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

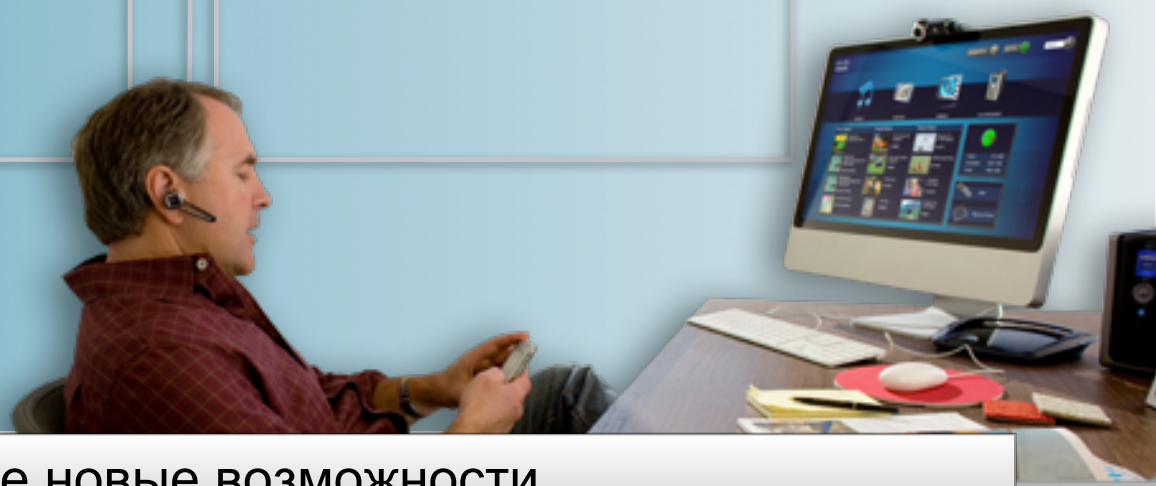
Простые и удобные средства управления

Предсказуемые OpEx

Минимальные сроки внедрения

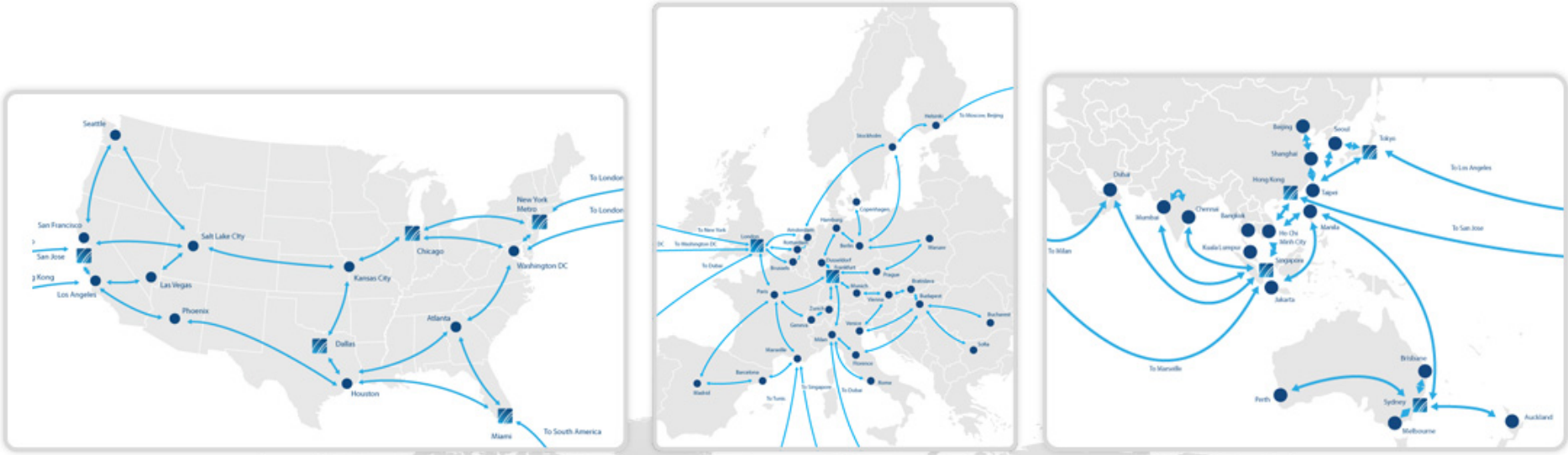
Нулевые CapEx

Освобождение ресурсов для бизнес задач



Откройте новые возможности

"Облачная" система безопасности Cisco

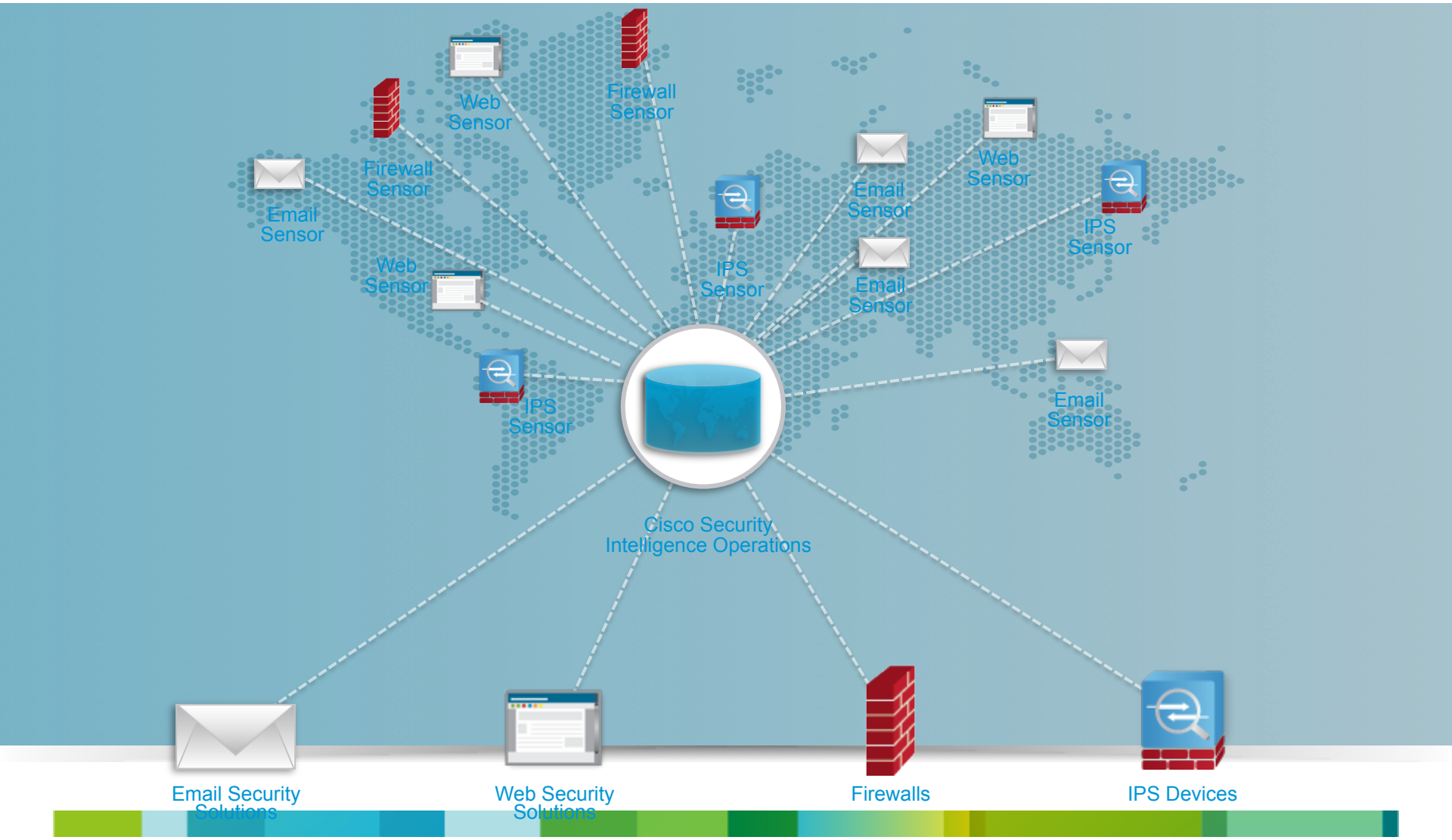


- Multi-tenant архитектура для обслуживания множества заказчиков
- Распределенная масштабируемая платформа с резервированием
- Постоянное наращивание производительности и внедрение новых ЦОД

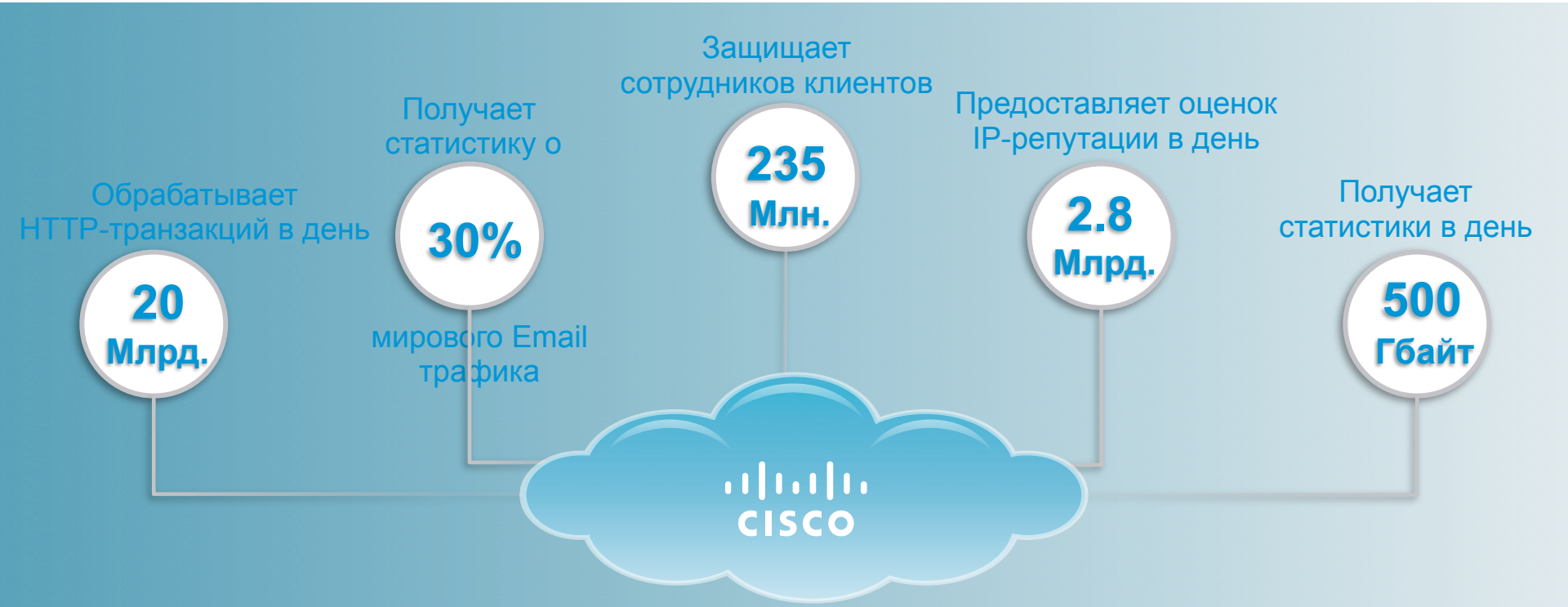
- Глобальная система мониторинга угроз
- Встроенная система управления и формирования отчетов
- Глобальная платформа для мобильных пользователей

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?

