websense
ESSENTIAL INFORMATION PROTECTION™

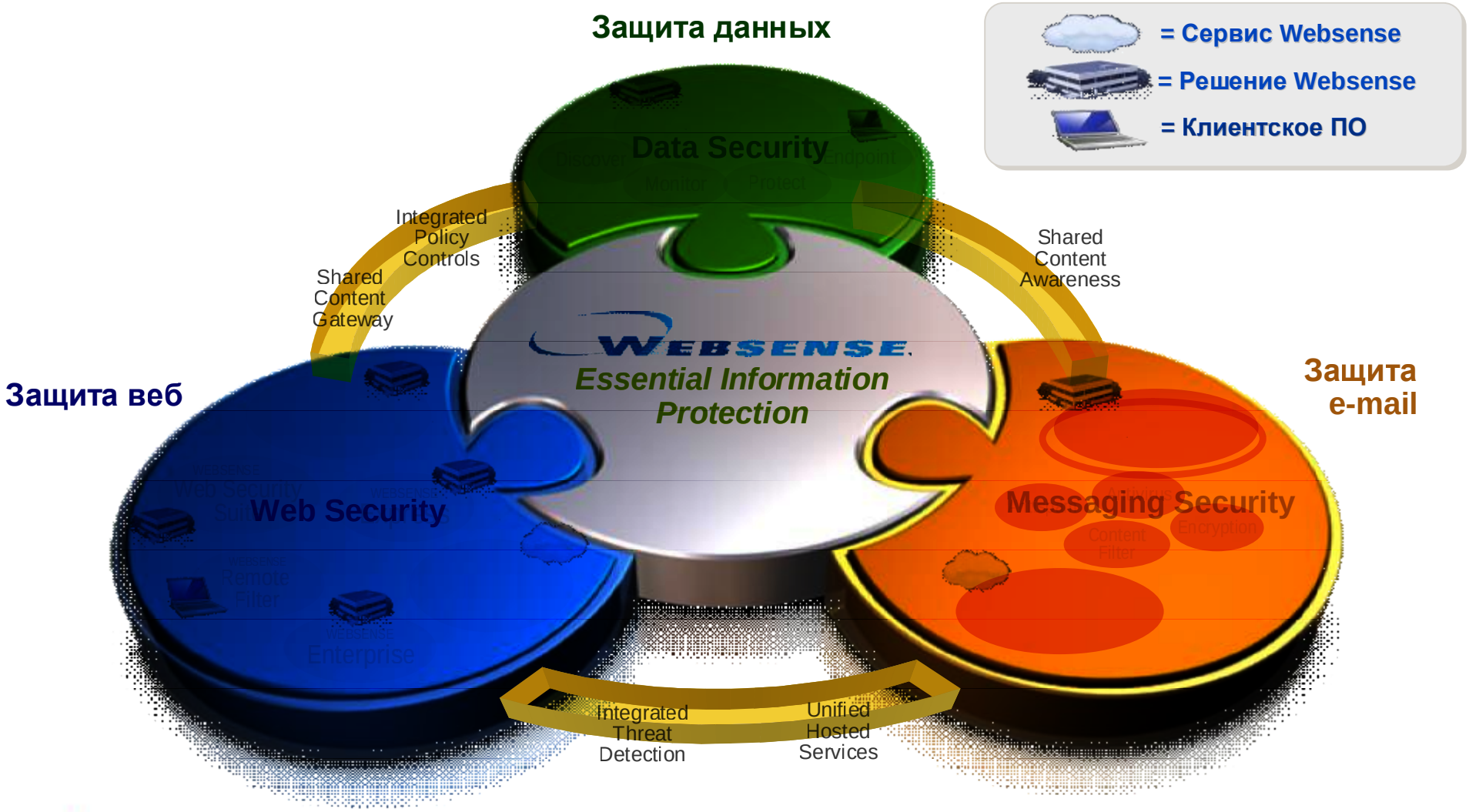
AMT GROUP

Пятый ежегодный семинар по информационной безопасности

Решения Websense для обеспечения веб-безопасности и предотвращения утечек конфиденциальных данных

Михайлов Александр
Директор по технологиям
Associates Distribution
Websense Authorized Distribution Partner

web security | data security | messaging security



websense
ESSENTIAL INFORMATION PROTECTION™

Websense – абсолютный мировой лидер рынка веб-безопасности (Q2 2008)

