websense
ESSENTIAL INFORMATION PROTECTION™

Смешанные атаки & угрозы Web 2.0: готовы ли вы к 2009?

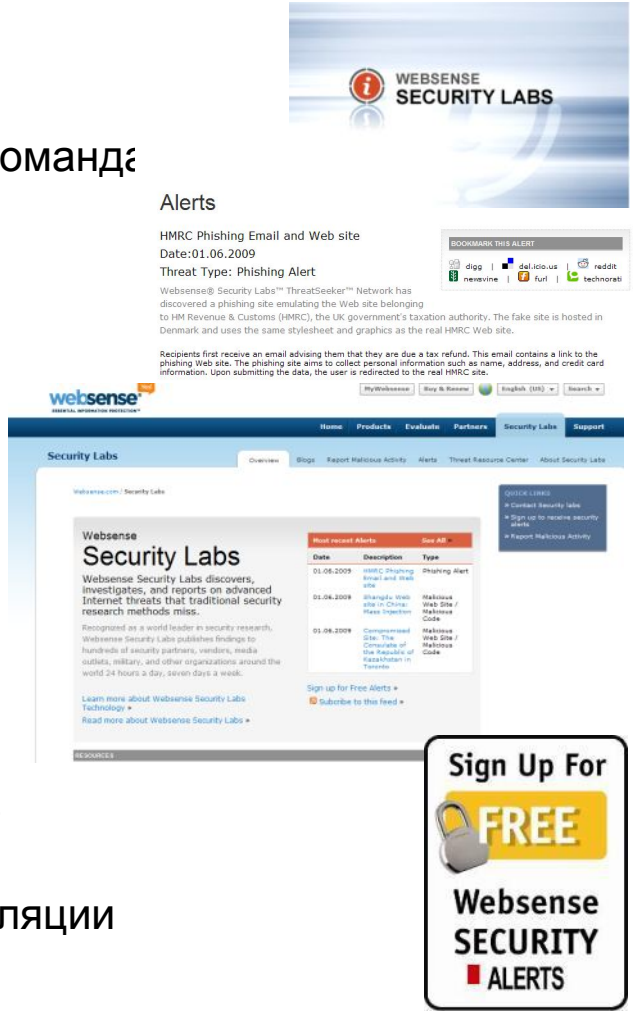
18 июня 2009

Мидхат Семирханов
Территориальный менеджер Россия и СНГ

Банковские Системы и Сети 2009, Ялта

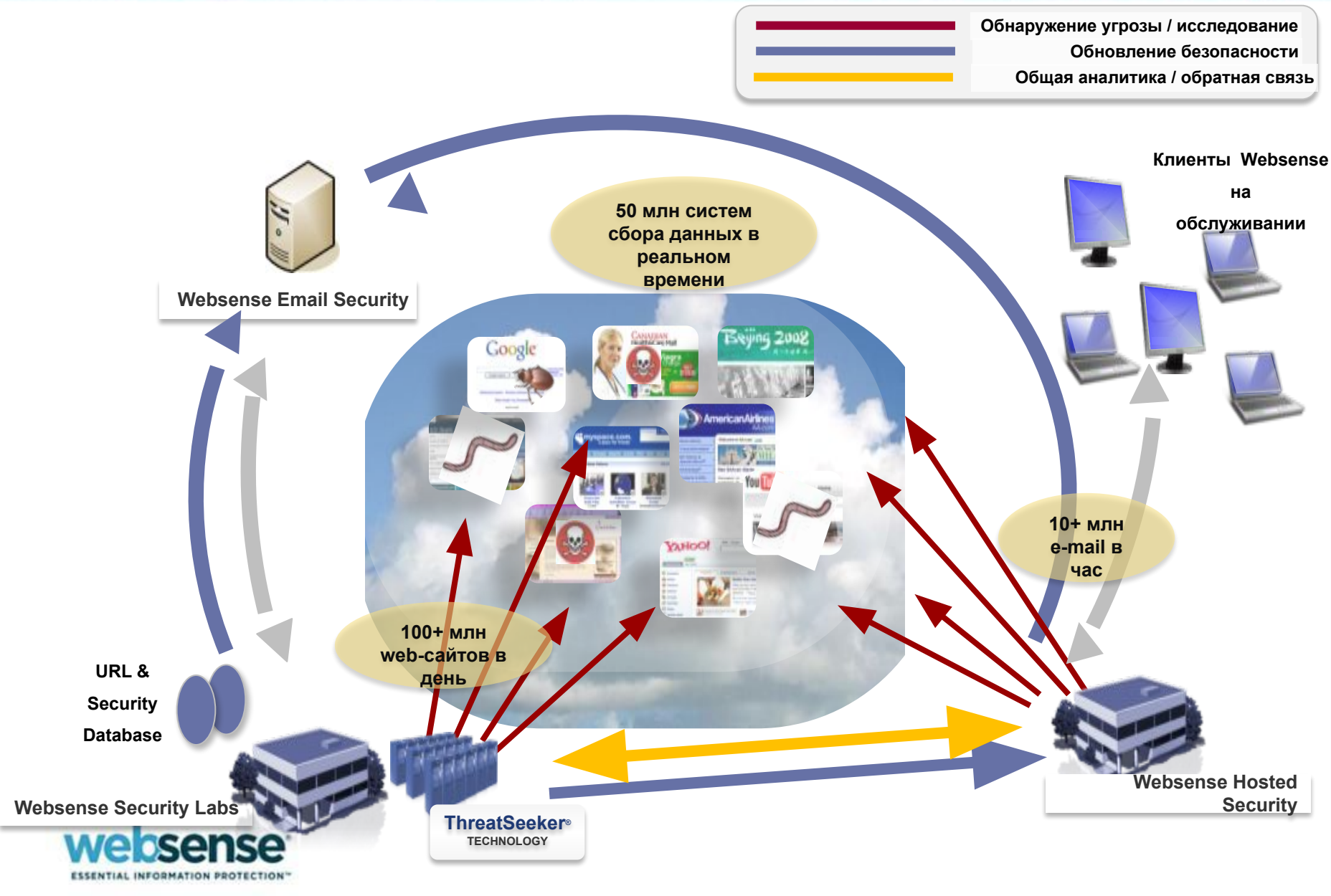
Обзор Websense Security Labs

- 100+ Исследователей и Разработчиков
- Серьезная команда экспертов по безопасности & команда исследований и разработок по безопасности
  - E-mail – угрозы
  - Web - защита
  - Утечка данных
- Экспертиза в следующих ключевых областях:
  - Продвинутые алгоритмы и обучение машин
  - Автоматизированный анализ эвристики
  - Обратный инжиниринг (перепроектировка)
  - JavaScript Deobfuscation
  - Уязвимость и анализ событий
  - Традиционные системы Honeypot
  - Следующее поколение Honeyclients/Honeypots
- Усиление автоматизированной технологии и корреляции данных между нашими 3 областями исследования



websense
ESSENTIAL INFORMATION PROTECTION™

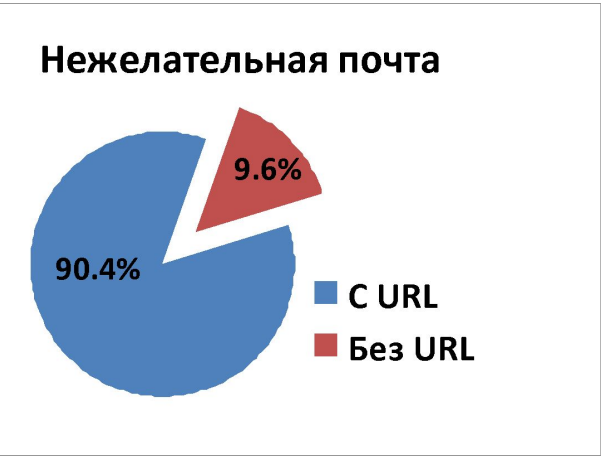
Сеть ThreatSeeker™



