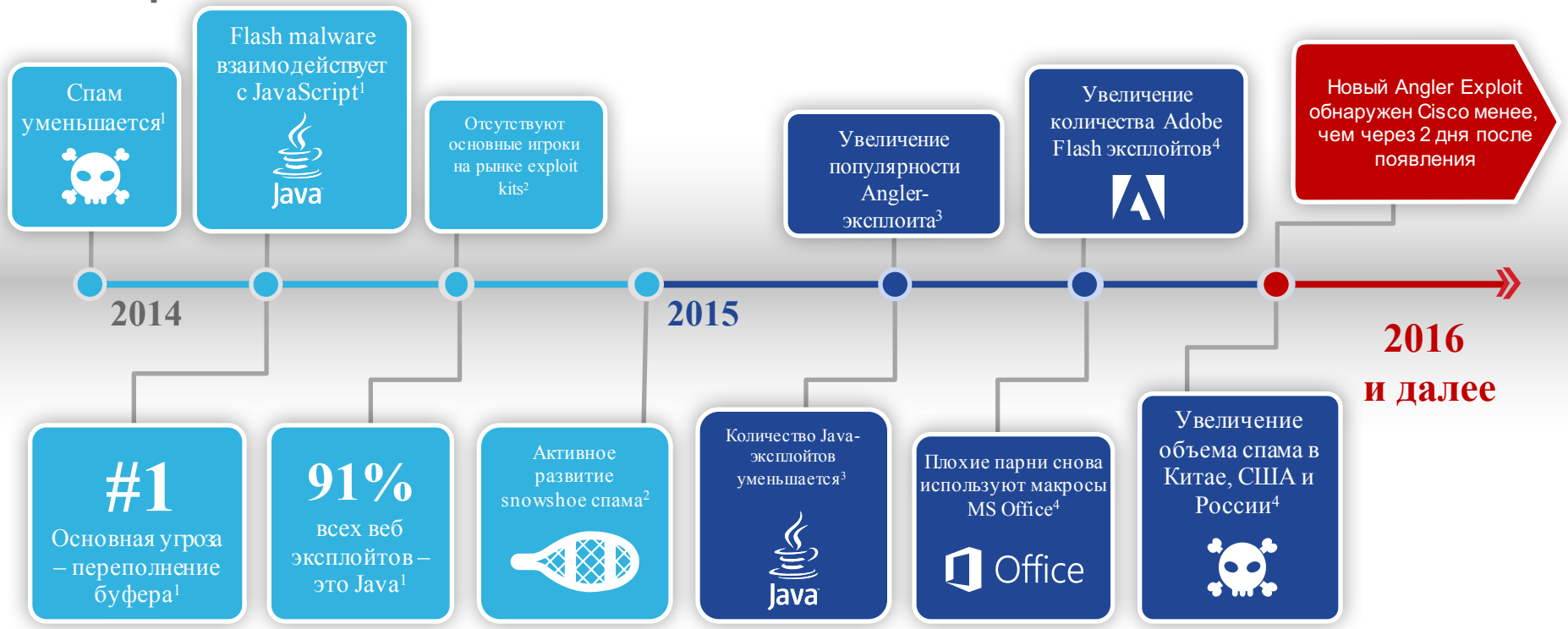
Решения Cisco по информационной безопасности

Алексей Лукацкий

Ландшафт угроз меняется с увеличивающейся скоростью



© 2015 Cisco and/or its affiliates. All rights reserved.

Source:
[1] Cisco Annual Security Report 2014
[2] Cisco Midyear Security Report 2014
[3] Cisco Annual Security Report, 2015
[4] Cisco Midyear Security Report 2015

Угрозы стали более быстрыми и гибкими, чем когда-либо

Продвинутая угроза

Ориентированные на цель, мультивекторные атаки

МИССИЯ	Мошенничество с онлайн-банками или кредитными картами, добыча Bitcoin, мошенничество с кликами,
МИССИЯ	Ransomware, информация об онлайн-банкинге
МИССИЯ	Жизненный цикл ботнет, рекламное мошенничество, malvertising, скоординированные атаки
МИССИЯ	Целевые атаки

Angler Exploit

Angler Exploit

40%
успешность

100%
увеличение инфицированных в 2015

- Развертывание скрытых опорных страниц
- Использование эксплойтов, таких как flash, для проникновения в компьютер
- Интеллектуально меняет технику для того, чтобы избежать обнаружения

© 2015 Cisco and/or its affiliates. All rights reserved.

И влияние бреши на безопасность имеет далеко идущие последствия

данных похищается в течение часов[1]

$3.8M

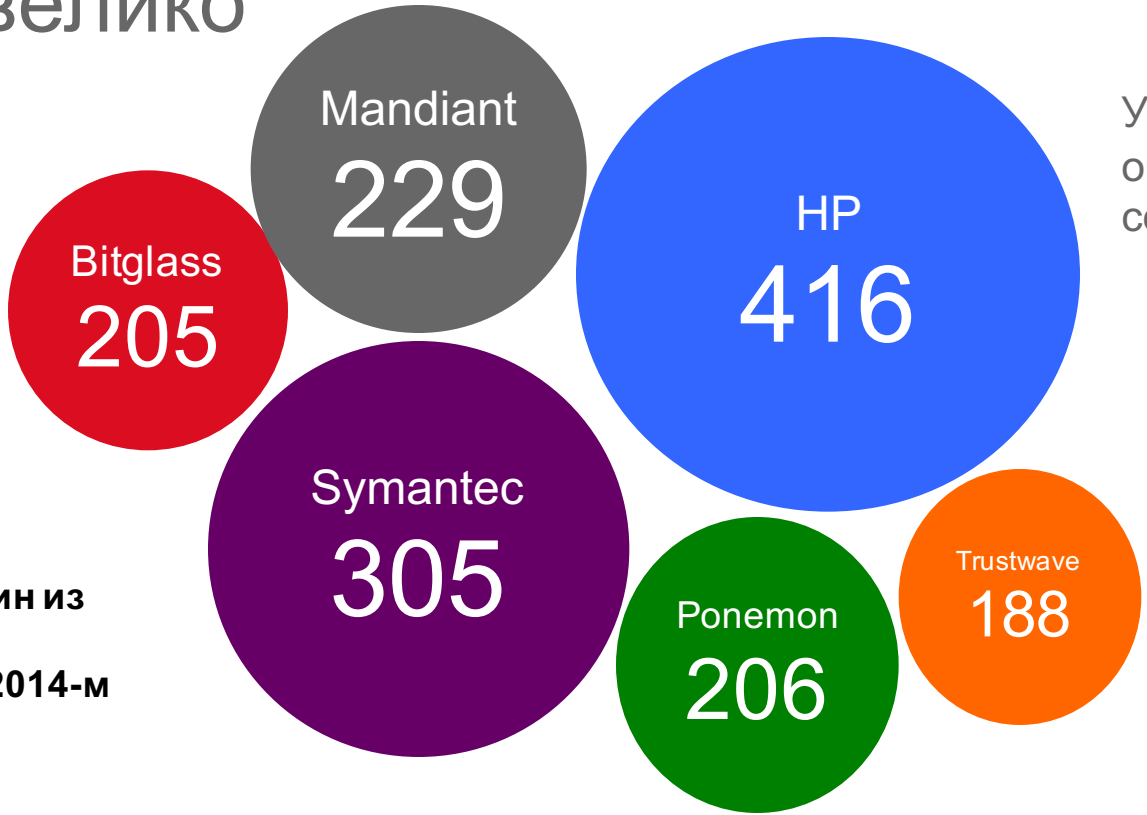
долларов тратятся на ликвидацию последствий бреши [2]

брешей не могут быть обнаружены **месяцами**[1]

Source:
[1] http://www.cisco.com/web/offer/emear/38586/images/Presentations/P16.pdf
[2] Ponemon Institute, 2015 Global Cost of Data breach

© 2015 Cisco and/or its affiliates. All rights reserved.

