RRC

Обзор платформы RSA NetWitness

Автор: Pete Kuzeev, Security Expert, RRC Moscow

Ресурсы: www.emc.com www.rsa.com www.netwitness.com

RRC

Что такое RSA NetWitness?

NetWitness

NetWitness
Корпоративная система безопасности

Инновационные решения – **защита** от промышленного шпионажа

Безотказная работа во внутренней сети **EMC**

RSA NetWitness
Актуальная информация от текущей ситуации

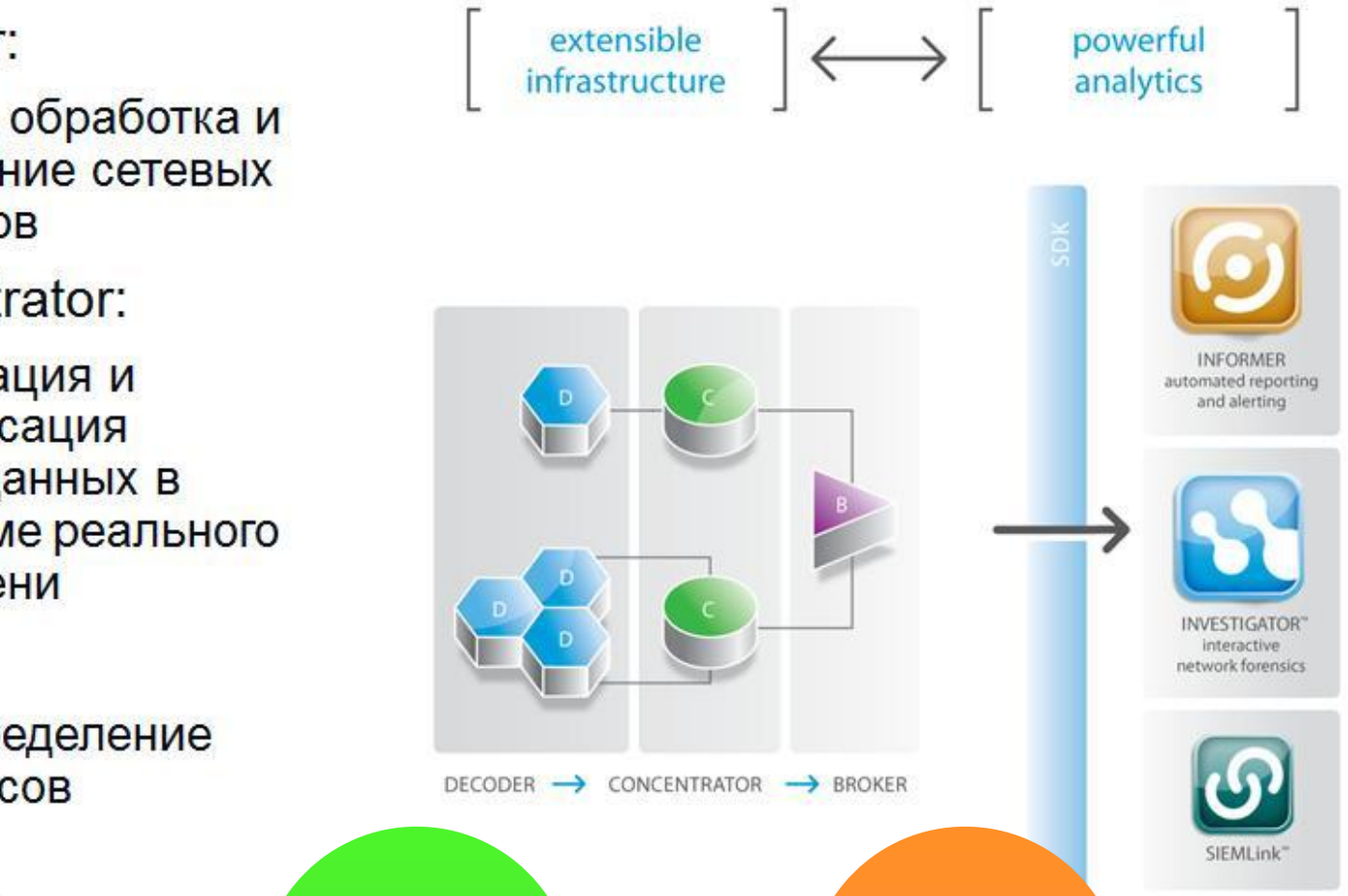
Детальный анализ – воссозданий сессий и анализ на **ВСЕХ** уровнях

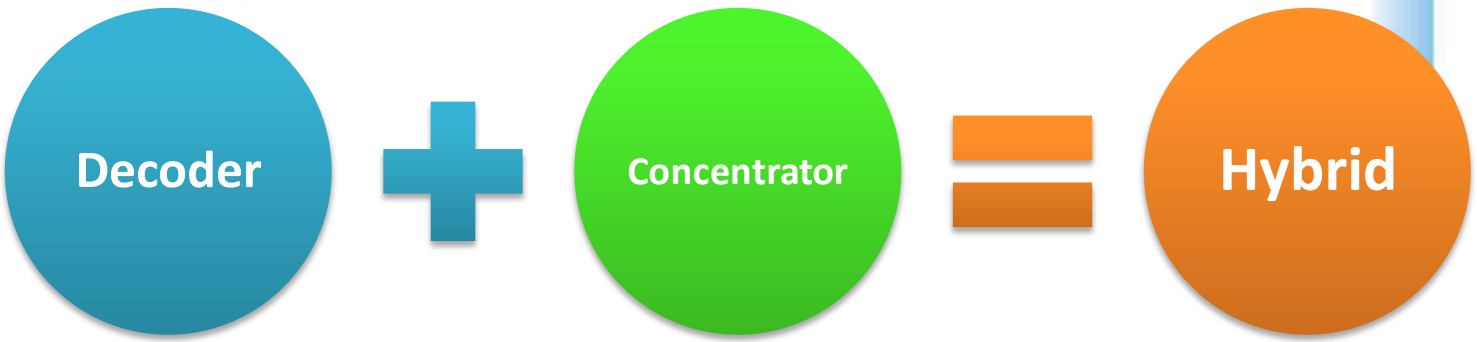
Революционный подход к мониторингу – сбор **ВСЕГО** трафика

RSA NetWitness

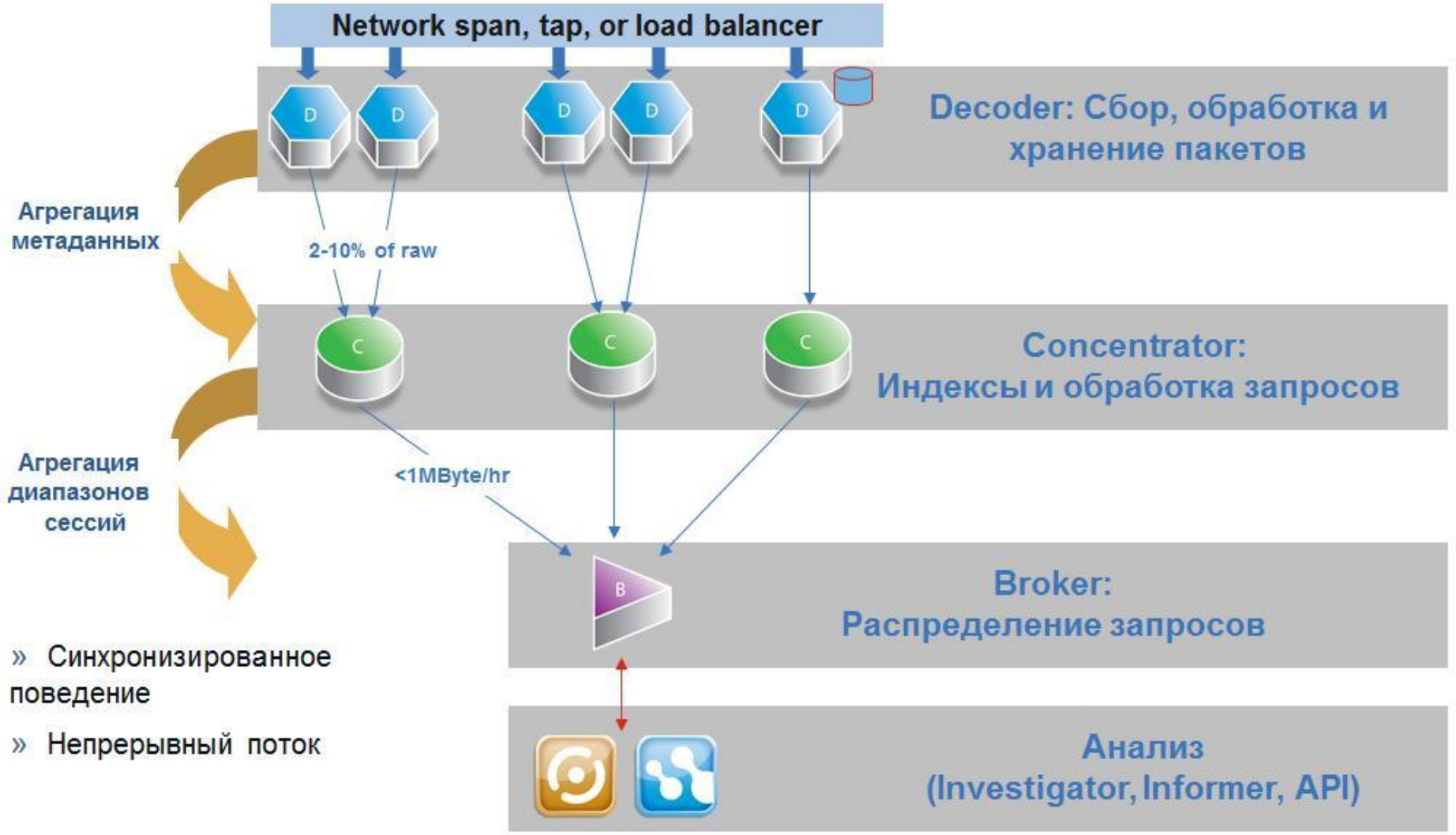
Архитектура решения

- **Decoder:**
  - Сбор, обработка и хранение сетевых пакетов
- **Concentrator:**
  - Агрегация и индексация метаданных в режиме реального времени
- **Broker:**
  - Распределение запросов





