
# EMC FORUM 2013

# LEAD YOUR TRANSFORMATION

15 октября | Москва, Центр международной торговли

## ОПЕРАТИВНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ НА БАЗЕ RSA SECURITY ANALYTICS

Александр Иржавский, НТЦ «Вулкан»

EMC²

# ПОТРЕБНОСТИ В ОПЕРАТИВНОМ АНАЛИЗЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИТ-инфраструктура и корпоративные сети становятся больше и сложнее

Атаки нарушителей становятся множественнее, динамичнее, изощреннее (APT)

Проблемы с безопасностью дорожают:

- Простои ИТ, производства, менеджмента
- Мошенничество и злоупотребления
- Утечка клиентской информации, персональных данных, ноу-хау
- Репутационные потери и отток клиентов

При этом: эффективность традиционных средств защиты мала

**60% компаний из FORTUNE500** получали на свои внутренние email адреса специально созданный вредоносный код

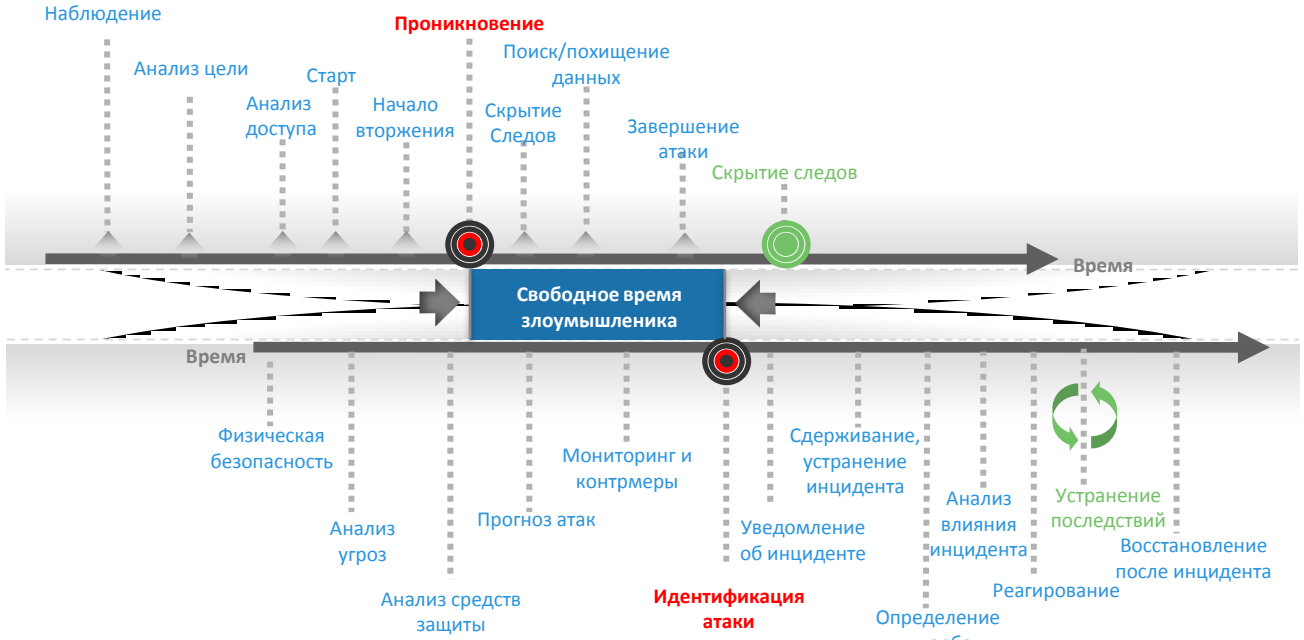
**В 88% компаний из FORTUNE500** была зарегистрирована активность ботнетов в локальных сетях

**79% успешных кибератак** требуют на расследование несколько недель

**30% из 60 миллионов** известных вариантов вредоносного кода было создано в прошлом году

Источники: RSA Security Brief, Ponemon Institute Survey Conducted «Growing Risk of Advanced Threats», Verizon 2011 Data Breach Investigations Report