Основные моменты Интернет-безопасности

Email и Web угрозы сближаются

- 5 лет назад, malware был приклеплен к e-mail
- Сегодня malware приходит с URL



На **46 %** увеличилось число злонамеренных Web-сайтов, идентифицированных Websense Security Labs за период 01.01.08 – 01.01.09

77 % Web-сайтов с вредоносным программным кодом являются законными сайтами, поставленными под угрозу

70 % 100 самых популярных сайтов или сами пострадали, или были вовлечены во вредоносную деятельность

39 % вредоносных Web-атак содержали код, крадущий информацию

websense
ESSENTIAL INFORMATION PROTECTION™

Каковы риски Web 2.0?

Многие системы обеспечения безопасности полагаются на взгляд назад:

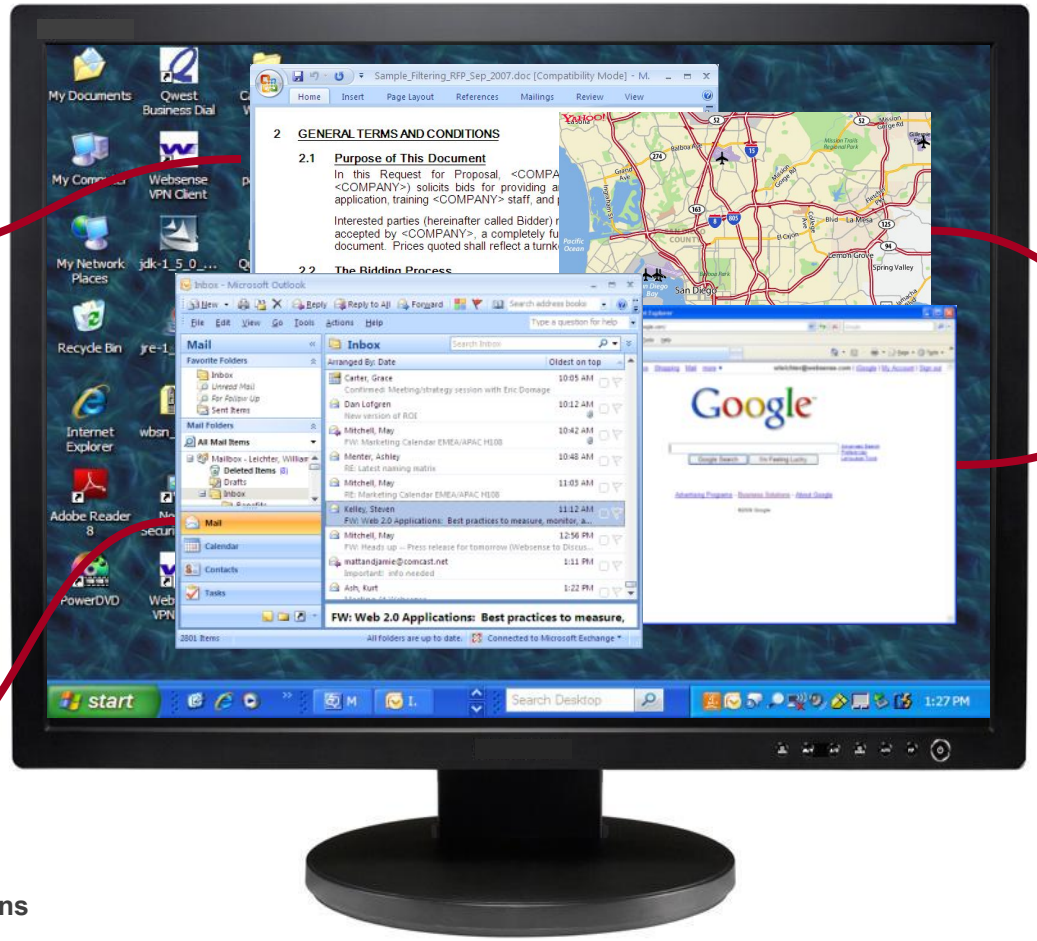
- Системы репутации распознают обычное содержание сайта – но не то, что на нем было размещено.
- Сигнатуры AV являются реактивными – ожидающими, когда ущерб будет нанесен
- Упрощенная, негранулированная политика может привести к избыточному блокированию и запрету доступа к необходимым ресурсам

