headtechnology
it-security

IronPort – Защита корпоративной электронной почты.

Web-безопасность.

Сергей Дугарёв, руководитель направления IronPort, заместитель директора компании Хедтекнолоджи (Украина), дистрибьютора IronPort Systems

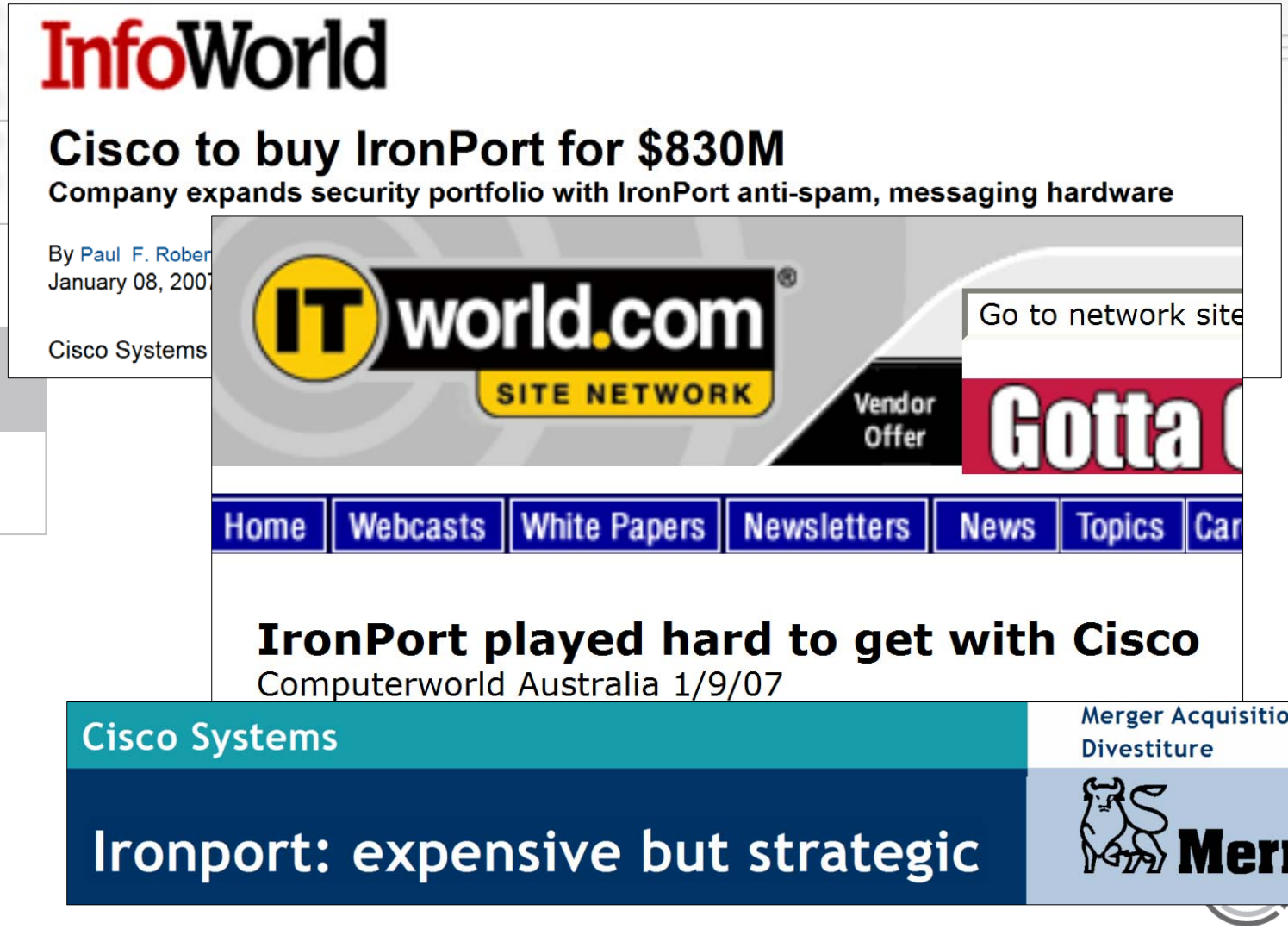
IRONPORT

Решения IronPort для обеспечения безопасности на периметре корпоративной сети.

- Начальная идея: создание быстрейшего и сильнейшего сервера для почтового шлюза;
- Расположение штаб-квартиры IronPort Systems: США, Калифорния, Силиконовая Долина
- Год основания: 2000.

IRONPORT

IronPort – A CISCO Business Unit



Сеть IronPort SenderBase®

Первая и самая большая система репутаций

Глобальный мониторинг почтового и веб трафика

120 000+ сетей
5 000 000 000+ запросов в день
150 параметров
25%+ мирового трафика

…результаты работы

спам, пойманный фильтром репутации

IronPort	**80%**
CipherTrust	50%
BorderWare	40%

Контролирумые сети

IronPort	**120,000**
CipherTrust	4,000
BorderWare	8,000

лидерство по защите от новых вирусов

IronPort	**13 hours***
McAfee, Symantec, Sophos, CA, F-Secure, ...	

** 6/2005 – 6/2006. 175 outbreaks identified. Calculated as publicly published signatures from the listed vendors.*

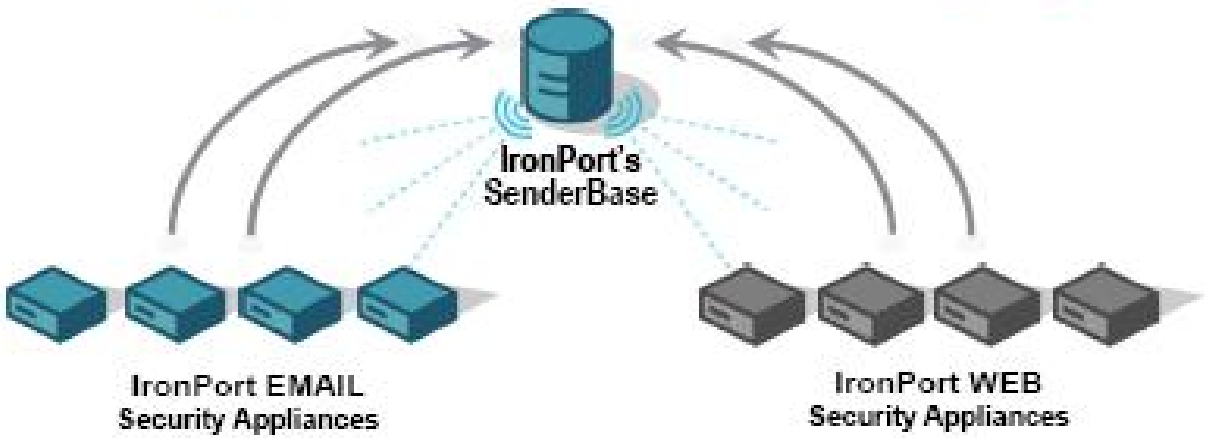
IRONPORT®

Source: www.ciphertrust.com and www.borderware.com, August 6, 2006

Сеть IronPort SenderBase®

Первая и самая большая система репутаций

Комбинированный анализ Web и E-mail трафика



- Просмотр как E-mail, так и Web трафика резко увеличивает вероятность обнаружения
  - - 83% спама & 80% общей почты содержат URLs
  - - Email – это основной вектор распространения Web-based malware

IRONPORT®

Source: www.ciphertrust.com and www.borderware.com, August 6, 2006

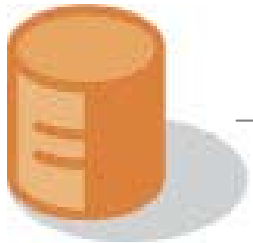
SenderBase®

Данные имеют значение

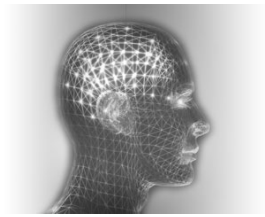
Параметры

- отчеты о жалобах
- Ловушки для спама
- Данные о структуре сообщения
- Глобальные данные
- Списки URL
- Списки скомпрометированных хостов
- Web-”пауки”
- Черные и белые списки IP
- Дополнительные данные

Предотвращение угроз в реальном времени

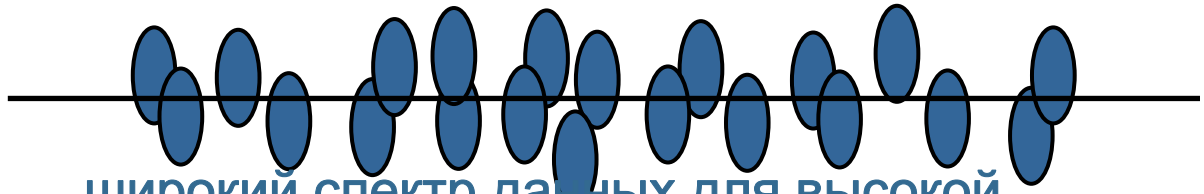


Данные SenderBase



Анализ данных/ моделирование безопасности

Репутация SenderBase от -10 до +10



широкий спектр данных для высокой точности репутации

IRONPORT

Чем подтверждается лидерство в данной области

- Подтверждено аналитиками
  - По результатам анализа компаний: Gartner, Meta, Radicati, IDC, Forrester, Bloor
- Подтверждено клиентами
  - Обслуживание 52 из 100 крупнейших компаний в мире
  - Обслуживание 12 из 15 крупнейших провайдеров
  - Обслуживание US Armed Forces
- Подтверждено технологиями
  - Первые с собственным разработанным высокопроизводительным MTA
  - Первые с Репутационными фильтрами
  - Первые с Антивирусными фильтрами
- Подтверждено во всем мире
  - Присутствие в 25 странах, более 600+ партнеров
  - Структуры IronPort работают в более чем 75+ странах