# УМЕНЬШЕНИЕ СВОБОДНОГО ВРЕМЕНИ ДЛЯ ЗЛОУМЫШЛЕННИКОВ




Источник: NERC HILF Report

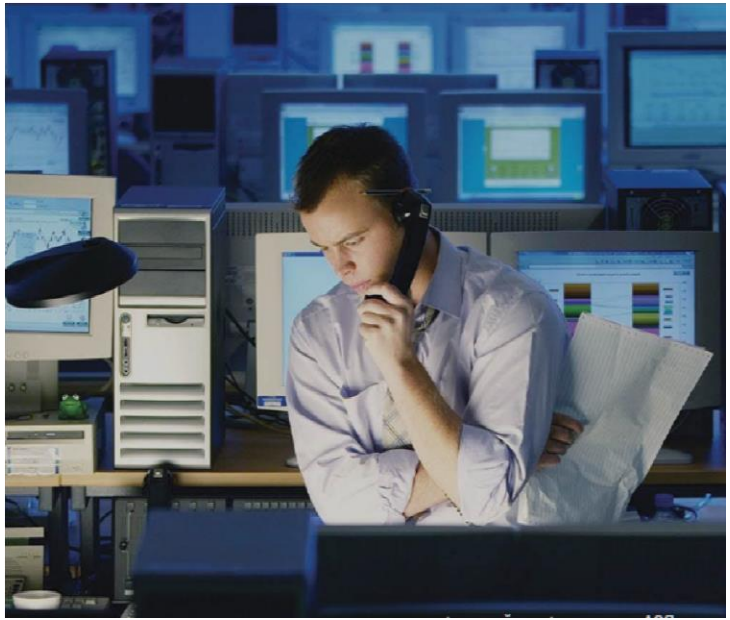
# БЕЗОПАСНОСТЬ СТАНОВИТСЯ ПРОБЛЕМОЙ БОЛЬШИХ ДАННЫХ

Высокий уровень подготовки злоумышленников означает необходимость анализа большего количества данных для идентификации атаки

Усложнение ИТ-инфраструктуры означает, что даже простые атаки можно замаскировать

Современные трудности, с которыми сталкиваются специалисты по ИБ:

- 40% опрошенных утверждают, что перегружены собираемыми данными об ИБ
- 35% опрошенных утверждают, что не имеют времени и компетенции для анализа всей собираемой информации



EMA, The Rise of Data-Driven Security, Crawford, Aug 2012

# НОВЫЕ ТРЕБОВАНИЯ К СИСТЕМАМ МОНИТОРИНГА ИБ

## Визуализация без ограничений

“Анализ всего, что происходит в ИТ-инфраструктуре”

## Оперативная аналитика

“Анализ и расследование потенциальных угроз в режиме, близком к реальному времени”

## “Интеллектуальные данные об угрозах”

“Идентификация целей, угроз и инцидентов ”

## Масштабируемость

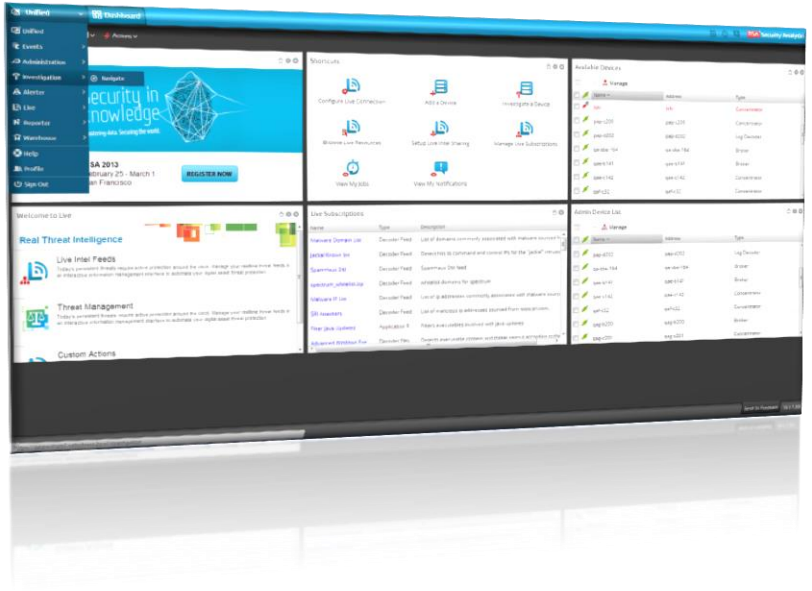
“Хранение и анализ как оперативных, так и долговременных даннных”