Обработка данных



» Синхронизированное поведение

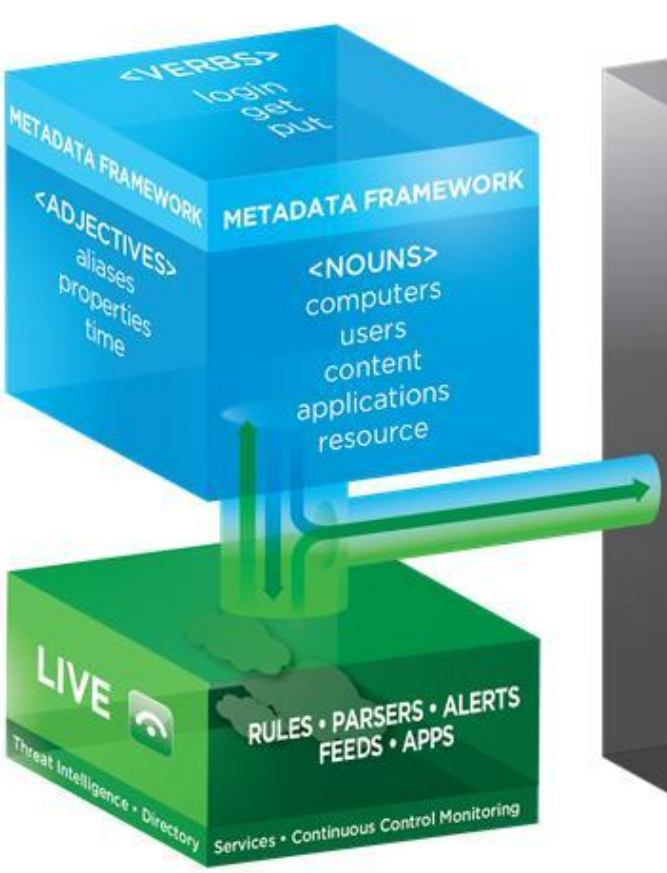
» Непрерывный поток

LIVE → VIsualise → Spectrum → Investigator → Informer

RRC

Набор аналитических приложений

Правила → Обработчики → Оповещения → Фиды → Приложения



Автоматизированный анализ вредоносного ПО

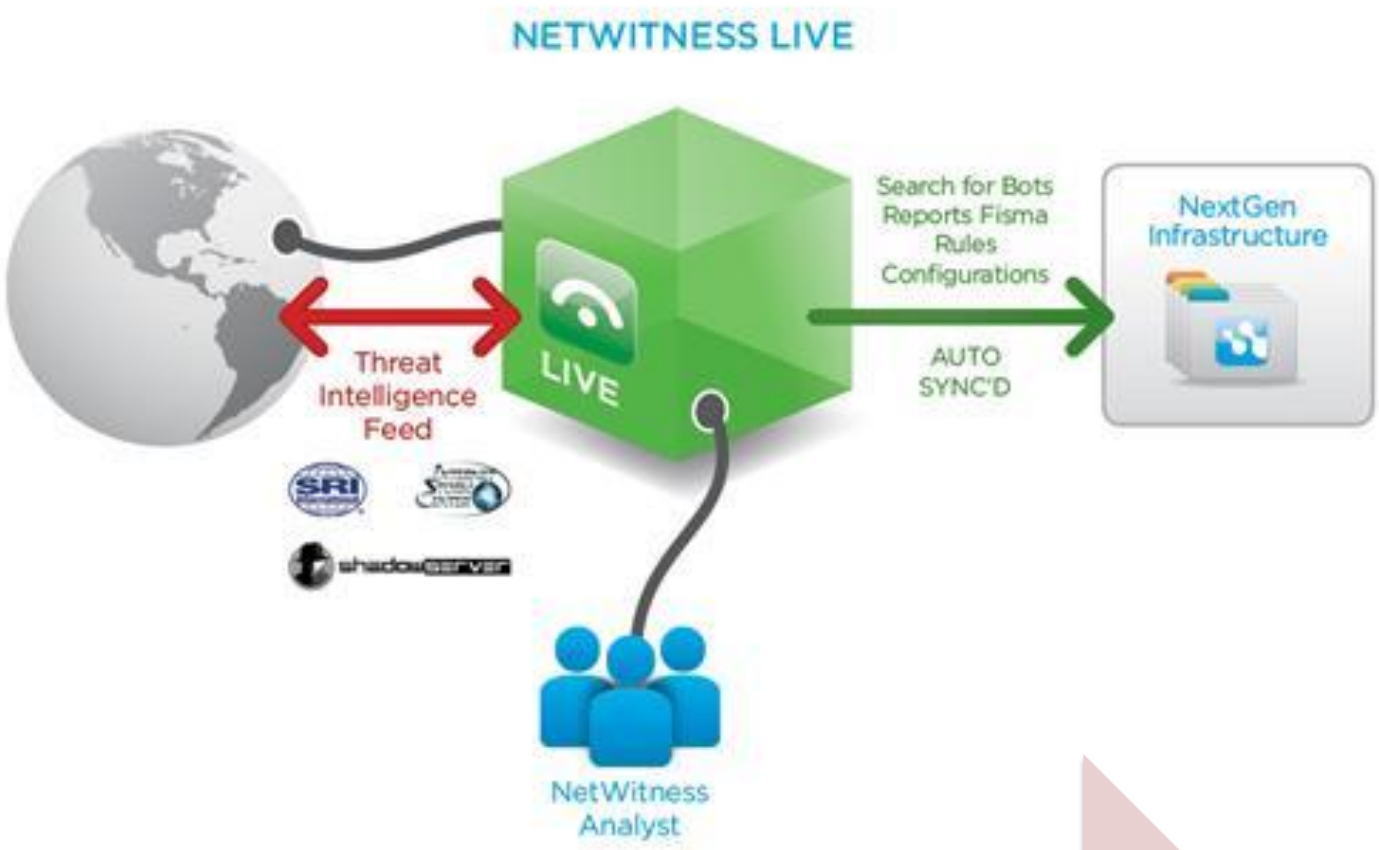
Автоматизированная отчетность и оповещение об обнаруженных угрозах

Модуль для расследований инцидентов

Визуализация сетевых сессий

RRC

Облачные сервисы



Вредоносное ПО

Ботнеты

Мошенничество

Рейтинги

Приоритезация рисков

Аналитические данные различных сообществ ИБ

Глобальный анализ угроз

Детализированная отчётность

RRC

Облачные сервисы – варианты подписок

BASIC
(FREE)

Open Source Threat Intelligence
Advanced Threat Content

- Informer Threat/Security Reports
- BOT/C&C reports
- Exploit Kit Identification
- Zero-Day Indicators
- Compromise Indicators
- Prioritized Risk Levels

INTELLIGENCE SOURCES

SRI International · shadowserver · Internet Storm Center

ENHANCED
(Subscription)

User Identity
Spam/Phish/Threat Intelligence

- Trend Intelligence
- Anonymous Proxies
- Website Classification
- Spam/Phish/Threat Intelligence
- NetWitness Identity (AD Integration)

INTELLIGENCE SOURCES

ZeuS Tracker · IID

PREMIUM
(Subscription)

Fraud Intelligence
Financial Services Intelligence

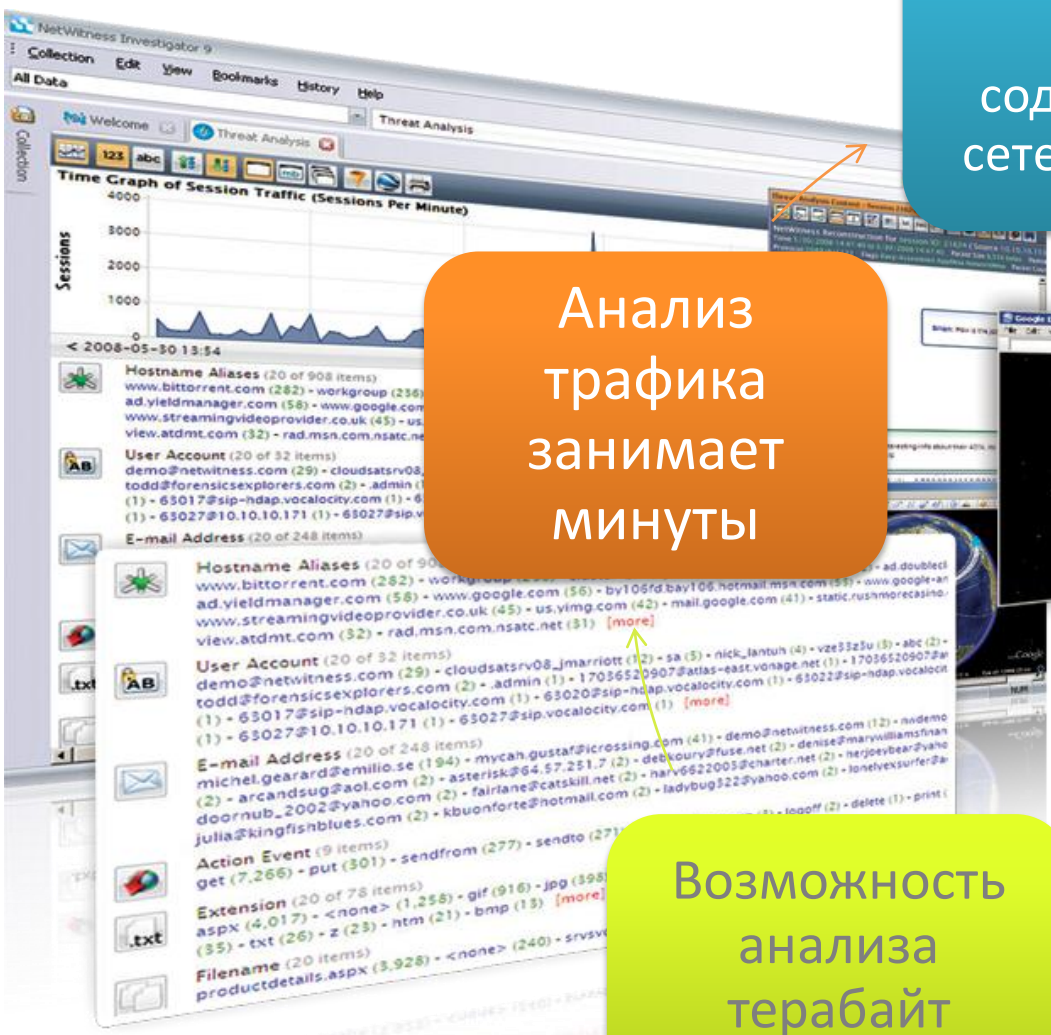
VeriSign · my | NetWatchman

Основная — Подписки для уязвимостей уровня critical бесплатны

Расширенная — Для крупных компаний, нуждающихся в дополнительных сервисах

Премиальная — Для предприятий госсектора, работающих с материалами высокой секретности

