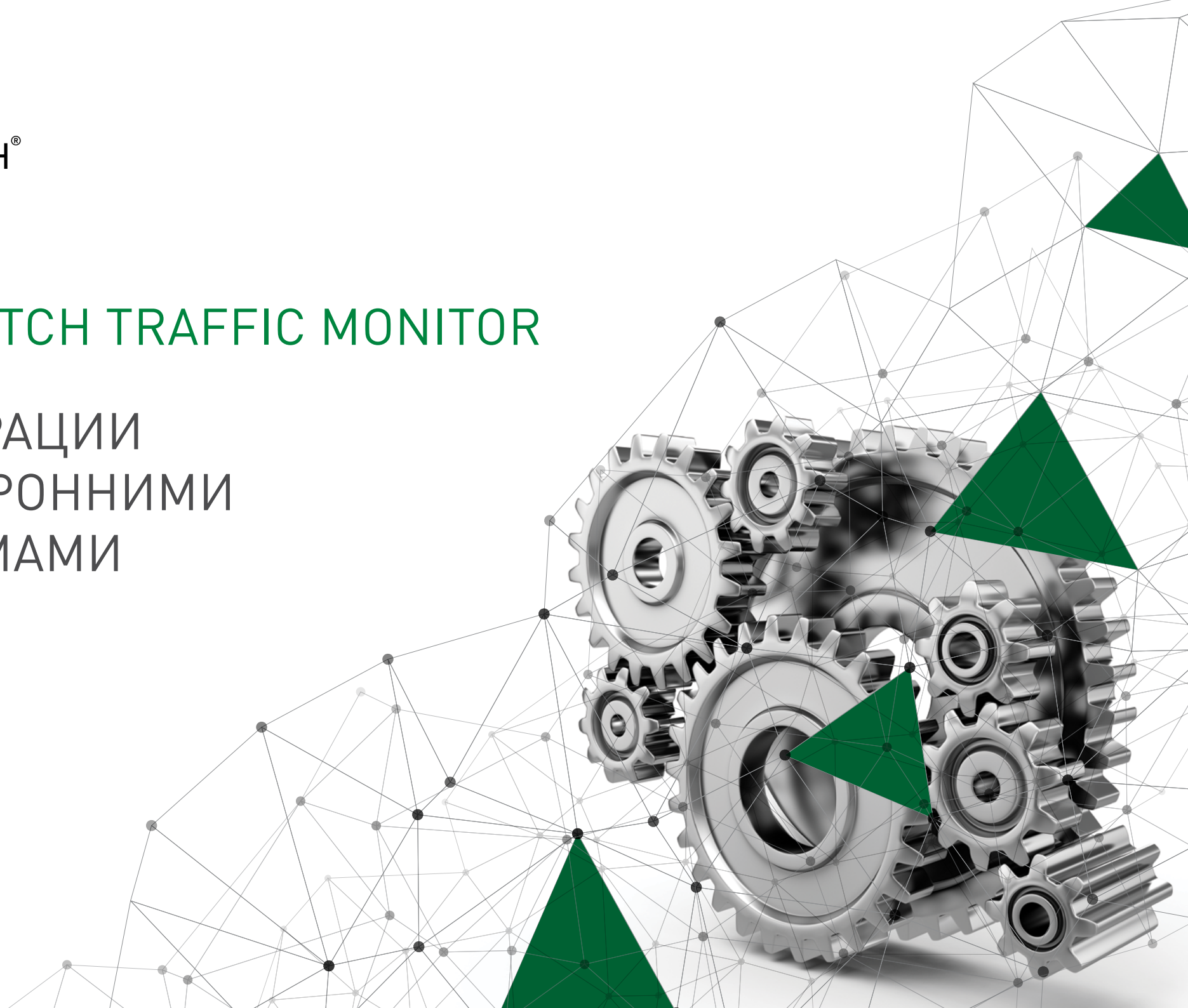
INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

INFOWATCH TRAFFIC MONITOR

ИНТЕГРАЦИИ СО СТОРОННИМИ СИСТЕМАМИ



Защита данных бизнес-приложений

Сегодня компании существуют в разнообразных рабочих средах: каждое бизнес-приложение решает свои задачи и генерирует большие объемы данных. Чаще всего выгрузки из этих систем никем и никак не контролируются, что неизбежно приводит к потере конфиденциальных данных и другой важной информации.

