websense
ESSENTIAL INFORMATION PROTECTION™

Информационная безопасность современности

web security | data security | messaging security

Архитектура TRITON

Комплексное решение

Web Security

Data Security

Email Security

Общая интеграция

Унификация платформы

SaaS

Appliance

Software

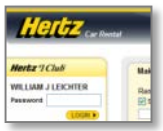
Полный контроль

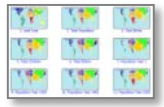
websense®

Yes!

ESSENTIAL INFORMATION PROTECTION™

Web-фильтрация. Web-мониторинг. Web-безопасность.





websense®

ESSENTIAL INFORMATION PROTECTION™

Определения

Задачи ИБ:

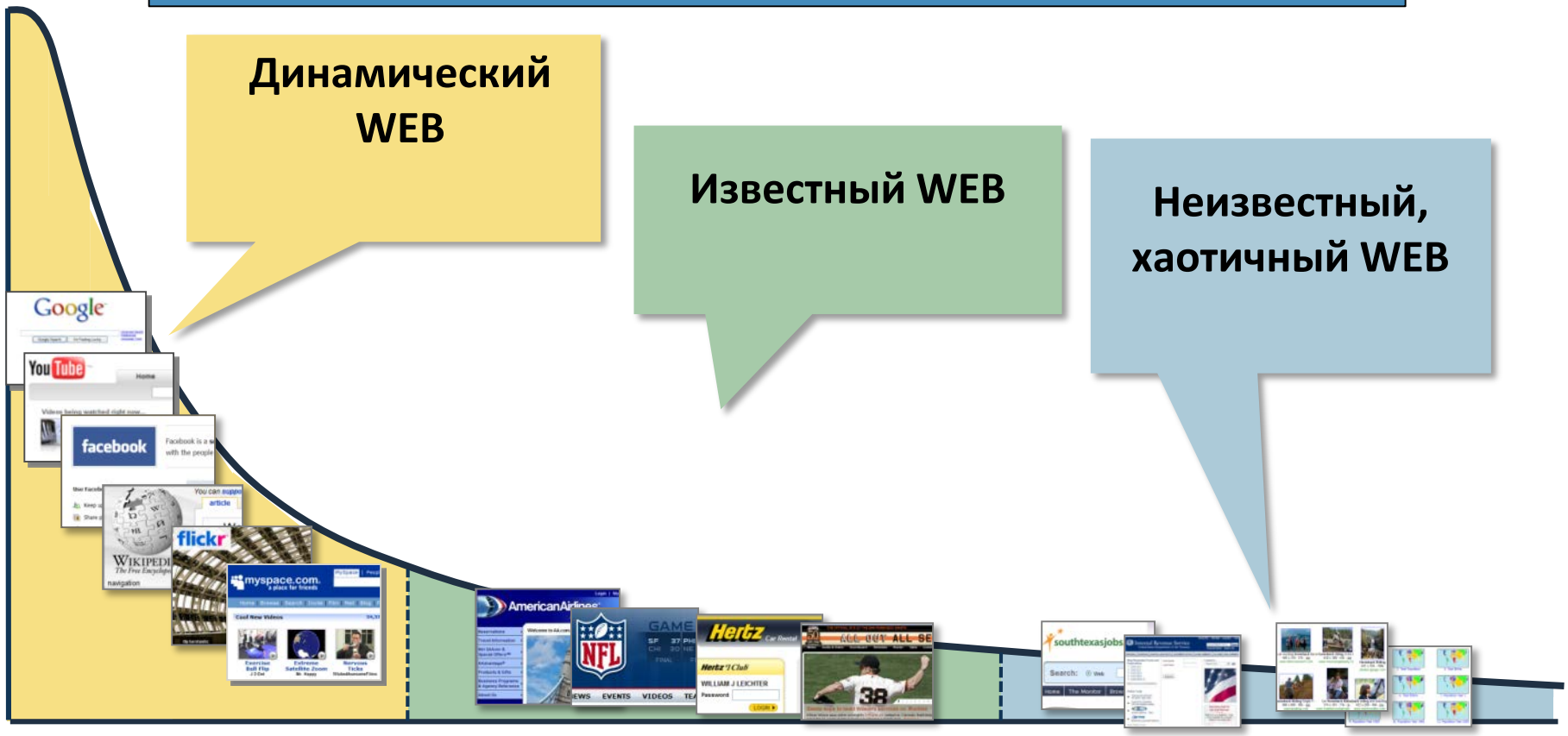
1. **Оптимизация использование Интернет в организации.**
2. **Уменьшение рисков.**

- **Веб мониторинг**
- **Веб фильтрация**
- **Веб защита**

websense
ESSENTIAL INFORMATION PROTECTION™

Web-сайты сегодня

70% из топ 100 самых популярных Web сайтов хранили или были вовлечены в вредоносную активность в течении последний 6 месяцев.



websense
ESSENTIAL INFORMATION PROTECTION™

Бизнес растет с помощью 2.0

Web 2.0 включает

- Социальные сети
- Hosted приложение
- Блоги, Wiki
- Хранение файлов
- RSS потоки

