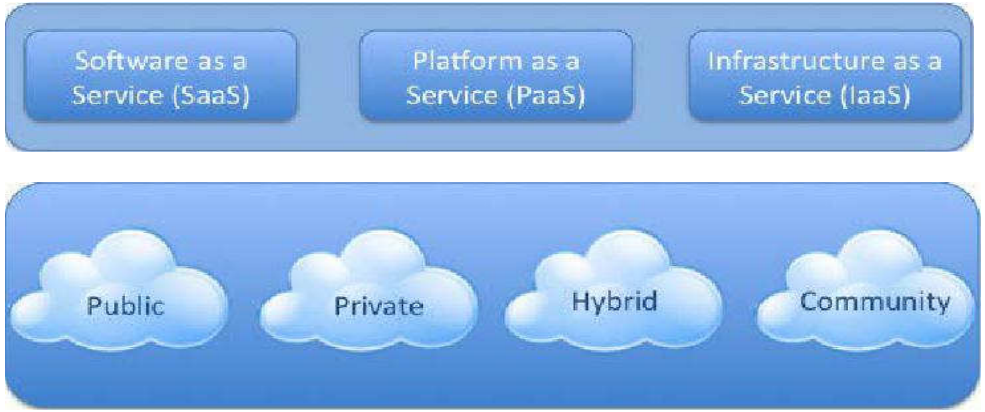
EMC FORUM 2012
ТРАНСФОРМИРУЙ
ИТ+БИЗНЕС+СЕБЯ

RSA NetWitness – система сбора и анализа сетевого трафика. Анализ информационного взаимодействия в «облаке»

Руководитель отдела НТЦ «Вулкан»
Александр Кузнецов

Информационное взаимодействие в «облаке»

- **Различные** ресурсы предоставляются **различным** лицам для решения **разнонаправленных** задач
- Ресурсы могут быть «белыми», «черными» и «серыми» ящиками



Кадр из мультфильма «По дороге с облаками»

Новые ИБ-потребности для «облака» и не только …

- Сокращение времени между началом атаки и ее идентификацией
- Наличие максимального объема данных для расследования инцидентов ИБ
- Качественная и интерактивная визуализация оперативной информации о сетевой активности и состоянии защищенности

Кадры из мультфильма «Partly cloudy»

Обеспечение ИБ «облака»

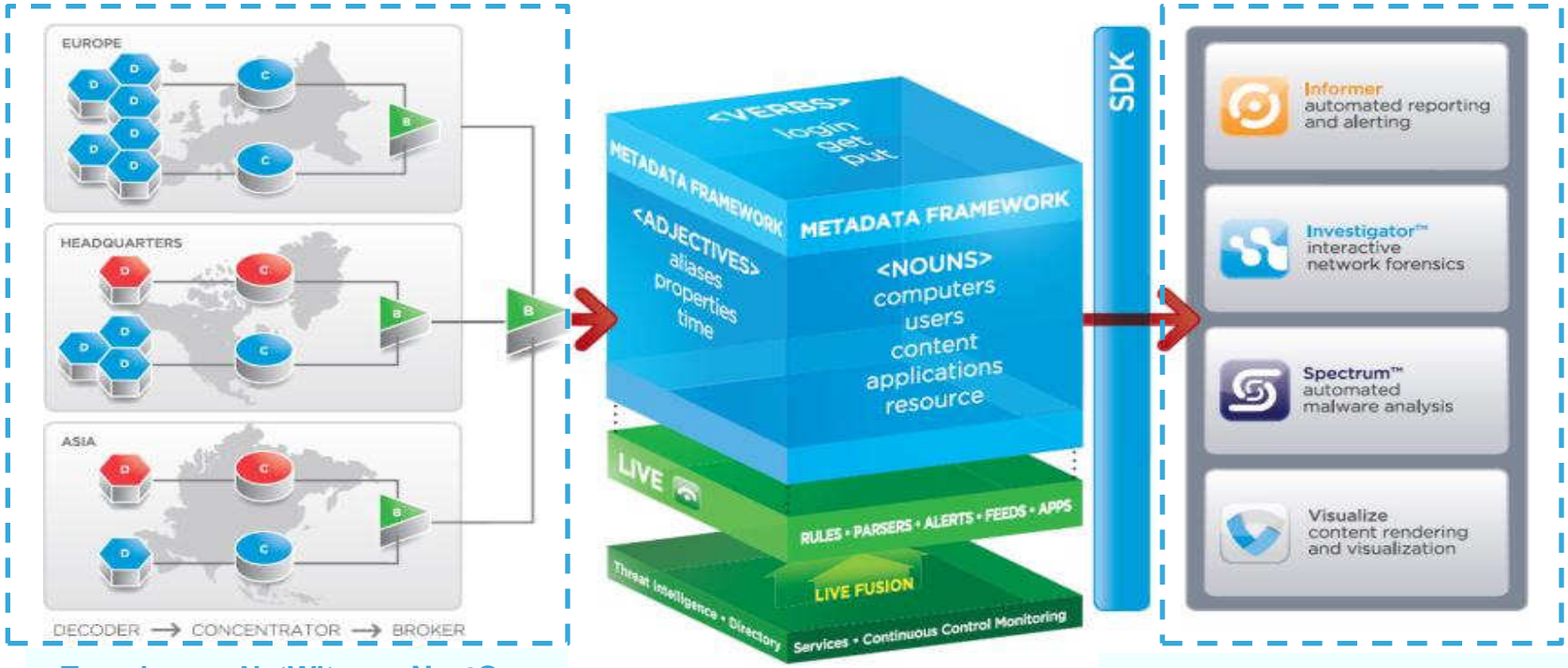
- Изолированность модели предоставления услуг
- Контроль действий системных администраторов провайдера
- Обеспечение конфиденциальности данных с возможностью контроля состояния защищенности со стороны клиента
- Гарантированное удаление данных