Возможности продукта

InfoWatch Traffic Monitor, наряду с бизнес-системами, выступает полноценным звеном корпоративной сети. Решение синхронизируется со сторонними корпоративными приложениями (ERP, CRM и др.), извлекает из них информацию и подвергает ее глубокому анализу, применяя весь спектр технологий анализа и политик. Данные из бизнес-систем автоматически попадают в ***InfoWatch Traffic Monitor***, благодаря чему решение защищает самые актуальные данные. Даже несмотря на то, что в CRM-систему менеджеры ежедневно вносят новых клиентов, ***InfoWatch Traffic Monitor*** будет защищать самую актуальную базу данных, с учетом всех обновлений.

Решаемые задачи

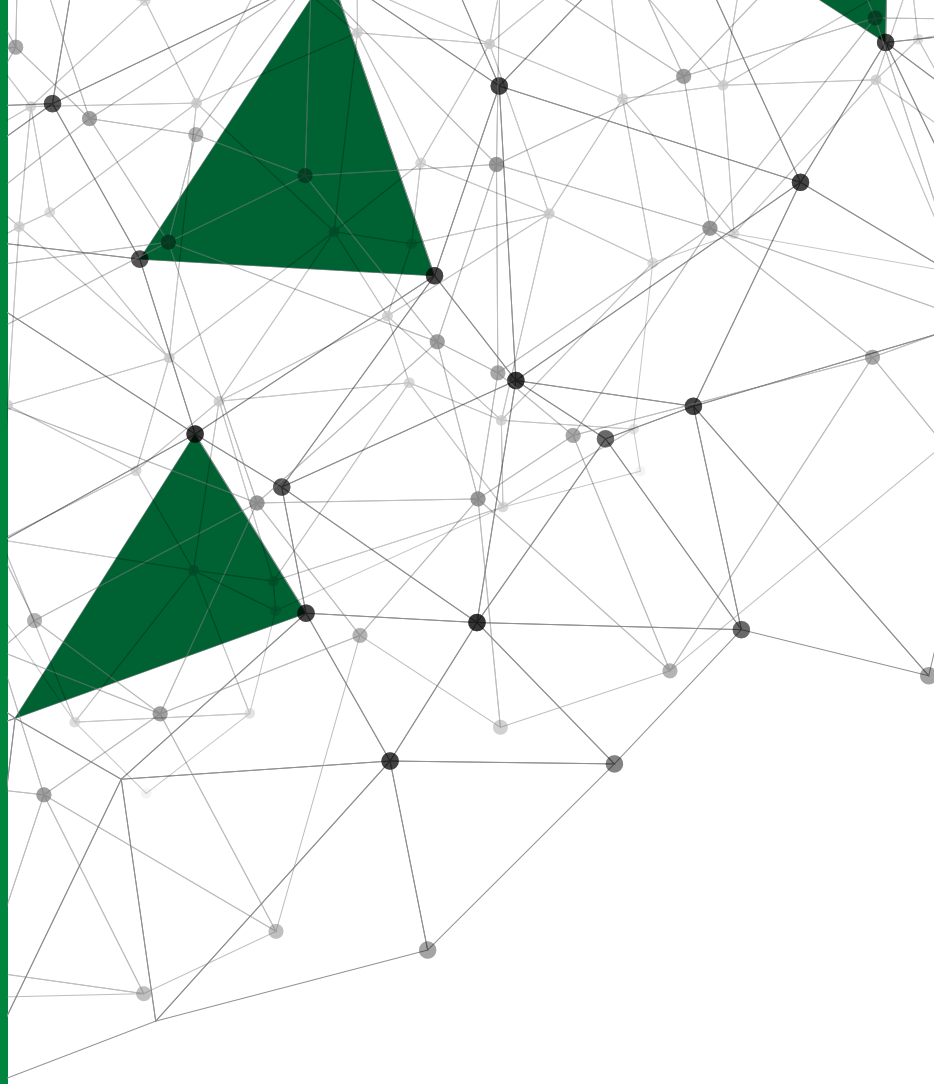
- Комплексный подход к борьбе с внутренними угрозами: никакие данные не остаются без внимания DLP-системы
- Удобное расследование инцидентов: все события аккумулируются в одном месте и хранятся в едином архиве
- Благодаря API заказчик сам определяет, данные каких систем попадут в InfoWatch Traffic Monitor для анализа