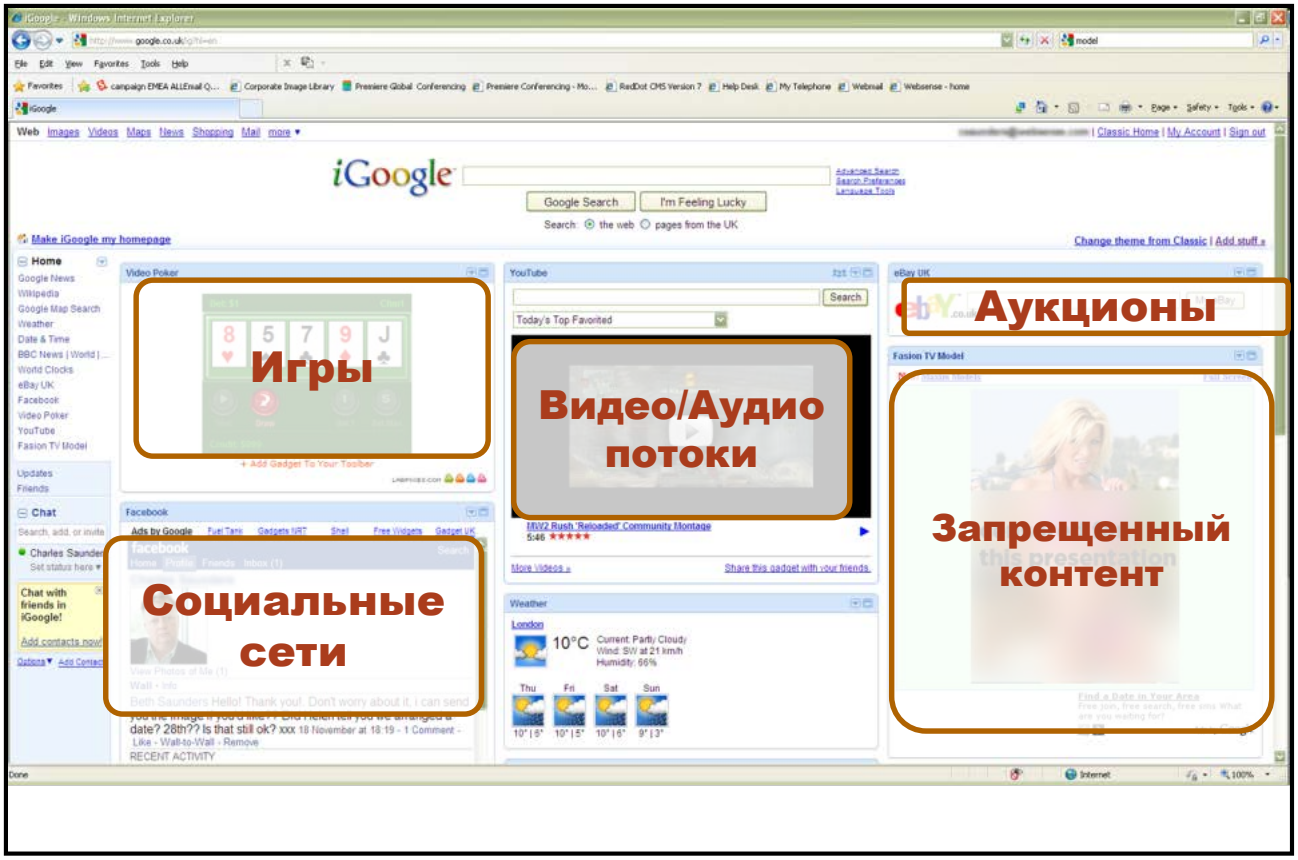
Новые технологии позволяют

- Создавать, отправлять
- изменять, редактировать
- взаимодействовать
- распространять информацию

Статическая URL-фильтрация мертва

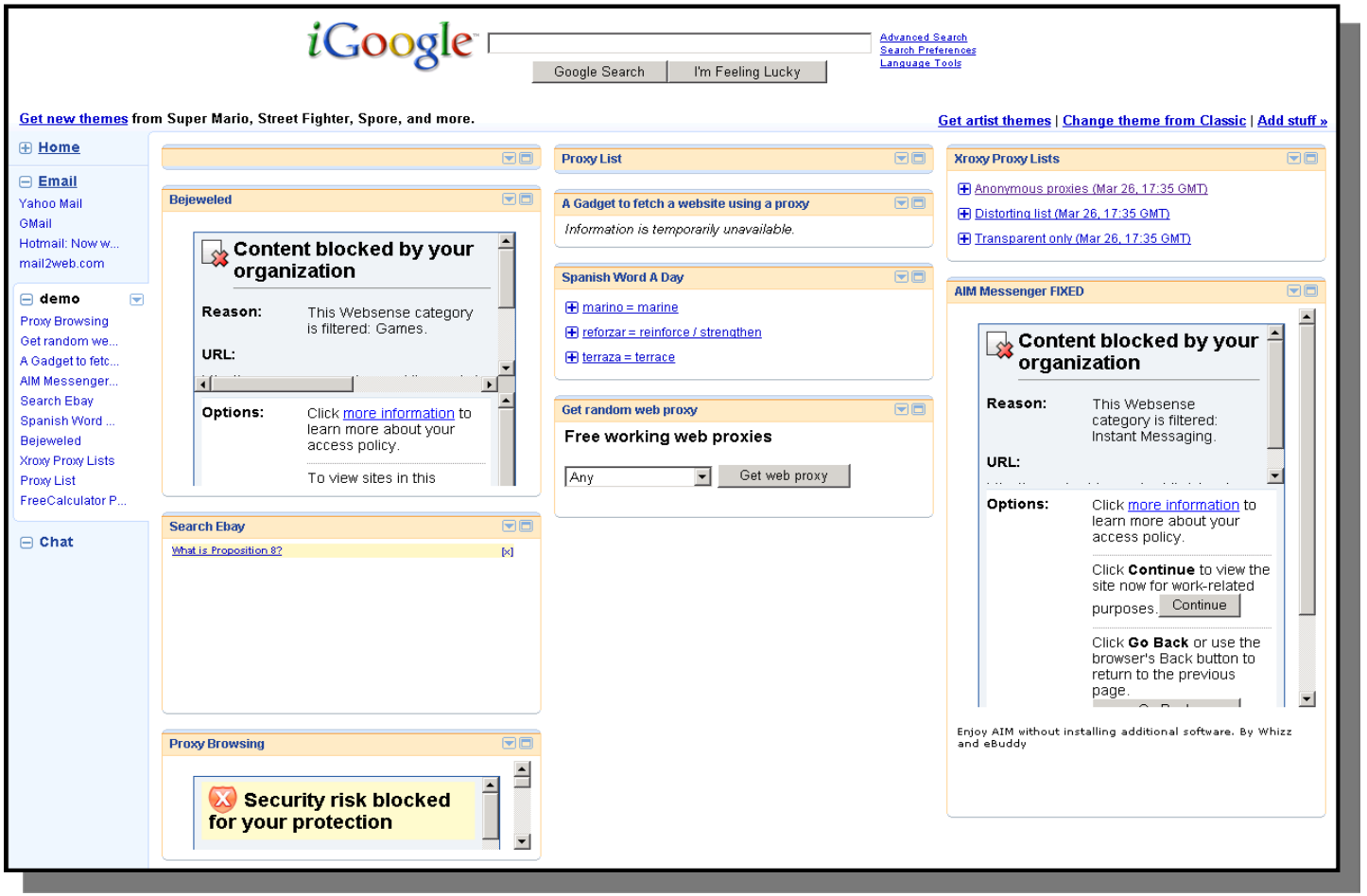
Понимание URL ссылки недостаточно.