# ЧТО ТАКОЕ SECURITY ANALYTICS?

RSA Security Analytics – новый подход к
борьбе с угрозами повышенной сложности (APT)

Унифицированная платформа нового поколения для:

- Мониторинга безопасности
- Расследования инцидентов
- Отчетности о соответствии требованиям




RSA Security Analytics объединяет три технологии:

- традиционные средства SIEM
- средства мониторинга сетевой безопасности
- технологии обработки и анализа Больших Данных

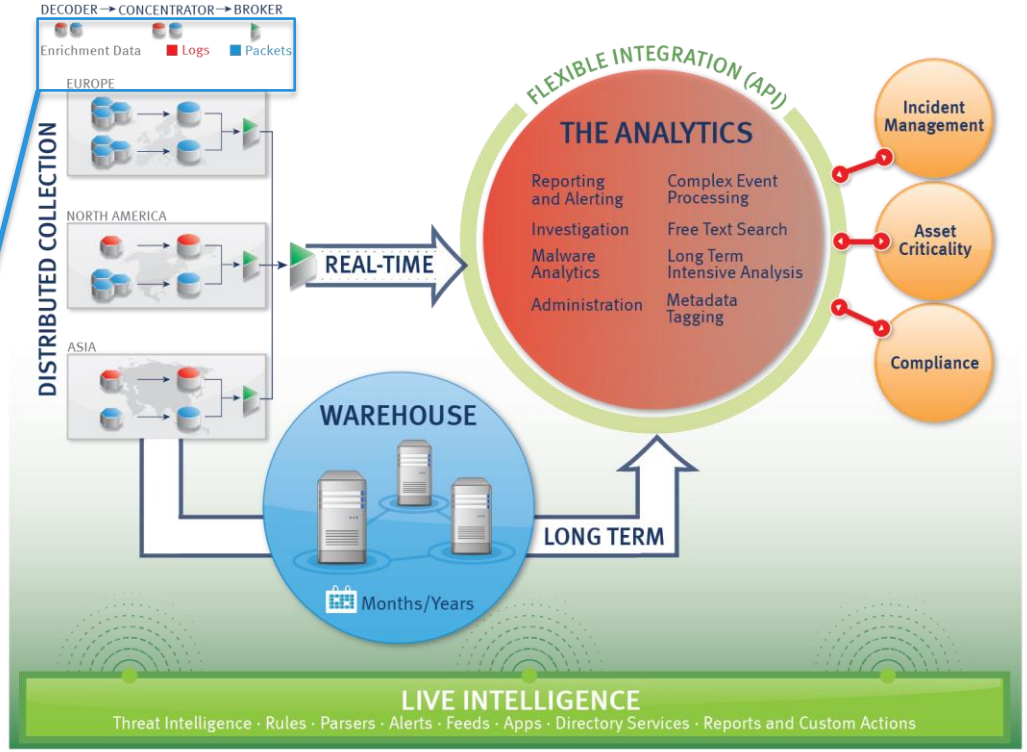
Главное отличие
Security Analytics
от других систем мониторинга ИБ

# АРХИТЕКТУРА
# RSA SECURITY ANALYTICS

Инфраструктура сбора данных
RSA NetWitness NextGen:

- Единая платформа для сбора и анализа:
  - информации о сетевом трафике
  - журналов событий

- Распределенная масштабируемая архитектура

# КОНСОЛИДАЦИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ДАННЫХ ОБ УГРОЗАХ


Сбор информации об интеллектуальных угрозах от сообщества ИБ & RSA FirstWatch

➔

Агрегация и консолидация наиболее значимой информации об угрозах и ее объединение с данными организации