MARKET QUADRANT – CORPORATE WEB SECURITY

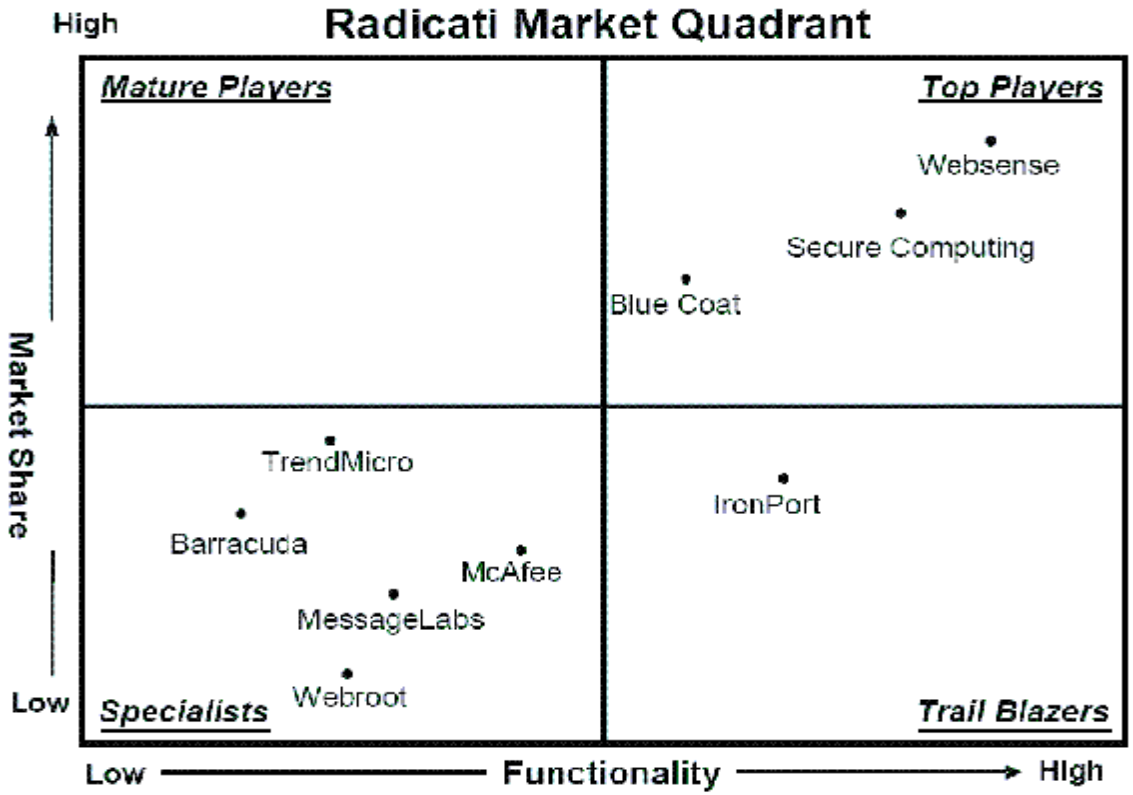


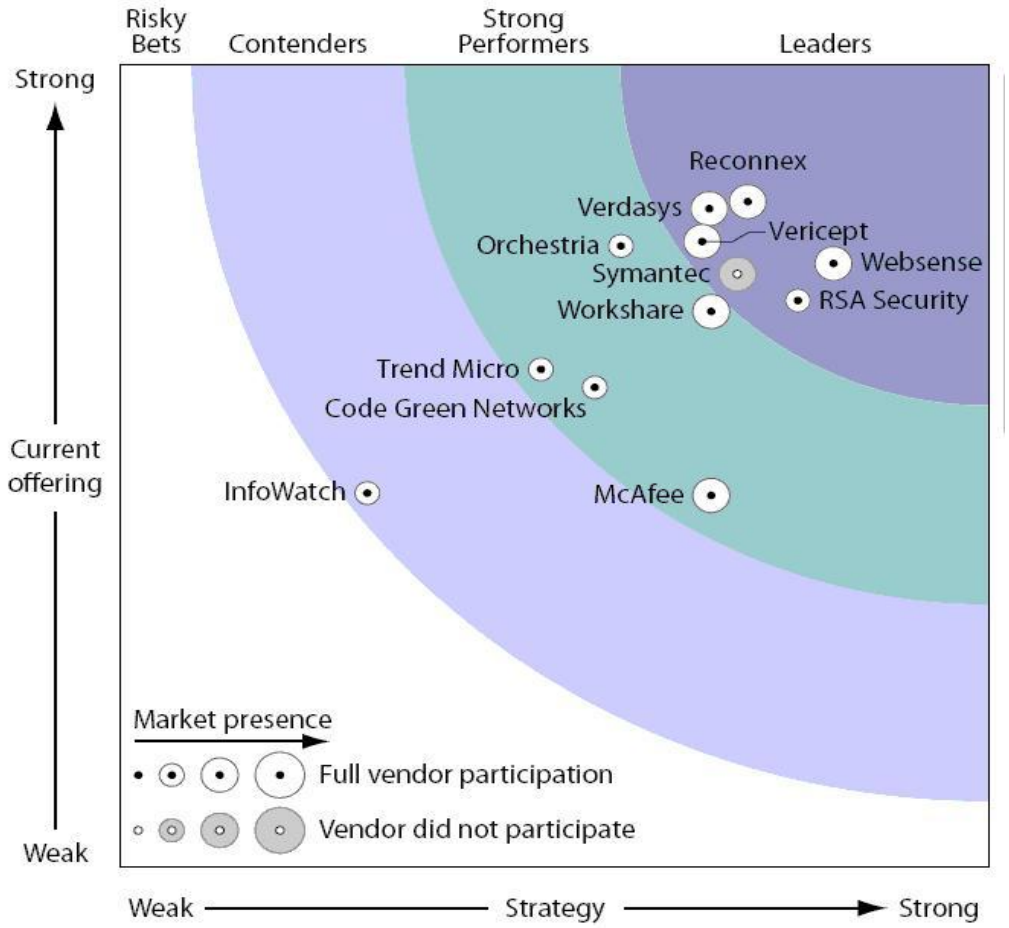
Figure 3: Corporate Web Security Market Quadrant, 2008