  Примеры :

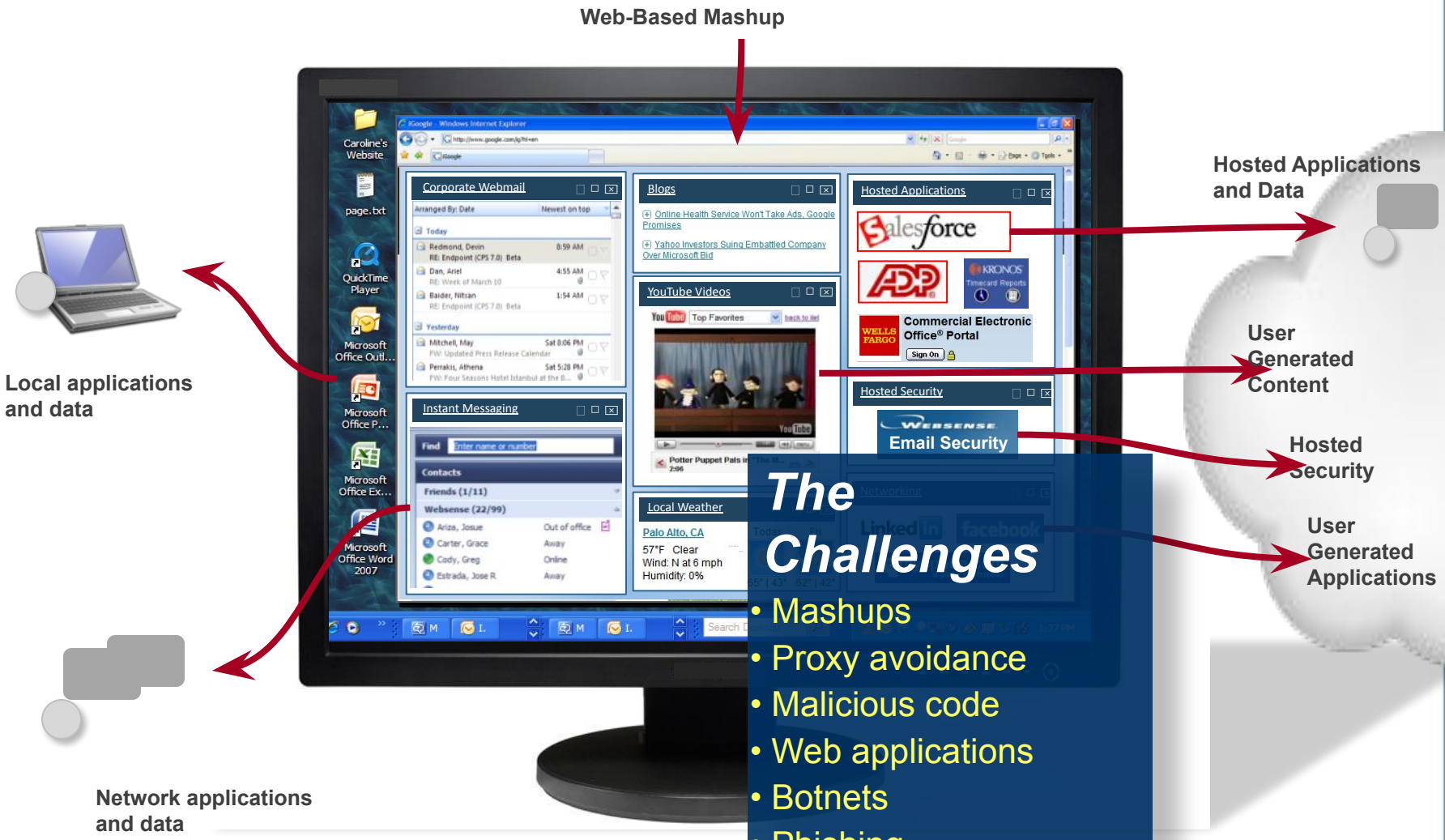
  – *Одноклассники* = **BAD**, блокируются все страницы
  – *Wikipedia* = **GOOD**, разрешен неограниченный доступ

websense
ESSENTIAL INFORMATION PROTECTION™

Панель сегодня

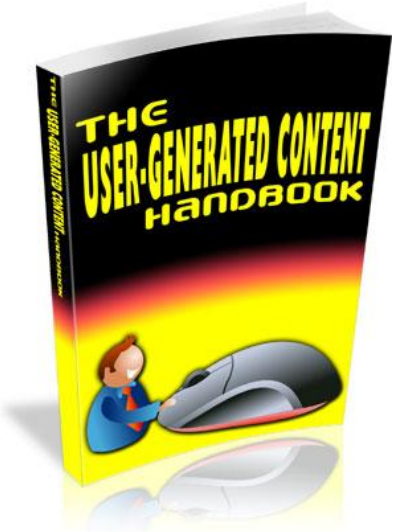


Панель завтра



Web 2.0 позволяет пользователям и хакерам...