➔

Автоматические обновления корреляционных правил, парсеров, отчетов, feed-ов, «черные» списки

Возможность воспользоваться сторонними данными об обнаруженных угрозах и применять их для анализа текущих и исторических данных

# RSA SECURITY ANALYTICS WAREHOUSE


Долгосрочное хранение и анализ

- Warehouse, оптимизированный для хранения данных ИБ
- Хранение метаданных сетевых пакетов и журналов событий, «сырых» журналов

Архитектура Hadoop для максимальной гибкости и масштабирования

Сложная обработка событий

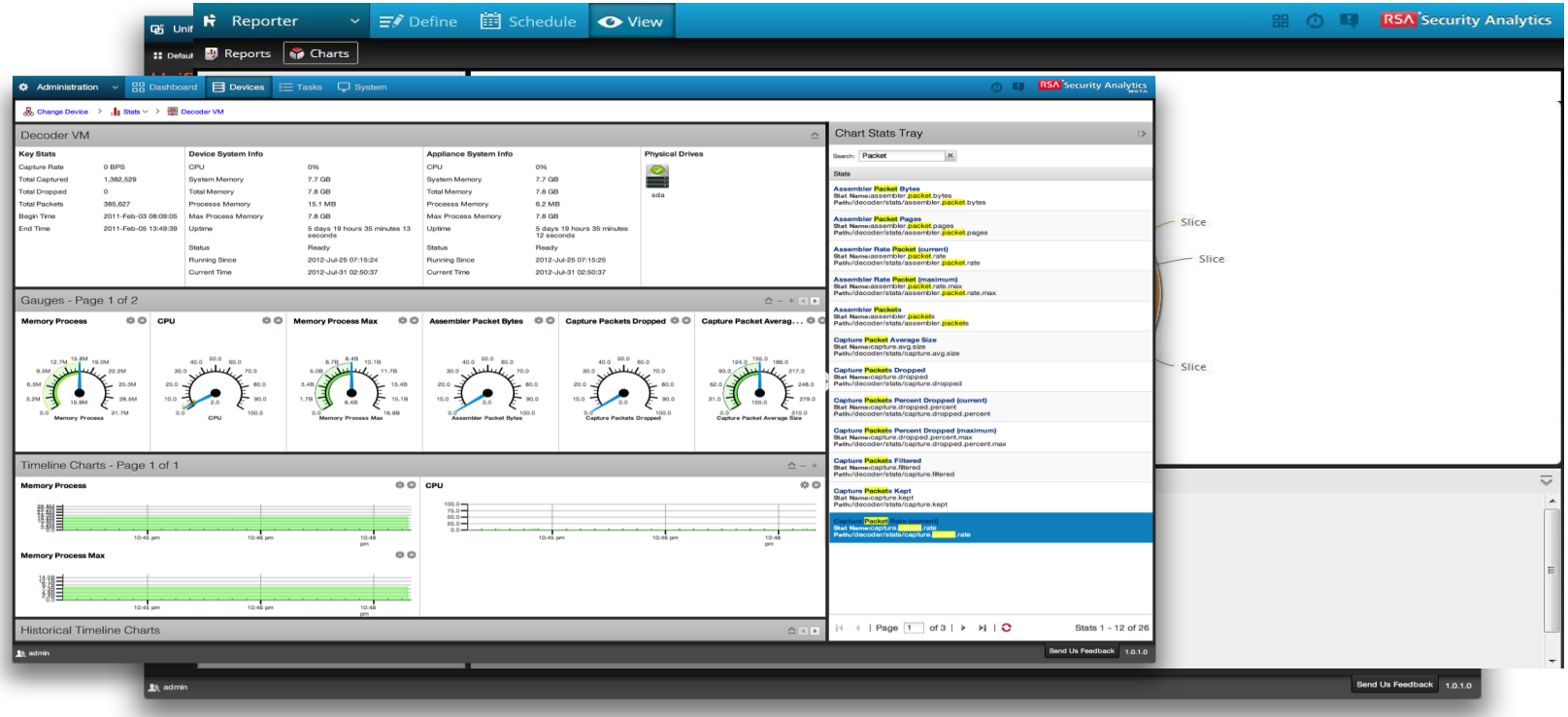
«Google-подобный» текстовый поиск

Соответствие требованиям регуляторов по долгосрочному хранению

# МОЩНАЯ АНАЛИТИКА RSA SECURITY ANALYTICS

- Всесторонний анализ ИБ организации
- Мониторинг в реальном времени и развитые средства расследований
- Интуитивно понятные аналитические средства
- Использование бизнес-контекста при расследованиях
- Автоматическая генерация разнообразных отчетов, включая отчеты за большие промежутки времени