Необходимо понимание содержимого на странице



Без Websense

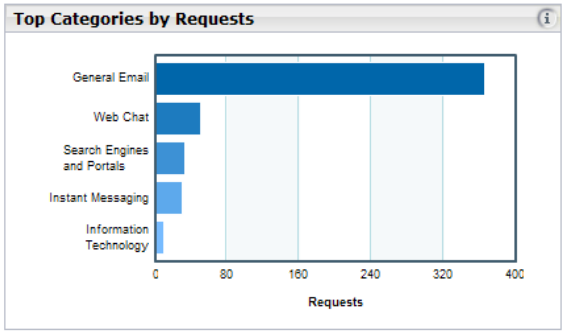
C Websense



websense
ESSENTIAL INFORMATION PROTECTION™

Фильтрация, мониторинг

Web Filter

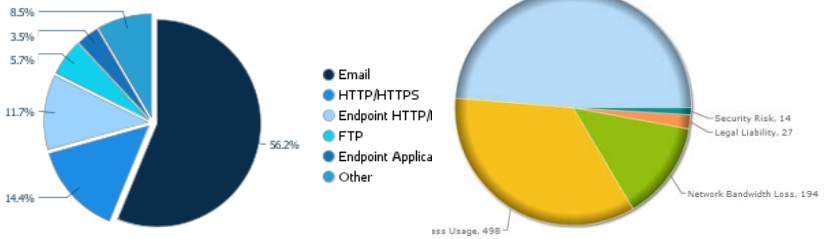


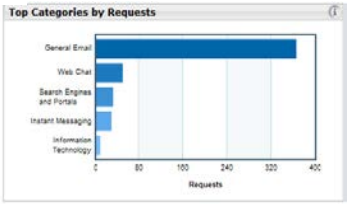
- **Передовое решение WEB-фильтрации**
- **Повышение производительности сотрудников**
- **Оптимизация использования ресурсов Интернет**

websense
ESSENTIAL INFORMATION PROTECTION™

Контроль безопасности компании

Web Security





- **Набор категорий безопасности URL:**
  - **Бот-сети, Шпионские программы**
  - **Фишинг и мошенничество, Перехватчики клавиатуры**
  - **Вредоносные веб-сайты**
  - **Потенциально нежелательные программы**
- **Службы WEB репутации**

Передовое решение WEB-фильтрации

Повышение производительности сотрудников

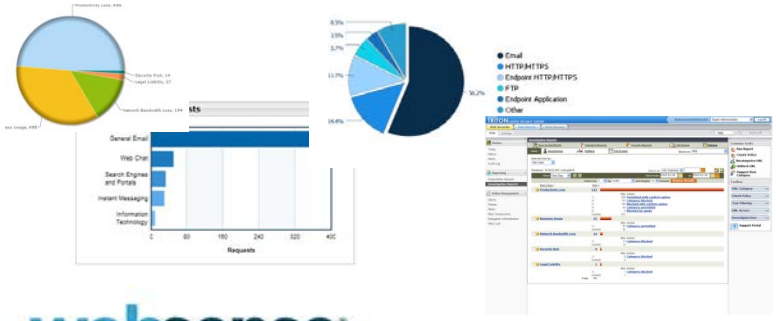
Оптимизация использования ресурсов Интернет

websense
ESSENTIAL INFORMATION PROTECTION™

WEB 2.0 Challenge

Web Security Gateway

- **Контентная фильтрация**
- **Категоризация WEB 2.0**
- **Анализ SSL**
- **Сканирующий Proxy Server**



Передовое решение WEB-фильтрации

Повышение производительности сотрудников

Оптимизация использования ресурсов Интернет

Набор категорий безопасности URL

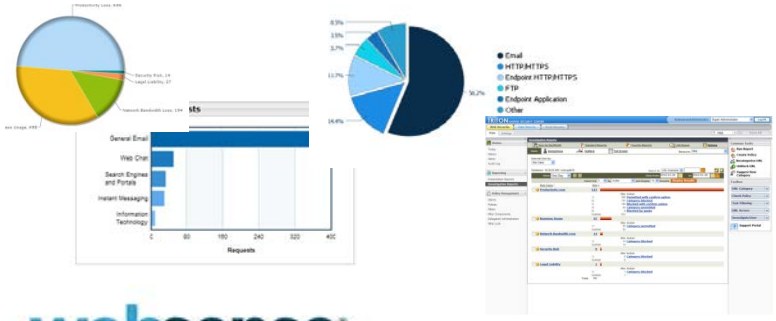
Службы WEB репутации

websense
ESSENTIAL INFORMATION PROTECTION™

WEB 2.0 Challenge

Web Security Gateway Anywhere

- **Контентная фильтрация**
- **Категоризация WEB 2.0**
- **Анализ SSL**
- **Сканирующий Proxy Server**
- **Web DLP**
- **Hosted Web Security**



Передовое решение WEB-фильтрации

Повышение производительности сотрудников

Оптимизация использования ресурсов Интернет

Набор категорий безопасности URL

Службы WEB репутации

websense
ESSENTIAL INFORMATION PROTECTION™

V10000, V5000 Appliances

• Внедрение передовых решений в сфере безопасности Интернет, данных и электронной почты

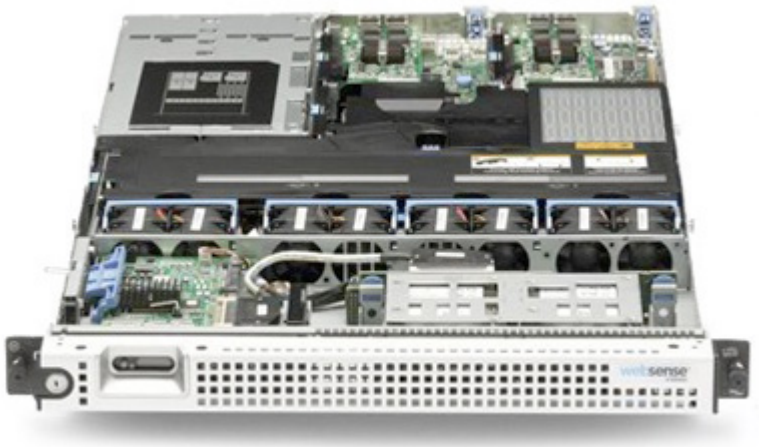
• Расширяемый функционал уровня корпоративного класса, который включает высокую

отказоустойчивость и доступность

• Простоту в использовании благодаря системе централизованного управления и отчетности

• Возможность расширения системы безопасности в будущем

• Привлекательную цену и безупречное качество



websense
ESSENTIAL INFORMATION PROTECTION™

ROI

К-во сотрудников с Internet доступом - 500
Средняя заработная плата сотрудника - 500$ (3.13$ в час)

Результаты в процессе работы тестового стенда:
минимум 10% времени сотрудники проводят на интернет сайтах, не относящихся к работе – минимум 4,5 часов в неделю (10% рабочего времени)

В итоге убыток:
3,13$ з/п в час * 4,5 часа/неделя * 50 недель/год * 500 человек = 352 125$/год.

websense
ESSENTIAL INFORMATION PROTECTION™

ROI

……убыток 352 125$/год.