- Контент, создаваемый пользователями, предоставляет бесконечные ресурсы для атакующих
- Многие Web 2.0 сайты открывают свободный:
  - Уважаемые Web-экаунты
  - Возможность отправлять и получать e-mail
  - Возможность иметь блоги и загружать свой контент
- Атакующие используют переходное доверие, что увеличивает возможность потери данных.



websense
ESSENTIAL INFORMATION PROTECTION™

Webscape сегодня

70 % топ-100 Web-сайтов пострадали, или были вовлечены во вредоносную деятельность за последние шесть месяцев

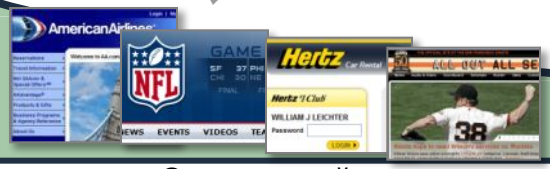
Web - трафик

ДИНАМИЧНЫЙ WEB
- Постоянное изменение содержания
- Миллионы различных страниц на сайте
- Причинение вреда законным сайтам
- Устаревшие системы обеспечения безопасности
- **Требует контент-анализа в реальном времени…**

ИЗВЕСТНЫЙ WEB

Отражающие события, региональные, тематические сайты
- Отсутствие вносимого пользователями контента
- Репутация, довольно эффективные базы данных URL

НЕИЗВЕСТНЫЙ WEB
- Барахло, персонал, жульничество, взрослый, и т.д.
- Ежедневно появляется миллион новых сайтов
- Репутация и базы данных URL не могут поддерживаться на высоком уровне.
- **Требует классификации и оценки безопасности - в реальном времени..**



Топ - 100 сайтов

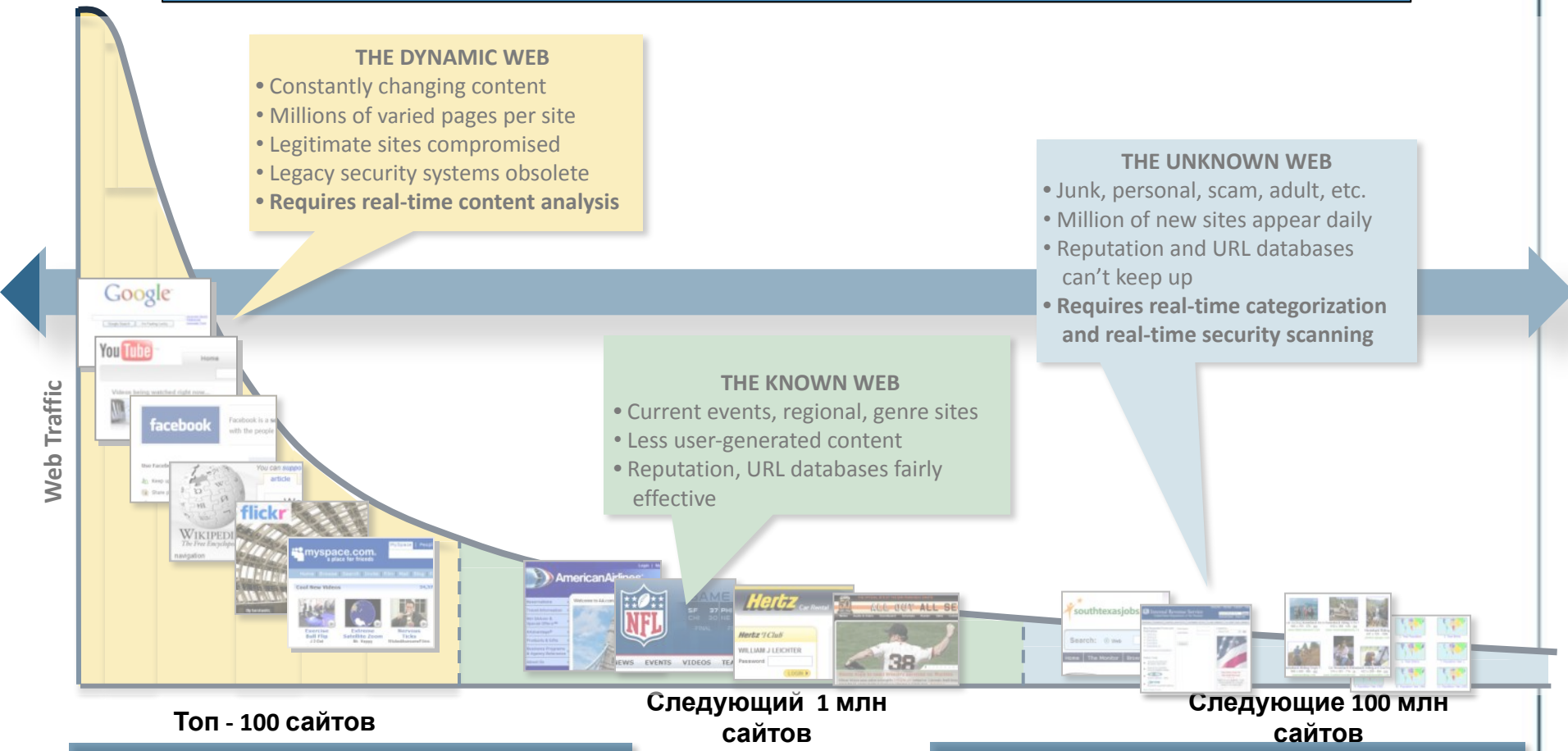
Следующий 1 млн сайтов

Следующие 100 млн сайтов

websense
ESSENTIAL INFORMATION PROTECTION™

Webscape сегодня

90% топ-100 Web–сайтов являются социальными сетями или поисковиками, и более 45% этих сайтов поддерживают создаваемый пользователями



