



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 Honeyrot
 - Следующее поколение Honeyclients/Honeybots
- Усиление автоматизированной технологии и корреляции данных между нашими 3 областями исследования



Alerts

HMRC Phishing Email and Web site

Date: 01.06.2009

Threat Type: Phishing Alert

Websense® Security Labs™ ThreatSeeker™ Network has discovered a phishing site emulating the Web site belonging to HM Revenue & Customs (HMRC), the UK government's taxation authority. The fake site is hosted in Denmark and uses the same stylesheet and graphics as the real HMRC Web site.

Recipients first receive an email advising them that they are due a tax refund. This email contains a link to the phishing Web site. The phishing site aims to collect personal information such as name, address, and credit card information. Upon submitting the data, the user is redirected to the real HMRC site.

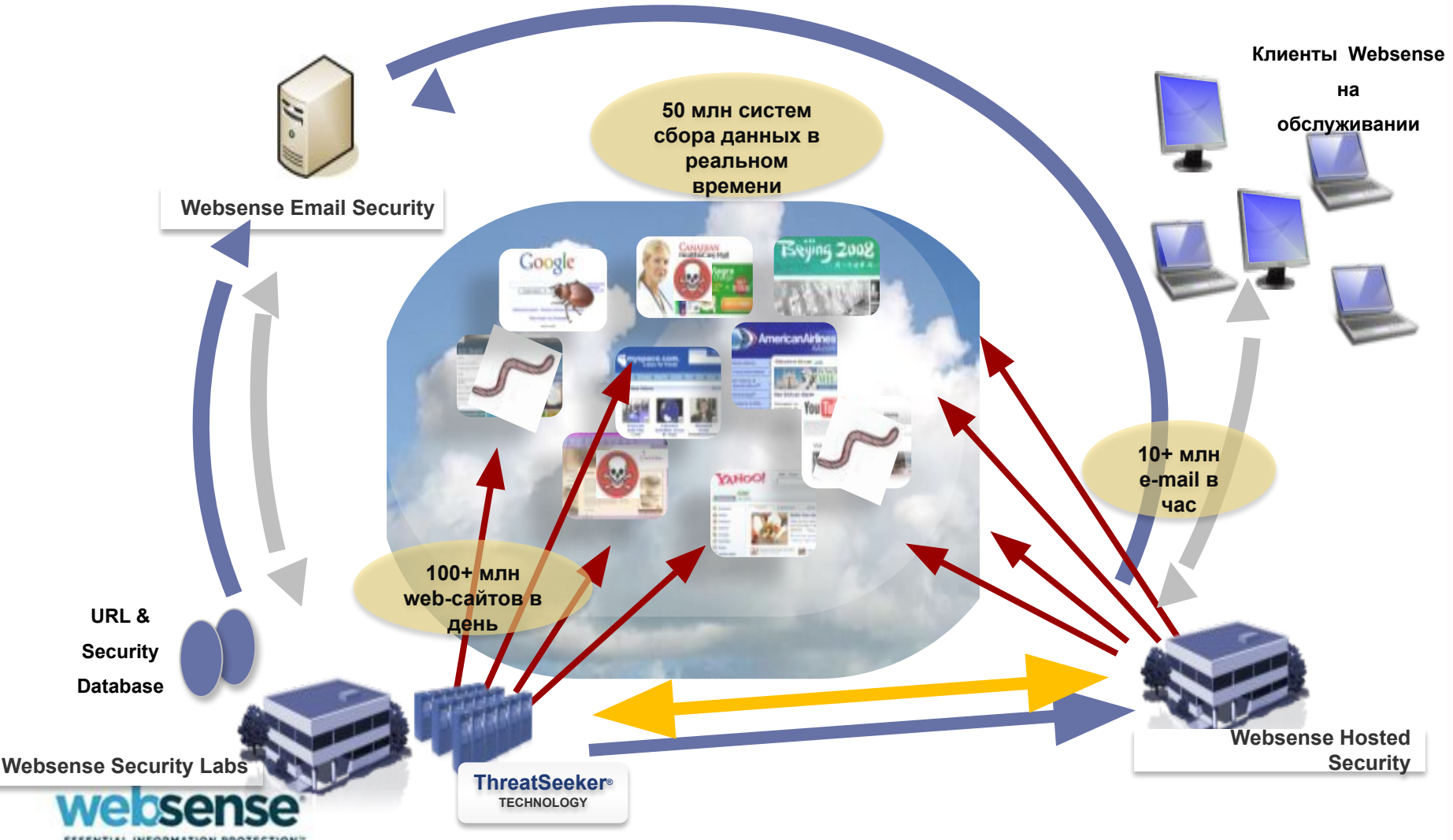
A screenshot of the Websense Security Labs website. The page title is 'WebSense Security Labs'. It features a navigation bar with links for Home, Products, Evaluate, Partners, Security Labs, and Support. Below the navigation bar, there's a section for 'WebSense Security Labs' with a description of their research and a 'Most recent Alerts' table. The table has columns for Date, Description, and Type. There are also links for 'Learn more about Websense Security Labs Technology' and 'Read more about Websense Security Labs'.