Варианты реализации

- Выгрузки событий из баз данных InfoWatch Traffic Monitor в SIEM-систему
- Загрузка событий из сторонних систем в InfoWatch Traffic Monitor
- Загрузка эталонных документов из сторонних систем в InfoWatch Traffic Monitor
- Перехват HTTP и HTTPS-трафика по ICAP

Преимущества совместной интеграции

- Гибкая интеграция в ИТ-инфраструктуру заказчика
- Расширение возможностей по контролю периметра
- Удобное проведение расследований инцидентов информационной безопасности
- Единый центр управления информационной безопасностью компании
- Минимизация финансовых, репутационных, операционных и других рисков



Интеграция с решениями класса SIEM

InfoWatch Traffic Monitor обладает возможностью интеграции с SIEM-системами, позволяя дополнить аналитику решений класса SIEM данными, полученными при перехвате информационных потоков по всем каналам передачи информации.

Совместное решение оперативно выявит инциденты и корректно на них отреагирует, тем самым повышая эффективность работы службы информационной безопасности. InfoWatch Traffic Monitor интегрируется с популярными на российском рынке SIEM-системами – HP ArcSight и Positive Technologies MaxPatrol.

Информация, которую InfoWatch Traffic Monitor передает в SIEM

- Инциденты, зарегистрированные InfoWatch Traffic Monitor
- Действия офицера безопасности в консоли InfoWatch Traffic Monitor
- Данные о сотрудниках, пытающихся получить доступ к системе, серверу и базе данных InfoWatch Traffic Monitor
- Состояние серверов и служб InfoWatch Traffic Monitor

Возможности интеграции

- Быстрая обработка инцидентов, планирование реакции на инцидент и корреляция действий с учетом других событий ИБ
- Предотвращение несанкционированного изменения политик и правил привилегированными сотрудниками
- Предотвращение нелегитимного доступа к DLP-системе и данным, хранящимся в архиве
- Мониторинг работоспособности DLP-системы и предотвращение случайного или преднамеренного выведения ее из строя

Разбор инцидентов при интеграции InfoWatch Traffic Monitor и Positive Technologies MaxPatrol SIEM

1. ***Active Directory сообщает Positive Technologies MaxPatrol SIEM:*** подбор пароля в учетную запись Windows, который является администратором DLP-системы
2. ***InfoWatch Traffic Monitor сообщает Positive Technologies MaxPatrol SIEM:*** добавление администраторских прав пользователю
3. ***InfoWatch Traffic Monitor сообщает Positive Technologies MaxPatrol SIEM:*** отключение DLP-системы пользователем, ставшим администратором
4. ***InfoWatch Traffic Monitor сообщает Positive Technologies MaxPatrol SIEM:*** включение DLP-системы, возврат прав

! **Офицер информационной безопасности делает заключение:**

«Кто-то подсмотрел пароль администратора DLP-системы и решил воспользоваться им в корыстных целях».

Преимущества для заказчика

1. Удобный процесс управления информационной безопасностью в компании

- Все инциденты информационной безопасности попадают в единую консоль SIEM
- Сопоставление событий из InfoWatch Traffic Monitor с событиями из других систем, передающих информацию в SIEM-систему для комплексного анализа ситуации и оперативного выявления реальных инцидентов
- Существенное упрощение процесса расследования инцидентов

2. Предотвращение возможных внутренних угроз

- Выявление сговоров между сотрудниками компании
- Сопоставление действий внешних злоумышленников с действиями сотрудников внутри организации
- Контроль действий сотрудников с правами администратора
- Контроль состояния серверов и служб работы DLP-системы

Загрузка событий из сторонних систем

Данная интеграция предназначена для обработки событий, переданных сторонними системами в InfoWatch Traffic Monitor для последующего анализа.

