ДиалогНаука

19 ноября 2013 г.

Обзор современных технологий и программного обеспечения для защиты от инсайдеров

Websense DSS

NetWitness (RSA Security Analytics)

Ванерке Роман

ЗАО «ДиалогНаука»

О компании «ДиалогНаука»

- ЗАО «ДиалогНаука» создано 31 января 1992 года. Учредители - СП «Диалог» и Вычислительный центр РАН.
- Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были Aidstest, ADinf, Sheriff, Doctor Web и DSAV.
- С 2004 года по настоящее время «ДиалогНаука» - системный интегратор, консультант и поставщик комплексных решений в сфере защиты информации.

ДиалОгНаука

Базовые понятия

- **Информация ограниченного доступа (ИОД)** - информация представляющая ценность для ее владельца, доступ к которой ограничивается на законном основании
- **Инсайдер (внутренний злоумышленник)** – сотрудник Компании, член какой-либо группы людей, имеющей доступ к ИОД, недоступной широкой публике. Может действовать изнутри Компании
- **Внешний злоумышленник (хакерство, вредоносный код)** – постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Действует извне, за периметром Компании.

Что является ценным для Компании?

Клиентская база (физические и юридические лица)

Схемы работы

Условия работы

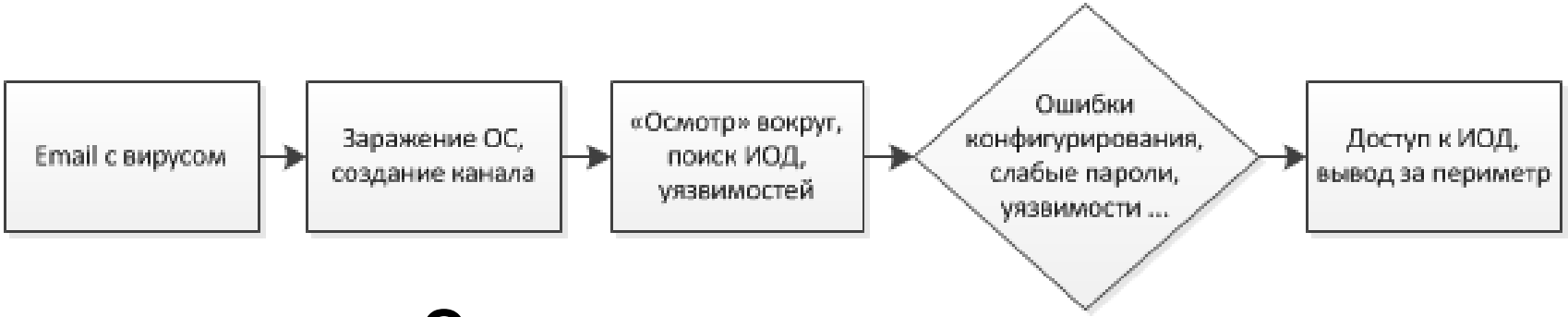
Стратегические планы, новые продукты, изменения, маркетинговые акции

Персональные данные, HR и прочее

ДиалОгНаука

Кому это может быть интересно?

- **Внешний злоумышленник** – кража информации с целью перепродажи (хакеры, конкуренты)
  - Хакерство (использование различных уязвимостей), вредоносный код
  - Web, Email
- **Внутренний злоумышленник** (инсайдер) – выгодно продать, открыть свой бизнес, попросить повышения
  - Прямой доступ к данным
  - Web, Email, USB, IM (Skype, ICQ)

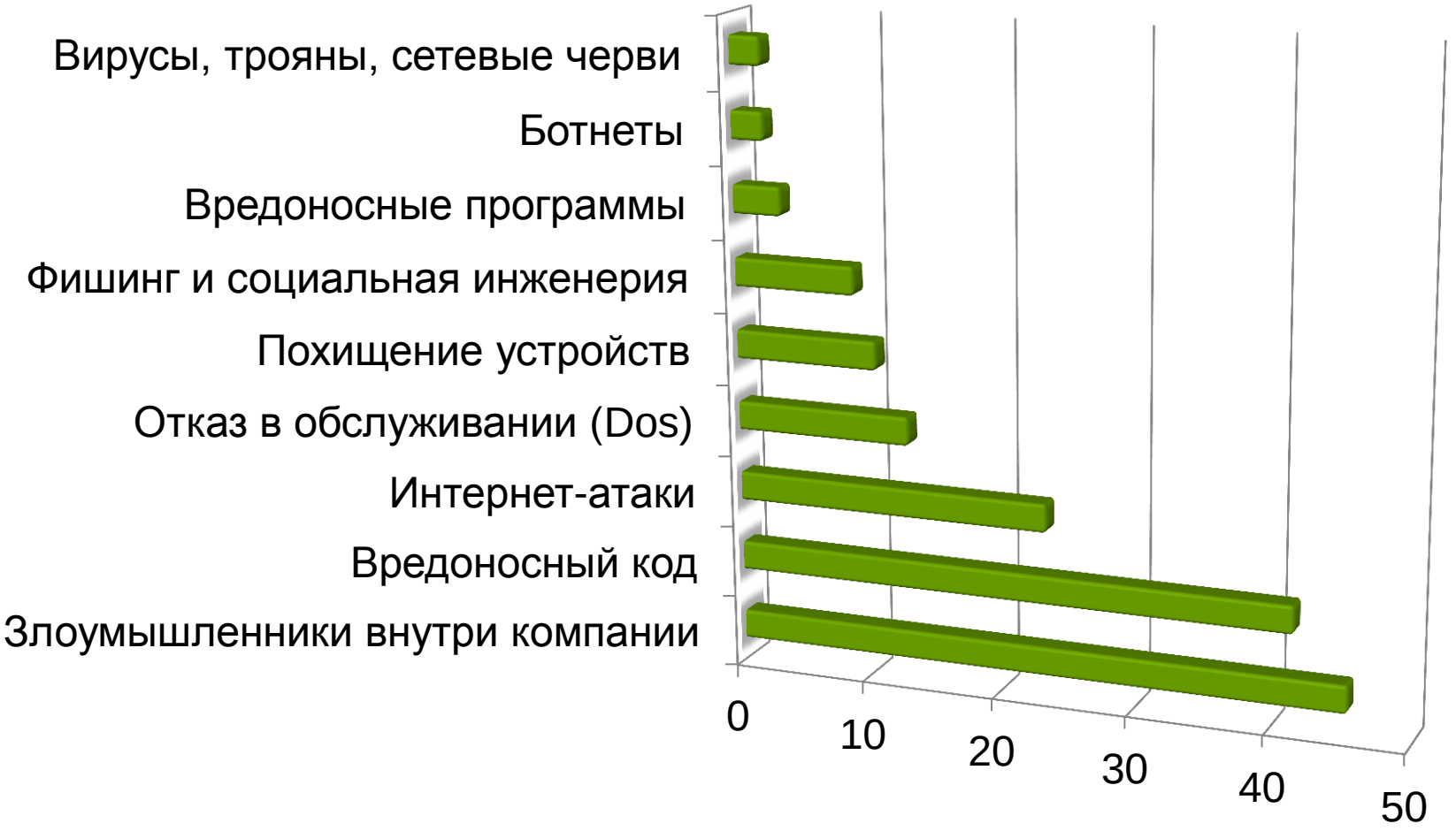


Основные этапы атаки

ДиалогНаука

Статистика обнаружения инцидентов

Среднее время обнаружения атак в днях



ДиалогНаука

Последствия от утечек

- Прямые, финансовые убытки (уход клиентов к конкурентам, потеря контрактов и т.д.)
- Потеря лояльности клиентов, партнеров, репутационный ущерб
- Потеря производительности (нарушение бизнес-процессов в Компании)
- Преследование по закону (штрафы, судебные разбирательства)

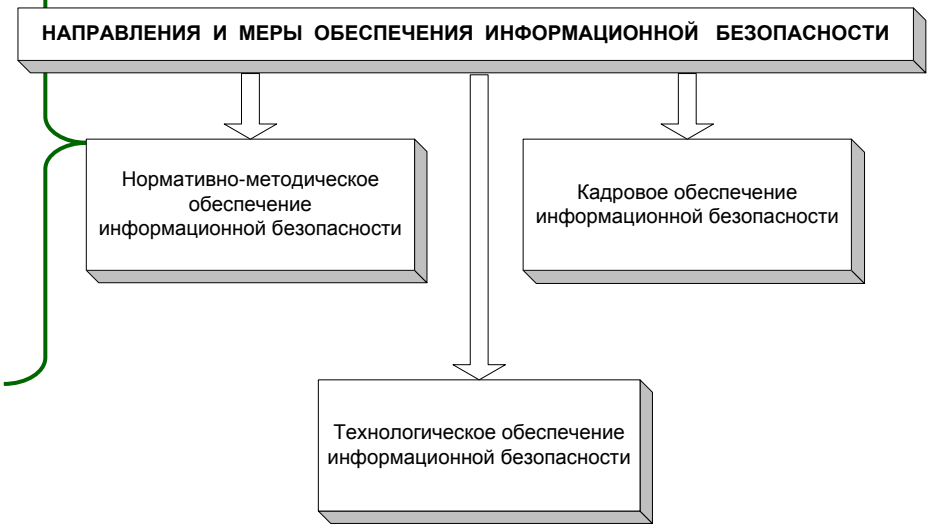
ДиалогНаука

Зачем защищаться?

- Минимизация рисков
- Соответствие требованиям (Compliance)
  - ФЗ о ПДн
  - Соглашения с контрагентами
  - PCI DSS
  - ISO 27000
- Повышение эффективности бизнеса (увеличение выручки)
- Уменьшение стоимости продуктов и услуг

Основные этапы проекта построения комплексной системы защиты от утечек

- Идентификация и классификация ИОД, определение собственников информации, бизнес-процессы
- Приоритезация ИОД по степени риска, требованиям аудита и регуляторов
- Определение политик хранения, обработки и передачи, как часть общего подхода к защите ИОД
- Выбор и развертывание системы защиты от утечек
- Разработка документации, обучение сотрудников
- Превентивное автоматическое реагирование
- Регулярный контроль и оценка эффективности



ДиалогНаука

Документы

ДиалогНаука

Техника

- Использование современных решений для выявления утечек ИОД
  - Анализатор информации на основе многих алгоритмов детектирования и измерения степени схожести
  - Охват всех основных каналов бизнес-коммуникаций
  - Автоматизированная система учета и обработки инцидентов
  - Отчеты для задач управления рисками на предприятии
- Обеспечение антивирусной защиты, реализация системы управления уязвимостями, регулярный анализ правил МЭ, построение системы управления доступ
- Создание системы мониторинга информационной безопасности

ДиалогНаука

Люди

- Обучение администраторов безопасности, ответственных за установку и обслуживание средств защиты
- Обучение пользователей, работающих со средствами защиты
- Аттестация специалистов по результатам программы обучения
- Укомплектование подразделений предприятия сотрудниками, ответственными за выполнение работ по защите от угроз безопасности

ДиалогНаука

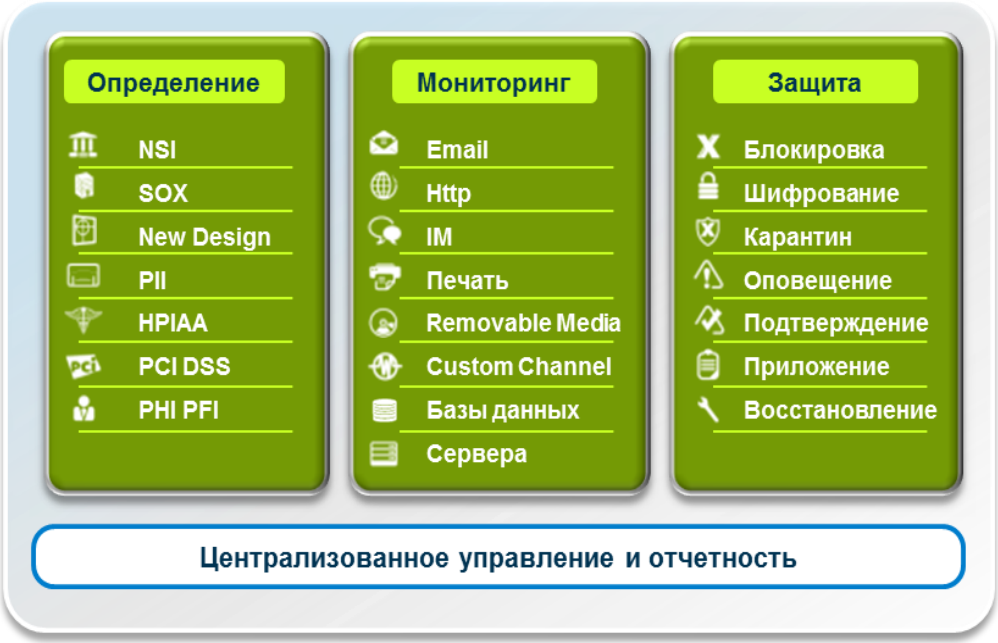
Websense Data Security

ДиалогНаука

Websense Data Security Suite

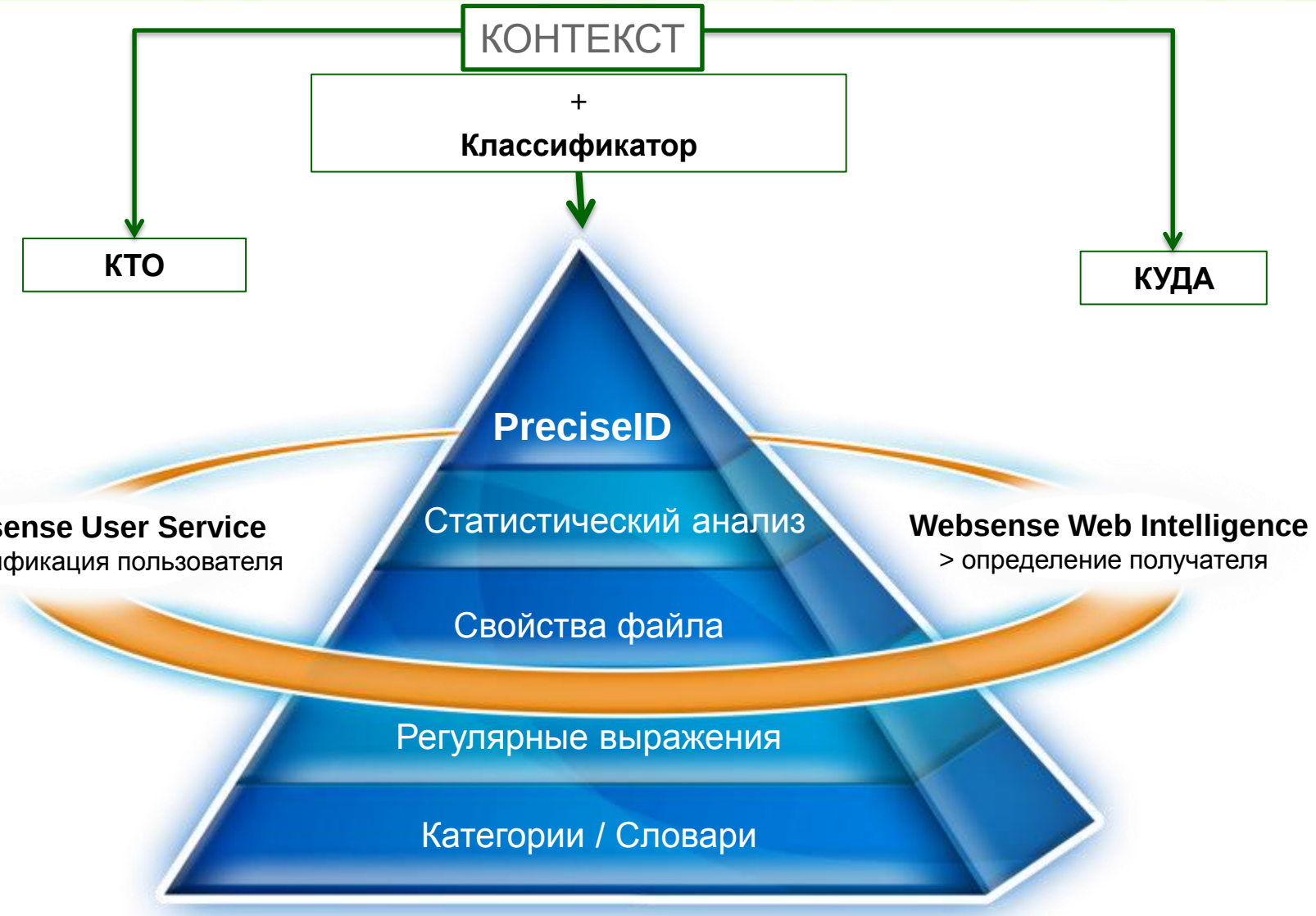
Лидирующая на рынке технология DLP для обнаружения, мониторинга и защиты конфиденциальных данных

- Единые политики
  - Предлагает унифицированный механизм создания политик
  - Управление всеми аспектами политики Data Loss Prevention
  - Мощные возможности мониторинга по отслеживанию всех изменений данных (хранимых и при перемещении)
- Низкая TCO и сложность
  - Модульная архитектура позволяет наиболее гибко соответствовать требованиям покупателя
  - Простое развертывание и меньшее число серверов



ДиалогНаука

Контекстный анализ



ДиалогНаука

Websense Data Security

Технологии идентификации ИОД

ДиалогНаука

Технологии идентификации

Готовые политики

Цифровые отпечатки

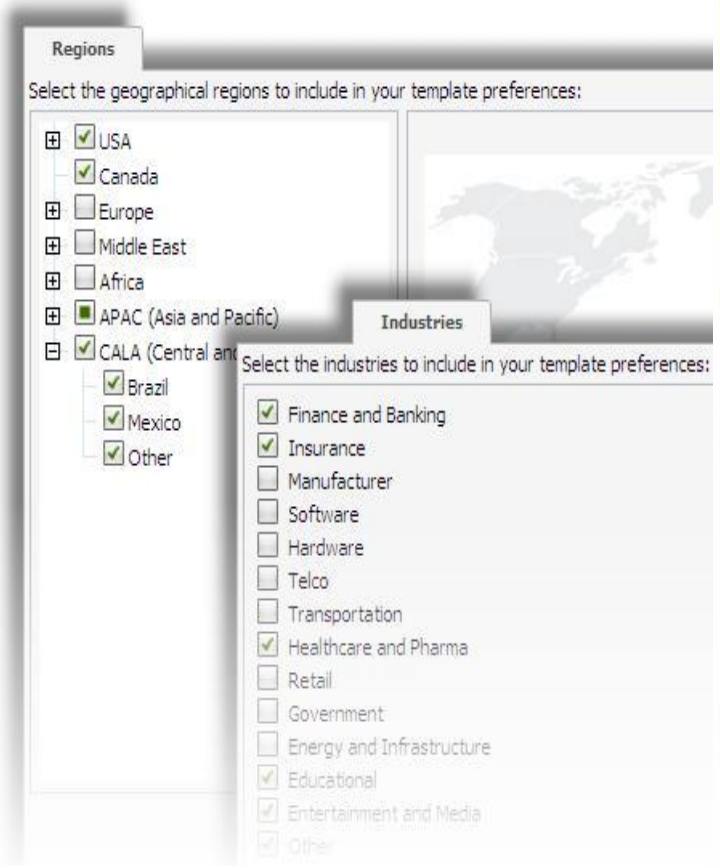
Machine Learning

ДиалогНаука

Готовые политики

- Различные классификаторы
  - Регулярные выражения, ключевые слова, словари
- Более 1100 готовых политик «из коробки», в том числе для РФ
- Удобный мастер настройки политик
- Определяет типы данных

  например: ПДн, PCI



ДиалогНаука

Цифровые отпечатки

- Цифровые отпечатки – все режиме для чтения:
  - Баз данных
  - Сетевых каталогов
  - SharePoint
  - SalesForce.com

- Подключение к базе данных через ODBC
  - Снятие цифровых отпечатков непосредственно с БД
  - Данные не покидают БД
  - Инкрементальные обновления базы отпечатков при росте исходной базы

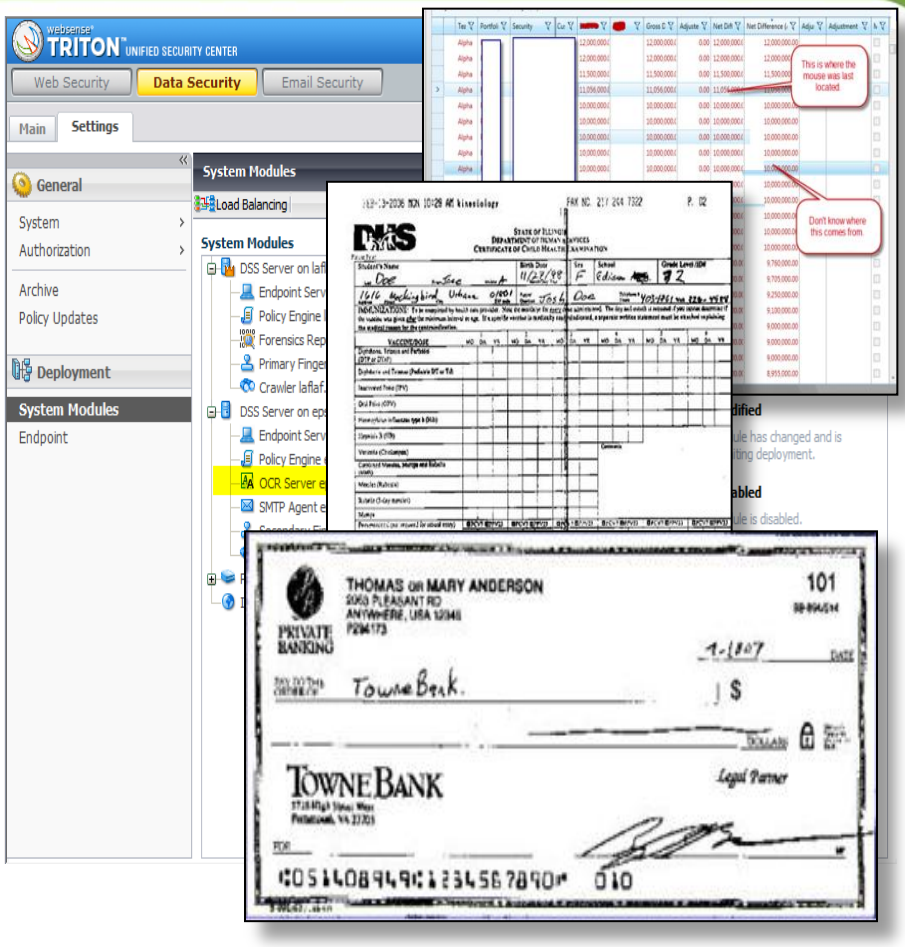
Machine Learning (ИИ)

- Удобный
  - Необходимо только указать каталог с документами
- Масштабируемость
- Высокая точность
  - Двухэтапный подход
  - Этап 1 – определение типа данных
  - Этап 2 – определение, является ли конфиденциальным

ДиалОгНаука

OCR Detection

- Используется механизмы оптического распознавания
- Определение КИ в картинках
  - Screen captures
  - Scanned checks
  - Scanned receipts
  - Fax pages
  - и т.п.
- Доступен для Web, Email и хранилищ



New 7.7

ДиалогНаука

Другие технологии Websense

- Распознавание типов файлов – около 400 форматов
  - Например, возможна блокировка зашифрованных файлов, документов САПР и файлов баз данных
  - Работа со свойствами файлов (имя, тип, размер)

ДиалогНаука

Сетевая DLP

Передача

(Data-in-Motion)

ДиалогНаука

Варианты контроля

SPAN-порт

- Смотрим – Не трогаем
- Видим входящий и исходящий незашифрованный трафик

In-Line

- Смотрим и трогаем
- Прокси для Web & FTP
- MTA для Email
- ActiveSync для Mobile

Агент

- Сетевые принтеры

Каналы и реагирование

Сетевая DLP

Web

Email

FTP

Сетевая печать

Active Sync

IM & Custom Channels

РЕАКЦИЯ В ЗАВИСИМОСТИ ОТ КАНАЛА

Audit
***Block**
Alert
Notify

Audit
Block
Quarantine
Encrypt**
Alert
Notify

Audit
***Block**
Alert
Notify

Audit
Block
Alert
Notify

Audit
Block
Alert
Notify

Audit
Block
Alert
Notify

* Требуется прокси

** Требуется шлюз шифрования

ДиалОгНаука

TruWeb и TruEmail DLP

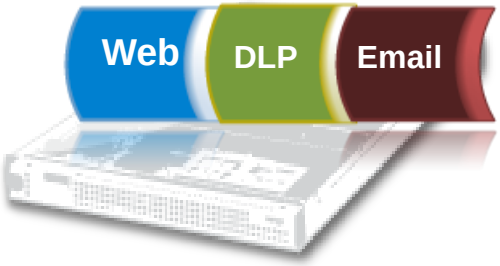
- Родная интеграция с промышленным DLP для решений Web и Email
- Работает на ПАК Websense V-Series
- Не требуется сторонних решений прокси и шлюзов шифрования

Web Security Gateway

- Промышленный DLP для Web
- Инспекция SSL
- Расширенная защита от веб-угроз

Email Security Gateway

- Промышленный DLP для Email
- Исходящее шифрование Email
- Anti-virus / Anti-spam
- URL Sandboxing



TRITON Security Gateway

- Интегрированная Web & Email DLP
- Инспекция SSL
- Исходящее шифрование Email
- Расширенная защита от веб-угроз

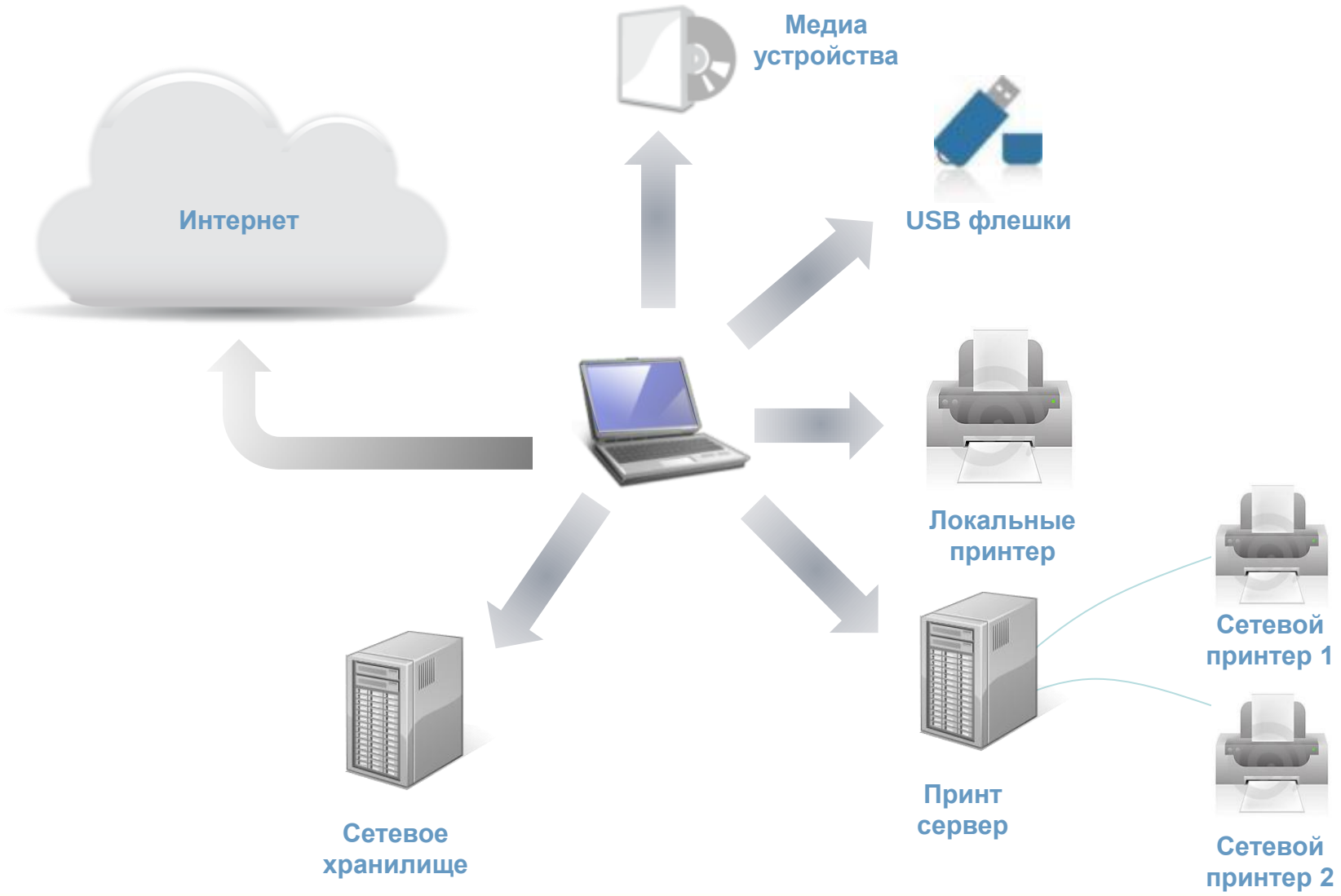
ДиалогНаука

Endpoint DLP

Использование

(Data-in-Use)

Каналы утечки на уровне АРМ



Детектирование и реагирование

Endpoint DLP

Приложения

Съемные устройства

Хранилища

ВАРИАНТЫ РЕАГИРОВАНИЯ

Permit
Confirm
Block
Email Quarantine
Alert
Notify

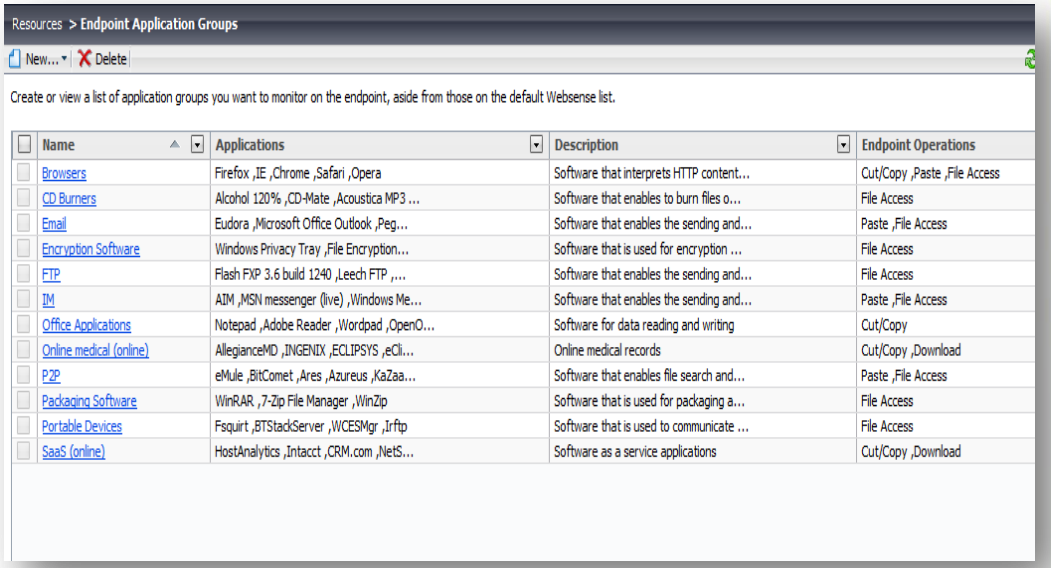
Permit
Confirm
Block
Encrypt to USB
Alert
Notify

Alert/Log
Scripts
Encrypt
Tombstone
Quarantine
EDRM

ДиалОгНаука

Контроль приложений

- Контроль приложений:
  - Copy/Cut/Paste
  - Файловый доступ
  - Print Screens

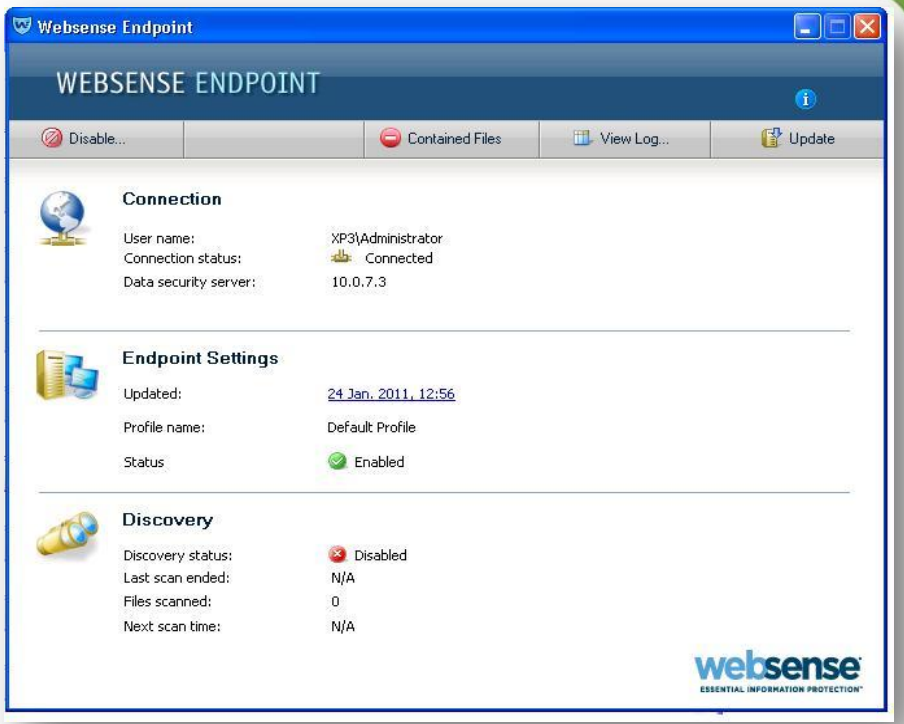


Name	Applications	Description	Endpoint Operations
Browsers	Firefox ,IE ,Chrome ,Safari ,Opera	Software that interprets HTTP content...	Cut/Copy ,Paste ,File Access
CD Burners	Alcohol 120% ,CD-Mate ,Acoustica MP3 ...	Software that enables to burn files o...	File Access
Email	Eudora ,Microsoft Office Outlook ,Peg...	Software that enables the sending and...	Paste ,File Access
Encryption Software	Windows Privacy Tray ,File Encryption...	Software that is used for encryption ...	File Access
FTP	Flash FXP 3.6 build 1240 ,Leech FTP ,...	Software that enables the sending and...	File Access
IM	AIM ,MSN messenger (live) ,Windows Me...	Software that enables the sending and...	Paste ,File Access
Office Applications	Notepad ,Adobe Reader ,Wordpad ,OpenO...	Software for data reading and writing	Cut/Copy
Online medical (online)	AllegianceMD ,INGENIX ,ECLIPSYS ,eCli...	Online medical records	Cut/Copy ,Download
P2P	eMule ,BitComet ,Ares ,Azureus ,KaZaa...	Software that enables file search and...	Paste ,File Access
Packaging Software	WinRAR ,7-Zip File Manager ,WinZip	Software that is used for packaging a...	File Access
Portable Devices	Fsquirt ,BTStackServer ,WCESMgr ,Irftp	Software that is used to communicate ...	File Access
SaaS (online)	HostAnalytics ,Intacct ,CRM.com ,NetS...	Software as a service applications	Cut/Copy ,Download

- Применяется к конкретным группам приложений

Защита агента

- Функции защиты агента:
  - Служба не может быть остановлена в оснастке “Services”
  - Процесс будет перезапущен, если был принудительно завершен
- Отключение защиты для задач обслуживания
  - Использование административного пароля



ДиалогНаука

Websense DLP

Хранение

(Data-at-Rest)

ДиалОгНаука

Варианты анализа

Безагентский

- Discovery в сети
- Проведение через LAN/WAN
- Управление с помощью Расписания

Агент

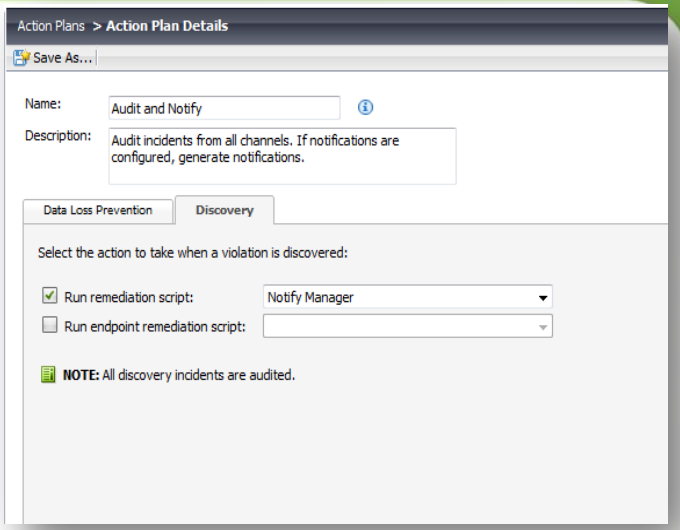
- Локальный Discovery
- Самое быстрое Discovery
- Управляется через Расписание, утилизацию CPU, электропитание

Гибридный

- Лучшее вариант
- Использование любой комбинации

Расширенные возможности реакции на инцидент

- Remediation Scripts
  - Доступно несколько готовых скриптов
  - Настраиваемые
- Доступные действия



Move/Quarantine

Encrypt**

Classification Tag
(Microsoft FCI)

Apply EDRM**

Purge/Delete

** Требуется стороннее решение

ДиалогНаука

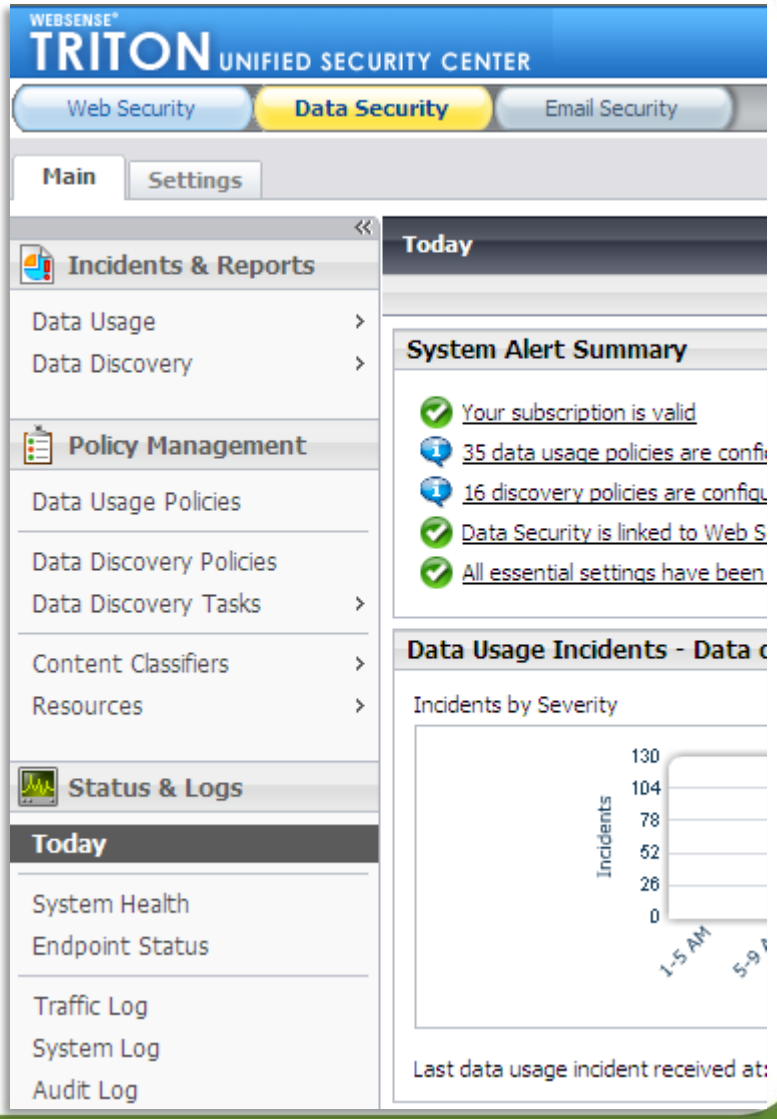
Websense DLP

Управление и отчетность

ДиалогНаука

Консоль TRITON

- Единая Web-консоль для управления всеми решениями Websense
- Ролевое управление и отчетность
- Управлением всеми компонентами DLP
  - Каналы TruWeb и TruEmail DLP
  - Enterprise Suite
  - Настройка отдельных модулей Data Security
    - Data Security Gateway
    - Data Endpoint
    - Data Discovery



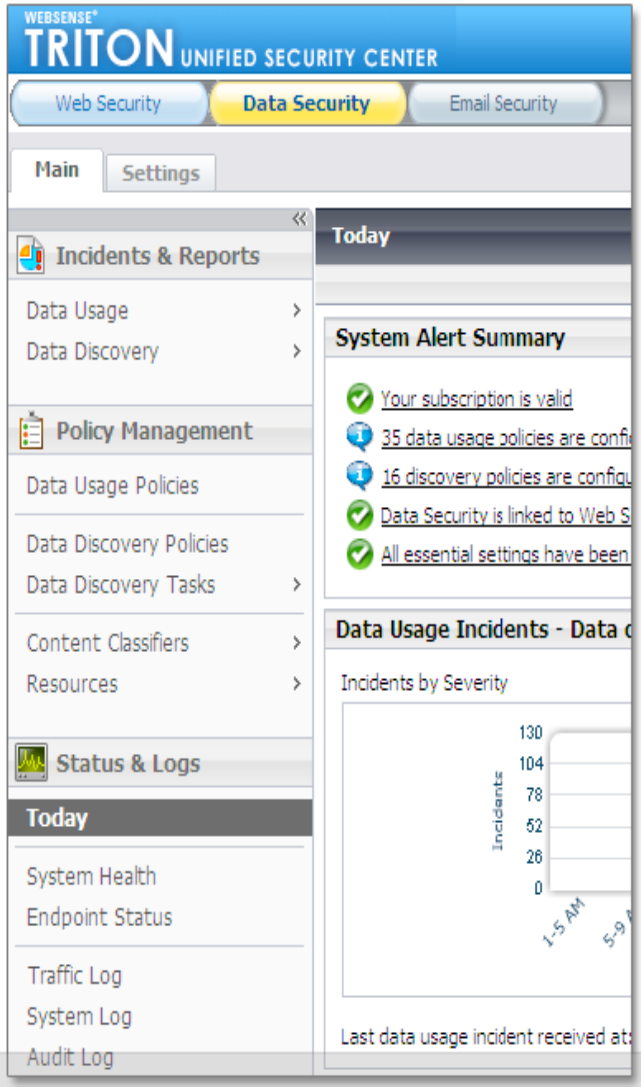
ДиалогНаука

Страница Today

- Несколько Dashboard’ов
- Показывает состояние:
  - System Health и активности
  - **Топ** нарушенных политик по серьезности
  - **Топ** каналов утечки по серьезности
  - **Топ** нарушителей политики
  - **Топ** мест хранения конфиденциальной информации

ДиалогНаука

Управление системой

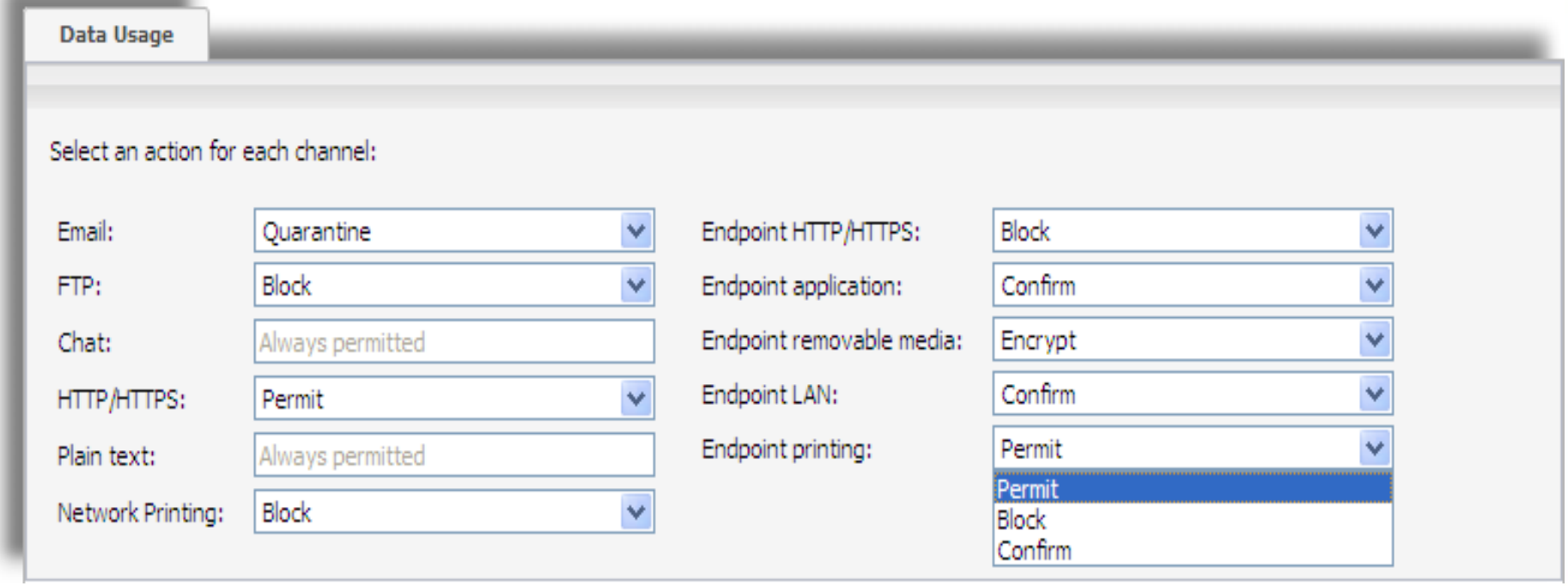


- Создание политик
  - Выбор способ идентификации (Классификатор)
  - Выбор каналов для мониторинга
  - Расписание задач Discovery
  - Установка серьезности и реакции
- Расследование инцидентов
- Отчетность

ДиалогНаука

Единая структура политик

- Политика может быть применена к одному или нескольким каналам
- Возможности гранулированного реагирования в зависимости от канала и серьёзности инцидента



ДиалОгНаука

Автоматизация реагирования

Кто	Что	Куда	Как	Действие
Отдел кадров	Исходный код	Поставщик	Передача файла	Аудит
Клиентская служба	Бизнес план	Персональный веб сайт	Web	Блокирование
Маркетинг	ПДн	Бизнес партнер	ICQ, Skype	Оповещение
Финансовый отдел	Слияния и поглощения	Блог	Peer-to-Peer	Удаление
Бухгалтерия	Информация о ЗП	Покупатель	Email	Шифрование
Отдел продаж	Финансовая отчетность	Вредоносный сайт	Печать	Карантин
Юридический отдел	Договора	USB	Съемные устройства	Подтверждение
Техподдержка	Техническая документация	Конкурент	Print Screen	
Инженеры	Результаты сравнений	Аналитик	Копирование/вставка	

ДиалогНаука

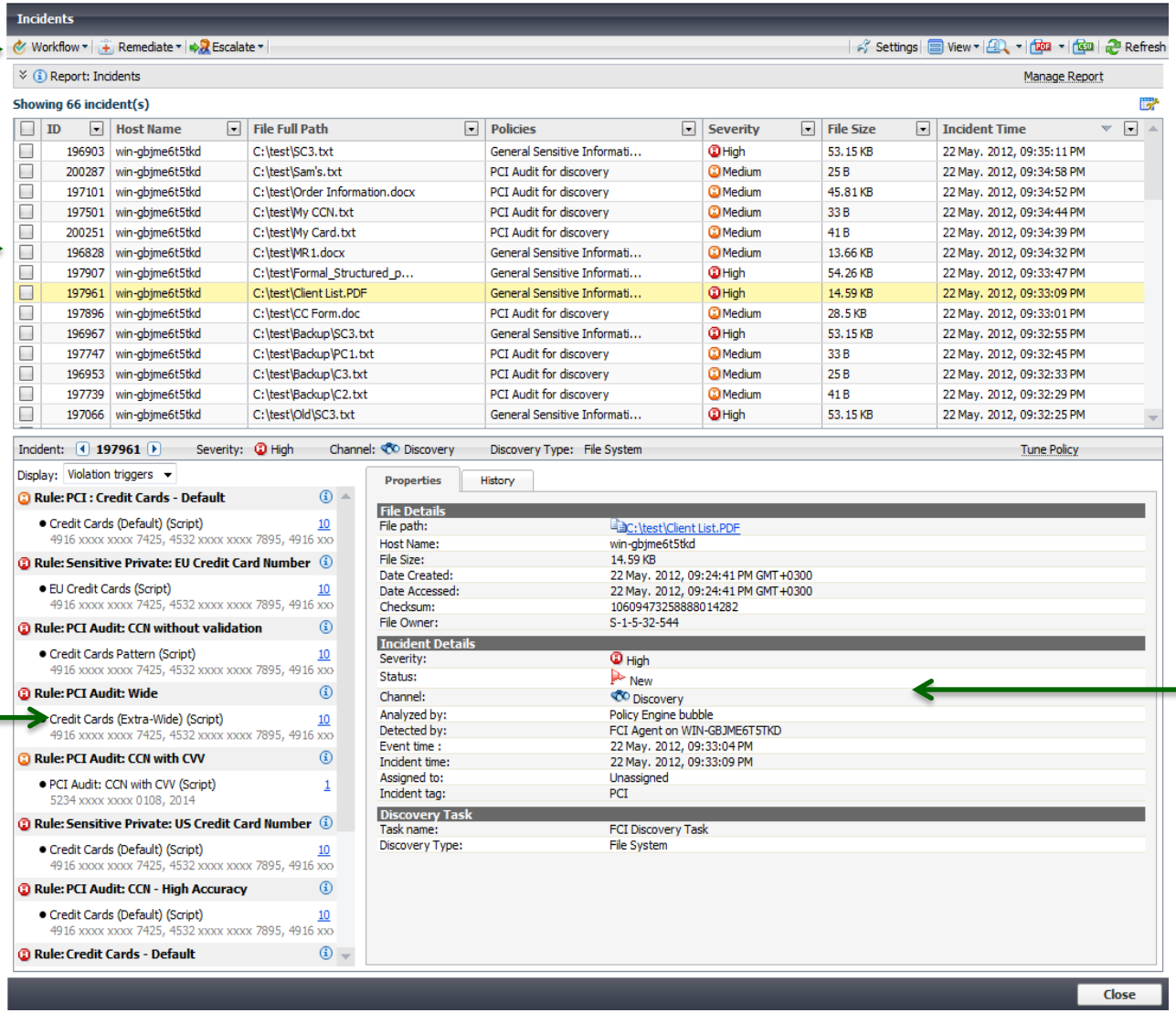
Управление инцидентами

Принятие мер

Список инцидентов

Триггеры нарушения

Детали инцидента



ДиалОгНаука

Исследовательские отчеты

- Дает представление
  - Топ Web получателях по
  - Топ Email получателей
  - Топ источников, соверш
  - Топ нарушенных полити
- Используется для:
  - Приоритезации меропри снижению риска
  - Определения необходи работников
  - Тюнинга политик
  - Определения «неправи процессов
  - Демонстрации соответс требованиям регулятор

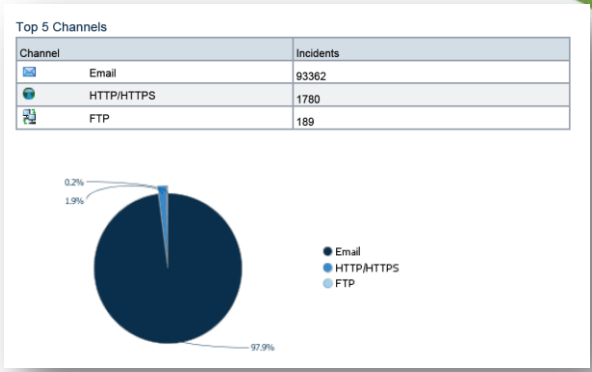
Show All 1

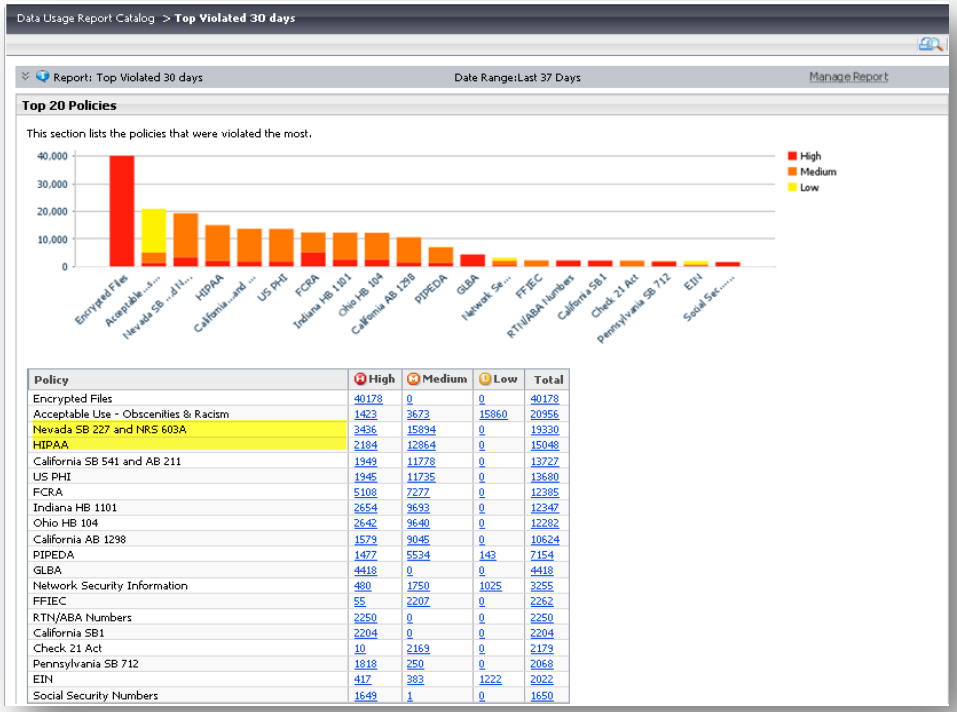
URL Category	High	Medium	Low	Total
General Email	157	289	278	724
Social Networking	8	36	265	309
Web Chat	0	2	265	267
Advertisements	7	30	81	118
Search Engines and Portals	16	47	35	98
Uncategorized	44	5	37	86
Information Technology	1	12	69	82
Internet Radio and TV	0	7	60	67
Government	30	0	37	67
Games	0	10	57	67
Business and Economy	2	2	36	40
Shopping	2	4	23	29
Job Search	1	25	2	28
Financial Data and Services	24	0	1	25
Personal Network Storage and Backup	0	5	17	22
Message Boards and Forums	0	1	16	17
Entertainment	0	5	8	13
Reference Materials	7	4	1	12
Advocacy Groups	0	0	11	11
News and Media	1	4	6	11
Educational Institutions	0	1	9	10
Travel	0	2	7	9
Instant Messaging	0	0	8	8
Illegal or Questionable	7	0	0	7
Professional and Worker Organizations	0	0	7	7
Society and Lifestyles	0	0	6	6
Blogs and Personal Sites	0	0	6	6
Streaming Media	0	1	5	6
Sports	0	0	5	5
Service and Philanthropic Organizations	0	1	4	5
Proxy Avoidance	0	0	2	2
Hosted Business Applications	0	2	0	2
Gay or Lesbian or Bisexual Interest	0	0	2	2
Phishing and Other Frauds	2	0	0	2
Personals and Dating	0	0	2	2

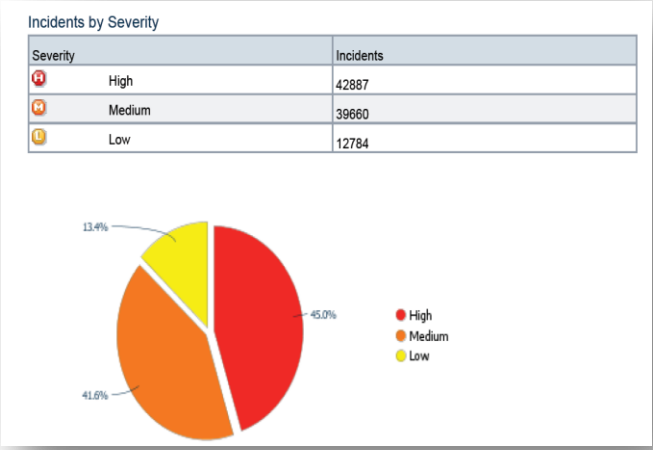
ДиалогНаука

Сводные отчеты для руководства

- Могут запускаться по расписанию
- Топ инцидентов за последние 24 часа
- Итоговые отчеты за 30, 60, 90 дней
- Трендовые отчеты
- И другие…







ДиалогНаука

Угрозы

Случайные

ОБУЧЕНИЕ РАБОТНИКОВ

Готовые шаблоны, оповещения/подтверждения, самостоятельный релиз

Преднамеренные (незлоумышленные)

ВИДИМОСТЬ

Уникальные совпадения, действия по серьезности инцидента, Source и Destination Awareness, Drip DLP

Инсайдер

РАСШИРЕННОЕ ДЕТЕКТИРОВАНИЕ

Drip DLP, контроль приложений, OCR распознавание

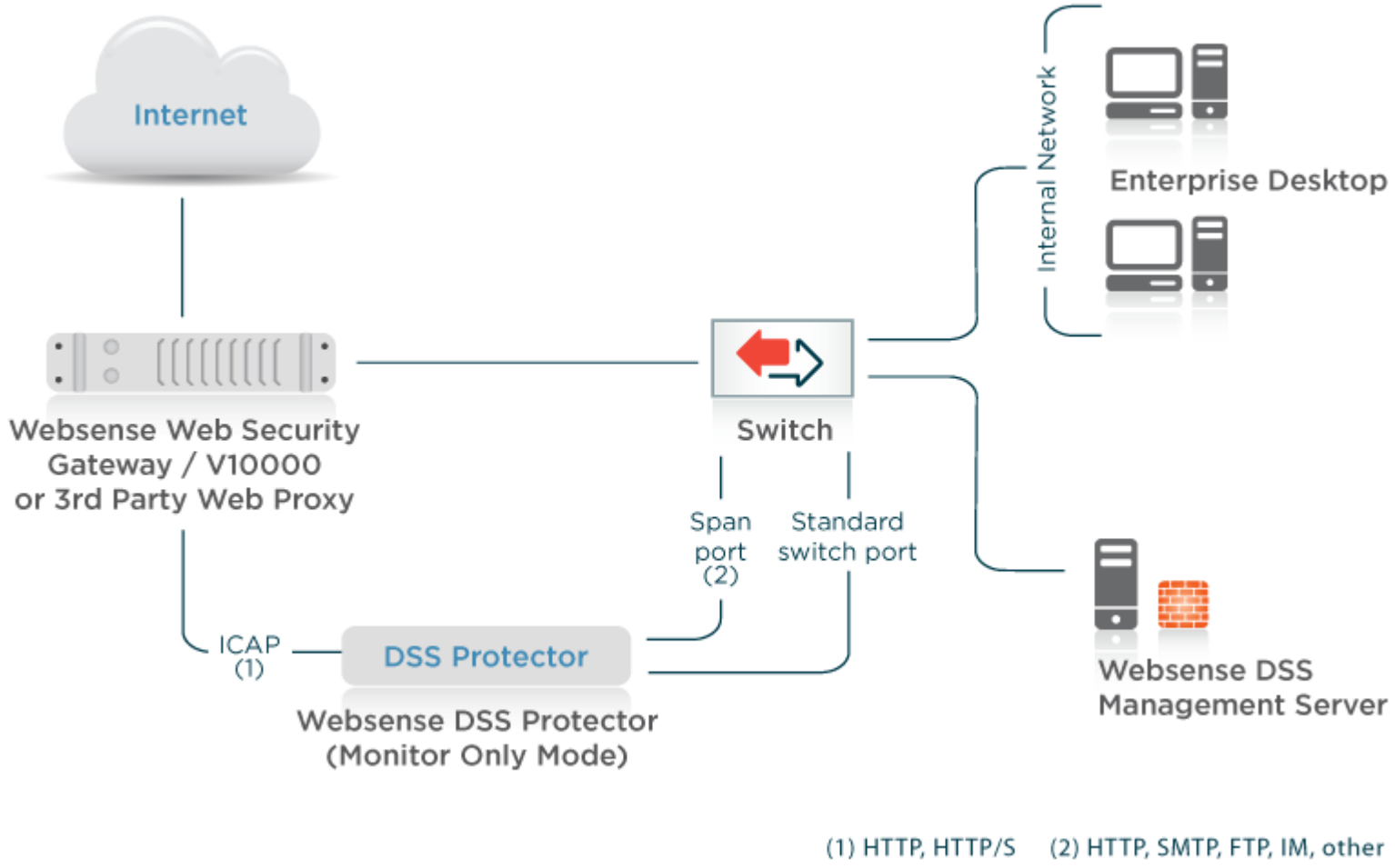
Внешний злоумышленник

WEBSENSE SECURITY LABS (ACE)

Дешифрование SSL, URL категории, геолокация, неавторизованное шифрование

ДиалогНаука

Архитектура
Пассивный мониторинг

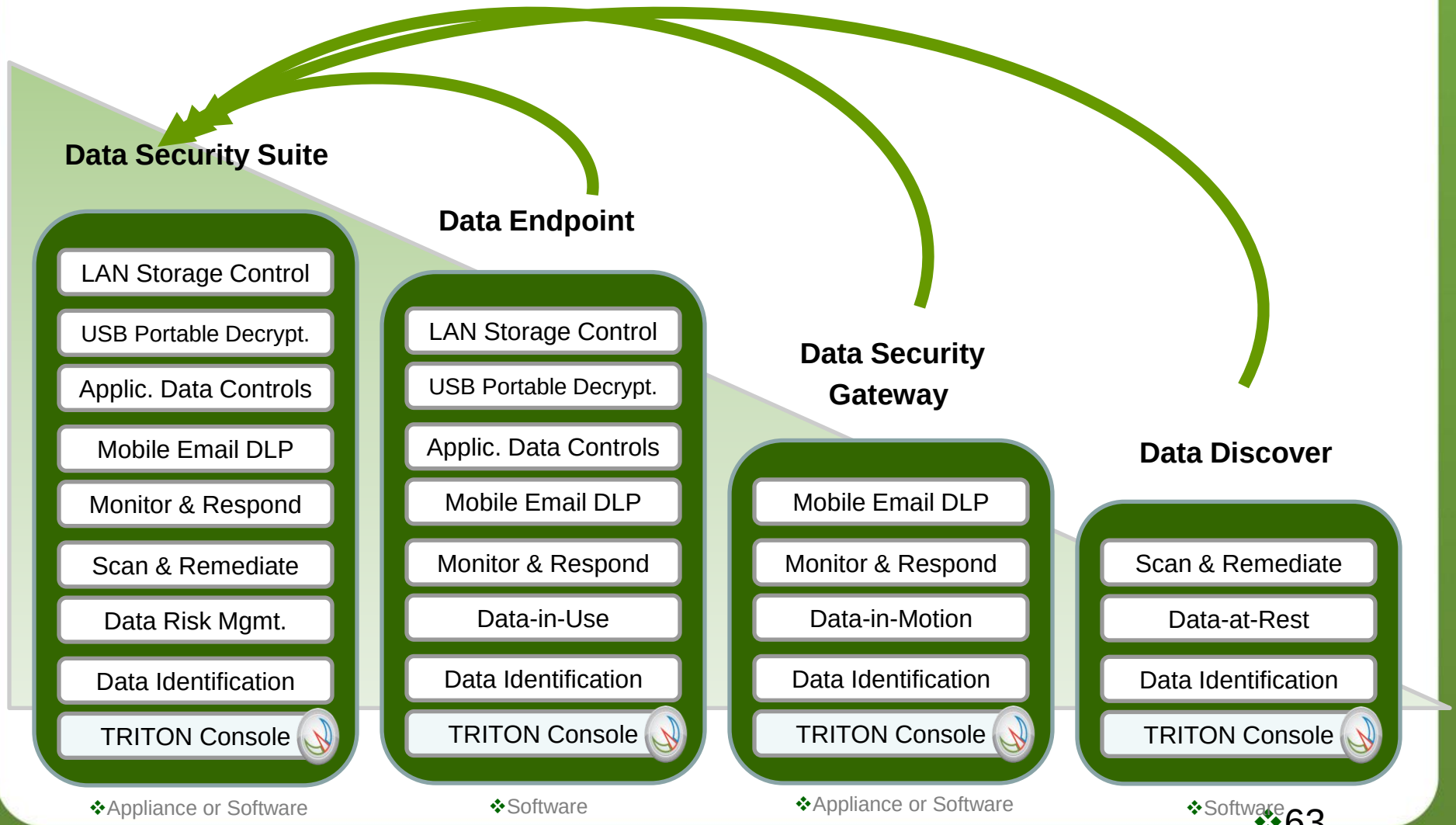


ДиалогНаука

Решение Websense DLP

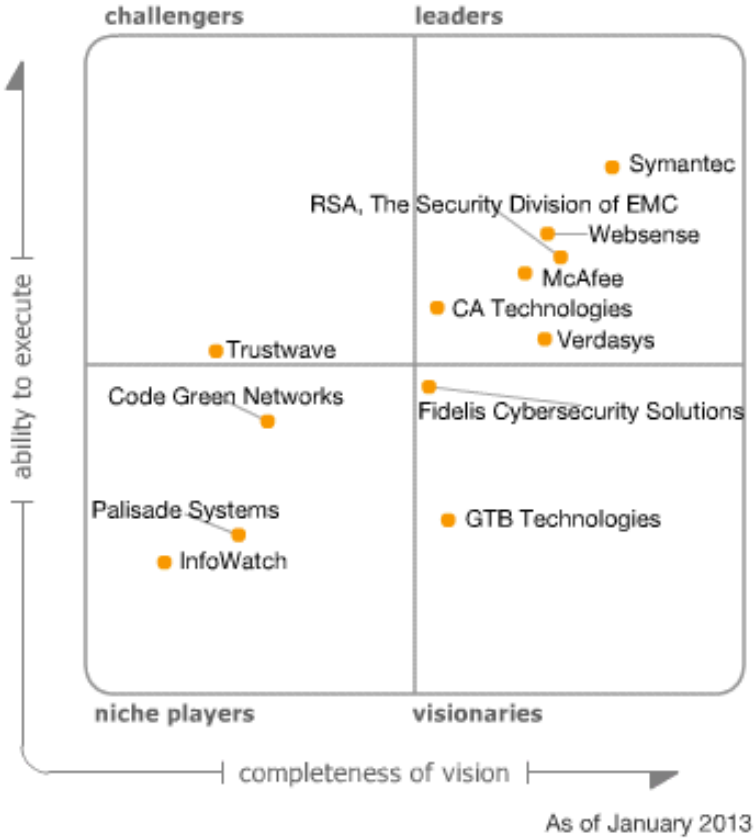
Пакеты

Пакеты Data Security

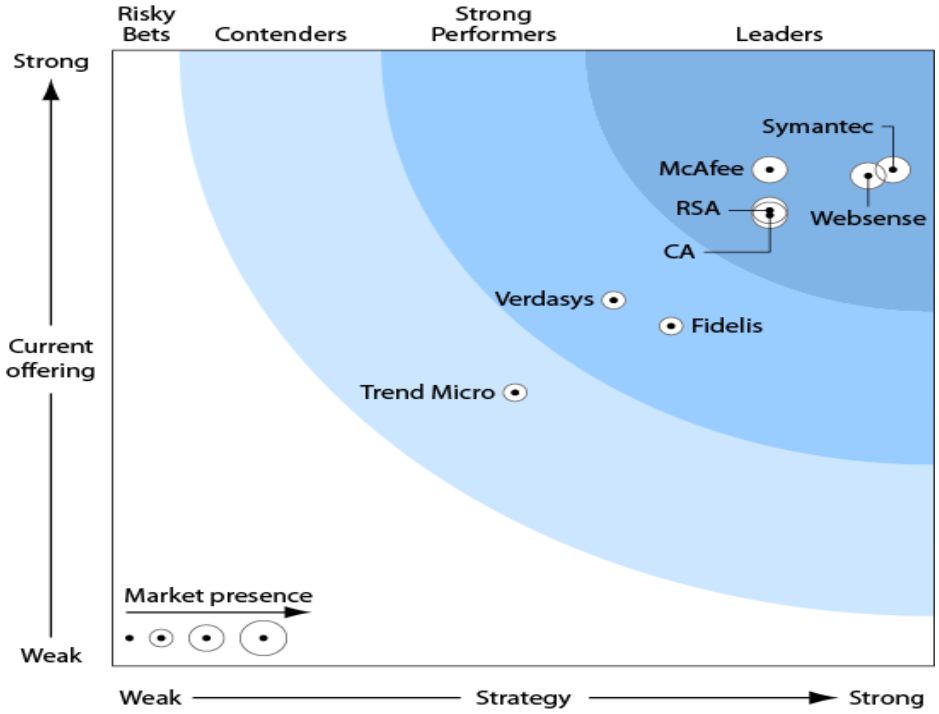


ДиалогНаука

Gartner, Forester



As of January 2013



ДиалогНаука

Вывод

- Комплексный подход к построению системы защиты
  - Более 90% утечек за прошлый год, согласно отчету Verizon, можно было предотвратить используя достаточно дешевые средства и способы защиты
- Руководство компании:
  - Минимизация финансовых потерь, репутационных рисков
- Отдел ИБ:
  - Предотвращение и расследование инцидентов, связанных с утечкой конфиденциальной информации
- Отдел HR:
  - Выявление неблагонадёжных сотрудников. Лояльность персонала
- Отдел ИТ:
  - Снижение нагрузки на сотрудников ИТ, привлекающихся к расследованию инцидентов

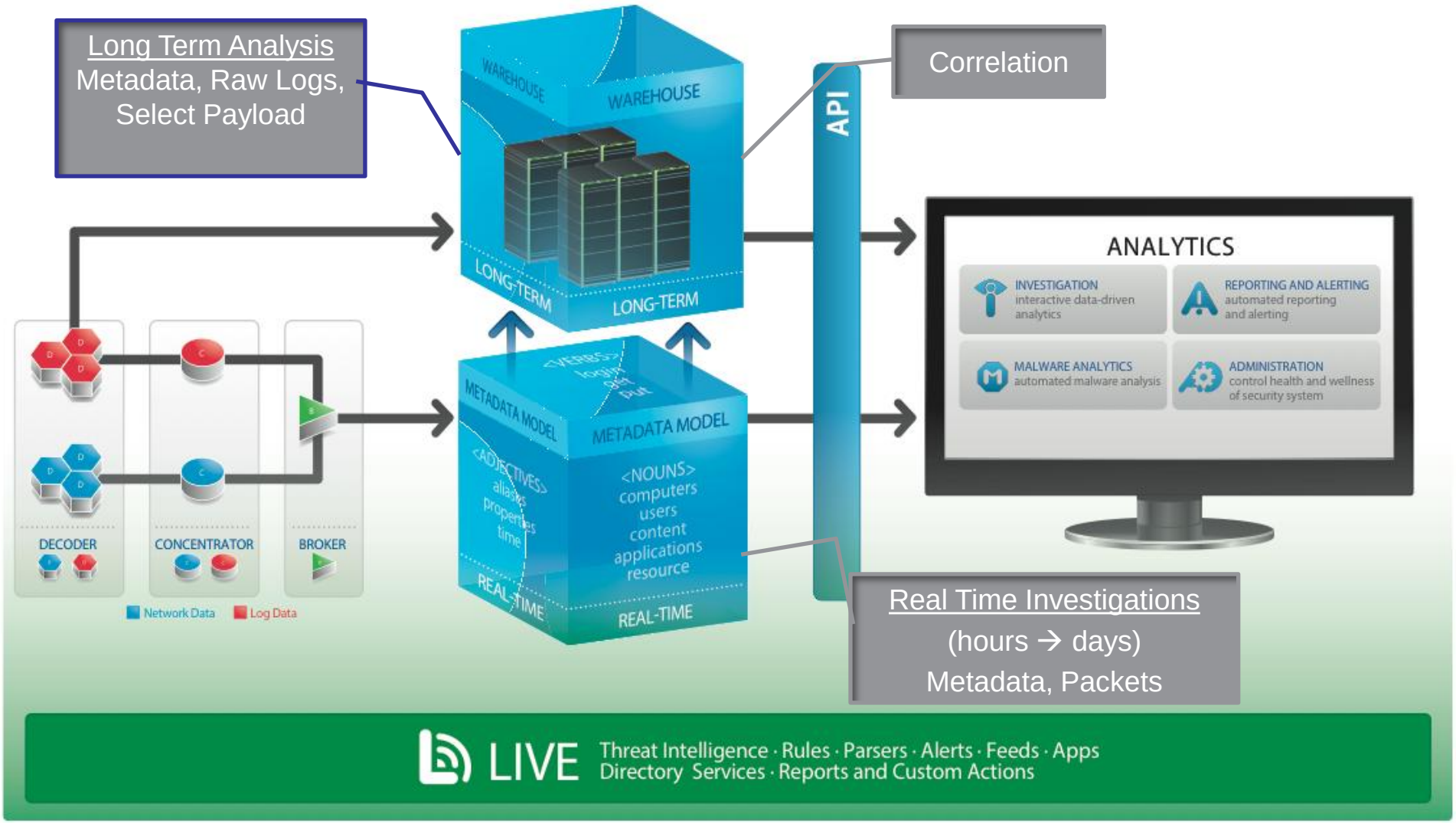
ДиалогНаука

Функциональное назначение Netwitness NextGen

- сбор и хранение пакетов данных, циркулирующих в ЛВС, которые могут быть использованы как доказательная база при расследовании инцидентов безопасности
- выявление нарушений политики ИБ, которые можно обнаружить на основе анализа сетевого трафика (передача паролей в открытом виде, использование несанкционированных протоколов, передача конфиденциальной информации в незашифрованном виде и др.)
- выявление нештатных ситуаций и сетевых аномалий, связанных с инцидентами безопасности (например, наличие протокола IRC по нестандартному порту или наличие SSL с самоподписанным сертификатом и др.)

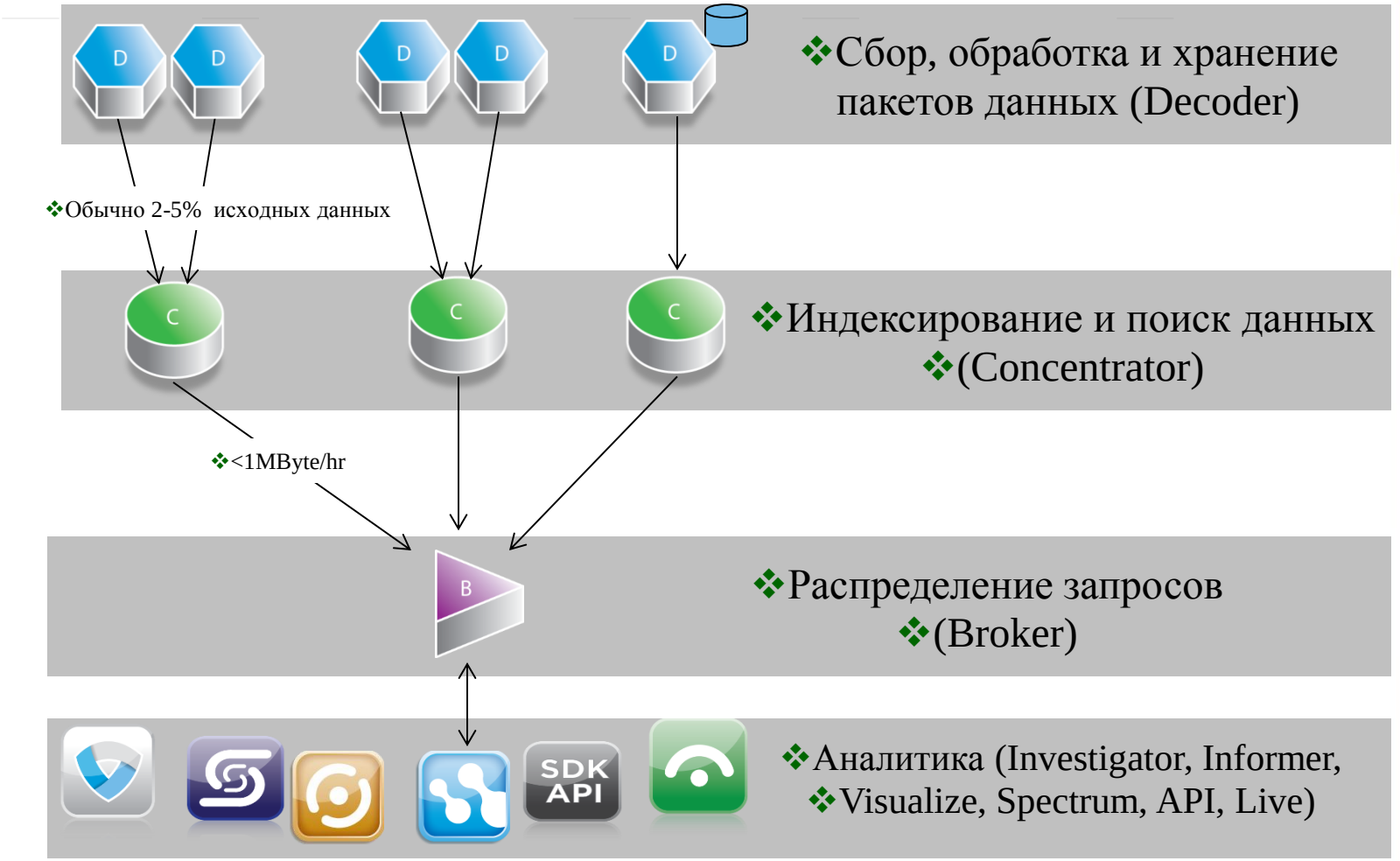
ДиалогНаука

Архитектура RSA Security Analytics



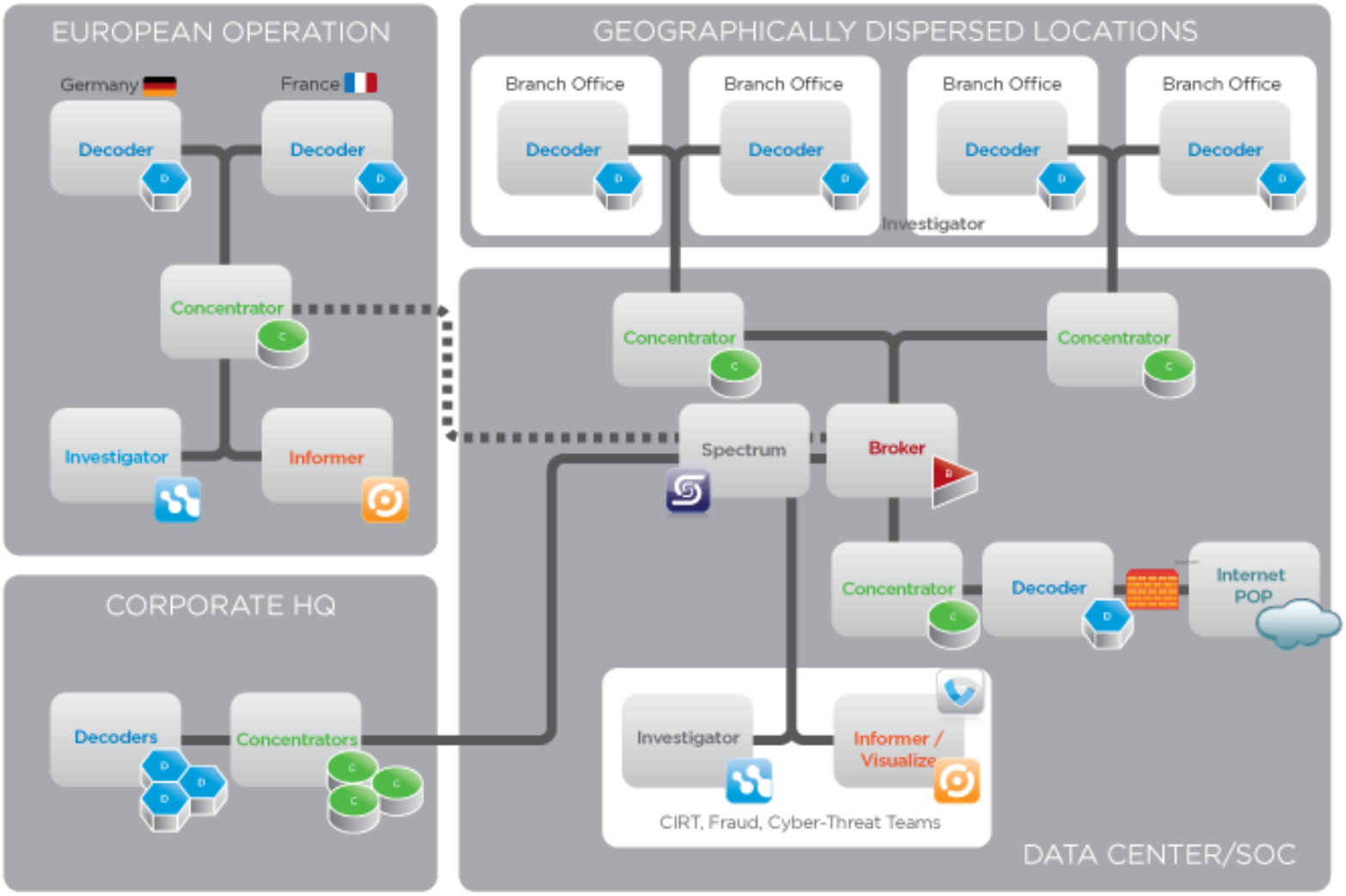
Архитектура NextGen

❖Зеркальный SPAN-порт, TAP-устройство, или балансировщик нагрузки



ДиалОгНаука

Масштабируемость



ДиалогНаука

NetWitness может интегрироваться с существующей ИТ-инфраструктурой

ArcSight CERTIFIED CEF COMPLIANT

SOURCEfire®

RSA SECURED®

EMC²

CISCO

paloalto NETWORKS

NetApp™

DELL

1Q Labs

splunk>

McAfee®

Microsoft®

VeriSign®

VSS monitoring

NETRONOME™

Lookingglass

Gigamon™

ДиалОгНаука

Компоненты NetWitness NextGen

ПРИЛОЖЕНИЯ

Informer – Визуализация, отчетность, и оповещения

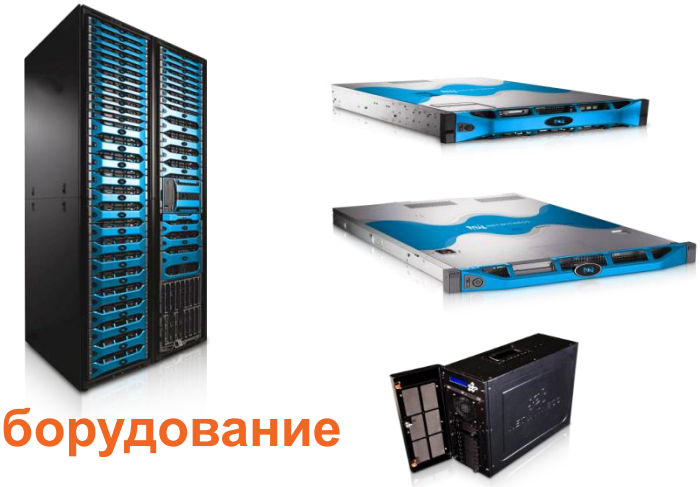
Investigator Enterprise – Интерактивный анализ информации

Live – Интеграция в реальном времени с внешними информационными службами

Spectrum – Автоматический анализ и приоритезация вредоносного кода

SIEMLink – Обеспечивает моментальный доступ к данным NetWitness из консоли вашего IDS или SIEM

SDK/API – открытый интерфейс для разработки собственных приложений на базе инфраструктуры Netwitness



Оборудование

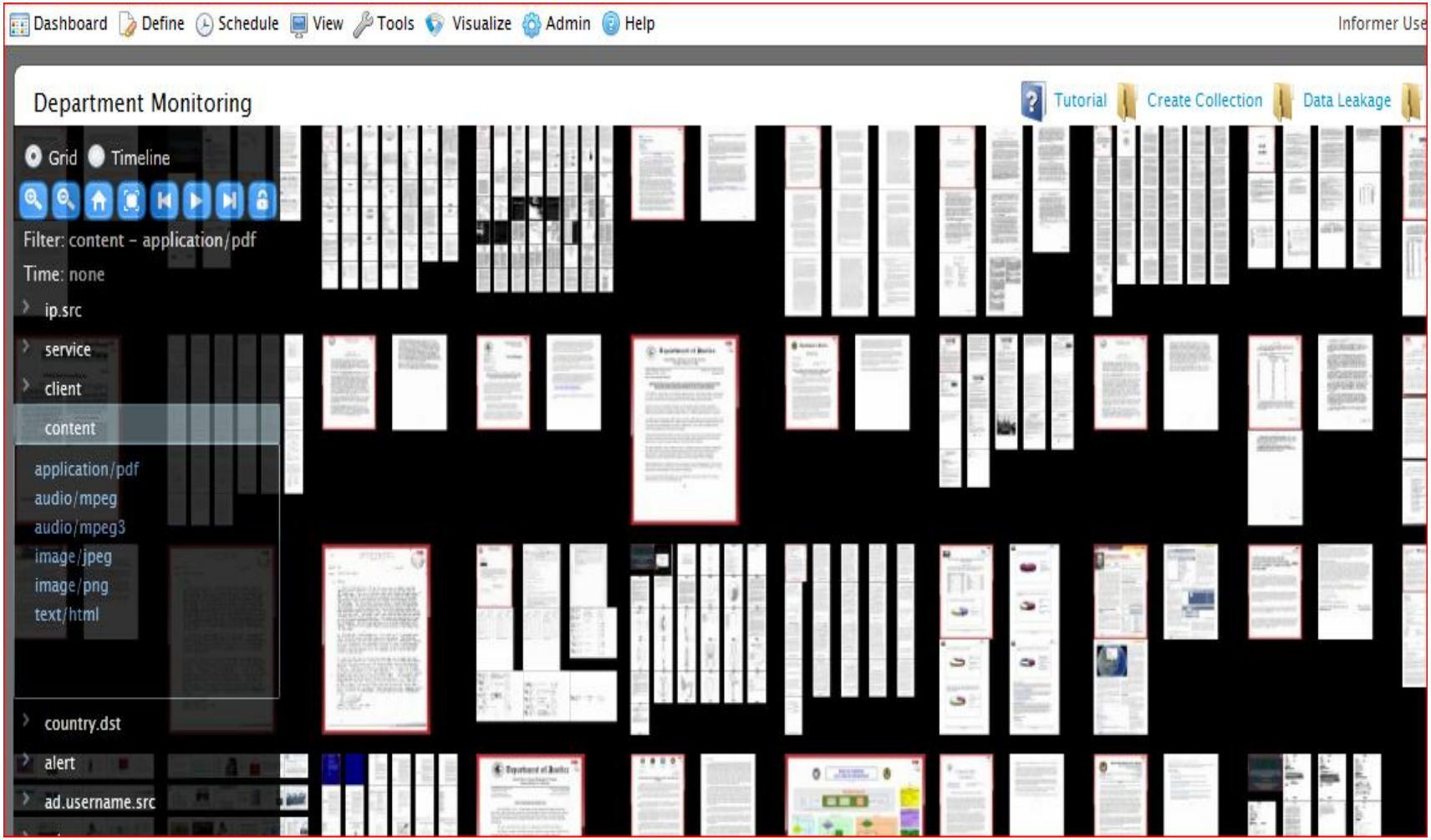
Decoder – устройства для перехвата и хранения сетевого трафика в реальном масштабе времени

Concentrator and Broker – устройства для агрегации и анализа данных, полученных от нескольких декодеров

Eagle – Портативное гибридное решение, объединяющее элементы Decoder, Concentrator и Investigator в одном устройстве

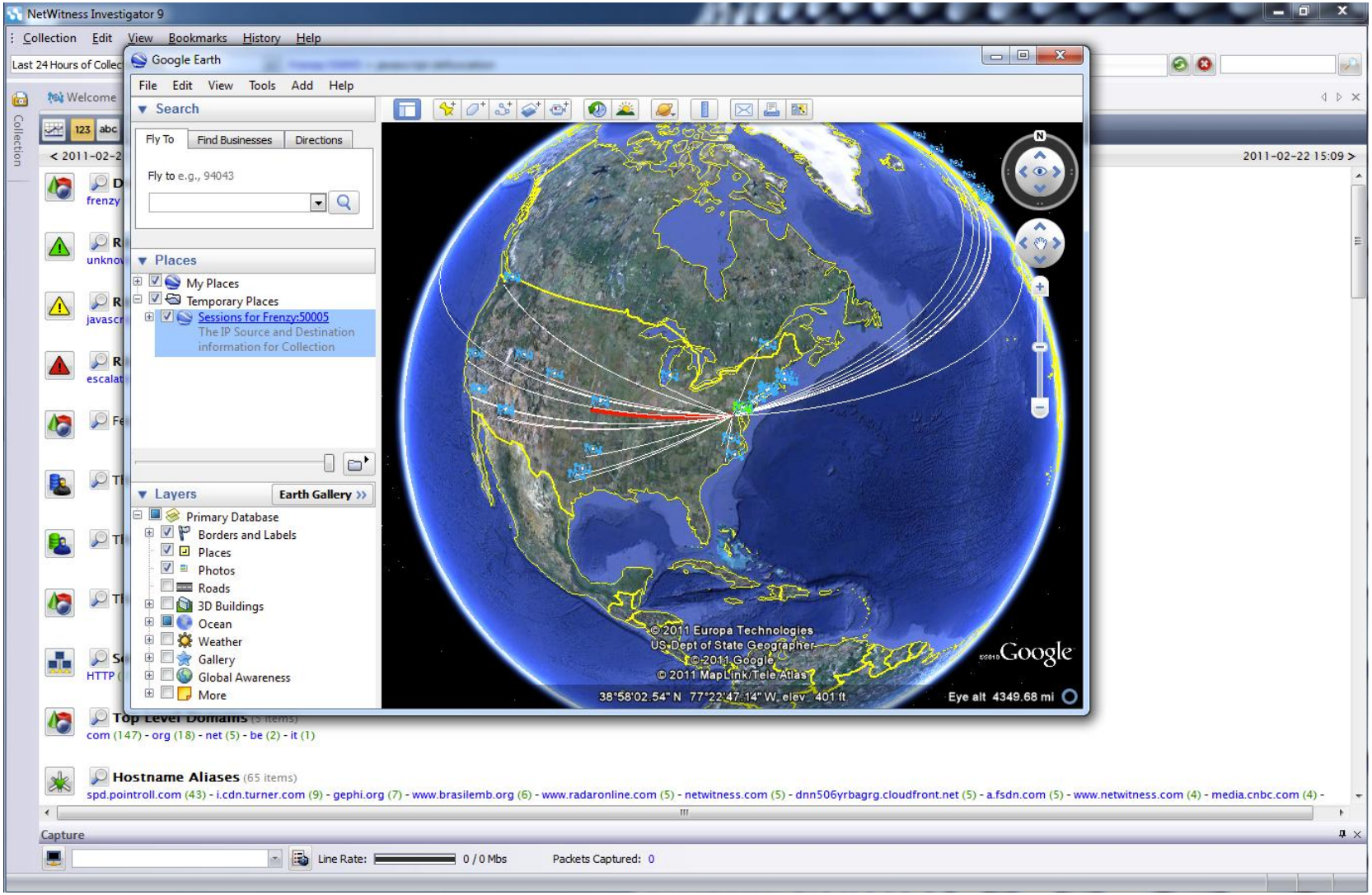
ДиалогНаука

NetWitness Visualize



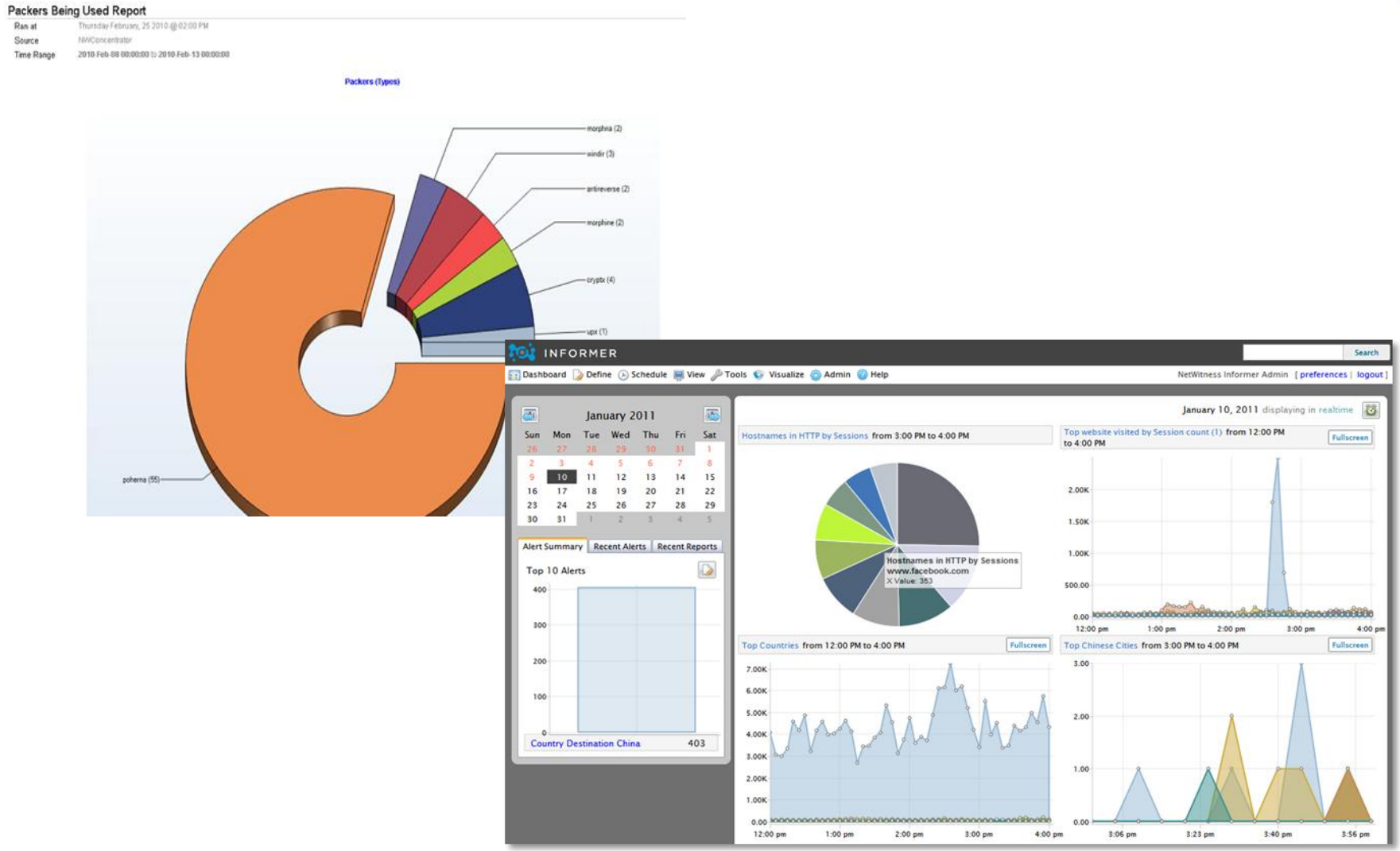
ДиалОгНаука

Поддержка технологии GeoIP



ДиалогНаука

Гибкая система отчетности



ДиалогНаука

Анализируемые протоколы

- исходящая электронная почта
- исходящий веб-трафик
- внутренняя электронная почта
- внутренний файловый обмен
- IP-телефония (VOIP)
- другие сетевые протоколы

ДиалогНаука

NetWitness + Websense

- **Websense Data Security** обеспечивает выявление фактов утечки конфиденциальной информации

- **NetWitness NextGen** обеспечивает ведение архива на основе перехвата и анализа сетевого трафика

NetWitness NextGen + **Websense DS** = эффективное комплексное решение для своевременного выявления и последующего расследования инцидентов безопасности

ДиалОгНаука

Преимущества NetWitness

- Хранение не только документов, но и всех пакетов данных, передаваемых в ЛВС
- Возможность хранения и обработки данных в реальном масштабе времени в сетях с пропускной способностью до 10 Гбит/с
- Ведение архива не только почтового трафика, а любых информационных потоков, передаваемых по сети
- Развитая система формирования отчетов
- Возможность анализа пакетов данных на 7-ми уровнях модели OSI
- Возможность расширения функциональных возможностей за счет добавления новых правил обработки сетевого трафика

