

Security As A Service





Сфера деятельности компаний – IT-Security

Headtechnology – дистрибьютор решений по информационной безопасности

Svit IT – интегратор решений по ИБ

Сотрудничество с 2007-го года
Более 30 совместных проектов



perfecting the art of network security



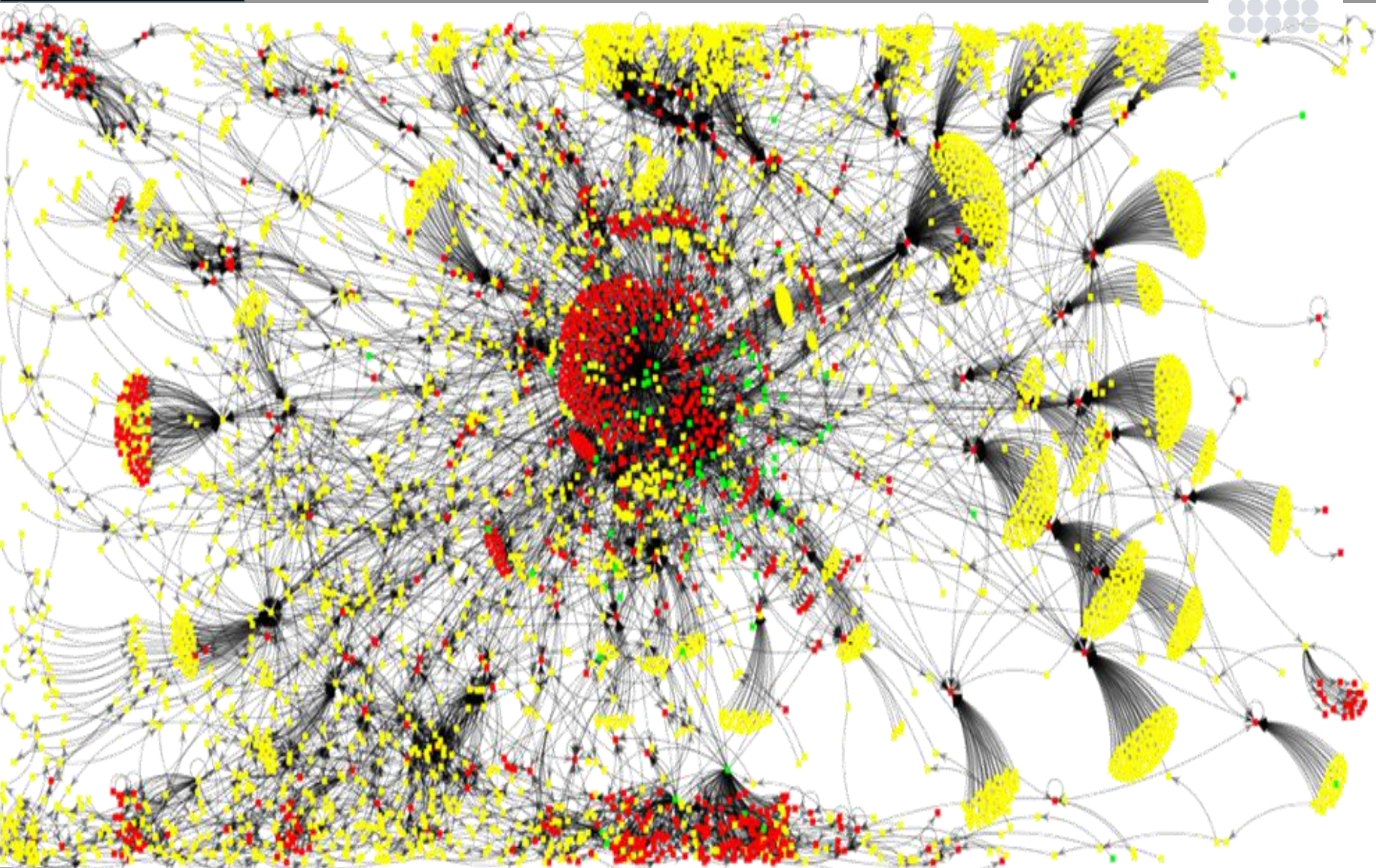
Control tomorrow's email risks today



Blue  Coat[®]



**Сделайте интернет
безопаснее**





• Домашние пользователи

- Заражение вирусами и другим вредоносным ПО
- Фишинговые атаки, кража персональных данных и мошенничество
- Любой контент доступен для детей
- Виртуальный мир становится важнее реального с развитием онлайн-игр и социальных сетей





■ Корпоративные клиенты

- Постоянная борьба с **web угрозами**
- Необходимость предотвращения **утечки данных**
- **Соответствие** корпоративным правилам использования Интернет
- Беспольный контент **переполняет сеть**
- Необходимость **защитить всех пользователей**, где бы они не находились
- **Возможность видеть** web и сетевые активности

