Надежная защита от внутренних и внешних угроз с помощью InfoWatch Traffic Monitor и Aladdin eSafe

Активное использование зашифрованных протоколов для передачи данных в Интернет (например, в системах онлайн платежей или в системах обмена сообщениями, таких как Google Talk) представляет серьезную угрозу информационной безопасности компаний. Анализ зашифрованных данных на предмет утечки данных или наличия в нем вредоносного ПО не возможен ни с помощью системы защиты от вторжений, ни межсетевого экрана, ни антивирусной системы, ни системы мониторинга трафика.

Комплексное решение для обеспечения информационной безопасности

Чтобы обеспечить полноценную информационную безопасность и гарантировать контроль, в том числе и за данными, отправляемыми с использованием зашифрованного протокола, компании InfoWatch и Aladdin представляют совместное решение – InfoWatch Traffic Monitor Enterprise и Aladdin eSafe Web Security Gateway SSL.

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 Aladdin 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.

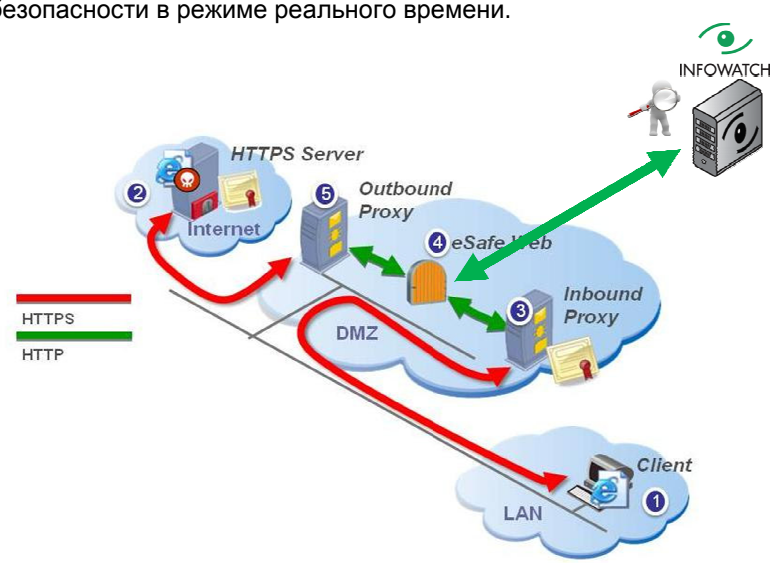

Схема работы решения

Преимущества совместного решения

- мониторинг и анализ данных, отсылаемых пользователями за пределы компании, включая web-почту, в том числе отправляемую с использованием https-протокола;
- анализ зашифрованного трафика (HTTPS, SSL, TLS);
- предотвращение утечки данных благодаря блокировке процесса передачи конфиденциальной информации в случае обнаружения ее несанкционированного использования;
- фильтрация активности и блокирование по сигнатурам интернет-приложений (шпионских программ, Интернет-пейджеров (IM);
- удобные политики управления цифровыми сертификатами;
- анализ HTML кода на наличие вредоносных скриптов и уязвимостей в Web-страницах, web почте и теле электронных сообщений;
- фильтрация URL в соответствии с категориями (70 категорий, 95 миллионов сайтов, 3 миллиарда индексированных страниц, 150000 обновлений ежедневно), заданным контентом, типами файлов;
- централизованное хранение данных, перехваченных по любому из каналов, для обеспечения доказательной базы при расследовании инцидентов в области ИБ;
- ретроспективный анализ для расследований по нарушениям политик информационной безопасности (forensics);
- гибкая система построения отчетов;
- обеспечение соответствия 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 и CheckMark Certified.

Компоненты решения

Совместное решение InfoWatch и Aladdin 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.

Устанавливаемое на интернет-шлюзе программное решение Aladdin eSafe Web Security Gateway SSL обеспечивает проверку данных, передаваемых по протоколам HTTPS, SSL, TLS на наличие вредоносного кода с возможностью его блокирования.

Функциональные возможности

Комплексный контроль шифрованного трафика

Совместное решение InfoWatch и Aladdin позволяет перехватывать любые данные, передаваемые по зашифрованному каналу HTTPS – сообщения веб-почты, форумов, чатов и т. д.

Многоуровневая система анализа

Различные технологии анализа и обнаружения утечки данных обладают разной эффективностью в зависимости от их характера. Надежную защиту конфиденциальной информации может обеспечить только комплексное использование подобных технологий. Совместное решение InfoWatch Traffic Monitor Enterprise и Aladdin eSafe 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 Enterprise 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