



Виртуализация без границ

# Cisco Security SAAS

## Облако как платформа безопасности контента

Павел Родионов  
Системный инженер

04 апреля 2012

# Содержание

1. Почему SaaS?
2. Облако Cisco Security Intelligence Operations
3. ScanSafe Cloud Web Security
4. Cloud Email Security Solution.

# Эволюция сервисов безопасности

## От приобретения оборудования до SaaS



# Преимущества SaaS

Простые и удобные  
средства управления

Предсказуемые OpEx

Минимальные сроки  
внедрения

Нулевые CapEx

Освобождение ресурсов  
для бизнес задач

Откройте новые возможности

# "Облачная" система безопасности Cisco



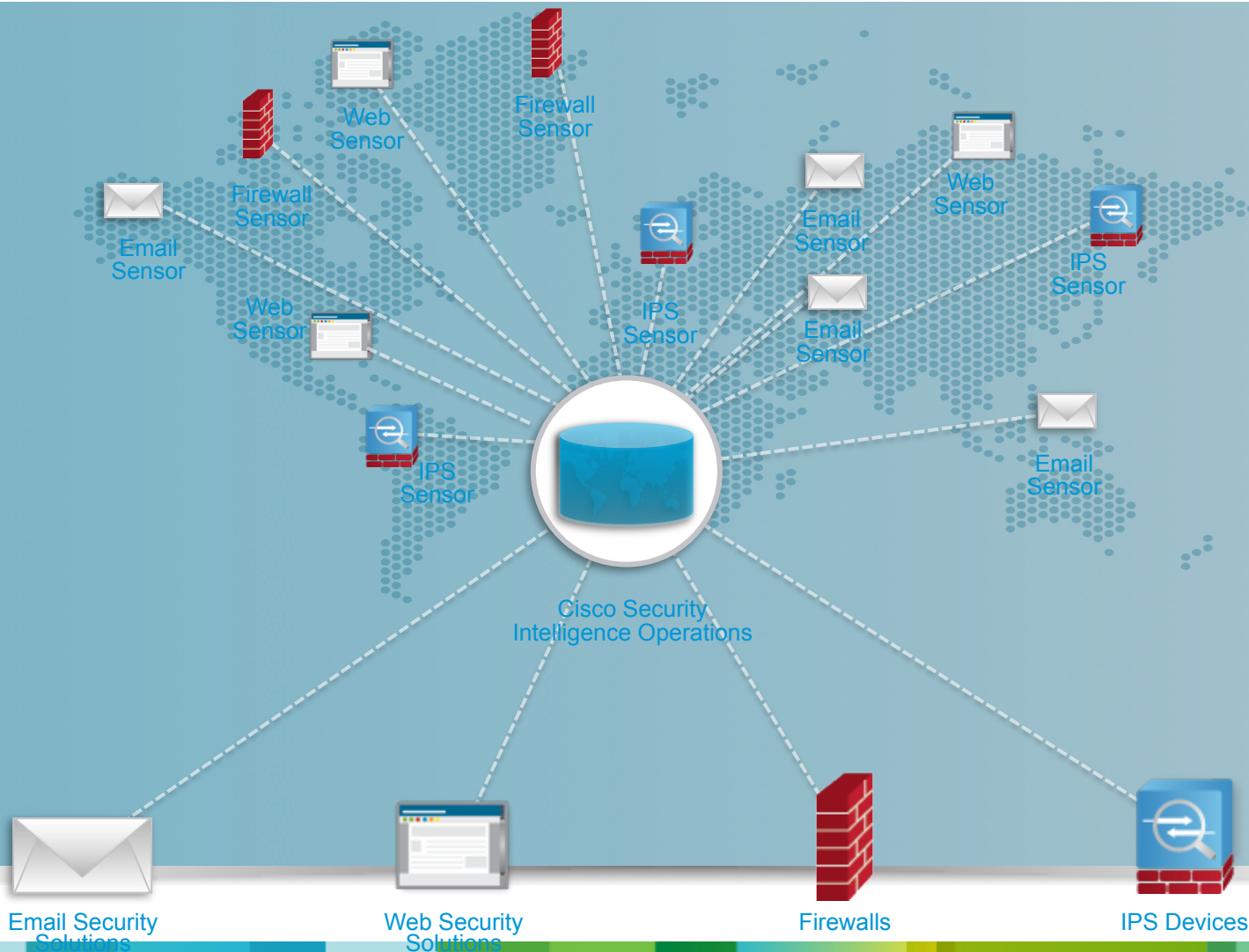
- Multi-tenant архитектура для обслуживания множества заказчиков
- Распределенная масштабируемая платформа с резервированием
- Постоянное наращивание производительности и внедрение новых ЦОД

## ■ Глобальная система мониторинга угроз

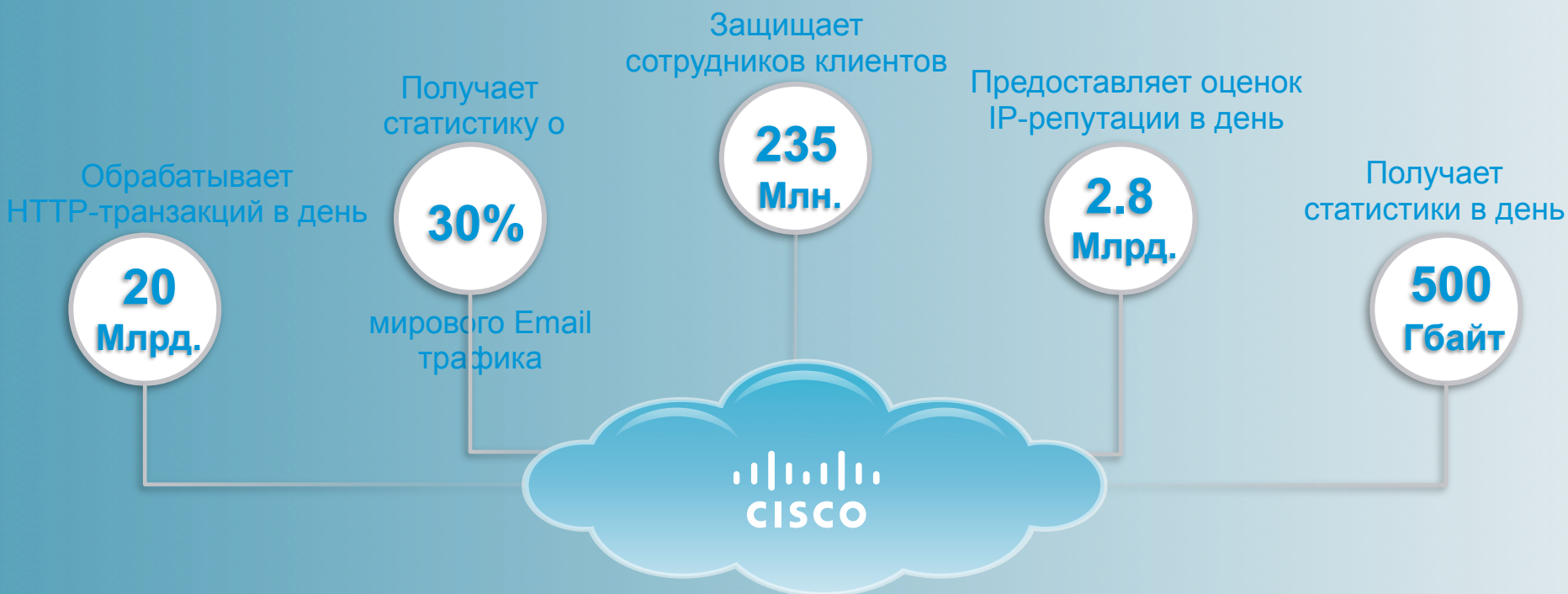
- Встроенная система управления и формирования отчетов
- Глобальная платформа для мобильных пользователей

# Cisco Security Intelligence Operations (SIO)

Глобальная система мониторинга угроз



# Характеристики облака Cisco



## Люди

Более 500 выделенных экспертов

## Ресурсы

Тысячи устройств в десятках ЦОД по всему миру

## Технологии

Передовые технологии безопасности, Глобальная система оценки угроз

# SaaS-платформа ScanSafe



# Что такое ScanSafe?



## Профиль компании:

- Основана в 2004г.
- Пионер и мировой лидер в области SaaS услуг Web и Email безопасности
- Клиенты - от SMB до Large Enterprise в более чем 100 странах
- 100% Uptime за всю историю предоставления услуг
- 80% продаж – через операторов связи
- Подразделение Cisco с Декабря 2009г.