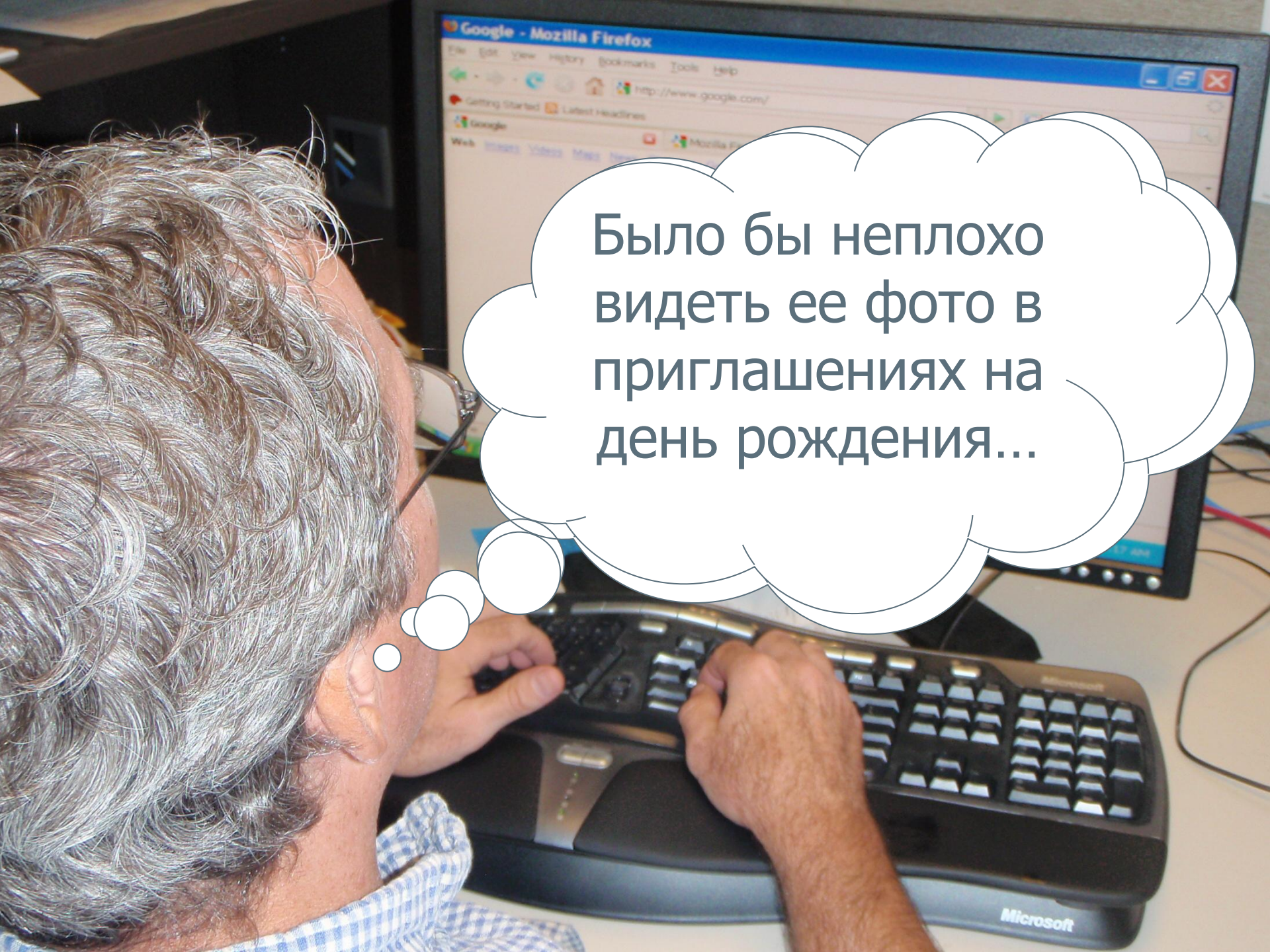
У 90% украинских компаний установлен Squid, либо Microsoft ISA в качестве прокси сервера. Нет ни одной компании, которая была бы довольна этими решениями.



“Как Hannah Montana сломала компьютер?”

Еще одна «хакерская группировка
из СНГ» 😊





Было бы неплохо
видеть ее фото в
приглашениях на
день рождения...



Google™

printable hannah montana party invitations

[Advanced Search](#)
[Language Tools](#)

Google Search

I'm Feeling Lucky

[Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2009 - [Privacy](#)



printable hannah maontana party invitations

Search

[Advanced Search](#)
[Preferences](#)

Google SafeSearch is ON Search: the web pages from the UK



Web [+ Show options...](#)

Did you mean: [printable hannah **montana** party invitations](#)

[%o° Free Printable Disney Character Birthday Party Invitations](#)

Kids Birthday party themed Invitations Free Printable Disney Character Birthday Party ...
Hannah Montana Birthday Party Invitation. June 22, 2006 ...
[disney-stationary.com/greeting-cards/birthday-invitations.php](#) - [Cached](#) - [Similar](#)

[Free Printable Disney's Channels Hannah Montana Birthday Party ...](#)

Free Printable Disney's Channels **Hannah Montana** Birthday Invitation Miley Cyrus.
[disney-stationary.com/.../Hannah-Montana-Birthday-Party-Invitation.php](#) - [Cached](#) - [Similar](#)

[Hannah Montana Invitations - Birthday Party, Custom, Personalized ...](#)

<http://www.personalizedpartyinvites.com> Get custom **Hannah Montana** birthday party invitations at www.personalizedpartyinvites.com There are several - Event ...
[sandiego.olx.com/hannah-montana-invitations-birthday-party-custom-personalized-printable-iiid-8884501](#) - [Cached](#) - [Similar](#)