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

c|net Security product of the year 2008

SC Magazine Awards 2009 Europe; SC Magazine RDS 08; SC Magazine RDS 07

Red Herring 100 Winner Europe

Check Point OPSEC Certified

Microsoft Gold Certified Partner

CISSP

2007 SIIA CODiE Winner

Customers

Rothschild

Shell

Disney

Bacardi

ICI

Standard Chartered

Louis Vuitton

IKEA

Quintiles Transnational

Partners

orange Business Services

at&t

Google

Sprint

TELUS

NEC

Облачные услуги Cisco ScanSafe

Web фильтрация

- Контроль использования
- Просмотр приложений
- Двунаправленный контроль

Web безопасность

- Защита от malware
- Анализ Web контента
- Эмуляция скриптов

Централизованный репортинг

Мобильная безопасноть

Зона охвата глобальных ЦОД

Current Datacenters
Bangalore
Chicago
Copenhagen
Dallas
Frankfurt
Hong Kong
London
Miami
New York Metro
Paris
San Jose
Singapore
Sydney
Tokyo
Zurich

In Progress Datacenters
Brazil
Canada (E), (W)
Dubai
Mexico
South Africa

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

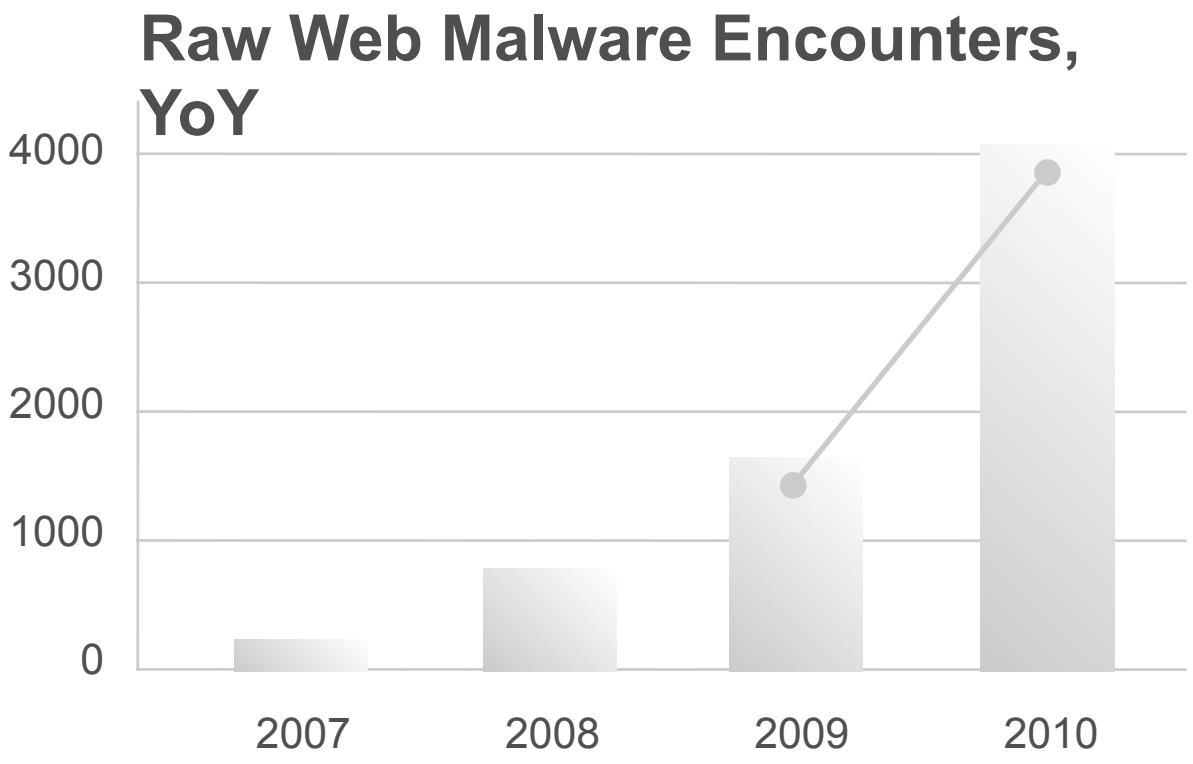
Несоответствие политик в предприятии

Потенциальные дыры в безопасности

Незавершенные системы репортинга и обзора

Web Malware продолжает расти угрожающими темпами

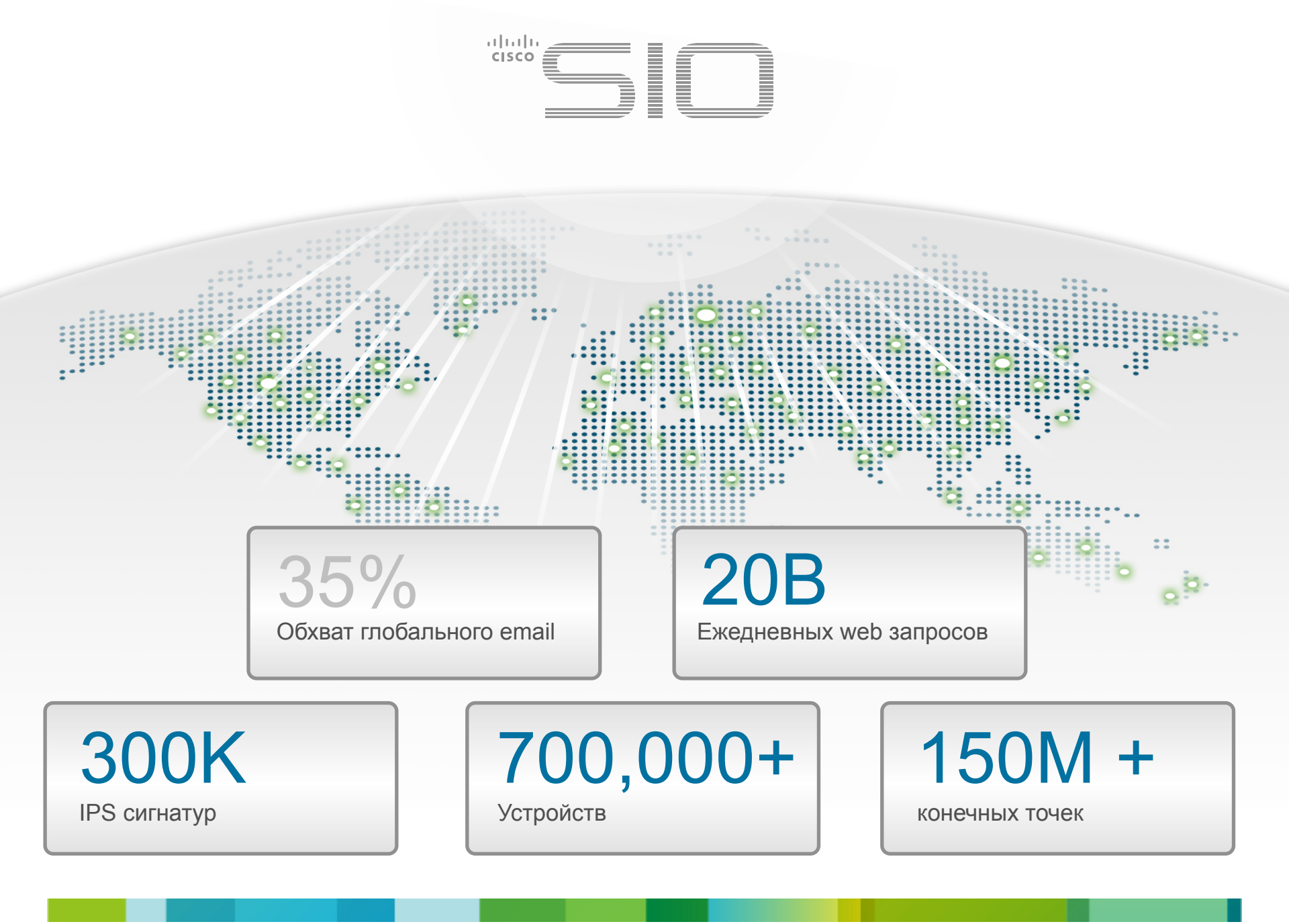
ScanSafe Focus Customer



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

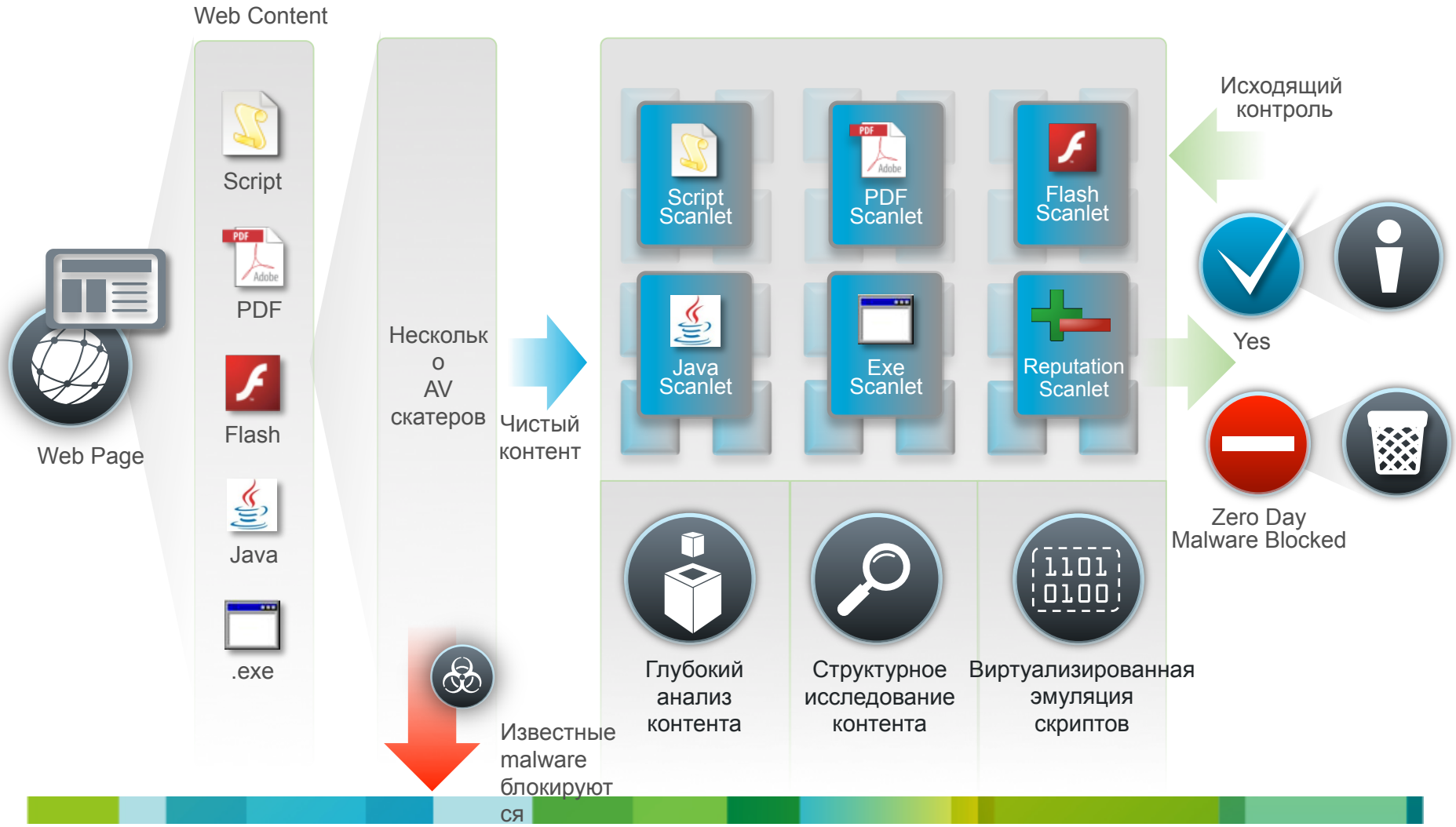
300K
IPS сигнатур

700,000+
Устройств

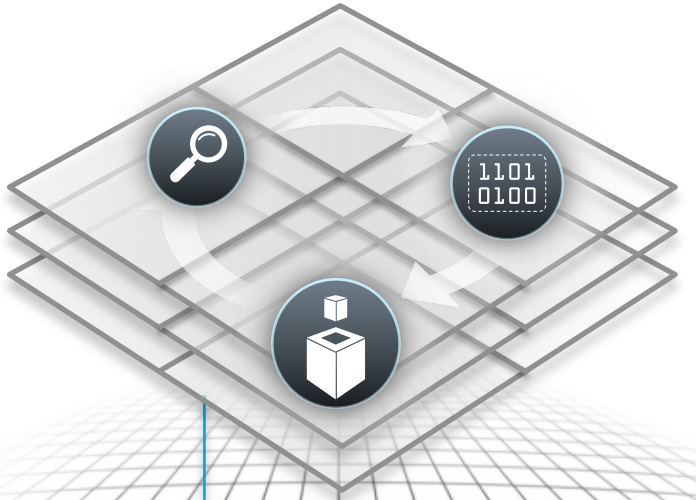
150M +
конечных точек

Архитектура защиты от атак malware 0 дня

Outbreak Intelligence



Outbreak Intelligence



Глубокий анализ контента

Структурное исследование

Эмуляция скриптов

Outbreak Intelligence

Миллиарды ежедневных запросов

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 50M узлов**
- **Динамическая категоризация**
- **Search*Ahead***

Application Visibility and Control

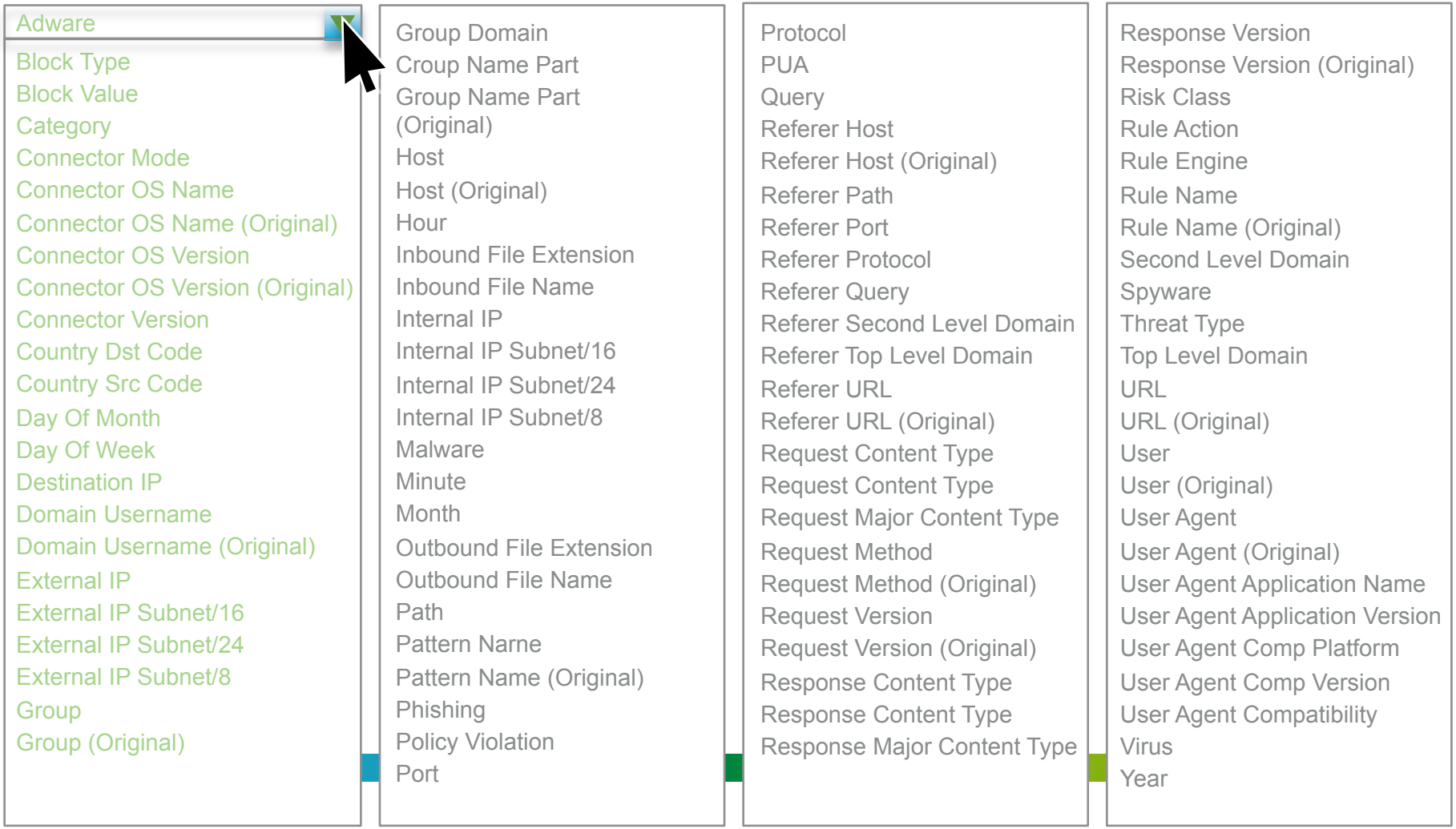
- **Контроль Web приложений, e.g., IM, Facebook, WebEx**
- **рейтинг контента**

