифрованный HTTPS-канал как на наличие вредоносного программного обеспечения в зашифрованных данных, так и на предмет передачи по такому каналу конфиденциальной информации.

Независимо от того, какого рода конфиденциальную информацию (технологическая информация или персональные данные, номера телефонов или кредитных карт и т.п.) нужно защитить, совместное решение InfoWatch и Blue Coat эффективно пресекает любые несанкционированные действия как со стороны сотрудников компании, так и со стороны внешних злоумышленников.

Таким образом, совместное решение успешно противодействует всем внешним и внутренним угрозам информационной безопасности в режиме реального времени.



Схема работы решения

Внешние и внутренние угрозы информационной безопасности

Информационные активы компании подвергаются постоянной угрозе, как извне, так и изнутри. К традиционным внешним угрозам относятся вирусы, шпионские программы, DoS-атаки и др. Под внутренними угрозами понимаются случайные или намеренные утечки конфиденциальных корпоративных данных.

Преимущества комплексного решения

- мониторинг и анализ данных, отсылаемых за пределы компании, в том числе с использованием https-протокола
- анализ SSL трафика (HTTPS, SSL, TLS)
- предотвращение утечки данных благодаря блокировке процесса передачи конфиденциальной информации в случае обнаружения ее несанкционированного использования
- защита от уязвимостей WEB 2.0
- анализ HTML кода на наличие вредоносных скриптов и уязвимостей в web-страницах, web почте и теле электронных сообщений
- фильтрация URL в соответствии с категориями, заданным контентом и типами файлов
- централизованное хранение всех перехваченных данных для обеспечения доказательной базы при расследовании инцидентов в области информационной безопасности (ИБ)
- ретроспективный анализ для расследований нарушений политик ИБ (forensics)
- гибкая система построения отчетов
- соответствие требованиям регулирующих органов и стандартов информационной безопасности, в том числе PCI DSS, Basel II, SOX (Sarbanes-Oxley), Федерального закона «О персональных данных» № 152-ФЗ
- сертификация ФСТЭК

Компоненты решения

Совместное решение InfoWatch и Blue Coat включает в себя систему защиты конфиденциальной информации InfoWatch Traffic Monitor, которая осуществляет:

- мониторинг и анализ данных, отсылаемых пользователями за пределы компании,
- предотвращение утечки данных путем блокирования процесса передачи при обнаружении нарушения политики безопасности (например, пересылка конфиденциальных данных пользователем, не уполномоченным на их распространение),
- хранение и анализ всех перехваченных данных и информации об инцидентах для проведения расследований по нарушениям политик информационной безопасности.

Многоуровневая защита входящих и исходящих данных от шпионских и вредоносных программ, вирусов, троянских программ, фишинга и т.п. осуществляется благодаря аппаратному решению Blue Coat ProxySG.

Blue Coat ProxySG позволяет управлять Web-приложениями и трафиком, создавая правила использования интернет в соответствии с корпоративной политикой безопасности. Использование интерфейса ICAP (Internet Content Adaptation Protocol) позволяет глубоко анализировать содержимое информационных потоков передаваемых в Интернет, не нарушая при этом требований регулирующих органов.

Функциональные возможности

Комплексный контроль зашифрованного трафика

Совместное решение InfoWatch Traffic Monitor и Blue Coat ProxySG позволяет контролировать защищенный HTTPS-канал как на предмет обнаружения вредоносного ПО в зашифрованном трафике, так и на предмет передачи по такому каналу конфиденциальной информации.

Многоуровневая система анализа

Различные технологии анализа и обнаружения утечек обладают разной эффективностью в зависимости от характера данных. Поэтому надежную защиту конфиденциальной информации может обеспечить только комплексное использование подобных технологий. Совместное решение InfoWatch и Blue Coat применяет несколько технологий контентного анализа для более точного детектирования конфиденциальной информации:

- Лингвистический анализ – автоматическое определение тематики текста на основании ключевых терминов.
- Анализатор шаблонов – поиск сложных алфавитно-цифровых объектов, как, например, номера паспортов и кредитных карт, и т.п.
- Цифровые отпечатки – определение степени схожести анализируемых документов с заранее заданными документами-образцами.

Подобный комплексный подход позволяет обнаруживать несанкционированное использование конфиденциальной корпоративной информации на любом этапе ее жизненного цикла, в том числе и сразу после ее создания, когда еще не существует никаких родственных или похожих документов. Результатом анализа является категоризация передаваемой за пределы компании информации и применение соответствующих политик безопасности.

Единая система настройки

InfoWatch Traffic Monitor позволяет централизованно осуществлять настройку всех компонентов решения и определять политики обработки данных из различных каналов. Решение поставляется с набором предустановленных настроек, что позволяет ввести его в эксплуатацию сразу же после подключения.

Соблюдение требований законодательства в отношении персональной информации

При обнаружении утечки данных, администратору системы безопасности предоставляется подробная информация о происшествии и самих данных, но без прямого доступа к ним. Благодаря этому не нарушается требование законов о защите прав сотрудников на тайну переписки.

Ретроспективный анализ и формирование доказательной базы

Все проанализированные данные помещаются в единое хранилище, что обеспечивает возможность построения полной картины использования критической информации и оптимизации политик работы с ней. Благодаря функции полнотекстового поиска, решение позволяет, в случае необходимости, формировать доказательную базу и проводить расследование инцидентов, связанных с нарушением информационной безопасности.

Контакты:

тел.: +7 495 22 900 22
Российская Федерация, 123458, Москва, проезд №607, дом 30, офис 507

www.infowatch.ru
sales@infowatch.ru