[Hannah Montana Birthday Party Invitations - Associated Content](#)

26 Mar 2008 ... At Disney-Stationary.com you can access a free printable **Hannah Montana** birthday party invitation. The cover features **Hannah Montana** and the ...
[www.associatedcontent.com/.../hannah_montana_birthday_party_invitations.html](#) - [Cached](#) - [Similar](#)

[Hanna Montana Happy Birthday Printable Invitations](#)

18 Aug 2009 ... Free **Printable Hannah Montana Birthday Party Invitations**: At Disney-Stationary.com you can
[xdesignstudios.com/.../index.php?...hanna-montana...printable-invitations](#) - [Similar](#)

[Hannah Montana Birthday Party Invitations: Free Printable Place ...](#)

Hannah Montana Invitations will set the theme of your celebration immediately when your



The page at <http://safeonlinescannerv4.com> says:



Warning!!! Your computer contains various types of vulnerabilities and threats.

Your system requires immediate anti viruses scan! Personal Antivirus can perform fast and free virus and malicious software scan of your computer .

OK

Cancel

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

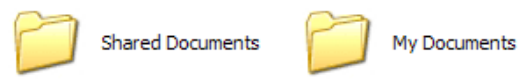
Details

My Computer System Folder

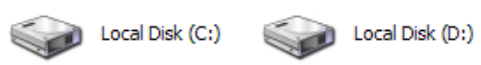
Your Info

IP: 65.46.48.194
 Country: United States
 City: Draper
 Your private data is under attack!

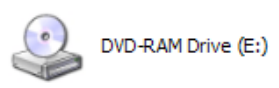
System scan progress



Hard drives



DVD



Scanning completed. 527 Probably harmful items was found!

Your Computer is Infected!

Threats and actions:

Name	Risk level	Date
Email-Worm.Win32.Net	Critical	11.18.2008
Email-Worm.Win32.Myd	Critical	11.18.2008
Win 32:Delf-XQ	Critical	11.18.2008

Description:

This program is potentially dangerous for your system. Trojan-Downloader stealing passwords, credit cards and other personal information from your computer.

Advice:

You need to remove this threat as soon as possible!

Windows Security Alert

To help protect your computer, Windows Web Security has detected trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
<input checked="" type="checkbox"/> Admess.Trojan	tcpservice2.exe
<input checked="" type="checkbox"/> zserv.Transponder.Trojan	ZServ.dll
<input checked="" type="checkbox"/> Wstart.TrojanDownloader	wstart.dll

Remove all **Cancel**

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gathered information can be passwords, e-mail addresses and all that data, which is important for you.