# УНИФИЦИРОВАННЫЙ ИНТЕРФЕЙС RSA SECURITY ANALYTICS

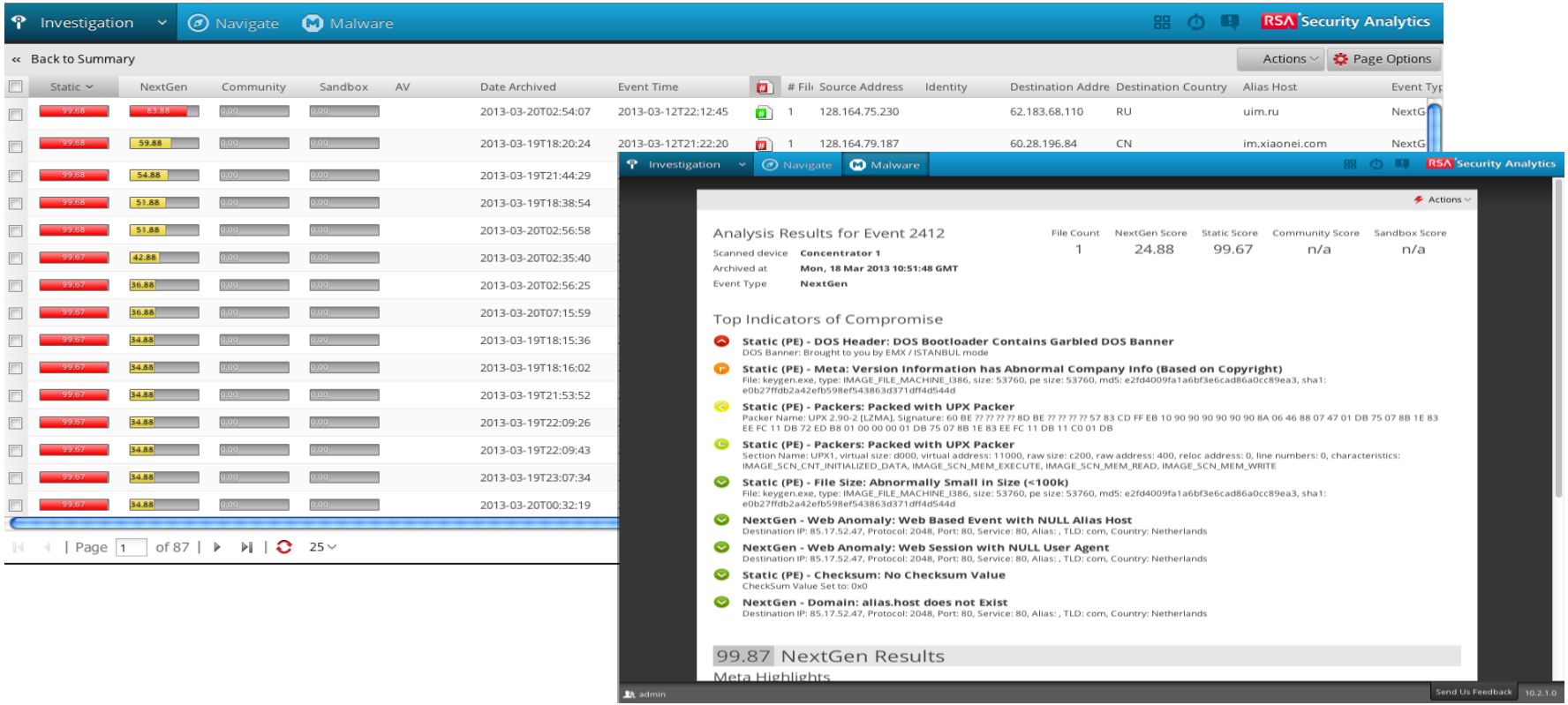


# АНАЛИЗ ВРЕДОНОСНОГО КОДА БЕЗ ИСПОЛЬЗОВАНИЯ СИГНАТУР

SA анализирует ВСЕ что происходит в сети по ВСЕМ протоколам, включая ВСЕ «исполняемое» содержимое.