Окупаемость решений Websense Web Security происходит за несколько недель!

Сотрудники имеют доступ в интернет, который им необходим для качественного выполнения работы.

Комплексная интеграция промышленного прокси-сервера, централизированное администрирование

websense
ESSENTIAL INFORMATION PROTECTION™

Data Security Solution
Решения для защиты данных

Задачи Data Loss Prevention

Гарантия непрерывности бизнеса путем управления рисками, защита от утечки конфиденциальной информации по всем возможным каналам передачи

websense
ESSENTIAL INFORMATION PROTECTION™

Websense Data Security Suite

Data Loss Prevention технология для идентификации, мониторинга и защиты конфиденциальной информации

- Сетевое DLP
- Endpoint DLP

websense
ESSENTIAL INFORMATION PROTECTION™

Websense Data Security Suite

Функции WebsenseDSS

Data Discover

обнаружение и классификация данных, хранящихся в сети организации

Data Monitor

мониторинг передаваемых данных для выявления нарушения политик безопасности

Data Protect (Data Security Gateway)

мониторинг и предотвращение утечек конфиденциальных данных на основе политик безопасности организации

Data Endpoint

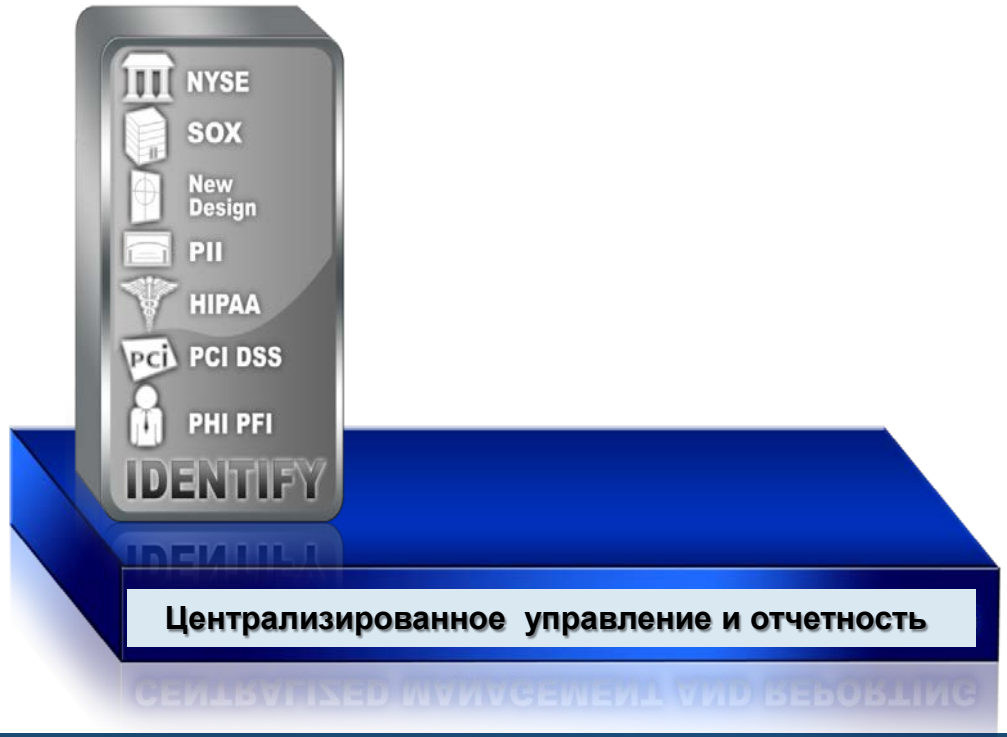
предотвращение утечек данных с компьютеров пользователей.

websense
ESSENTIAL INFORMATION PROTECTION™

Websense DLP Solution

Идентификация

Модуль Data Discover



Точная идентификация - PreciseID

websense
ESSENTIAL INFORMATION PROTECTION™

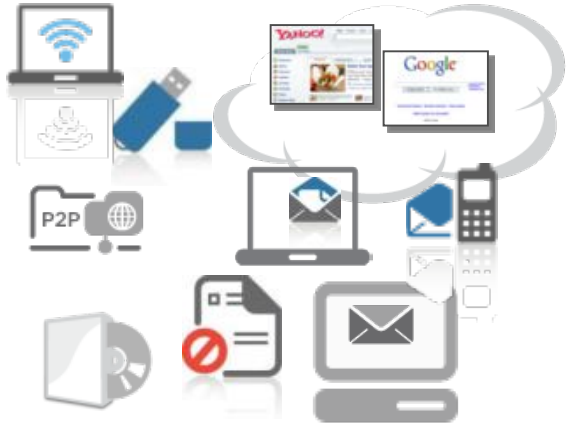
Цифровые отпечатки

Digital Fingerprints

Снятие с файлов одного или несколько «отпечатков» (хэш-функции).

Отпечатки используются для:

- **обнаружения защищенных документов в каналах передачи данных**
- **предотвращения не авторизованных действий с данными (пересылка, печать, копирование и пр.)**



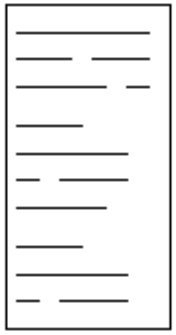
websense
ESSENTIAL INFORMATION PROTECTION™

Цифровые отпечатки

Создание Fingerprint:

Запись
базы данных
или документ

Чтение



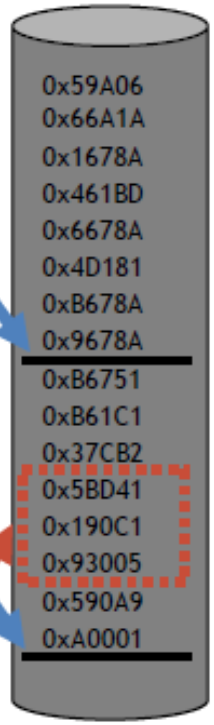
Алгоритмическое
преображение

010111001
101001100
00101100
100100
1000111
011
0110011
0111101

Односторонняя
математическая
репрезентация

0xB6751
0xB61C1
0x37CB2
0x5BD41
0x190C1
0x93005
0x590A9
0xA0001

Fingerprint
хранилище
и индексация



Определение:

Исходящий контент
(E-mail, Web, Fax,
Print, etc.)