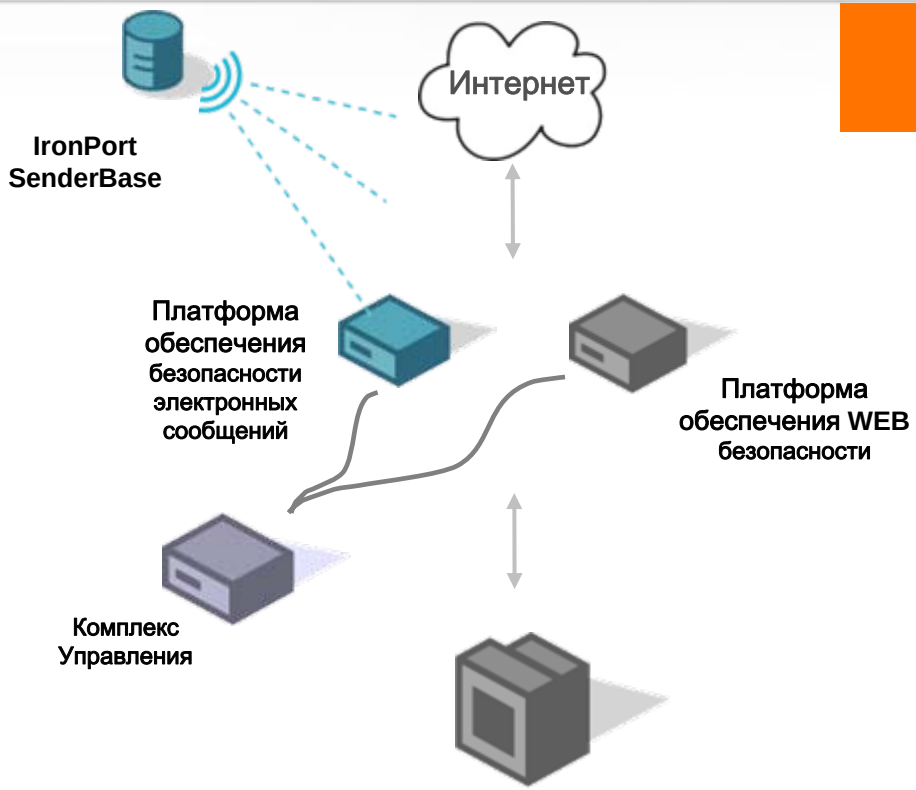
IRONPORT

Некоторые клиенты IronPort в Украине и в России

IRONPORT

Клиенты-провайдеры

Продукты IronPort



Устройства обеспечения безопасности электронной почты IronPort

- Высокопроизводительные устройства безопасности электронной почты, защищающие от спама и вирусов, позволяющие создавать политики для почты

IronPort X1050 (X1060)

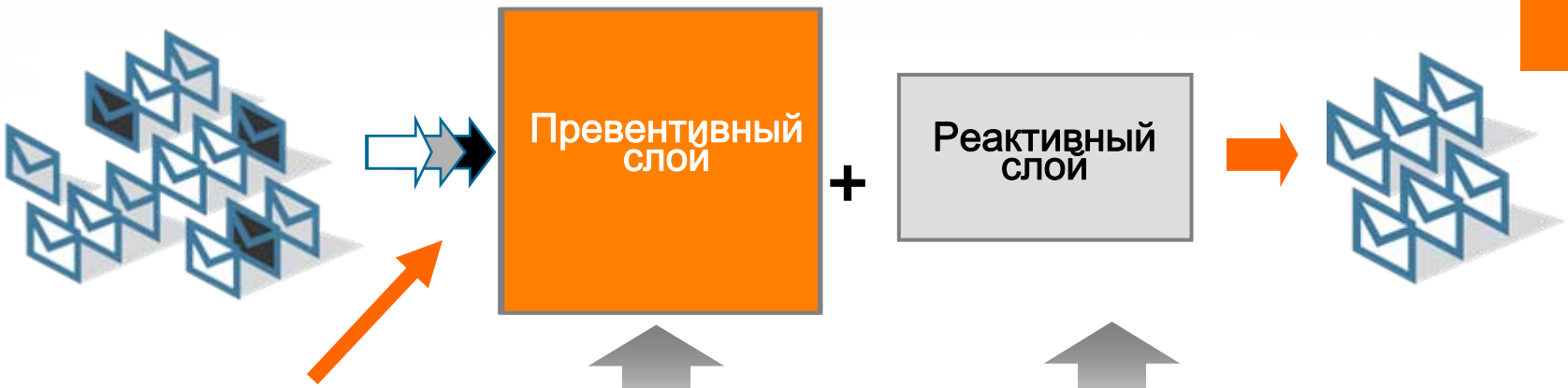
IronPort C350/C650 (C360/C660)

IronPort C150 (C160)

IRONPORT

Многоуровневая безопасность

Превентивная + реактивная = тщательная защита



Блокирует около 80% спама прямо на шлюзе!

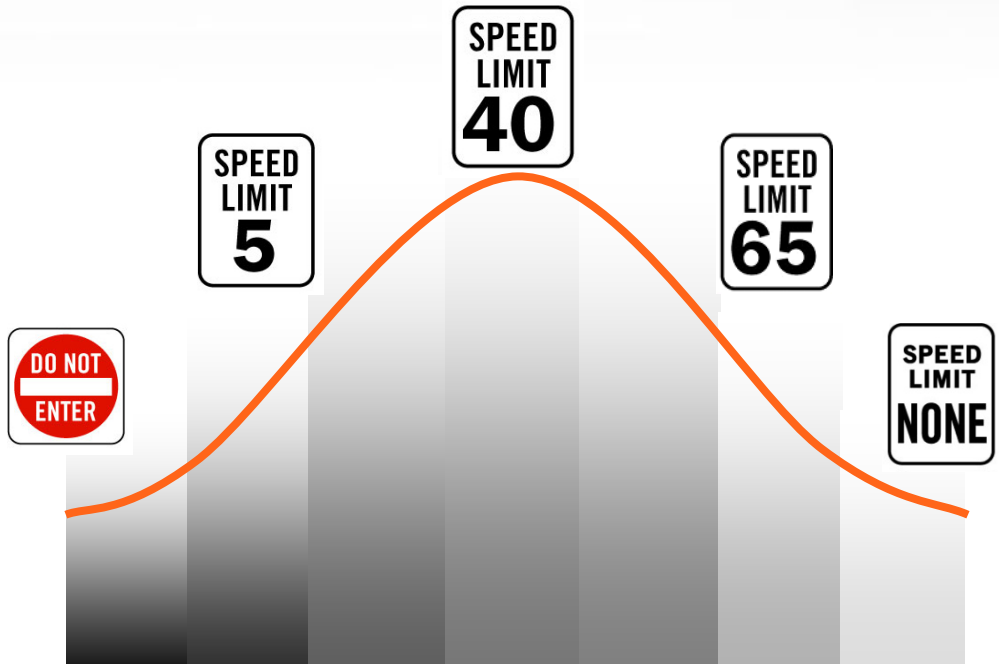
Превентивный слой	Реактивный слой
Немедленная реакция на угрозы	Адаптируется со временем
Высокая производительность	С большим объемом вычислений
Жесткий внешний слой	Мелкозернистый внутренний слой
Блокировка или ограничение скорости	Удаляйте или отправляйте в карантин

IronPort Reputation Filters останавливают более 80% нежелательной почты до ее прихода…

- IronPort использует репутацию для применения политик
- Изощренный ответ изощренным угрозам

IRONPORT

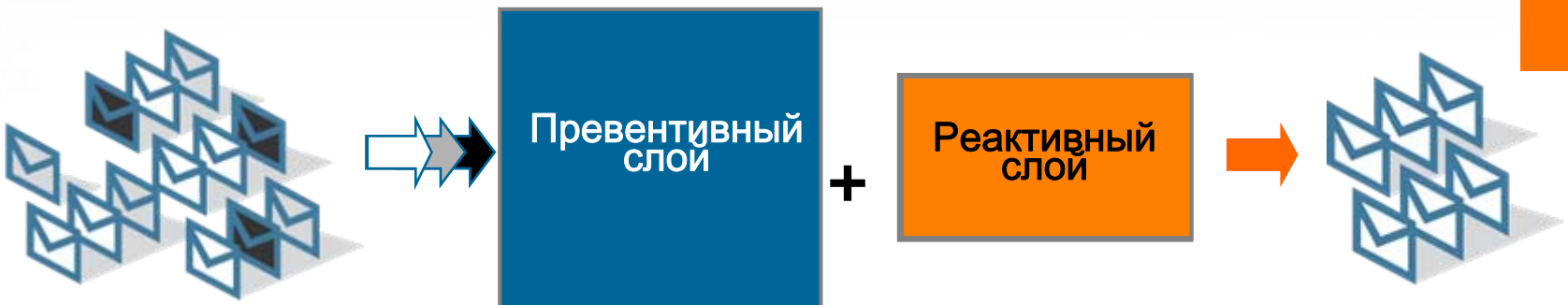
Ограничение объёма и скорости почтового трафика соответственно репутации отправителя



- гораздо больше, чем только черные и белые списки
- в режиме реального времени
- предустановленные политики применяются автомати

Многоуровневая безопасность

Превентивная + реактивная = тщательная защита



Немедленная реакция на угрозы	Адаптируется со временем
Высокая производительность	С большим объемом вычислений
Жесткий внешний слой	Мелкозернистый внутренний слой
Блокировка или ограничение скорости	Удаляйте или отправляйте в карантин

Архитектура IronPort
для многоуровневой безопасности электронной почты

IronPort

Многоуровневая защита от спама

Лучшая в своем классе

IronPort's Reputation Filters (RF) – внешний слой защиты
IronPort Anti-Spam (AS) – защищает от широкого спектра угроз – спам, phishing, fraud