### Awards



Security product  
of the year 2008



**Microsoft**  
GOLD CERTIFIED  
Partner



2007 SIIA  
//CODiE//  
WINNER

### Customers



Shell



Disney



BACARDI



ROTHSCHILD



Standard  
Chartered



LOUIS VUITTON



IKEA



QUINTILES  
TRANSNATIONAL

### Partners



Business  
Services



Google™



Sprint



TELUS®

NEC

# Облачные услуги Cisco ScanSafe

## Web фильтрация

- Контроль использования
- Просмотр приложений
- Двусторонний контроль

## Web безопасность

- Защита от malware
- Анализ Web контента
- Эмуляция скриптов

Централизованный репортинг

Мобильная безопасность

# Зона охвата глобальных ЦОД



# ОБЛАЧНАЯ ИНФРАСТРУКТУРА



# Бизнес-драйверы облачной веб безопасности

## Заражение malware



Потери данных  
Потеря  
производительности  
Большое количество IT  
ресурсов для избежания

## Увеличивающаяся нагрузка на IT



Увеличение  
ответственности IT  
Расширение  
организации и  
увеличение количества  
офисов

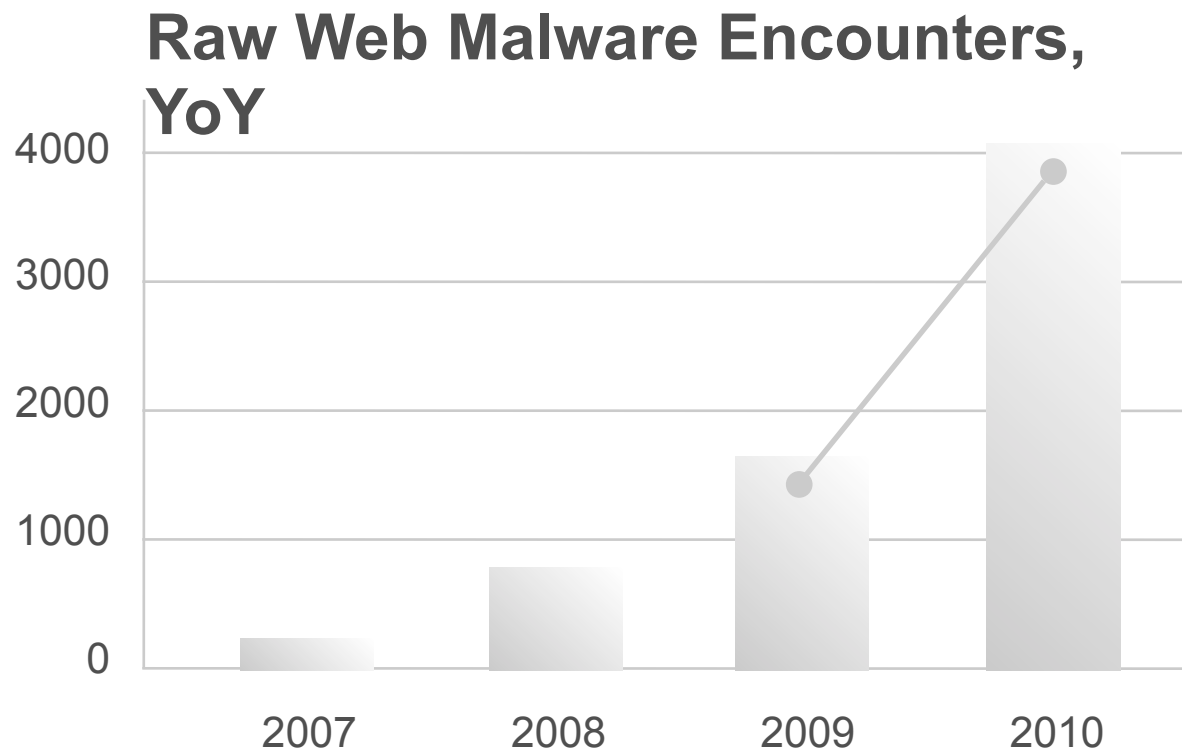
## Несоответствие политик в предприятии



Потенциальные дыры в  
безопасности  
Незавершенные  
системы репортинга и  
обзора