Websense – мировой лидер рынка DLP (Gartner, Forrester Wave Q2 2008)

Gartner

Figure 1. Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention

Forrester Wave



websense
ESSENTIAL INFORMATION PROTECTION™

websense
ESSENTIAL INFORMATION PROTECTION™

Веб-фильтрация и веб-безопасность
Websense Web Security

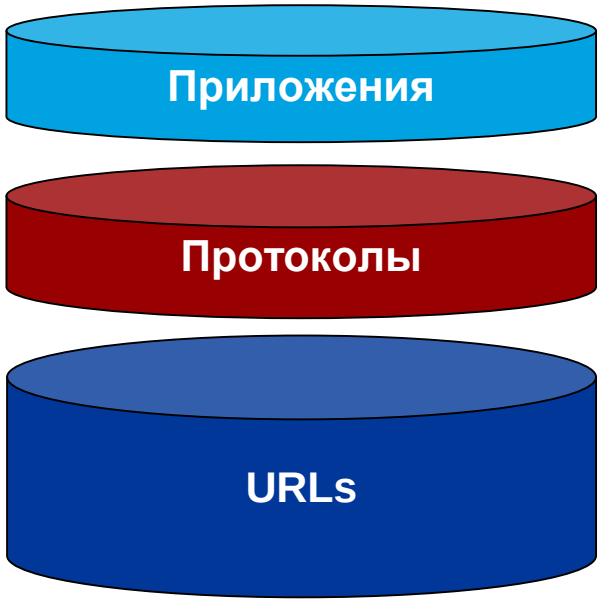
web security | data security | messaging security

Принципы защиты Websense

- "We Find Them Before They Find You"
  - Не надо ждать
  - Не надо угадывать
  - Не надо все время подстраивать

Мы найдем их до того,
как они найдут вас

- Тематические категории URL
  - более 100 категорий, более 35 млн. URL
- Категории безопасности URL
  - шесть категорий
- Обновление в реальном времени
- Категории протоколов
  - более 100 протоколов, 15 категорий
- Сигнатуры нежелательного трафика
- Цифровые отпечатки нежелательных и вредоносных приложений
  - более 50 категорий, более 2 млн. приложений



Websense Master Database – 100+ категорий

- Аборты
  - Сторонники
  - Противники
- Азартные игры
- Безвкусное содержание
- Бизнес и экономика
  - Финансовые данные и услуги
- Военная агрессия и экстремизм
- Здоровье
- Игры
- Интернет-общение
  - Веб-чаты
  - Электронная веб-почта
- Информационные технологии
  - Веб-хостинг
  - Компьютерная безопасность
  - Обход прокси-серверов
  - Поисковые машины и порталы
  - Сайты трансляции URL
  - Хакерство
- Лекарства и наркотики
  - Пищевые добавки
  - Лекарства по рецепту
  - Марихуана
  - Наркотики
- Материалы для взрослых
  - Нагота
  - Нижнее белье и купальники
  - Половое воспитание
  - Секс
  - Содержание для взрослых
- Насилие
- Незаконное или сомнительное содержание
- Новости и СМИ
  - Альтернативные журналы
- Образование
  - Культурные учреждения
  - Образовательные материалы
  - Образовательные учреждения
  - Справочные материалы
- Общественные организации
  - Общественные организации и партии
  - Профессиональные и рабочие организации
  - Службы и благотворительные организации
- Общество и образ жизни
  - Алкоголь и табак
  - Геи, лесбиянки и бисексуалы
  - Персональные веб-сайты
  - Рестораны и обеды
  - Знакомства и брак
  - Хобби
- Органы власти
  - Военные
  - Политические
- Особые события
- Поиск работы
- Покупки
  - Интернет-аукционы
  - Недвижимость
- Пропаганда
- Пропускная способность
  - Интернет радио и ТВ
  - Интернет-телефония
  - Личные сетевые хранилища и архивы
  - Одноранговый обмен файлами
  - Потоковая информация
- Продуктивность
  - Доски объявлений и клубы
  - Загрузка бесплатного и коммерческого ПО
  - Интерактивное маклерство и торговля
  - Мгновенный обмен сообщениями
  - Оплачиваемая навигация
  - Реклама
- Путешествия
- Развлечения
  - MP3 и загрузка аудио
- Расизм и ненависть
- Религия
  - Нетрадиционные религии, оккультизм и фольклор
  - Традиционные религии
- Спорт
  - Спортивная охота и клубы стрелков
- Транспортные средства
- WEBSENSE SECURITY FILTERING
  - Бот-сети
  - Вредоносные веб-сайты
  - Перехватчики клавиатуры
  - Потенциально нежелательные программы
  - Фишинг и прочее мошенничество
  - Шпионские программы
- Web Reputation
  - Потенциально вредоносный код
  - Повышенный риск
  - Актуальные эксплойты