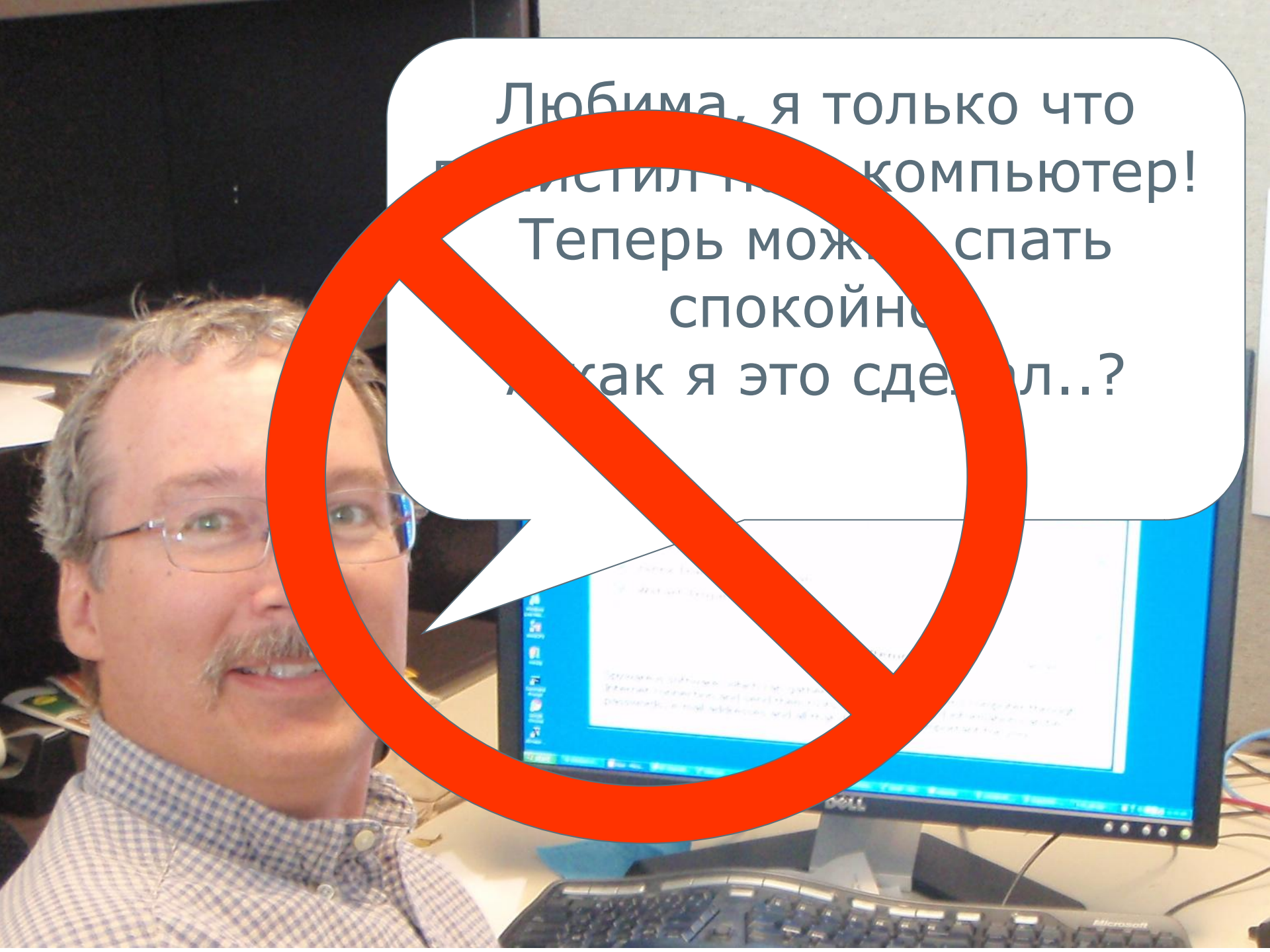
Full system cleanup

Хорошая
программа! С ее
помощью я вылечу
свой компьютер!

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gathered information can be passwords, e-mail addresses and all that data, which is important for you.

Remove all

Cancel



Любима, я только что
успел установить компьютер!
Теперь можно спать
спокойно
как я это сделаю..?



- **Домашние пользователи**
 - Дать родителям **контроль**
 - Ограничить **доступ к любому контенту (см. Фантазии правительства)**
 - Защитить от **фишинга**
 - **К9** для домашних пользователей
 - Заработать на **рекламе**
 - А есть еще **школы** и пр. учебные заведения
 - Сделать интернет **безопасным**



K9 Web Protection

from **BlueCoat**



■ **Корпоративные клиенты**

- Дать возможность **контроля** по любому типу контента
- Защитить от **вирусов и зловредов** на уровне провайдера
- **Блокировать нелегитимные** подключения
- Предоставить **отчеты**
- Защитить от **утечки** данных
- Ускорить необходимые бизнесу **приложения**
- Заработать на **Рекламе**

■ **Сделать интернет инструментом для бизнеса**

■ **Экономия на трафике**



Они используют BlueCoat



TeliaSonera



at&t

true



С почтой надо работать, а не разгребать



Drops > 9 mm become unstable and break apart due to aerodynamic pressure

$$VF_g = \frac{g\rho_p\pi d^3}{6}$$

Force of Gravity

$$F_f = 3\pi d\mu V$$

Force of Friction

$$V_t = \frac{\rho_p g d^2}{18\mu}$$

Stokes Law

$$V_s = \frac{2}{9} \frac{(\rho_p - \rho_f)}{\mu} g R^2$$

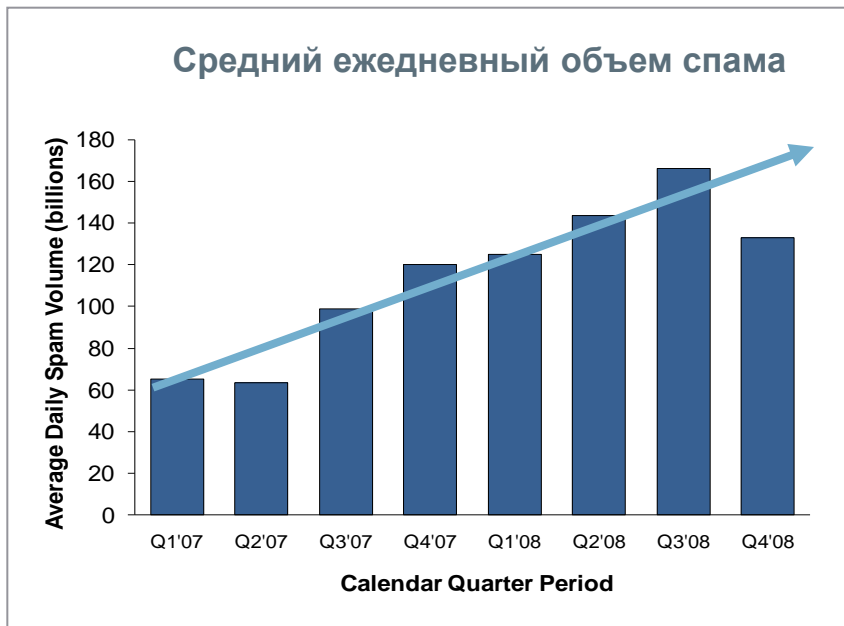
V_s is the particles' settling velocity (m/s)
(vertically downwards if $\rho_p > \rho_f$, upwards if $\rho_p < \rho_f$)
 g is the gravitational acceleration (m/s^2)
 ρ_p is the mass density of the particles (kg/m^3)
 ρ_f is the mass density of the fluid (kg/m^3)

Drops < 1 mm experience little or no distortion from friction or aerodynamic variables



Больше спама

- Ежедневный объем спама увеличивается каждый год вдвое
- Достигло 180 млрд. сообщений в день



Больше спамеров

- Больше спамеров рассылают спам с узлов, принадлежащим ботнетам
- Увеличивается сложность malware