# Web Malware продолжает расти угрожающими темпами

ScanSafe Focus Customer



139% увеличение с 2009 до 2010

В 2010 году предприятия в среднем сталкивались со 135 атаками web malware

Source: Cisco ScanSafe



**35%**

Обхват глобального email

**20B**

Ежедневных web запросов

**300K**

IPS сигнатур

**700,000+**

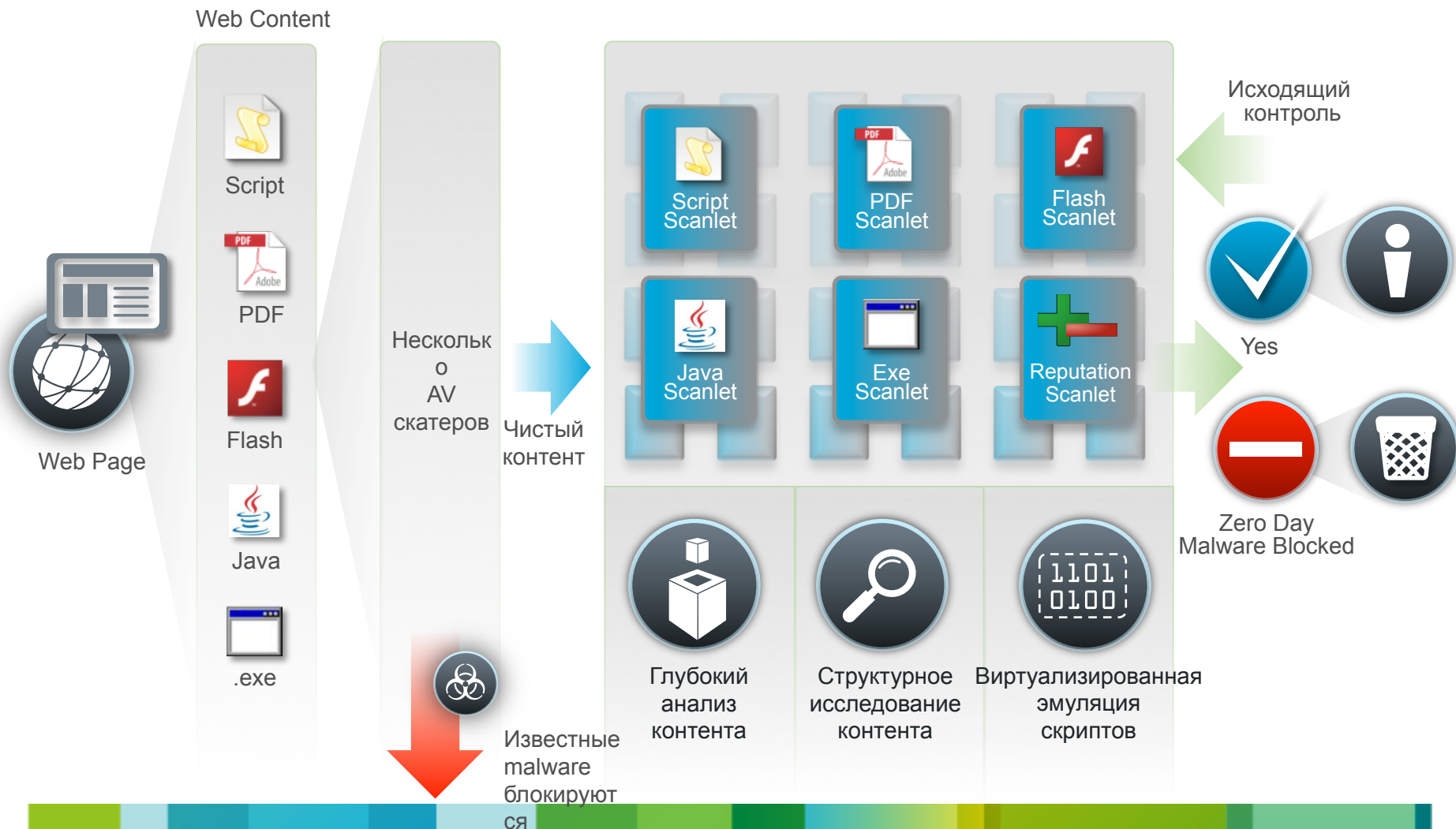
Устройств

**150M +**

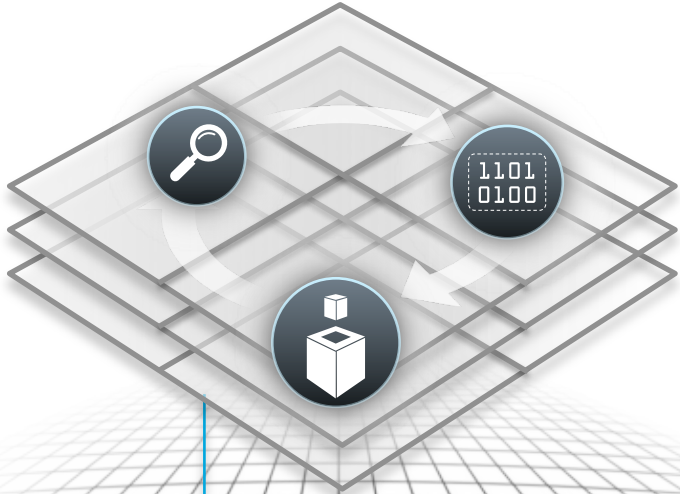
конечных точек

# Архитектура защиты от атак malware 0 дня

## Outbreak Intelligence



# Outbreak Intelligence



Глубокий анализ  
контента



Структурное  
исследование



Эмуляция  
скриптов

# Outbreak Intelligence

Миллиарды ежедневных запросов

20B  
Requests



**Identified: Malicious**  
**Content:** Obfuscated  
**Content:** PDF  
**Scanning Tower:** 1220b  
**Server:** 02106  
**Action:** Blocked



Глубокий анализ  
контента



Структурное  
исследование



Эмуляция  
скриптов

# Полное знание контекста

Кто



Время



Объект



Job Sites



Human Resource

Instant Message



No File Transfer

Facebook



Lunch Hour

Streaming Media



Business-related Content

P2P



All

Приложение



Место



Соответствие



# Правила использования для Web 2.0

## Применение правил использования

- Снижение потерь производительности
- Уменьшение риска нарушения законодательства
- Управление трафиком Web 2.0 и Web приложениями

### URL Filtering



- URL база данных, содержащая более 50М узлов
- Динамическая категоризация
- *SearchAhead*

### Application Visibility and Control



- Контроль Web приложений, e.g., IM, Facebook, WebEx
- рейтинг контента

# Система репортинга ScanSafe WIRe

- ✓ Высокая производительность
- ✓ Глобальный охват
- ✓ Хранение данных
- ✓ Детальный просмотр
- ✓ Стоимость
- ✓ Сложность

# Глубина охвата

Для каждого запроса и 10 тыс настраиваемых отчетов сохраняется более 100 атрибутов

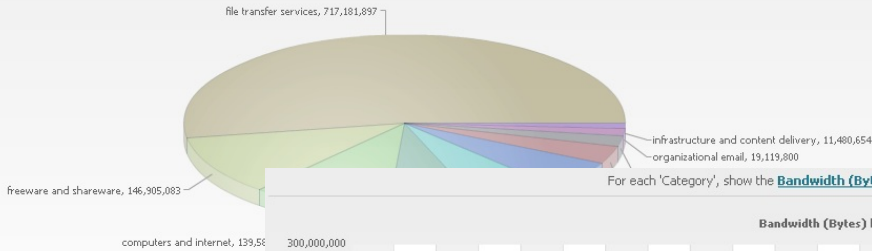
Adware	Group Domain	Protocol	Response Version
Block Type	Croup Name Part	PUA	Response Version (Original)
Block Value	Group Name Part (Original)	Query	Risk Class
Category	Host	Referer Host	Rule Action
Connector Mode	Host (Original)	Referer Host (Original)	Rule Engine
Connector OS Name	Hour	Referer Path	Rule Name
Connector OS Name (Original)	Inbound File Extension	Referer Port	Rule Name (Original)
Connector OS Version	Inbound File Name	Referer Protocol	Second Level Domain
Connector OS Version (Original)	Internal IP	Referer Query	Spyware
Connector Version	Internal IP Subnet/16	Referer Second Level Domain	Threat Type
Country Dst Code	Internal IP Subnet/24	Referer Top Level Domain	Top Level Domain
Country Src Code	Internal IP Subnet/8	Referer URL	URL
Day Of Month	Malware	Referer URL (Original)	URL (Original)
Day Of Week	Minute	Request Content Type	User
Destination IP	Month	Request Content Type	User (Original)
Domain Username	Outbound File Extension	Request Major Content Type	User Agent
Domain Username (Original)	Outbound File Name	Request Method	User Agent (Original)
External IP	Path	Request Method (Original)	User Agent Application Name
External IP Subnet/16	Pattern Narne	Request Version	User Agent Application Version
External IP Subnet/24	Pattern Name (Original)	Request Version (Original)	User Agent Comp Platform
External IP Subnet/8	Phishing	Response Content Type	User Agent Comp Version
Group	Policy Violation	Response Content Type	User Agent Compatibility
Group (Original)	Port	Response Major Content Type	Virus
			Year

# Обзор, тренды и проведение исследований

What was the Bandwidth consumption by Category?

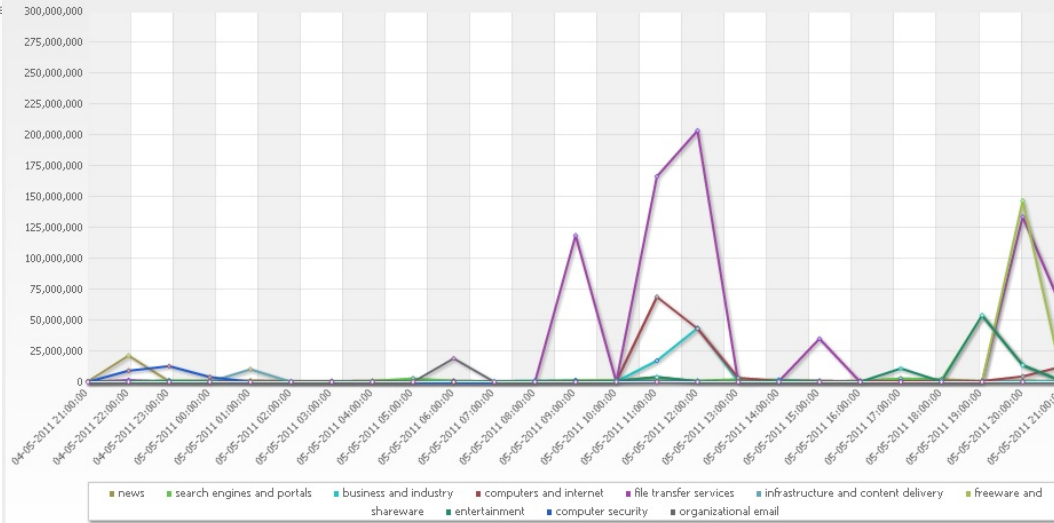
For each 'Category', show the [Bandwidth \(Bytes\)](#) (click to change)

Bandwidth (Bytes) by Category



For each 'Category', show the [Bandwidth \(Bytes\)](#) (click to change) over time.