Наиболее популярные категории URL J

General Email

Personals and Dating

Adult Content

Society and Lifestyles

Vehicles

Search Engines and Portals

News and Media

Streaming Media

Personals and Dating

Message Boards and Forums

Adult Content

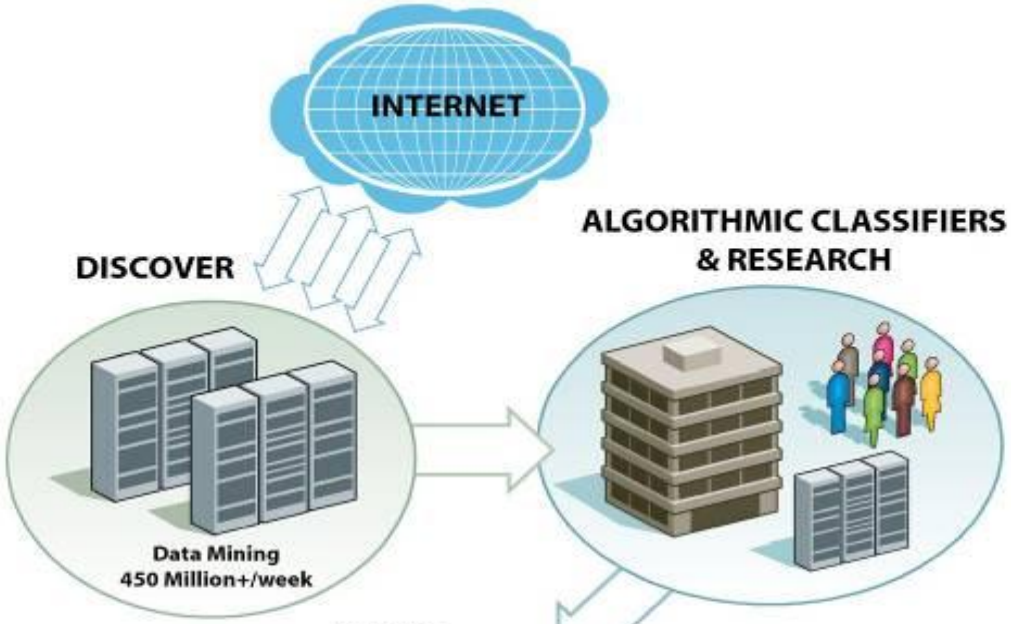
Advertisements

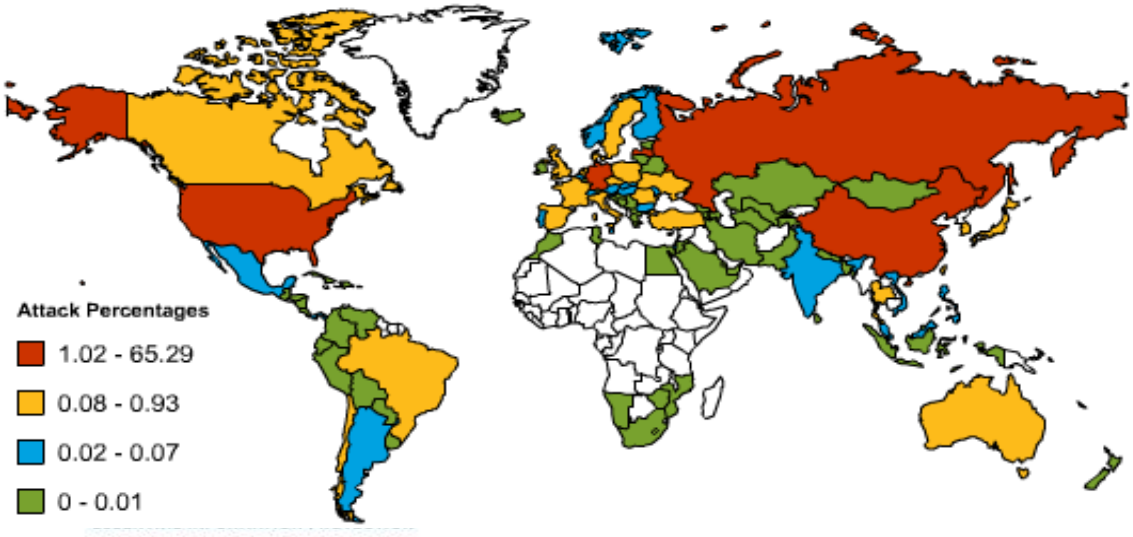
Корпоративные политики

- Фильтрация по категориям - действия фильтра
  - Разрешение
  - Блокировка
  - Разрешение с подтверждением
  - Разрешение с использованием квоты по времени
- Фильтрация по типам файлов
  - Аудио
  - Архивы
  - Исполняемые файлы
  - Видео
  - Определенные пользователем форматы
- Фильтрация по ключевым словам и regexp в URL
- Фильтрация по превышению лимита загрузки полосы пропускания
- Привязка политик к пользователям, группам, доменам или OU