Inbound Security



- Объем спама
- Направленные атаки
- Смешанные атаки
- Мошенничество

DLP/ Encryption



- Требования секретности
- Государственные регуляторы
- PCI
- ISO
- Потери данных
- Кража конфиденциальных данных

Архивация



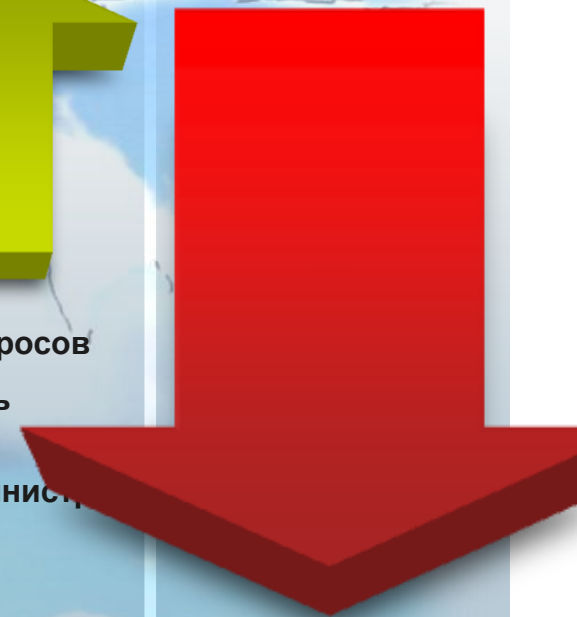
- Число запросов
- Переполнение почтовых серверов
- Соответствие требованиям
- Доступность информации

Поиск



- Число запросов
- Сложность запросов
- Цена администрирования

Бюджет

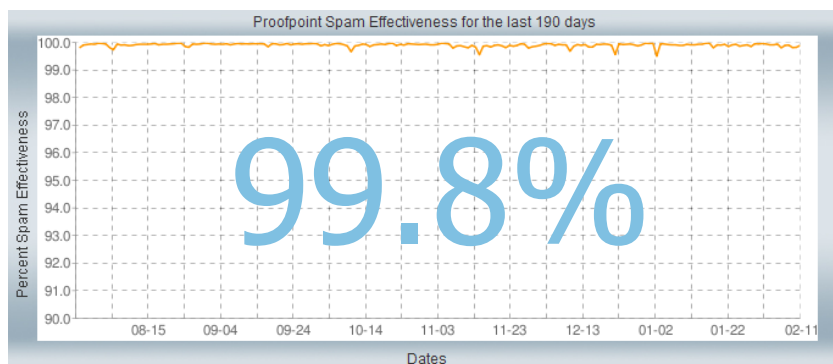


Появление новых угроз, рисков и нормативов требуют нового подхода



Надежность

- 99.999% доступность сервиса



> Точность

99% отсеивание спама

100% контроль вирусов

> Скорость и производительность

Доли секунды задержки в доставке
от 300,000 сообщений/час до бесконечности
от 10,000 конкурентных соединений
до 20 секунд любой поиск по запросу в архиве





- Обеспечить защиту от **спама** почти на 100%
- Обеспечить возможность **архивации почты** на оборудовании провайдера
- **Гарантировать** пересылку больших файлов
- Не уронить свой имидж – **определить ботнеты** внутри сети
- **Электронная почта должна ускорять бизнес, а не останавливать его**

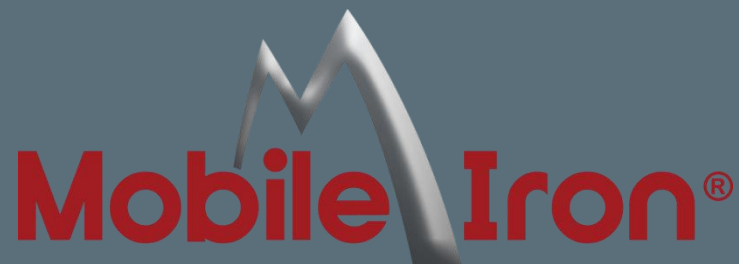
■ **Экономия на трафике**





- Apple выбрал Proofpoint для защиты более 3.3 млн. пользователей их сервиса для защиты от спама и вирусов.
- Дополнительные сведения:
 - b. Proofpoint был на 4-8% эффективнее конкурентов
 - d. Эффективнее защищал от фишинг атак
 - e. Лучше масштабировался
 - f. Фильтрация исходящей почты = отсутствие исходящего спама

