

Функциональные характеристики

Назначение

Программный продукт предназначен для мониторинга и анализа HTTP-трафика веб-приложений в режиме реального времени. Область применения — веб-ориентированные информационные системы и интернет-сервисы, функционирующие по протоколам HTTP/HTTPS.

Программный продукт обеспечивает непрерывный сбор, разбор и анализ параметров входящих запросов и ответов, выявляет отклонения от нормального поведения трафика, фиксирует аномальные паттерны обращений и предоставляет операционному персоналу инструментарий для оперативной диагностики и анализа состояния сервисов.

Применение программного продукта позволяет:

- сократить время обнаружения и устранения инцидентов эксплуатации;
- повысить стабильность и доступность веб-сервисов;
- снизить трудоёмкость диагностики инцидентов;
- повысить управляемость и наблюдаемость веб-инфраструктуры.

Функциональные возможности

- **Сбор и разбор HTTP-трафика.** Перехват и синтаксический разбор HTTP-запросов и ответов с извлечением атрибутов: метод, URI, заголовки, тело запроса, код состояния ответа, время обработки.
- **Анализ паттернов трафика.** Выявление отклонений в структуре и содержимом HTTP-запросов от нормального поведения, характерного для штатного функционирования приложения и его пользователей.
- **Контроль объёмных и частотных характеристик трафика.** Измерение интенсивности потока запросов, обнаружение аномальных всплесков нагрузки и нетипичных паттернов активности источников трафика.

- **Корреляция и обогащение данных.** Сопоставление и агрегация данных из потока запросов, их преобразование для проведения углублённого анализа и построения информационных панелей.
- **Ведение журнала событий.** Регистрация выявленных отклонений с возможностью последующей выборки, фильтрации и интеграции с внешними системами мониторинга и оповещения.

Входные данные

Входными данными являются HTTP/HTTPS-запросы и ответы, передаваемые между конечными пользователями и веб-приложениями заказчика. Из трафика извлекаются следующие атрибуты:

- метод HTTP-запроса, URI, версия протокола;
- заголовки запроса и ответа;
- тело запроса;
- код состояния HTTP-ответа;
- IP-адрес источника запроса;
- время обработки запроса.

Выходные данные

По результатам обработки входящего трафика программный продукт формирует:

- журнал событий с зафиксированными отклонениями и их атрибутами;
- метрики трафика (интенсивность, распределение по методам, URI, кодам состояния, источникам);
- оповещения при выявлении аномалий или превышении заданных пороговых значений.

Режим функционирования

Программный продукт функционирует в непрерывном режиме (24 часа в сутки, 7 дней в неделю) без плановых остановок. Обработка входящего трафика выполняется в режиме реального времени.