IRONPORT

IronPort Анти-Спам

Обзор прессы

InfoWorld

2007 Технология года: Лучший Анти-Спам

Январь 2007

Протестированные конкуренты :
Symantec, Microsoft, Mirapoint, ProofPoint

“легкая установка”

“прекрасная спам фильтрация”

“нет необходимости дополнительных настроек”

“минимальный уровень ложных срабатываний”

info security

Победитель номинации лучший анти-спам

Декабрь 2006

Протестированные конкуренты:
CipherTrust, Borderware, Sophos, SonicWall

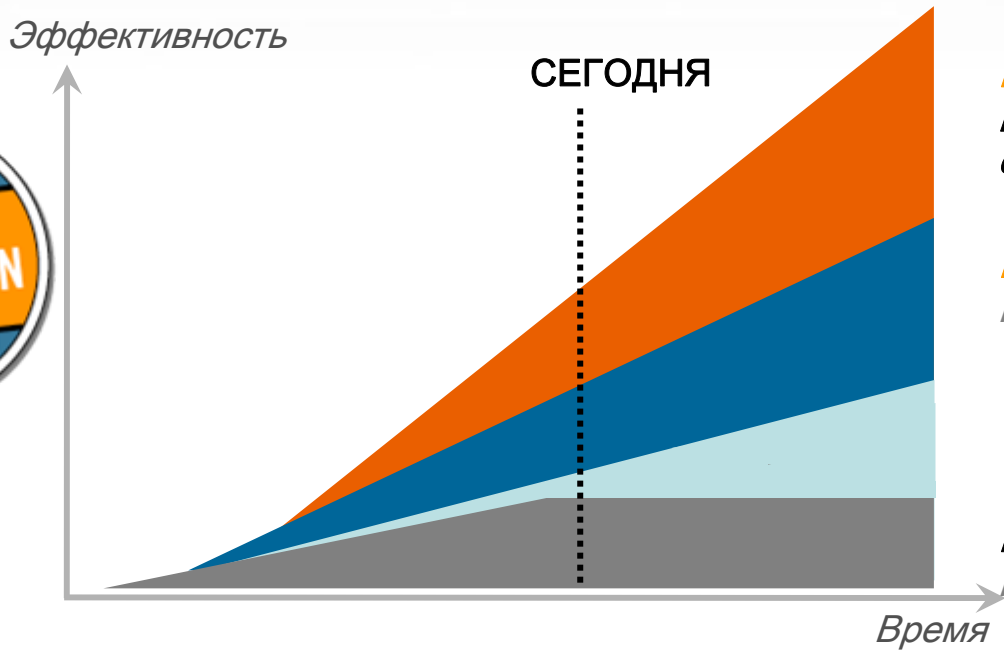
“Превосходство IronPort . . . видится очень ясно”

“Мы не потеряли ни одного легитимного сообщения”

“...(IronPort) абсолютный победитель тестов”

IRONPORT

IronPort AntiSpam
разширяем реактивную защиту



Куда? **Репутация Web**
Куда Вы попадете, перейдя по ссылке?

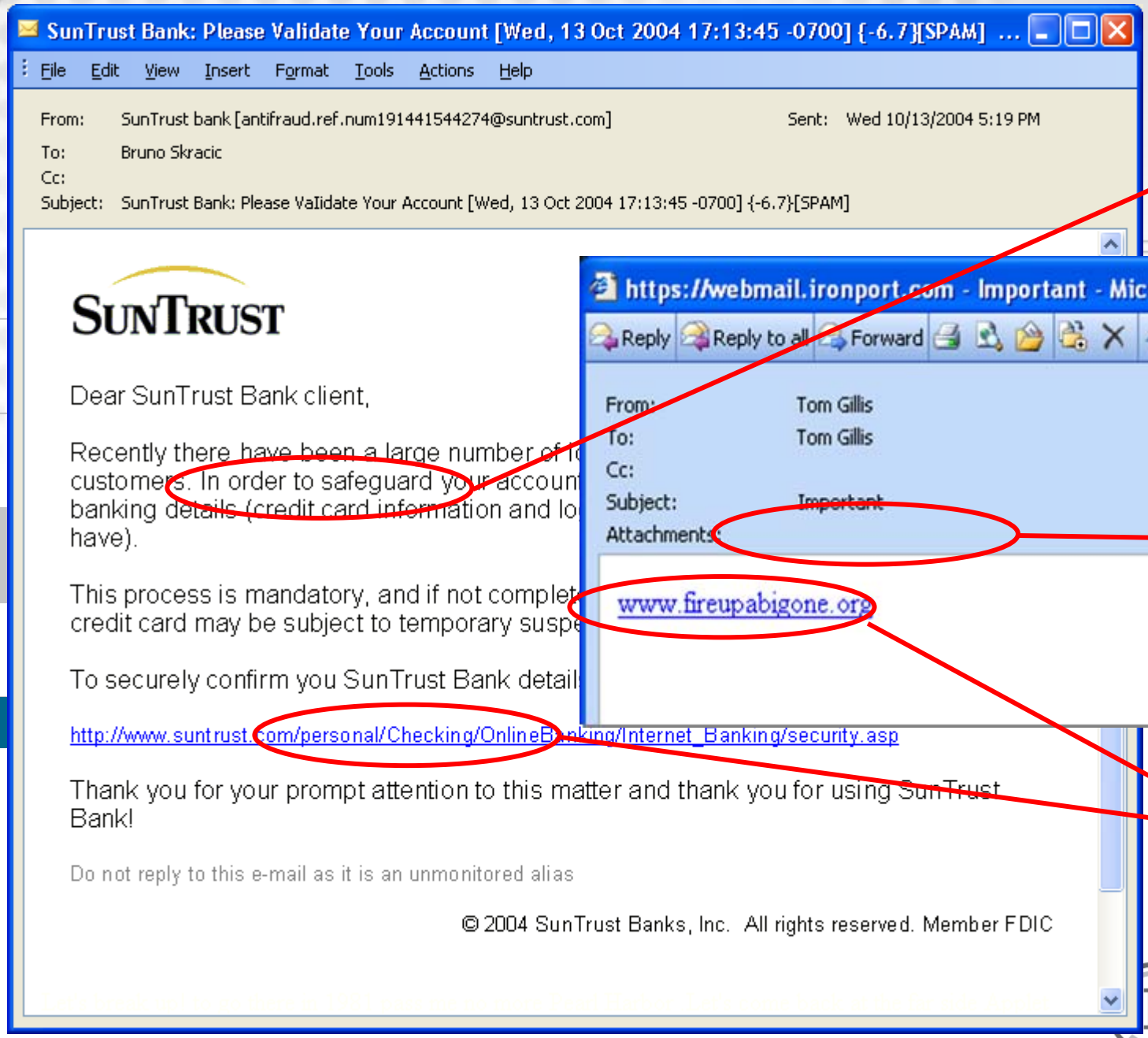
Кто? Репутация почты
Кто посылает Вам это письмо?

Что? Содержание письма
Что содержит в себе письмо?

Как? Структура письма
Как составлено сообщение?

- Использование только контентных фильтров недостаточно
- Репутационная система улучшает защиту
- Борьба с новыми угрозами требует анализа веб-репутации

IRONPORT



нет плохого контента

нет вложений

URL

IRONPORT

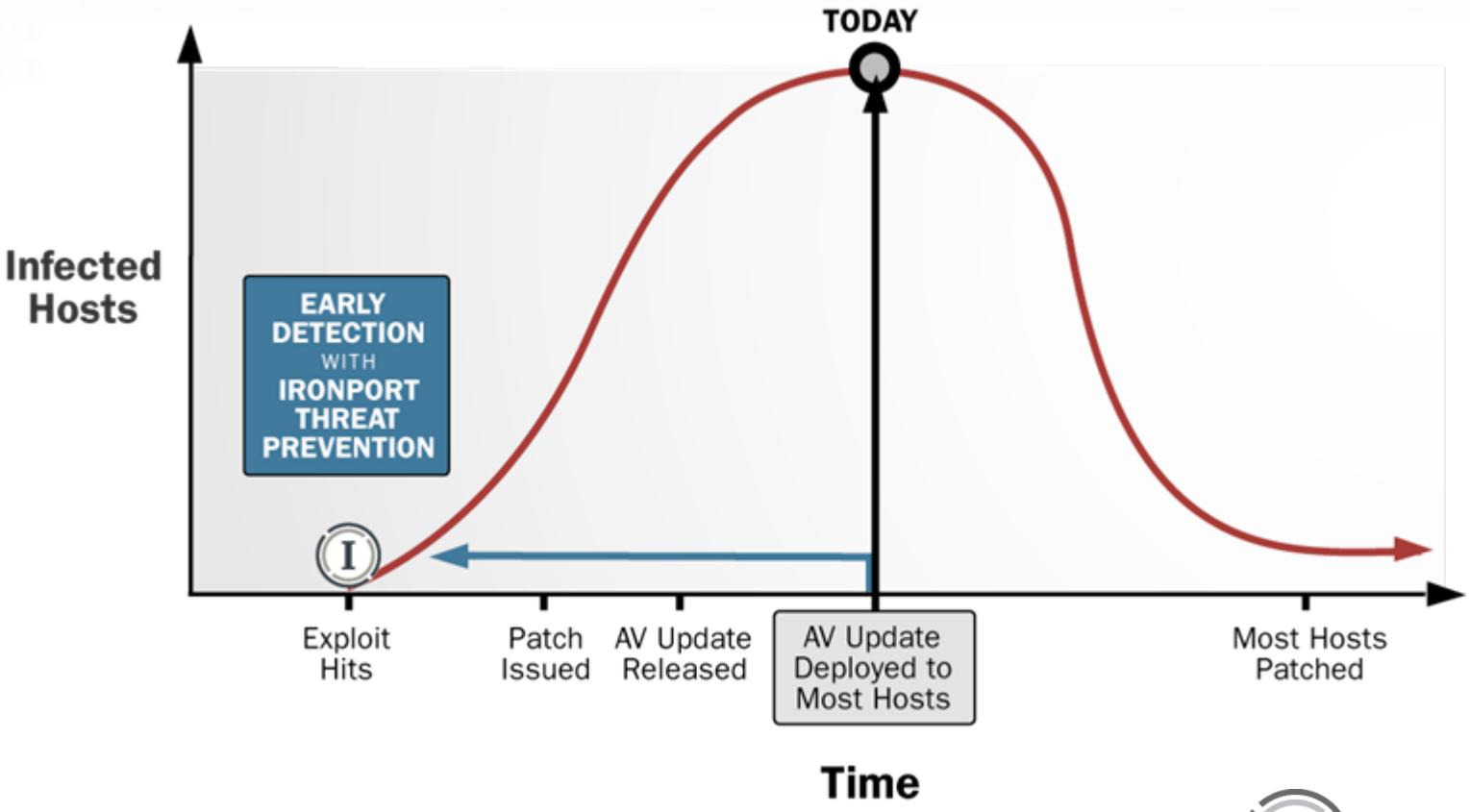
Ведущая, многоуровневая защита от вирусов