Подразделение Websense Security Labs

- Обнаруживает и изучает Интернет-угрозы, в том числе вредоносный код и фишинг
- Исследует и классифицирует угрозы
- Своевременно публикует обновления продуктов и и информации для клиентов и профессионального сообщества безопасности
- Оперативно защищает клиентов от веб-угроз





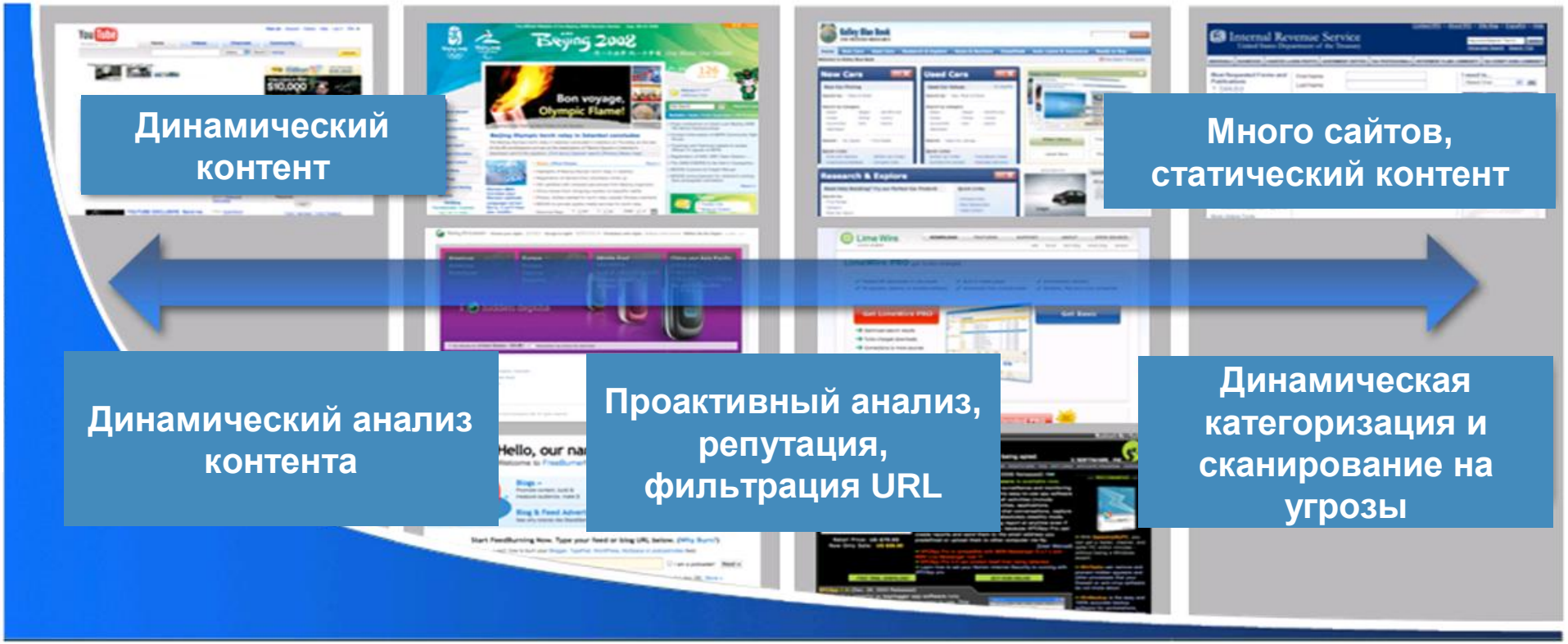
Состояние безопасности Интернета 2008

- Более 45% сайтов первой сотни поддерживают пользовательский контент
- 75% веб-сайтов с обнаруженным вредоносным кодом – это известные легальные сайты, защита которых была нарушена
  - рост 50% за последние 6 месяцев
- 60% сайтов первой сотни либо содержали вредоносный код, либо были вовлечены в мошеннические схемы в первой половине 2008
- 12% зараженных веб-сайтов содержали код, созданный с помощью готовых «ключей к уязвимостям»
  - снижение на 33% по сравнению с декабрем 2007
  - следовательно, атаки стали более фокусными

websense
ESSENTIAL INFORMATION PROTECTION™

Websense Security Labs: State of Internet Security Q1-Q2, 2008
http://www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf

Подходы к защите



Первая сотня	Текущие события Следующие 10 тыс.	Региональные, по интересам Следующий миллион	Персональные сайты, малые компании, вредоносные сайты Следующие 100 млн.