Bandwidth (Bytes) by Hour



Rule Action Block Type  Bytes Received

Launch search

1 2 3 4 5 next > last >> 591 results

st	Category	Rule Action	Block Type	Bytes Received	
	promo / advertising	block	adware	0	
xm	software and hardware vendors / distributors	block	adware	0	
xm	software and hardware vendors / distributors	block	adware	0	
	search engines / directories / portals	block	adware	0	
	general news / newspapers / magazines	block	adware	0	
	promo / advertising	block	adware	0	
	promo / advertising	block	adware	0	
112.207.net	promo / advertising	block	adware	0	
112.207.net	promo / advertising	block	adware	0	
112.207.net	promo / advertising	block	adware	0	
112.207.net	promo / advertising	block	adware	0	
112.207.net	promo / advertising	block	adware	0	
112.207.net	promo / advertising	block	adware	0	
112.207.net	promo / advertising	block	adware	0	
112.207.net	promo / advertising	block	adware	0	
am.102.122.207.net	software and hardware vendors / distributors	block	spyware	0	
sm.102.122.207.net	software and hardware vendors / distributors	block	spyware	0	
sm.102.122.207.net	software and hardware vendors / distributors	block	spyware	0	
sm.102.122.207.net	software and hardware vendors / distributors	block	spyware	0	
05-11-2010 11:49:22	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0
05-11-2010 11:49:31	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0
05-11-2010 11:50:08	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0
05-11-2010 11:50:13	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0
05-11-2010 11:50:21	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0
05-11-2010 11:50:31	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0
05-11-2010 11:50:49	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0
05-11-2010 11:50:57	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0
05-11-2010 11:50:58	americanexpress.com.102.122.207.net	software and hardware vendors / distributors	block	spyware	0

# Безопасность мобильных пользователей со ScanSafe



- Безопасность и политики даже вне сети и вне VPN
- Подключение к ближайшему ЦОД
- Бесшовная интеграция с Cisco AnyConnect клиент

# Клиент Cisco AnyConnect Secure Mobility

## Оптимизация

- Обнаружение ближайшего шлюза
- Обнаружение доверенной сети

## Всегда безопасный

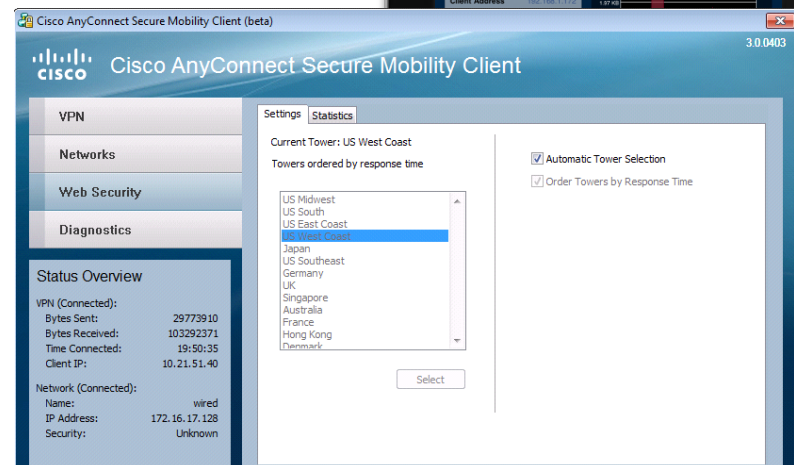
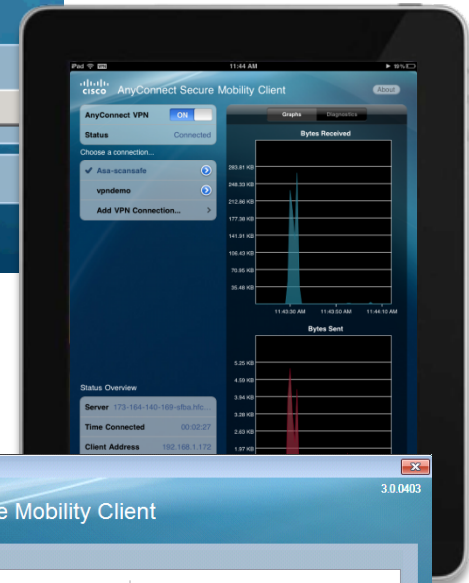
- работа даже вне VPN
- Защита от атак 0-го дня

## Всесторонний

- Поддержка Windows, Mac, iPhone&iPad

## Прозрачный

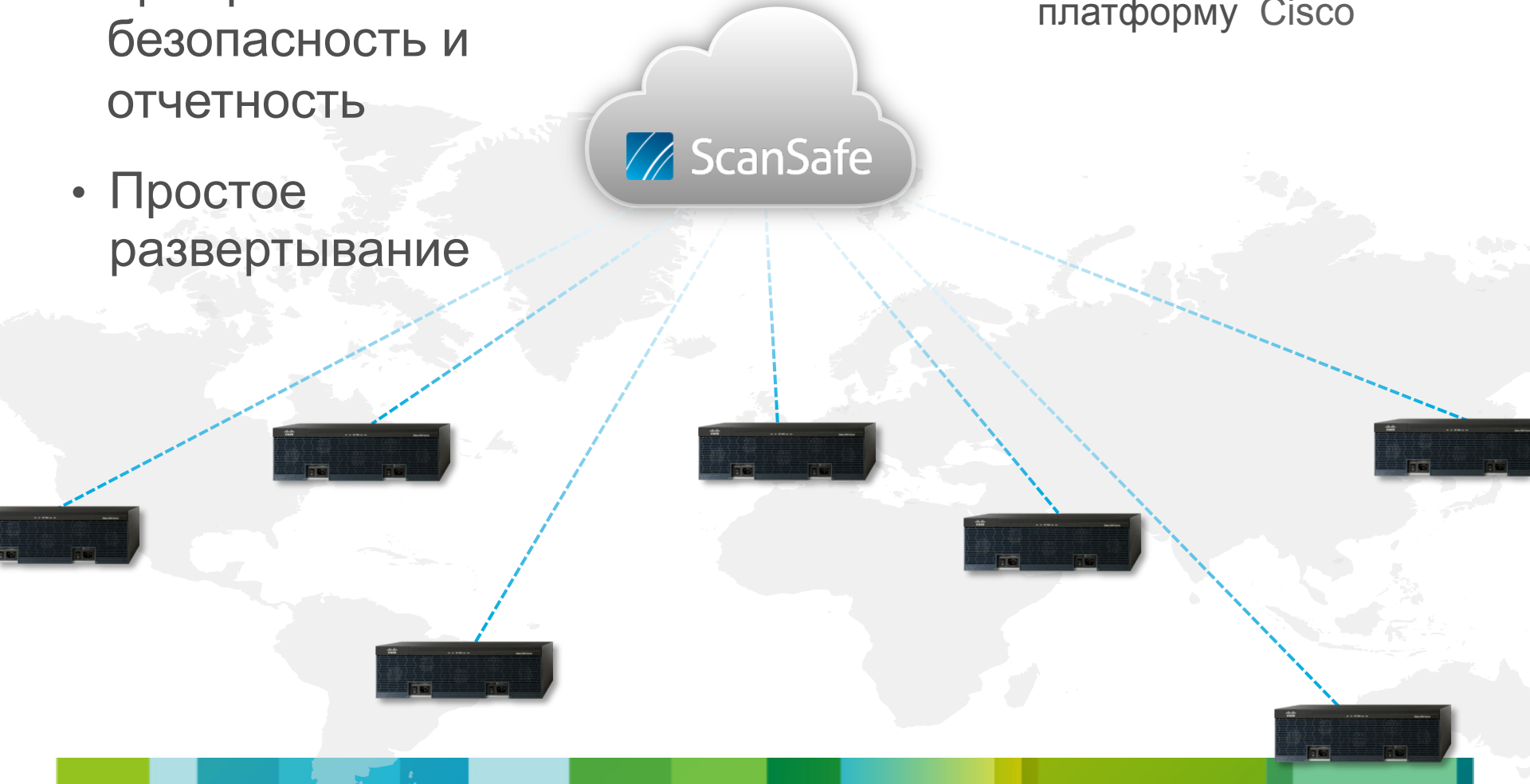
- Прозрачная работа
- Обнаружение Hotspot/Captive Portal