Время обнаружения целенаправленных угроз велико

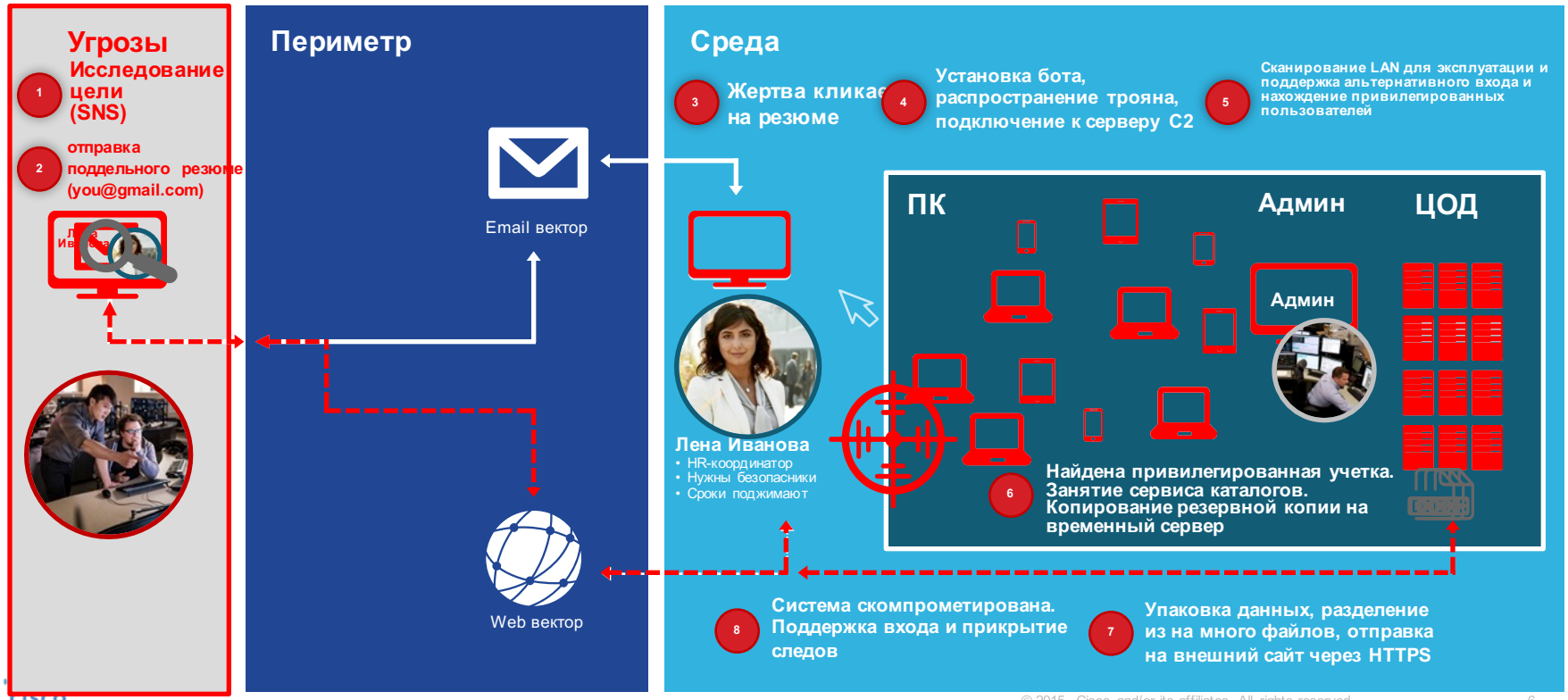


У Cisco время обнаружения (TTD) составляет 17 часов

2287 дней – один из самых долгих инцидентов в 2014-м году

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Продвинутые угрозы легко распространяются по старым сетевым инфраструктурам

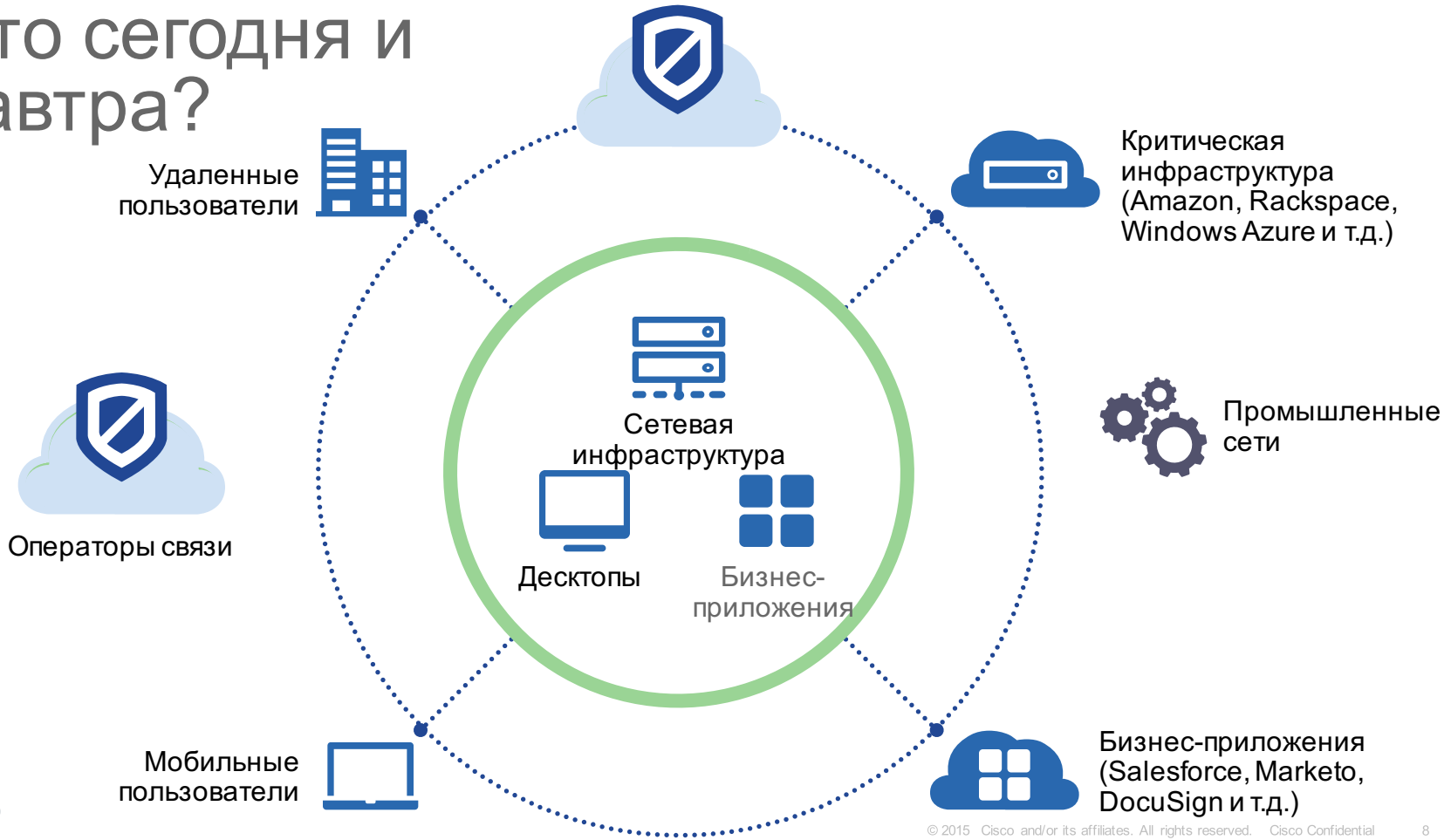


© 2015 Cisco and/or its affiliates. All rights reserved.

Так было в прошлом

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Что сегодня и завтра?



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Много систем безопасности не поддерживаются в актуальном состоянии

© 2015 Cisco and/or its affiliates. All rights reserved.