Date	Description	Type
01-06-2009	HMRC Phishing Email and Web site	Phishing alert
01-04-2009	Change Mail Site in China: Mass Injection	Malicious Web Site / Malicious Code
01-04-2009	Compromised Site: The Corporate of the Republic of Kazakhstan in Russia	Malicious Web Site / Malicious Code



Сеть ThreatSeeker™

Обнаружение угрозы / исследование
Обновление безопасности
Общая аналитика / обратная связь

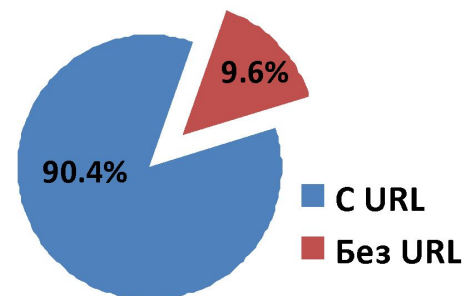


Основные моменты Интернет-безопасности

Email и Web угрозы сближаются

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

Нежелательная почта



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

Каковы риски Web 2.0?

Многие системы обеспечения безопасности полагаются на взгляд назад:

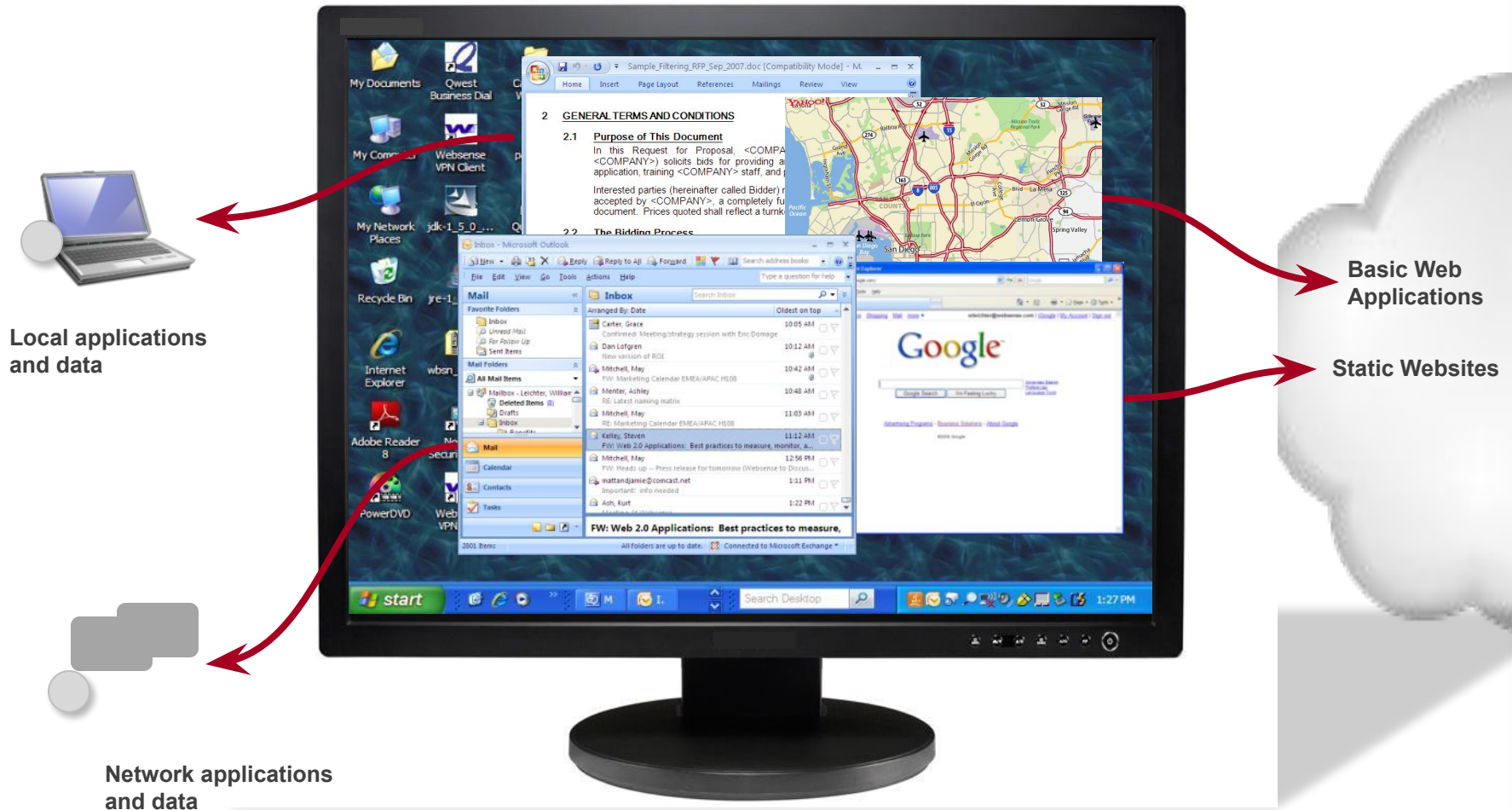


- Системы репутации распознают обычное содержание сайта – но не то, что на нем было размещено.
- Сигнатуры AV являются реактивными – ожидающими, когда ущерб будет нанесен
- Упрощенная, негранулированная политика может привести к избыточному блокированию и запрету доступа к необходимым ресурсам