Топ - 100 сайтов

Следующий 1 млн сайтов

Следующие 100 млн сайтов

Требует действующего анализа в реальном времени

Требует превентивного минирования и анализа репутации.

websense
ESSENTIAL INFORMATION PROTECTION™

Сходившиеся Угрозы Поставляют Хиты Брендам

- С 1 января 2008 по 1 января 2009 число вредоносных Web-сайтов **увеличилось на 46%.**
- **77 % Web-сайтов** с вредоносным кодом являются законными сайтами, которые были поставлены под угрозу
- Сайты, дублирующие известные сайты, служили каналом распространения для мошенников - продавцов программного обеспечения

Увеличение использования Web 2.0 сайтов в злонамеренных целях

- Поисковые сайты и сайты социальных сетей предоставляют игровую площадку для хакеров

- Содержание Web 2.0 использует слабости инфраструктуры Сети
- Вредоносные ссылки, замаскированные как популярные видеоклипы, поощряют пользователей загружать «Троянов", чтобы украсть доступные данные
- Зараженные машины пользователей распространяют ссылки через эти социальные сети в других вредоносных целях.

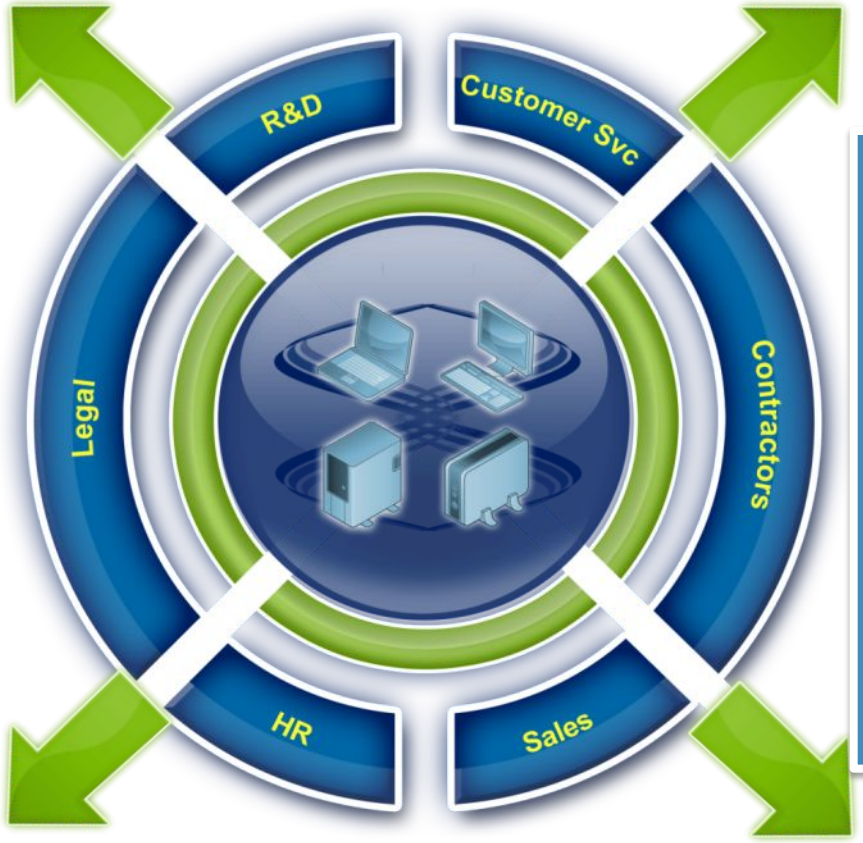
Топ-100 самых популярных Web-сайтов, многие из которых являются социальными сетями, Web 2.0 и поисковые сайты, являются наиболее популярной целью для атак.

websense
ESSENTIAL INFORMATION PROTECTION™

Проблема утечек данных

Конфедециальная информация

Информация о клиентах



39 % вредоносных Web-атак содержат код кражи данных

57 % атак с кражей информации были совершены через Web – их число выросло на 24% за последние 6 месяцев