websense
ESSENTIAL INFORMATION PROTECTION™

Websense Security Gateway

- Динамическая категоризация
  - Позволяет «на лету» определять категорию для неизвестных сайтов и Web 2.0
    - *Аналитическая «машина» контентного анализа*
    - *Работает с текстом веб-страниц*
    - *Более 500 000 слов, фраз, строк Юникод и контекстных признаков*
    - *Более 2000 правил-классификаторов – обновляются производителем в реальном времени*
    - *Русскоязычный контент поддерживается*
  - Определяет контент, не используя сканер враждебного кода
    - *В т.ч. хакерские сайты, попытки обхода прокси-серверов и порнографию*
- Active Security – технологии ThreatSeeker
  - Основан на анализе активного содержимого веб-страниц
  - Безопасность, ориентированная на веб-угрозы: программы-шпионы, фишинг, и т.д.
  - Обновляется в реальном времени

websense
ESSENTIAL INFORMATION PROTECTION™

websense
ESSENTIAL INFORMATION PROTECTION™

Предотвращение утечек данных Websense Data Security

web security | data security | messaging security

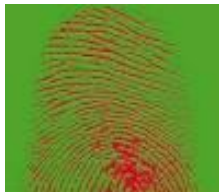
Отличие решений предотвращения утечек от систем контентной фильтрации

- Специализация на предотвращении утечек
  - Фильтры и DLP-решения часто обслуживают разные отделы
  - DLP – решения поддерживают участие нетехнических специалистов (например, руководителей) о ежедневной работе
- Алгоритмы идентификации конфиденциальных данных
  - Фильтры – ключевые слова, регулярные выражения
  - DLP – ключевые слова, регулярные выражения, fingerprints, метки файлов и другие методы
- Охват каналов утечки
  - Фильтры ориентированы на один из каналов (SMTP, HTTP, IM, …)
  - DLP охватывают максимум каналов утечки
- Обнаружение данных во время хранения (отличие DLP)
- Автоматизация работы службы безопасности
  - “Incident Workflow and Case Management” (отличие DLP)

- Схожая функциональность:
  - Политики, основанные на пользователях и группах
  - Правила реагирования

Технология анализа содержимого второго поколения

- Защита всех данных: структурированных и неструктурированных, размещённых в любом хранилище
  - Защита около 400 форматов файлов (в том числе САПР/АСУ)
    - *Самый полный охват*
    - *Обнаружение по содержимому*
    - *Анализ по полному содержанию, а не только по ключевым словам*
  - Идентификация и классификация по:
    - *Типам файлов*
    - *Сигнатурам файлов (точное сопоставление документов)*
    - *Ключевым фразам*
    - *Регулярным выражениям*
    - *Счетчикам пороговых значений*
    - *Сочетаниям вышеуказанных технологий*
    - *Любым базам данных*
  - Автоматическое и ручное сканирование данных, в том числе обновлений содержания баз данных



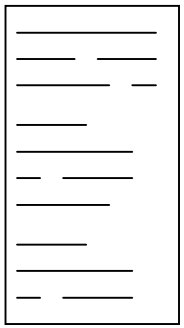
Есть ряд технологий классификации и идентификации данных, но только PreciseID™ предоставляет требуемые точность и надежность

Принцип работы Precise ID

Создание отпечатка:

Данные в реляционных СУБД и файлы

Экстракция



Алгоритмическое преобразование

010111001
101001100
00101100
100100
1000111
011
0110011
0111101

Односторонняя математическая функция

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

Хранение и индексация отпечатков

Обнаружение:

Исходящий контент (E-mail, Веб, Факс, Печать, etc)