Система репортинга ScanSafe WIRe

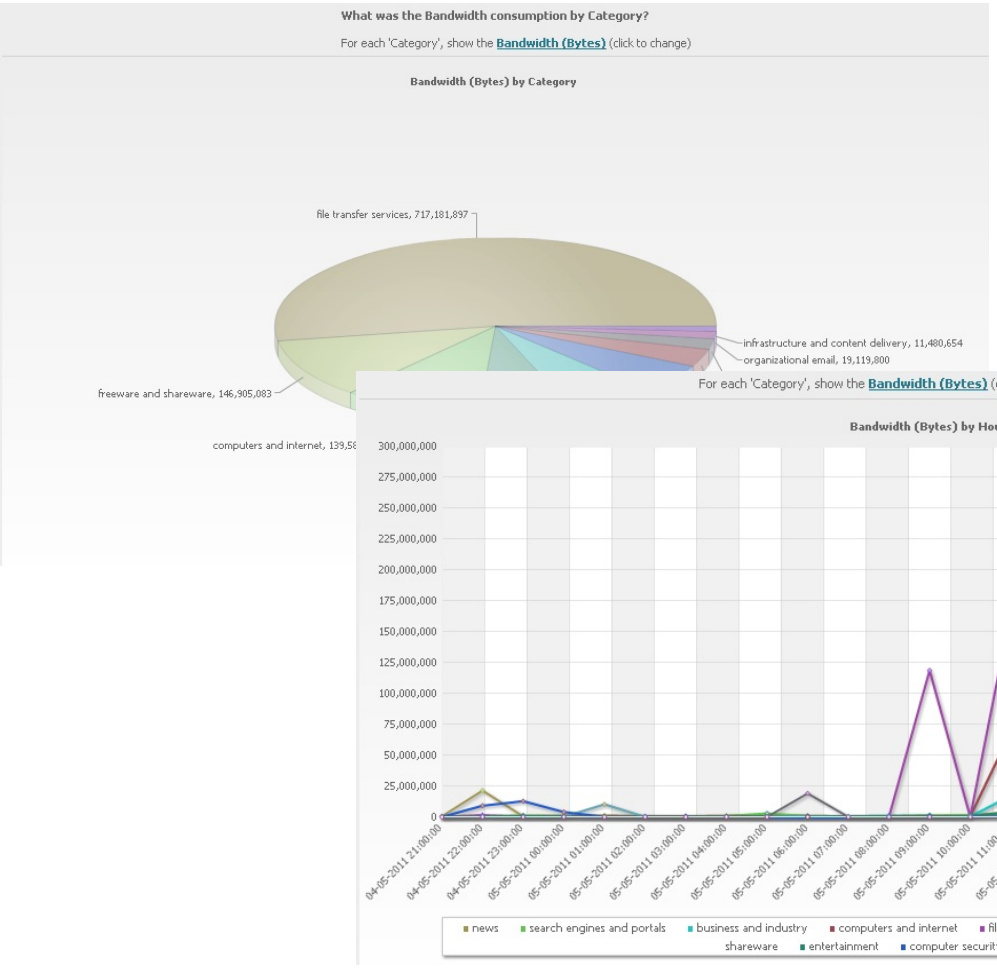
- ✓ Высокая производительность
- ✓ Глобальный охват
- ✓ Хранение данных
- ✓ Детальный просмотр
- ✓ Стоимость
- ✓ Сложность

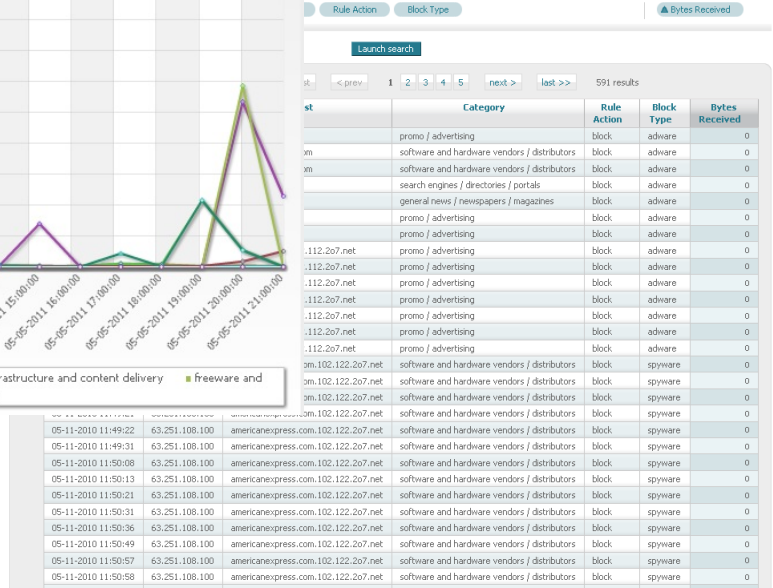
Глубина охвата

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



Обзор, тренды и проведение расследований





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

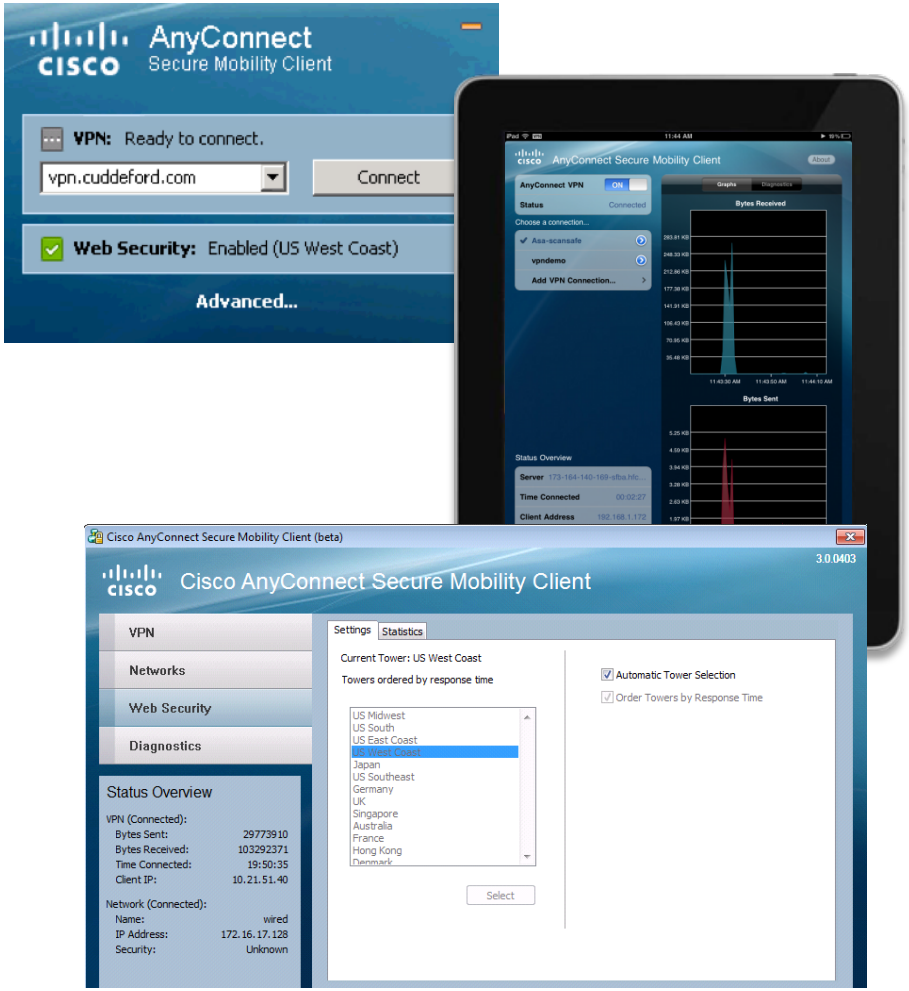
- работа даже вне VPN
- Защита от атак 0-го дня

Всесторонний

- Поддержка Windows, Mac, iPhone&iPad

Прозрачный

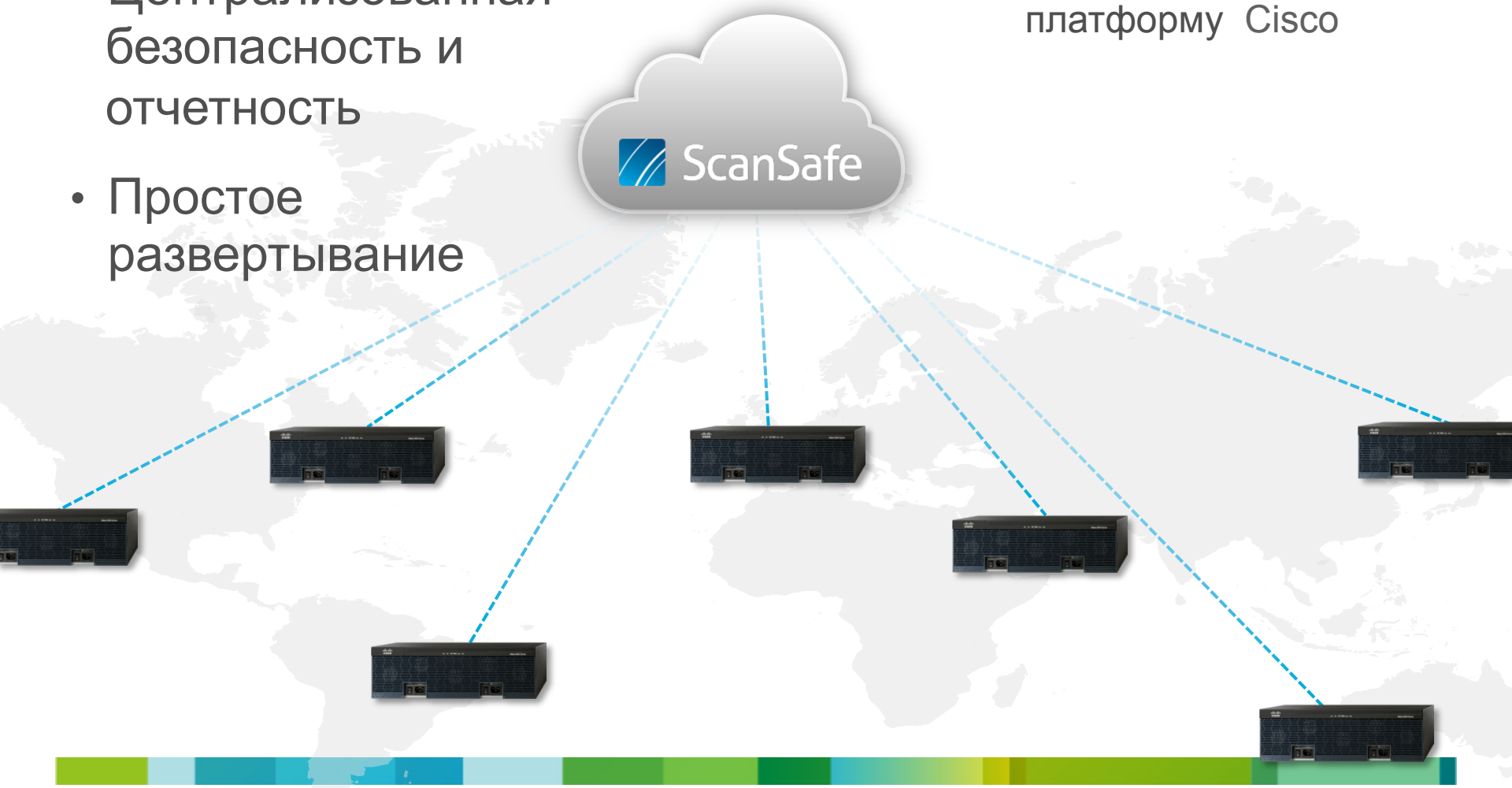
- Прозрачная работа
- Обнаружение Hotspot/Captive Portal