# Безопасность филиалов в облаке

- Централизованная безопасность и отчетность
- Простое развертывание

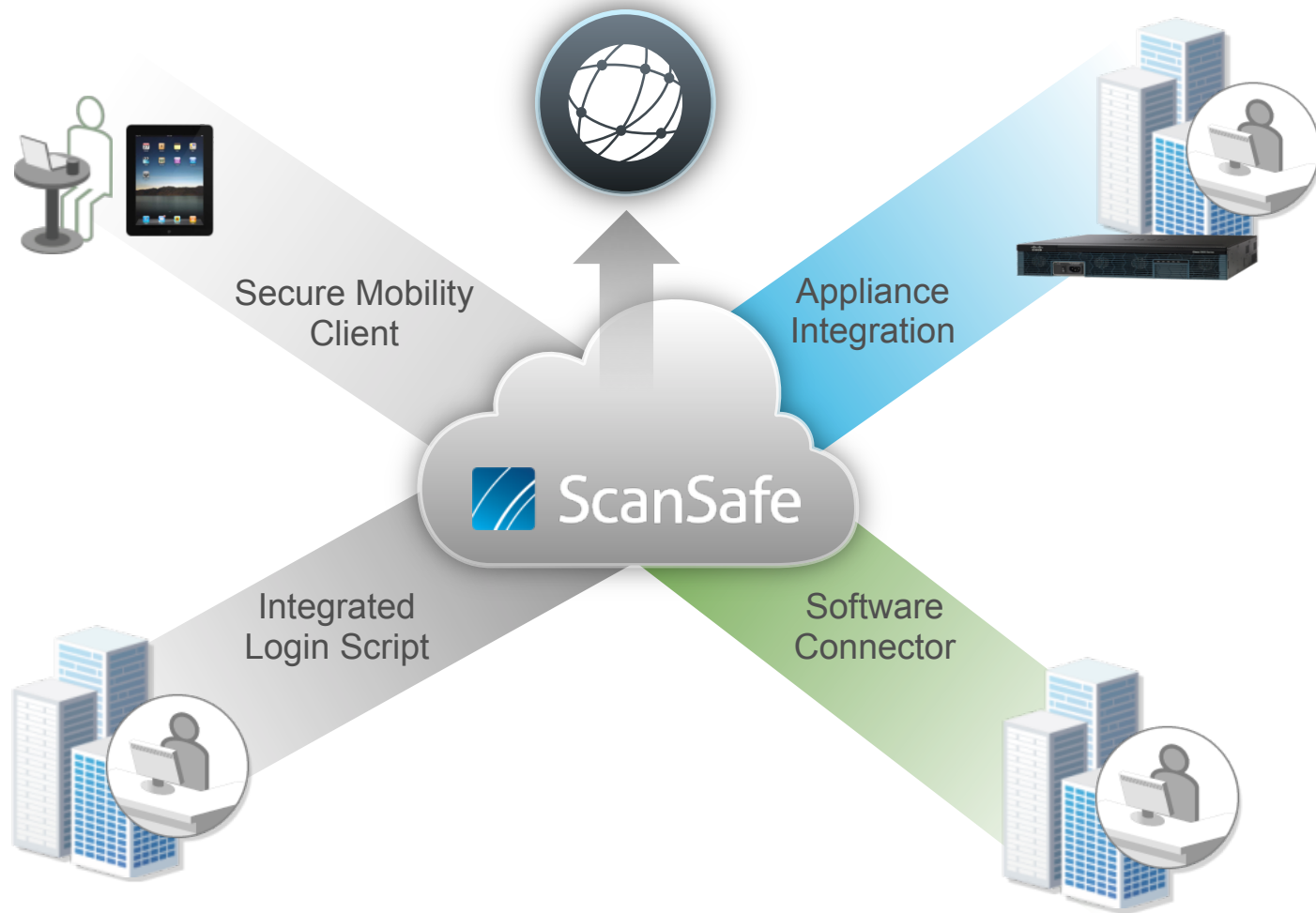
- Расширение инвестиций в платформу Cisco



# ISR Web Security со Cisco ScanSafe



# Выбор вариантов развертывания



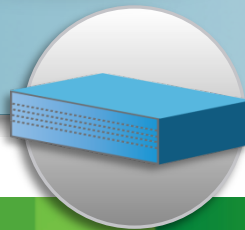
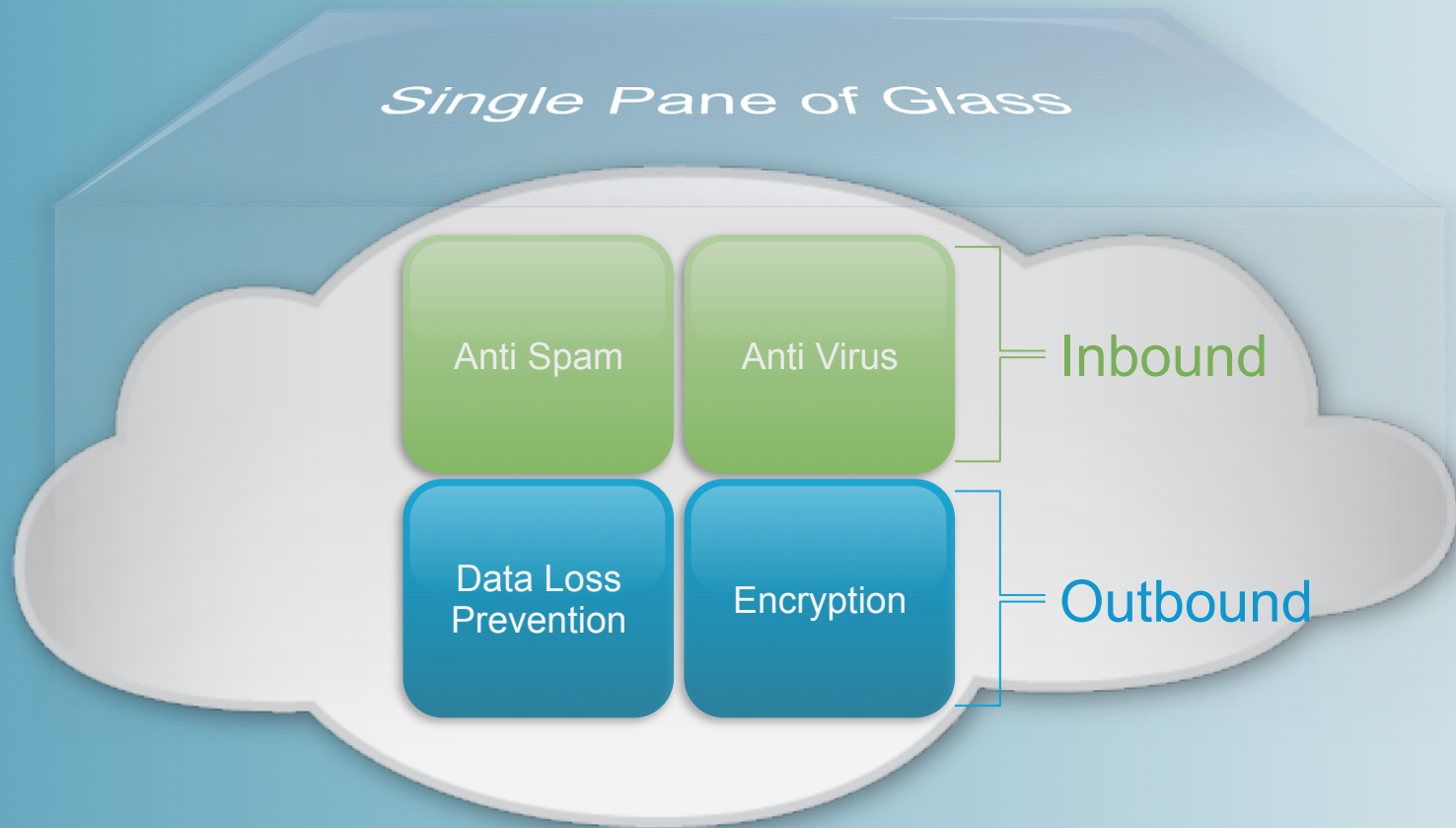
# В чем преимущества ScanSafe?