Поддерживаемые классы событий:

Электронная почта – любые события обмена электронными письмами, включая вложения

Беседа – любые события беседы, представляющие собой обмен только текстовыми сообщениями в рамках одного приложения

Принтеры и МФУ – события преобразования данных на «специализированных» устройствах ввода и вывода изображений/документов

Интернет-активность – события запросов из веб-браузеров и аналогичных программ, осуществляемое по протоколам HTTP/HTTPS

Обмен файлами – любые события, связанные с передачей файлов между произвольными отправителями и получателями

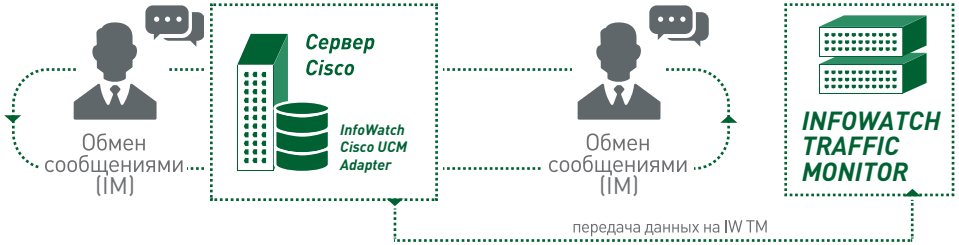
Голосовая беседа – любое событие голосового или видеоразговора, между людьми, который может происходить в произвольном канале

Фото – любые события, связанные с фотографированием потенциально конфиденциальных документов на камеру устройства

Мультимедиа – события создания произвольных аудио- и видеопотоков при помощи устройств

Принцип работы InfoWatch CISCO UCM Adapter

Одним из популярных каналов коммуникации в корпоративной среде является Cisco Unified Communications Manager. Чтобы контролировать данный канал с помощью InfoWatch Traffic Monitor, был разработан InfoWatch Cisco UCM Adapter. Данный адаптер перехватывает текстовую информацию, передаваемую через коммуникатор, и загружает ее в DLP-систему с помощью InfoWatch Traffic Monitor Software Development Kit. Далее InfoWatch Traffic Monitor подвергает все перехваченные события анализу, применяя все технологии анализа и политики, как и для стандартных кана¬лов, поддерживаемых DLP-системой.