RRC Investigator – Ответы на ваши вопросы



Интерактивный анализ содержимого сетевых сессий

Анализ трафика занимает минуты

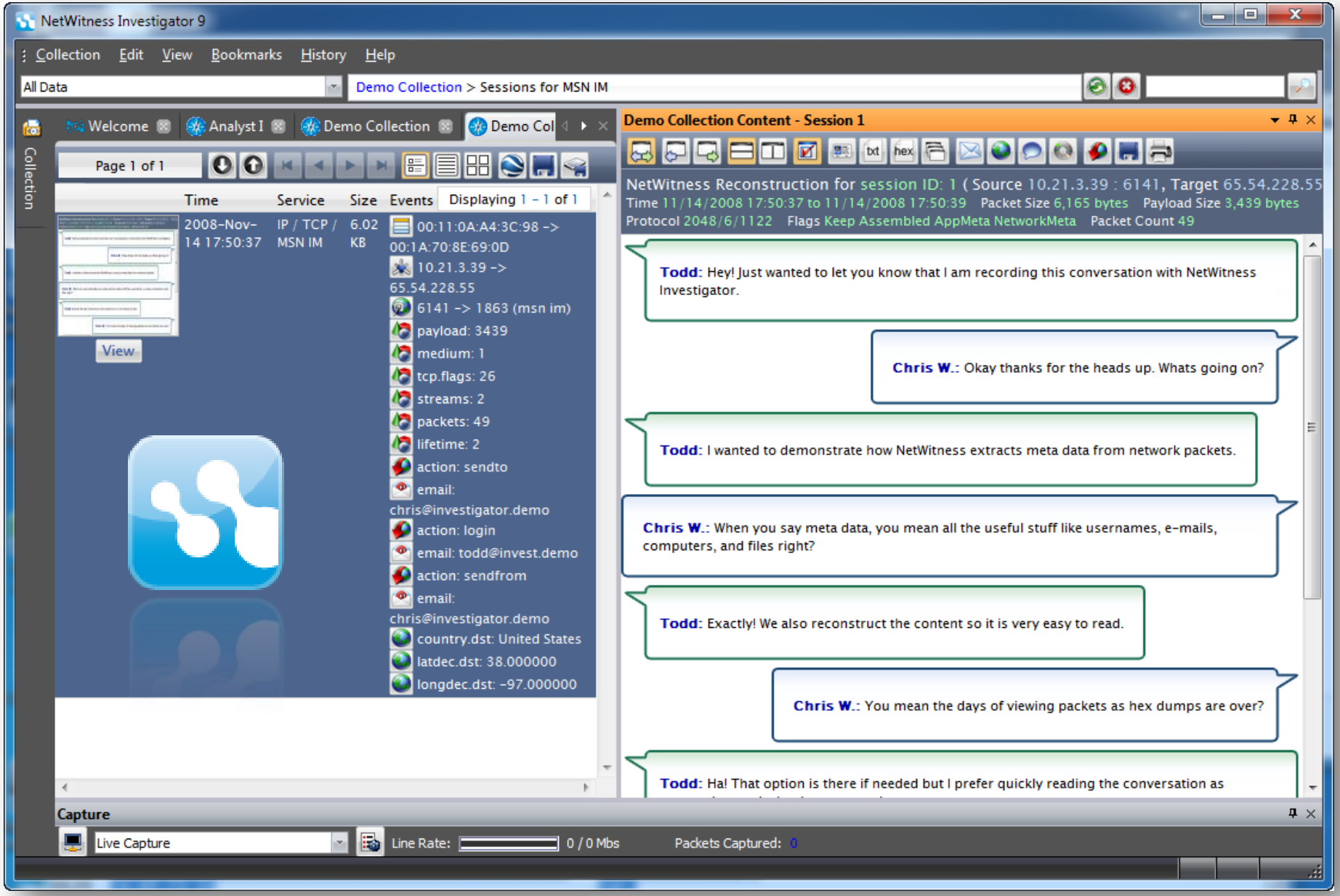
Любые направления анализа – гибкость в расследованиях