- **Защита основного канала распространения угроз:** Защиты от ВПО, ограничение доступа к сайтам по категориям, DLP, проверка HTTPS
- **Предсказуемые затраты:** переход от CapEx к OpEx
- **Для клиентов с большим кол-во филиалов:** нет необходимости покупать много устройств или пропускать весь трафик через HQ
- **Для клиентов с мобильными сотрудниками:** возможность обеспечить защиту от угроз и политику доступа в Интернет вне зависимости от местоположения сотрудника
- **Унификация и централизация:** настройка политик и мониторинг из одной точки
- **Скорость внедрения:** Не нужно ждать оборудования и окончания его запуска



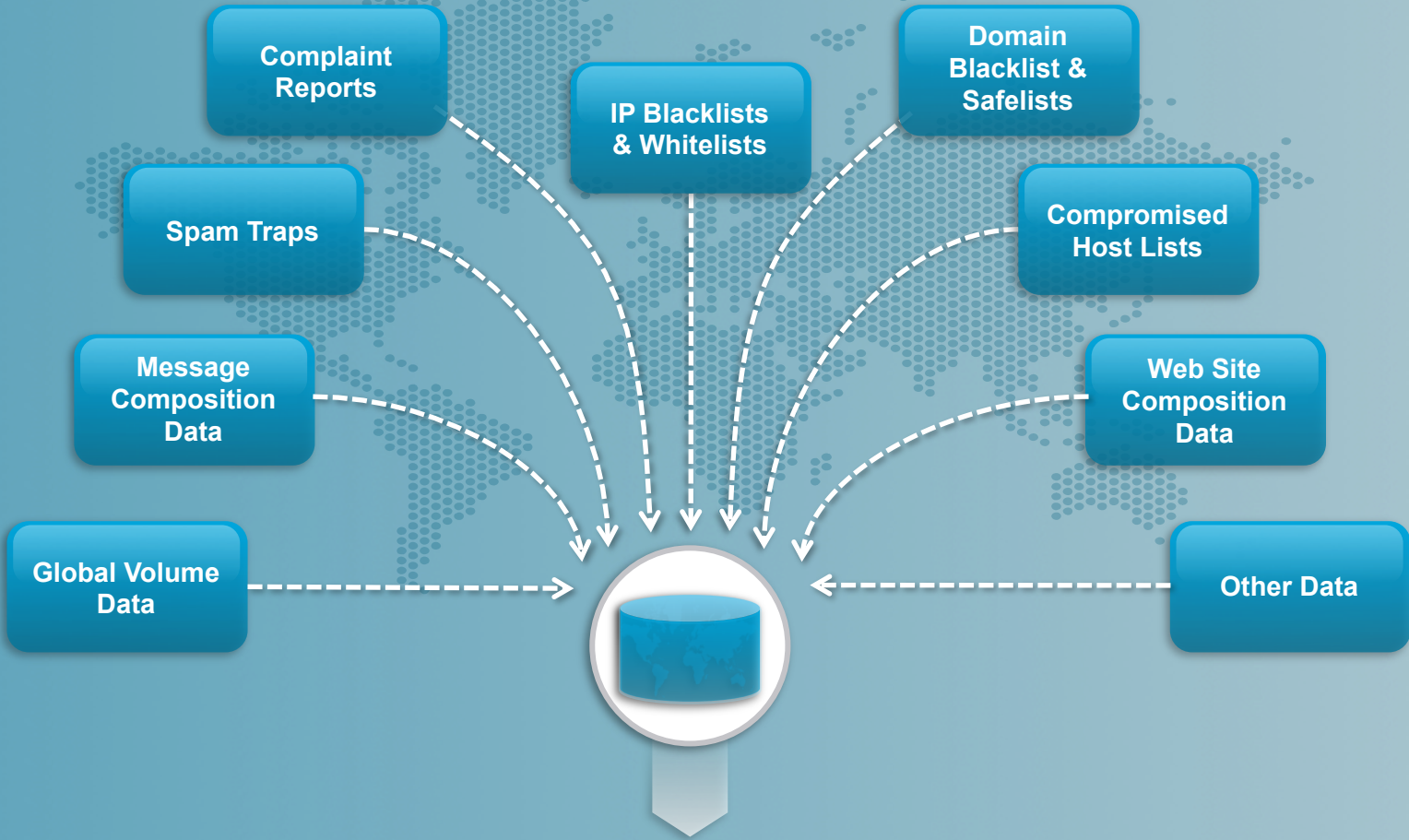
# Электронная почта Варианты внедрения

# Архитектура Email безопасности



# SensorBase

Email репутация



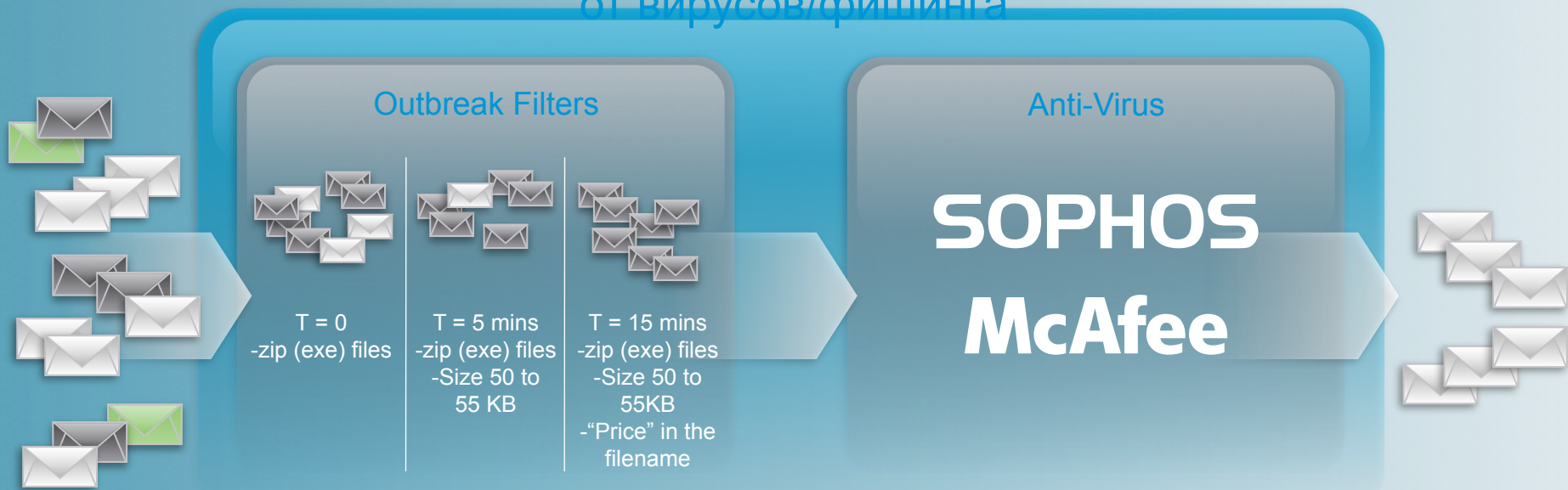
IP Reputation Score



# Антивирусная архитектура

Эшелонированная оборона

Многоуровневая защита  
от вирусов/фишинга



# Управление исходящими сообщениями

Web Protection



HTTP



HIPAA



Trade  
Secrets



PCI

SMTP



Security Enforcement Array



HR/Legal  
Review

✓ Corporate  
Policies



Encryption

✓ HIPAA  
PCI  
SB-1386



Dropped  
Attachment

✓ Company  
Reputation

Обнаружение

Коррекция

# Cisco IronPort AsyncOS

## Набор инструментов для защиты заказчиков

### TLS шифрование

Шифрование на уровне шлюз-шлюз

### HTML Sanitization

избежать поддельных URLs

### SPF проверка

Проверка того, что письмо было отправлено сервером, авторизованным отправлять почту для данного домена