IronPort's Virus Outbreak Filters (VOF) – остановите вирус за 14 часов до появления сигнатур
Sophos AntiVirus (AV) – основанное на сигнатурах решение с превосходной точностью

IRONPORT

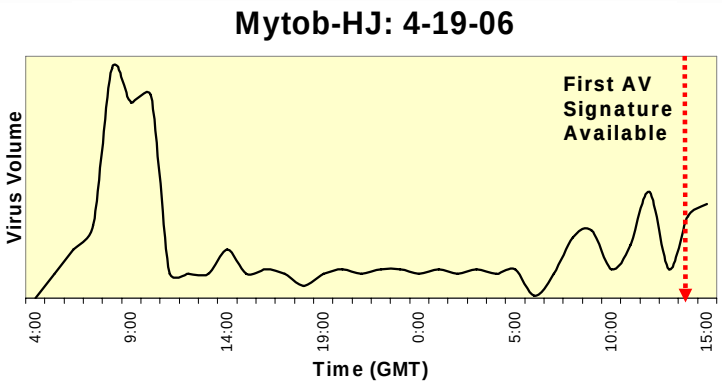
IronPort Outbreak Filters

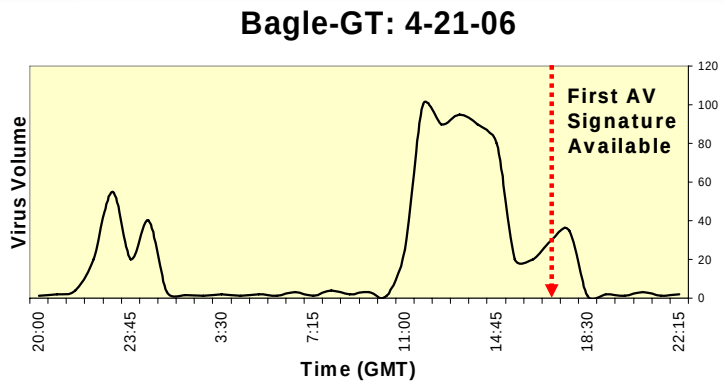
Минимизируйте интервал времени реакции!

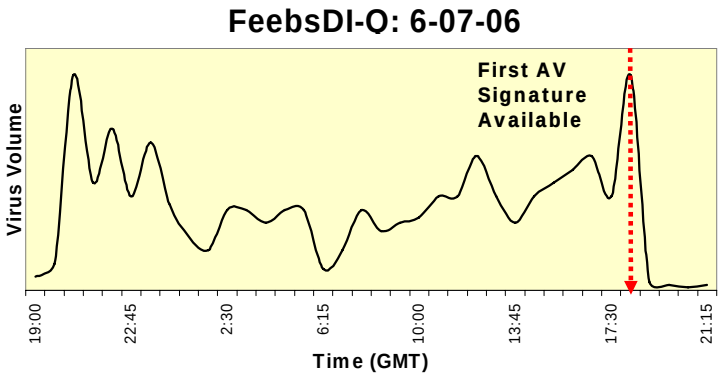


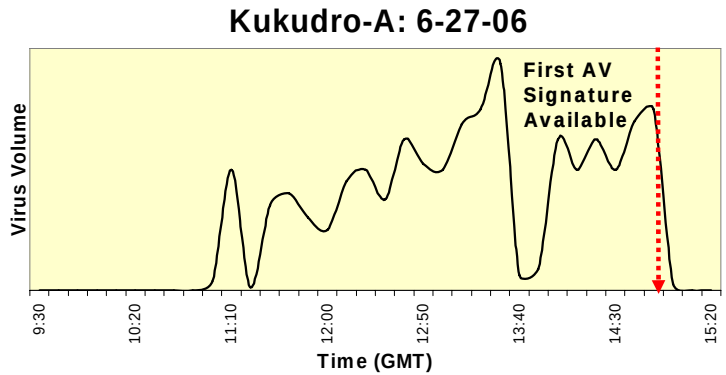
IRONPORT

Обычные антивирусы реагируют недостаточно быстро . . .









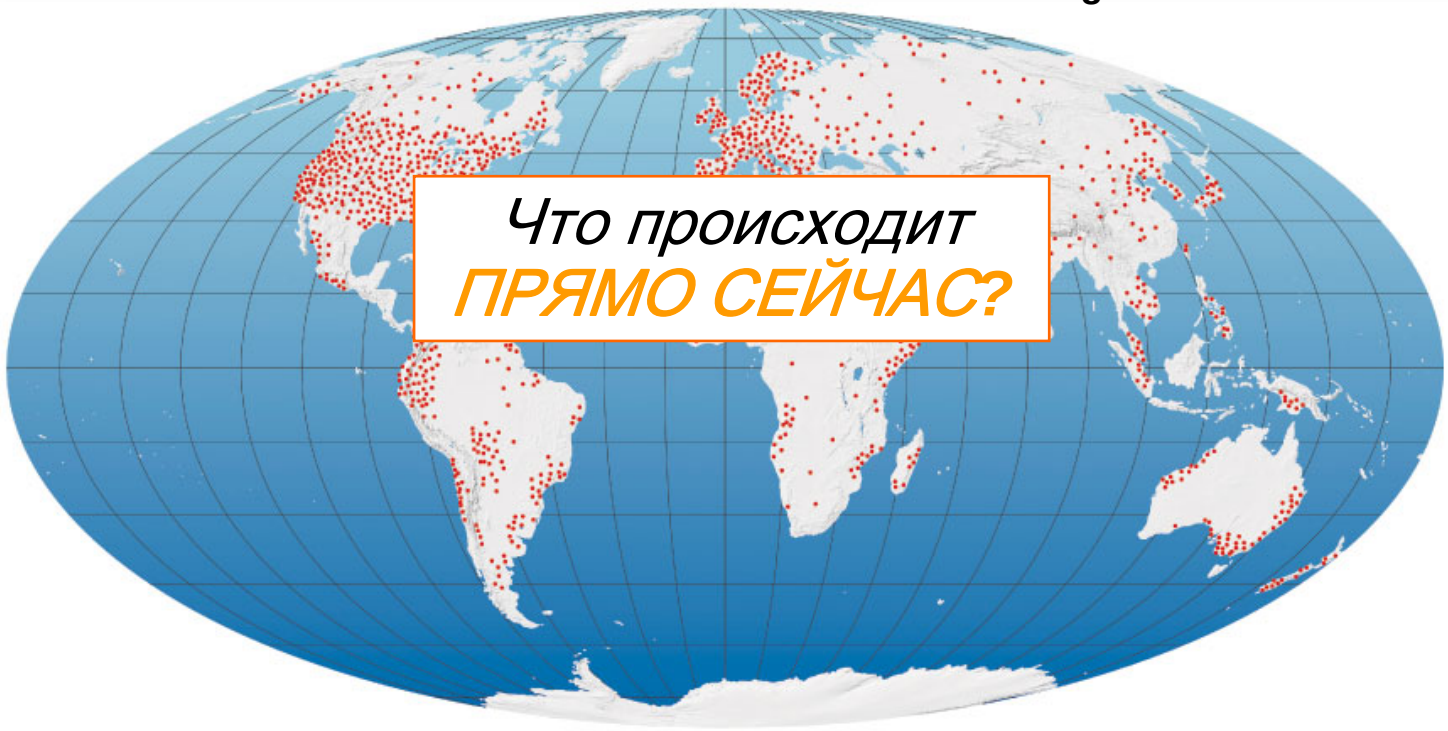
Для разработки и выпуска сигнатур требуется время…

IRONPORT

IronPort SenderBase® Network

Первая, *самая большая, лучшая система репутаций*

Global Email and Web Traffic Monitoring

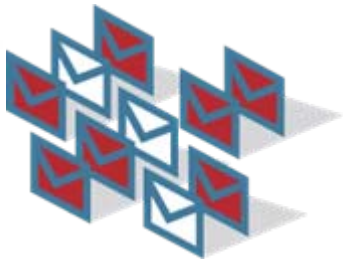


Охвачено **более 100,000** комп.сетей
Анализируются **более 20M IP адресов**
Обзор **более 25%** трафика email
Анализируется **более 110** параметров

IRONPORT

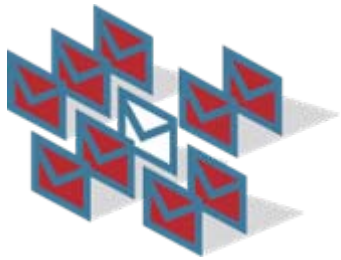
Как работает Virus Outbreak Filters

Динамический карантин в действии



T = 0

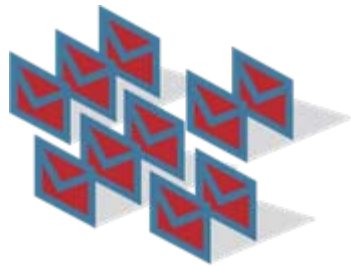
– zip (exe)



T = 5 минут

-zip (exe)

- от 50 до 55 КБайт



T = 10 минут

–zip (exe)

– от 50 до 55 КБайт

– в названии “Price”

Сообщения сканируются и удаляются

T = 8 часов

– Отпустить сообщения, если произошло обновление сигнатур

превентивная защита (VOF)

реактивная защита (Sophos)

IRONPORT

Преимущество Virus Outbreak Filters

Название вируса	Дата	Описание вируса	Задержка сигнатур (hh:mm)
Troj/Dloadr-BCK	7/24/07	Устанавливает вредоносное ПО.	10:06
Troj/Yar-A	5/24/07	Рекламное сообщение, предлагающее трейлер фильма «Пираты Карибского моря 3“. Загружает шпионское ПО.	3:20
Trojan.Dropper	5/10/07	Троян, который пытается загрузить злонамеренный код.	10:40
W32.Virut!dr	4/12/07	Спам сообщение, предлагающее получателю открыть зараженное приложение, обозначенное как “document.txt.exe” и “video.zip”.	31:12
Troj/DwnLdr-GFN	3/4/07	Устанавливает скрытый канал связи через протокол HTTP, обеспечивая обход фаервола.	17:31
W32/WowPWS-AU	3/3/07	Червь, рассылающий массированный спам с темой "Chinese test missile obliterates satellite!“. Предлагает получателю открыть зараженный файл.	6:51
Troj_Agent.JAW	1/14/07	Спам сообщение с вложением PDF формата, при попытке открыть вложение устанавливается тайный канал для доступа хакерам.	20:08

Среднее время задержки.....более 13 часов*

*Всего блокировано вспышек * 175*

*Общее время защиты *.....более 94 дней*

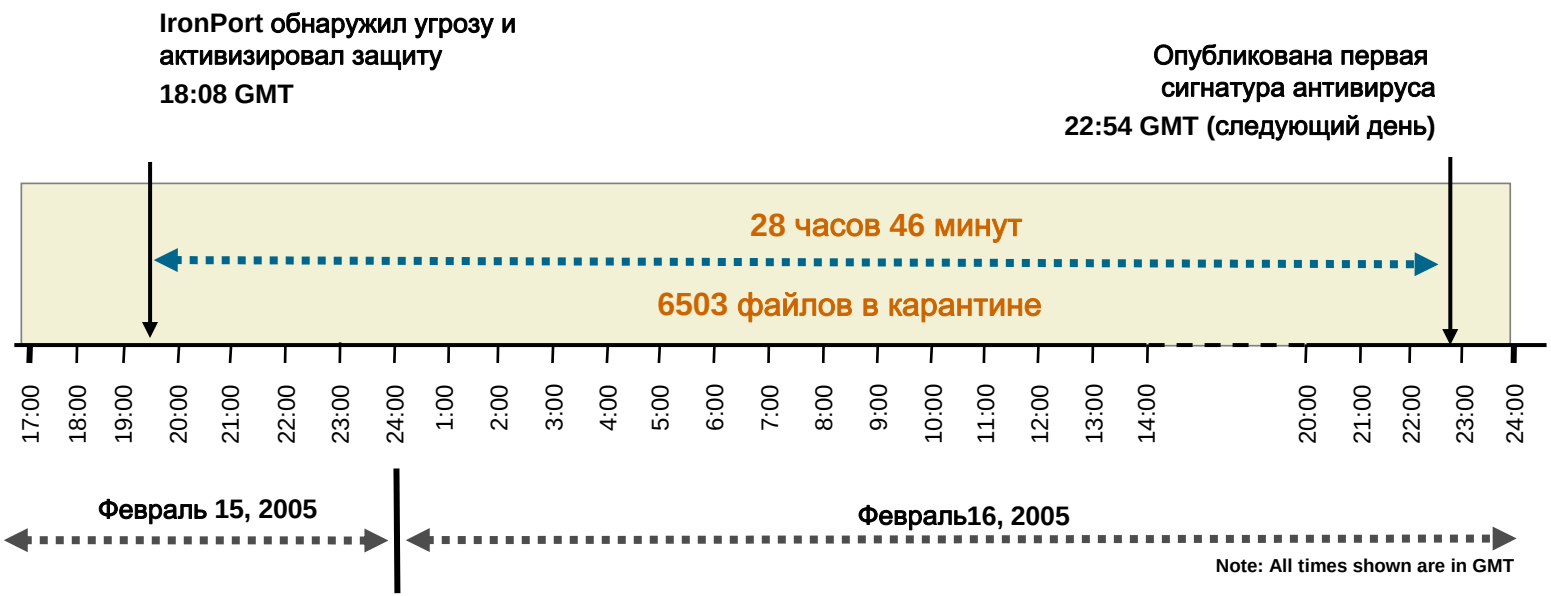
IRONPORT

IronPort Outbreak Filters

Защита компании G2000 от MyDoom.BB

Вариант MyDoom—MyDoom.BB (Февраль 15, 2005)

Компания G2000 защищена IronPort's Virus Outbreak Filters



$65K сохранено@ $200/на рабочее место, 5% заражено

IronPort Virus Outbreak Filter успешное применение

ACS

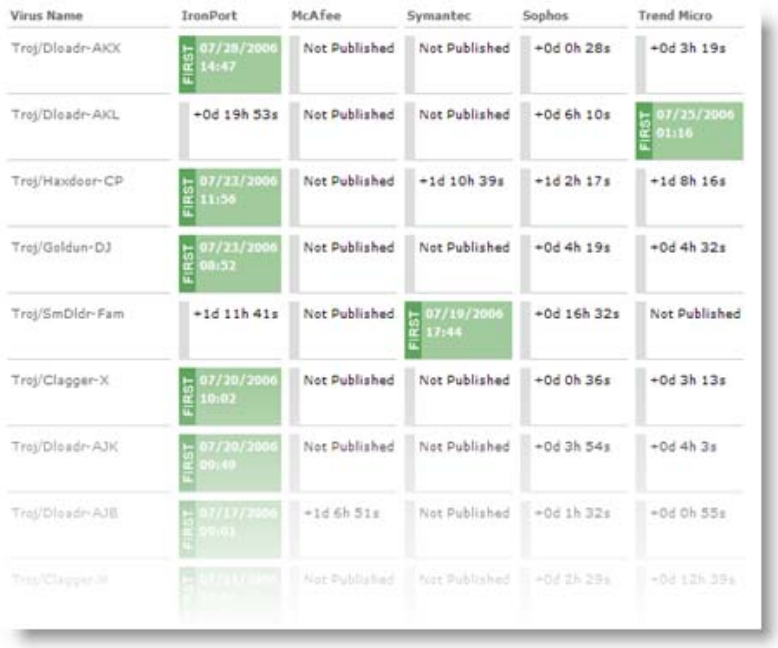
“мы сохранили $1.2M в течении 7 месяцев с помощью Outbreak Filters”

“С Outbreak Filters мы не пропустили ни одной атаки!”

AIR FRANCE

JOHNS HOPKINS UNIVERSITY

“было обнаружено 24,000 сообщений с вирусами за 9 месяцев”



Virus Name	IronPort	McAfee	Symantec	Sophos	Trend Micro
Troj/Dloadr-AKX	FIRST 07/28/2006 14:47	Not Published	Not Published	+0d 0h 28s	+0d 3h 19s
Troj/Dloadr-AKL	+0d 19h 53s	Not Published	Not Published	+0d 6h 10s	FIRST 07/25/2006 01:16
Troj/Haxdoor-CP	FIRST 07/23/2006 11:56	Not Published	+1d 10h 39s	+1d 2h 17s	+1d 8h 16s
Troj/Goldun-DJ	FIRST 07/23/2006 08:52	Not Published	Not Published	+0d 4h 19s	+0d 4h 32s
Troj/SmDldr-Fam	+1d 11h 41s	Not Published	FIRST 07/19/2006 17:44	+0d 16h 32s	Not Published
Troj/Clagger-X	FIRST 07/20/2006 10:02	Not Published	Not Published	+0d 0h 36s	+0d 3h 13s
Troj/Dloadr-AJK	FIRST 07/20/2006 09:49	Not Published	Not Published	+0d 3h 54s	+0d 4h 3s
Troj/Dloadr-AJB	FIRST 07/17/2006 09:03	+1d 6h 51s	Not Published	+0d 1h 32s	+0d 0h 55s
Troj/Clagger-M	[illegible]	Not Published	Not Published	+0d 2h 29s	+0d 12h 39s

Отчеты о Virus Outbreak Filters

Ежедневно публикуются на:
http://www.ironport.com/toc

**Предполагается, что открыто 20% зараженый сообщений и $500 за восстановление каждого зараженного компьютера.*

IronPort. Сканирование контента.