С функциями для реагирования на продвинутые угрозы

ДО	ВО ВРЕМЯ	ПОСЛЕ
Глобальная информация об угрозах	Сигнатуры, антивирус, антиспам, аномалии	Песочницы и ретроспектива
Web/Email репутация	URL фильтрация	Анализ угроз и IoC
DNS и IP фильтрация	Репутация файлов и узлов	Динамическая сегментация
Сегментация	Обнаружение эксплойтов	Исполняемая информация

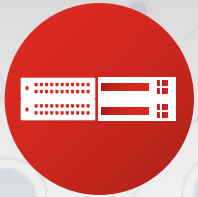
© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco защищает на протяжении всего цикла атаки

ASA NGFW	FirePOWER NGIPS и WIPS	Lancope Stealthwatch
ISE & TrustSec	WSA и CWS	Threat Grid
AnyConnect	ESA	Cognitive Threat Analytics
OpenDNS Investigate	Cloud Access Security	OpenDNS Investigate и CTA
	Advanced Malware Protection	
OpenDNS Umbrella		
Talos		

Разные варианты реализации

ПО



Физическое

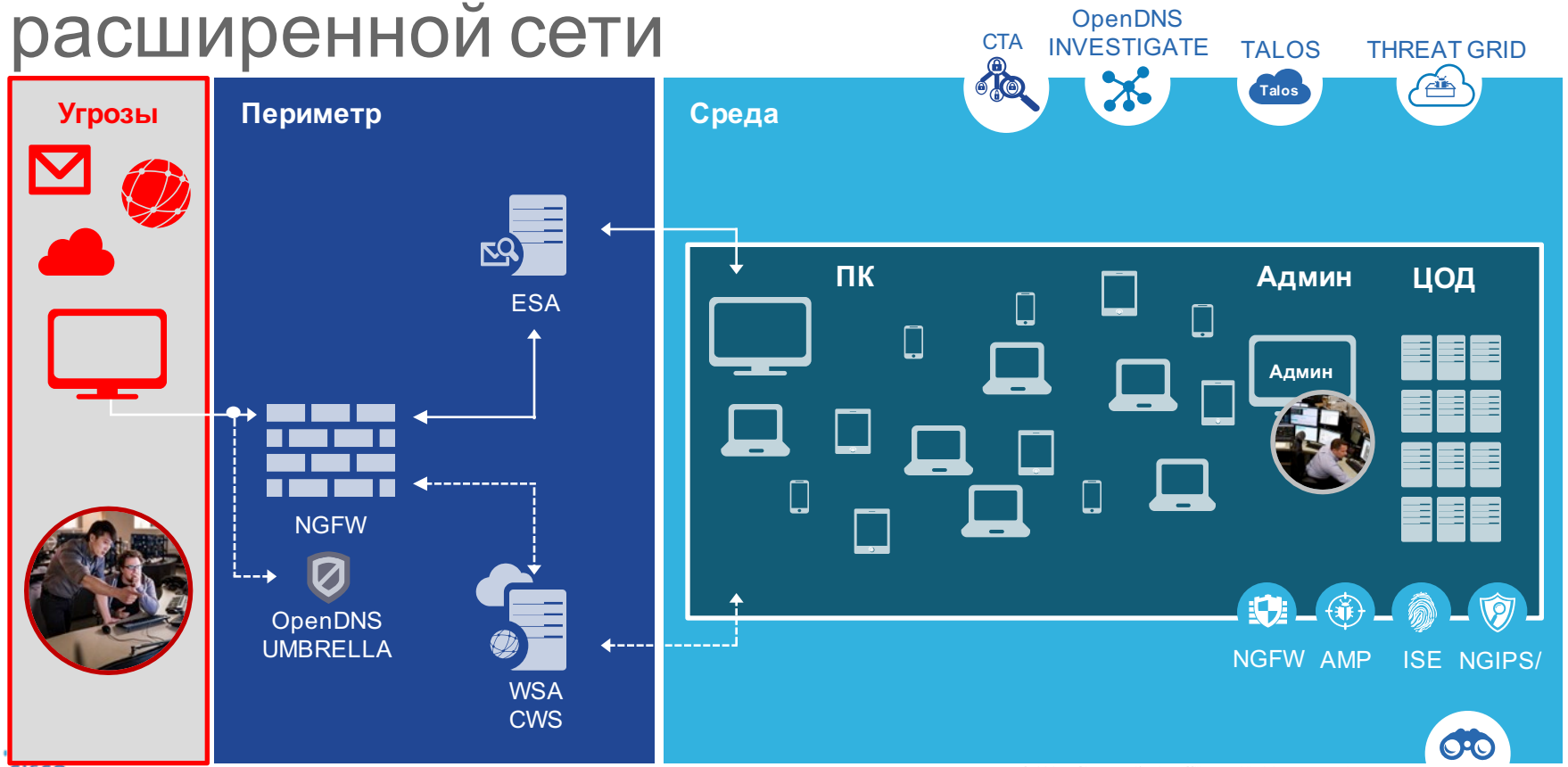
Виртуальное

Облачное
(как сервис)

Единые функции | Открытые API | Гибкое лицензирование

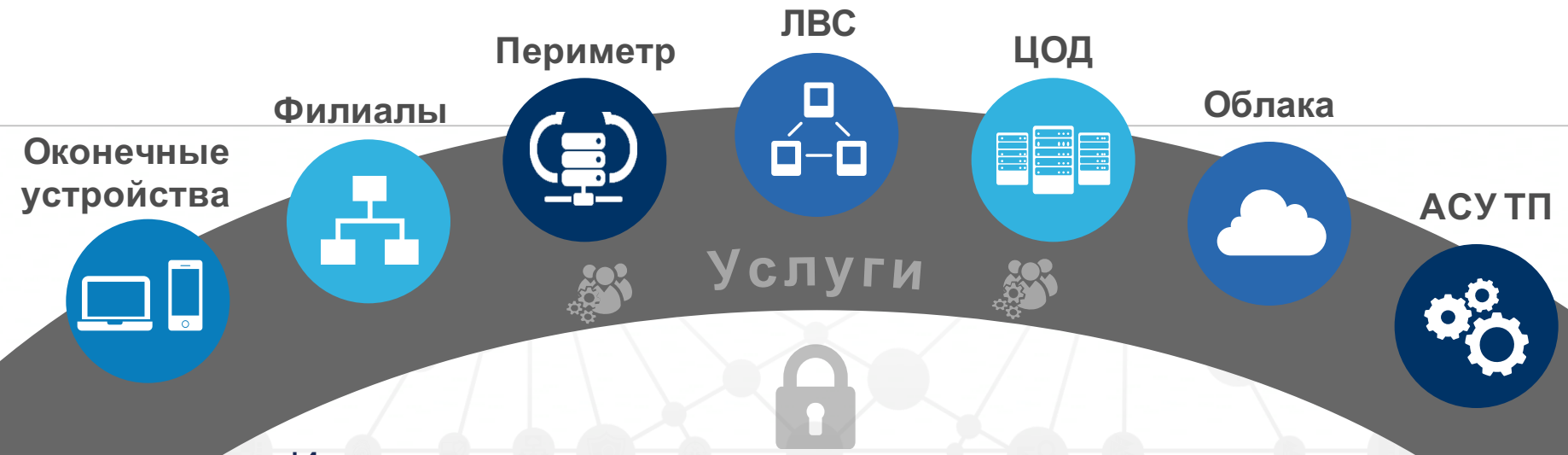
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

И интегрированными решениями по всей расширенной сети



© 2015 Cisco and/or its affiliates. All rights reserved.

Повсеместная безопасность

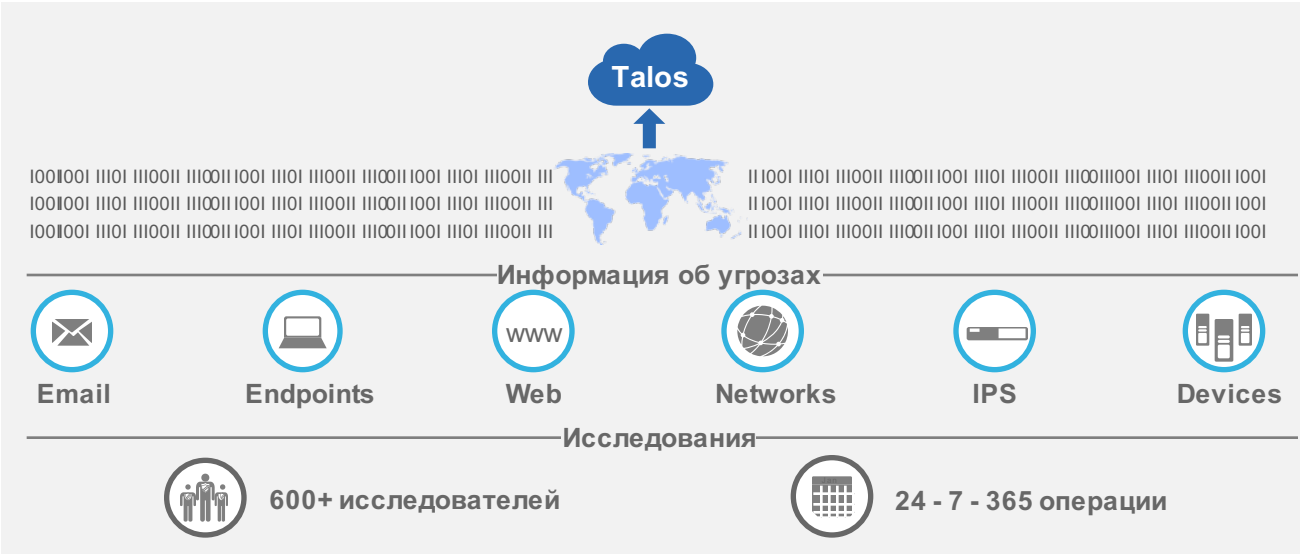


Интеграция и максимальное покрытие от уровня сети до оконечных устройств, от ЦОДов до облаков, от ЛВС до промышленных сегментов
– ДО, ВО ВРЕМЯ и ПОСЛЕ

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Начнем с наиболее интеллектуальной защиты от угроз

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection



Быть уверенными
Talos идентифицировал сеть “Kyle/Stan, “String of Paerls”, и “Angler” exploits раньше, чем кто-либо другой

Обнаружить угрозы, которые не может обнаружить компьютер
600+ исследователей на нашей стороне ищут новые продвинутые угрозы

Получить информацию об угрозах, которая связана с вашим бизнесом
Получить локализованную и специфичную информацию об угрозах, так как Talos глобально агрегирует миллионы источников информации.