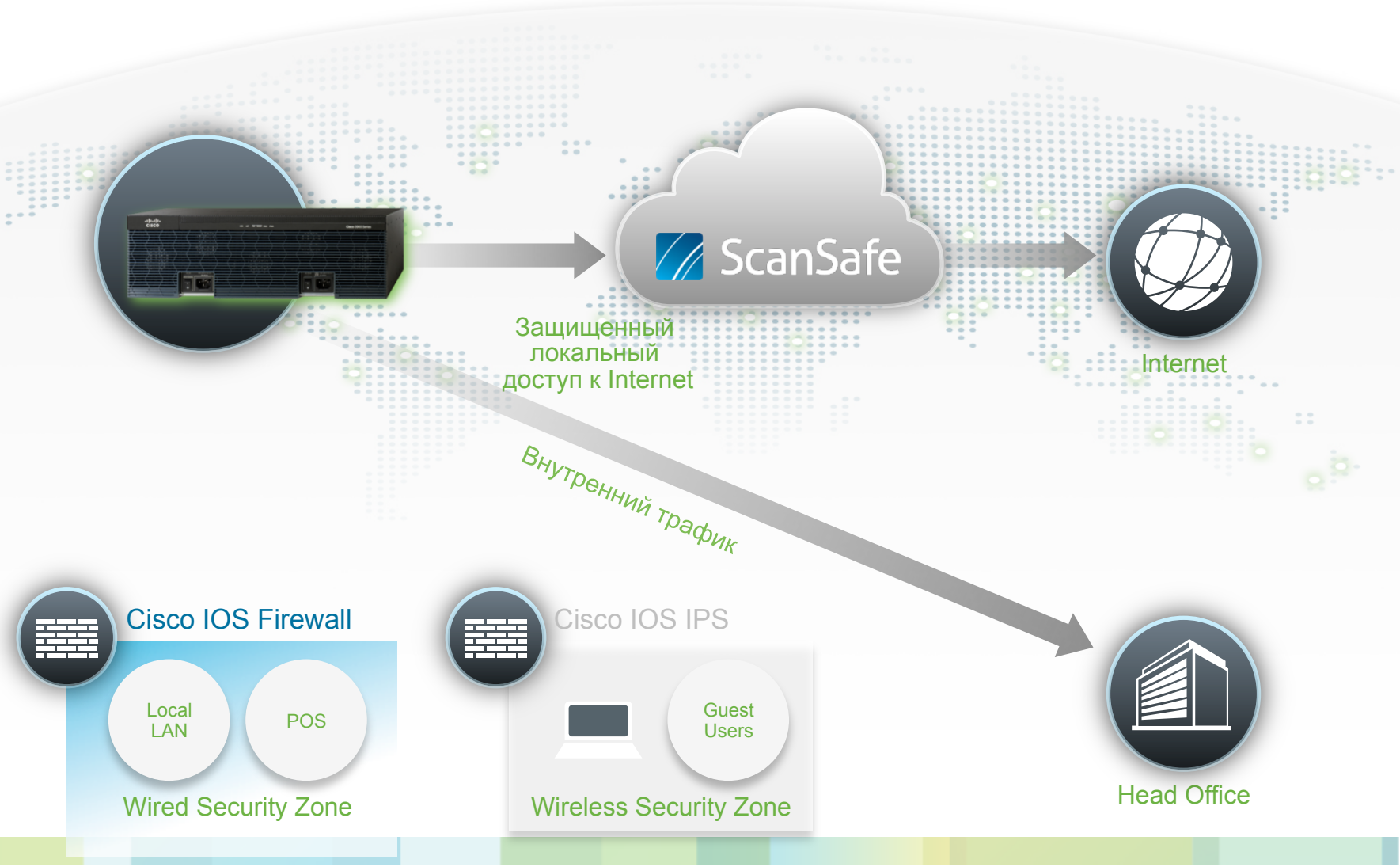
Безопасность филиалов в облаке

- Централизованная безопасность и отчетность
- Простое развертывание

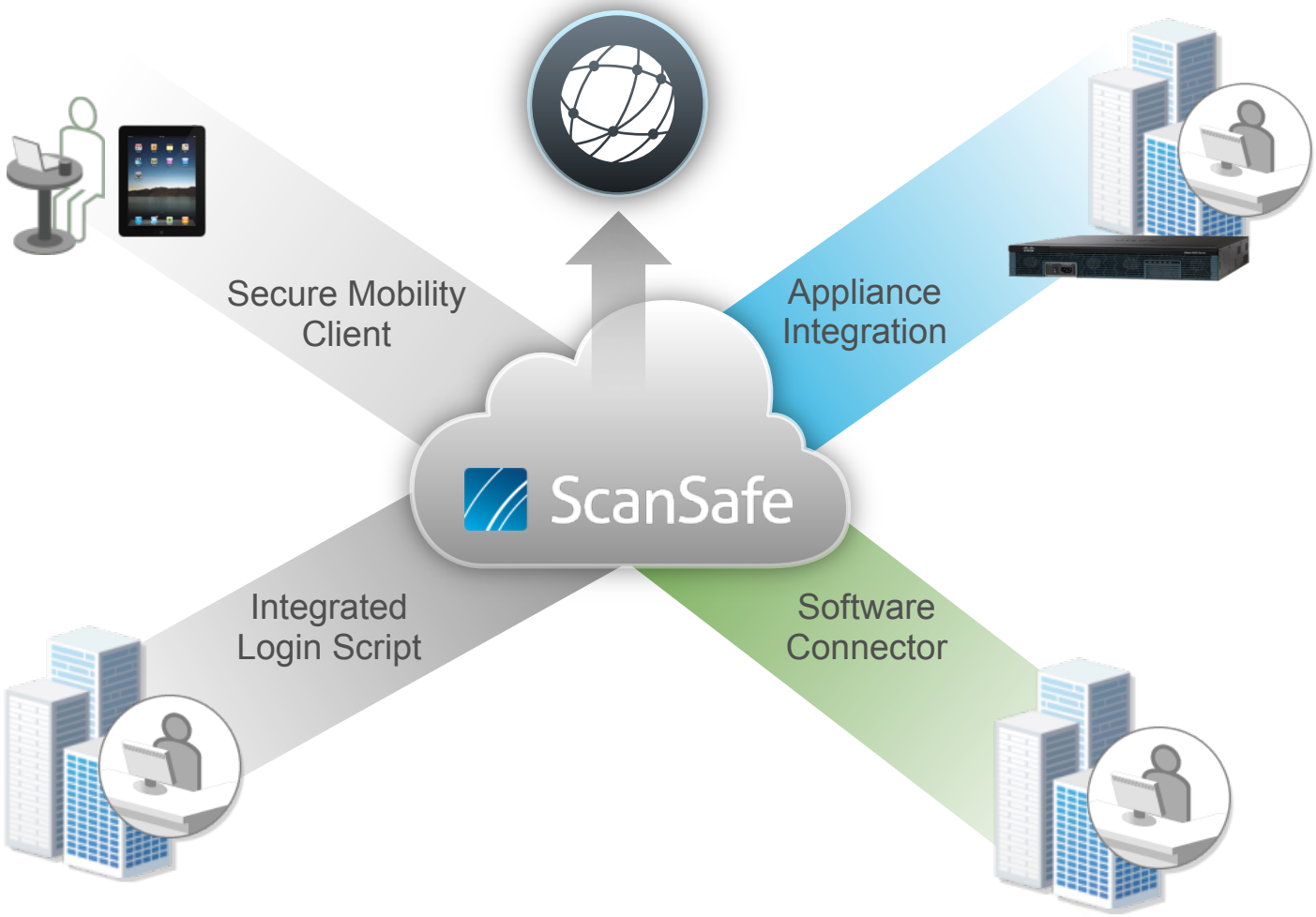
- Расширение инвестиций в платформу Cisco