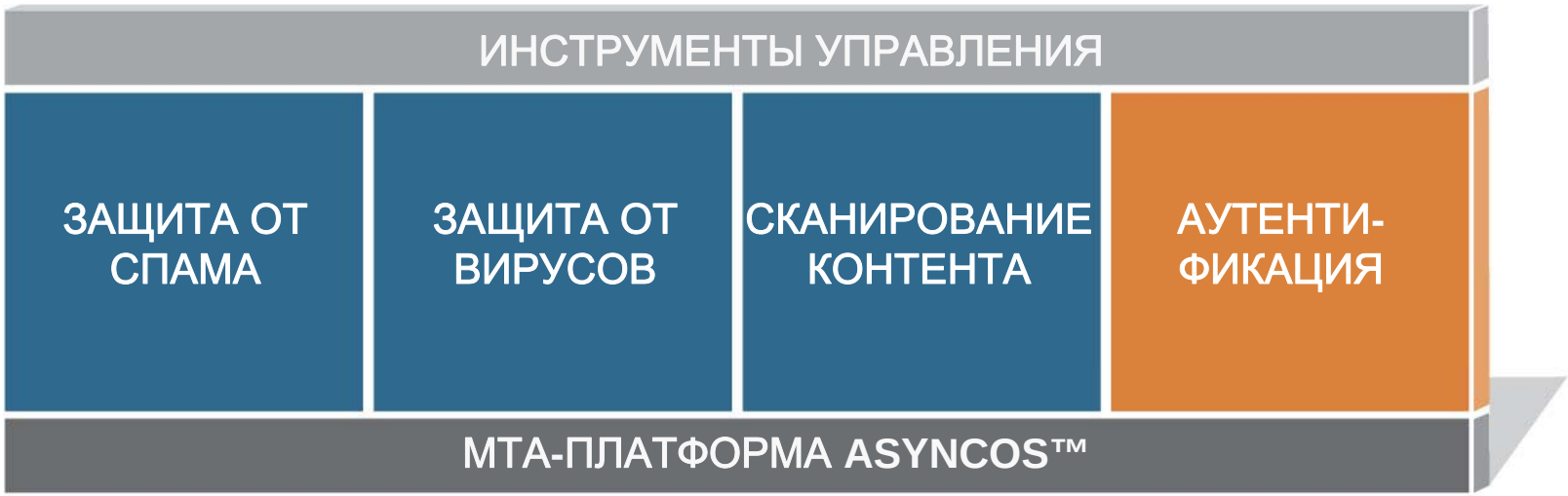
Фильтрация входящих / исходящих сообщений для соответствия требованиям

- **Применение гибких политик** от блокирования вложений до более сложных корпоративных политик
- **Гибкие решения и шифрование** обеспечивают защищенность коммуникации

IRONPORT

Email идентификация

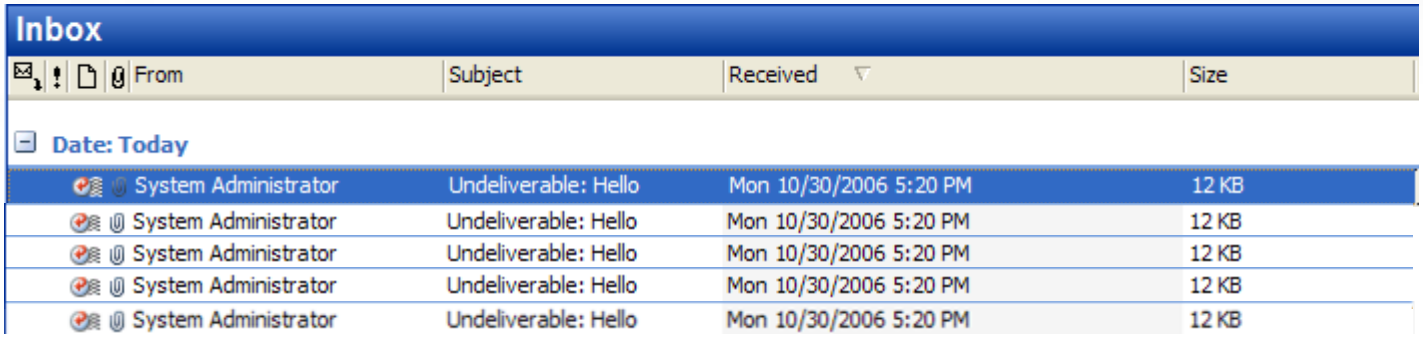
Высокая защищенность и защита подлинности



- **DomainKey Signing** – устанавливает и защищает вашу идентичность в интернете
- **IronPort Bounce Verification** – защищает от bounce (уведомление об ошибке при доставке) атак
- **Directory Harvest Attack Prevention** –блокирует попытки массированного сканирования ваших адресов электронной почты

IRONPORT

Проблема обратных сообщений



Inbox

From	Subject	Received	Size
Date: Today			
System Administrator	Undeliverable: Hello	Mon 10/30/2006 5:20 PM	12 KB
System Administrator	Undeliverable: Hello	Mon 10/30/2006 5:20 PM	12 KB
System Administrator	Undeliverable: Hello	Mon 10/30/2006 5:20 PM	12 KB
System Administrator	Undeliverable: Hello	Mon 10/30/2006 5:20 PM	12 KB
System Administrator	Undeliverable: Hello	Mon 10/30/2006 5:20 PM	12 KB

From: System Administrator
Sent: Tuesday, March 16, 2004 8:58 AM
To: doryan@unforgettable.com
Subject: Undeliverable:ÞÉ ØÓ - çîëîòàÿ ôîðìóëà ñòðîéíîñòè.

Your message did not reach some or all of the intended recipients.

Subject: ЮЙ ШУ - золотая формула стройности.
Sent: 3/16/2004 8:32 AM

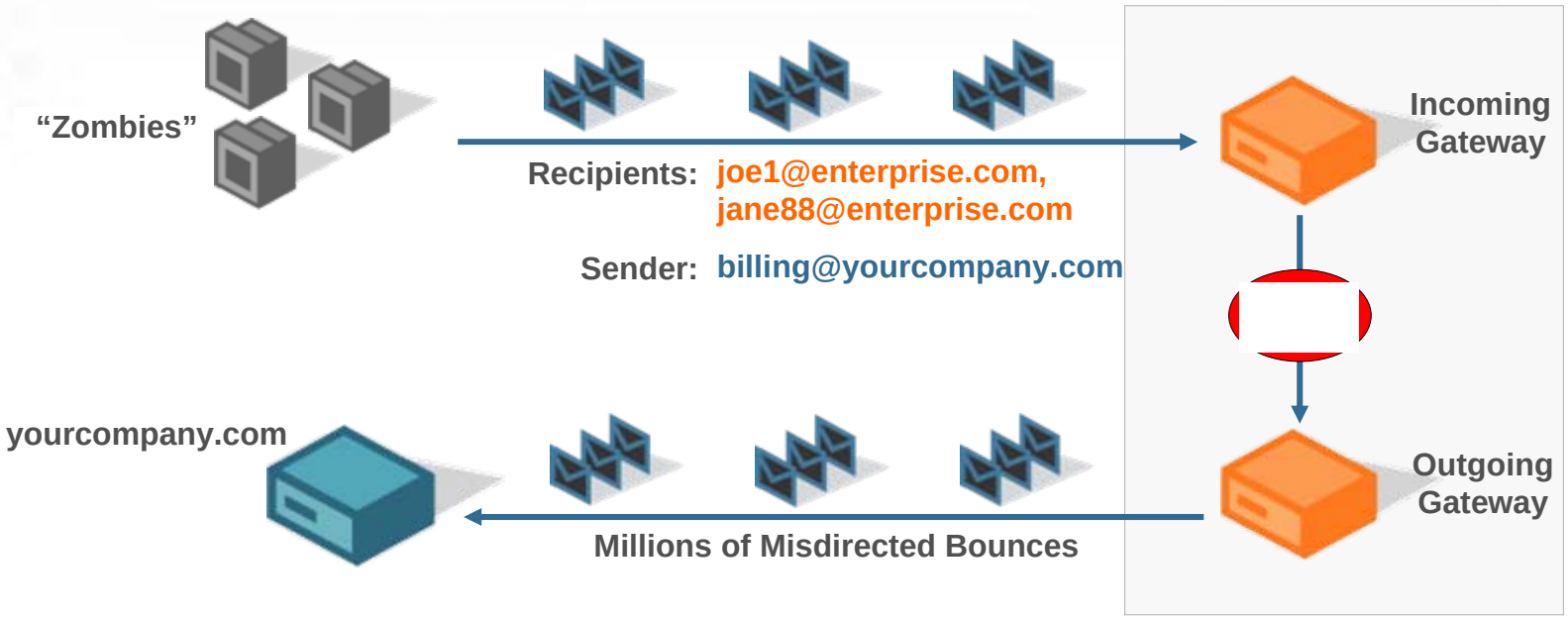
The following recipient(s) could not be reached:

doryan@unforgettable.com on 3/16/2004 8:57 AM
The e-mail account does not exist at the organization this message was sent to. Check the e-mail address, or contact the recipient directly to find out the correct address.
< mta13.adelphia.net #5.1.1 smtp; 550 <doryan@unforgettable.com>: User unknown>

IRONPORT

IronPort Bounce Verification™

сегодня уже 9% сообщений – с ложным обратным адресом



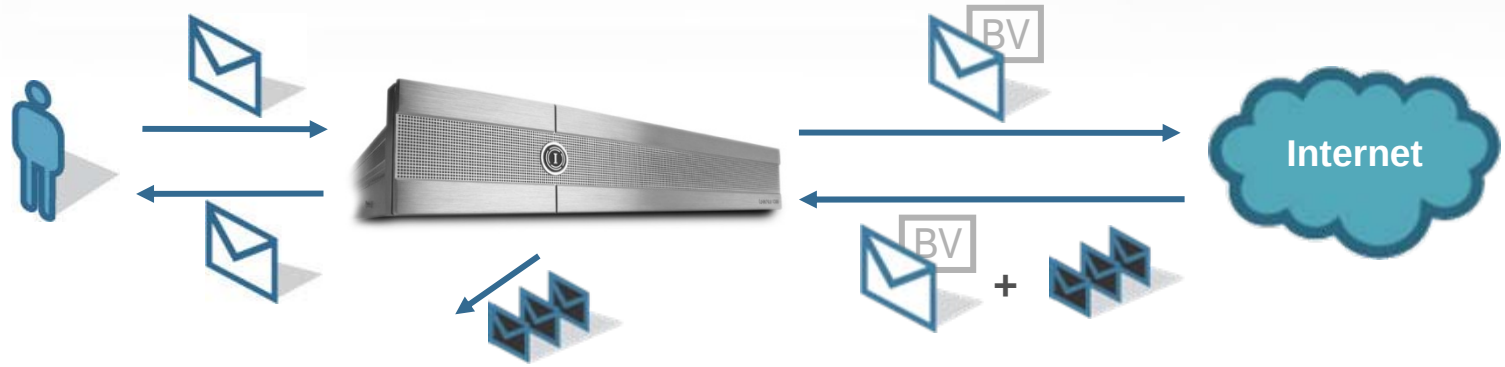
Более чем 55% из F500 имели опыт задержки сервиса или полной его недоступности из-за сообщений с ложным обратным адресом

IRONPORT

*Source: IronPort Threat Operations Center,
INTERNET EMAIL TRAFFIC EMERGENCY: SPAM "BOUNCE" MESSAGES ARE COMPROMISING NETWORKS, April 2006.

