RT Protect NTA

PT

Информационная безопасность

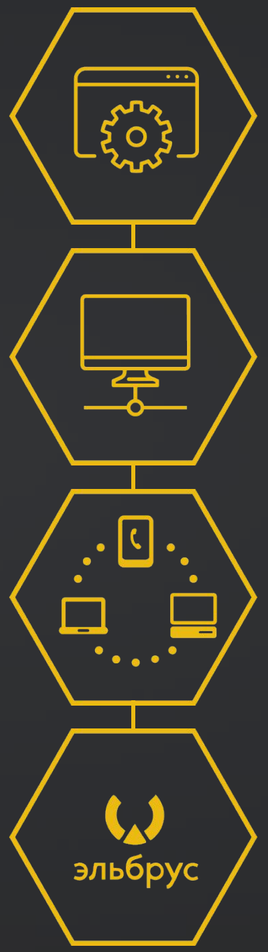
PT- Информационная безопасность занимается разработкой и внедрением решений в сфере информационной безопасности, позволяющих решать широкий спектр задач по защите информации.

Наши сотрудники – эксперты с многолетним опытом работы в области ИБ. При разработке продуктов мы используем как собственную практику их использования в реальных инфраструктурах, так и лучшие мировые решения построения безопасных систем.

RT Protect NTA – аппаратно-программный комплекс, позволяющий осуществлять контроль всего сетевого трафика компании (локального и взаимодействия с сетью Интернет), обнаруживать атаки злоумышленников и соблюдать политики информационной безопасности. Комплекс является эффективным и удобным инструментом для анализа сетевых взаимодействий и контроля сетевой активности пользователей и ПО.

Клиенты

- Подразделения ИБ и IT
- Компании, заинтересованные в контроле интернет-активности своих сотрудников
- Интернет-провайдеры



На оборудовании архитектуры x86-64 Комплекс позволяет без потерь обрабатывать сетевой поток на скорости до 20 Гбит/с (10 Гбит/с full-duplex).

Для анализа сетевых потоков на скорости до 2 Гбит/с **RT Protect NTA** требуются ресурсы, сопоставимые с недорогим ПК.

Один Комплекс одновременно позволяет обрабатывать сетевые потоки с нескольких независимых сетевых интерфейсов.

RT Protect NTA также работает на российском оборудовании архитектуры «Эльбрус».

Комплекс RT Protect NTA подходит для компаний любого масштаба, имеет интуитивно понятный интерфейс, гибкие настройки и оптимальное ресурсопотребление.

Для чего нужен RT Protect NTA

Предупреждает кибератаки на активы предприятия

Обнаруживает утечки конфиденциальной информации

Контролирует действия сотрудников в Интернете

Собирает статистику и позволяет анализировать весь трафик в удобном формате отчетов

Собирает доказательную базу и помогает расследовать инциденты ИБ

Позволяет минимизировать финансовые и репутационные риски

2,5 трлн руб.
потери экономики России от кибератак в 2019 году

10,52 млрд
атак вредоносных программ зарегистрировала в 2018 году компания SonicWall

На 61%
выросло число утечек конфиденциальных данных в России за первое полугодие 2019 года (по сравнению с аналогичным периодом 2018 года)

PT
Информационная безопасность

Что умеет RT Protect NTA

RT Protect NTA помогает эффективно контролировать сетевую активность организации, выявлять факты нарушения политики безопасности, в том числе утечки конфиденциальной информации, отказ в работе сетевых сервисов и нарушения стандартного профиля сетевых взаимодействий.

Захват трафика

Захват сетевого трафика с нескольких сетевых интерфейсов одновременно с возможностью фильтрации.

Индексация и классификация трафика

Расчет и запись статистики сетевого трафика в реальном времени, включает в себя не менее 20 сетевых параметров индексации

Запись трафика

Гарантированная запись сетевого трафика на диск со скоростью до 20 Гбит/с и предоставление его для анализа.

Мониторинг в реальном времени

Оперативный мониторинг состояния сети организации в графическом и табличном представлении.

Анализаторы трафика

Выявление аномалий и атак в автоматическом режиме с применением методов математической статистики и машинного обучения.

Интеграция с SIEM-системами

Идентификация географической принадлежности сетевых адресов индексируемого трафика

Интеграция с внешними анализаторами трафика

Перенаправление трафика на внешние системы обнаружения вторжений.