Извлечение

Алгоритмическое
преображение

010111001
101001100
00101100
100100

Односторонняя
математическая
репрезентация

0x5BD41
0x190C1
0x93005

Fingerprint
Создание

Real-Time
Fingerprint
сопоставление

websense
ESSENTIAL INFORMATION PROTECTION™

Сценарий идентификации

- Понимание классификаторов
- Снятие отпечатков
- Сканирование одноразово и по расписанию:

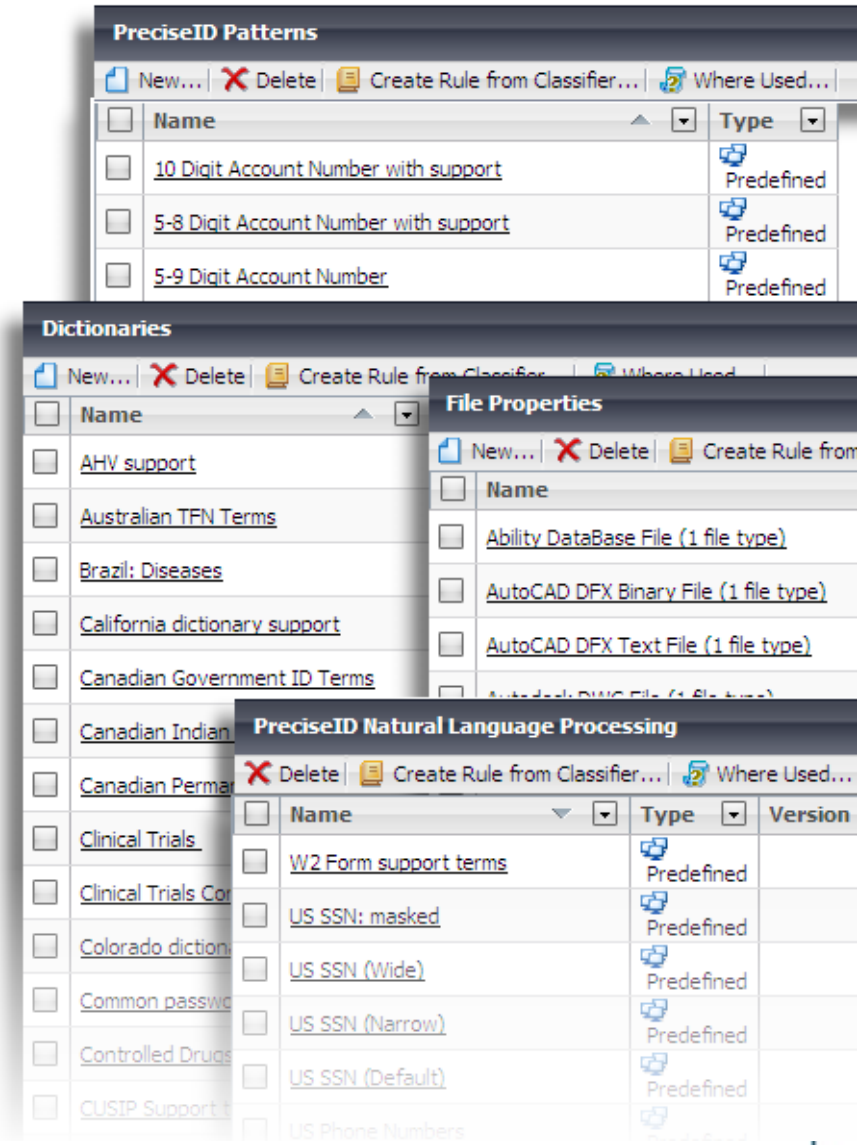
Файловые хранилища
Базы данных
Microsoft SharePoint
Microsoft Exchange и остальные mail сервера

- Создаем политики по сканированию и мониторингу данных **in rest**

websense
ESSENTIAL INFORMATION PROTECTION™

Контентная классификация

- Стандартные блоки идентификации
- Встроенные классификаторы
  - Образцы
  - Словари
  - Свойства файлов
- Расширение для создания собственных классификаторов



websense
ESSENTIAL INFORMATION PROTECTION™

Классификация

Информацию можно классифицировать:

- По произвольному количеству категорий (политик конфиденциального содержимого), определяемых как стандартными шаблонами, так и администратором.
- По уровню критичности инцидента (низкий, умеренный, высокий)
- По любым другим атрибутам инцидента (например, имя и расширение файла, владелец файла, тип АРМ (стационар/ноутбук), и т.д.)

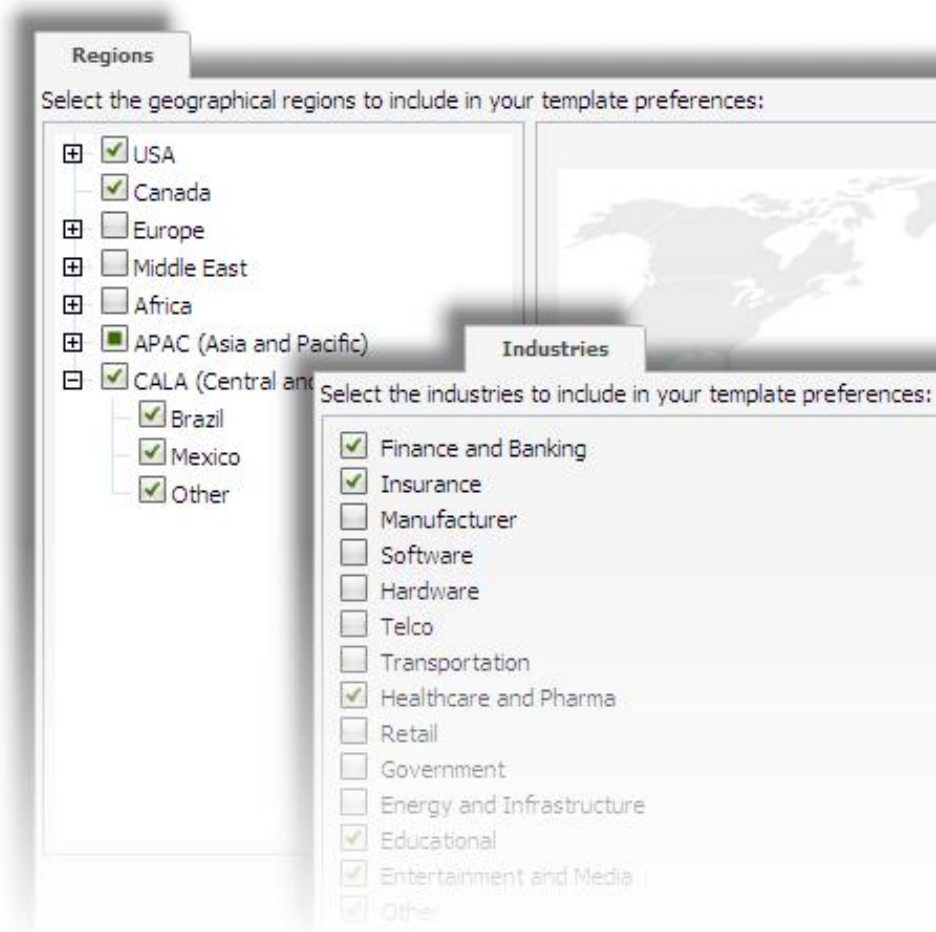
Websense DLP Solution

Мониторинг

Модуль Data Monitor

Monitor

- Более 1000 правил, политик, расширений
- Встроенные шаблоны для типовых данных и регулирования класса конфиденциальности
- Шаблоны соответствия региону и сферы деятельности