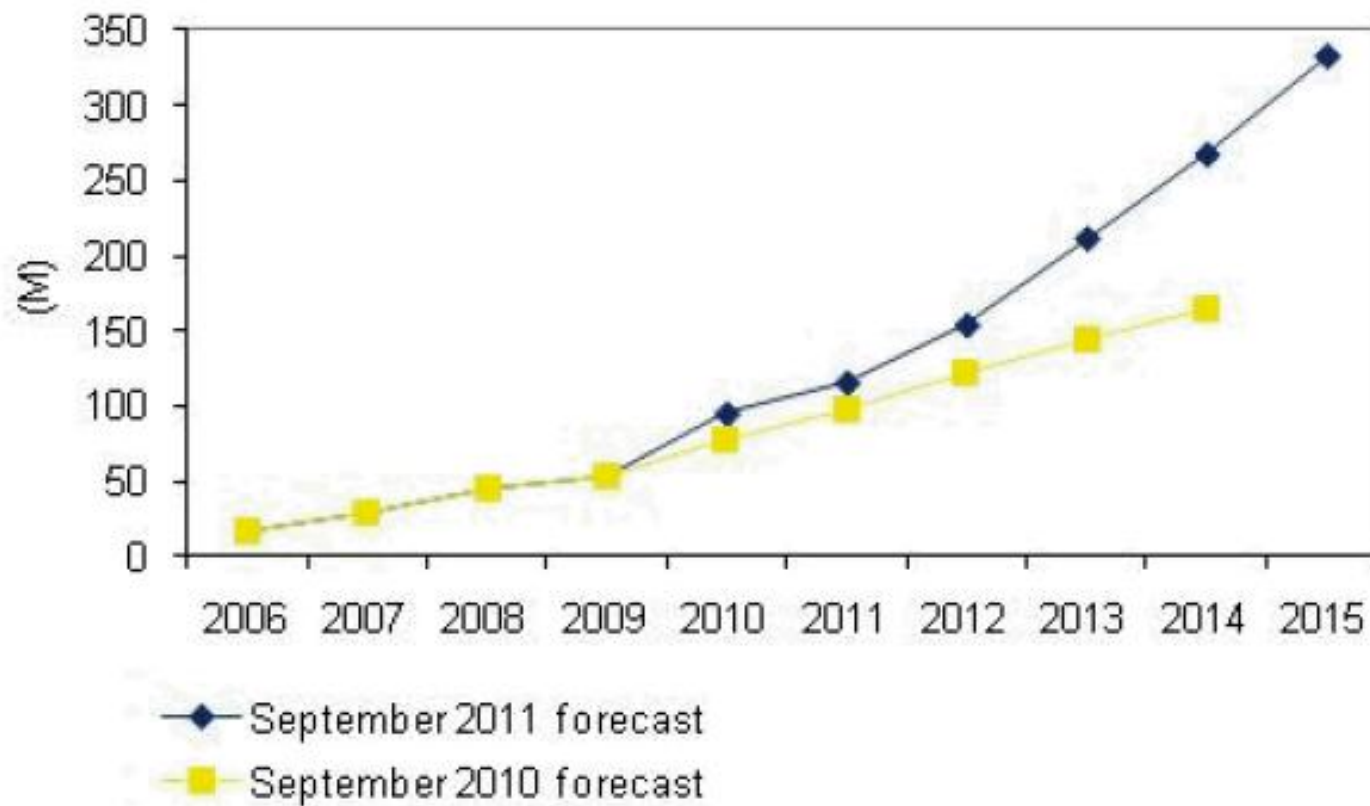




Мобильность клиентов может быть безопасной



Worldwide Business Use Smartphone Shipments, 2006–2015: Comparison of September 2010 and September 2011 Forecasts



Source: IDC, September 2011



[Please help, I've lost my iPad - FlyerTalk Forums](#)

[www.flyertalk.com](#) > ... > [Delta SkyMiles](#) - Перекласти цю сторінку

15 Jan 2012 – Half asleep from a redevye on **my** previous flight, I left **my** seatback of seat 3A on 1/13 on DL 5256 from ATL to CAK. Tracking th

[Lost iPad: Apple Support Communities](#)

<https://discussions.apple.com/thread/2736260?start=0&tstart...> - США

11 Aug 2011 – **I've lost my iPad** in a London taxi and would like to kn
can remotely deactivate the iPad. The iPad has 3G, however, the 3G ..