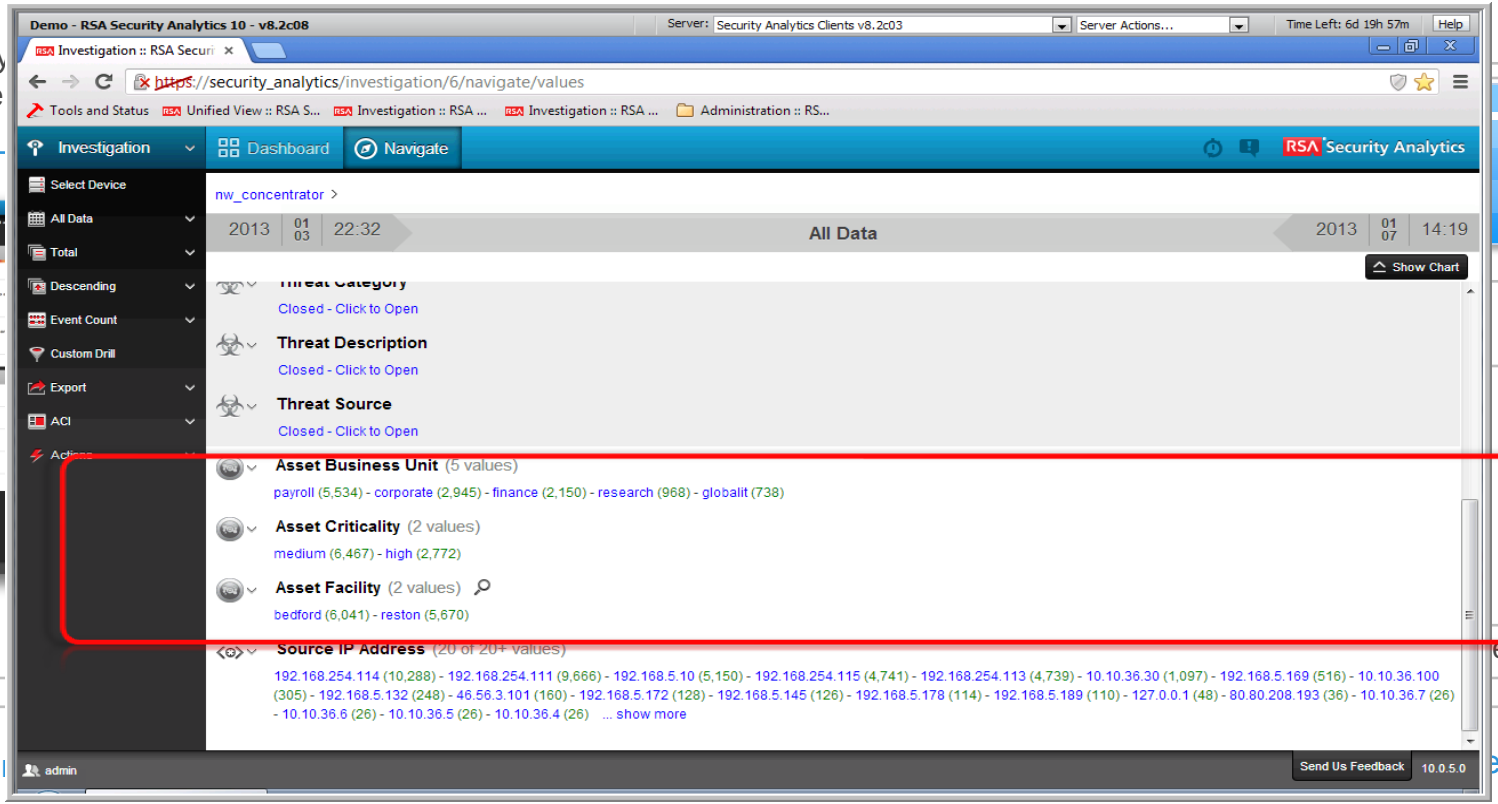
| | |
|---|---|
| NextGen | •Анализирует появление файла в сети и соответствующие сетевые сессии<br>*Например: страна происхождения, время создания, размер содержимого* |
| Статический анализ файла | •JavaScript / Obfuscation, PDF Executable, Alerts present<br>•Size, Meta Tags, Cleaned, Packed, Obfuscated, и т.д. |
| Community | •Анализ информации из внешних источников - информационных и репутационных партнеров |
| Sandbox | •Анализ поведения файлов в защищенной виртуальной среде<br>•Может использоваться локально или как SaaS-подписка |