websense
ESSENTIAL INFORMATION PROTECTION™

Гибкость политик

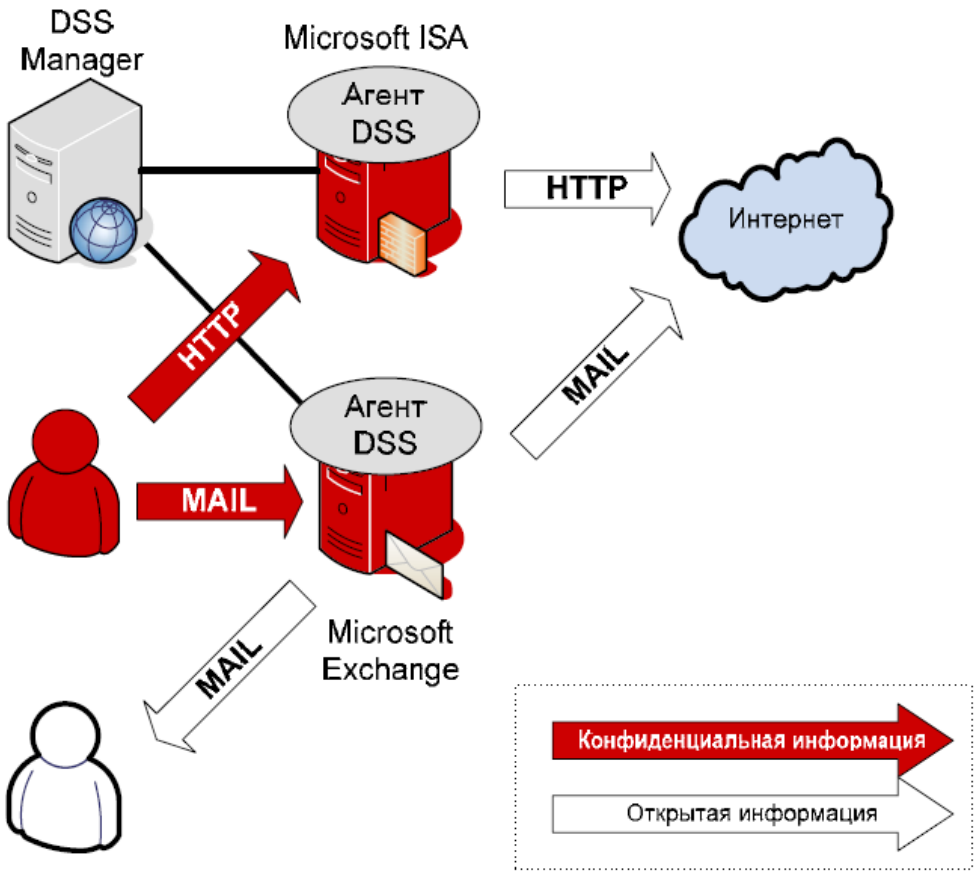
- Политика может быть применена к одному каналу коммуникации, многократным каналам или ко всем каналам

  - **Web**
  - **Сетевой принтер**
  - **Локальный принтер**
  - **USB**
  - **LAN Storage**
  - **CD Burning Apps**
  - **Email**
  - **Endpoint Apps**
  - **Browser**
  - **CD Burning Apps**
  - **FTP**
  - **Instant Messenger**
  - **P2P Apps**

Контроль каналов утечки

- **Все основные каналы утечки, в том числе HTTP, SMTP, FTP, IM (AOL, MSN, Yahoo, ICQ);**
- **Сетевые принтеры, OCR модуль**
- **HTTPS (перешифрация сообщений, атака типа man-in-the-middle)**
- **Контроль «на лету» операций PrintScreenи Copy-Paste**
- **Контроль сменных носителей, запущенных приложений.**

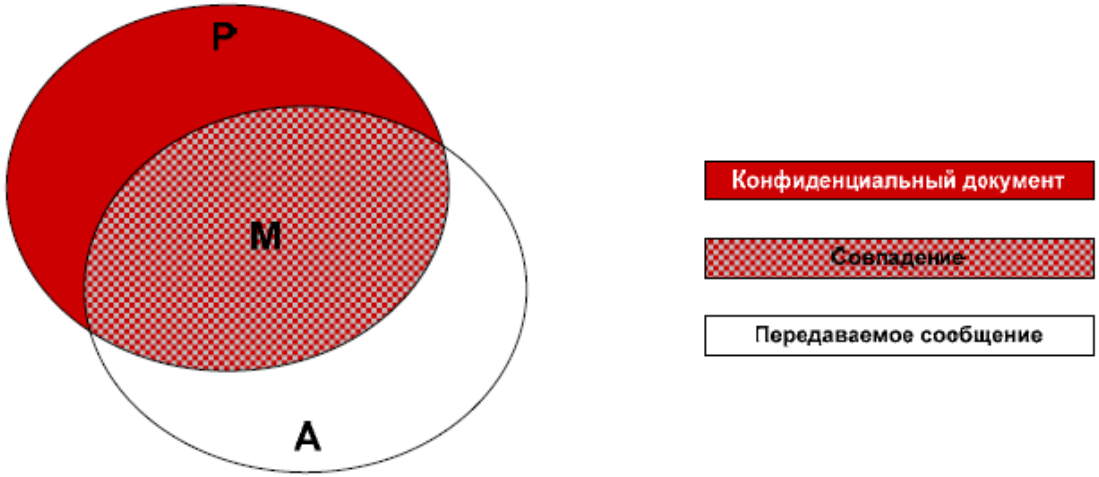
Пример схемы



websense
ESSENTIAL INFORMATION PROTECTION™

Примеры срабатывания условий:

- ❑ Сообщение содержит почти весь конфиденциальный документ и много незначащего текста.
- ❑ Почти все сообщение состоит только из одной страницы конфиденциального документа.
- ❑ Сообщение содержит несколько страниц конфиденциального документа и много незначащего текста.