[I've lost my Ipad, how can I find it...: Apple Support Communities](#) -

[Lost all the sound on my iPad game apps: Apple Support ...](#) - 26 6

[TS1741 I've lost my apple tv remote can...: Apple Support ...](#) - 2 6e

[I've lost my iPad. Is there a way...: Apple Support Communities](#) - 1

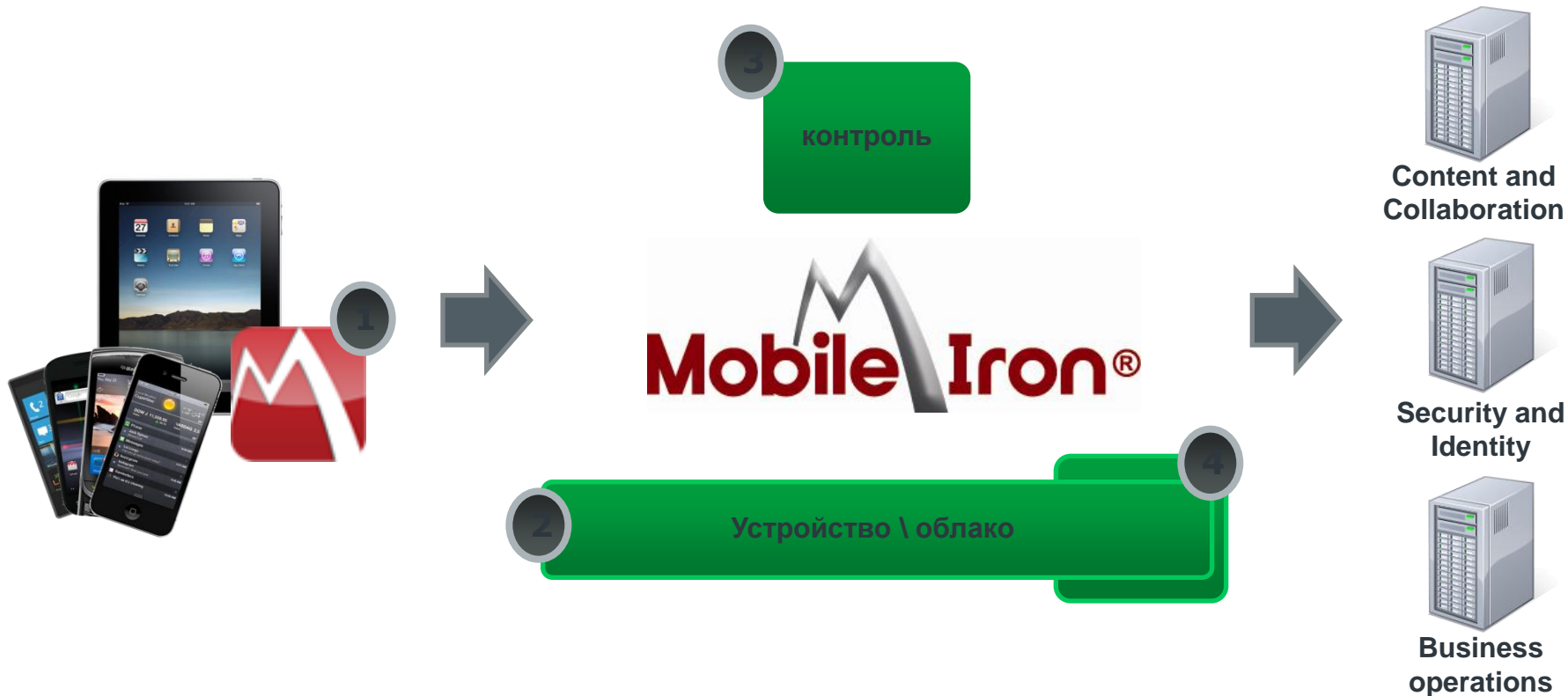
Інші результати з домену [discussions.apple.com](#) »

Forecast по проблемам для ИБ и ИТ ☺





- **Учет устройств и управление ими**
- **Конфигурация устройств**
- **Политика шифрования (телефон, карта памяти)**
- **Блокировка безопасности (фотокамера, карта памяти, Bluetooth, Wi-Fi)**
- **Принудительное использование паролей**
- **Удаленная блокировка и стирание данных**
- **Самообслуживание конечных пользователей**
- **Уйти от BlackBerry ☺**



1

Клиент

Secure app storefront
Posture monitor (jailbreak)
Enforcement

2

Multi-OS ядро (HW/cloud)

инвентаризация
политики
безопасность
приложения
уведомления

3

Access control

Allow/block email
Allow/block apps (coming)
Automated workflow
ActiveSync policy

4

Enterprise integration

Email
AD/LDAP
Certificates
BES
Archival
Custom (Passport API)



- Применение политики **BYOD**
- Защита мобильных **данных**
- **Безопасный** доступ к корпоративным ресурсам
- **Контроль** использования корпоративных устройств
- Применение единой политики **безопасности** для всех устройств
- Борьба с утечкой **данных**
- **Шифрование** почты
- **Ускорить бизнес**





Защитите Ваших клиентов от DDoS

Киев, 23 апреля 2012г.



Результаты опроса 225 компаний в США среди лиц принимающих решения по управлению ИТ за 2011г. :

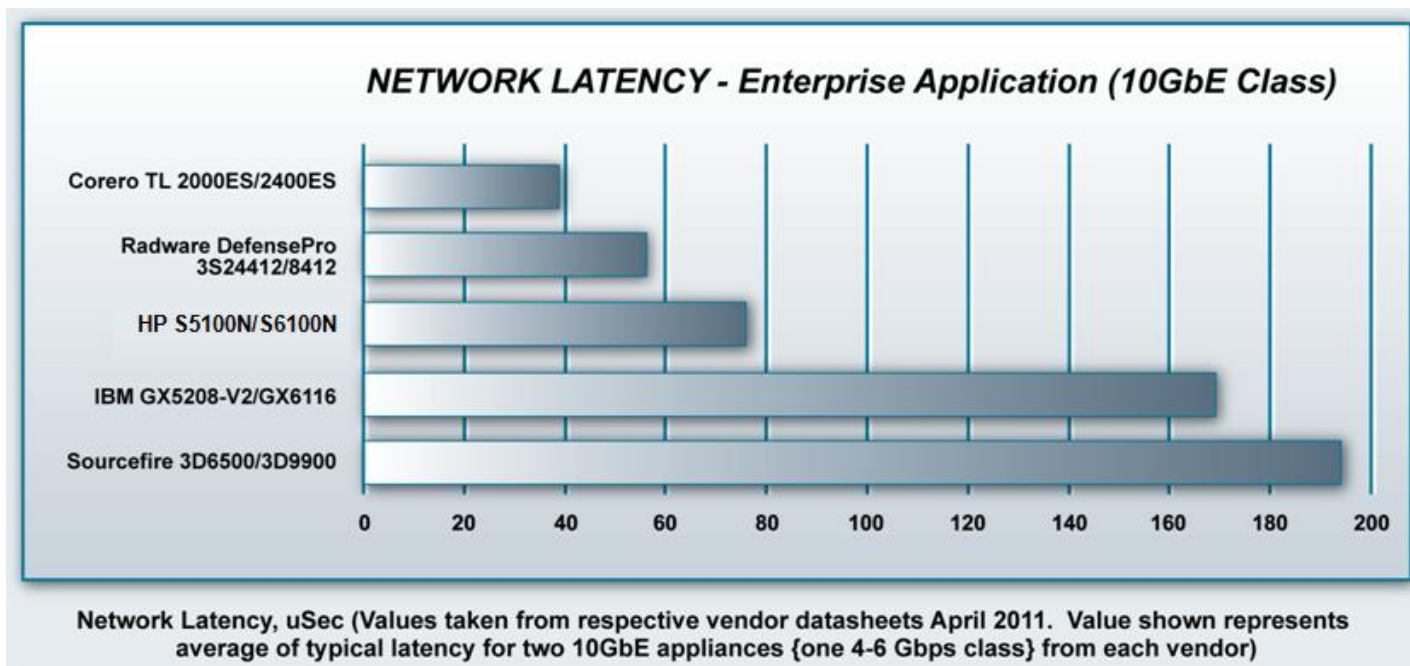
- 78% очень серьёзно обеспокоены DDoS атаками
- 67% ожидают, что частота и масштабы DDoS атак сохраняться либо вырастут в течении следующих 2 лет
- 63% компаний пережили 1 или более атак
- 11% подверглись более 6 атакам
- Опрос проведён Merrill Research