Интуитивное представление данных

Возможность анализа терабайт данных в сутки

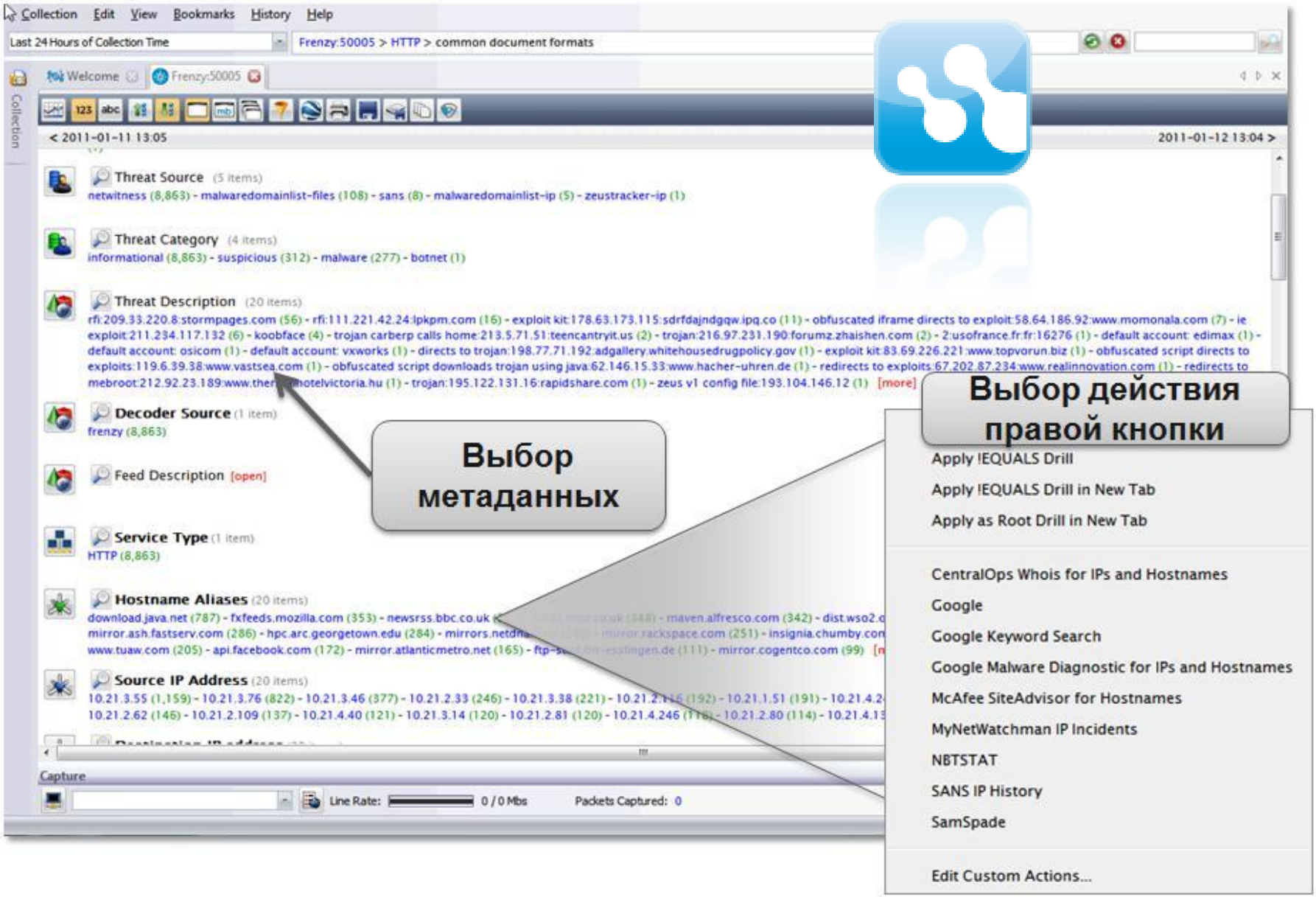
RRC

Investigator – Анализ сессий



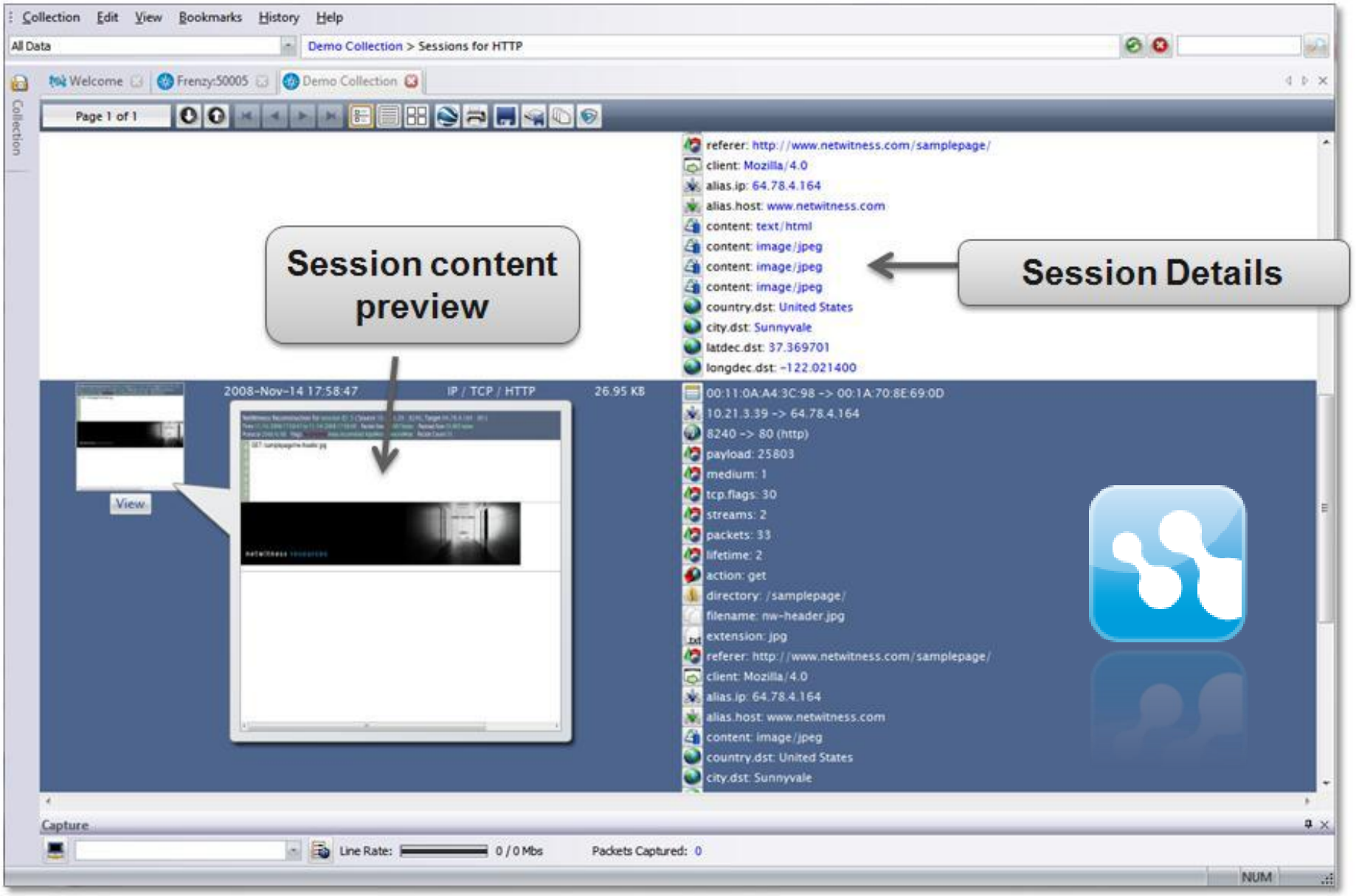
RRC

Investigator – Навигация



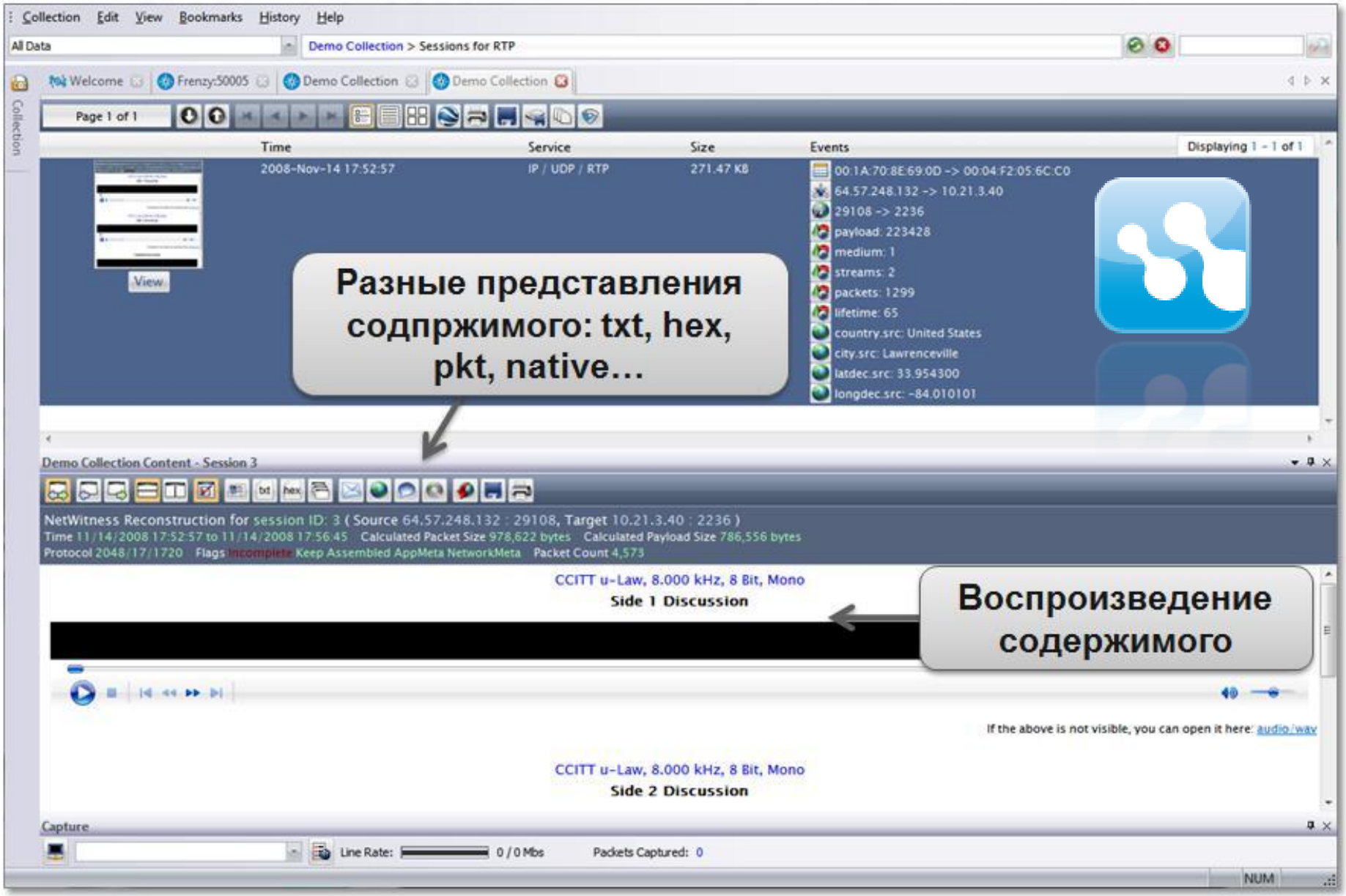
RRC

Investigator – Анализ сессий



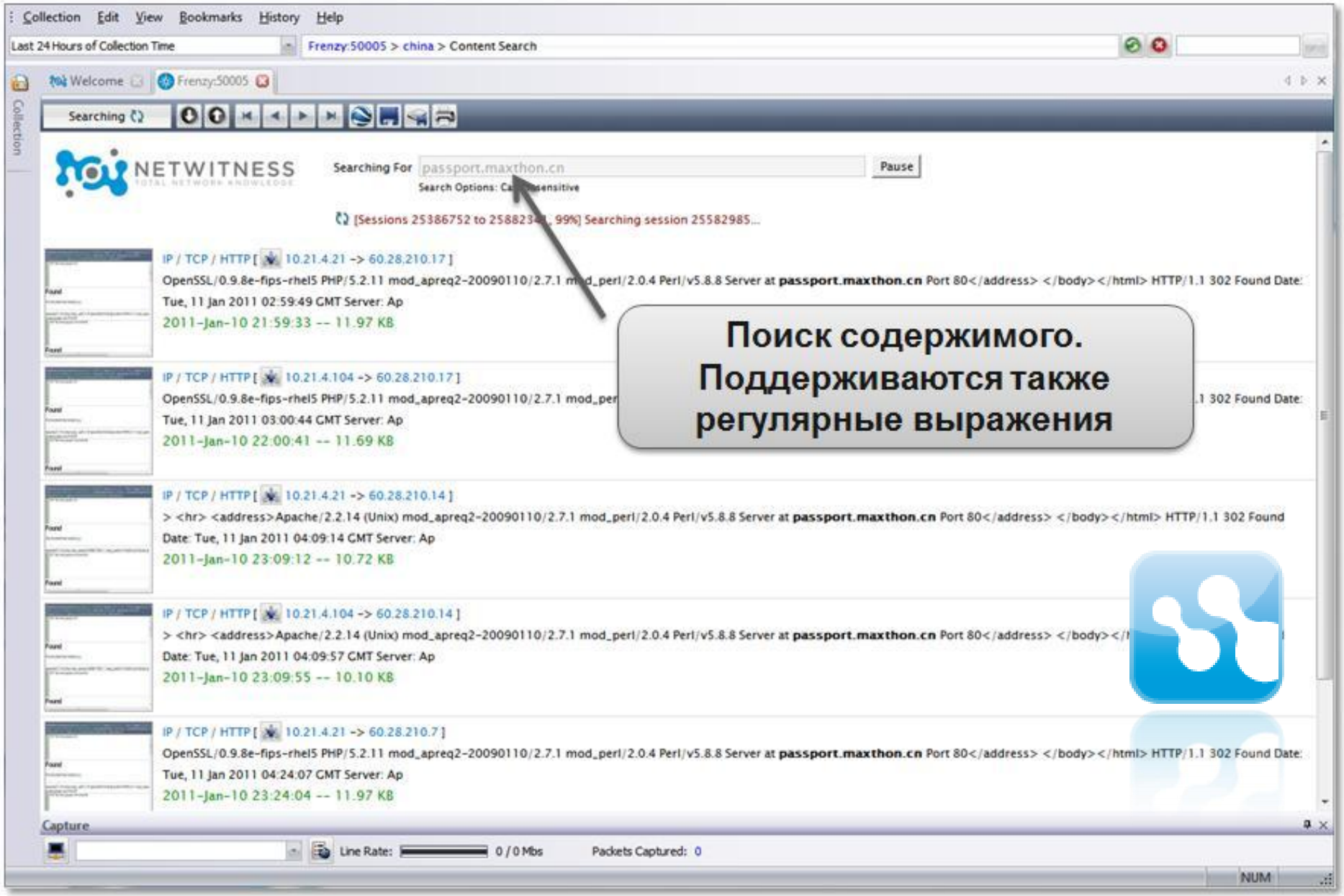
RRC

Investigator – Анализ содержимого



RRC

Investigator – Контекстный поиск



RRC

Spectrum – Безсигнатурный анализ

Аналитика по объекту не сводиться к простому сигнатурному анализу, используется уникальный алгоритм, отрабатывающий тысячи параметров

Благодаря NetWitness Live появляется возможность использования актуальный базы знаний и быть готовым к возможным угрозам

Глубокий анализ в режиме реального времени позволяет получать детальную и максимально приближенную к реальности картину сетевой активности

Система приоритезации вредоносного ПО подсказывает каким областям и объектам следует уделить внимание в первую очередь