Постоянно быть обновленным
Получить автоматические обновления каждые 3-5 минут на все ваши устройства

© 2015 Cisco and/or its affiliates. All rights reserved.

В центре внимания Cisco — анализ угроз!

Приобретение компании Sourcefire Security
- Ведущие в отрасли СОПВ нового поколения
- Мониторинг сетевой активности
- Advanced Malware Protection
- Разработки отдела по исследованию уязвимостей (VRT)
- Инновации в ПО с открытым исходным кодом (технология OpenAppID)

Коллективные исследования Cisco – подразделение Talos по исследованию и анализу угроз
- Подразделение Sourcefire по исследованию уязвимостей — VRT
- Подразделене Cisco по исследованию и информированию об угрозах — TRAC
- Подразделение Cisco по безопасности приложений — SecApps

Приобретение компании Lancope
- Исследования угроз

AMP + FirePOWER
AMP > управляемая защита от угроз

Cognitive + AMP

Коллективный анализ вредоносного кода > Система коллективной информационной безопасности

Приобретение компании Cognitive Security
- Передовая служба исследований
- Улучшенные технологии поведенческого анализа в режиме реального времени

Приобретение компании ThreatGRID
- Коллективный анализ вредоносного кода
- Анализ угроз
- «Песочница»

Приобретение компании OpenDNS
- Анализ DNS/IP-трафика
- Анализ угроз

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

5 департаментов Talos

80 МЛРД

DNS-запросов в день

18.5 МЛРД

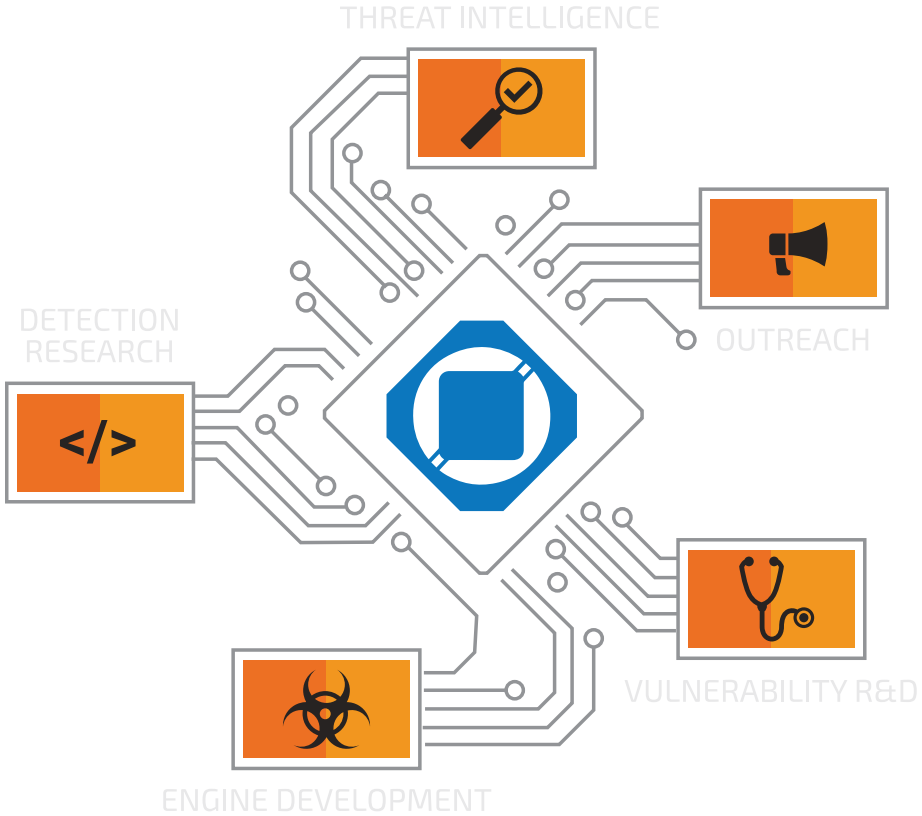
Файлов в день

16 МЛРД

Web-запросов в день

500 МЛРД

сообщений email в день



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Усилить и защитить сети от продвинутых угроз

- Global Intelligence
- **NGIPS & NGFW**
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

© 2015 Cisco and/or its affiliates. All rights reserved.

Введение в устройства Firepower NGFW

- Global Intelligence
- **NGIPS & NGFW**
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

Модульный

Выгоды
- Стандартная и возможностью взаимодействия
- Гибкая архитектура

Свойства
- Безопасность, основанная на шаблонах
- Защищенные контейнеры для пользовательских приложений
- Restful/JSON API
- Внешнее оркестрация/управление

Сверхвысокая производительность

Свойства
- Полный набор устройств
- Ведущая производительность (9000 Series)
  - 240 Gb пропускная способность
  - 30 Gb+ на поток
  - Задержки менее 5 мкс
  - 10G/40G I/O; 100G готовность
  - Терабитный backplane
  - Кластеризация до 5 устройств для получения 1.2 Тбит/с мощности

Многосервисная безопасность

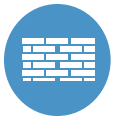
Выгоды
- Интеграция лучшей безопасности
- Динамическое объединение сервисов
- Поддержка любой сети, от низконагруженной, высокозагруженной, ЦОД, SP

Свойства*
- Контейнеры Firepower Threat Defense
  - NGIPS, AMP, URL, Приложения, Visibility & Control (AVC)
- ASA контейнер
  - Stateful FW, Virtual Private Network (VPN), CGNAT
- Другие контейнеры
  - Radware DDoS
  - Другие партнеры экосистемы

© 2015 Cisco and/or its affiliates. All rights reserved.

Введение в устройства Firepower NGFW

- Global Intelligence
- **NGIPS & NGFW**
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection



NGFW

Блокирование и мониторинг неавторизованного доступа и активности на L2-7

NGIPS

Обнаружение, предотвращение и реагирование на угрозы сети в режиме реального времени.

AMP

Идентификация и нацеливание на бреши и malware для анализа и реагирования

URL фильтрация

Ограничение доступа к определенным узлам и подузлам, как и к категориям веб сайтов.

VPN

Защита удаленных пользователей и подключений узел-узел с детальным контролем.