ISR Web Security co Cisco ScanSafe



Выбор вариантов развертывания

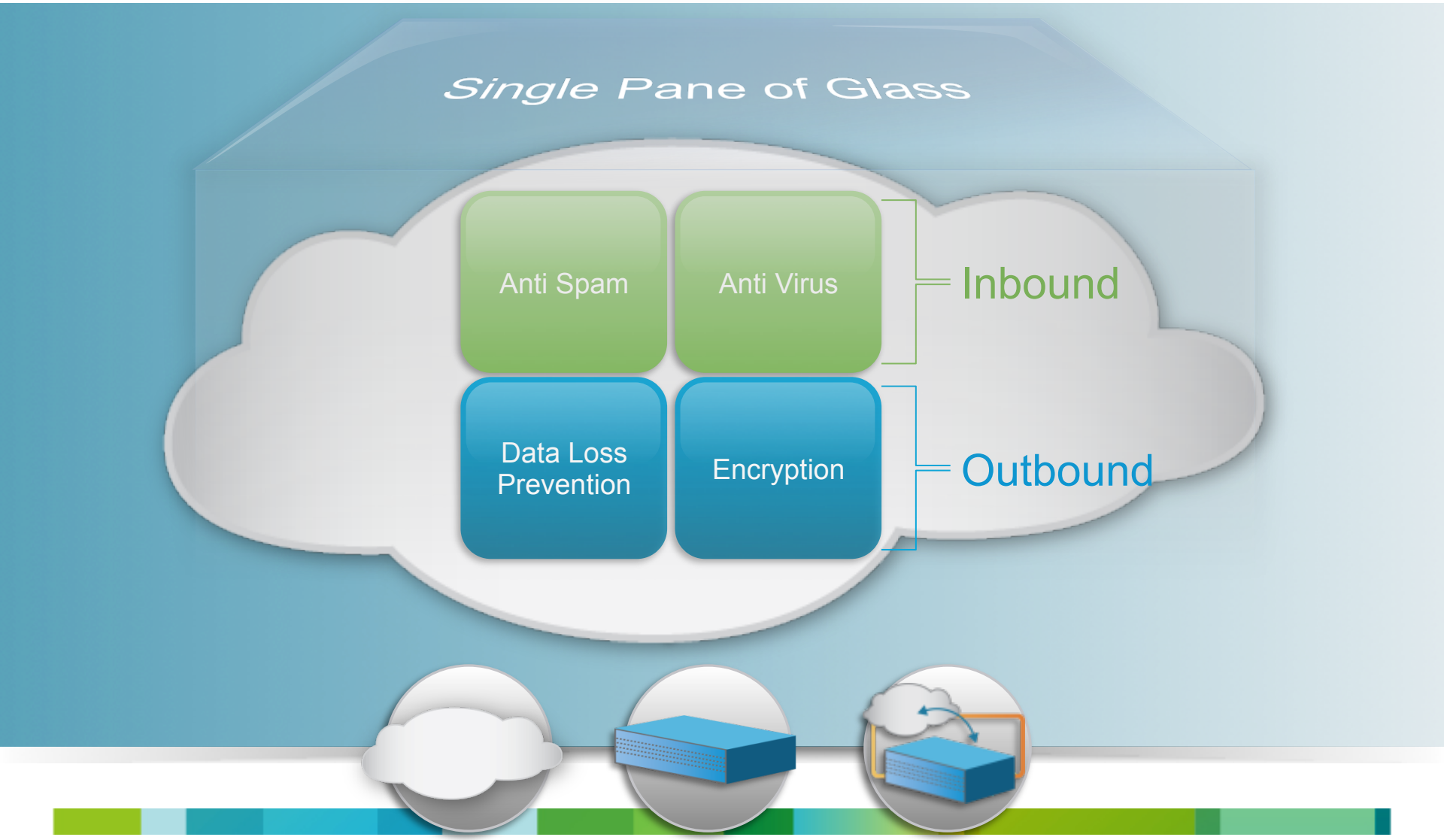


В чем преимущества ScanSafe?

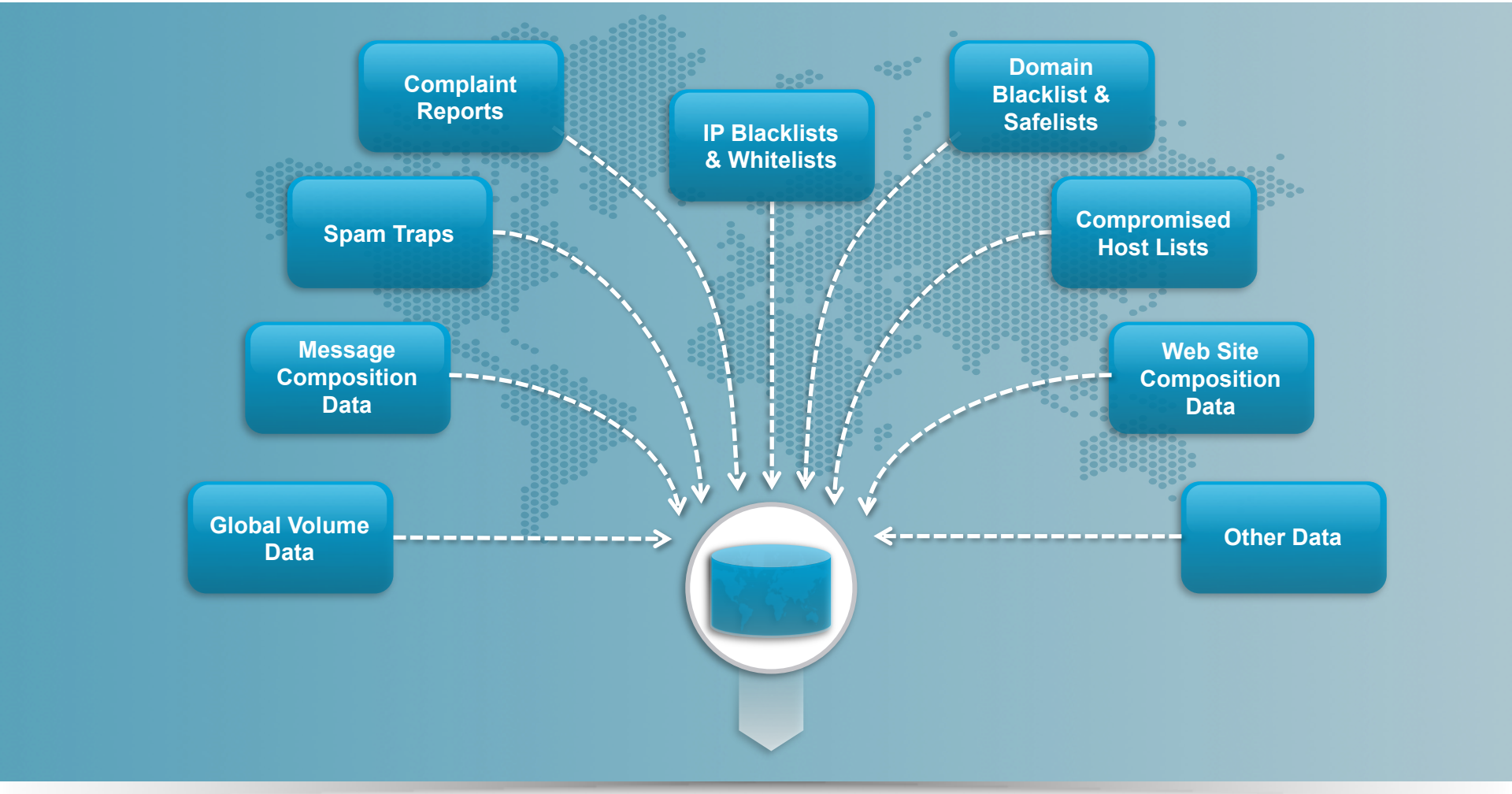
- **Защита основного канала распространения угроз**: Защиты от ВПО, ограничение доступа к сайтам по категориям, DLP, проверка HTTPS
- **Предсказуемые затраты**: переход от CapEx к OpEx
- **Для клиентов с большим кол-во филиалов**: нет необходимости покупать много устройств или пропускать весь трафик 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