# АВТОМАТИЧЕСКИЙ СКОРИНГ ВРЕДОНОСНОГО КОДА



# ИСПОЛЬЗОВАНИЕ БИЗНЕС-КОНТЕКСТА

Security Analy
бизнес-конте




Данн

ecurity

елях

# РЕЗУЛЬТАТ

Уменьшение риска интеллектуальных целевых атак

Уменьшение времени анализа с нескольких дней до нескольких минут

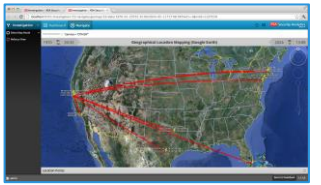
Уменьшение свободного времени злоумышленников

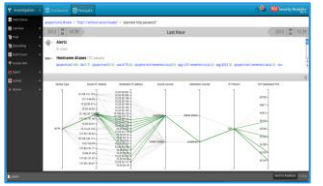
Повышение эффективности процессов обеспечения ИБ

Навыки подразделений ИБ улучшаются за счет использования интеллектуальных данных

Информация хранится централизованно, и расследования проводятся значительно быстрее

Применяется более гибкая модель управления безопасностью на основе анализа рисков





# ЧТО ПОСТАВЛЯЕТСЯ?

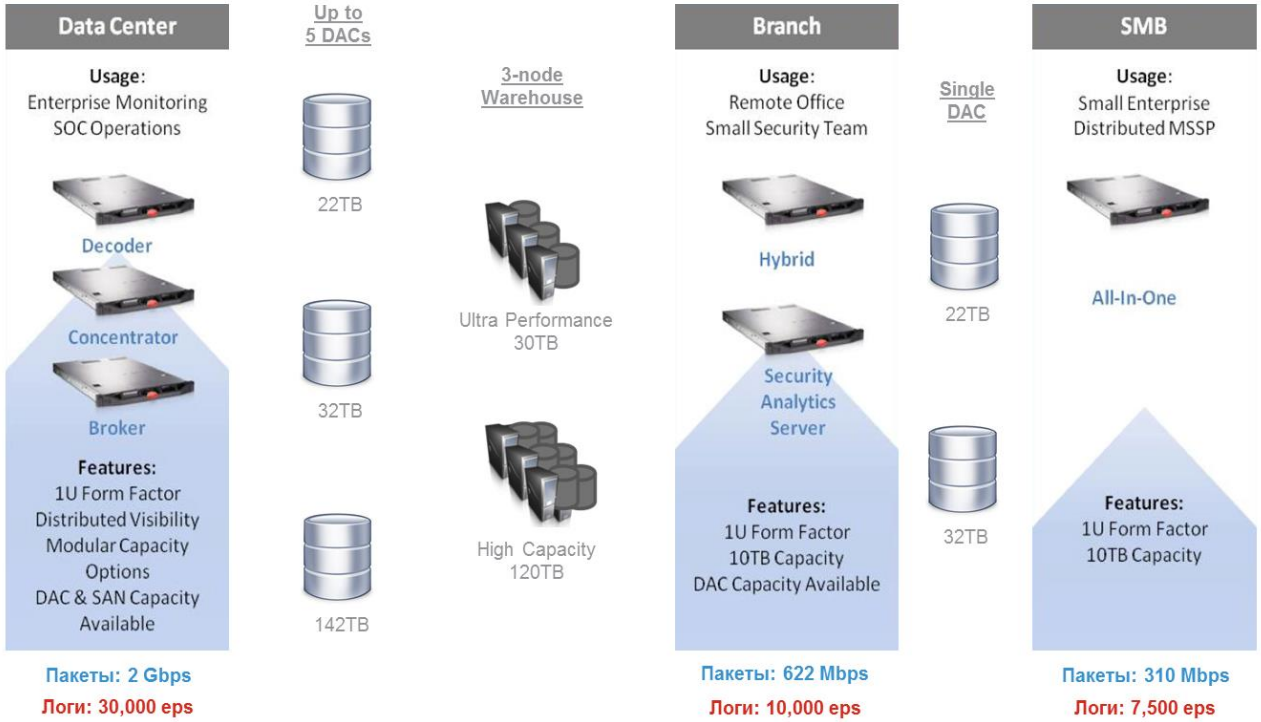
**Единая аппаратная платформа**

- Для всех компонентов (Decoder, Concentrator, Broker)