Возможности RSA NetWitness

RSA® NETWITNESS

- Сбор, хранение и обработка всех проходящих по сети пакетов
- Анализ гигантских (терабайты) объемов данных
- Восстановление, визуализация и интерактивный анализ сетевых сессий с интуитивно понятным представлением данных (голос, файлы, почтовые сообщения, диалоги IM, web-страницы)
- Контекстный поиск по содержимому сессий
- Выделение и анализ метаданных сетевых сессий
- Автоматизированный бессигнатурный поиск вредоносного ПО в сетевом трафике с приоритезацией угроз
- Формирование многоуровневой отчетности

Архитектура RSA NetWitness



Платформа NetWitness NextGen

Решения NetWitness AppSuite

Платформа NetWitness NextGen

- **Decoder** – устройство-сниффер
- **Concentrator** – объединяет метаданные для анализа
- **Broker** – устройство, обрабатывающие запросы

Модельный ряд NetWitness NextGen

Portable Tactical	Branch Fixed Capacity	Data Center High Performance	Service Provider Unlimited Scalability
Варианты использования: Incident Response, Tactical Operations	Remote Office, Managed Services, Small Security teams	Enterprise Monitoring, SOC Operations	National Monitoring, Large SOC Operations, Indefinite retention
NWA50 "Eagle" 	NWA200 Hybrid  NWA100 Broker 	SMC S4  Broker, Concentrator, Decoder	
Пропускная способность	100Mbps	250Mbps	1Gbps	10Gbps	40Gbps
Расчет хранения	1TB/day	2.5TB/day	10TB/day	100TB/day	400TB/day

Вопрос хранения – «большой» вопрос

- 100 Мбит/с ~ 1Тбайт/день HDD с каждой точки сбора
- «+ 10%» от данного объема для метаданных

NetWitness AppSuite – Informer

- Формирование отчетности и оповещений об обнаруженных угрозах, в том числе поддерживается экспорт данных во внешние система (форматы HTML, CSV и PDF)

- Визуализация сетевых сессий (изображений, файлов, аудио и т.д.) с поддержкой multi-touch и drill-down

NetWitness AppSuite – Investigator

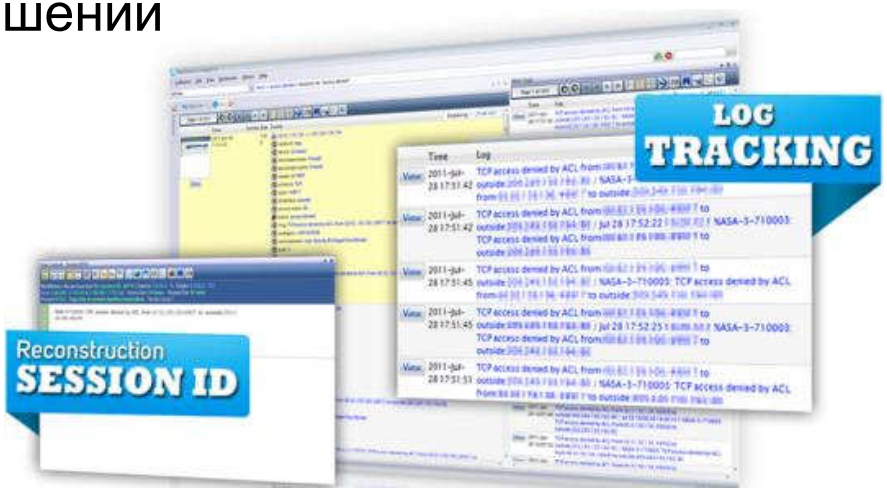
- Работа с метаданными и интерактивный анализ содержимого сетевых сессий, а также интуитивное представление результатов обработки