Third Party

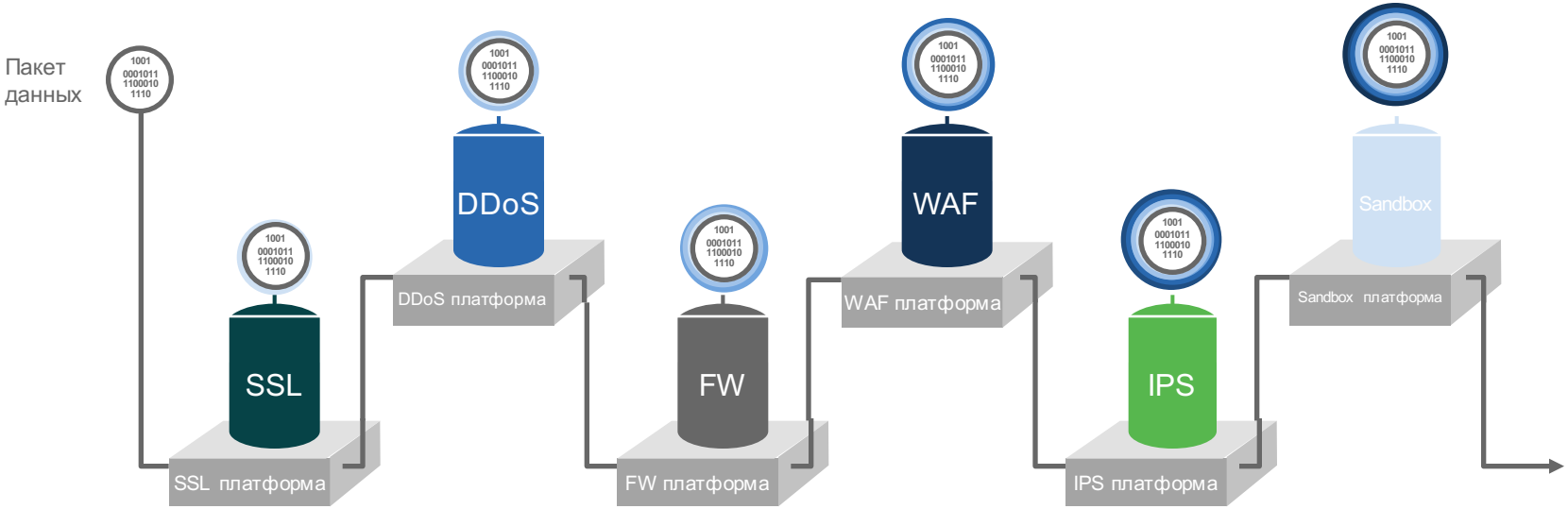
Открытый API позволяет применять диапазон дополнительных инструментов для настраиваемой защиты.

Integrated Intelligent Services Framework

Интеллектуальная обработка для более эффективного обнаружения, высокой производительности и упрощенного управления.

© 2015 Cisco and/or its affiliates. All rights reserved.

Традиционная безопасность: разрозненные, неэффективные, дорогие



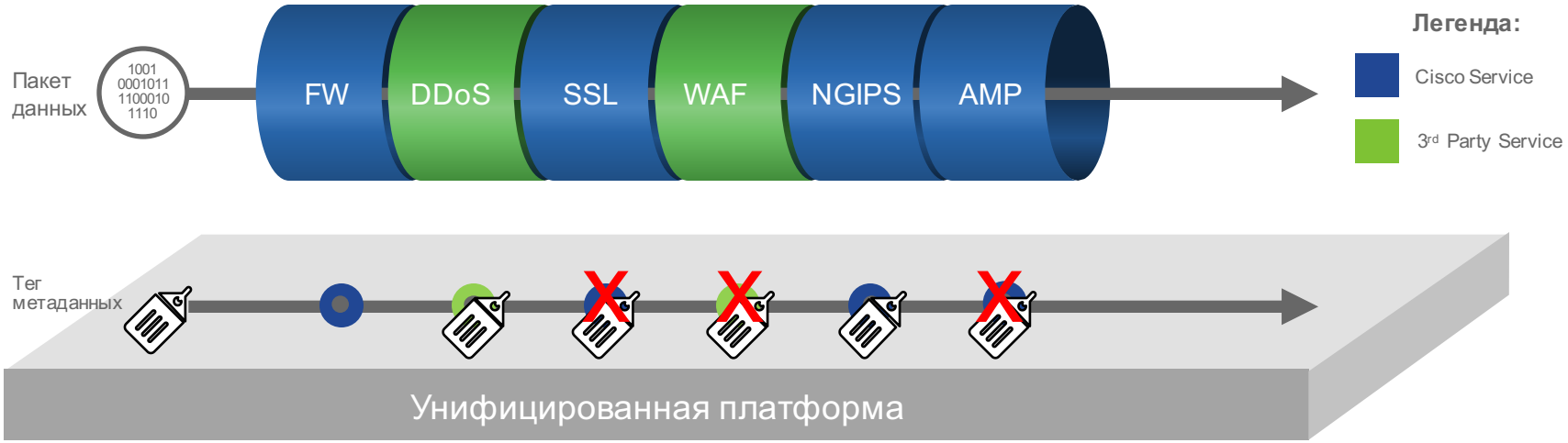
Менее эффективна | Увеличенная задержка | Замедляет обработку | Статическая и ручная

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco трансформирует интеграцию сервисов безопасности

© 2015 Cisco and/or its affiliates. All rights reserved.

Смотрим вперед: интеллектуальное соединение сервисов



Разумные метки снимают необходимость в дополнительной инспекции

Автоматизирует информацию о сервисах безопасности

Оптимизирует ИБ через цепочку сервисов

© 2015 Cisco and/or its affiliates. All rights reserved.

Введение в устройства Wireless IPS

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

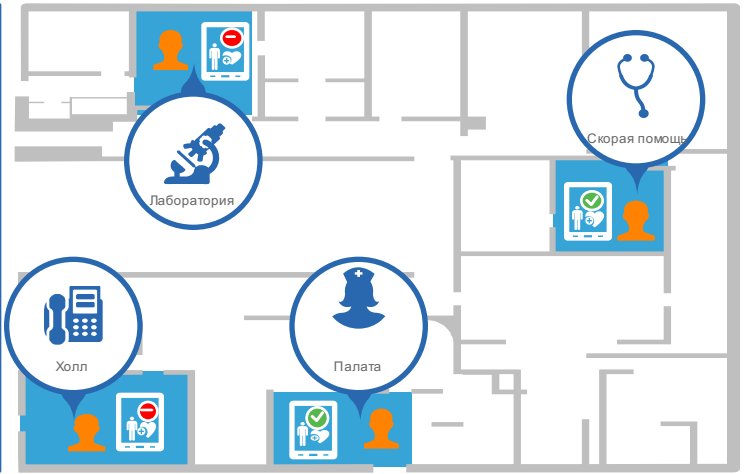
Обнаружение посторонних в беспроводной сети

Администратор определяет иерархию местоположения и предоставляет пользователям конкретные права доступа на основе их местоположения.

Местоположения для доступа к данным клиента

Данные клиента

	Холл	Палата	Лаборатория	Скорая помощь
Врач	Нет доступа к данным пациента	Доступ к данным пациента	Нет доступа к данным пациента	Доступ к данным пациента



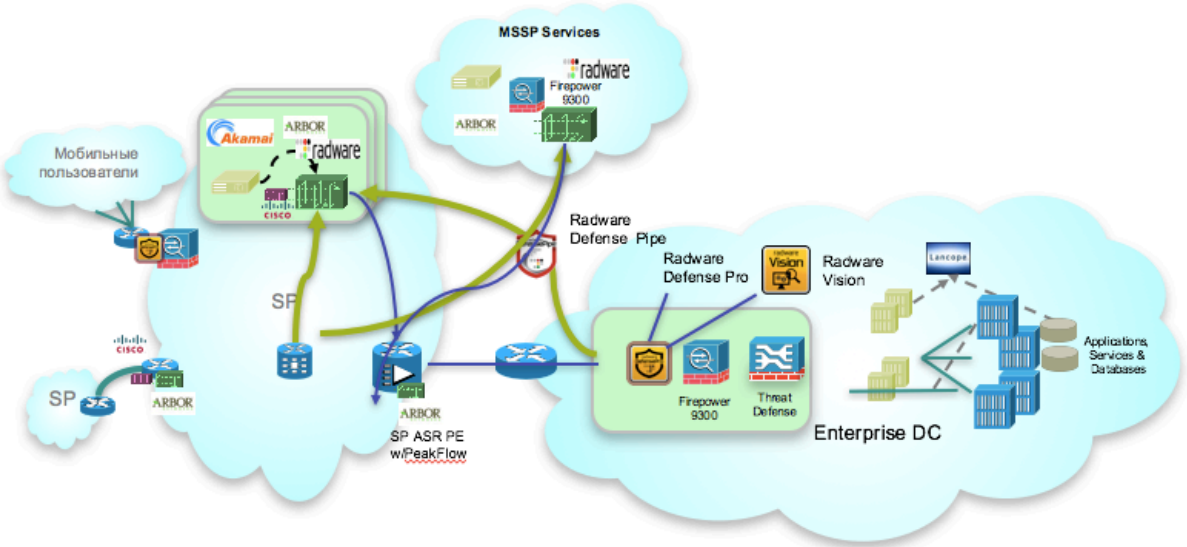
Возможности

- Конфигурация иерархии местоположений по всем объектам местоположения
- Применение атрибутов местоположения MSE в политике авторизации
- Периодическая проверка MSE на предмет изменения местоположения
- Обнаружение посторонних точек доступа и беспроводных клиентов
- Нейтрализация беспроводных атак и подавление посторонних

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Нейтрализация DDoS-атак

- Global Intelligence
- **DDoS**
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection



Возможности

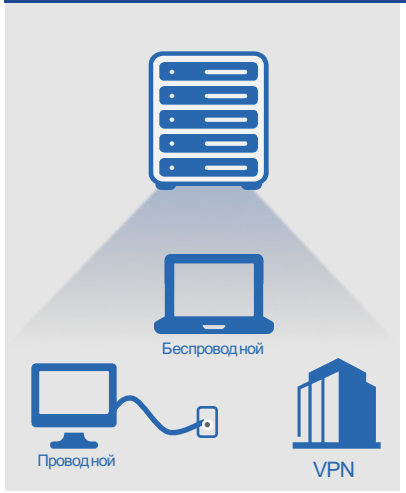
- Наличие базовых возможностей в сетевой операционной системе Cisco IOS, CatOS, NX-OS, IOS XE, IOS XR
- Базовые возможности в Cisco ASA 5500-X, Cisco NGIPS, Lancope StealthWatch
- Обнаружение и нейтрализация широкого спектра DDoS-атак – направленных на канал и на приложения
- Интеграция с сетевой инфраструктурой (Cisco ASR) и инфраструктурой безопасности Cisco (Cisco Firepower 9300)

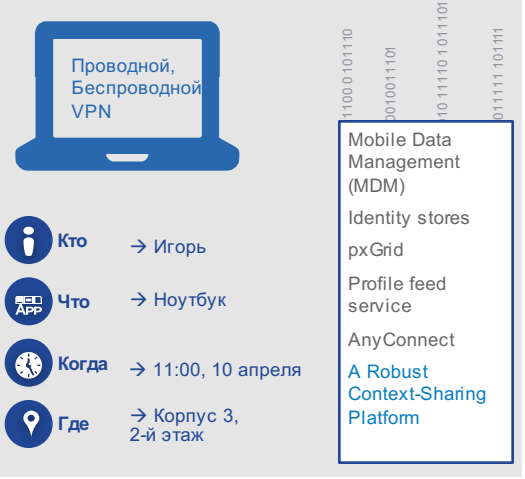
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

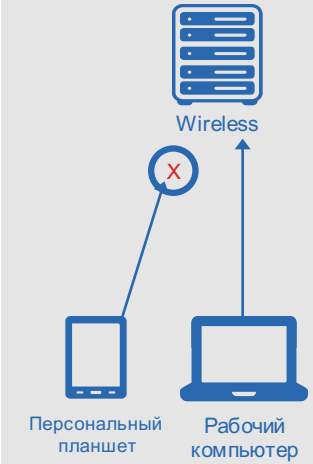
Ограничить доступ и распространение инфекции

- Global Intelligence
- NGIPS & NGFW
- **Identity & Access Control**
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

Identity Services Engine







Унифицированный безопасный контроль доступа

ISE централизует и упрощает создание сетевых политик доступа и управление для того, чтобы предоставить безопасный доступ к сети для конечных пользователей вне зависимости от того, откуда они подключаются.

Превосходный контекст и видимость

Возможность видеть всех пользователей и подключенные устройства в сети обеспечивает более точную идентификацию пользователей/устройств и простое подключение пользователей/устройства.

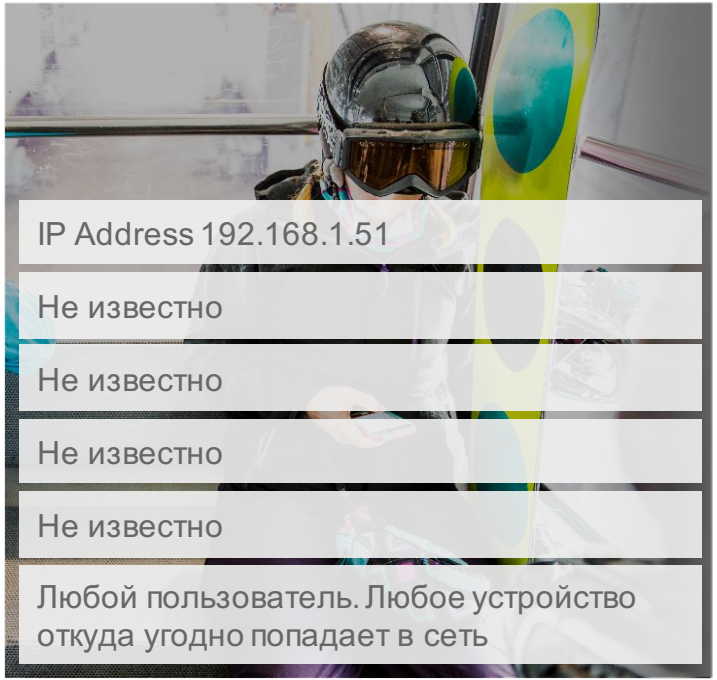
Детальный контроль пользователя

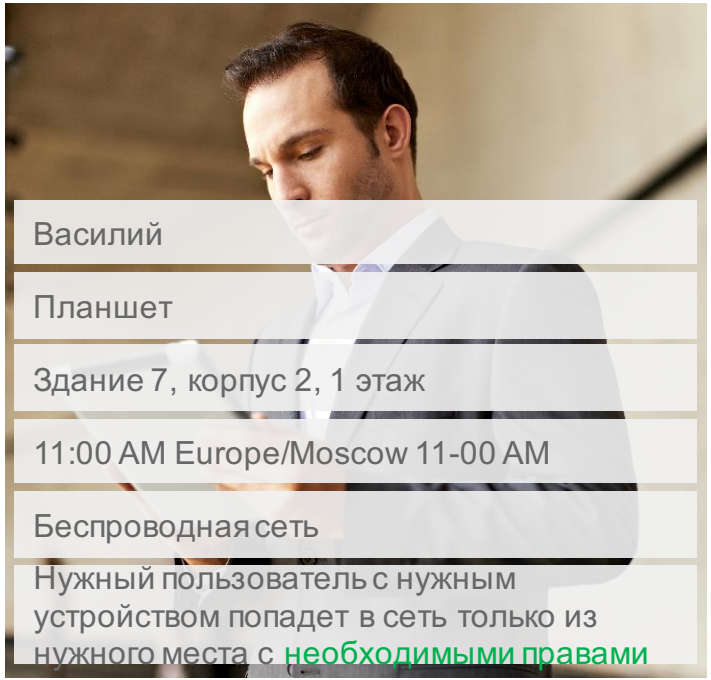
ISE использует свое продвинутые возможности обзора для того, чтобы предоставить возможности управления пользователями на основе типа устройства, времени доступа местоположения и запрашиваемых ресурсов.

© 2015 Cisco and/or its affiliates. All rights reserved.

ISE дает нам контекст безопасности

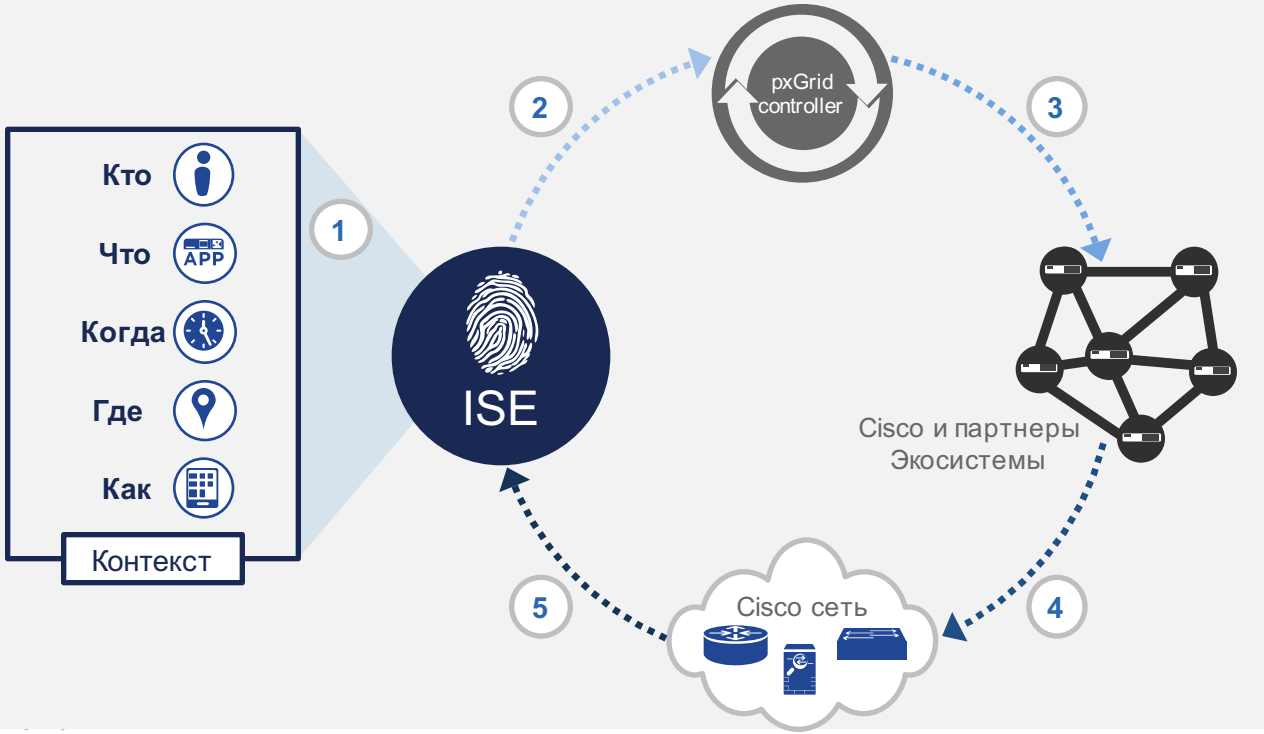
Контекст:	Отсутствие контекста	Богатый контекст
Кто	IP Address 192.168.1.51	Василий
Что	Не известно	Планшет
Где	Не известно	Здание 7, корпус 2, 1 этаж
Когда	Не известно	11:00 AM Europe/Moscow 11-00 AM
Как	Не известно	Беспроводная сеть
Результат	Любой пользователь. Любое устройство откуда угодно попадает в сеть	Нужный пользователь с нужным устройством попадет в сеть только из нужного места с необходимыми правами





© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Включите другие решения по ИБ в единую систему

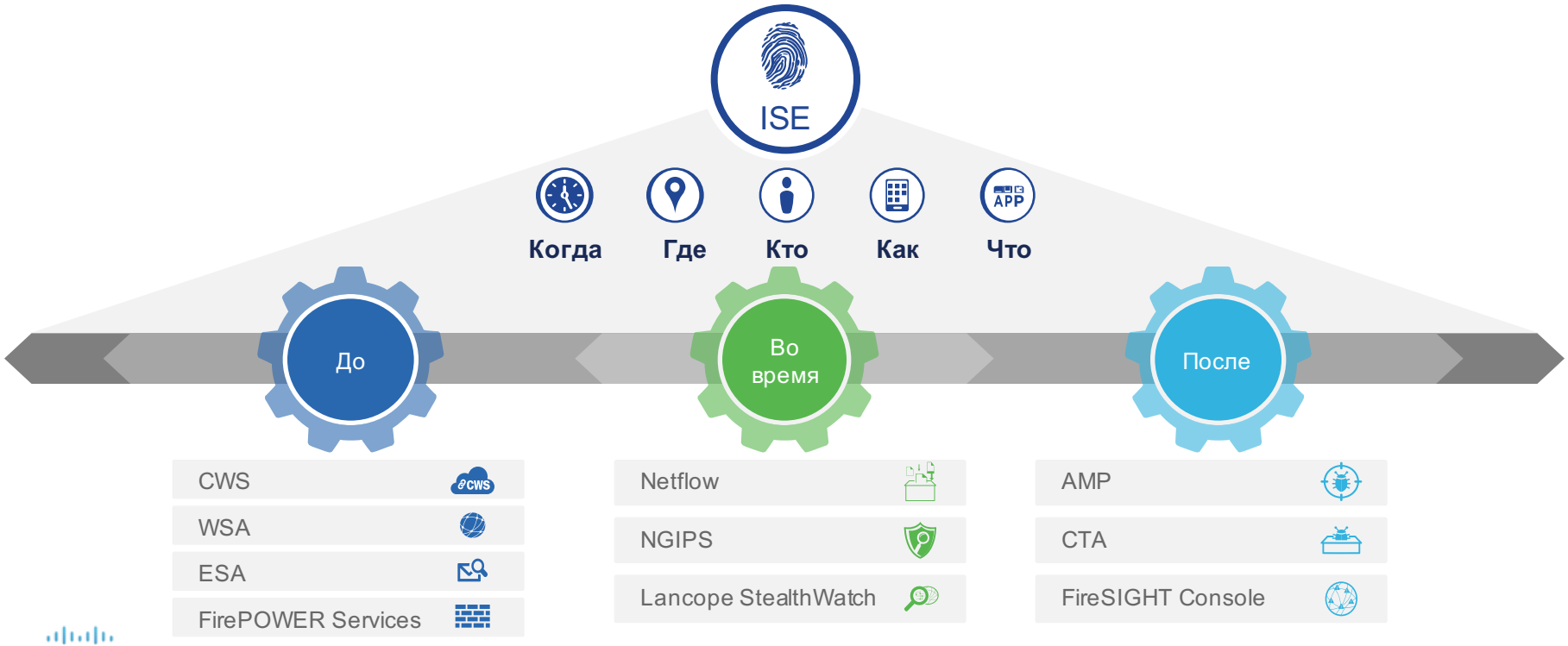


1. ISE собирает контекст из сети
2. Контекст обменивается по технологии pxGRID
3. Партнеры используют контекст для повышения видимости и борьбы с угрозами
4. Партнеры могут запросить ISE о блокировке угрозы
5. ISE использует данные партнера для обновления контекста и политики доступа

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

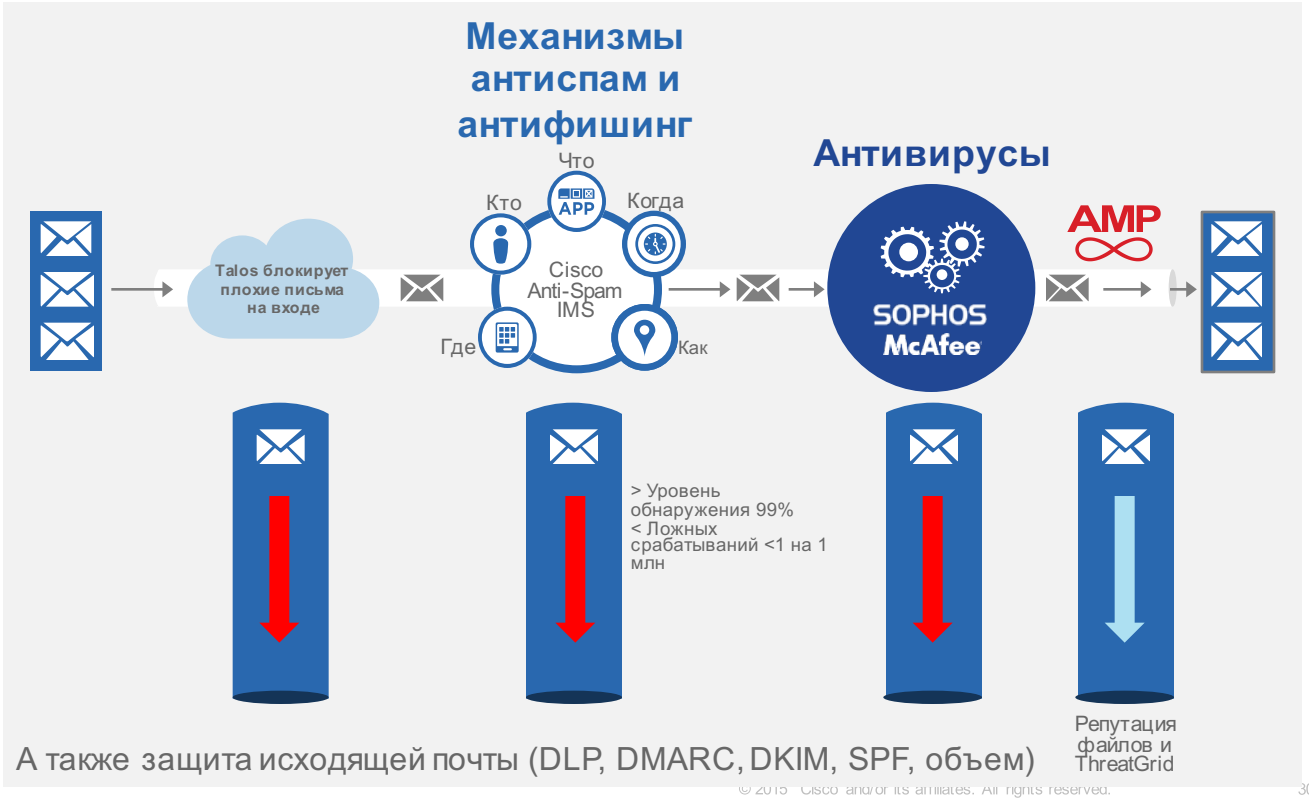
ISE это краеугольный камень сквозной сетевой безопасности Cisco