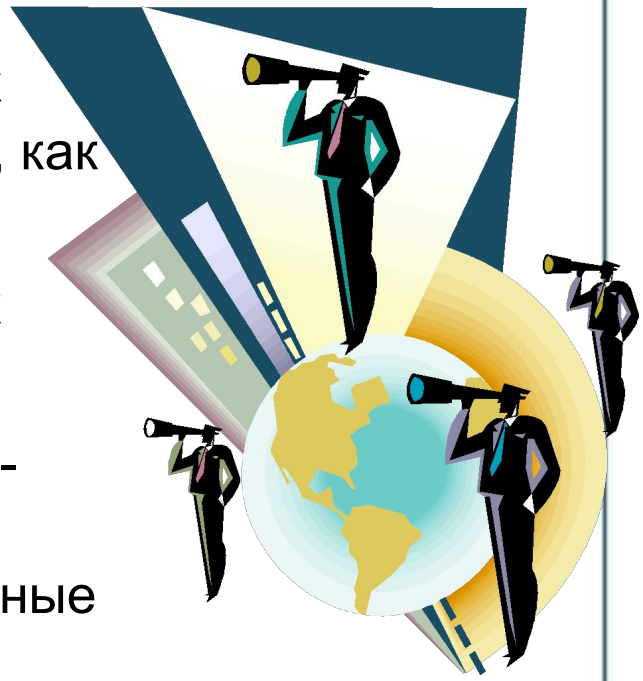
Регулирующая информация

Финансовая информация

websense
ESSENTIAL INFORMATION PROTECTION™

Прогноз безопасности 2009

- “Облако” будет использоваться все чаще во вредоносных целях
- Увеличится использование во вредоносных целях Rich Internet Applications (RIAs), таких, как Flash и Google Gears (=приспособления)
- Нападающие используют в своих интересах программируемый Web
- Существенное повышение количества Web - спама и внесение вредоносного контента в блоги, пользовательские форумы и социальные сети
- Атакующие будут двигаться к распространению модели управления botnets и приему malcode
- Продолжение осады Web-сайтов с "хорошей" репутацией.



websense
ESSENTIAL INFORMATION PROTECTION™

Защита Вашей существенной информации

Midkhat Semirkhanov
24 марта 2009

Готов ли ваш план безопасности к 2009?

- Web 2.0 открывает новые возможности, но создает новые риски
- Converged email и Web 2.0 threats становятся нормой
- Смешанные атаки увеличивают риск потери данных
- Можете ли вы сказать “ДА” Web 2.0 без угрозы для безопасности?
- Первое, что вам необходимо – защитить вашу **существенную информацию**

Websense Комплексная защита информации

websense
ESSENTIAL INFORMATION PROTECTION™

Передовая классификация – это различие

Почта

Web

Деловая информация

Classification - Websense Unique Intellectual Property

WEBSENSE ThreatSeeker Technology

PreciseID TECHNOLOGY

0 нераспознанных

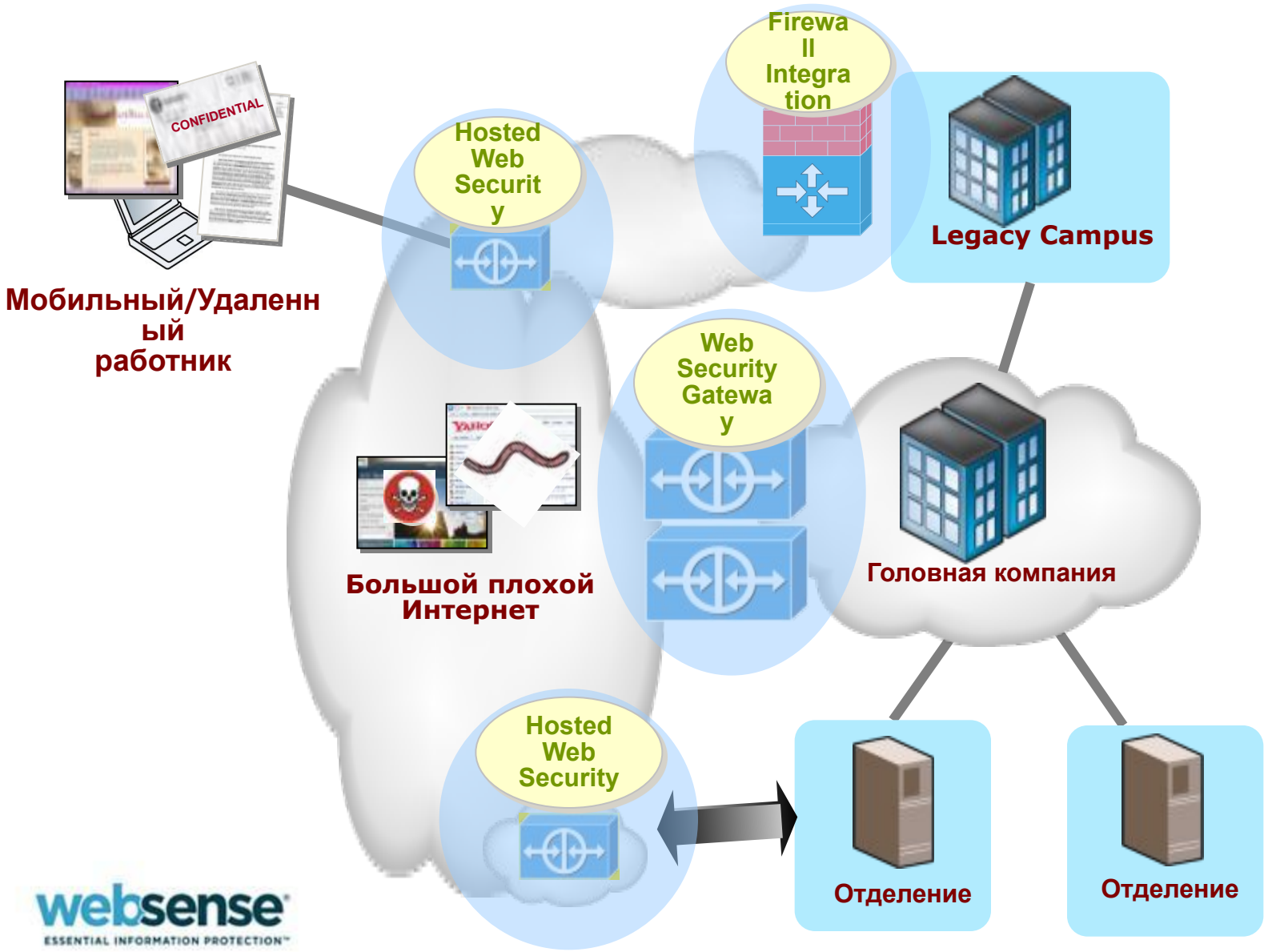
- - -

“Узнать неизвестное”