NetWitness AppSuite – Spectrum

- Бессигнатурный анализ вредоносного ПО на основе тысяч критериев и показателей
- Выявление «постоянных угроз повышенной сложности» (APT)

NetWitness AppSuite – NetWitness to Log

- Корреляционный анализ данных из журналов событий и данных о сетевой активности
- Расширяет аналитические возможности SIEM-платформы RSA enVision, а также других SIEM-решений



NetWitness AppSuite – Live

- Сервис глобального анализа угроз, предоставляющий оповещения, отчеты и индикаторы различных угроз
- Три уровня: **Basic**, **Enhanced** и **Premium**

- Informer Threat / Security Reports
- Zero-Day Indicators / Compromise Indicators
- RSA Security Threat Blacklist
- NetWitness Identity (AD Integration)
- Verisign® iDefense®

Преимущества

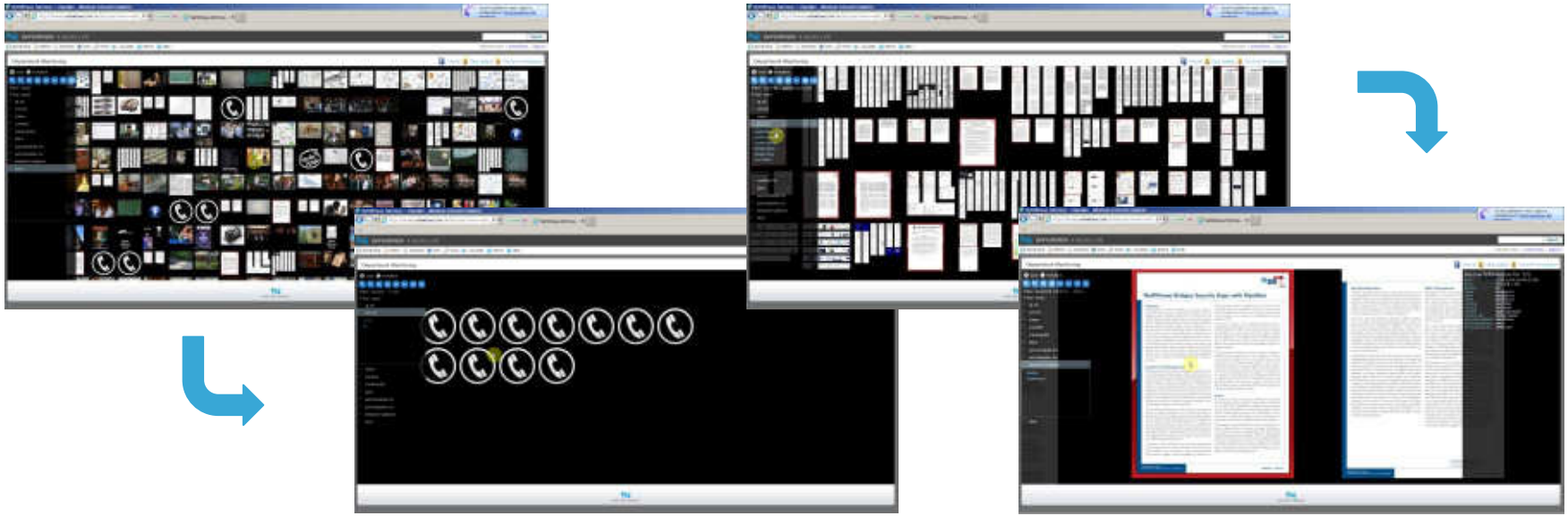
- **Обработка данных:** на уровне ПО (гибкость)
- **Балансировка нагрузки:** иерархическая архитектура
- **Описание метаданных:** с использованием XML разметки (гибкость настройки)
- **Приложения для обработки данных:** большой выбор из NetWitness AppSuite

Результаты применения RSA NetWitness

- Понимание «чем дышит» сетевая ИТ-инфраструктура
- Уменьшение времени реакции персонала на ИБ-инциденты и прерывания в оказании ИТ-услуг
- Оперативная визуализация информации о сетевой активности
- Доказательная база для расследования ИБ-инцидентов
- Статистические данные для анализа рисков ИБ
- Корреляция и аналитика

Visualize

- Техническая демонстрация



Спасибо за внимание!
Ваши вопросы…

EMC FORUM 2012
ТРАНСФОРМИРУЙ
ИТ+БИЗНЕС+СЕБЯ

Научно-технический центр «Вулкан»
105318 г. Москва, ул. Ибрагимова, д. 31, корп. 50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru