ДиалОгНаука

18 апреля 2013 г.

# Websense Data Security

## защита от утечки конфиденциальной информации

***Ванерке Роман***

*Руководитель отдела технических решений*

*ЗАО «ДиалогНаука»*

ДиалогНаука

# Содержание

- Базовые понятия
- Проблематика утечек данных
- Основные этапы проекта
- Архитектура и возможности Websense Data Security
- Пример использования Websense Data Security
- Выводы

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.

ДиалОгНаука

# Что является ценным для Компании?

Клиентская база (физические и юридические лица)


Схемы работы

Условия работы

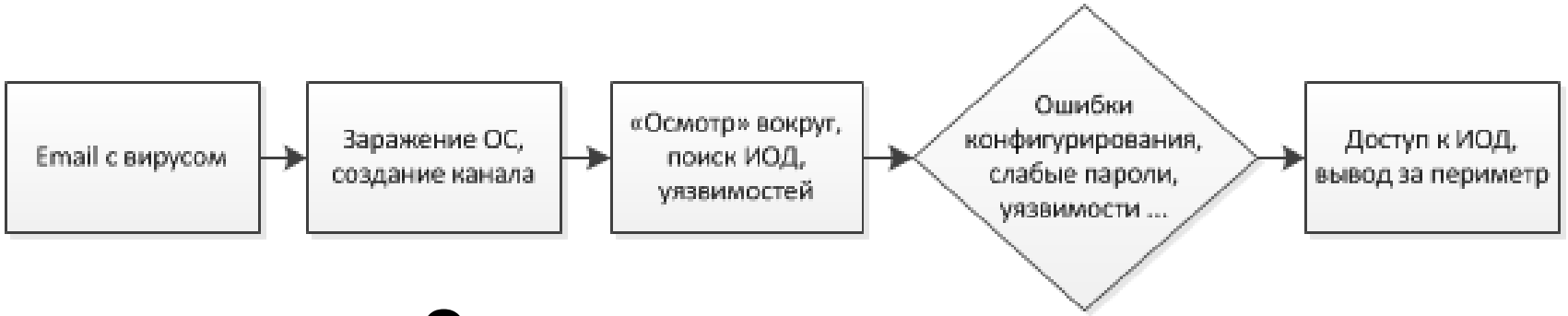
Стратегические планы, новые продукты, изменения, маркетинговые акции


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

# 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

# Стоимость утечки

- По западной статистике стоимость утечки одной записи ~ **200$** (прямые убытки, затраты на решение проблемы, оповещение, судебные тяжбы и т.п.)
- Оценить репутационные риски крайне трудно
  - По разным оценкам от 5% годовой выручки до потери бизнеса.
- Законопроект № 12389-6 «О внесении изменений в КоАП РФ».
  - Ст. 13.11. Нарушение установленного законодательством РФ порядка обработки ПДн:
    - Для должностных лиц – от 30 000 до 50 000 руб.
    - Для юридических лиц– **от 200 000 до 500 000 руб**.
  - Повторное нарушение:
    - Для должностных лиц – 50 000 руб. или дисквалификация до года
    - Для юридических лиц – **от 500 000 до 1 000 000 руб.**

ДиалогНаука

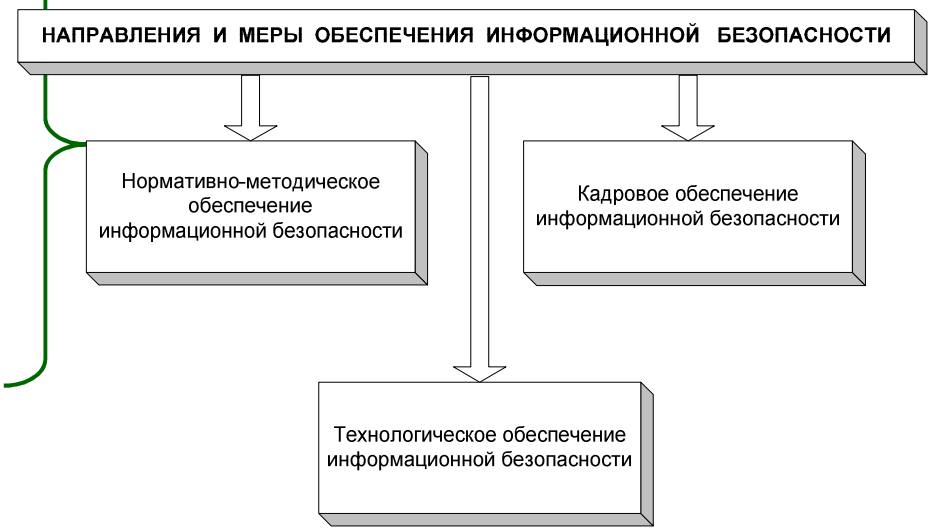

# Зачем защищаться?

- 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

ДиалогНаука

# 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

# Возврат инвестиций (ROSI, ALE и т.п.)

- **ROI** – плохо применима для оценки систем ИБ
- **ROSI** – оценка затрат потенциального ущерба (утечки) к стоимости владения системой (TCO)
  - Необходима оценка рисков, чтобы понимать возможный ущерб при утечке тех или иных данных
- **ALE** – учитывается стоимость одной утечки и количество утечек в год
  - Необходимо знать стоимость одного инцидента
  - Необходимо иметь статистику по инцидентам в Компании

ДиалогНаука

# Сравнение Websense с InfoWatch

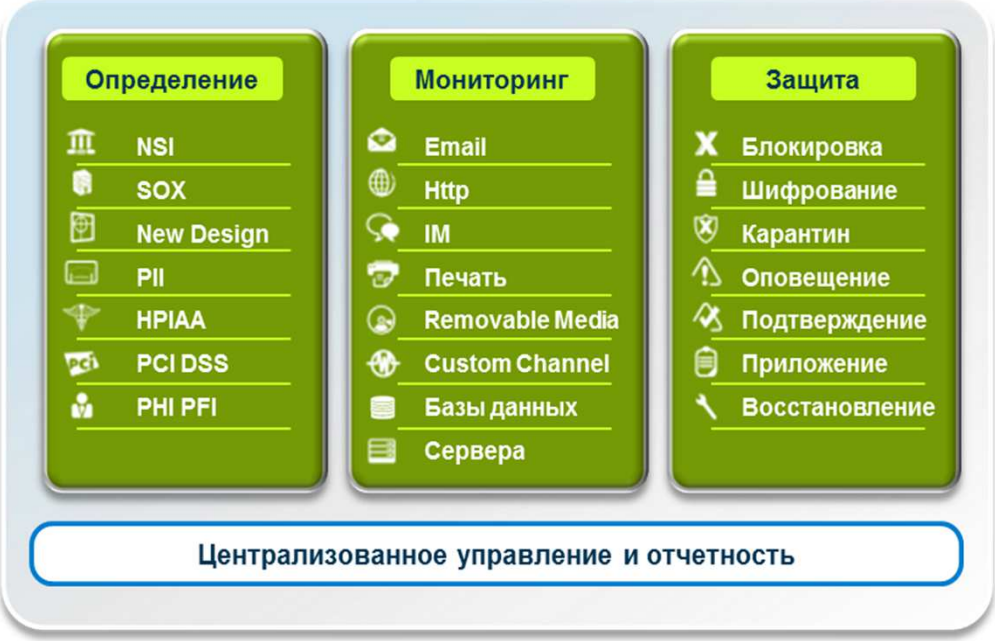
| Websense Data Security Suite | InfoWatch Traffic Monitor Enterprise |
|---|---|
| Технология цифровых отпечатков PreciseID™ (международный патент), 27+ алгоритмов опознавания конфиденциальной информации | Лингвистический анализатор локальной разработки; технология цифровых отпечатков (выпущена в конце 2009 года) |
| Обнаружение ИОД из СУБД методами цифровых отпечатков | отсутствует |
| SMTP, HTTP/HTTPS, FTP, ICQ, Skype, сетевая и локальная печать, съемные носители | SMTP, HTTP/HTTPS, ICQ, сетевая и локальная печать, съемные носители |
| Аудит и обнаружение ИОД в сети и на рабочих станциях | отсутствует |
| Достаточно использования СУБД MS SQL Express | Использование промышленной СУБД Oracle 11g |
| Средняя трудоемкость внедрения | Высокая трудоемкость внедрения |

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

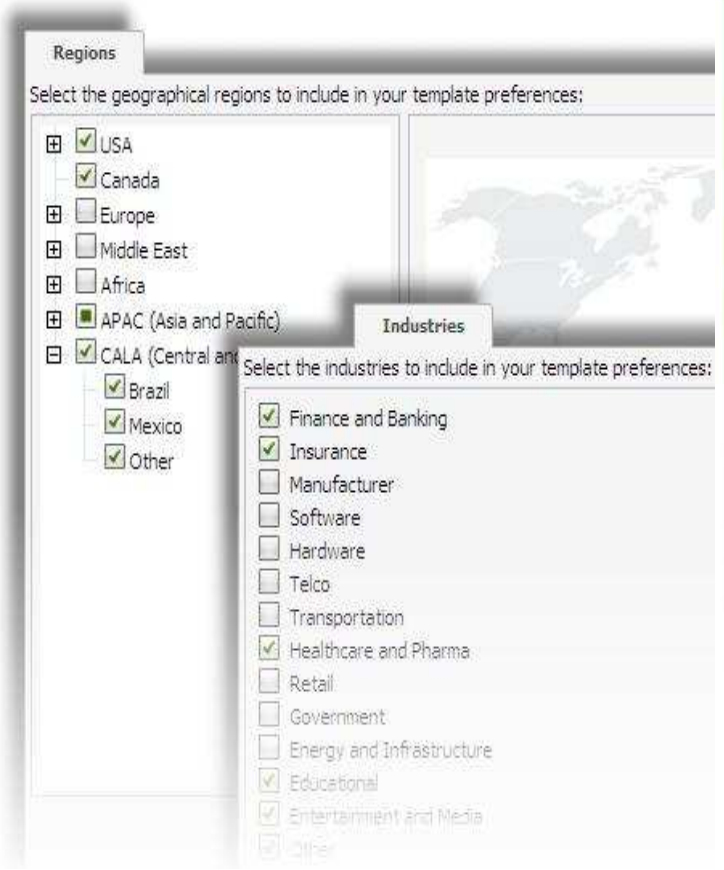
Цифровые отпечатки

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

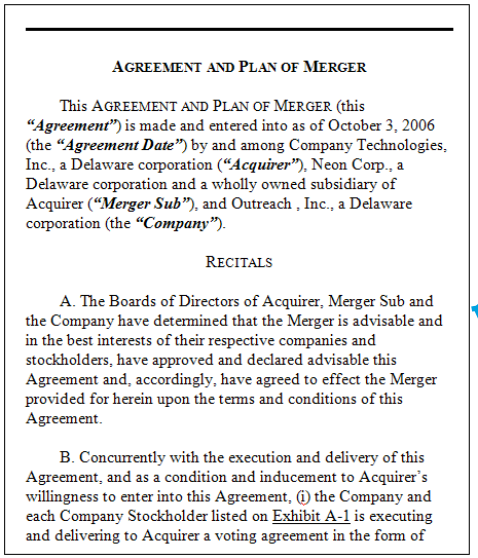
- Цифровые отпечатки – все режиме для чтения:
  - Баз данных
  - Сетевых каталогов
  - SharePoint
  - SalesForce.com


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

ДиалОгНаука

# Высокая устойчивость к изменению

## Данные внутри защищённого файла



AGREEMENT AND PLAN OF MERGER

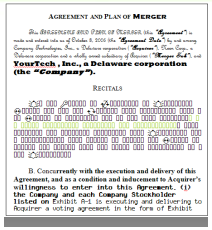
This AGREEMENT AND PLAN OF MERGER (this *"Agreement"*) is made and entered into as of October 3, 2006 (the *"Agreement Date"*) by and among Company Technologies, Inc., a Delaware corporation (*"Acquirer"*), Neon Corp., a Delaware corporation and a wholly owned subsidiary of Acquirer (*"Merger Sub"*), and Outreach , Inc., a Delaware corporation (the *"Company"*).

RECITALS

A. The Boards of Directors of Acquirer, Merger Sub and the Company have determined that the Merger is advisable and in the best interests of their respective companies and stockholders, have approved and declared advisable this Agreement and, accordingly, have agreed to effect the Merger provided for herein upon the terms and conditions of this Agreement.

B. Concurrently with the execution and delivery of this Agreement, and as a condition and inducement to Acquirer's willingness to enter into this Agreement, (i) the Company and each Company Stockholder listed on Exhibit A-1 is executing and delivering to Acquirer a voting agreement in the form of

***Изменение формата***

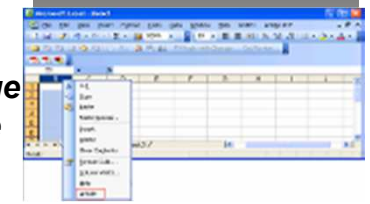


***Изменение типа файла***

***Зашумление (flooding)***

***Копирование и вставка***

***Скрытые данные***



***Изменение структуры***

***Встраиваемые файлы***

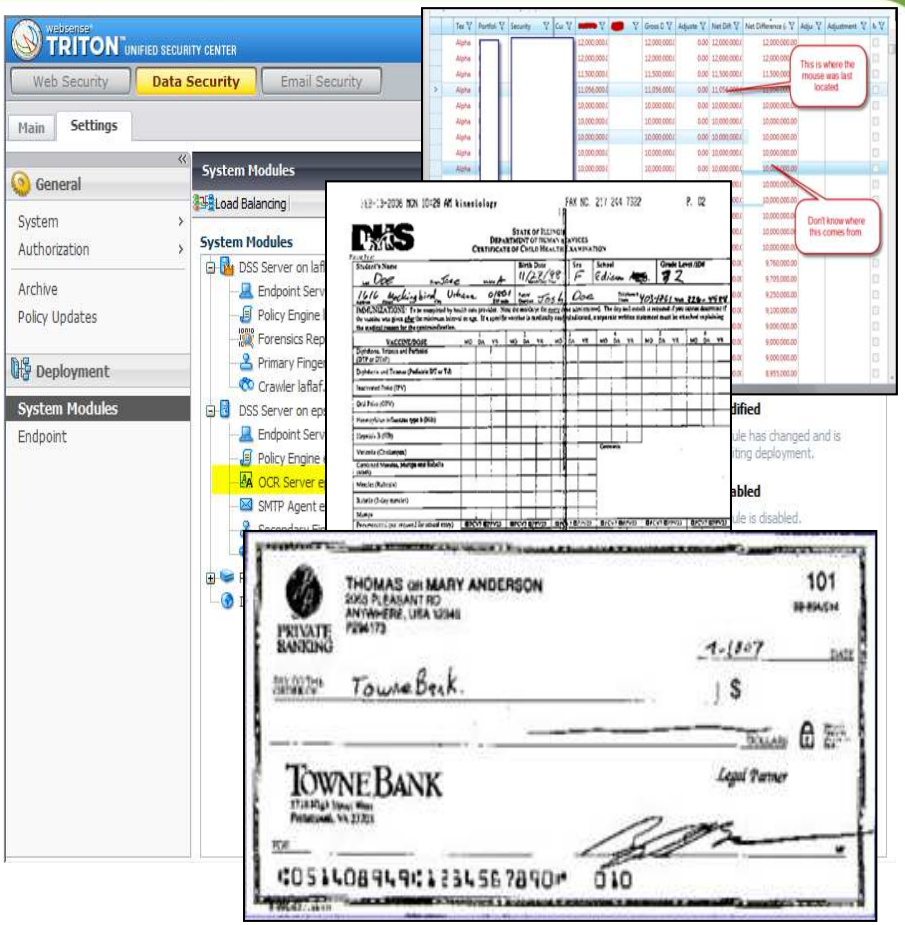
# Machine Learning (ИИ)

- 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

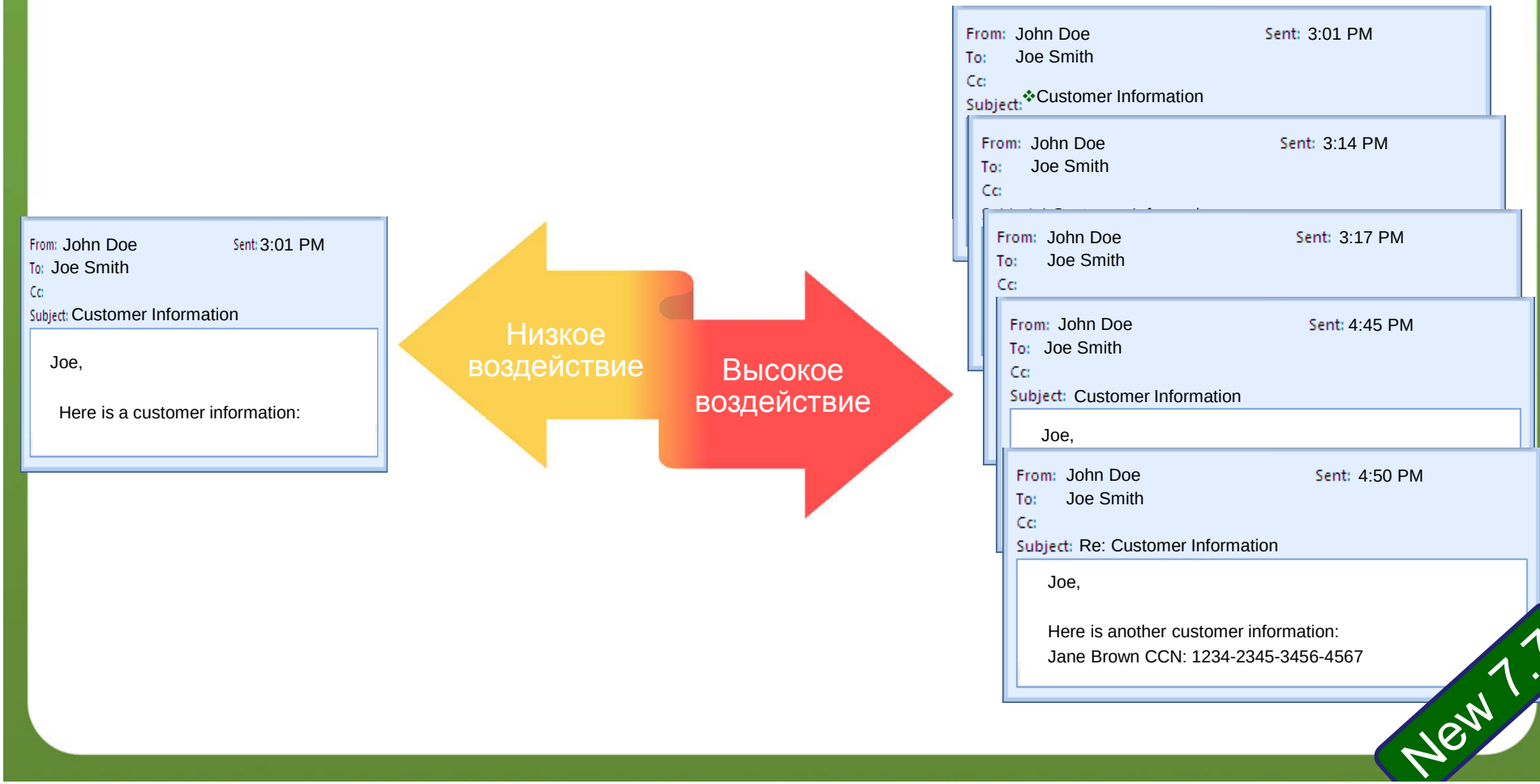



New 7.7

# Идентификация «медленных» утечек

- Идентификация утечек за промежуток времени

❖**Within 2 Hours**



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

ДиалогНаука

# Каналы и реагирование


* 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

# Web Linking Service


**Competitor Alerts**

Data: HIPAA

Source: 10.14.222.21

Channel: Web

Destination: 92.10.219.62

**Websense Alerts**

Data: HIPAA & PII, Customer Database

Source: Tina Doh x1234
tinad@acmehosptial.com
Title: Associate
Dept. Accounting
Manager: Mike Brown

Channel: Web

Destination: gmail.com
Type: Personal webmail site
Location: Mountain View, CA

Интеграция Websense Web и Data Security.

Разрешение IP источника и назначения в реальном времени.

Dramatically Reduces Operational Bottlenecks:

- Manual look up of source and destination IP address
- Approx. 10 minutes each
- Hundreds to thousands web incidents a day

ДиалогНаука

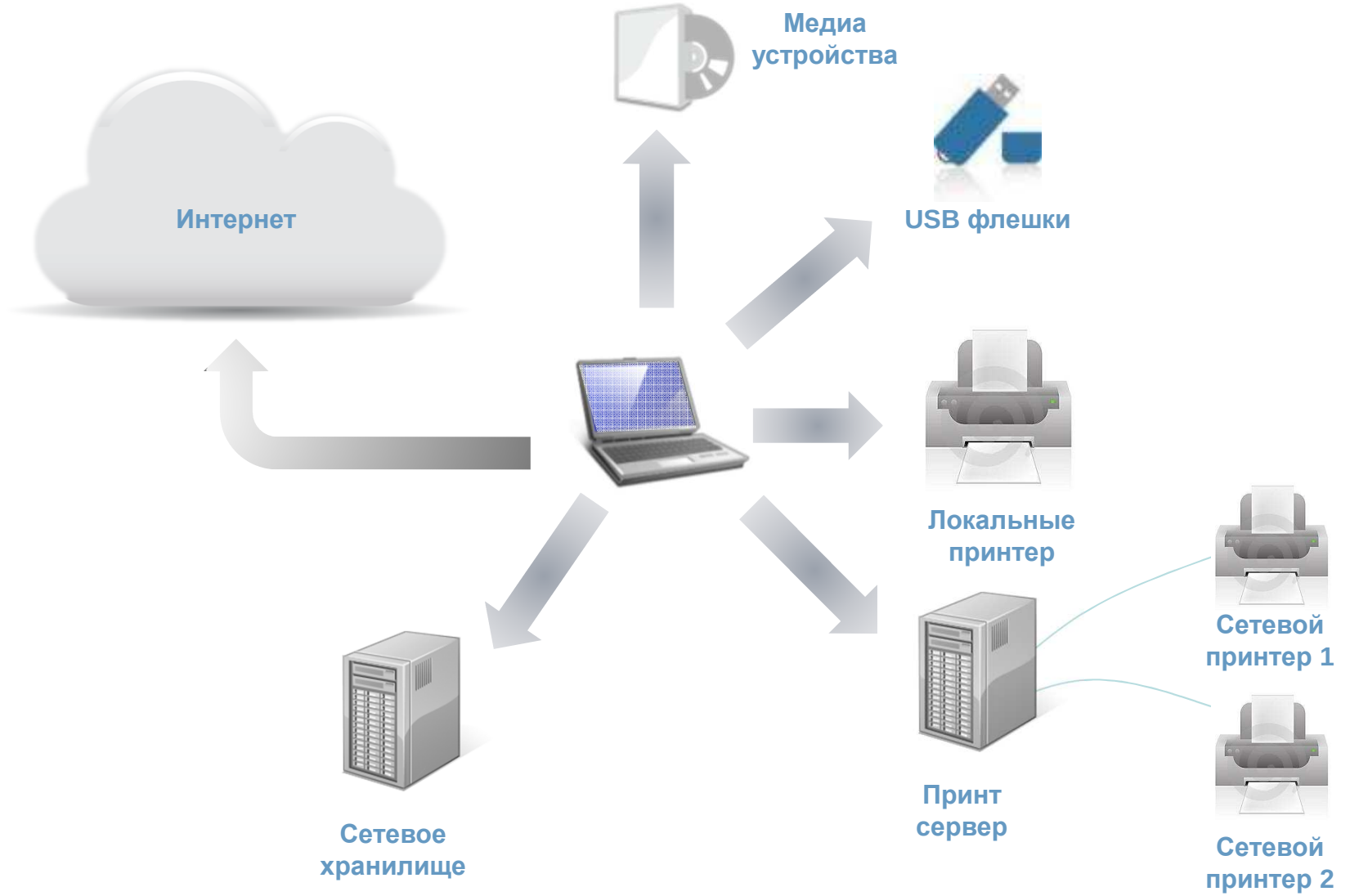
# Endpoint DLP

***Использование***

***(Data-in-Use)***

ДиалогНаука

# Каналы утечки на уровне АРМ



ДиалогНаука

# 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


- Применяется к конкретным группам приложений

Resources > **Endpoint Application Groups**

New... | Delete

Create or view a list of application groups you want to monitor on the endpoint, aside from those on the default Websense list.

| 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 |

# Шифрование файлов (USB)

- **Вариант 1: Требуется DLP Endpoint**
  - Родное шифрование с помощьюDLP Endpoint
  - Не требуется пароль
  - Для дешифрования требуется DLP Endpoint

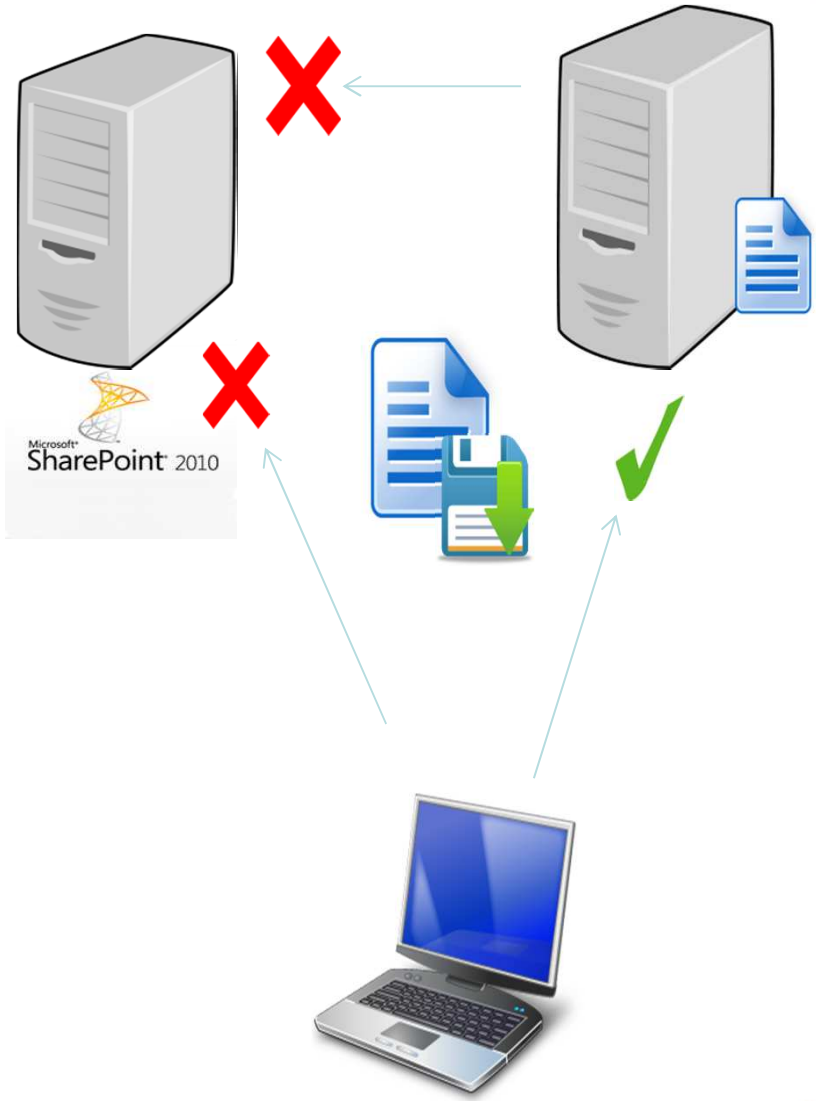
- **Вариант 2: Портативное шифрование**
  - Родное шифрование с помощьюDLP Endpoint
  - Утилита для дешифрования копируется на USB
  - Пользователь задает пароль
  - Дешифрование с внешних систем с использованием утилиты дешифрования

Пользователь задает пароль

ДиалогНаука

# Контроль LAN

- Контроль мест хранения конфиденциальных данных
- Преимущества:
  - Управление распространением данных (контроль границ ИСПДн, например)
  - Минимизация неавторизованного доступа
  - Улучшенное управление данными



# 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

# Поддерживаемые платформы

| | |
|---|---|
| **Клиенты Endpoint** | Windows 7 32 & 64 bit |
| | Windows Vista 32 & 64 bit |
| | Windows XP 32 & 64 bit |
| | Windows Server 2008 32 & 64 bit |
| | Windows Server 2003 32 & 64 bit |
| | MAC OSX 10.6 – Snow Leopard – 32 & 64 bit |
| | MAC OSX 10.7 – Lion – 32 & 64 bit |
| | Linux - USB and Discovery |

**v. 7.7.2 (Август 2012)**

- Removable media write
- CD write
- Discovery
- File Access
- Endpoint LAN
- Endpoint Email
- Trusted Applications
- Anti-Tampering

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

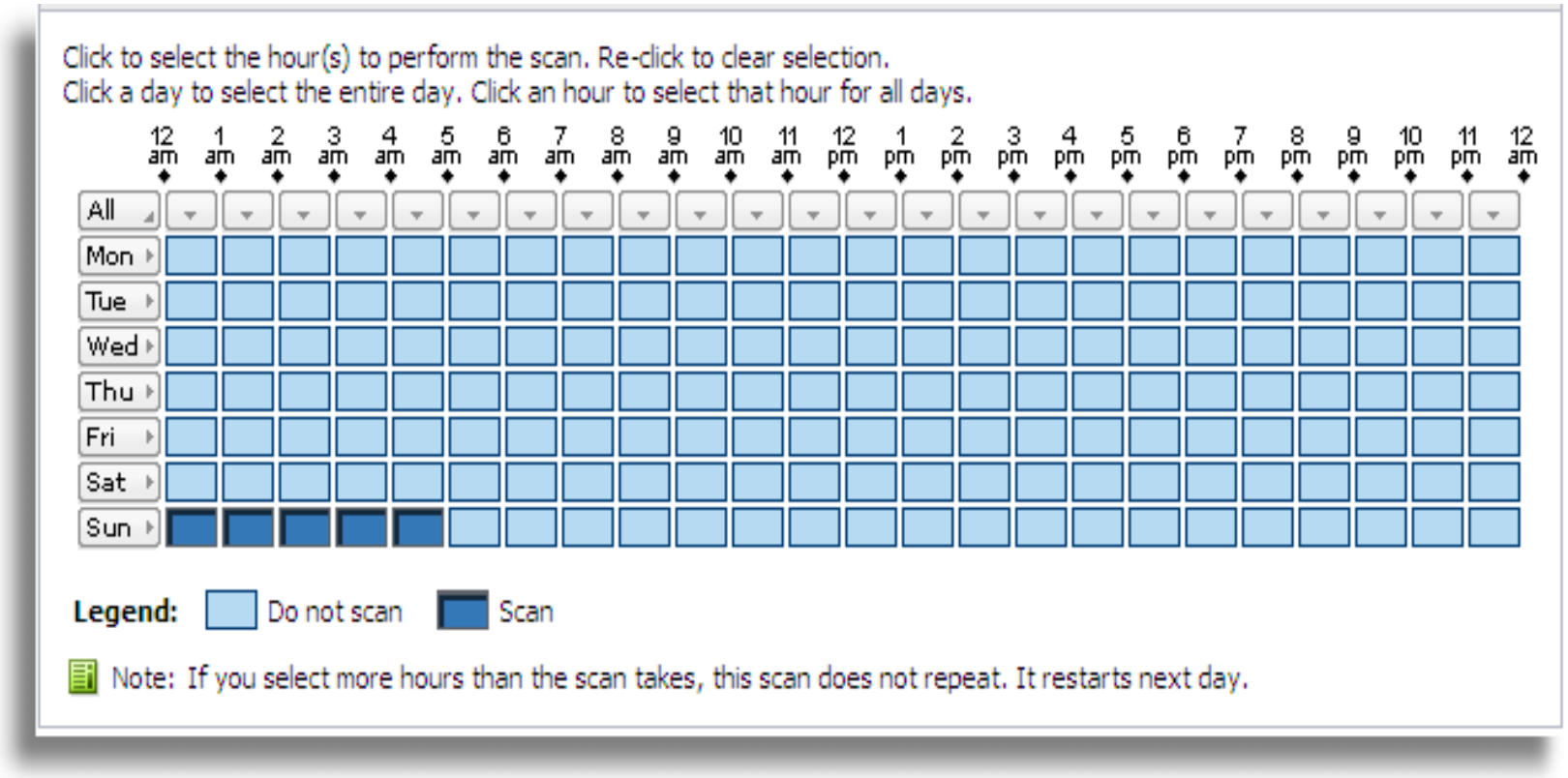
**Гибридный**


- Лучшее вариант
- Использование любой комбинации

ДиалогНаука

# Расписание

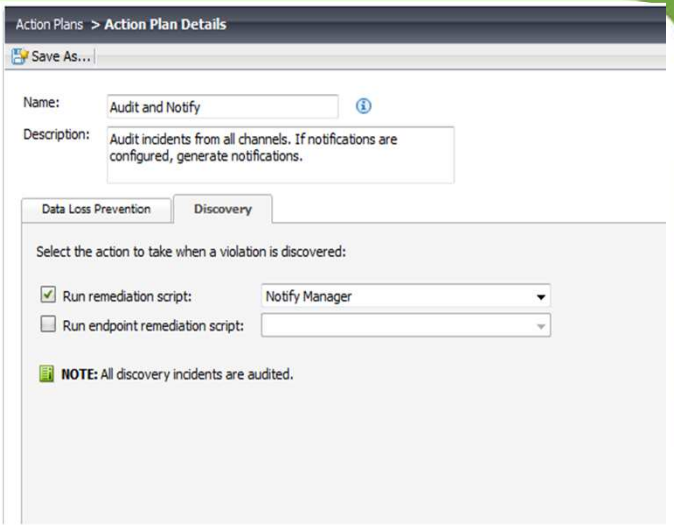
- Гибкая настройка расписания задач Discovery
  - Единожды или Повторяющиеся в определенные дни/часы



ДиалогНаука

# 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

# 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

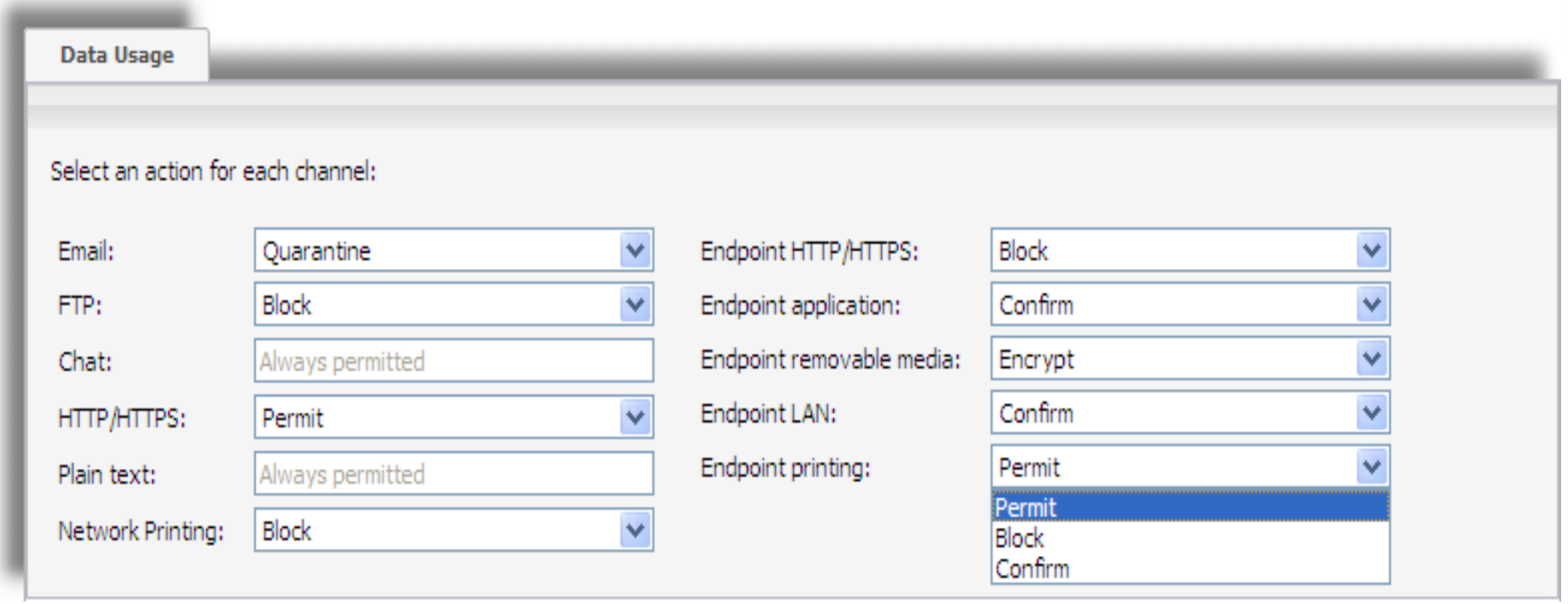
# Управление системой


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

ДиалогНаука

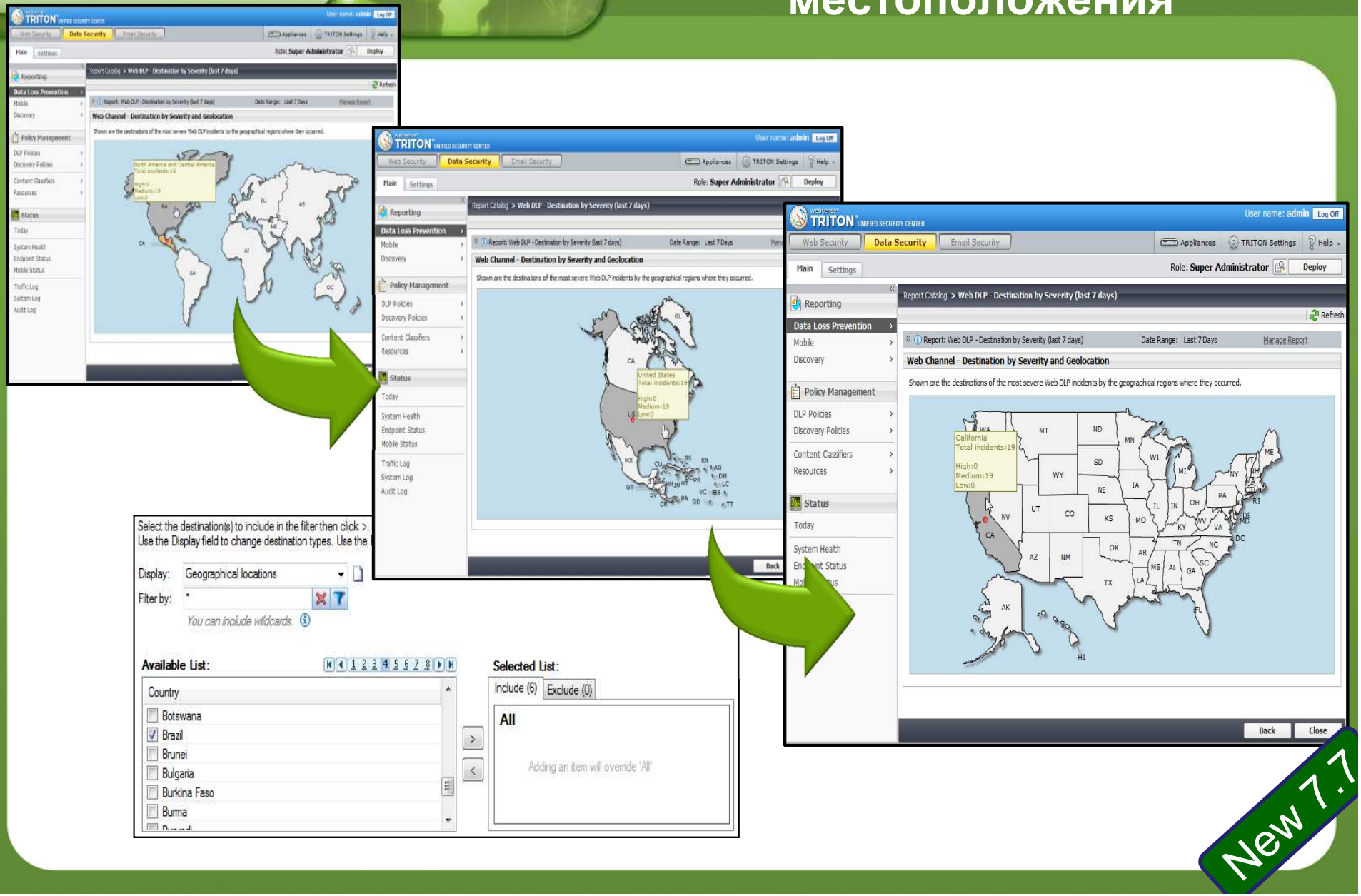
# Единая структура политик

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



ДиалОгНаука

# Применение политик в зависимости от местоположения



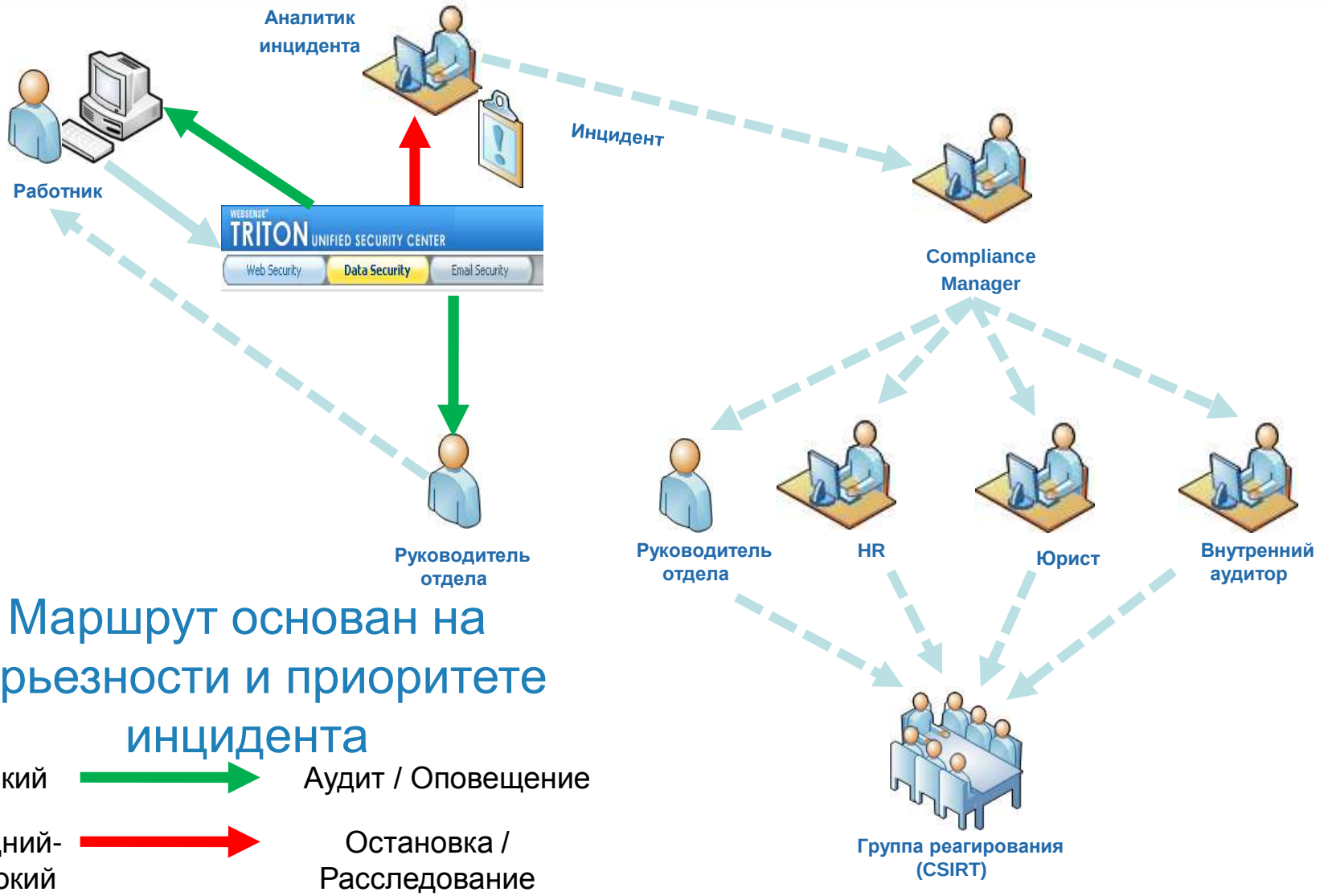

New 7.7

ДиалогНаука

# Автоматизация реагирования

ДиалогНаука

# Анализ инцидента (Логика)




## Маршрут основан на серьезности и приоритете инцидента

Низкий → Аудит / Оповещение

Средний-Высокий → Остановка / Расследование

ДиалОгНаука

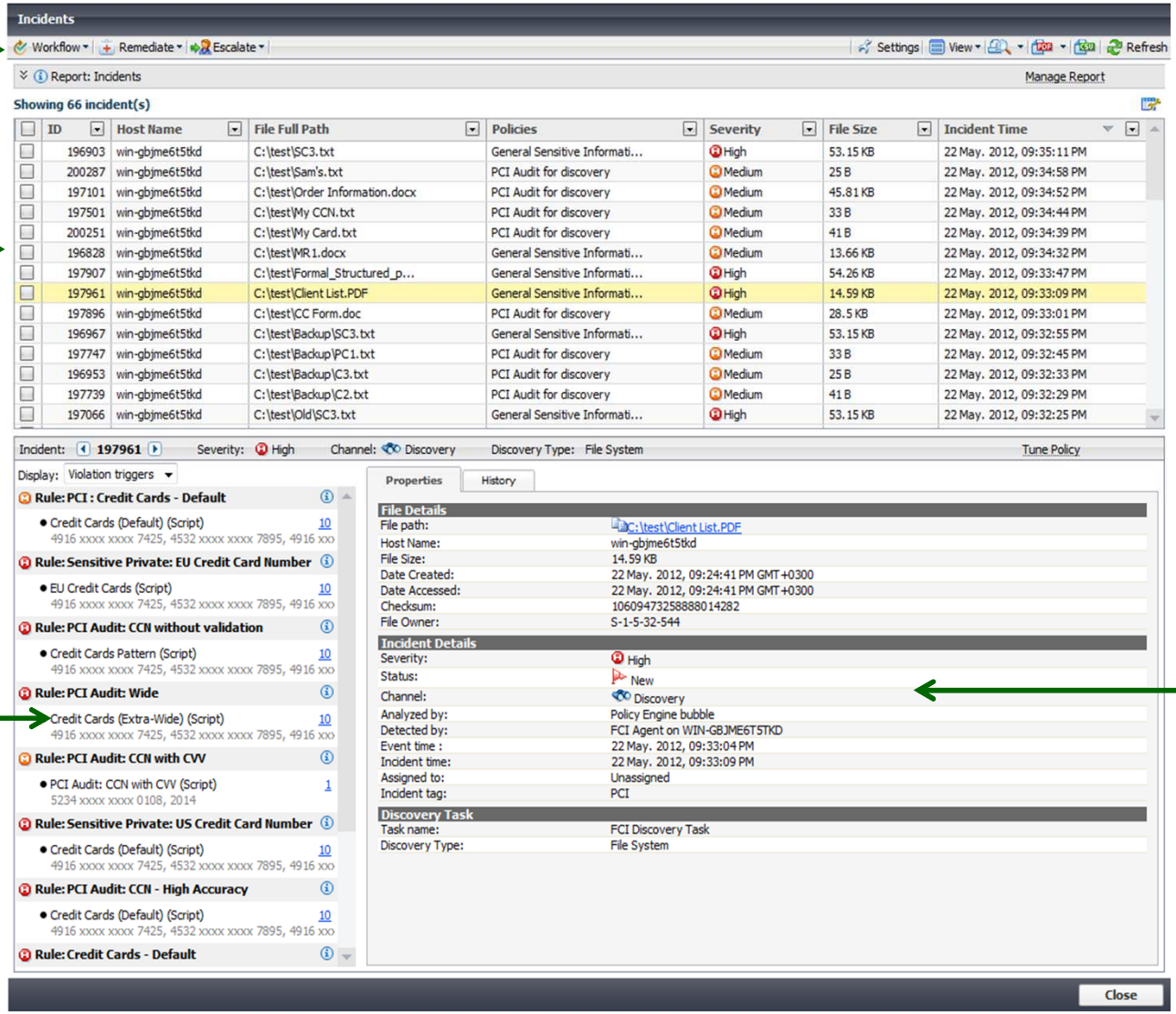
# Управление инцидентами

Принятие мер

Список инцидентов

Триггеры нарушения

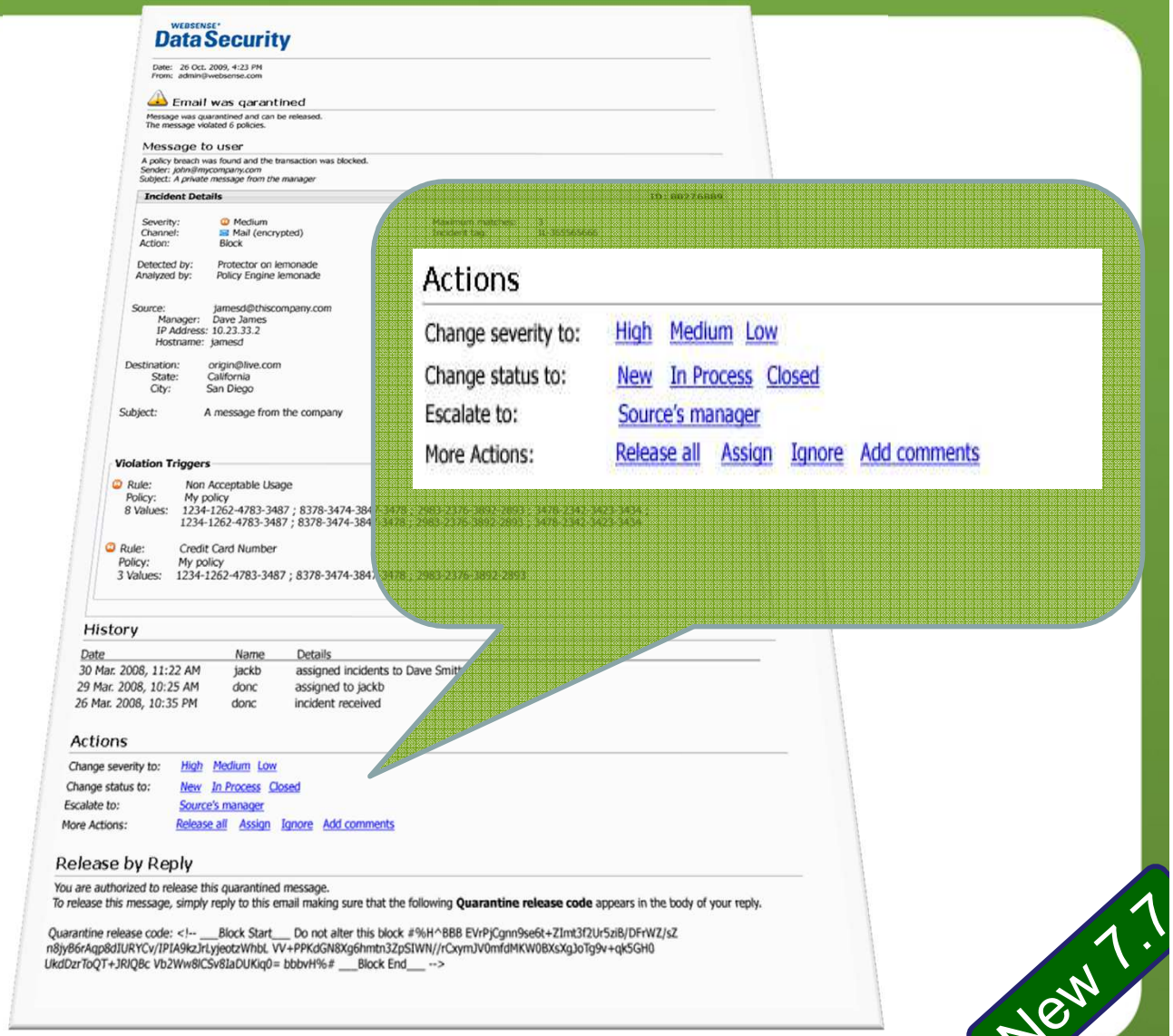
Детали инцидента



ДиалОгНаука

# Управление инцидентом с использованием почты

- Выбор действий из оповещения:
  - изменение серьезности
  - эскалация
  - назначение
  - игнорирование
  - и др.




New 7.7

ДиалОгНаука

# Исследовательские отчеты

- Дает представление
  - Топ Web получателях п
  - 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

| 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 |

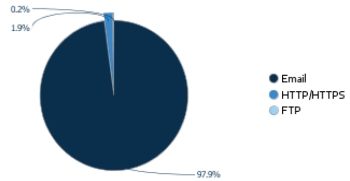
ДиалОгНаука

# 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…

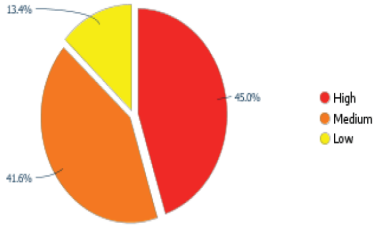
Top 5 Channels

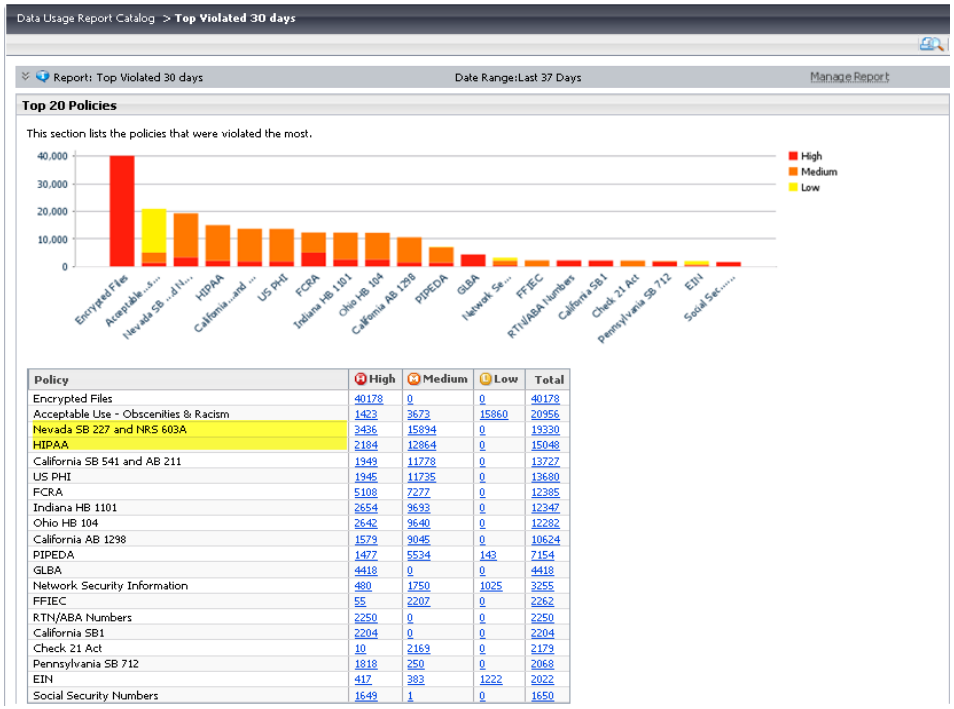
| Channel | Incidents |
|---|---|
| Email | 93362 |
| HTTP/HTTPS | 1780 |
| FTP | 189 |




Incidents by Severity

| Severity | Incidents |
|---|---|
| High | 42887 |
| Medium | 39660 |
| Low | 12784 |




| Policy | High | Medium | Low | Total |
|---|---|---|---|---|
| Encrypted Files | 40178 | 0 | 0 | 40178 |
| Acceptable Use - Obscenities & Racism | 1423 | 3673 | 15860 | 20956 |
| Nevada SB 227 and NRS 603A | 3436 | 15894 | 0 | 19330 |
| HIPAA | 2184 | 12864 | 0 | 15048 |
| California SB 541 and AB 211 | 1949 | 11778 | 0 | 13727 |
| US PHI | 1945 | 11735 | 0 | 13680 |
| FCRA | 5108 | 7277 | 0 | 12385 |
| Indiana HB 1101 | 2654 | 9693 | 0 | 12347 |
| Ohio HB 104 | 2642 | 9640 | 0 | 12282 |
| California AB 1298 | 1579 | 9045 | 0 | 10624 |
| PIPEDA | 1477 | 5534 | 143 | 7154 |
| GLBA | 4418 | 0 | 0 | 4418 |
| Network Security Information | 480 | 1750 | 1025 | 3255 |
| FFIEC | 55 | 2207 | 0 | 2262 |
| RTN/ABA Numbers | 2250 | 0 | 0 | 2250 |
| California SB1 | 2204 | 0 | 0 | 2204 |
| Check 21 Act | 10 | 2169 | 0 | 2179 |
| Pennsylvania SB 712 | 1818 | 250 | 0 | 2068 |
| EIN | 417 | 383 | 1222 | 2022 |
| Social Security Numbers | 1649 | 1 | 0 | 1650 |

ДиалогНаука

# Угрозы

Случайные

Преднамеренные (незлоумышленные)

Инсайдер

Внешний злоумышленник

## ОБУЧЕНИЕ РАБОТНИКОВ

Готовые шаблоны, оповещения/подтверждения, самостоятельный релиз

## ВИДИМОСТЬ

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

## РАСШИРЕННОЕ ДЕТЕКТИРОВАНИЕ

Drip DLP, контроль приложений, OCR распознавание

## WEBSENSE SECURITY LABS (ACE)

Дешифрование SSL, URL категории, геолокация, неавторизованное шифрование

ДиалОгНаука

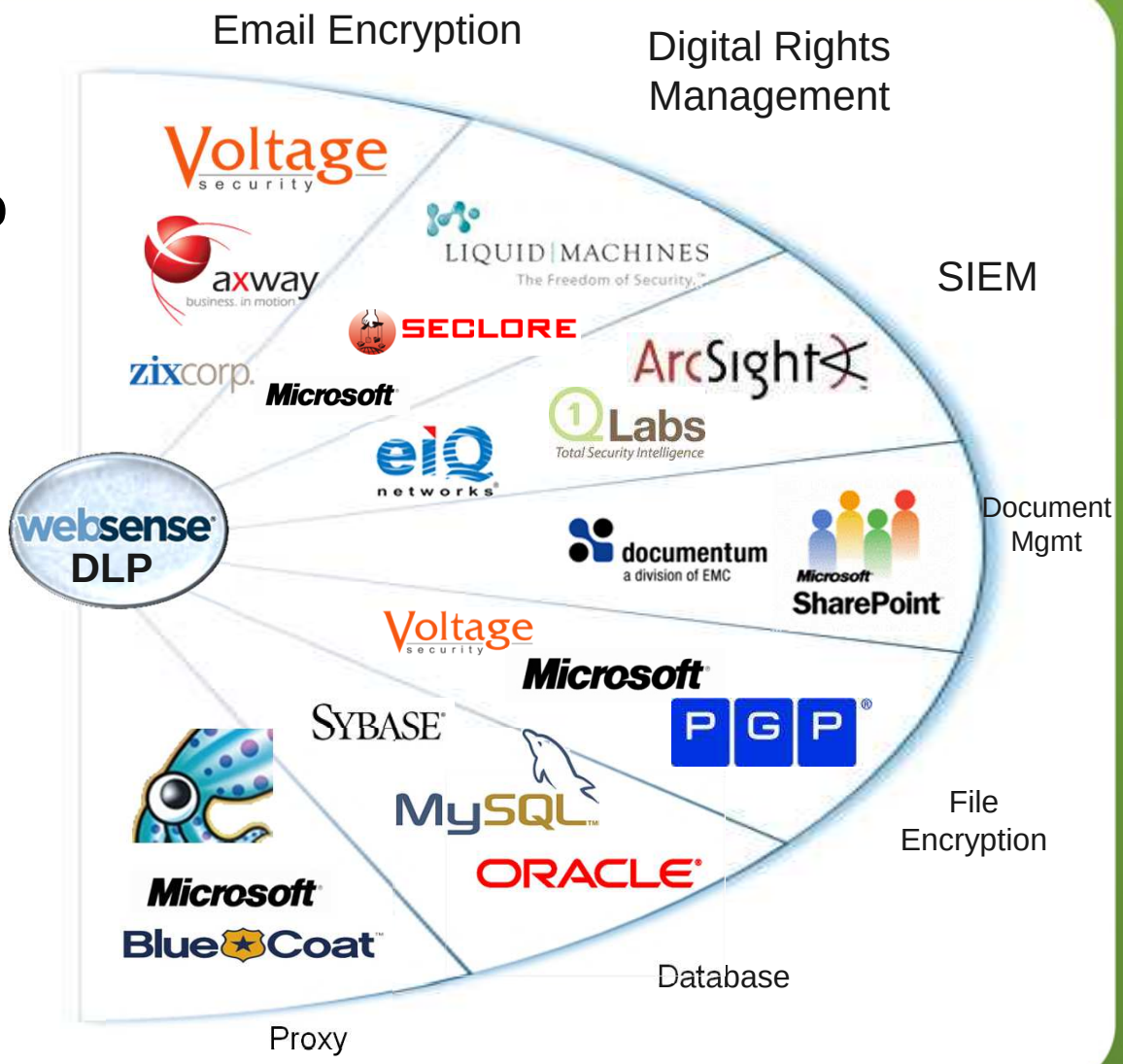
# Data Security

*Интеграция технологий*

ДиалогНаука

# Интеграция в ИТ-инфраструктуру

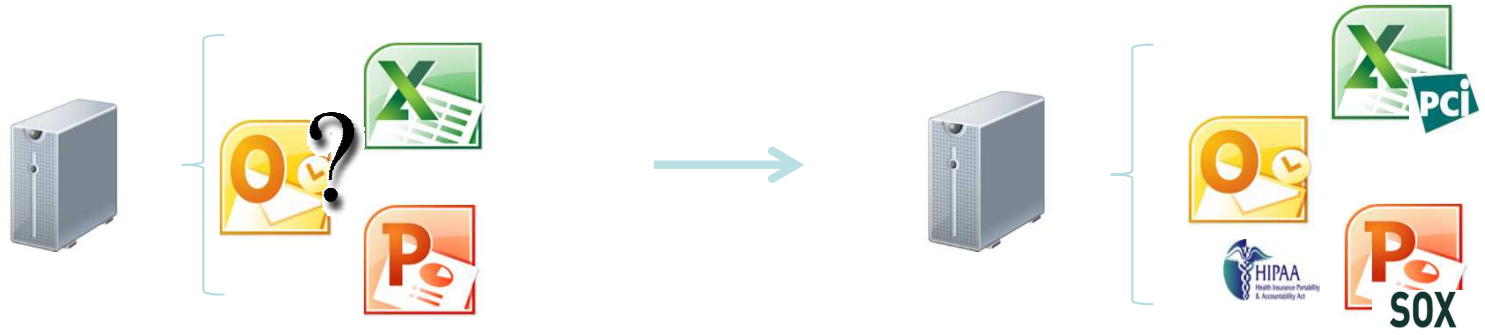
- DLP – это краеугольный камень программ по защите данных
- Основанный на стандартах обеспечивает совместимость с решениями третьих компаний (Open API и ICAP)



ДиалогНаука

# Интеграция с Microsoft FCI

- Обеспечивает классификацию данных
- Microsoft File Classification Infrastructure использует Websense DLP для классификация контента как он сохраняется на сервере
- Конфиденциальные документы тегируются на основе контента (PCI, SOX, HIPPA)
- Microsoft Dynamic Access Control назначает Группам/Пользователям права доступа к КИ

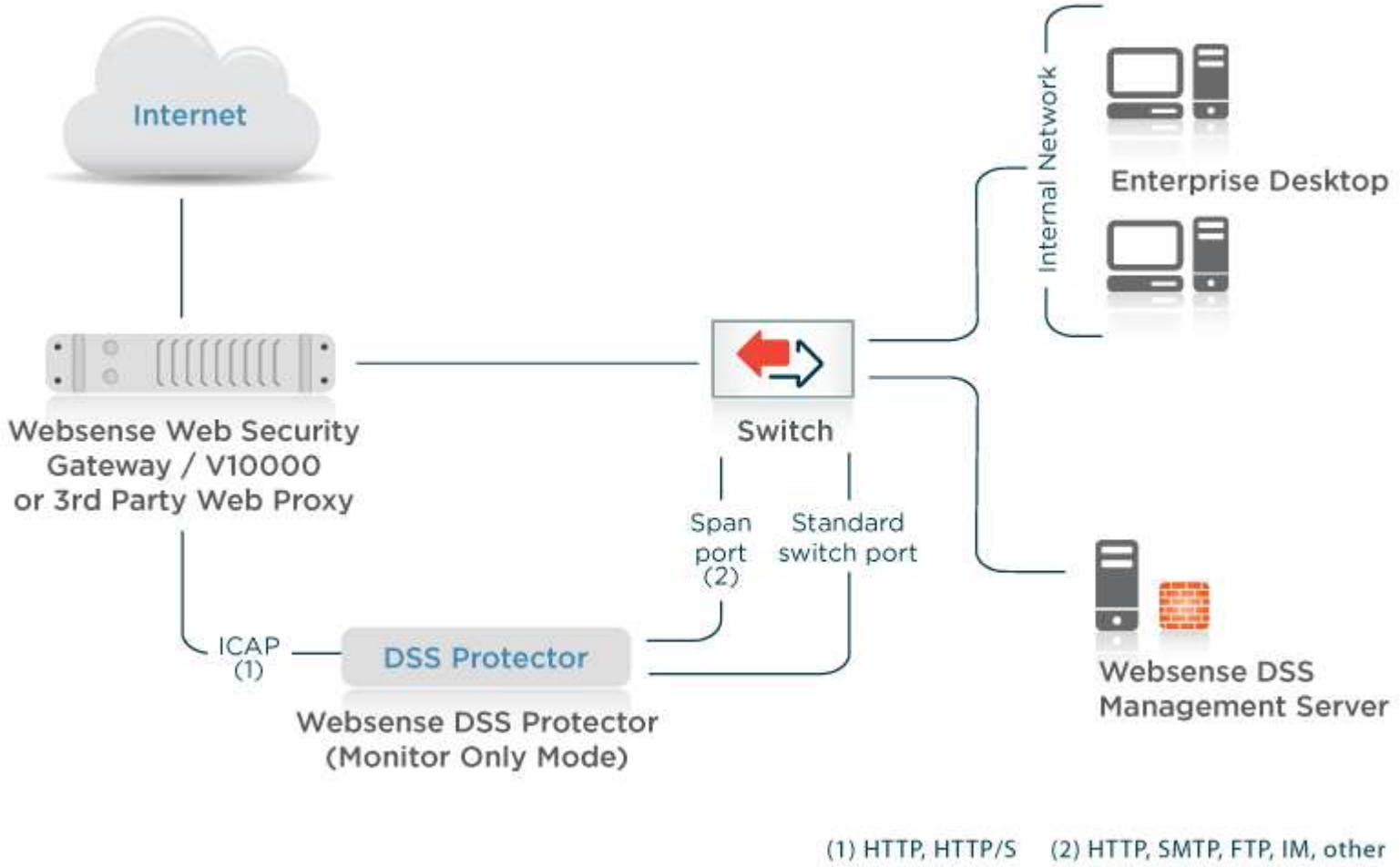



ДО

ПОСЛЕ

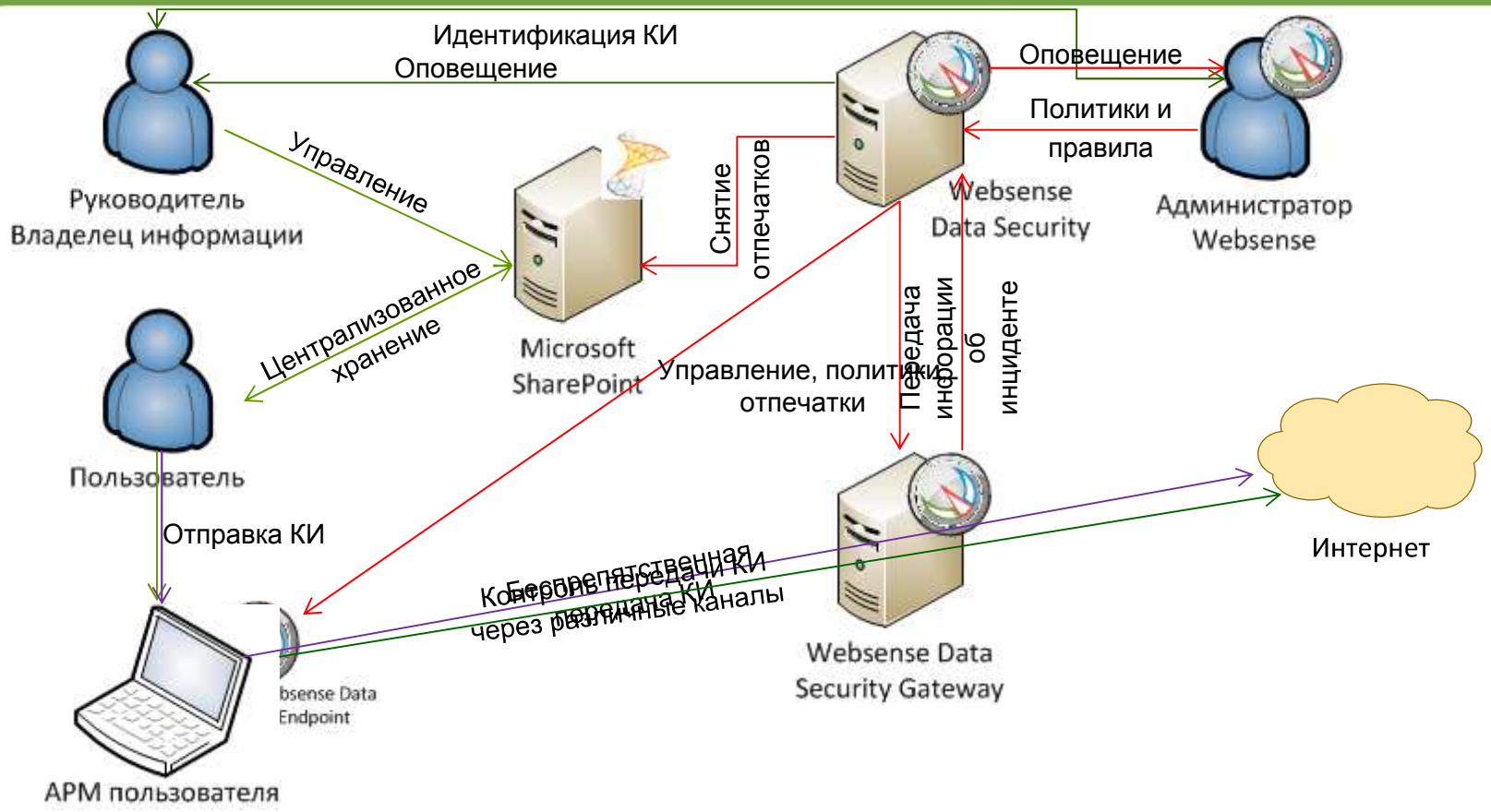
ДиалогНаука

# Архитектура
# Пассивный мониторинг



ДиалОгНаука

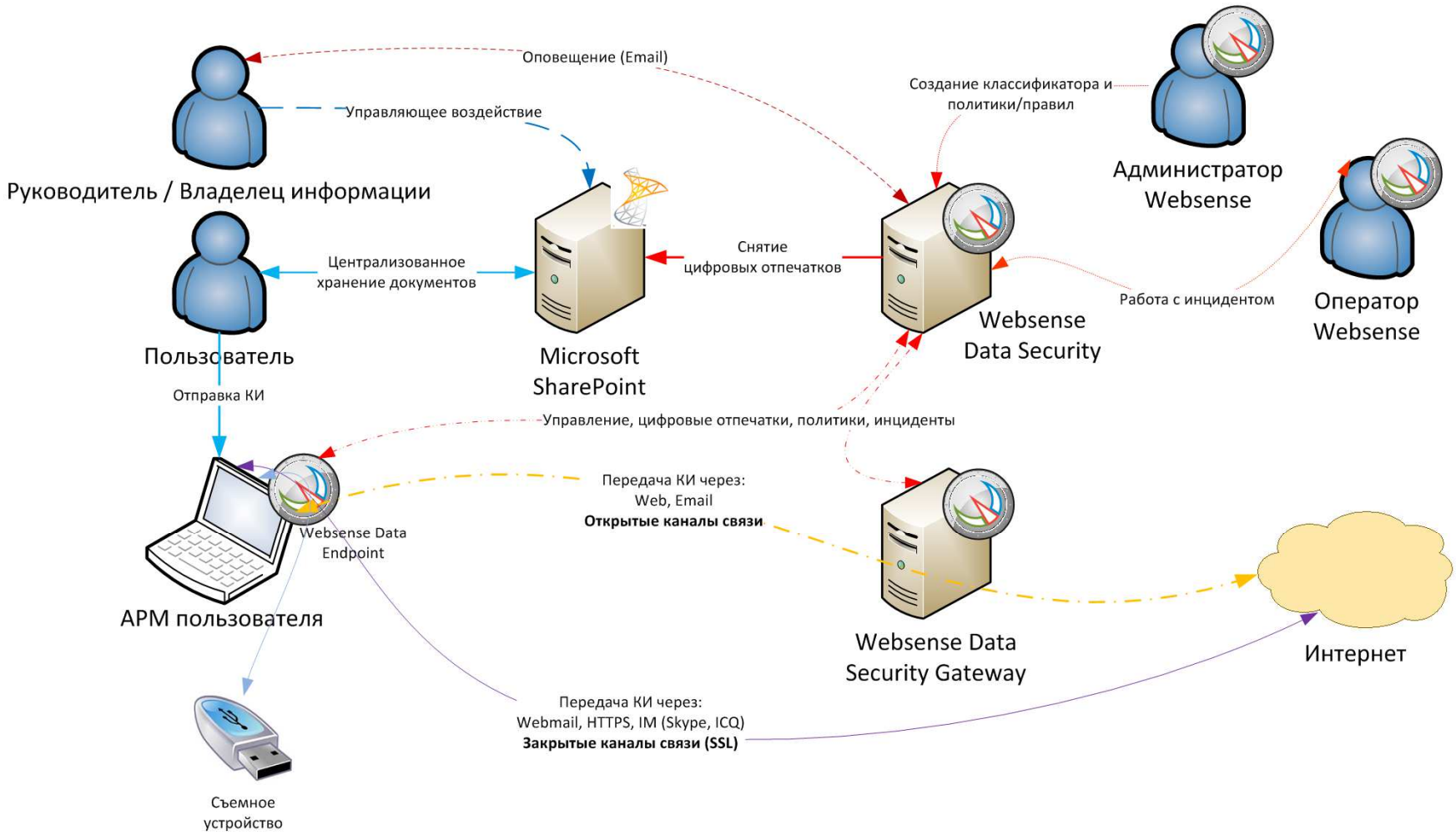
# Пример. Интеграция с SharePoint




Простые и удобные механизмы интеграции системы в инфраструктуру для работы с КИ

ДиалОгНаука

# Тоже самое, только картинка посложнее ☺



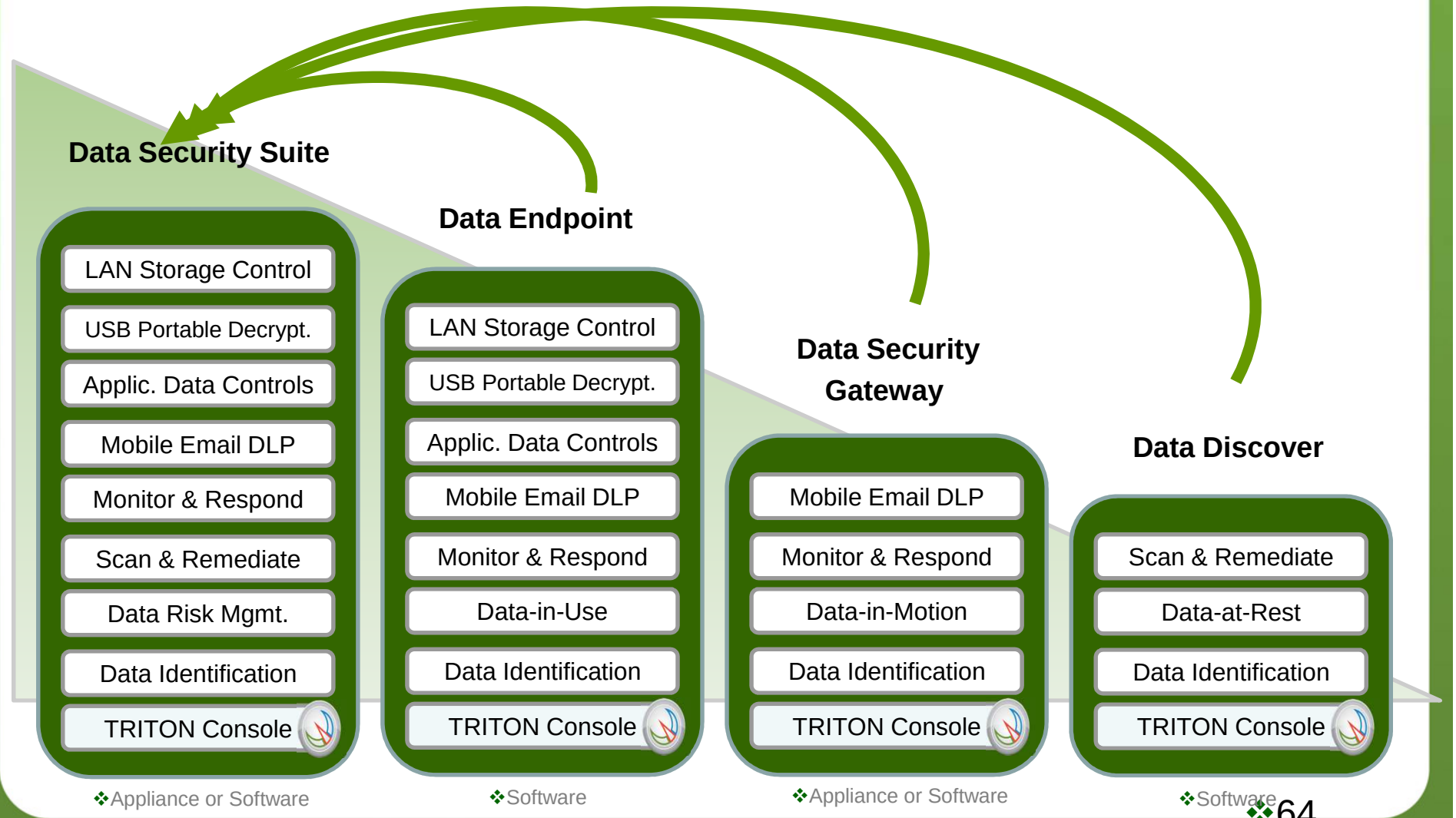
ДиалОгНаука

# Решение Websense DLP

*Пакеты*

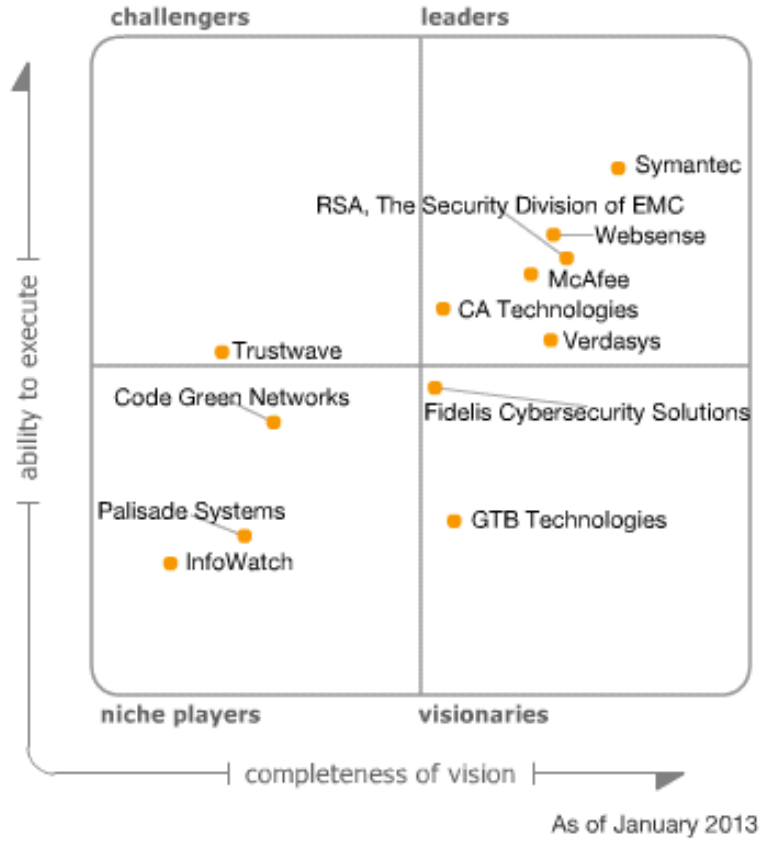
ДиалогНаука

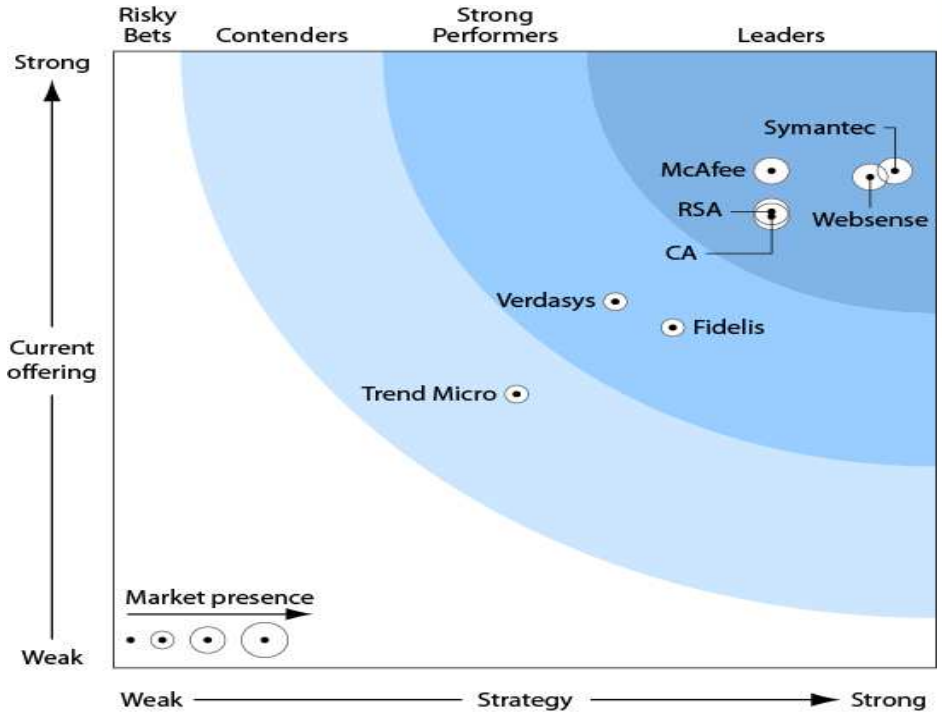
# Пакеты Data Security



ДиалогНаука

# Gartner, Forester



ДиалОгНаука

# Ключевые клиенты Websense в РФ

## Финансовый сектор

ВТБ

УРАЛСИБ

Ренессанс Капитал

Кредит ЕвропаБанк

Банк Союз

Банк Интеза

БТА Банк

ОТП Банк
Доверяя друг другу

Финансовая корпорация Открытие

## Промышленность

ЛУКОЙЛ
Нефтяная компания

Газпром

Газпром нефть

Enel ОГК-5

Норильский никель

Северсталь
Российская Сталь

СИБУР

«Сахалин Энерджи»
Быть ведущим источником энергии для Азиатско-Тихоокеанского региона

## Телекоммуникации

МТС

COMSTAR

МТТ

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

# Спасибо за внимание

## Вопросы?

**ЗАО «ДиалогНаука»**
Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

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