Примеры :

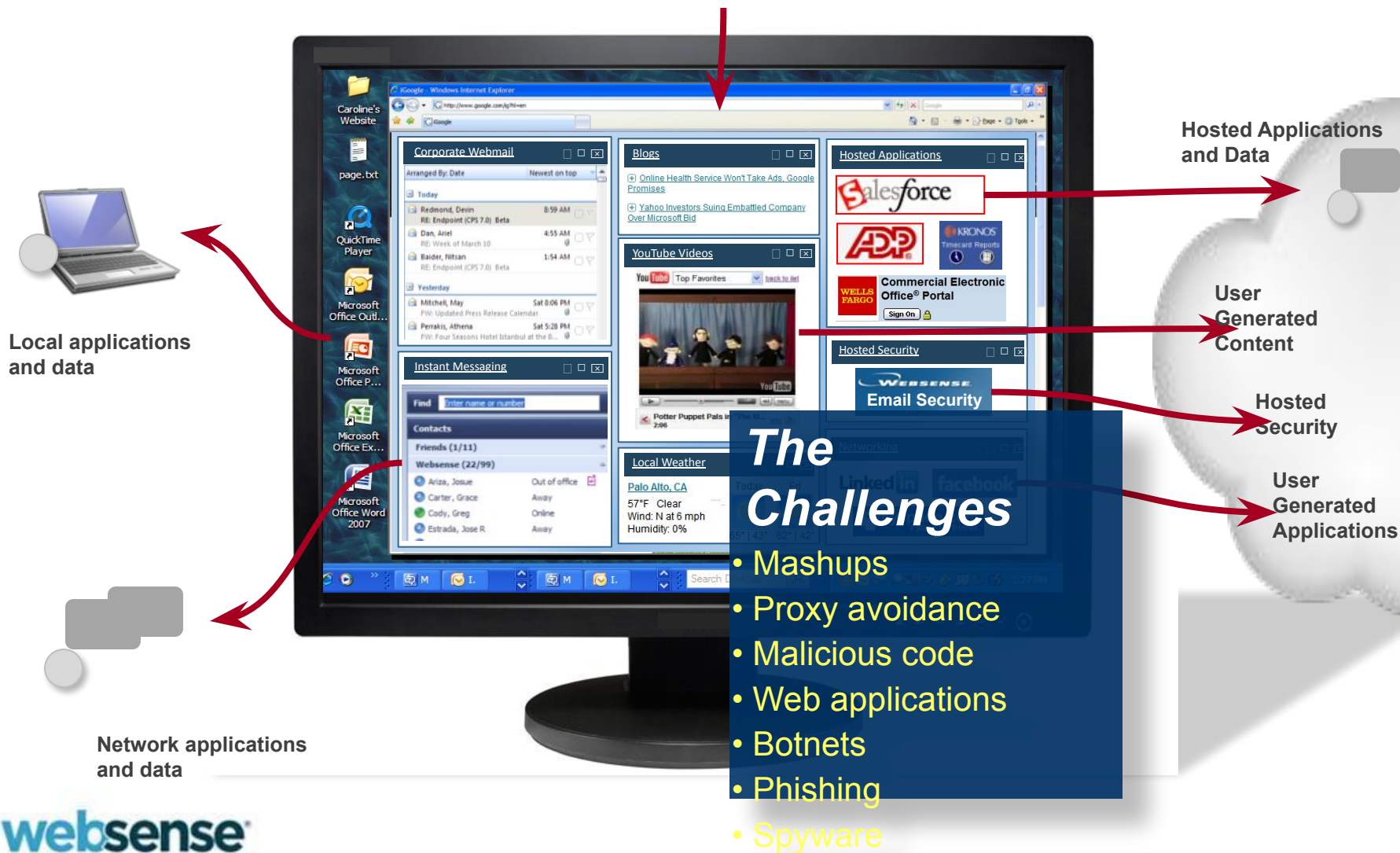
- *Одноклассники* = **BAD**, блокируются все страницы
- *Wikipedia* = **GOOD**, разрешен неограниченный доступ

Панель сегодня



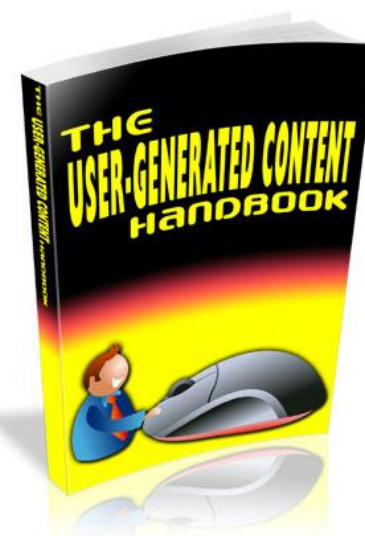
Панель завтра

Web-Based Mashup



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.



Webcare сегодня

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

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

- Баракло, 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..**



Webcare сегодня

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

THE DYNAMIC WEB

- Constantly changing content
- Millions of varied pages per site
- Legitimate sites compromised
- Legacy security systems obsolete
- **Requires real-time content analysis**

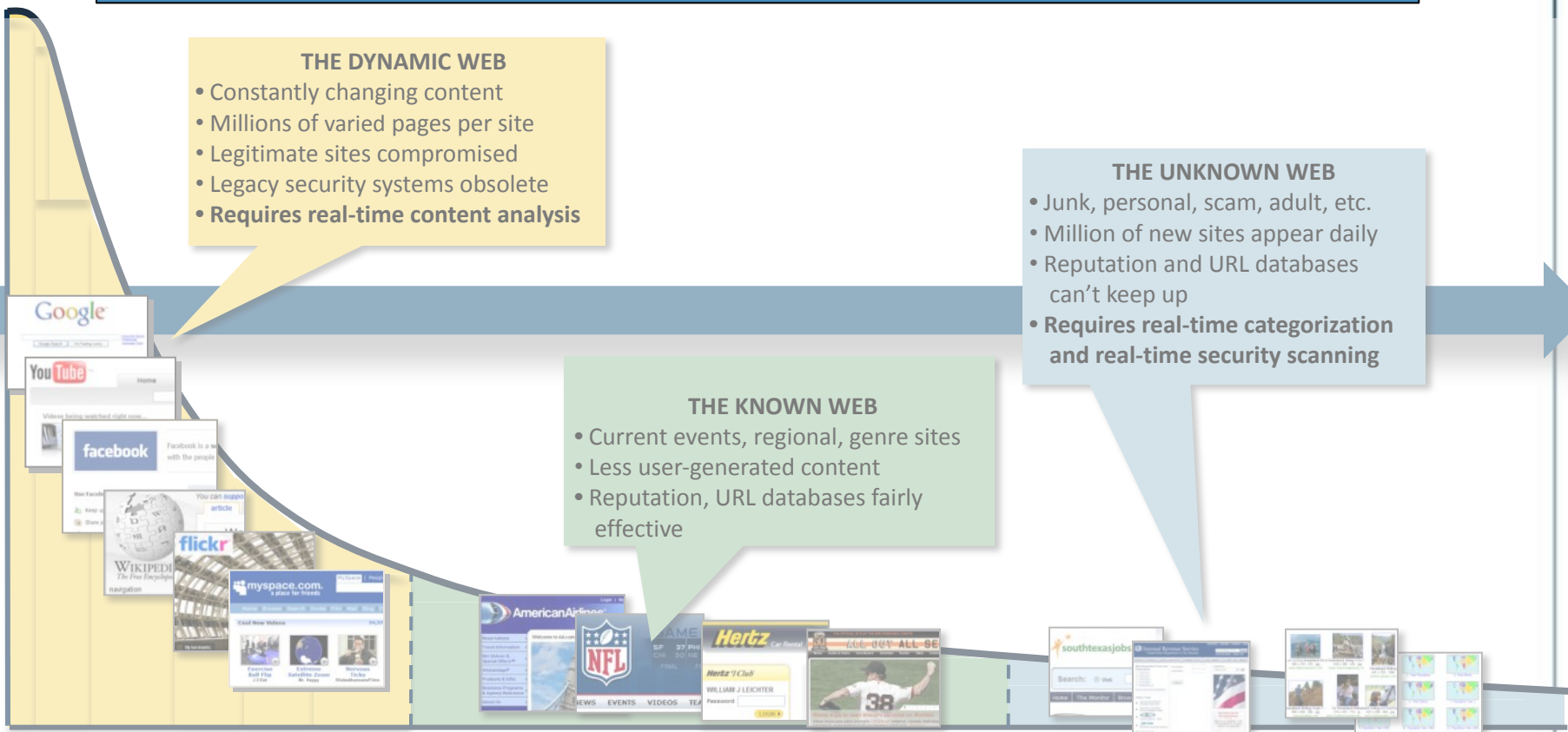
THE UNKNOWN WEB

- Junk, personal, scam, adult, etc.
- Million of new sites appear daily
- Reputation and URL databases can't keep up
- **Requires real-time categorization and real-time security scanning**

THE KNOWN WEB

- Current events, regional, genre sites
- Less user-generated content
- Reputation, URL databases fairly effective

Web Traffic



Топ - 100 сайтов

Следующий 1 млн сайтов

Следующие 100 млн сайтов

Требует действующего анализа в реальном времени

Требует превентивного минирования и анализа репутации.

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

- Поисквые 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.

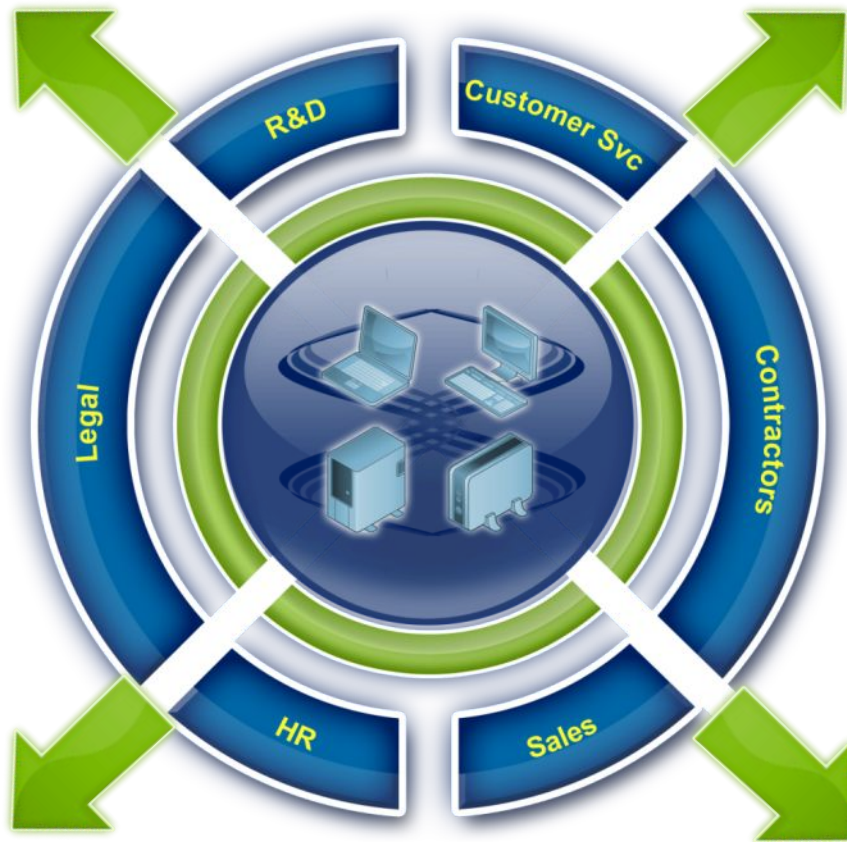


Топ-100 самых популярных Web-сайтов, многие из которых являются социальными сетями, Web 2.0 и поисковые сайты, являются наиболее популярной целью для атак.

Проблема утечек данных

Конфеденциальная 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

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.





Защита Вашей существенной информации

Midkhat Semirkhanov
24 марта 2009

Готов ли ваш план безопасности к 2009?

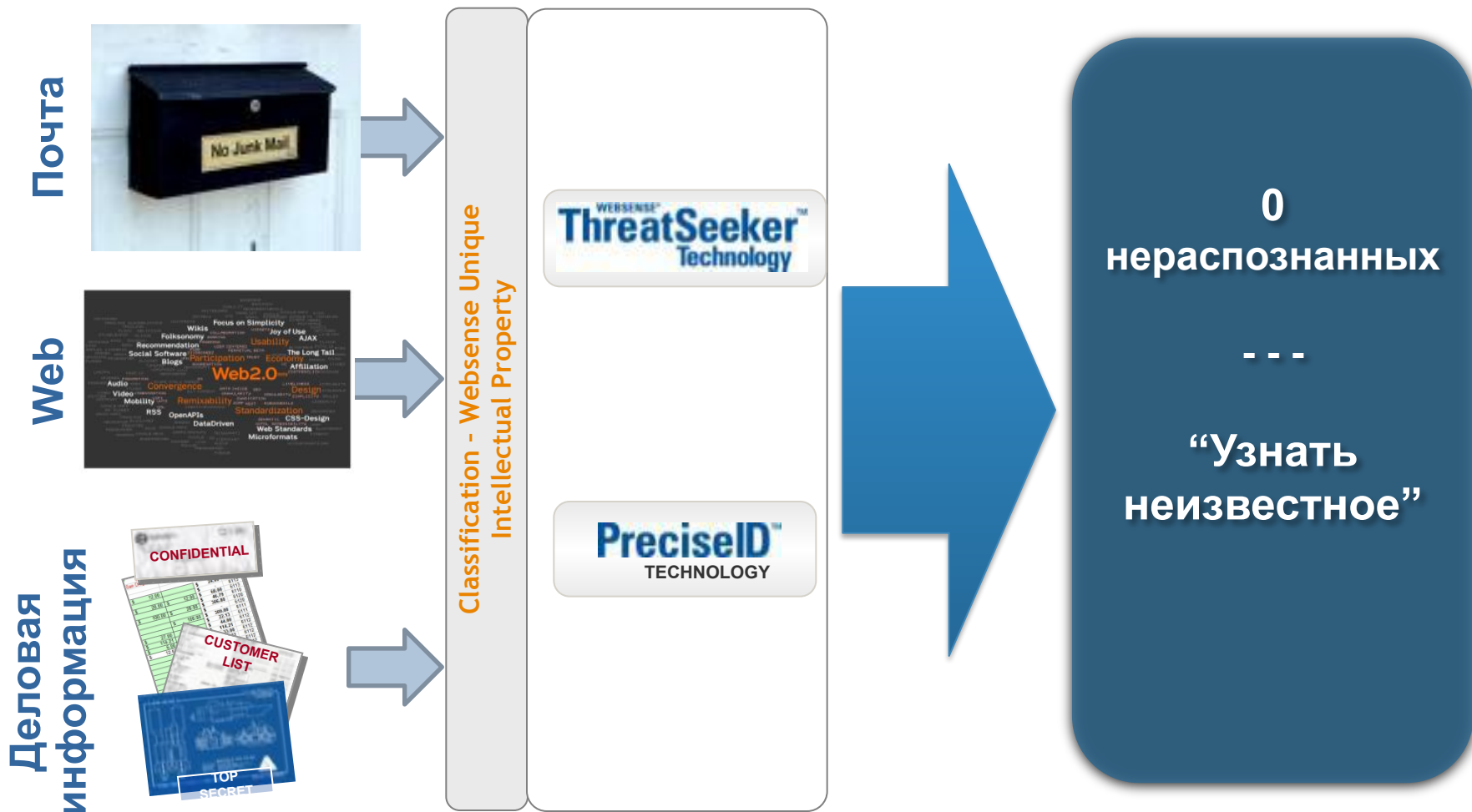
- Web 2.0 открывает новые возможности, но создает новые риски
- Converged email и Web 2.0 threats становятся нормой
- Смешанные атаки увеличивают риск потери данных
- Можете ли вы сказать “ДА” Web 2.0 без угрозы для безопасности?
- Первое, что вам необходимо – защитить вашу **существенную информацию**