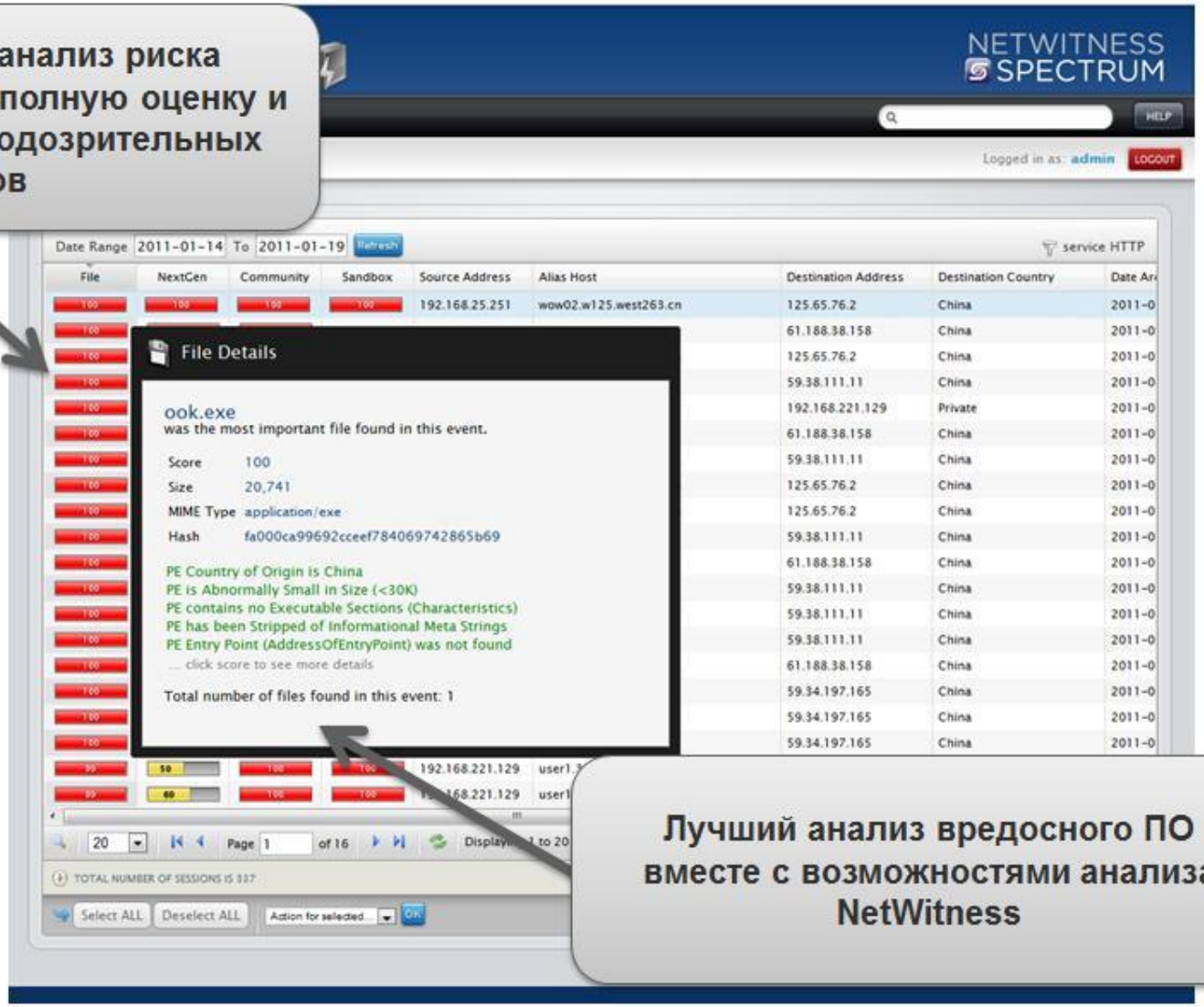
RRC Spectrum – Инструментальная панель

Настраиваемая приборная панель обеспечивает непрерывный анализ угроз в реальном времени

RRC

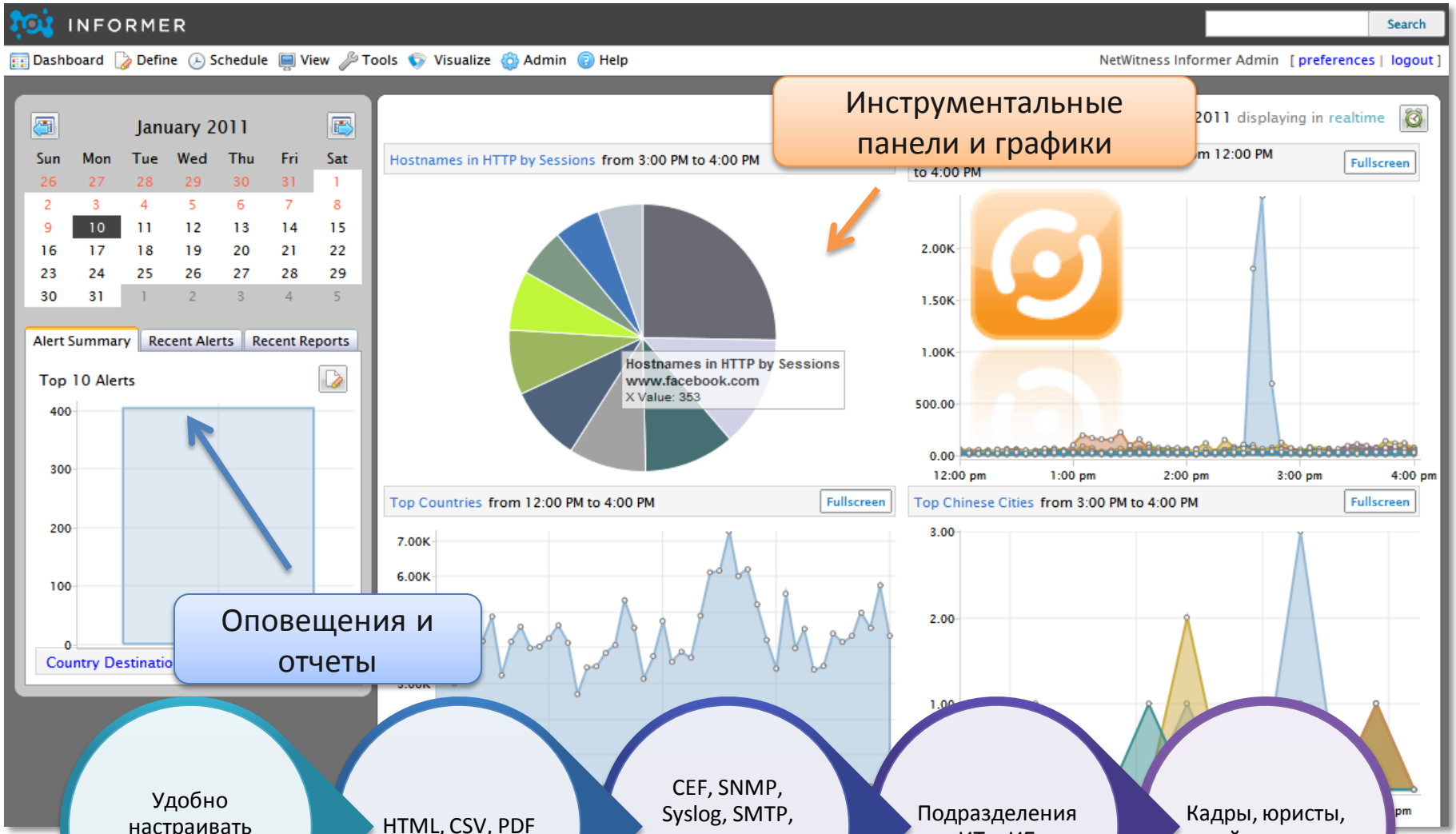
Spectrum – Приоритезация угроз

Многосторонний анализ риска обеспечивает самую полную оценку и приоритетизацию подозрительных файлов



Лучший анализ вредосного ПО вместе с возможностями анализа NetWitness

RRC Informer – Автоматизация и оповещение



Удобно настраивать оповещения

HTML, CSV, PDF

CEF, SNMP, Syslog, SMTP, интеграция с SIEM

Подразделения ИТ и ИБ

Кадры, юристы, хозяйственники

RRC

Visualize – потрясающая наглядность

Революционный интерфейс для анализа содержимого сетевого трафика, установленных сессий и других сетевых действий

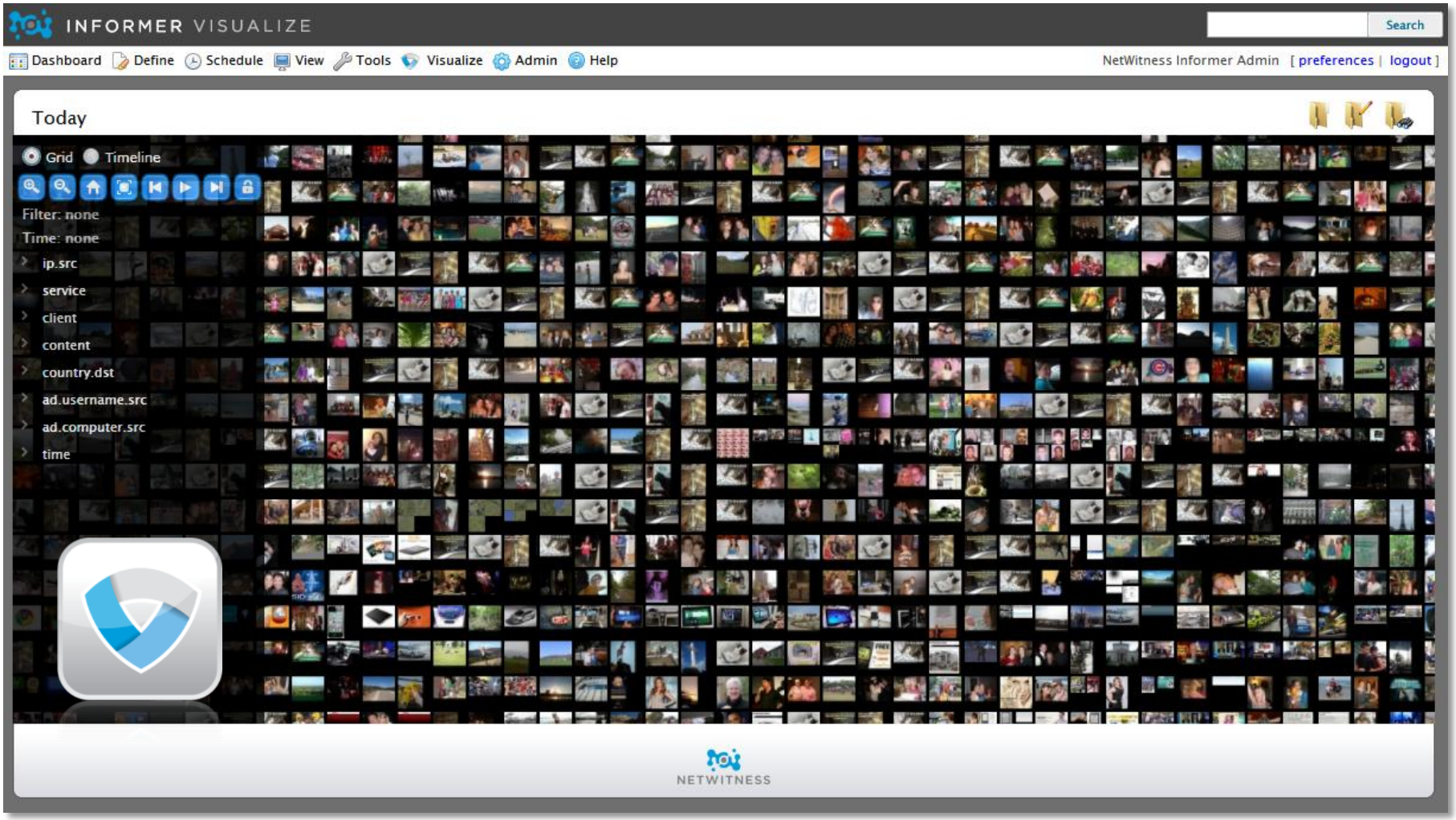
Извлекает в интерактивном режиме и представляет для анализа изображения, объекты, аудио, видео

Поддерживает возможности задания временных интервалов для воспроизведения содержимого

Доступны функции быстрого обзора и сортировки , навигация по содержимому, создание линков