IronPort Bounce Verification™

Защищает от атак на базе несуществующего отправителя



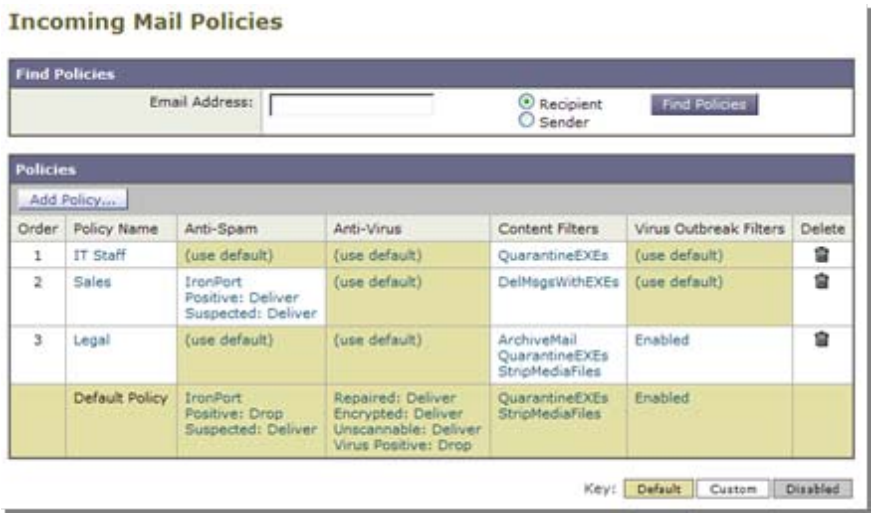
- Вся исходящая почта проверяется и маркируется как **легитимная** с существующим отправителем
- Прозрачно для пользователя, не требует каких-либо модификаций
- Освобождает ресурсы технической помощи по решению данных проблем

IRONPORT INNOVATION

IRONPORT

IronPort Email Security Manager

Общий взгляд на политики для всей организации



Incoming Mail Policies

Find Policies

Email Address: [ ] ◉ Recipient ○ Sender [Find Policies]

Policies

[Add Policy...]

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	IT Staff	(use default)	(use default)	QuarantineEXEs	(use default)	🗑
2	Sales	IronPort Positive: Deliver Suspected: Deliver	(use default)	DelMsgsWithEXEs	(use default)	🗑
3	Legal	(use default)	(use default)	ArchiveMail QuarantineEXEs StripMediaFiles	Enabled	🗑
	Default Policy	IronPort Positive: Drop Suspected: Deliver	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	QuarantineEXEs StripMediaFiles	Enabled	

Key: Default Custom Disabled

Категории: по домену, имени пользователя или LDAP

IT

- Разрешайте все медиа-файлы
- Заносите в карантин исполняемые файлы

SALES

- Помечайте и доставляйте спам
- Удаляйте исполняемые файлы

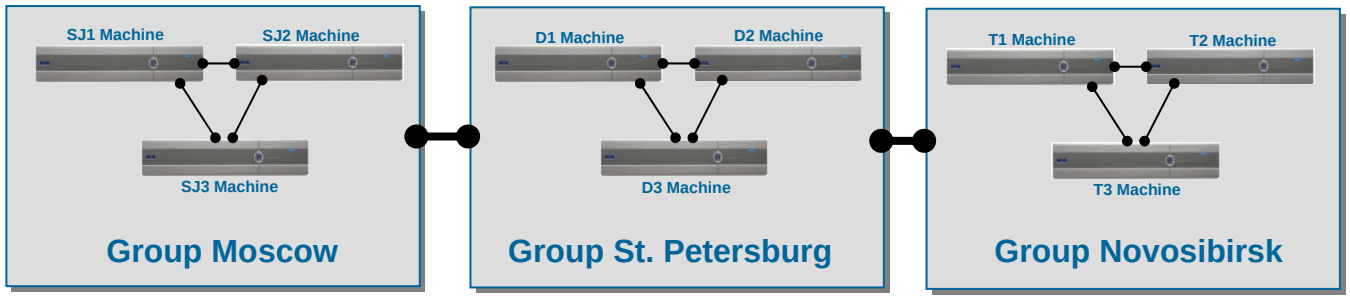
LEGAL

- Архивируйте всю почту
- Отключите Virus Outbreak Filters для файлов .doc

IRONPORT

Централизованное управление IronPort

- Подключайтесь где угодно, контролируйте везде
- Интерфейс обеспечивает согласованность конфигурации
- Применяйте изменения для машин, групп или кластеров
- Тестируйте на одной системе, затем переходите на кластер

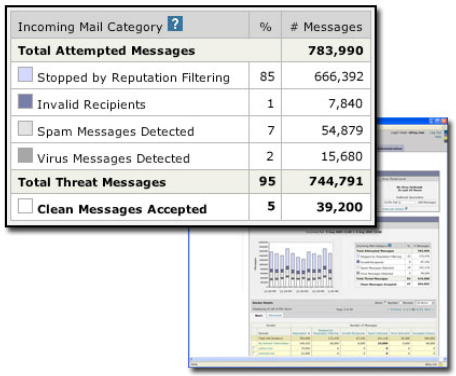


IRONPORT

IronPort Email Security Monitor™

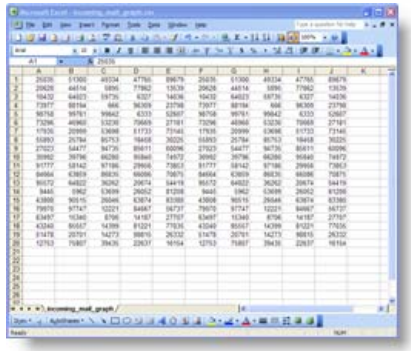
Мощная отчетность в реальном времени

Integrated Real-Time Graphical Reports

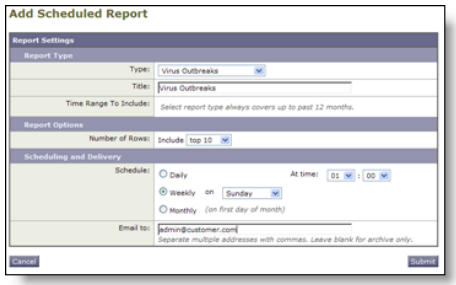


Incoming Mail Category	%	# Messages
Total Attempted Messages		**783,990**
Stopped by Reputation Filtering	85	666,392
Invalid Recipients	1	7,840
Spam Messages Detected	7	54,879
Virus Messages Detected	2	15,680
Total Threat Messages	**95**	**744,791**
Clean Messages Accepted	**5**	**39,200**

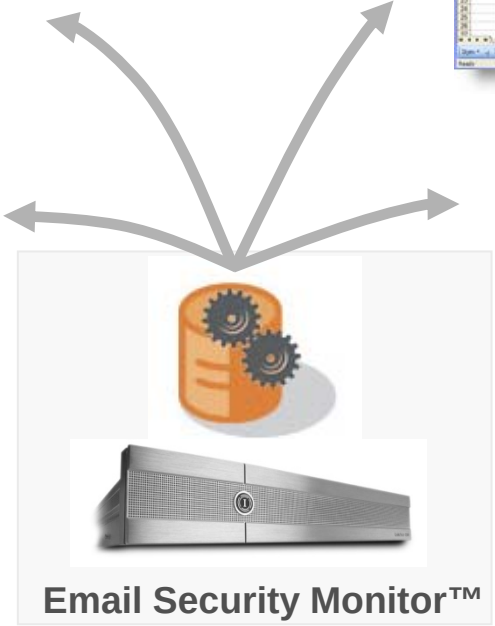
CSV Export



Scheduled Delivery



Search by Domain



Email Security Monitor™

IRONPORT®

17 Mar 2008 00:00 to 30 Mar 2008 23:59

Государственный сберегательный банк России

Incoming Mail Summary

Message Category	%	Messages
• Stopped by Reputation Filtering	98.2%	1.0M
• Stopped as Invalid Recipients	0.0%	12
• Spam Detected	1.7%	17.2k
• Virus Detected	0.0%	0
• Stopped by Content Filter	0.0%	0
Total Threat Messages:	**99.9%**	**1.0M**
• Clean Messages	0.1%	1,277
Total Attempted Messages:		**1.0M**

IRONPORT

IronPort S-Series™
Безопасный & Контролируемый Web трафик

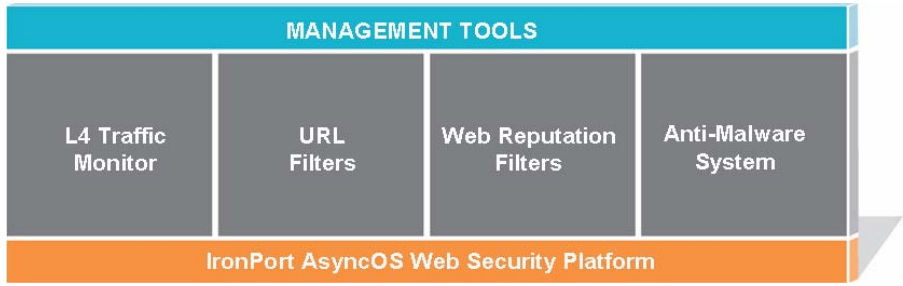
Устройства **IronPort** для обеспечения **WEB** безопасности