### Возможность LDAP

LDAP ссылки, несколько LDAP серверов, установка за 3 шага

### DKIM подпись и проверка

Проверка отправителя

### Bounce Verification

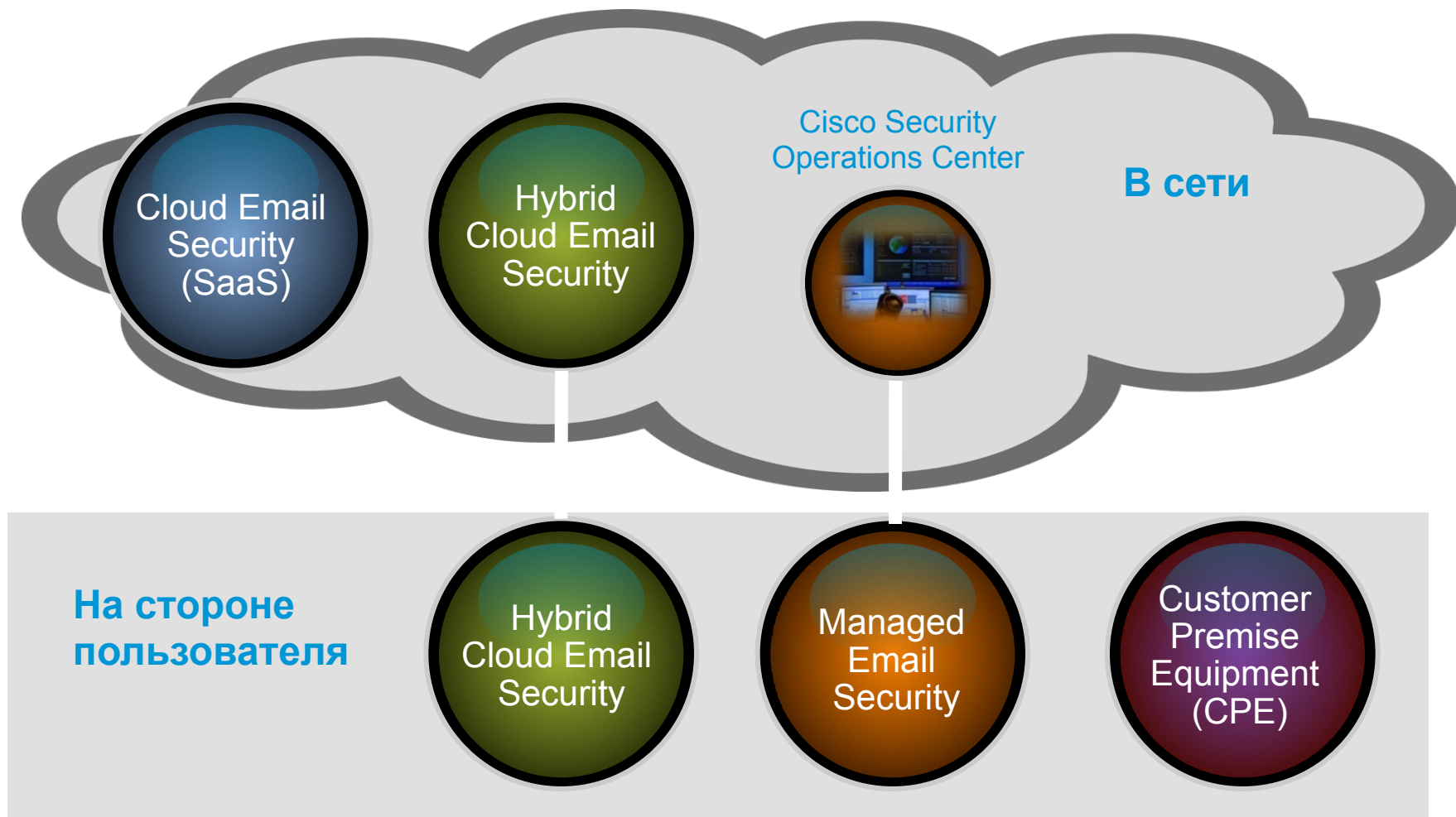
Избежать перенаправленных bounces

**Спам-карантин, черные и белые списки для пользователей**  
Контроль пользователей

### Проверка получателя

Удалить сообщения, которые отправлены на несуществующий адрес

# Набор гибких опций внедрения

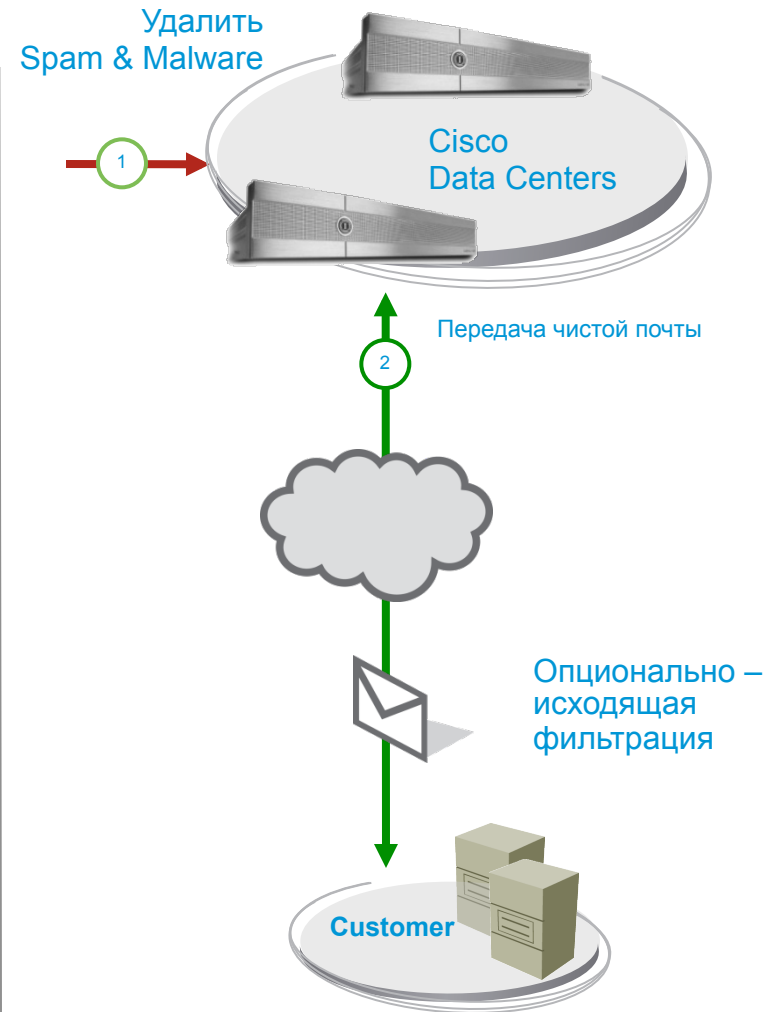


Common Policy | Centralized Reporting | Consistent Protection

# Cloud Email Security

Выделенное решение снижает нагрузку и ускоряет внедрение

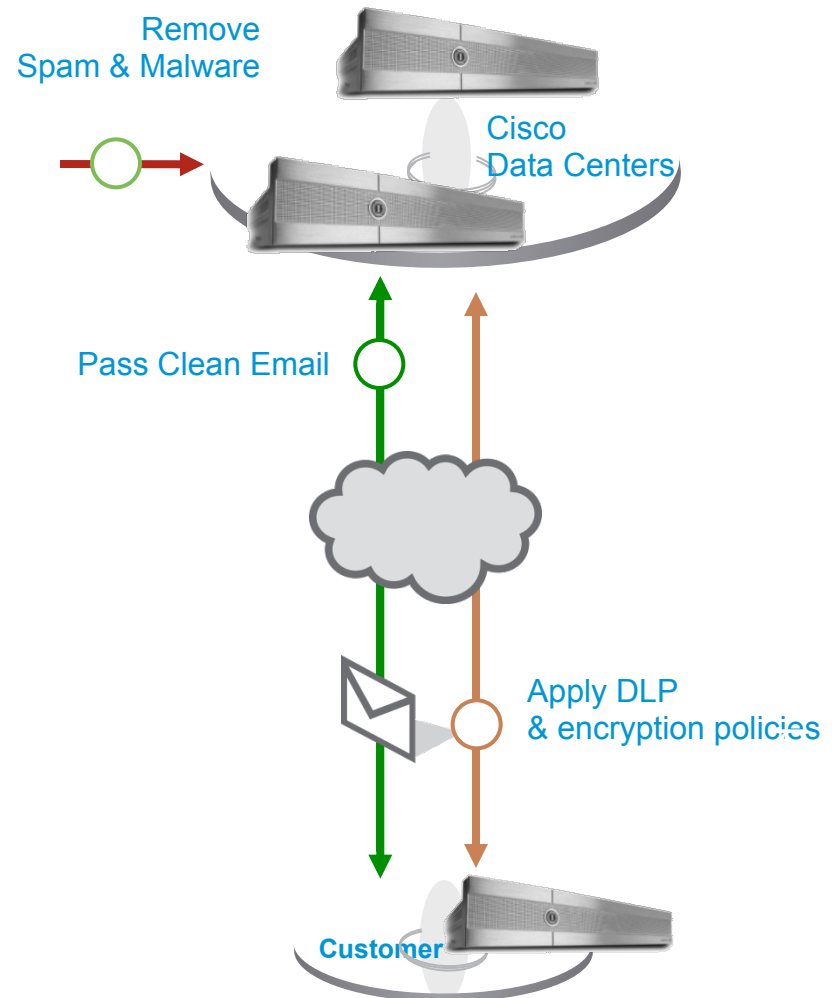
- Безопасности Email в облаке снижает нагрузку на ЦОД
- «Выделенное» решение снижает риск общего сбоя ('shared fate' risk)
- Управляемая инфраструктура гарантирует производительность для будущего роста



# Гибридный Cloud Email Security

## Оптимальный дизайн, максимальная гибкость

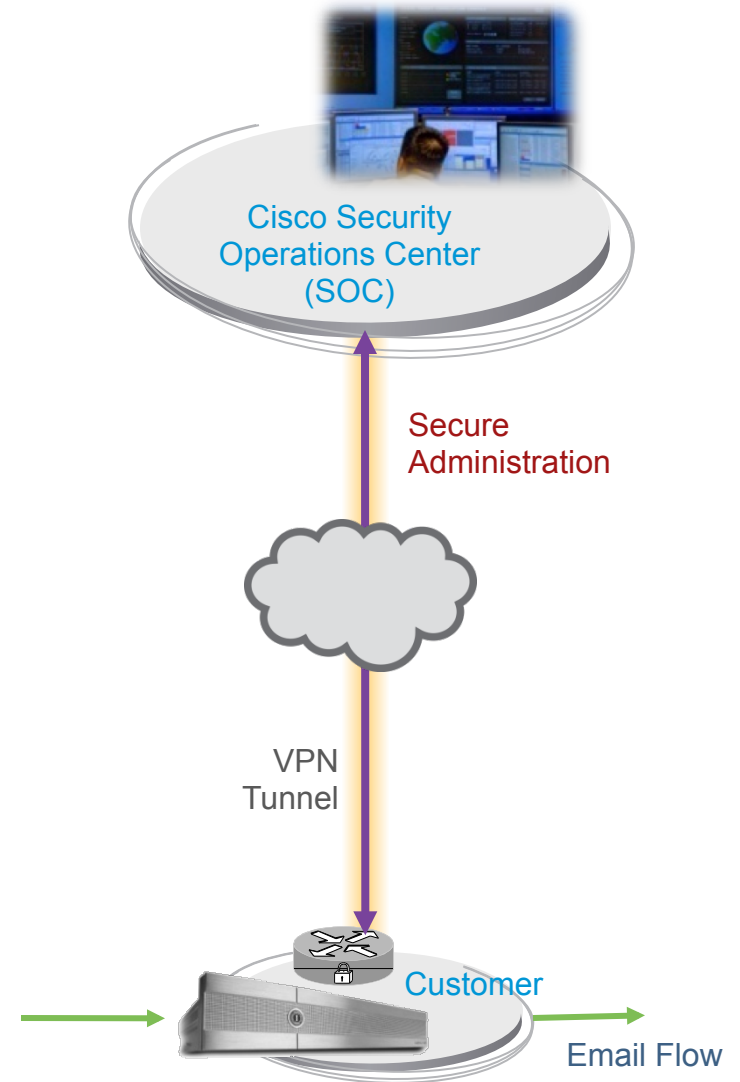
- Гибридный дизайн подразумевает разнесенное управление – на площадке и в облаке
- Устройства на площадке пользователя контролируют исходящую почту, политики DLP и шифрование