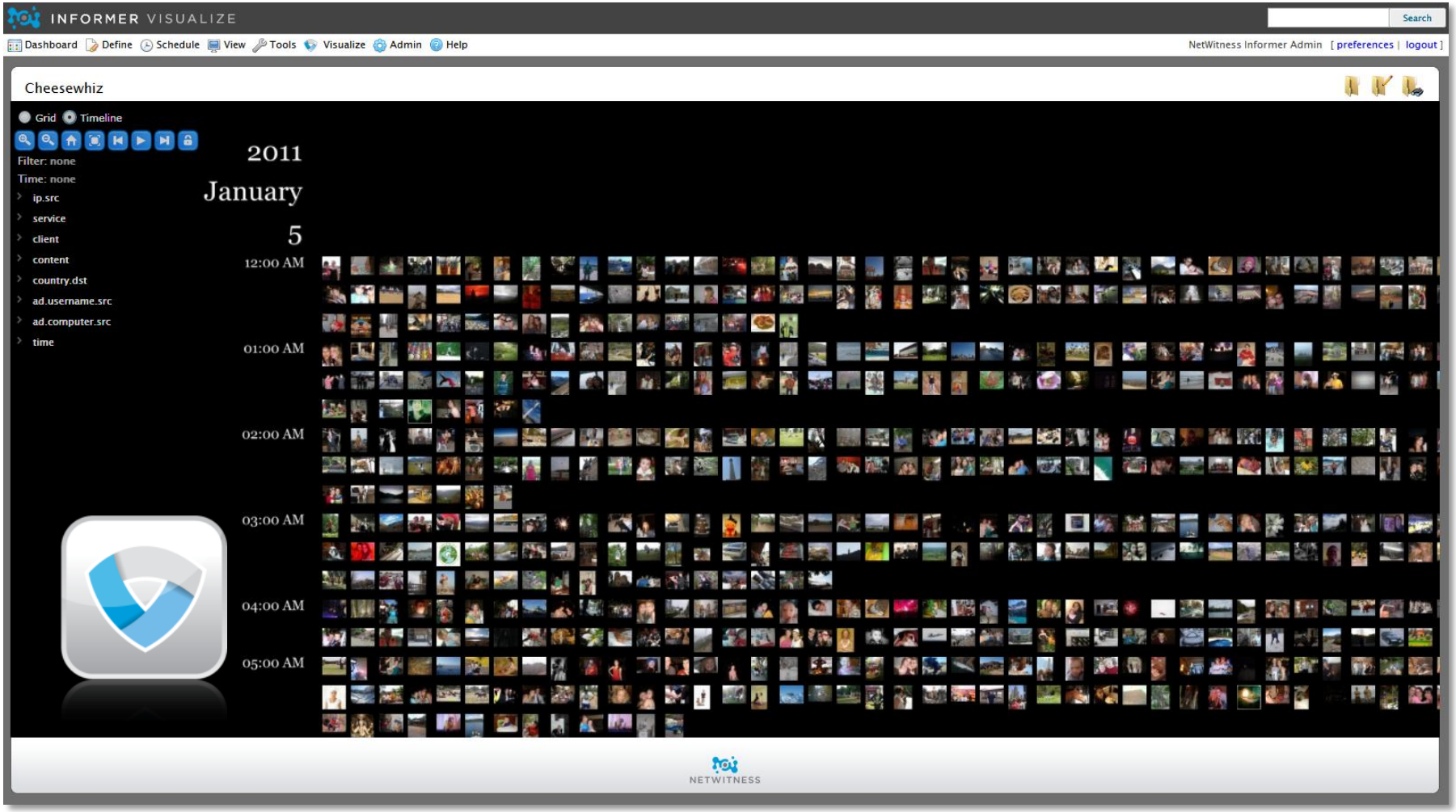
RRC

Visualize – интерфейс



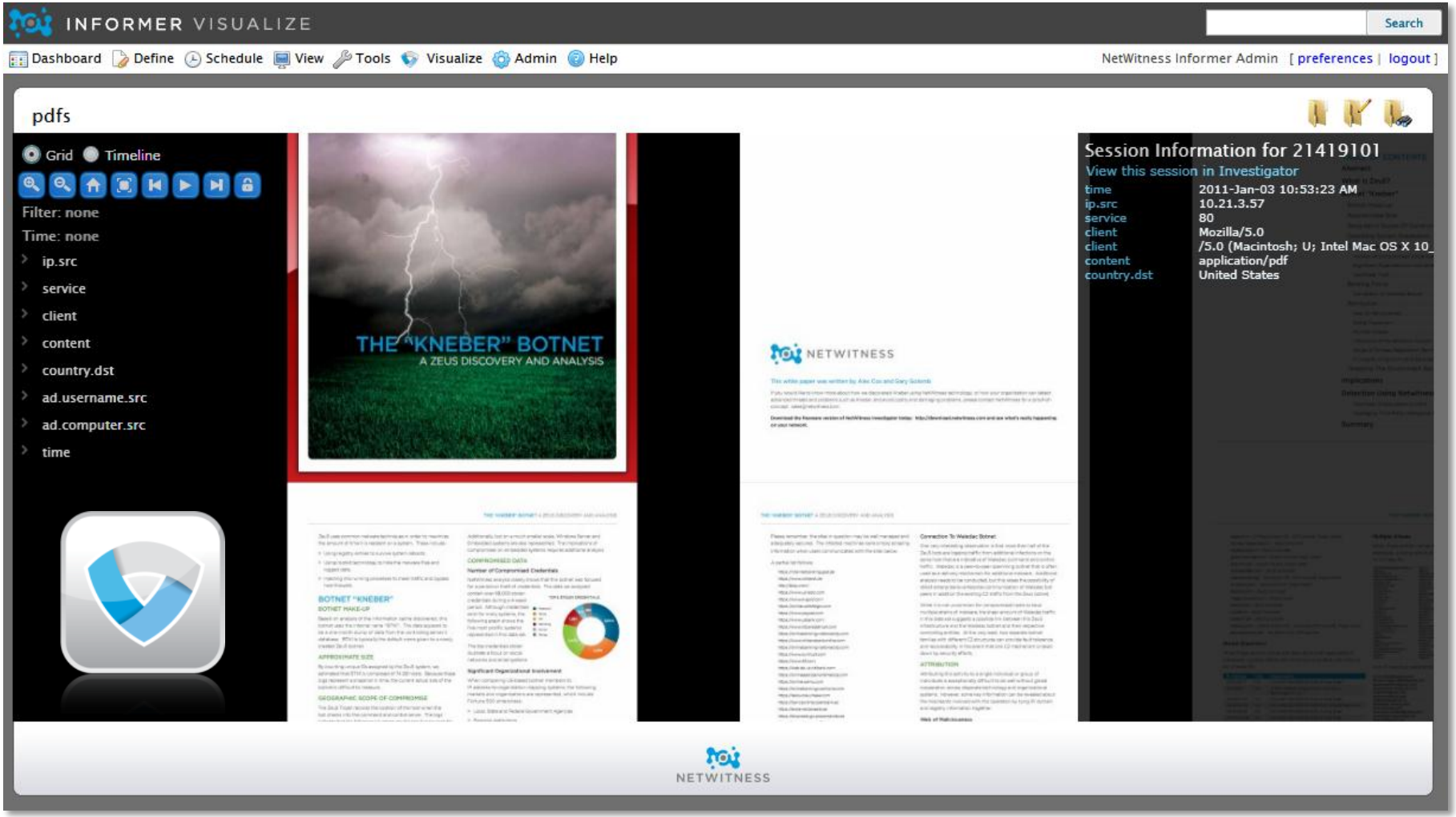
Адрес источника → Служба → Клиент → **Содержимое** → Страна назначения → Время

RRC Visualize – сортировка по времени



Адрес источника → Служба → Клиент → Содержимое → Страна назначения → **Время**

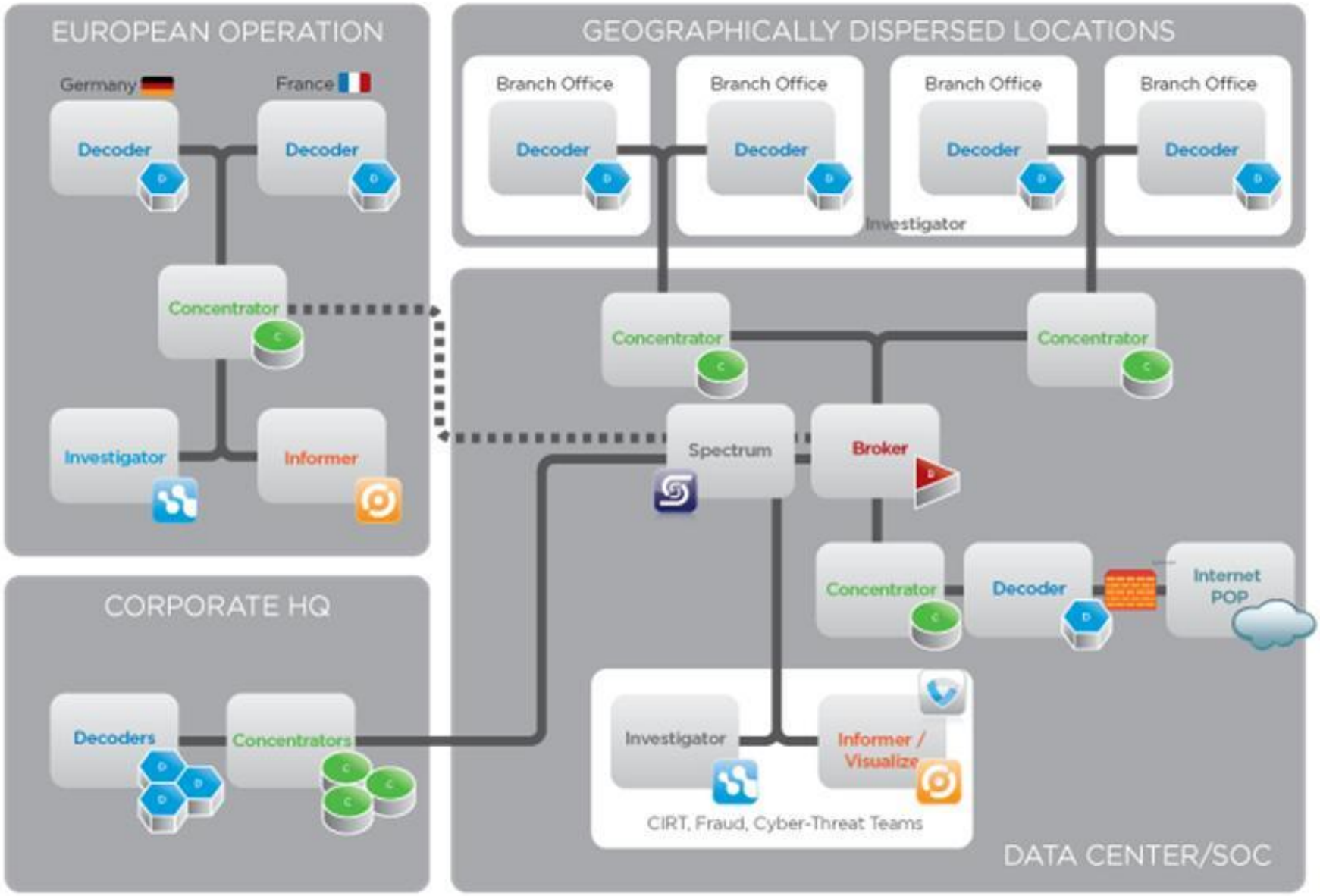
RRC Visualize – навигация по содержимому