Сколько бы не было “БЕЗОПАСНОСТИ”
внутри Вашей компании, когда Вы
подвержены направленной DDoS атаке
это уже не имеет значения.
Ведь Вы в оффлайне!





- Самая высокая надежность в отрасли и минимальные задержки
- 64-ядерные процессоры от Tileria
- Защищенная специализированная ОС








- **Защита:** 3DP (DDoS Defense, Firewall и IPS) технологии защиты «в трех измерениях» – активно нейтрализуют как классические атаки сетевого уровня, так и уровня приложений, или же специализированные атаки направленные на «убийство» конкретных сервисов
- **Производительность масштабов провайдера:** самые низкие задержки (<50 микросекунд) и наибольшая пропускная способность (до 20 Гбит на 1 устройство) = проблем со скоростью просто нет
- **Масштабируемость:** до 8 устройств в кластере по технологии ProtectionCluster™ = отказоустойчивость и линейное увеличение мощности, например до 160 Гбит на кластер
- **Надежность:** специализированное «железо» почти без подвижных составляющих, резервным питанием, сроком наработки на отказ 20-30 лет и «zero-power bypass»
- **«Зелёная» архитектура:** 64-ядерные процессоры Tiler, минимальный форм-фактор (1 юнит) и мизерное энергопотребление (<100 Ватт)

Сервис SecureWatch® PLUS



Подготовка 	Бдительность 	Реакция 
<p>Определение четкой политики защиты от DDoS и общей стратегии снижения воздействий атак</p>	<p>Предоставление обновлений ПО и “Protection Pack” сразу по необходимости</p>	<p>Гарантированная доступность экспертизы в режиме 24x7 и оповещение о DDoS атаках</p>
<p>Документирование логической и физической топологии сетевой инфраструктуры Заказчика</p>	<p>Предоставление постоянного анализа защищенности среды основываясь на публикациях новых угроз от Corero</p>	<p>Инициировать процедуры коммуникации и сотрудничества с командой безопасности Заказчика</p>
<p>Бэйслайнинг по протоколам, типам трафика, средней сетевой загрузки и потоков трафика</p>	<p>Предоставление непрерывных функций мониторинга и журналирования</p>	<p>Запустить процедуры по удаленному доступу к системам DDS Заказчика</p>
<p>Разработка безопасной конфигурации удаленного доступа</p>	<p>Еженедельно предоставляются отчеты и анализ происходящих событий</p>	<p>Проанализировать происхождение, критичность и воздействие DDoS атаки</p>
<p>Постоянная доработка и оптимизации для защиты от переменных векторов атак</p>	<p>Мониторинг аппаратной платформы и инцидентов в режиме 24x7 из защищенного Corero SOC</p>	<p>Настройка механизмов защиты для дальнейшего снижения воздействий атаки по необходимости, при изменении вектора атаки</p>
<p>Утверждение процедур коммуникаций и сотрудничества</p>	<p>Оповещение об атаках в режиме 24x7 по оговоренным процедурам</p>	<p>Непрерывная проверка оптимальности настроек по отношению к текущей атаке</p>



Преимущества:

- Интернет канал «очищенный» от трафика атак
- Без потери легитимного трафика
- Заказчик получает не просто устройство, а решение оптимизированное под его инфраструктуру и сервисы
- Весь сервис проводится профессионалами и самим производителем по всему миру 24x7
- Первая линия поддержки, тестирование и локальные консультации проводятся специалистами СВІТ ІТ

Примеры услуг:

- Сервис от «Вашей компании» по защите от DDoS
- Размещение устройства DDS на Вашей площадке и управление им специалистами Заказчика и сервиса SecureWatch



Клиент доволен 😊