- Decoder и Concentrator используют либо SAN либо Direct Attached Capacity (DAC)

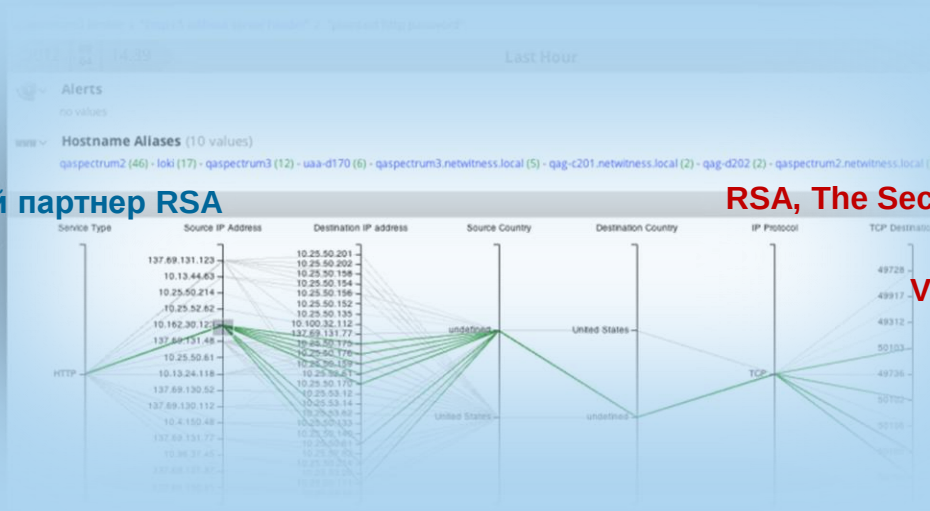
**Хранение данных:**

- Direct Attached Capacity (DAC)
  - Подключение через SAS
  - Высокая емкость 32TB (для Decoder)
  - Высокая производительность 17.4 TB (для Concentrator)
- SAN
  - Подключение через Fiber Channel
  - Высокоемкостные и высокопроизводительные конфигурации
  - От 46TB до 1.5 PB (XXL) общей емкости

# ВАРИАНТЫ КОМПЛЕКТАЦИИ



# ГДЕ ПОДРОБНЕЕ ОЗНАКОМИТЬСЯ И ПРОТЕСТИРОВАТЬ РЕШЕНИЕ?




**Александр Иржавский**
**НТЦ «Вулкан», официальный партнер RSA**

**A.Irzhavsky@ntc-vulkan.ru**
**+7 (495) 663-95-16**

**Владимир Вакациенко**
**RSA, The Security Division of EMC - Россия**

**Vladimir.Vakatsienko@emc.com**
**+7 (495) 785-66-22**

# СПАСИБО ЗА ВНИМАНИЕ!

КОНТАКТЫ
Александр Иржавский
a.irzhavsky@ntc-vulkan.ru


EMC²