Адрес источника → Служба → Клиент → Содержимое → **Страна назначения** → Время

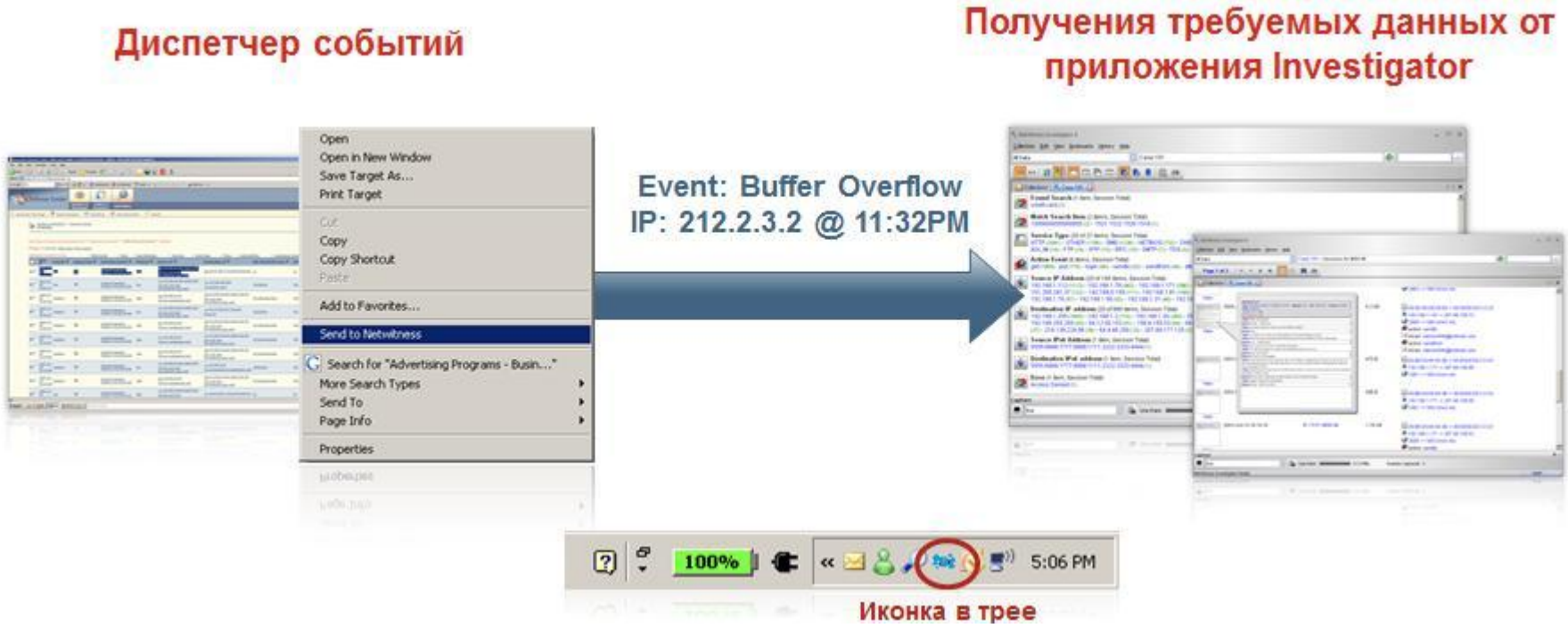
RRC

Пример внедрения



RRC

NetWitness SIEMLink



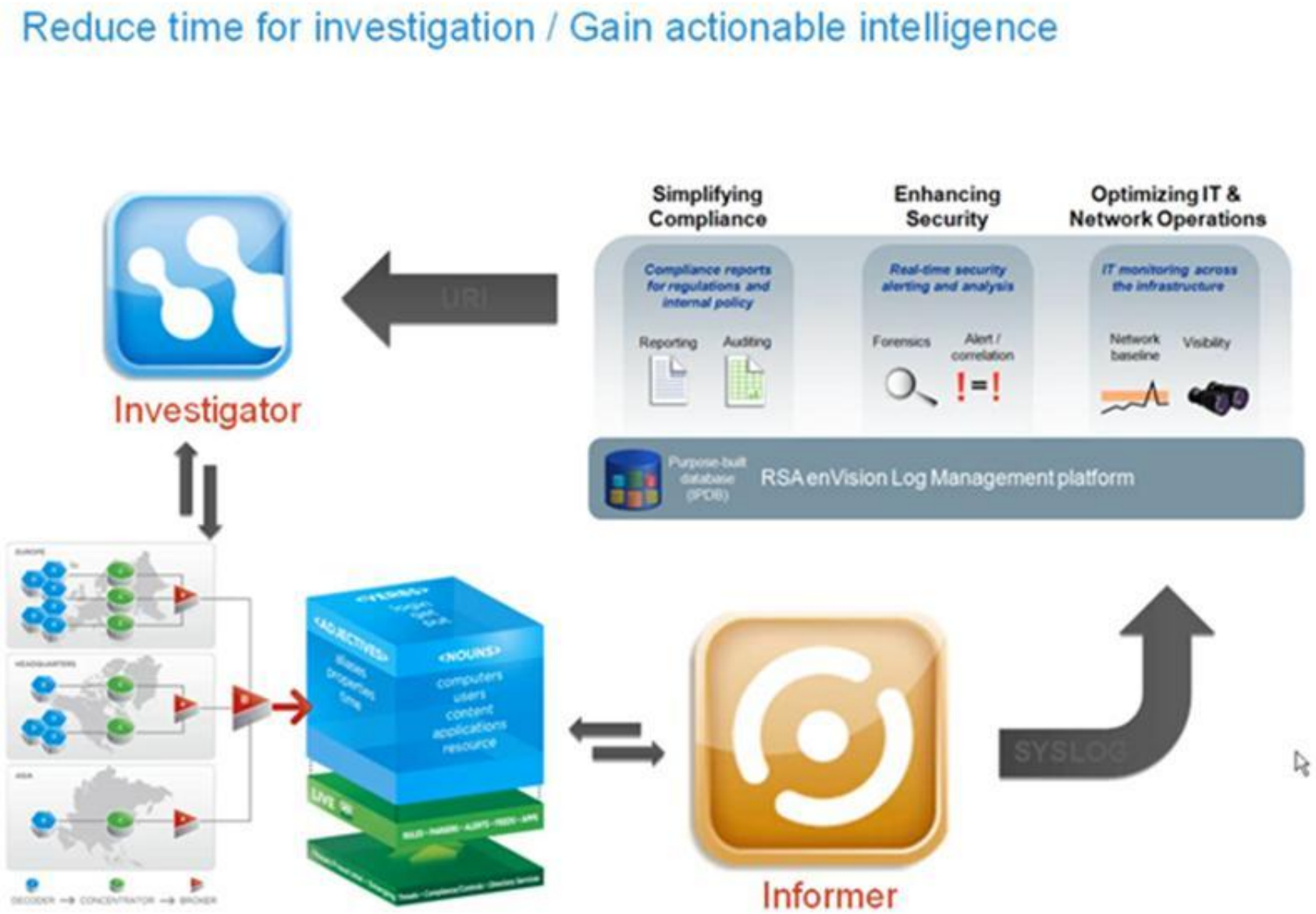
Windows приложение, обеспечивающее обмен данными NetWItness и произвольными сторонними приложениями

Совместим со всеми распространёнными SIEM, IDS/IPS и системами сетевого мониторинга