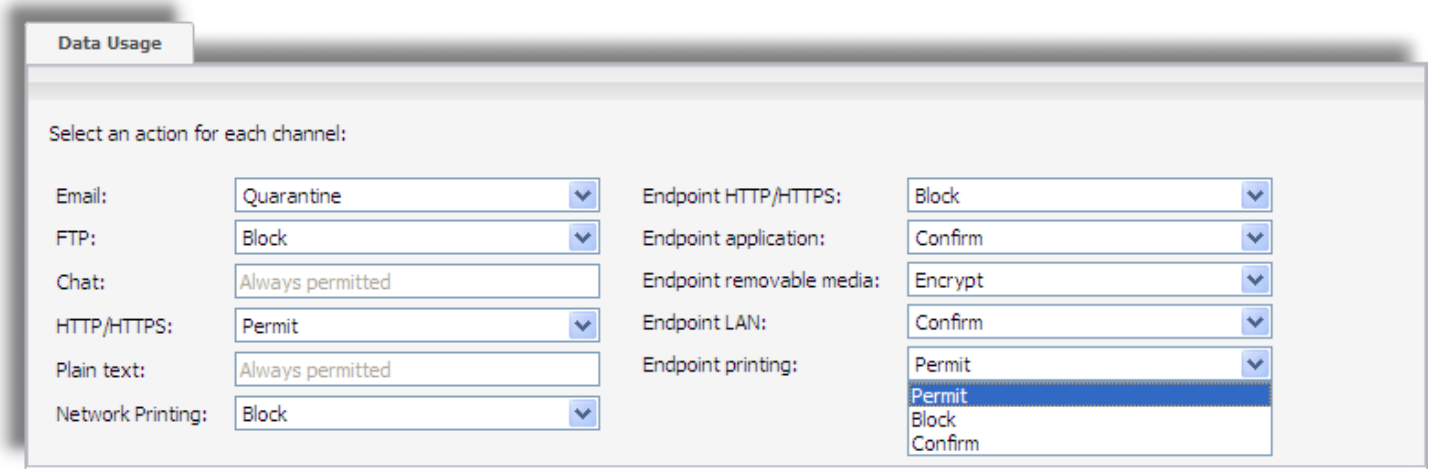
Websense DLP Solution

Мониторинг

Модуль Data Protect

План действий

- Определение действия при нарушении правила
  - Отдельное реагирование для каждого канала
- Определение действий на основе уровня нарушения



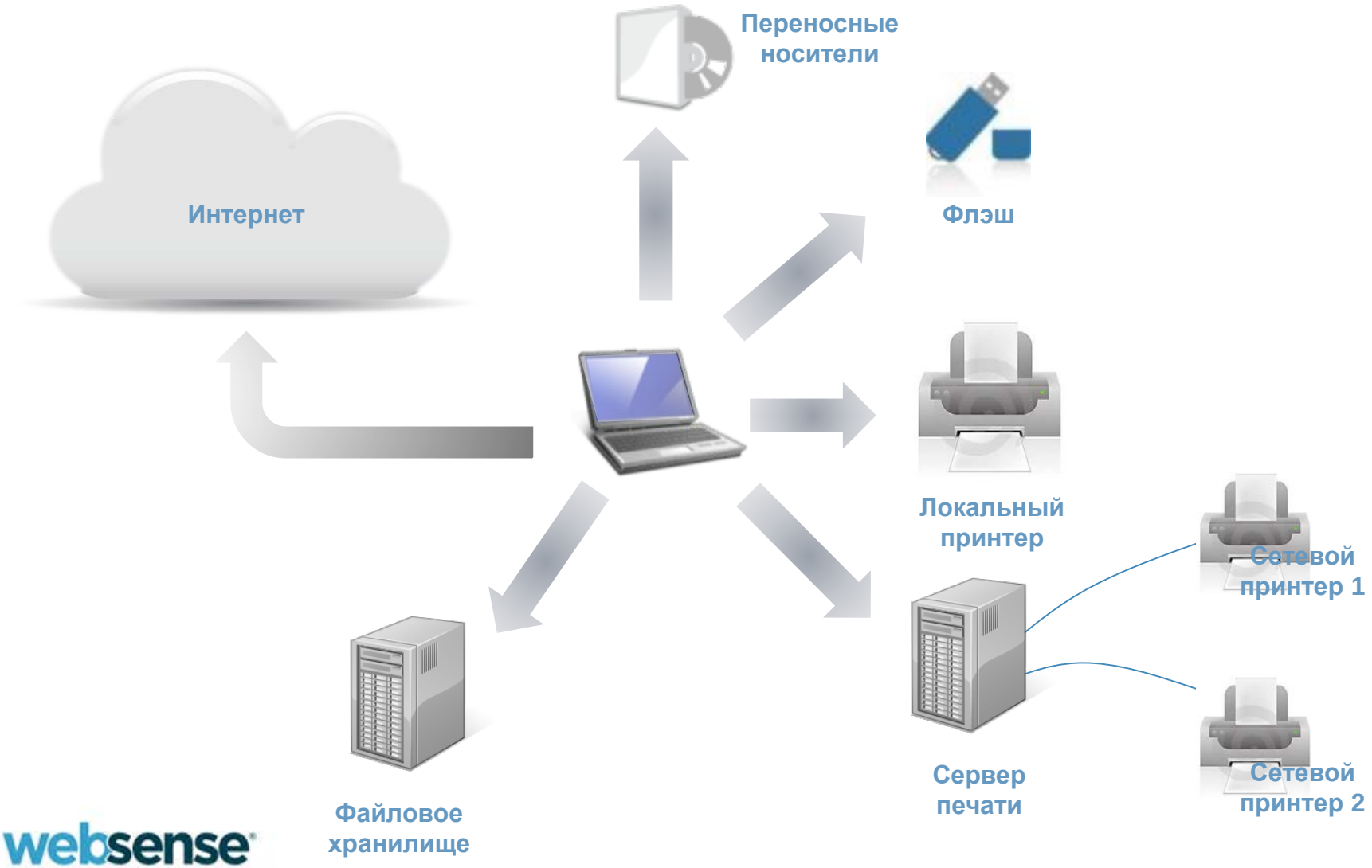
* Severity is user-defined based on number of matches

websense
ESSENTIAL INFORMATION PROTECTION™

Защита данных на основе мониторинга и идентификации

- Встроенные действия доступны для каналов
  - Разрешить
  - Блокировка
  - Подтверждение
  - Карантин
  - Шифрование
  - Карантин и шифрование при выходе
- Кто может совершать действия
- Какие действия
- В какое время