Комплексная защита информации

websense
ESSENTIAL INFORMATION PROTECTION™

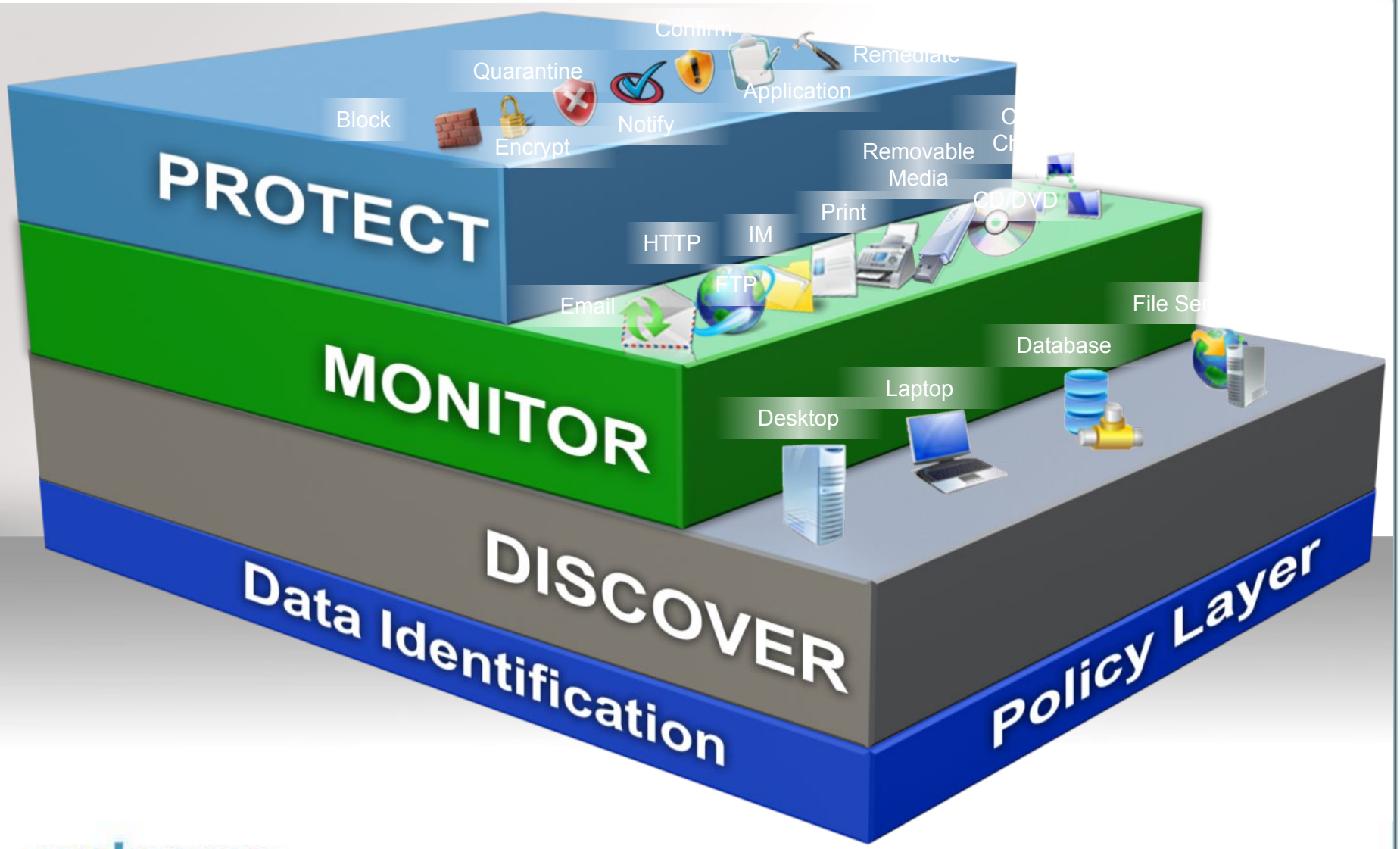
“Система” Web-безопасности



websense
ESSENTIAL INFORMATION PROTECTION™

Websense Data Security Suite

Комплексное предотвращение потери данных

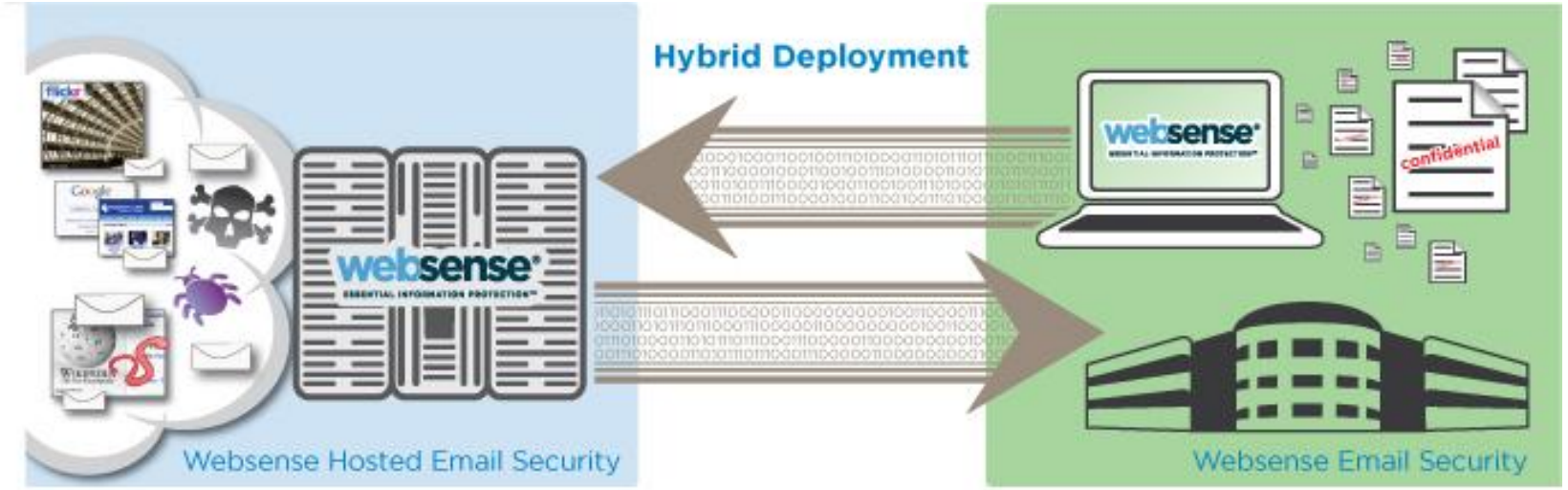


websense
ESSENTIAL INFORMATION PROTECTION™

Подход Websense к безопасности сообщений

Остановите угрозы прежде, чем они достигнут Вашей сети

Управляйте несоответствующим содержанием и утечками данных

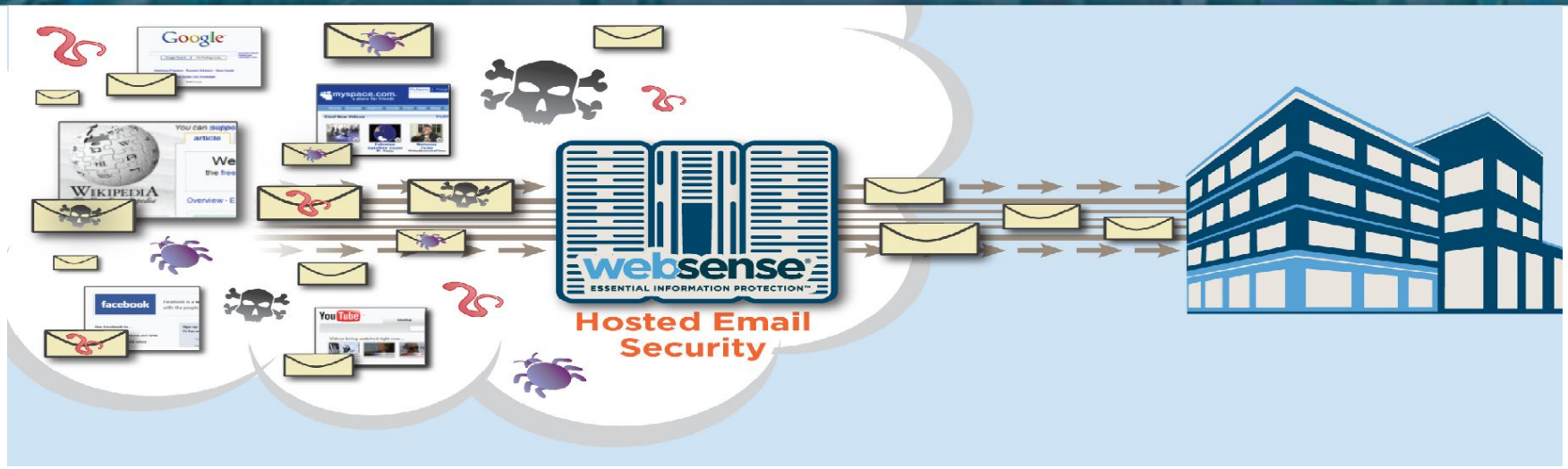


Преимущества:

- Ведущая защита от сходившейся электронной почты и угроз Web 2.0
- Сокращенный и стабилизированный входящий трафик -> требуется меньшее хранилище и пропускная способность
- Безграничная возможность перехвата спама -> не нужно обновлять «железо»
- Простая установка
- Включает Data Security Suite intelligence

websense
ESSENTIAL INFORMATION PROTECTION™

Websense-безопасность входящей почты



- Небольшие затраты и невысокая сложность
  - Нет необходимости покупки и поддержания оборудования
  - Упрощенное администрирование
- Усиленная защита
  - Упор на безопасность от смешанного e-mail и угроз Web 2.0