# Managed Email Security

Возложите задачу обеспечения безопасности email на экспертов

- Самый высокий уровень аутсорсинга.
- Предсказуемая модель стоимости
- Сервисная архитектура позволяет приложениям располагаться на площадке пользователя
- Cisco SOC предлагает удаленный мониторинг и управление в режиме 24/7



# Гибкость в работе

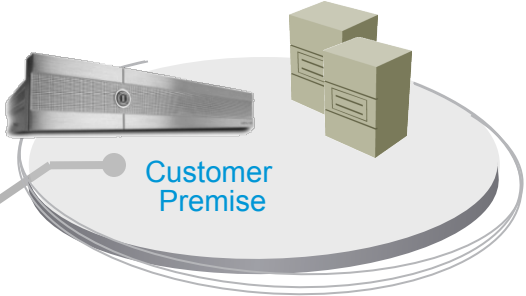
## Объединенное управление

Customer

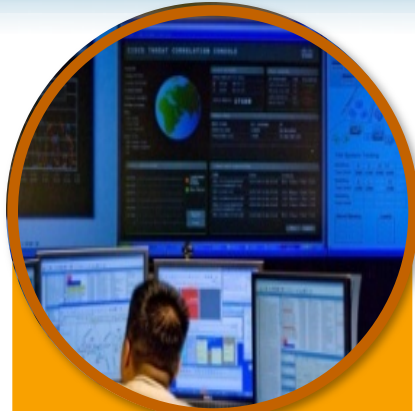
Message Tracking | Ticket Management | Reporting



Reporting



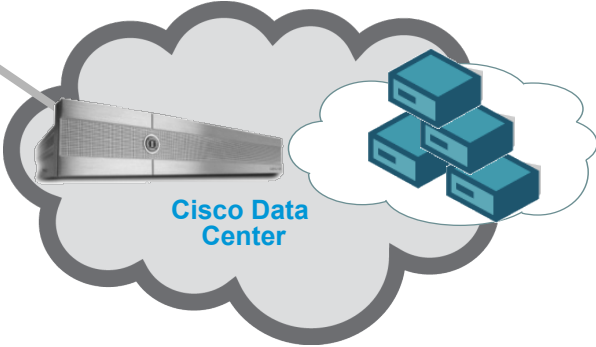
## Shared Access & Control



Cisco



Configuration



System Health | System Upgrades | Config Changes

# Облачная безопасность и Cisco

Expanding the Vision

IronPort

ScanSafe

WebEx

Шифрование



Unified Computing  
Виртуализация

Облачная  
платформа

# Оцени контент форума и получи приз!

- Призы ждут всех, кто:
  - заполнил общую анкету
  - заполнил 3 и более сессионных анкет
- Онлайн-анкеты доступны на сайте <http://vfq.com.ua>
- Анкеты также можно заполнить, воспользовавшись терминалами в зоне общения.

# Спасибо!

Просим Вас оценить эту лекцию.  
Ваше мнение очень важно для нас.

Онлайн-анкеты: <http://vfq.com.ua>