Экстракция

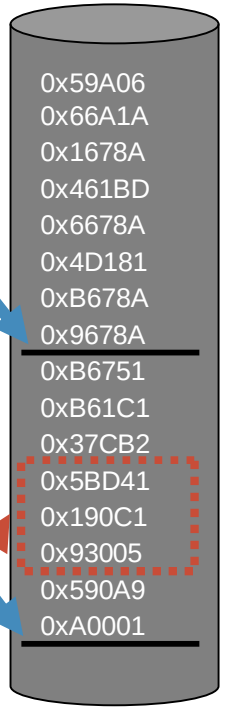
Алгоритмическое преобразование

0101110011
0100110000
101100
100100

Односторонняя математическая функция

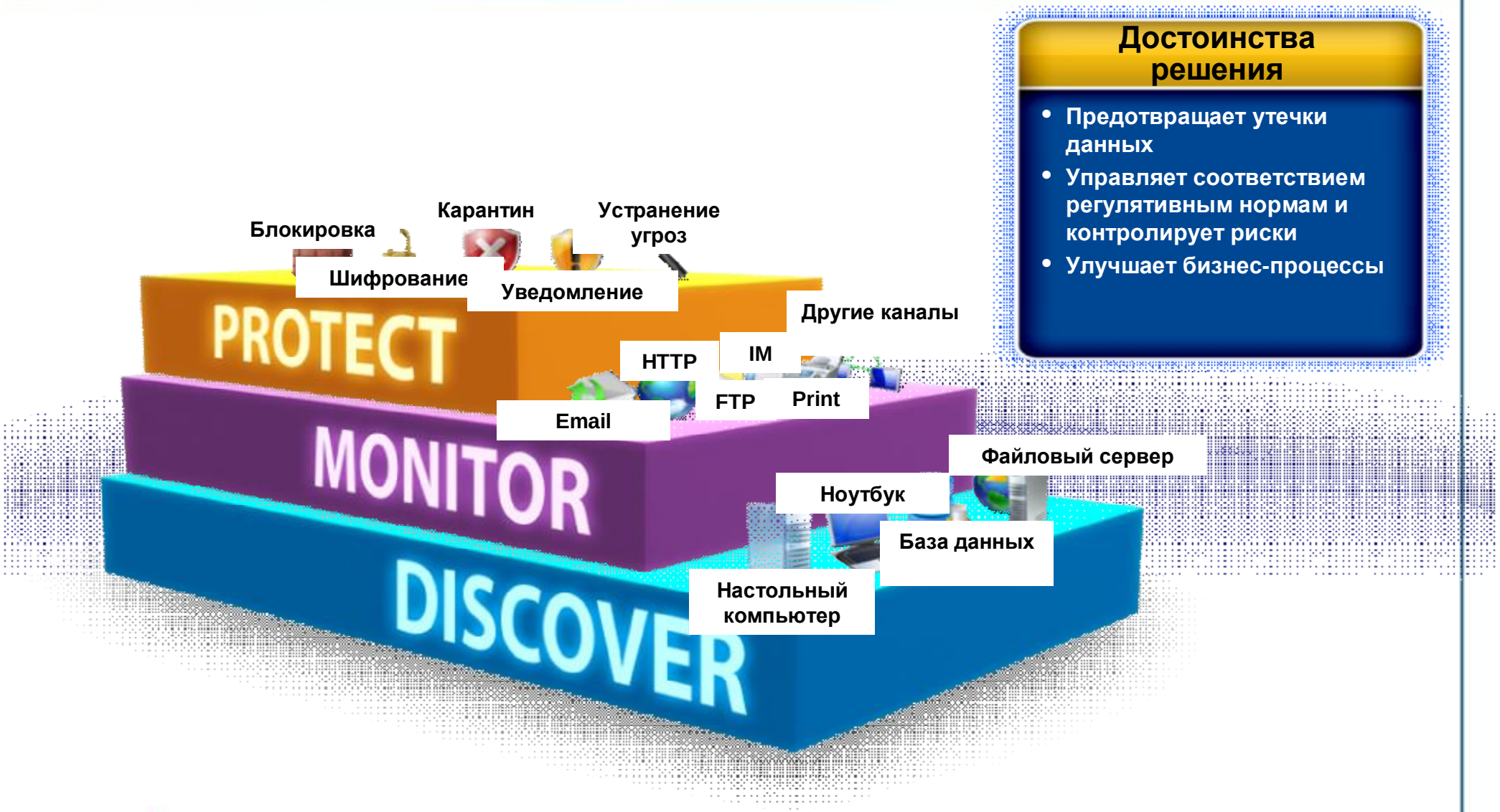
0x5BD41
0x190C1
0x93005

Формирование отпечатка



Сравнение отпечатков в реальном времени

Websense Data Security Suite

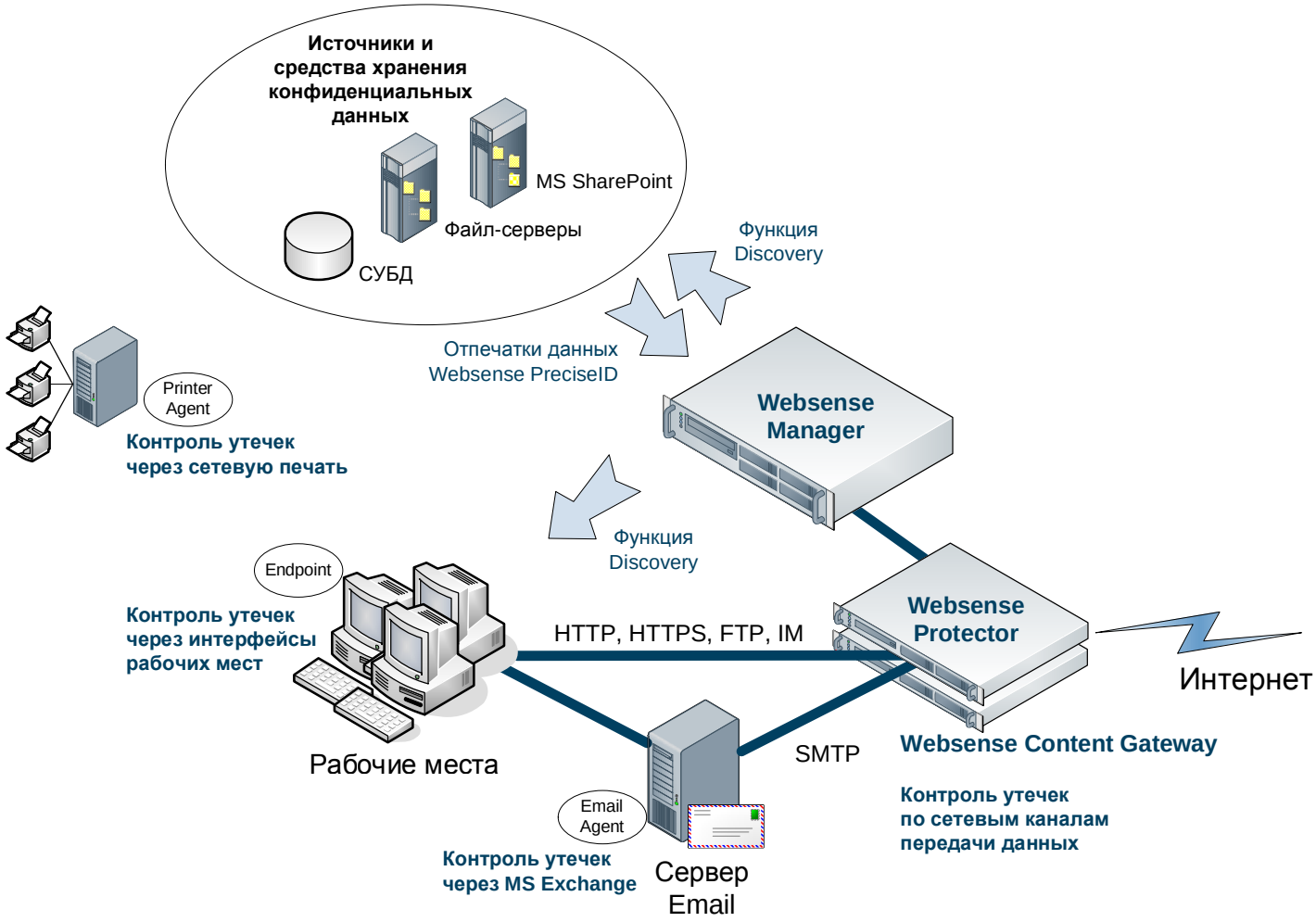


Достоинства решения

- Предотвращает утечки данных
- Управляет соответствием регулятивным нормам и контролирует риски
- Улучшает бизнес-процессы

websense
ESSENTIAL INFORMATION PROTECTION™

Схема работы Websense Data Security



Интеграция с Websense WCG и WSS

- Интеграция с Websense Content Gateway (модуль)
  - Расшифровка сессий SSL и анализ содержимого для обнаружения утечек данных
  - Кэширующий прокси-сервер протоколов HTTP, HTTPS и FTP-поверх-HTTP
  - Поддержка явного режима работы прокси-сервера
  - Поддержка прозрачного режима работы прокси-сервера с использованием WCCP
  - Централизованное управление доверием к сертификатам веб-серверов Интернет (EVA)
- Интеграция с решением веб-фильтрации и веб-безопасности Websense Security Suite
  - Привязка политик предотвращения утечек к категориям веб-сайтов
  - Прозрачная идентификация пользователей домена
  - Блокировка коммуникационных приложений, трафик которых невозможно проанализировать на предмет утечек (напр. Skype)

История успеха (DLP)

- ФК «УРАЛСИБ»
  - Финансовая корпорация "УРАЛСИБ" - многопрофильная финансовая структура, успешно развивающая коммерческий и частный банковский, инвестиционный и страховой бизнес.
- Стоявшая задача