  - Опирающиеся на ведущие отрасли SLAs
  - Задействован ThreatSeeker Network
- Управление контролем
  - Гибкая настройка политик, возможность изменения установок, управление карантином, формирование отчетов
  - Возможность доступа 24 x 7

websense
ESSENTIAL INFORMATION PROTECTION

РЕЗЮМЕ

В сегодняшних угрозах безопасности доминируют сходящиеся угрозы & риски потери данных

- **Websense позволяет вам сказать “Да” Web 2.0**
  - Уникальные возможности для удовлетворения новых потребностей безопасности
  - Непревзойденная экспертиза в превентивном обнаружении угроз.
- **Комплексный портфель продуктов**
  - Интегрированная безопасность Web, данных и сообщений
  - Никакой другой вендор не может построить комплексную политику «КТО, ЧТО, ГДЕ и КАК»
- **Websense является лидером рынка**
  - Более 50,000 клиентов по всему миру
  - Лидер по доле рынка и инновациям в обеспечении комплексной защиты информации

Спросите Вашего Партнера или Торгового представителя о том, как получить Hosted Email Security на ОДИН год БЕСПЛАТНО!

Загрузите наш отчет об угрозах сегодня:
http://www.websense.com/site/buzzroom/featuredstories/security.html

Questions

- **СПАСИБО ЗА ВНИМАНИЕ!**