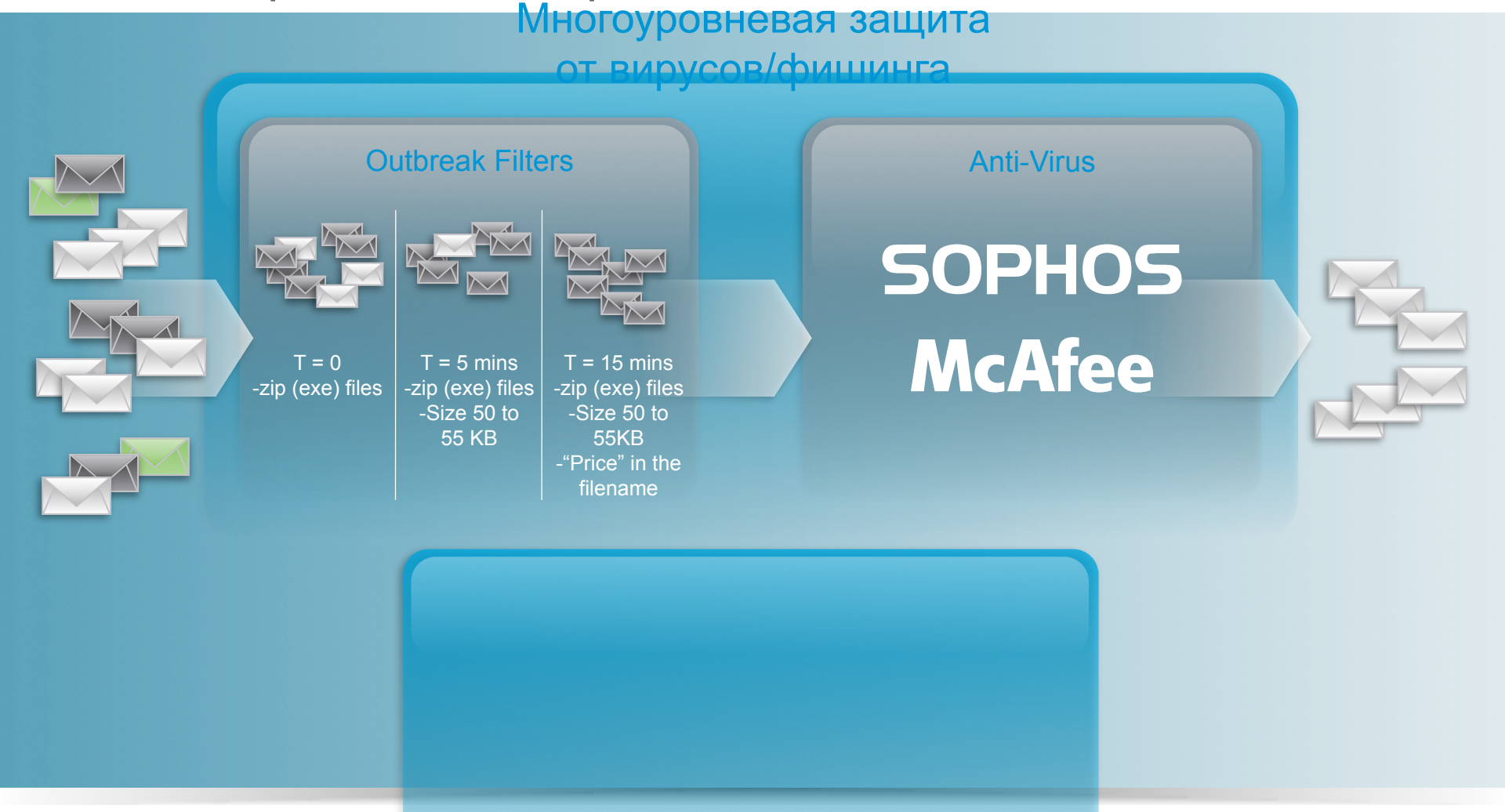


SensorBase
Email репутация

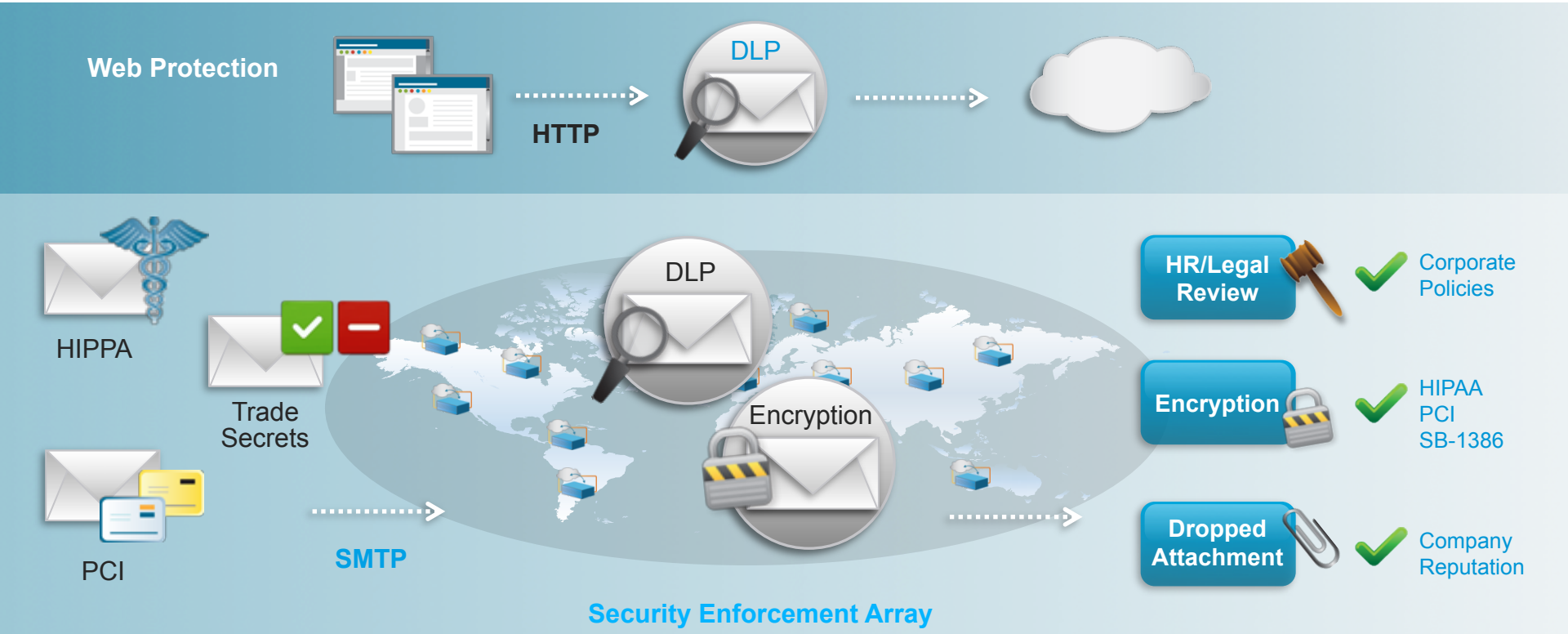


Антивирусная архитектура

Эшелонированная оборона



Управление исходящими сообщениями



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 отправено сервером, авторизованным отправлять почту для данного домена

Возможност LDAP
LDAP ссылки, несколько LDAP серверов, установка за 3 шага

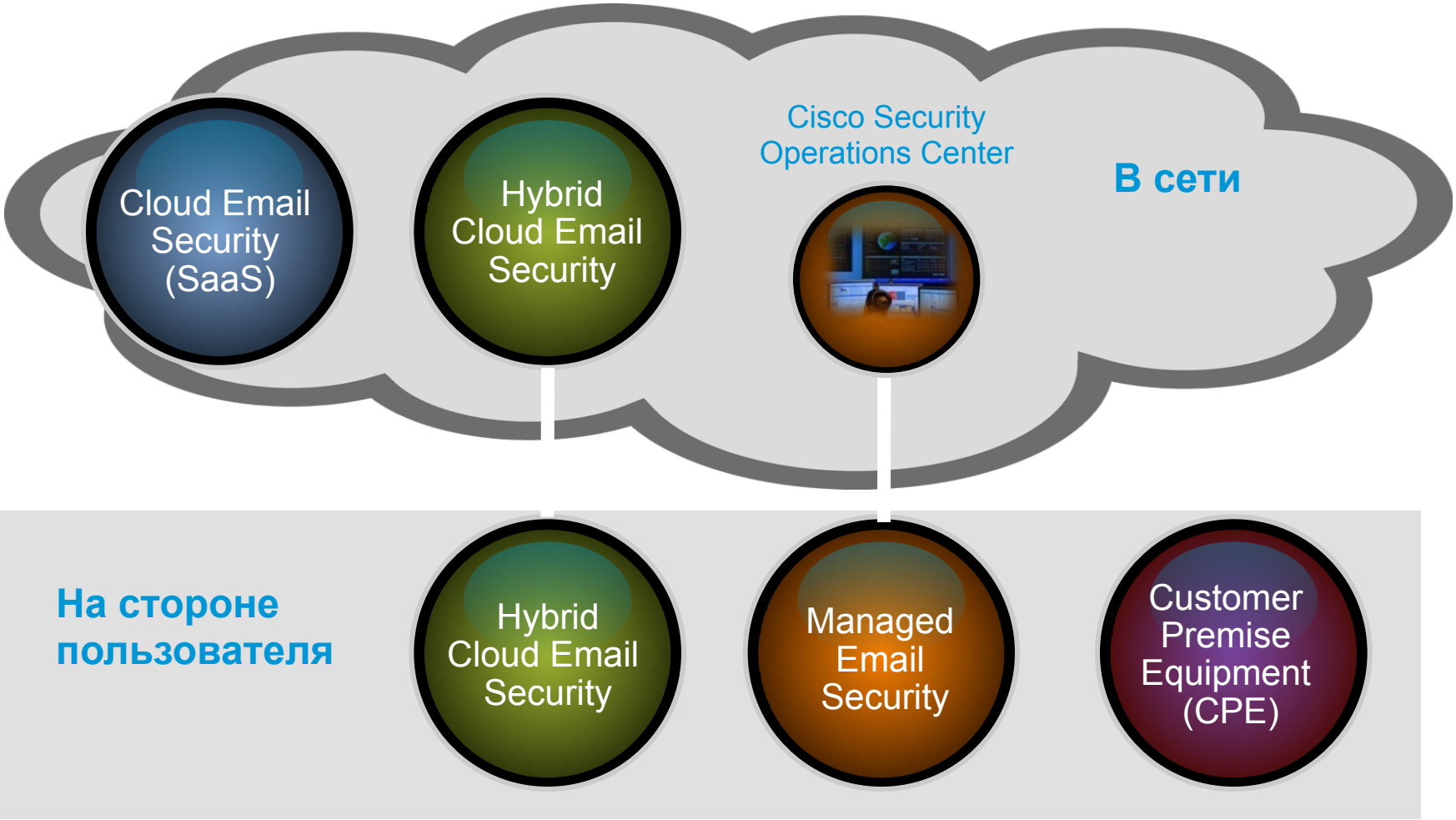
DKIM подпись и проверка
Проверка отправителя