  - Выбор и внедрение решения по предотвращению утечек корпоративных данных
- Выбор решения
  - Рассмотренные решения: Websense, Infowatch, Vontu, McAfee и другие решения из имеющихся на рынке РФ
  - По результатам тестирования выбрано DLP-решение ***Websense Data Security Suite*** (Websense Content Protection Suite)

Технологические преимущества Websense

- Разнообразие методов идентификации содержания информационного обмена (контента)
  - «Отпечатки» данных, ключевые слова, регулярные выражения, словари
- Множество поддерживаемых каналов передачи:
  - электронная почта (SMTP, Exchange)
  - веб (HTTP, HTTPS, FTP)
  - мгновенный обмен (AOL, Yahoo, MSN Messenger)
  - сетевая печать
  - сменные носители, локальная печать (Endpoint)
- Защита от утечек из баз данных
- Возможность обнаружения конфиденциальной информации на серверах и компьютерах сотрудников
- Автоматизация работы по расследованию инцидентов
- Широкие возможности разделения прав доступа и делегирования полномочий

Недостатки конкурирующих решений

- Необходимость предоставления подрядчикам доступа к конфиденциальным данным
- Длительные сроки внедрения
- Сложность эксплуатации
- Ограниченность технологий идентификации конфиденциальных данных
  - Лингвистические технологии имеют большой уровень ложных срабатываний;
  - Регулярные выражения сложны в написании и отладке, не обеспечивают должного уровня распознавания конфиденциального контента;
  - Сложности при обеспечении предотвращения утечек данных из СУБД;
  - Невозможность защиты аудио и графических документов

websense
ESSENTIAL INFORMATION PROTECTION™

СПАСИБО

web security | data security | messaging security