Поддерживает возможность контекстного вызова из произвольных Web консолей

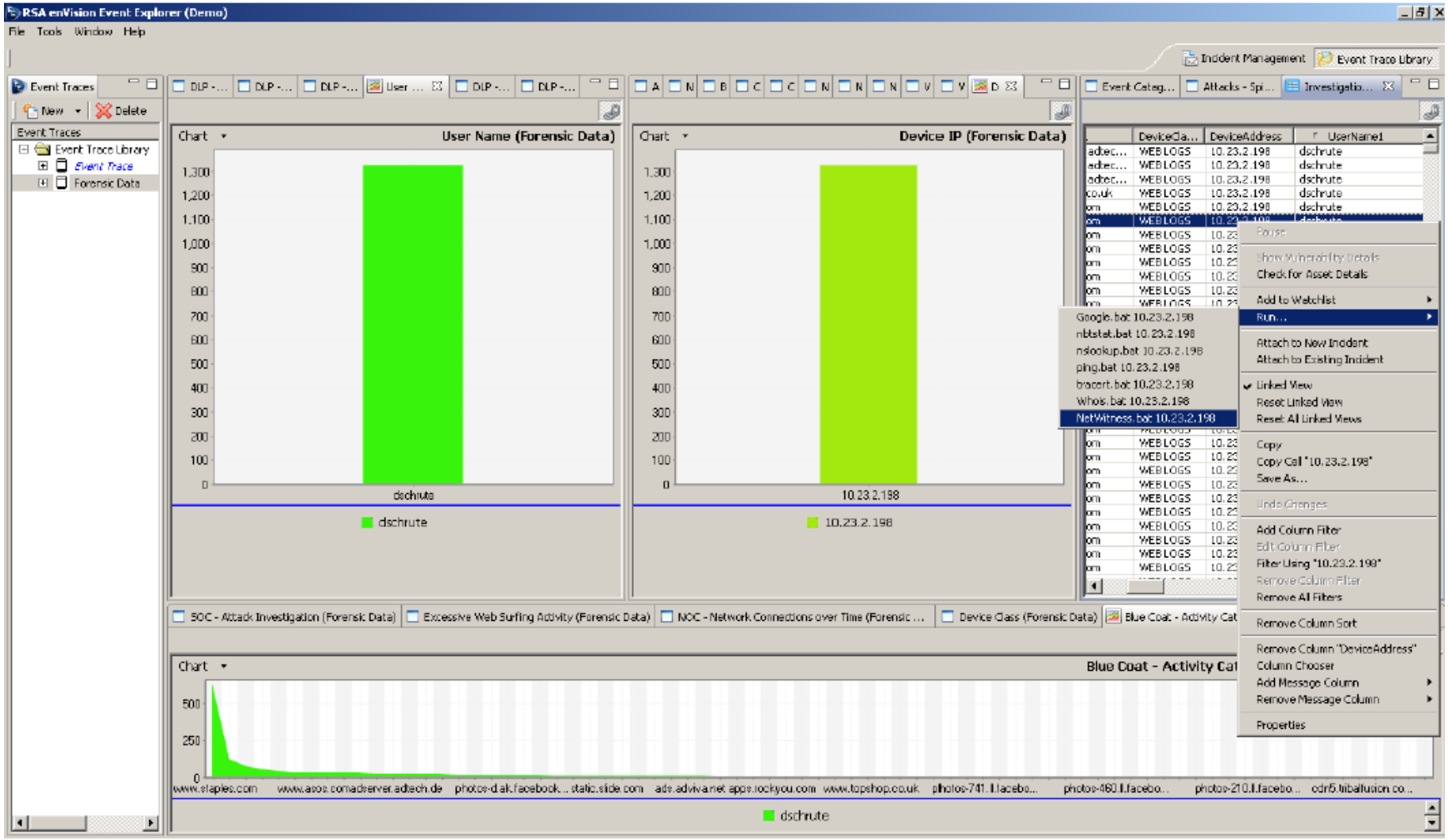
RRC

Интеграция с RSA enVision



RRC

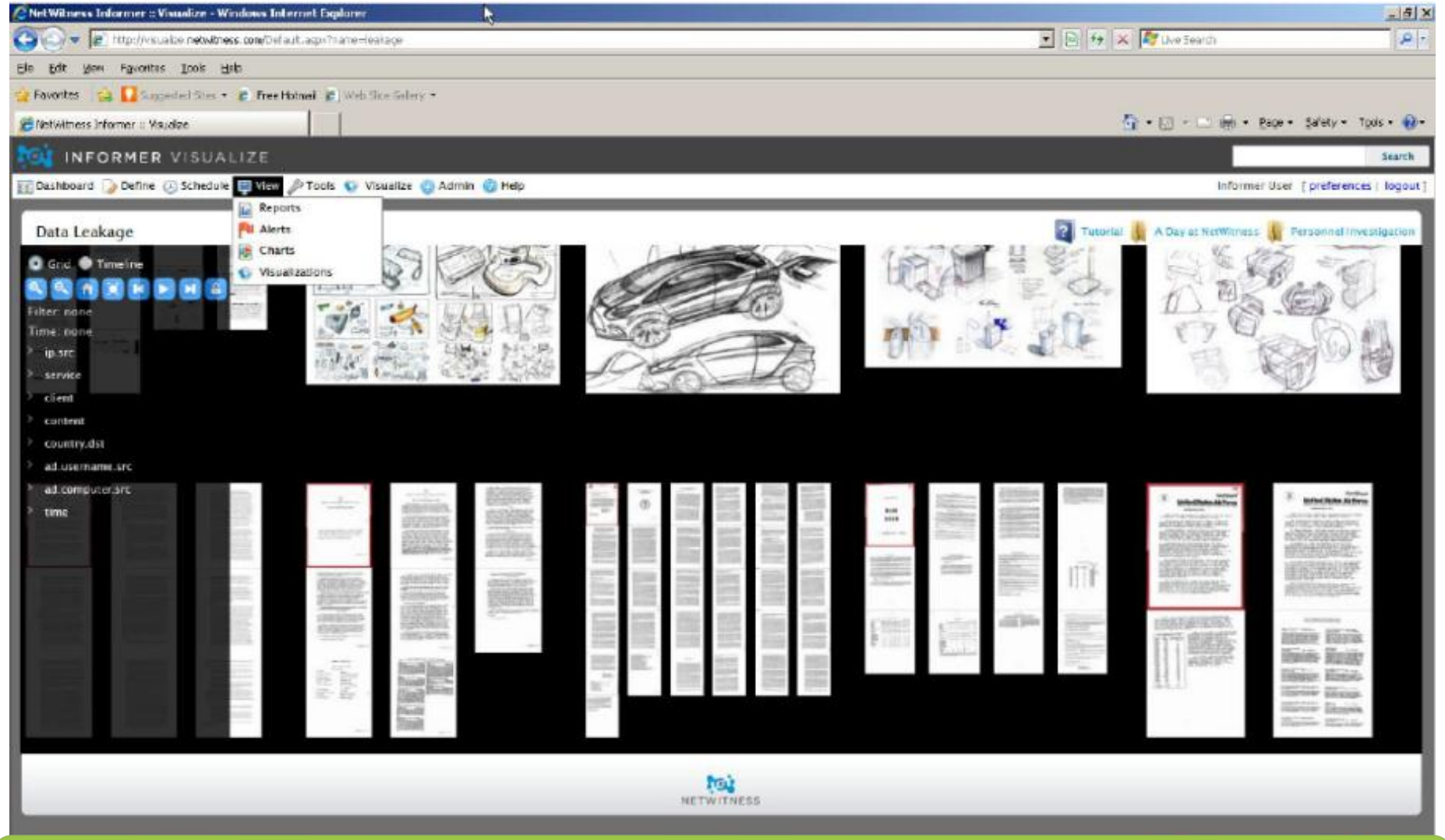
RSA enVision – ловим активность



Открываем интерфейс NetWitness из RSA enVision и смотрим, какие данные передавал пользователь, плоть до real time видео/аудио сессий

RRC

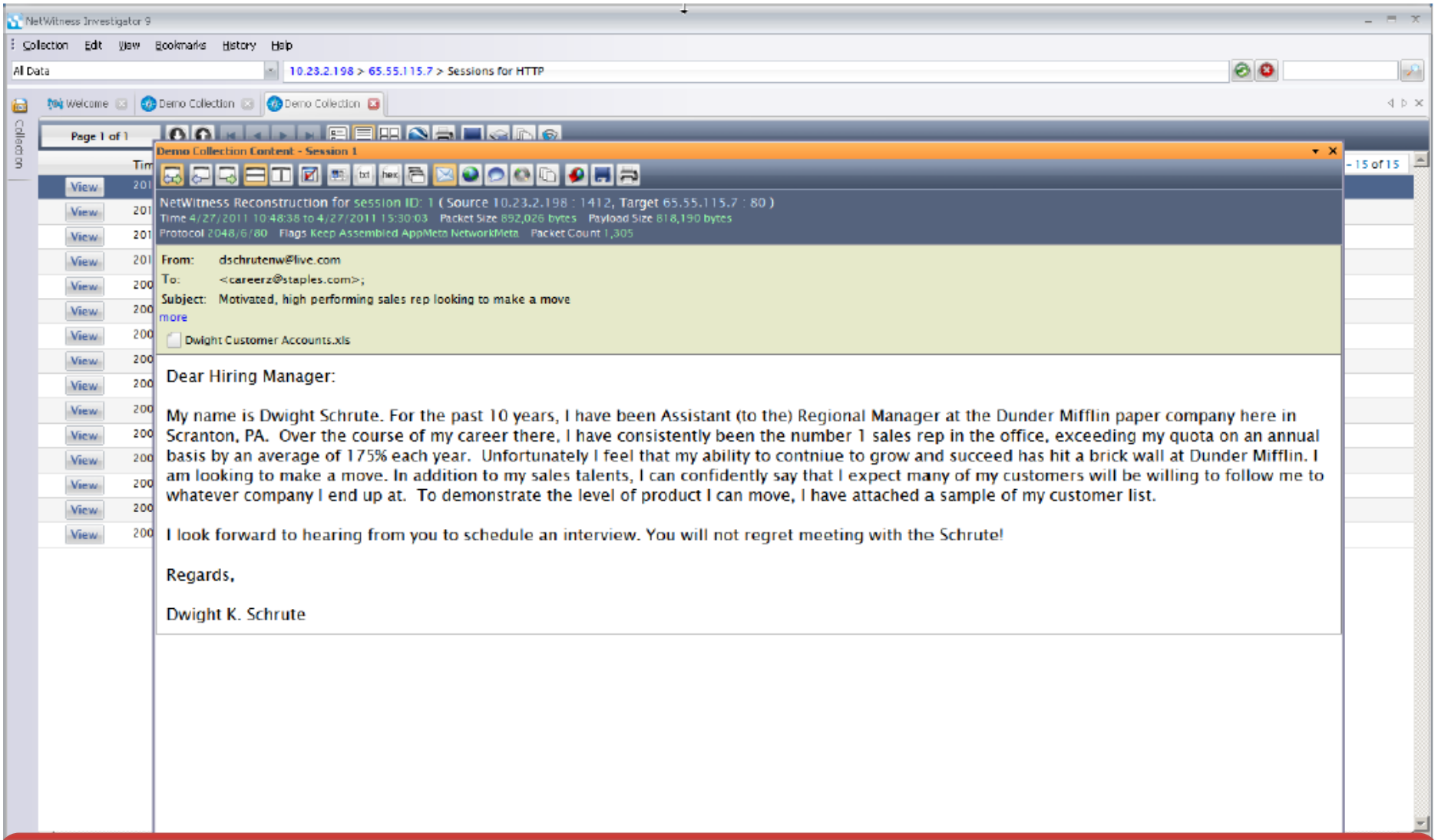
RSA enVision – пример инсайда



Возросший трафик пользователя связан с тем, что он пытается предавать конкурентам коммерчески значимую информацию

RRC

RSA enVision – пример инсайда



После этого в его планы входит занять у конкурента удобную вакансию

RRC

Аппаратное обеспечение

Portable Tactical	Branch Fixed Capacity	Data Center High Performance	Service Provider Unlimited Scalability
Usage: Incident Response Tactical Operations	Usage: Remote Office Managed Services Small Security teams	Usage: Enterprise Monitoring SOC Operations	Usage: National Monitoring Large SOC Operations Indefinite retention
NWA50 "Eagle"	NWA200 Hybrid	NWA1200/2400 Decoder	
			
	NWA100 Broker	NWA1200/2400	
			
		NWA100 Broker	
			
Features: •Briefcase form-factor •Encrypted/Removable Drives •2TB Retention	Features: •1U form-factor •Fixed capacity •Distributed visibility •8TB Retention	Features: •1U & 2U form-factors •Bandwidth Scalable •Distributed visibility •12 or 24TB Retention •DAS & SAN Storage Available	Features: •1U & 2U form-factors •Bandwidth Scalable •Distributed visibility •12 or 24TB Retention •DAS & SAN Storage Available

EMC² where information lives

NetApp

Throughput	100Mbps	250Mbps	1Gbps	10Gbps	40Gbps
Saturated Storage	1TB/day	2.5TB/day	10TB/day	100TB/day	400TB/day

Вопросы

www.netwitness.com
www.rrc.ru

Спасибо за внимание!

pkuzeev@rrc.ru
Skype – **zerottl**
+7 **985** 9994824

RSA®
The Security Division of EMC

NETWITNESS