WebSense Комплексная защита информации

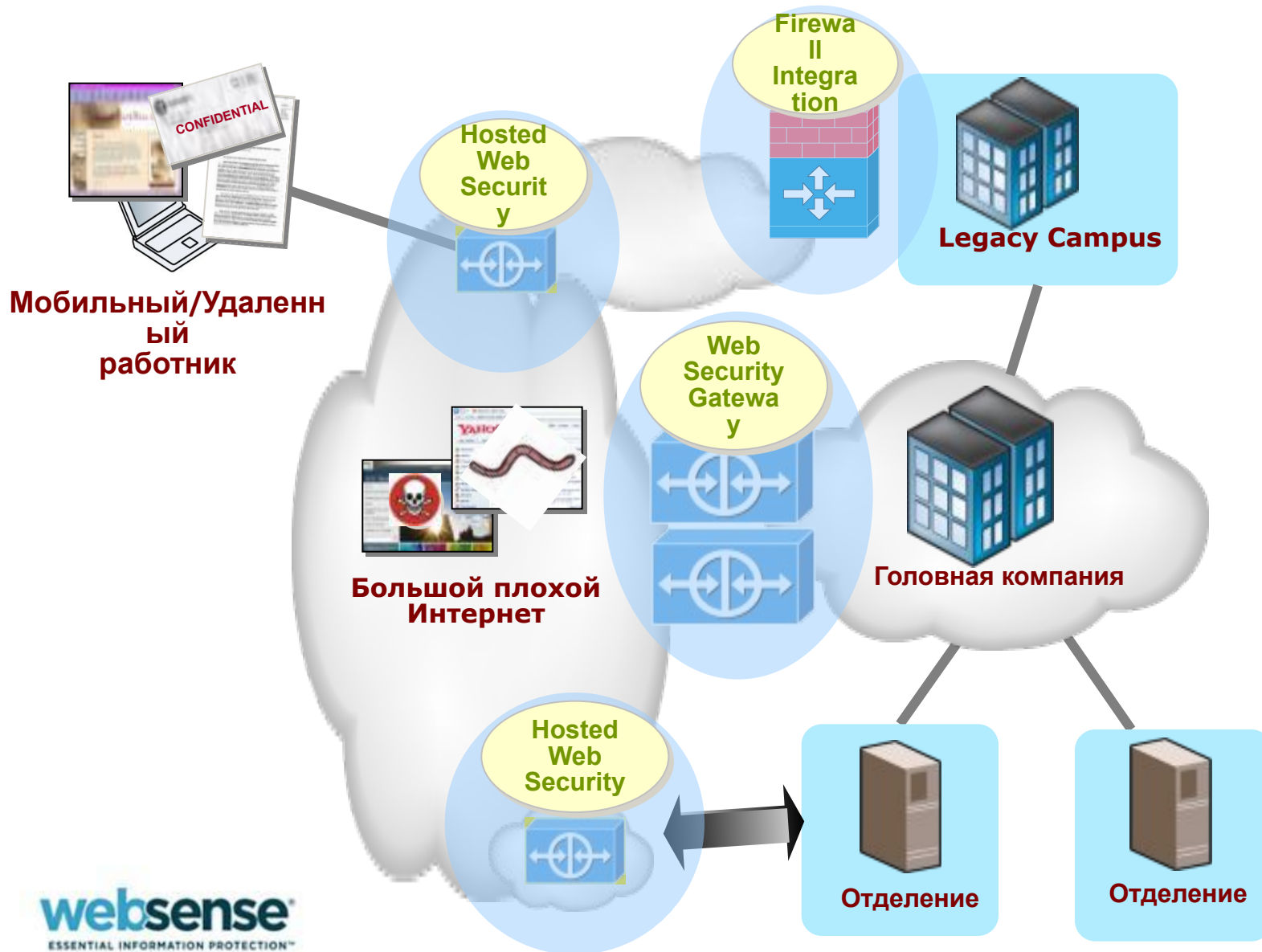


Передовая классификация – это различие



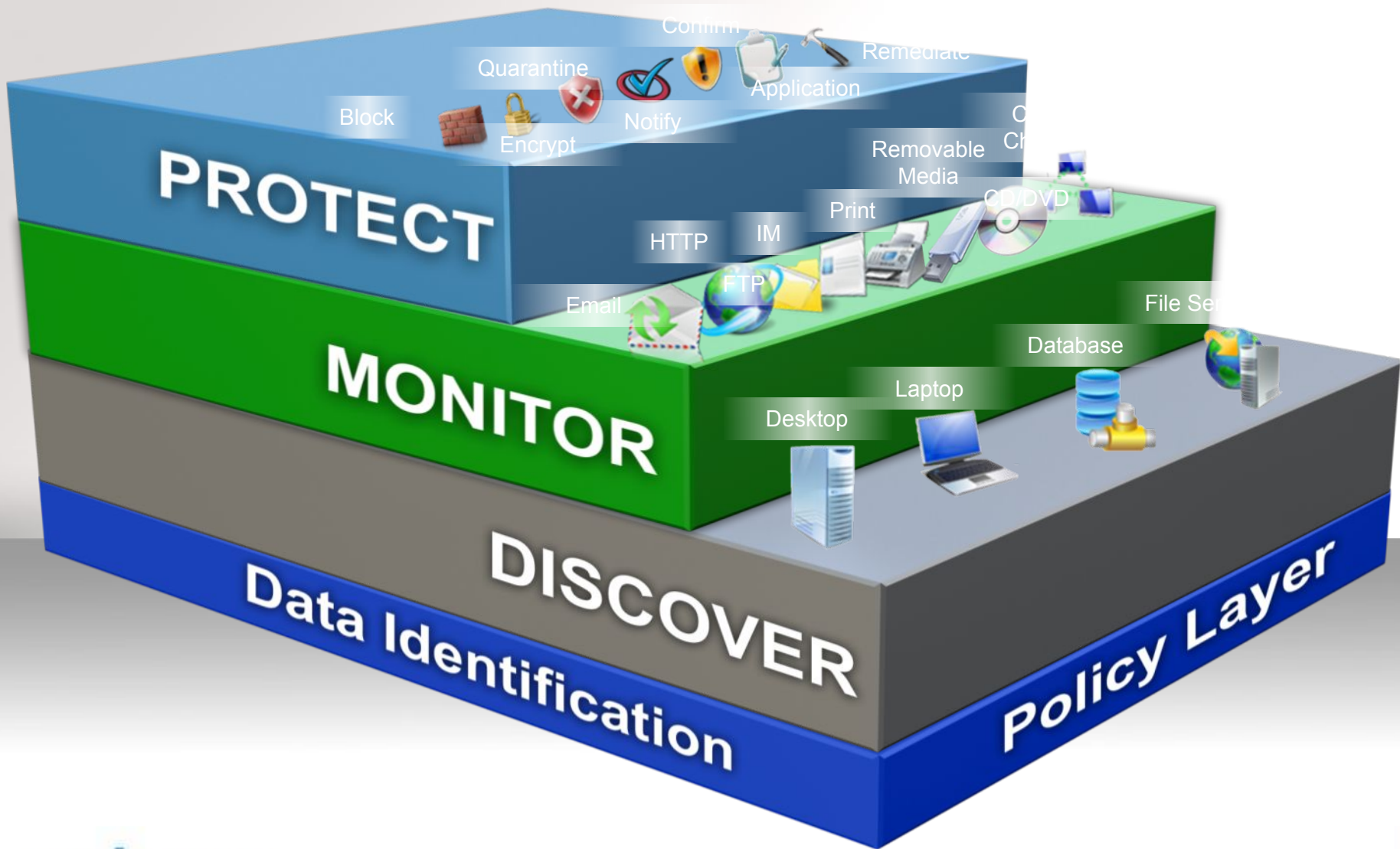
Комплексная защита информации

“Система” Web-безопасности



Websense Data Security Suite

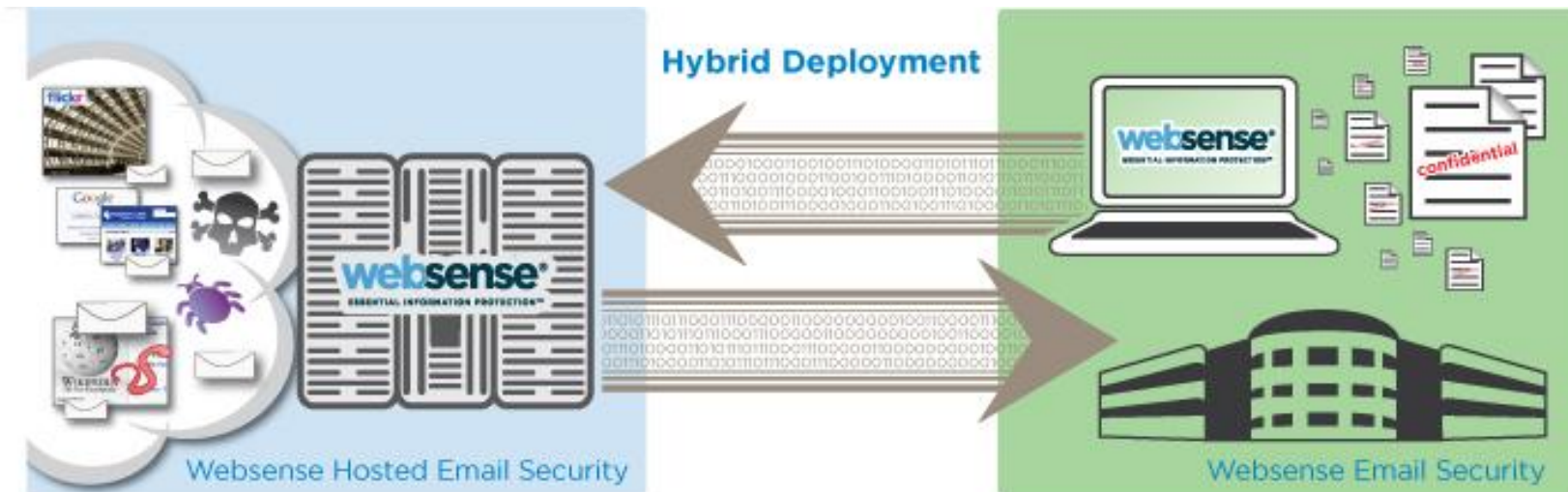
Комплексное предотвращение потери данных



Подход Websense к безопасности сообщений

Остановите угрозы
прежде, чем они
достигнут Вашей сети

Управляйте несоответствующим
содержанием и утечками данных



Преимущества:

- Ведущая защита от сходящейся 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-безопасность входящей почты

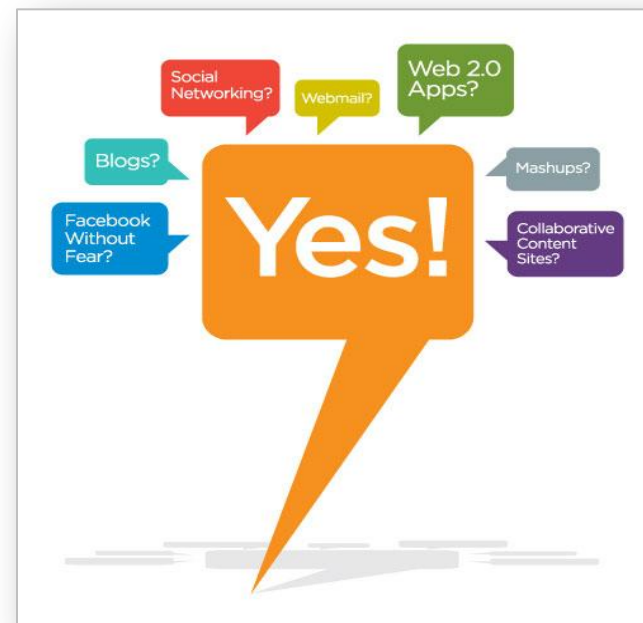


- **Небольшие затраты и невысокая сложность**
 - Нет необходимости покупки и поддержания оборудования
 - Упрощенное администрирование
 - **Усиленная защита**
 - Упор на безопасность от смешанного e-mail и угроз Web 2.0
 - Опирающиеся на ведущие отрасли SLAs
 - Задействован ThreatSeeker Network
 - **Управление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

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!