ДиалогНаука

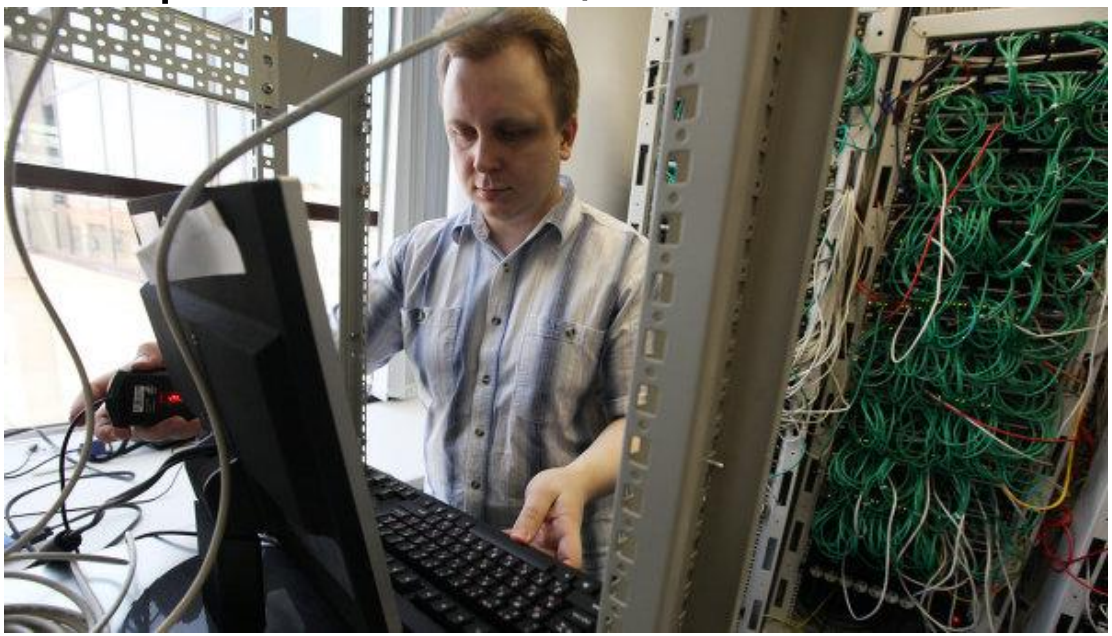
Результаты внедрения NetWitness

- Повышение скорости расследования инцидентов безопасности за счет создания полноценного архива и доказательной базы
- Увеличение эффективности от использования других средств защиты информации (DLP-решений, систем IDS/IPS, средств мониторинга событий ИБ SIEM и др.)
- Выявление инцидентов безопасности на основе детального анализа сетевого трафика
- Создание платформы для последующего внедрения центра управления информационной безопасностью

ДиалОгНаука

Друг или враг?

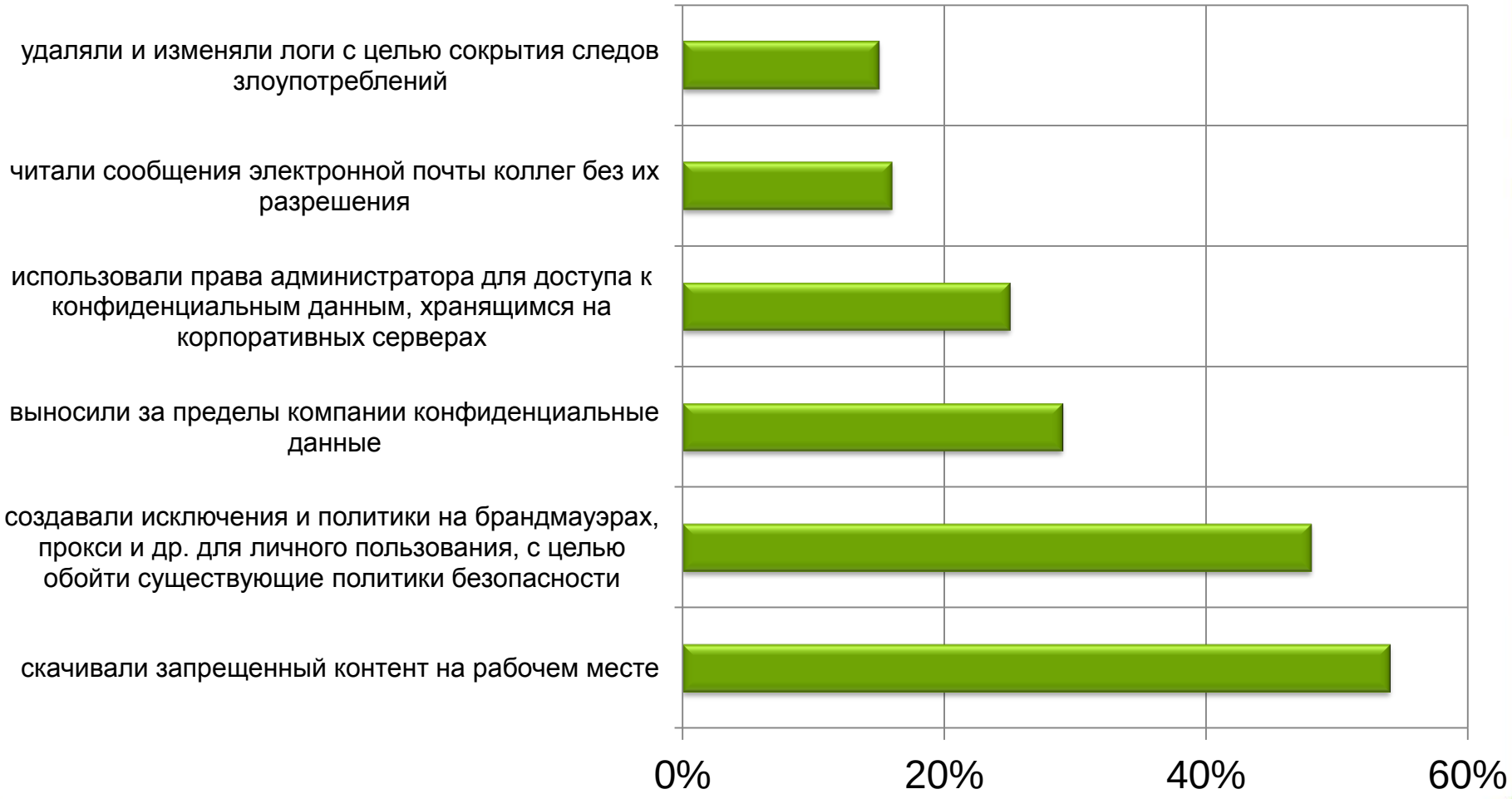
- Знает архитектуру сети
- Понимает организацию шлюза доступа в интернет
- Располагает информацией о системах защиты
- Владеет учетными записями администратора на серверах и рабочих станциях



ДиалогНаука

Статистика злоупотреблений системных администраторов

ТОП 6 злоупотреблений



ДиалОгНаука

Вопросы при управлении серверами

- Кто и как входил в системы?
- Что делают системные администраторы и как их контролировать?
- Почему сервера периодически перезагружаются?
- Почему некоторые сервисы больше недоступны?
- Чем занимаются пользователи на терминальных серверах?

ДиалОгНаука

Основная идея

Контроль действий
администраторов

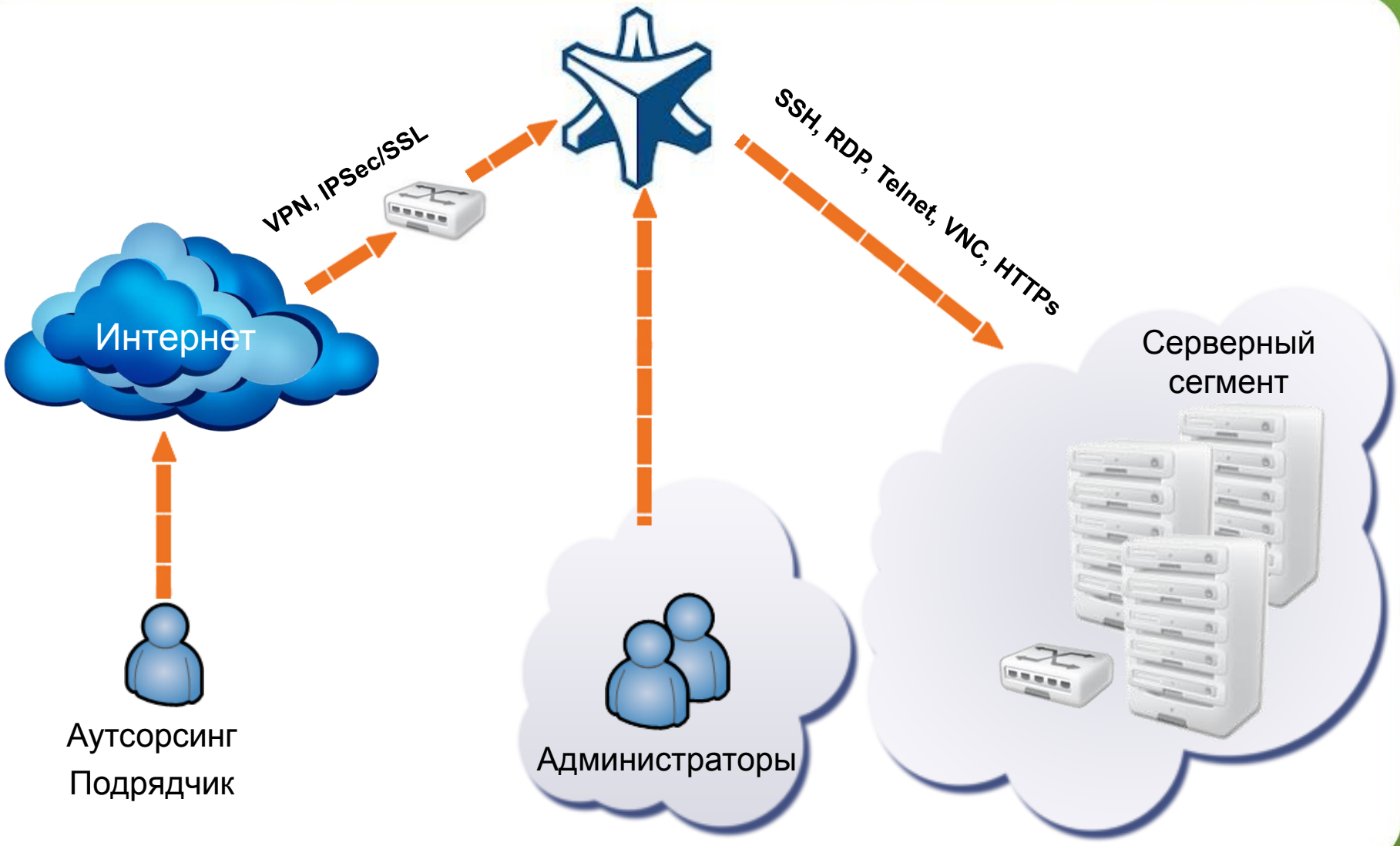
Предоставление
доступа к серверам

Централизованное
управление доступом

BalaBit Shell Control Box

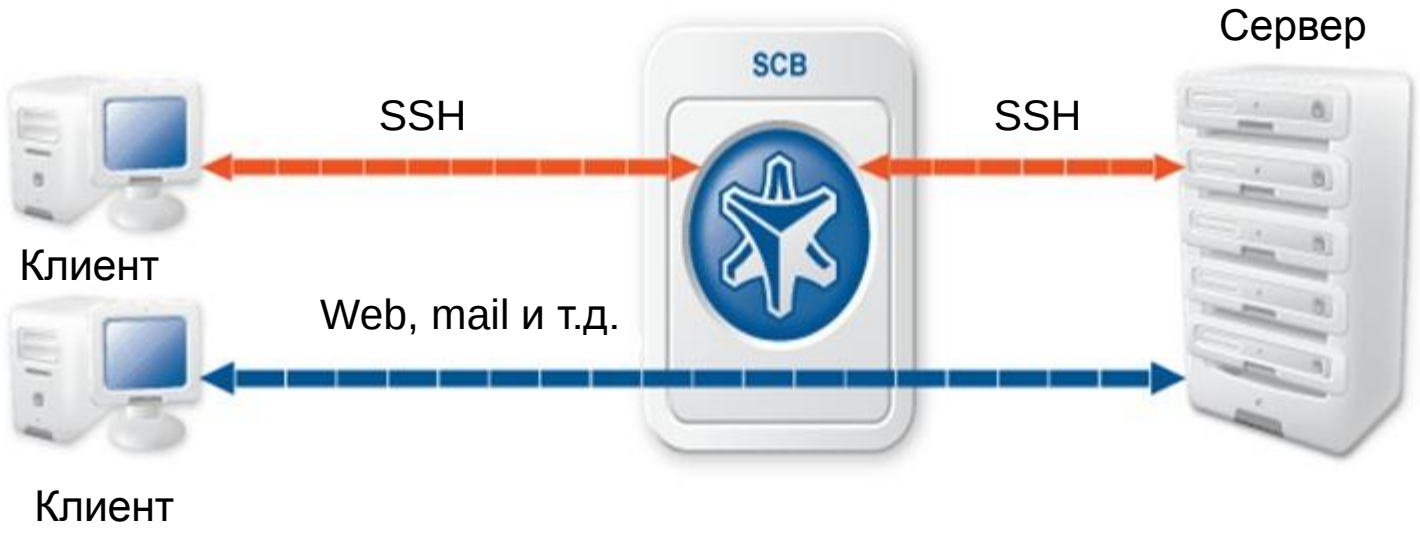
ДиалОгНаука

Схема взаимодействия



Функционирование

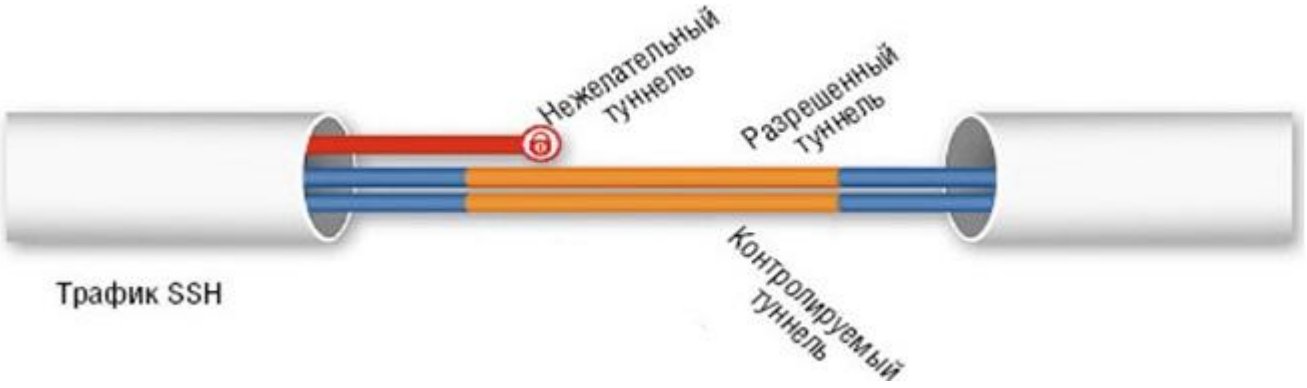
Перехватывает только административный трафик, остальной тип трафика пропускается в режиме Bypass



ДиалОгНаука

Возможности Shell Control Box

- Технология основана на Man-In-The-Middle
- Контроль над различными уровнями
  - vpn, port-forward, scp/sftp etc.
  - Print-, disk- sharing
- Принудительная строгая аутентификация, шифрование



ДиалОгНаука

Возможности Shell Control Box

- Наблюдение и аудит работы администраторов систем
- Настраиваемые сценарии реагирования
- Сбор информации для возможных расследований (контентный поиск)
- Управляемый контроль доступа к серверам
- Fine-tuned контроль над работой серверов
- Простая интеграция в существующую инфраструктуру
- Запись и шифрование данных аудита
- Авторизация «Четыре глаза»
- Идентификация защищаемых серверов