Идентификация протоколов

Определение более 1000 сетевых протоколов, включая прикладной уровень приложений и сервисов.

Ретроспективный анализ

Детализация сетевой активности ранее накопленных данных с учетом специфики расследуемого инцидента, а также возможность применения новых анализаторов и методов анализа.

Интеграция с SIEM-системами

Экспорт событий ИБ в сторонние системы.

Как это работает

RT
Информационная безопасность

Хранит трафик с метаинформацией.

RAID-массив

Выявляют аномалии и атаки в автоматическом режиме с применением методов математической статистики и машинного обучения.

Анализаторы

Централизованный мониторинг и управление всеми компонентами

Управляющий сервер

Захватывает и сохраняет весь трафик сети.

Интернет

Сетевой шлюз

Дампер

Консоль оператора

Интуитивно понятный web-интерфейс. Предоставляет данные для анализа трафика и выполнения расследований.

Локальная сеть

Архитектура RT Protect NTA

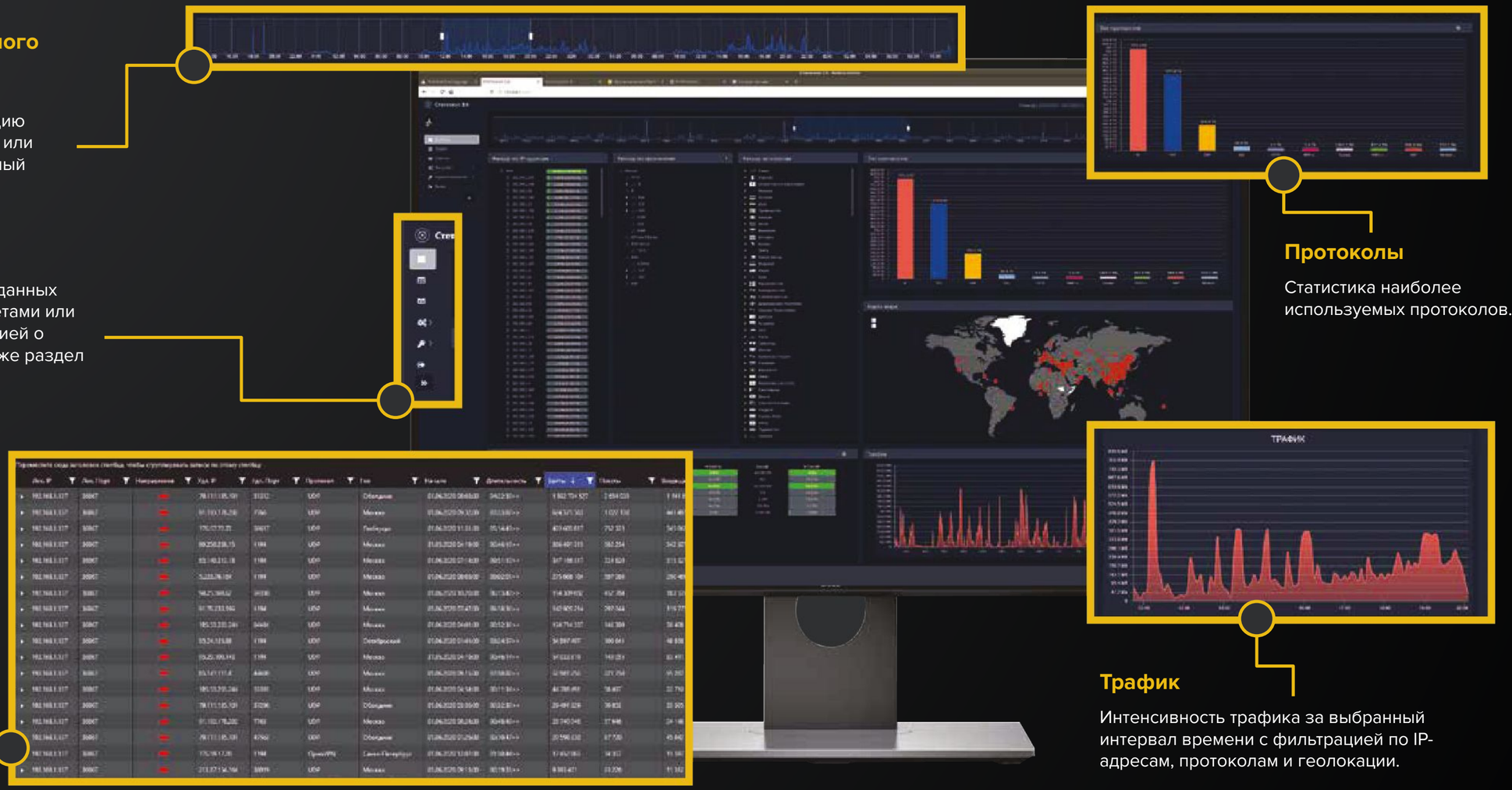
Индексатор

Индексирует и классифицирует трафик, записывает метаинформацию в БД.