IRONPORT®

IronPort S-Series

- Контроль & безопасность Web трафика (HTTP;HTTPS;FTP)
- Комплексное управление & доступность
- Лидирующая в отрасли точность против WEB угроз
- Производительность корпоративного уровня

Решение IronPort по Web безопасности



Новое поколение платформ Web безопасности

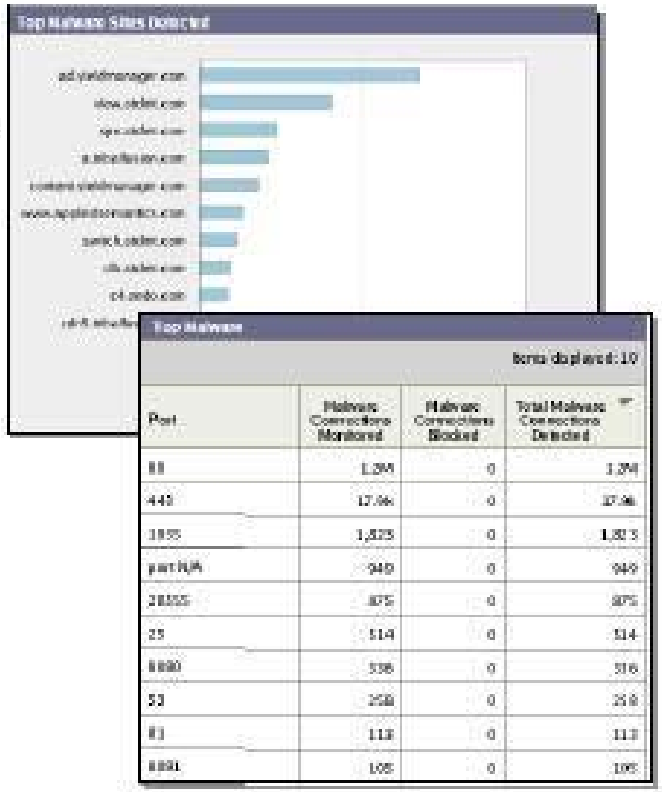
AsyncOS™

Бесподобная масштабируемость

Обнаружение существующих зараженных клиентов
Монитор трафика L4

Мониторинг трафика "Phone Home"

- Layer 4 Traffic Monitor
  - Сканирует весь трафик, все порты и протоколы
  - Обнаружение вредоносного ПО, которое не использует порт 80
- Большая база anti-malware
  - Автоматически обновляемые правила Anti-Malware
  - Генерирование правил в реальном времени с помощью "Dynamic Discovery"



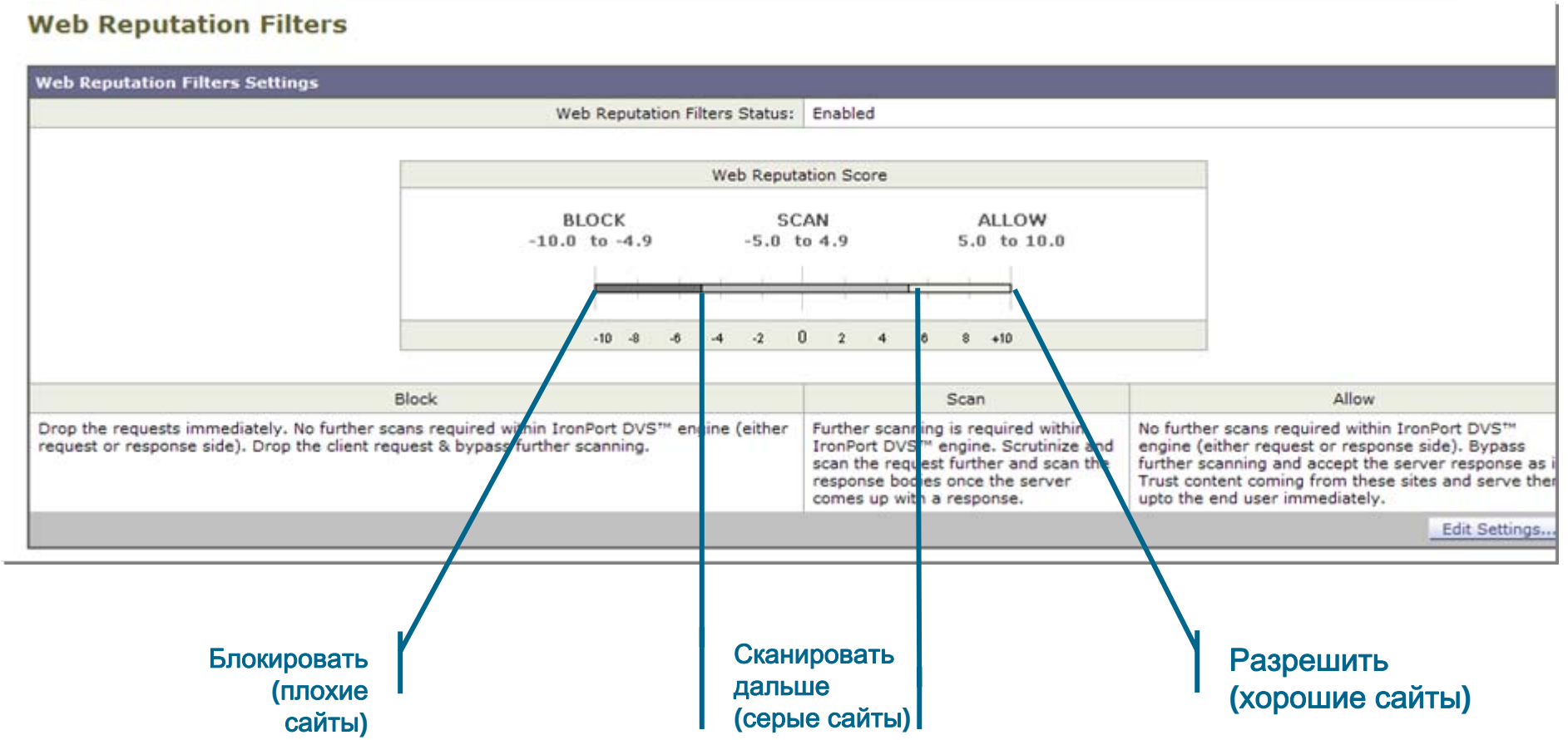
IronPort фильтры URL

Лидирующая точность и контроль

- Самая большая и полная База данных
  - 52 категории, более 21M сайтов, ~3.5B web страниц
  - 1/3 базы данных интернациональна
- 24 x 7 наблюдение
- Регулярное, автоматическое обновление

Репутационные Фильтры Web

Политики, базирующиеся на репутационных оценках в базе данных Sender Base



Блокировать (плохие сайты)

Сканировать дальше (серые сайты)

Разрешить (хорошие сайты)

Динамическое применение политик

- **Фильтры WEB репутации IronPort** – это мощный первый рубеж обороны
- **Система обнаружения вредоносного ПО IronPort** – обеспечивает изощренный второй рубеж обороны.

Webroot

Самая большая, наиболее точная база сигнатур

- Система автоматического поиска угроз (Phileas™)
- Упреждающее определение угроз
- Проверено собственной исследовательской группой анализа угроз

- Бесплатное ПО с рекламой
- Диспетчеры систем
- Ложные ссылки (фарминг)
- Сканеры паролей
- Browser Hijackers
- Руткиты
- Browser Helper Objects
- Ки-логгеры
- Трояны
- Фишинг & и т.д.…

PC MAGAZINE EDITORS' CHOICE
July 17, 2006
Spy Sweeper 5.0

WEST COAST LABS CHECK MARK
SEE YOUR SAFEGUARDS AT www.check-mark.com
Anti-Spyware INSTALLED

PC WORLD WORLD CLASS 2006
Spy Sweeper 4.5
July 2006

c|net Download.com 5-Star Rating

Интегрированная авторизация

- Авторизация, базирующаяся на запросах (Basic/LDAP)
- Авторизация, базирующаяся на соединениях (NTLM)

Защищенный LDAP

NTLM/Active Directory

LDAP

Web Security Monitor™

- *Обзор системы*
- *Тенденции Web трафика*
- *Активность на узле*
- *Детально по узлу*
- *Активность клиента*
- *Детально по клиенту*
- *Детально по категориям*
- *Детально по вредоносному ПО*
- *Тенденции вредоносного ПО*
- *Диспетчер трафика L4*
- *Web репутация*

Исчерпывающая стратегия & понимание безопасности

Политика тестирования

- **бесплатное тестирование в течение 30 дней**
  - начинается с подбора тестового устройства и активации ключей
  - возможно продление тестирования
- **для каждого тестирования**
  - каждая организация получает то устройство, которое рекомендуется именно для её нужд
  - разные виды тестирования
  - полная техподдержка при тестировании

IronPort

Контактная информация

Дугарёв Сергей

руководитель направления IronPort,

заместитель директора

headtechnology Ukraine

официальный дистрибьютор **IronPort Systems** в Украине

ул. Леваневского 6, офис 79

03058, Киев, Украина

тел.: +380 44 353-3020

моб.: +380 96 458-2142

факс: +380 44 457-8541

e-Mail: s.dougaryov@headtechnology.com.ua

Internet: www.headtechnology.com.ua

Вопросы?

headtechnology
it-security

Благодарю за внимание!

IRONPORT