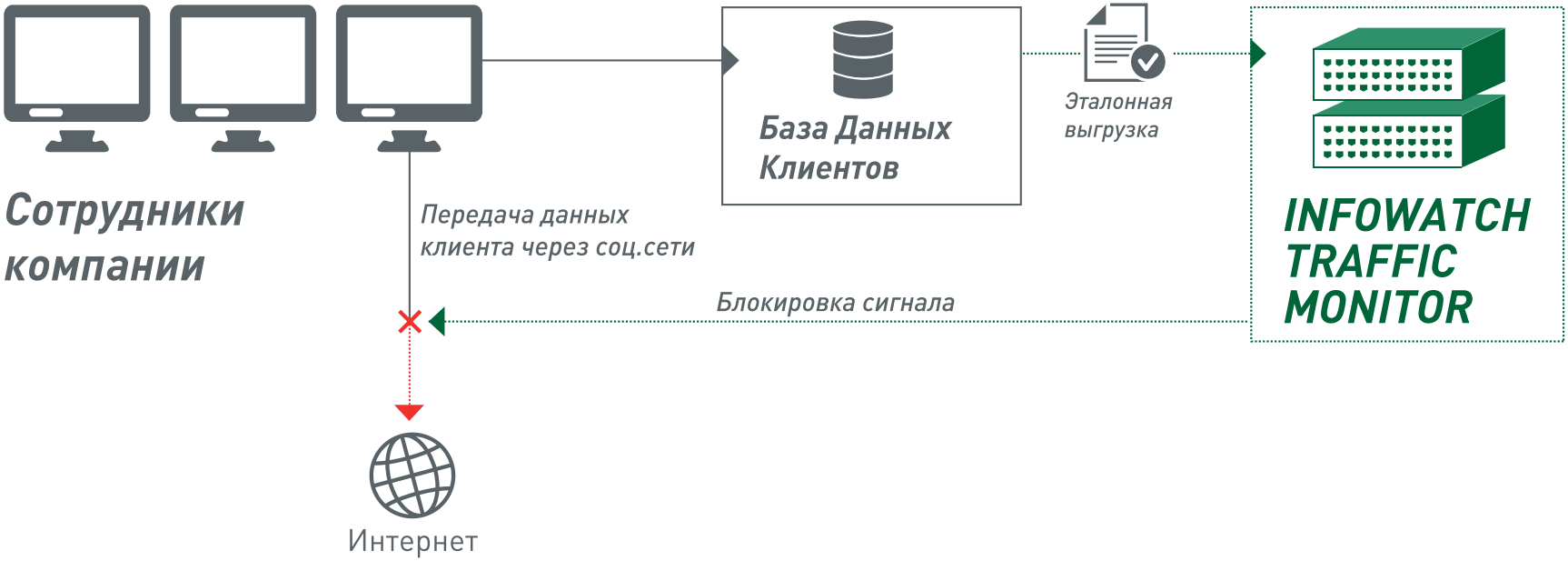
Преимущества для заказчика

1. ***Расширение периметра безопасности компании (контроль новых каналов передачи данных)***
2. ***Единый центр создания политик корпоративной информации***
3. ***Оперативное реагирование на инциденты информационной безопасности***
   - Оповещение офицера безопасности о возможных внутренних угрозах
   - Создание базы инцидентов в едином месте
4. ***Предотвращение возможных внутренних угроз***
   - Выявление сговоров между сотрудниками компании
   - Сопоставление действий внешних злоумышленников с действиями сотрудников внутри организации
   - Всесторонний анализ результатов наблюдения за периметром
5. ***Минимизация репутационных, операционных и финансовых рисков***

Загрузка эталонных документов из сторонних систем

Данная интеграция позволяет загрузить необходимую табличную информацию из базы данных стороннего приложения (ERP, CRM и других) в базу данных InfoWatch Traffic Monitor.

Сторонние системы могут самостоятельно формировать документы, представляющие собой эталонные выгрузки баз данных, и передавать их в InfoWatch Traffic Monitor. Переданные выгрузки детектируются и анализируются InfoWatch Traffic Monitor при попытках передачи по любому каналу. Правила детектирования выгрузок задаются в консоли InfoWatch Traffic Monitor, сторонние системы только загружают или обновляют содержимое выгрузки.



Принцип работы InfoWatch Diasoft Adapter

Разработанный адаптер позволяет загружать базы данных из решений Diasoft (FLEXTERA и FA#) в InfoWatch Traffic Monitor для дальнейшего детектирования и анализа в информационных потоках компании. Офицер безопасности задает период обновления табличных данных или обновляет их самостоятельно. Все перемещения конфиденциальных данных контролируются InfoWatch Traffic Monitor, что минимизирует возможные риски утечки.

1. Сотрудник, подавший документы на увольнение, пытается скопировать на личный USB-носитель базу данных клиентов → InfoWatch Traffic Monitor фиксирует факт нарушения политики безопасности и оповещает офицера безопасности

2. Сотрудник департамента финансового планирования пытается переслать на внешнюю почту планы развития компании в новом регионе → InfoWatch Traffic Monitor фиксирует все вложения из баз данных, пересылаемые по любым каналам передачи информации

Преимущества для заказчика

1. ***Оперативное реагирование на инциденты информационной безопасности***
   - Оповещение офицера безопасности о возможных внутренних угрозах
   - Создание базы инцидентов в одном месте
2. ***Минимизация репутационных, операционных и финансовых рисков***
3. ***Предотвращение возможных внутренних угроз***
   - Выявление сговоров между сотрудниками компании
   - Сопоставление действий внешних злоумышленников с действиями сотрудников внутри организации
   - Защита клиентских баз и персональных данных
   - Выявление маршрутов передвижения информации и мест ее хранения

Перехват HTTP и HTTPS-трафика по ICAP

Данная интеграция предназначена для перехвата и анализа HTTP и HTTPS-трафика, передаваемого через прокси-сервер с поддержкой протокола ICAP.

Прокси-сервер с поддержкой протокола ICAP перехватывает HTTP и HTTPS-трафик и передает его на сервер InfoWatch Traffic Monitor для анализа и загрузки в базу данных.