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

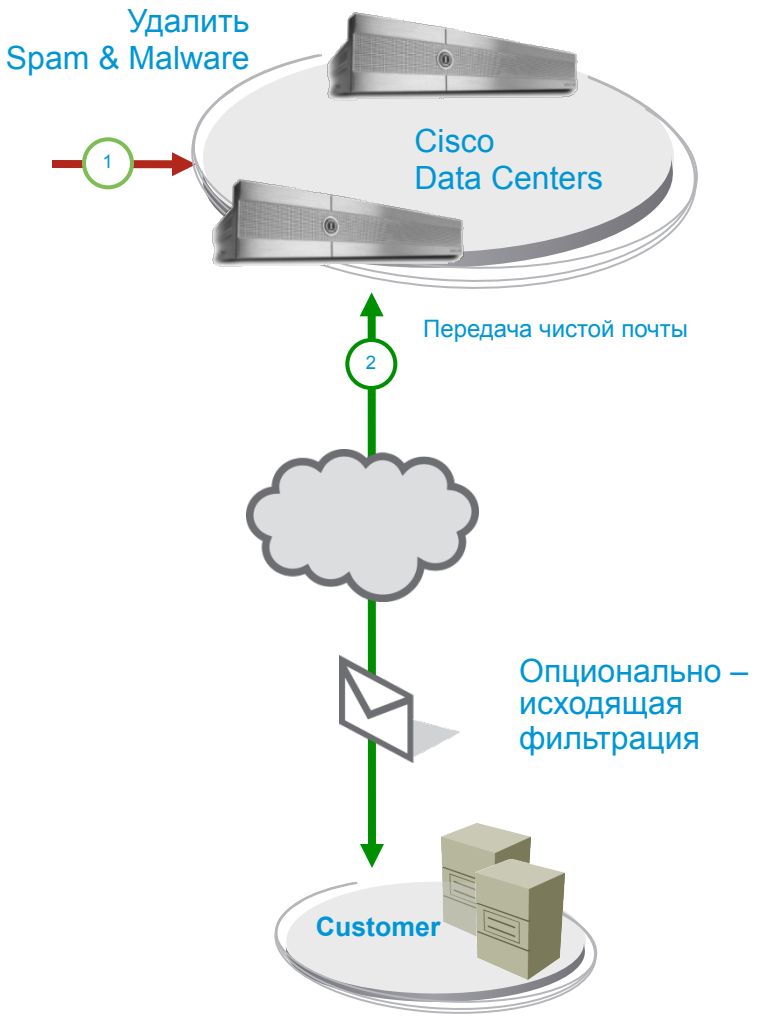


Common Policy | Centralized Reporting | Consistent Protection

Cloud Email Security

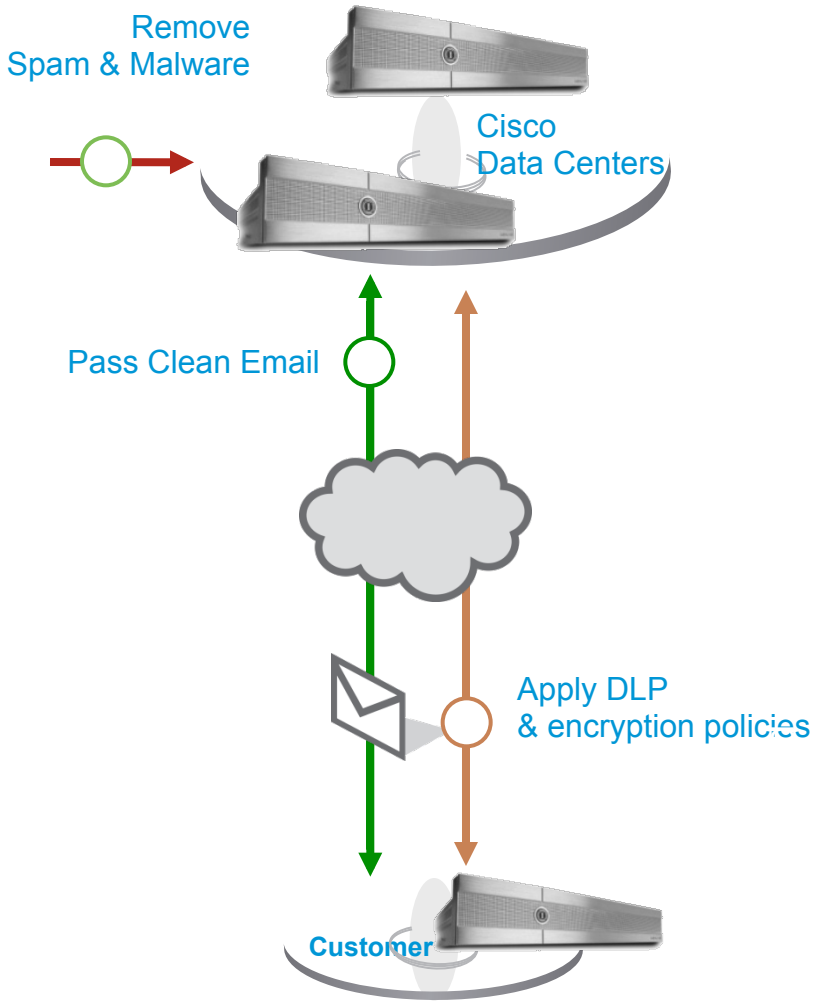
Выделенное решение снижает нагрузку и ускоряет внедрение

- Безопасностьи Email в облаке снижает нагрузку на ЦОД
- «Выделенное» решение снижает риск общего сбоя (‘shared fate’ risk)
- Управляемая инфаструктура гарантирует производительность для будущего роста



Гибридный Cloud Email Security
Оптимальный дизайн, максимальная гибкость

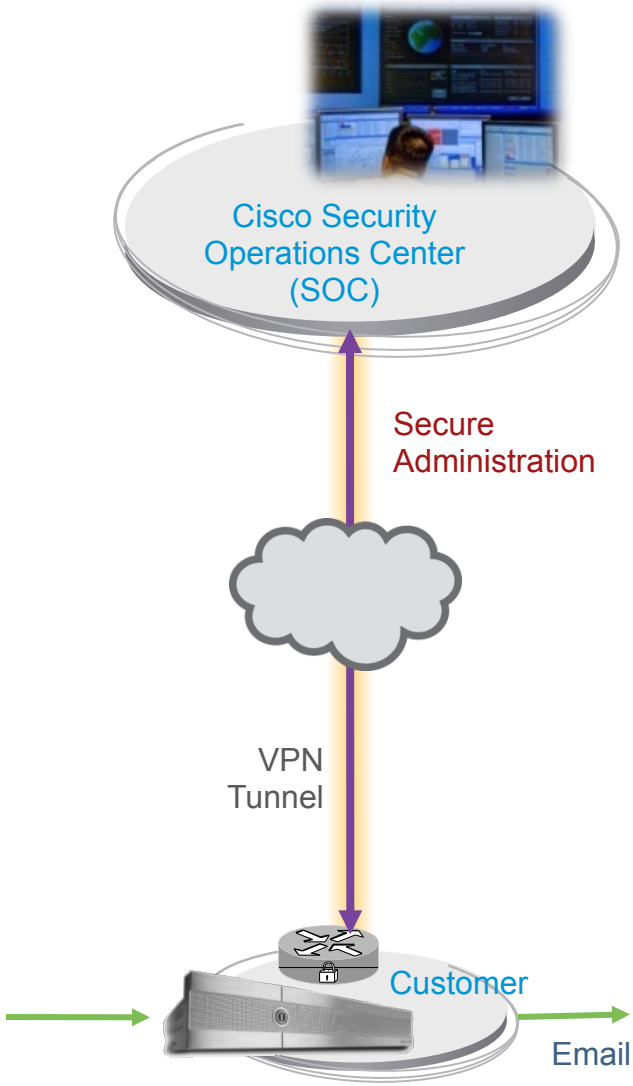
- Гибридный дизайн подразумевает разнесенное управление – на площадке и в облаке
- Устройства на площадке пользователя контролируют исходящую почту, политики DLP и шифрование



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

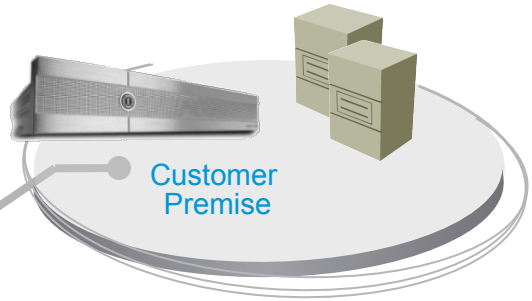


Гибкость в работе
Объединенное управление

Message Tracking | Ticket Management | Reporting

Customer

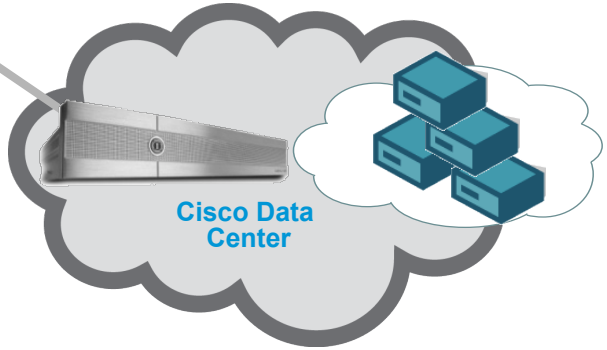
Reporting



Shared Access & Control

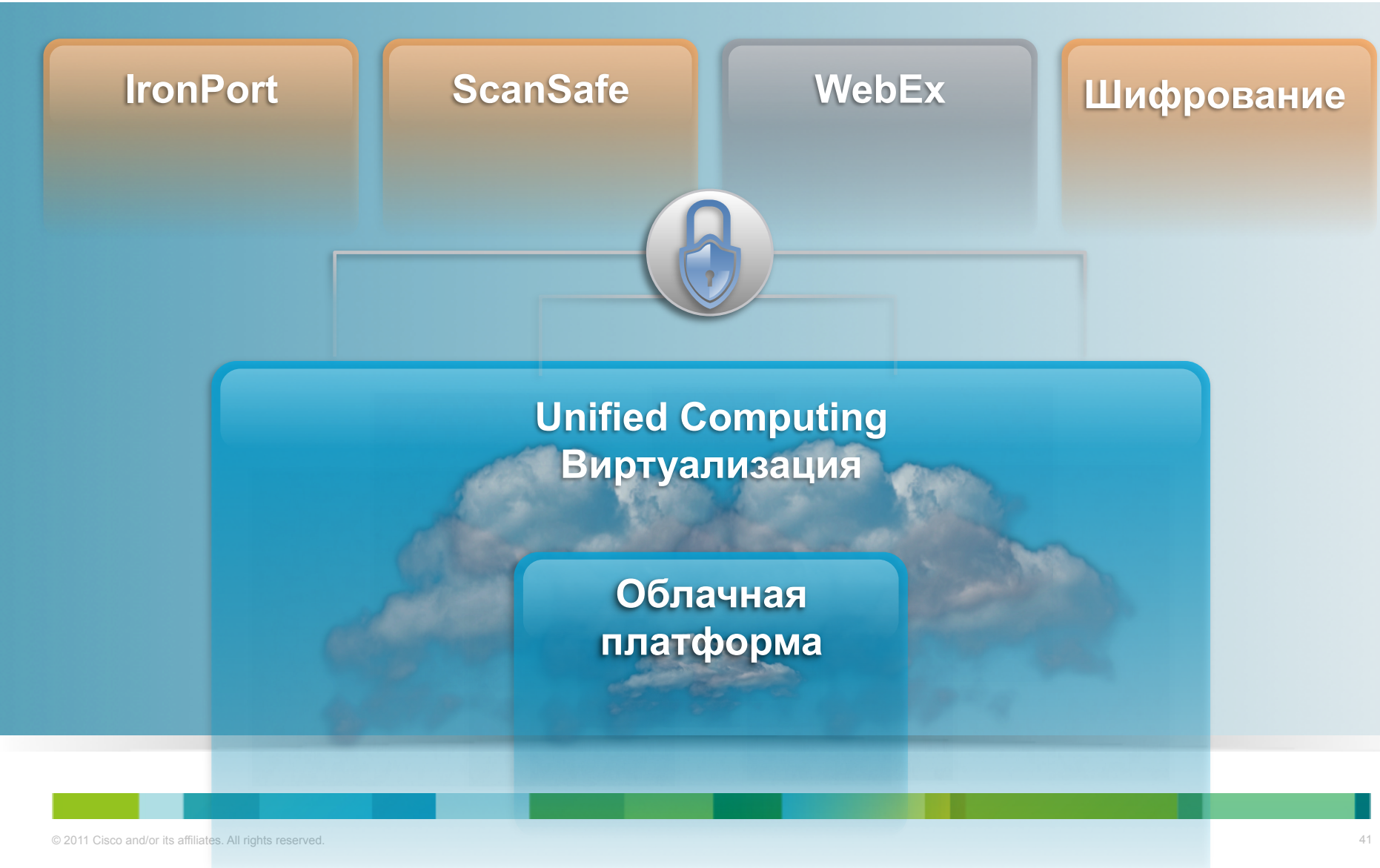
Cisco

Configuration



System Health | System Upgrades | Config Changes

Облачная безопасность и Cisco
Expanding the Vision



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