Защита конечных точек: Data Endpoint

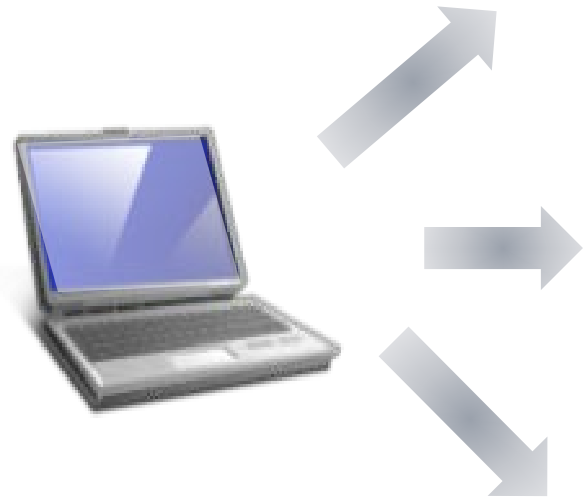


websense
ESSENTIAL INFORMATION PROTECTION™

Endpoint DLP

Реализация функционала на рабочей станции

- Идентификация
- Мониторинг
- Защита



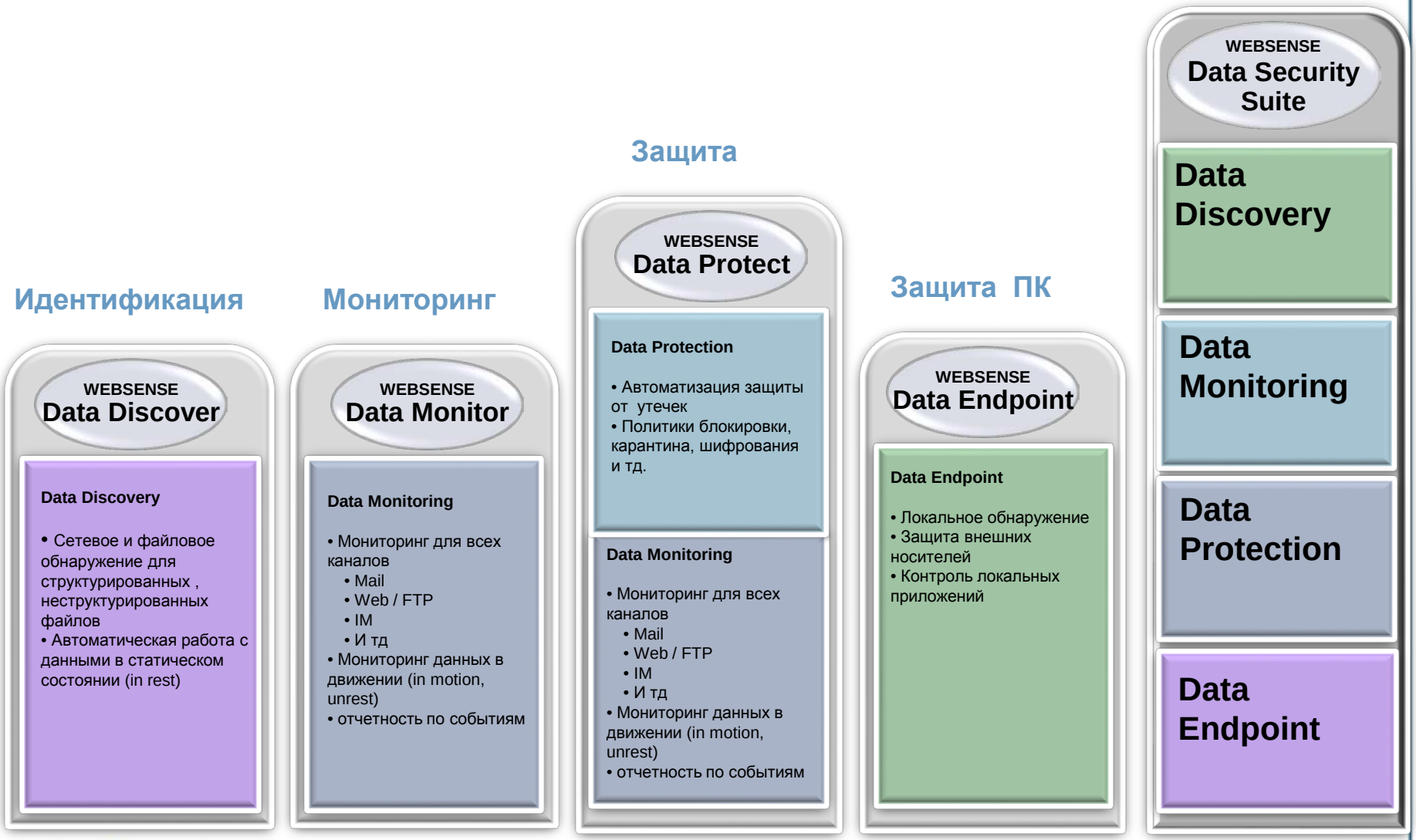
Основные задачи:

- Буфер обмена
- Работа с мобильными станциями
- Взаимодействие с сетевым DLP по работе с каналами

Управление предотвращением утечки: схема

websense
ESSENTIAL INFORMATION PROTECTION™

Варианты внедрения



Решение для любой задачи

	Web DLP	Data Monitor	Data Protect	Data Endpoint	Data Discover	Data Security Suite
Data идентификация	●	●	●	●	●	●
Централизированное управление	●	●	●	●	●	●
Уведомление	●	●	●	●	●	●
WEB Мониторинг	●	●	●	●		●
Защита WEB	●		●	●		●
EMAIL Мониторинг		●	●			●
Защита EMAIL			●			●
Закачки WEB				●		●
Защита внешних LAN				●		●
Контроль внешних устройств				●		●
Контроль приложение				●		●
Обнаружение на конечных точках				●		●
Обнаружение в сети					●	●

● Available with v7.6

websense
ESSENTIAL INFORMATION PROTECTION™

Triton Enterprise

TRITON Enterprise:

- Websense Web Security Gateway
- Websense Data Security Suite
- Websense Email Security Gateway

Выгоднее, чем
WSG + DSS отдельно

Комплексное решение

websense
ESSENTIAL INFORMATION PROTECTION™

Сценарий сотрудничества в сделке

- **Презентация, Демонстрация**
- **Пилотный проект**
- **Специальные условия**

websense
ESSENTIAL INFORMATION PROTECTION™

Спасибо!

websense
ESSENTIAL INFORMATION PROTECTION™