В данной схеме на сервере InfoWatch Traffic Monitor используется автоматически устанавливаемый модуль InfoWatch ICAP. Схема поддерживает обработку данных пользователя при следующих методах аутентификации: NTLM, LDAP, Basic, Digest.

Варианты движения HTTP-трафика

Режим копии – копия HTTP-трафика передается на сервер InfoWatch Traffic Monitor для анализа, при этом трафик проходит через прокси-сервер к следующему звену сети

Режим блокировки – HTTP-трафик анализируется системой InfoWatch Traffic Monitor и, в зависимости от наличия нарушений, либо разрешает передачу трафика, либо запрещает передачу трафика. Трафик блокируется, а пользователь, отправивший трафик, получает сообщение с предупреждением

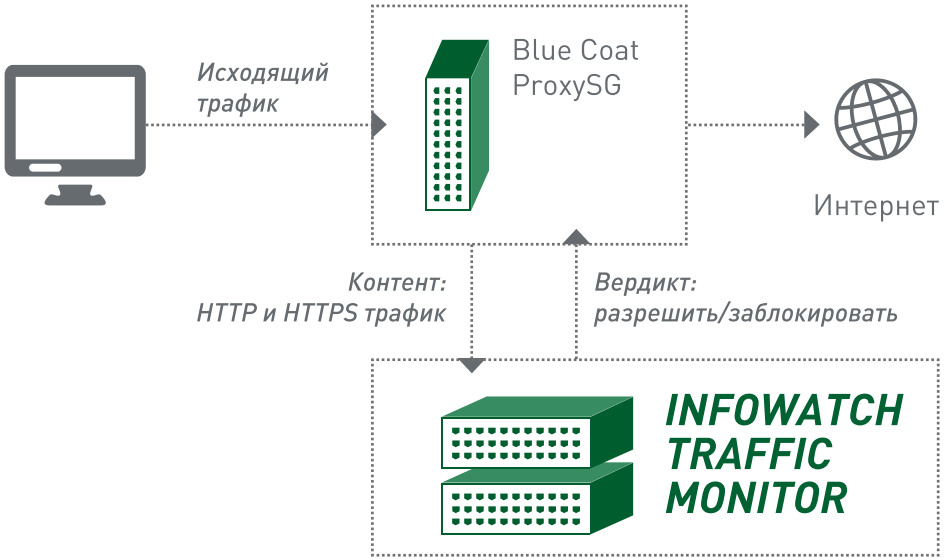
Поддерживаемые прокси-сервера

- Cisco Ironport
- SQUID (при условии, что пакет собран с поддержкой ICAP)
- Blue Coat SG
- MDaemon
- Zimbra ZCS
- Microsoft Forefront Threat Management Gateway 2010 SP2 (требуется установка веб-фильтра)

Работа с другими прокси-серверами, поддерживающими ICAP, возможна, но требует предварительной проверки на совместимость.

Принцип работы и возможности интеграционного решения InfoWatch Traffic Monitor и Blue Coat ProxySG

- мониторинг и анализ данных
- предотвращение утечки данных (блокировка передачи конфиденциальной информации)
- анализ SSL-трафика (HTTPS, SSL, TLS)
- фильтрация URL по различным параметрам
- централизованное хранение перехваченных данных
- расследование нарушений политик ИБ
- гибкая система построения отчетов



Преимущества для заказчика

1. ***Контроль HTTP и HTTPS-трафика***
2. ***Предотвращение возможных внутренних угроз***
   - Выявление сговоров между сотрудниками компании
   - Сопоставление действий внешних злоумышленников с действиями сотрудников внутри организации
   - Блокировка доступа к нежелательному контенту
3. ***Оперативное реагирование на инциденты информационной безопасности***
   - Оповещение офицера безопасности о возможных внутренних угрозах
   - Создание базы инцидентов в одном месте
4. ***Минимизация репутационных, операционных и финансовых рисков***

INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Бизнес-центр «Верейская плаза»

121357, Москва,ул. Верейская,
д.29, стр.134

www.infowatch.ru

+7 (495) 22-900-22
+7 (499) 37-251-74
sales@infowatch.ru