Возможности Shell Control Box

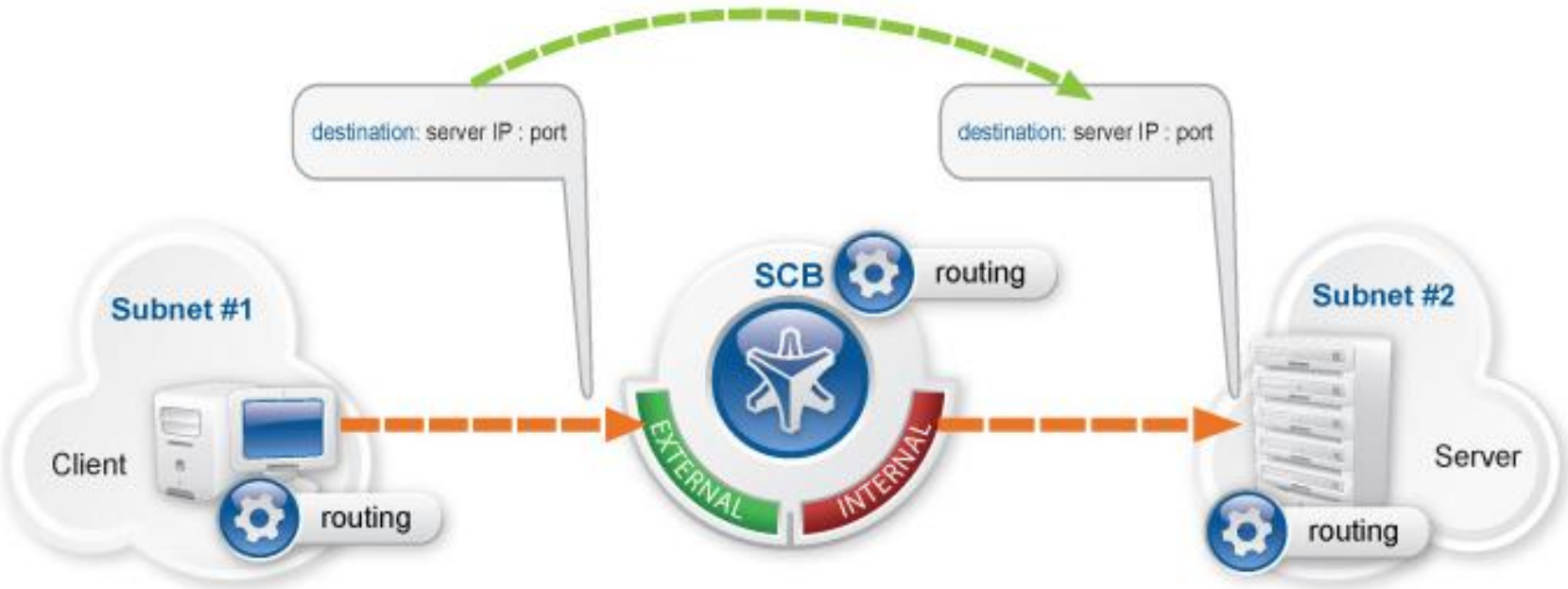
- Инспекция протоколов
- Поддержка отказоустойчивости (HA и Heartbeat)
- Легкое управление через Web браузер
- Автоматическое архивирование и резервное копирование данных
- Пересылка контента на внешние IDS и DLP
- Поиск и повтор сессий подобно видео-файлу
- Ролевое управление доступом к SCB
- Гибко настраиваемые формы отчетов

Bridge mode

SCB действует как сетевой switch и соединяет сетевой сегмент администраторов с сегментом защищаемых серверов на уровне передачи данных (замена MAC адресов в ARP ответе)

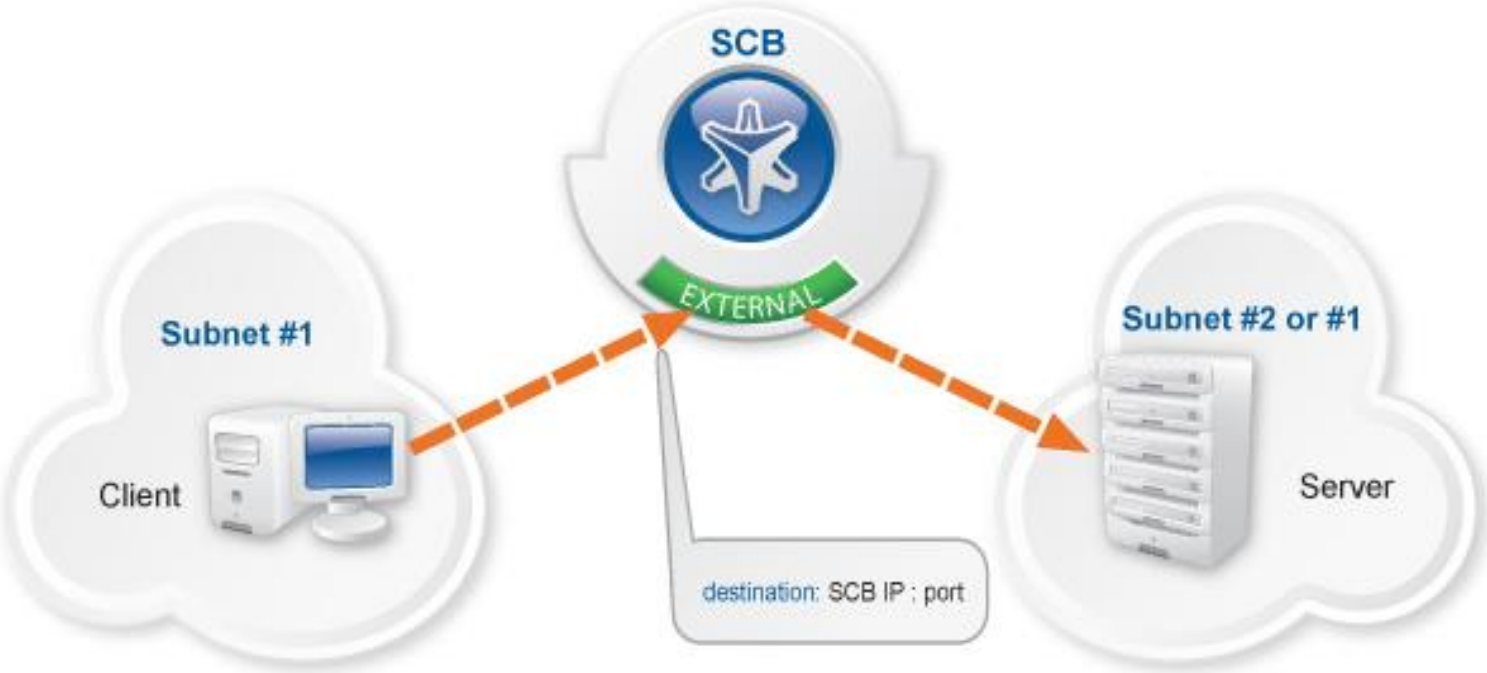
Router mode

SCB действует как прозрачный маршрутизатор, соединяющий сетевой сегмент администраторов с сегментом защищаемых серверов на сетевом уровне (IP маршрутизация)



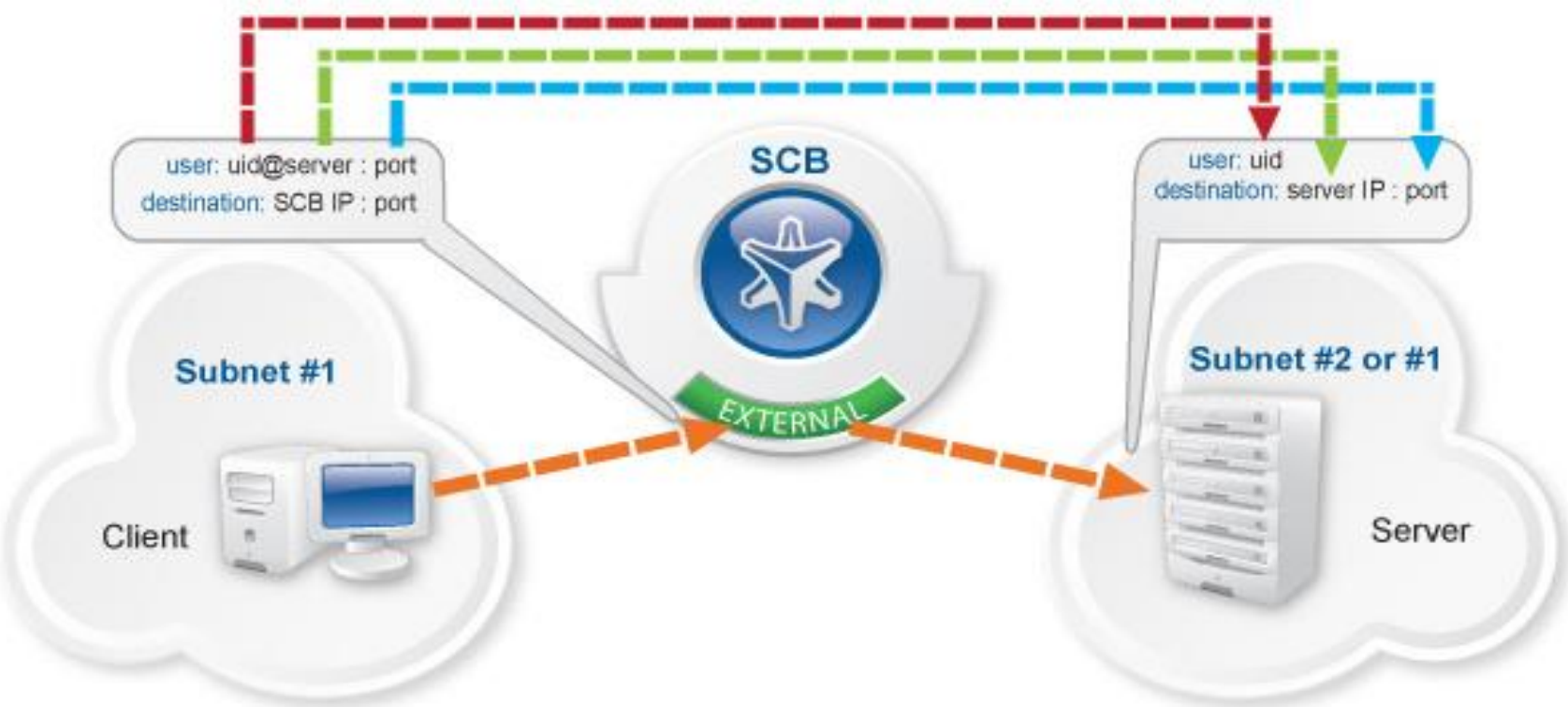
Bastion mode

Обращения только к SCB, защищаемые сервера не доступны. SCB определяет с каким сервером соединиться на основе параметров входящего соединения (IP адреса администратора и IP адреса и порта сервера назначения)



Nontransporent

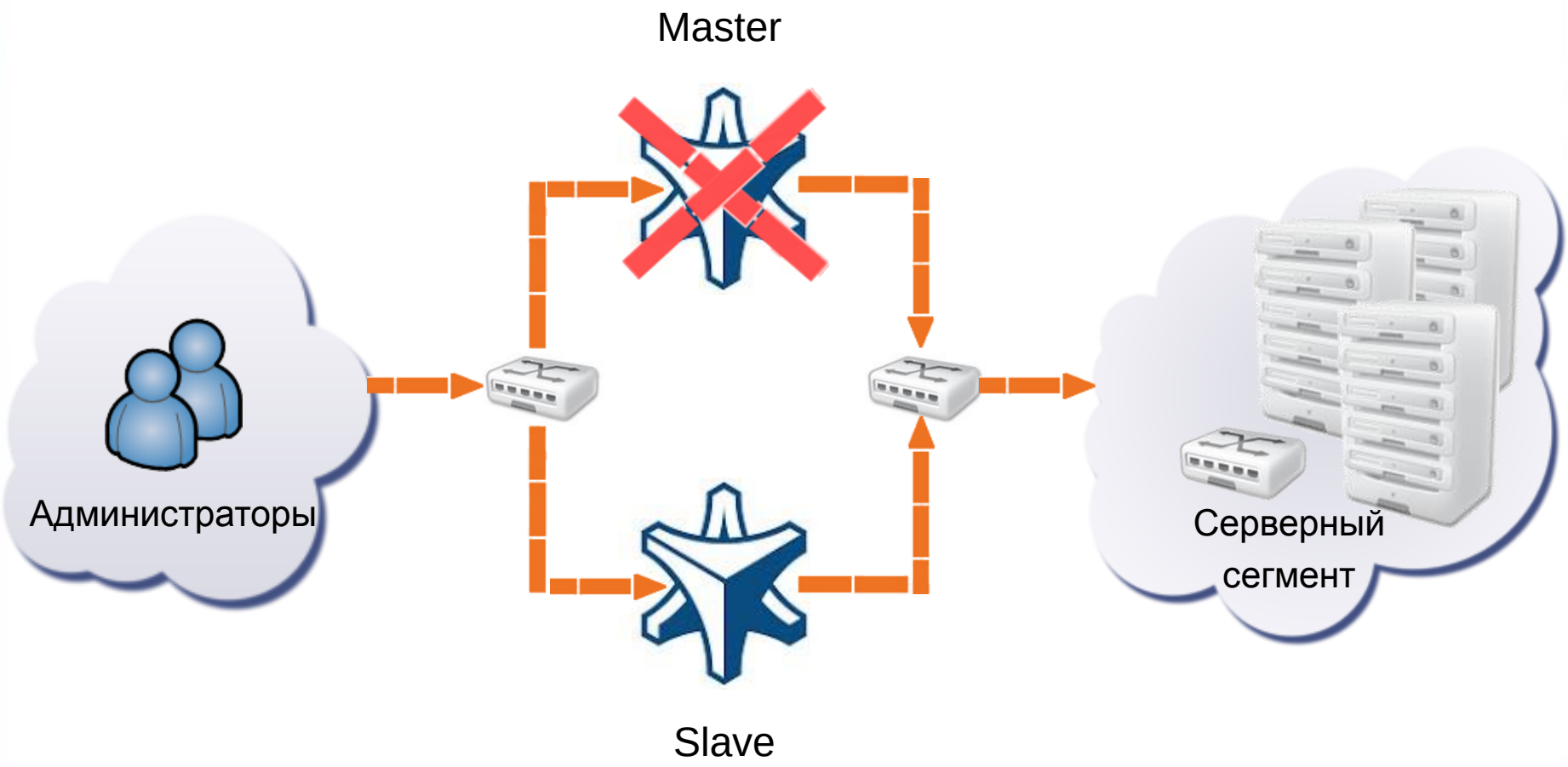
Разрешает доступ пользователей к серверам при помощи включения имени сервера назначения в имя пользователя:
username@targetserver:port@scb_address



ДиалОгНаука

Объединение в кластер

Обеспечение высокой доступности и отказоустойчивости



ДиалОгНаука

Примеры применения Shell Control Box

- Централизованное ограничение политик доступа
- Запрет парольной аутентификации через SSH
- Запись подключений терминальных клиентов
- Запрет доступа пользователя с именем «Администратор»
- Сервера доступны только в рабочее время
- Просмотр в реальном времени сессии с критическими серверами
- Помещение зашифрованных и подписанных данных аудита на CIFS сервер
- Передача SFTP файлов на DLP систему

ДиалогНаука

Варианты лицензирования

BalaBit Shell Control Box N1000

- 1xQuad Core CPU, 4 GB RAM, 1 TB HDD – RAID1.
- Лицензия для аудита 10 серверов, с возможностью расширения до неограниченного количества серверов

BalaBit Shell Control Box N1000d

- 2xQuad Core CPU, 24 GB RAM, резервный источник питания, 1 TB HDD – RAID1.
- Лицензия для аудита 10 серверов, с возможностью расширения до неограниченного количества серверов.

BalaBit Shell Control Box N10000

- 2xQuad Core CPU, 24 GB RAM, резервный источник питания, 10 TB HDD in internal storage, RAID 50.
- Лицензия для аудита 50 серверов, с возможностью расширения до неограниченного количества серверов.

BalaBit Shell Control Box VA

- Виртуальная машина для Vmware ESXi
- Лицензия для аудита 5 серверов, с возможностью расширения до неограниченного количества серверов.

Вопросы?

ЗАО «ДиалогНаука»
Телефон: +7 (495) 980-67-
Факс: +7 (495) 980-67-75

Роман Ванерке
http://www.DialogNauka.ru
e-mail: rv@DialogNauka.ru