База данных

Хранит статистику трафика, события анализаторов и политики фильтрации трафика.

Интерфейс оператора



Выбор временного интервала

Удобный способ получить детализацию статистики трафика или событий ИБ за нужный интервал времени.

Главное меню

Выбор режима отображения данных между агрегированными отчетами или детализированной информацией о трафике и событиях ИБ, а также раздел управления Комплексом.

Главное меню

Получение детальной информации по сетевым сессиям и событиям ИБ. Возможность фильтрации и экспорта.

Протоколы

Статистика наиболее используемых протоколов.

Трафик

Интенсивность трафика за выбранный интервал времени с фильтрацией по IP-адресам, протоколам и геолокации.

PT
Информационная безопасность

Сценарии использования

Выполнение анализа в реальном времени и ретроспективно.

Сетевой трафик

Представление сетевой активности с удобным механизмом фильтрации.

События ИБ

Единая система отчетов по событиям ИБ от различных анализаторов.

Преимущества Комплекса

Плюсы решения RT Protect NTA

Уникальный развивающийся функционал

Реализована плагинная архитектура, позволяющая гибко расширять базовую функциональность анализаторов Комплекса. Применяются методы математической статистики, сигнатурного анализа и машинного обучения (ML/AI).

Эргономика

Интуитивно понятный интерфейс позволяет легко начать работу с Комплексом по решению задач мониторинга сети.

Гибкая ценовая политика

Аппаратные и программные компоненты подбираются с учетом скорости сетевых потоков, времени хранения данных и планируемых к использованию анализаторов.

Простота внедрения и масштабируемость

Простая процедура развертывания не требует изменения сетевой инфраструктуры. Для анализа потоков на скорости 1 Гбит/с достаточно обычного персонального компьютера, а для анализа каналов до 10 Гбит/с нет необходимости в дорогом серверном оборудовании.

Импортозамещение

Российская разработка. Поддержка отечественной платформы «Эльбрус». Возможность применения в государственных органах РФ.

Интеграционные возможности

Интеграция с существующими системами анализа трафика (IDS/IPS) и системами обработки событий ИБ (SIEM).

Поддержка

Оказание поддержки и сопровождение на всех этапах эксплуатации Комплекса, от внедрения Комплекса до расследования инцидентов ИБ.

RT Protect NTA полезен для большинства компаний и имеет ряд преимуществ по сравнению с другими решениями.

Технические характеристики

Мы поставляем RT Protect NTA в виде комплексного решения: сервер с предустановленным программным обеспечением. Это позволяет гарантировать соответствие всем техническим требованиям и правильную настройку параметров, а значит и надежную работу всего Комплекса.

Типовое решение представляет собой сервер с предустановленным ПО «Стетоскоп» и при необходимости ответвитель сетевого трафика (TAP) для безопасного внедрения в действующую сеть.

Также в комплект типового решения включено более 20 анализаторов контроля пороговых значений, анализа по белым/черным спискам (IP, DNS, геолокация), базам «плохих» IP, DNS и сервисов.

Характеристики

Скорость канала	20 Гбит/с
Количество сессий в секунду	100 000 Сервер
Форм-фактор	1U-4U
Длительность хранения данных	От нескольких дней до нескольких лет

Партнеры

Ростелеком

ПАО «Ростелеком»

РТ
Информационная безопасность

Нам доверяют

Ростех
РТ-Энергоэффективность

РТ
Развитие бизнеса

Ростех
Техприемка

Ростех

KAMAZ

ОАК
Объединенная авиастроительная корпорация

ОДК

КБП

СИБЕР

Нацимбио

Высокоточные комплексы

УВЗ

НОВИКОМБАНК

Контакты

Адрес: 117587, г. Москва, Варшавское шоссе, дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru

РТ
Информационная безопасность