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Остановите спам, фишинговые атаки и предотвратите утечку данных

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- **Email**
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

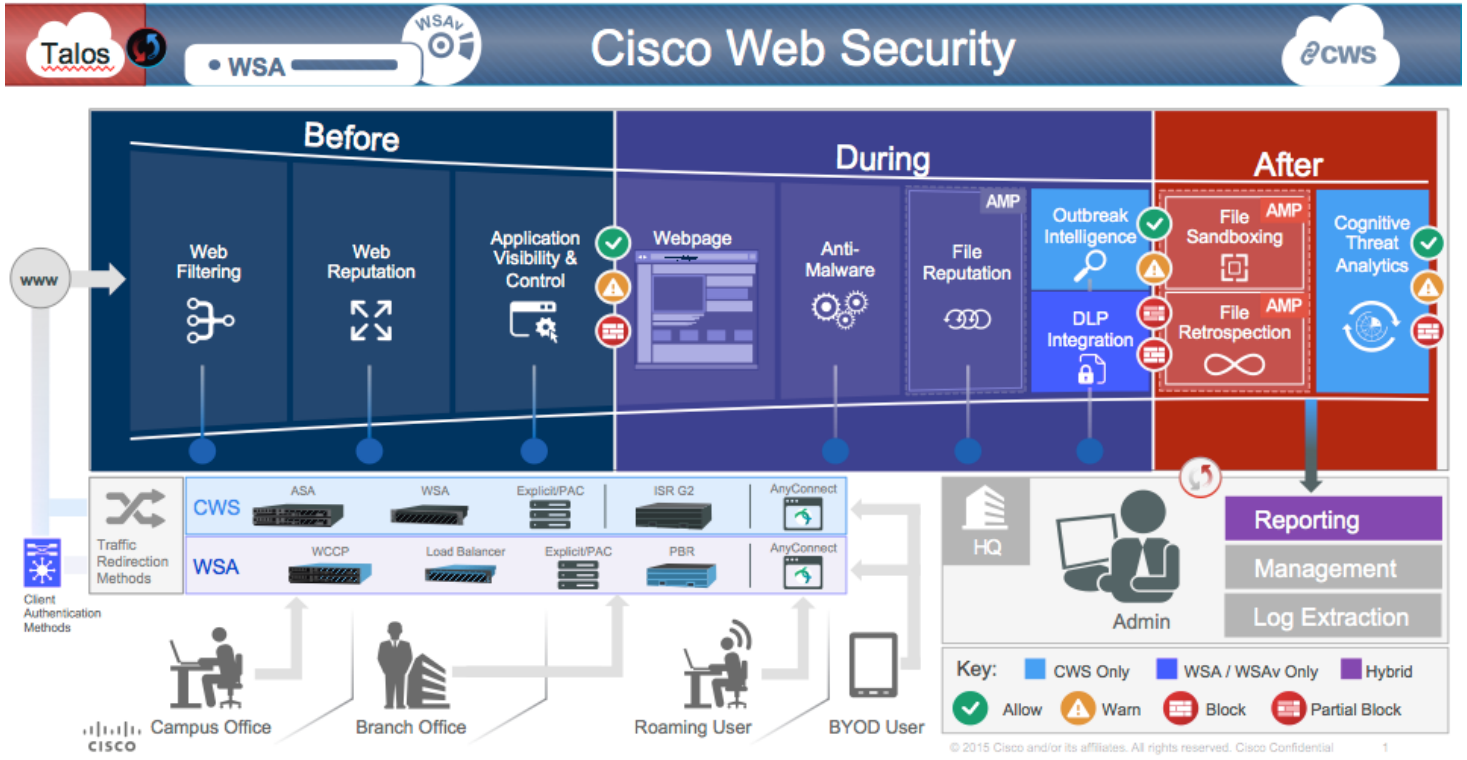


А также защита исходящей почты (DLP, DMARC, DKIM, SPF, объем)

© 2015 Cisco and/or its affiliates. All rights reserved.

Получите детальный контроль над веб-угрозами

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- **Web**
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection



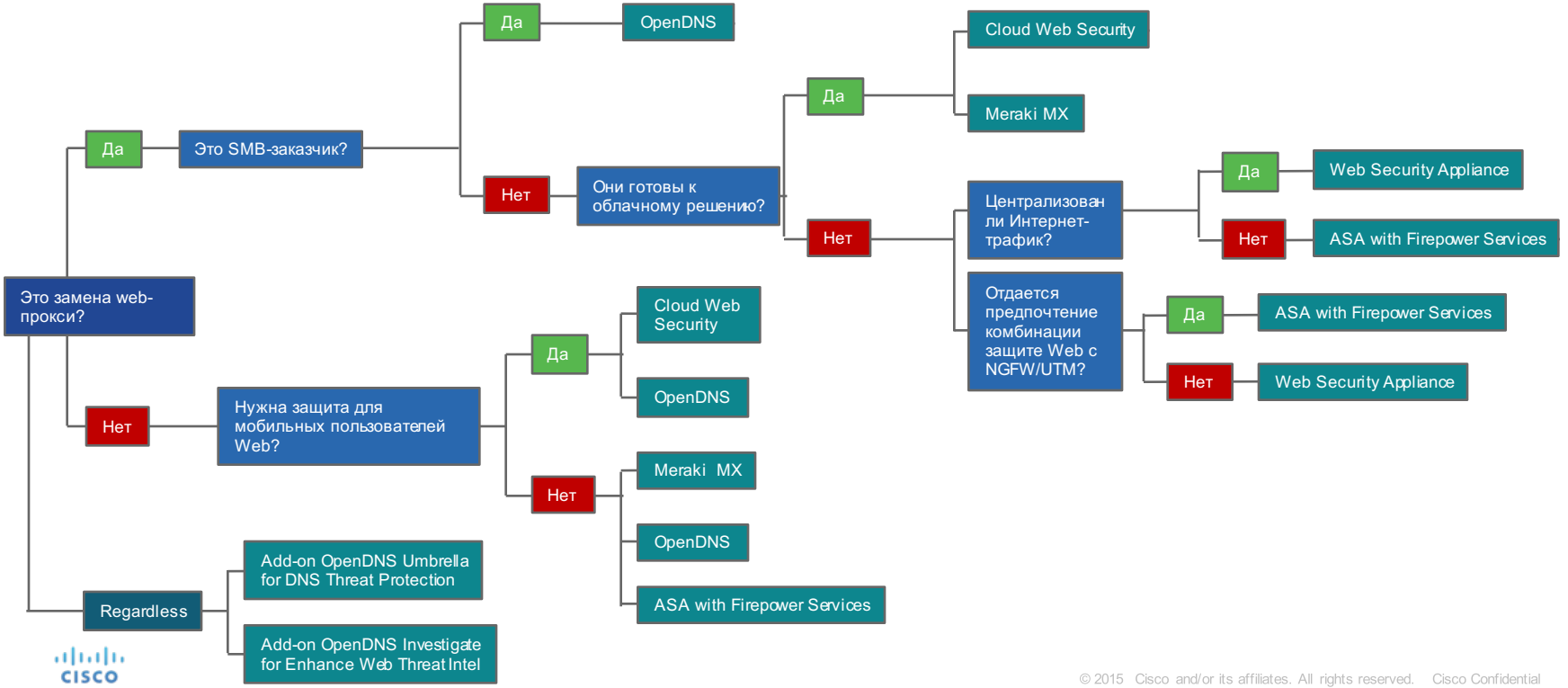
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

© 2015 Cisco and/or its affiliates. All rights reserved.

Решение	ASA FirePOWER	WSA / CWS	OpenDNS Umbrella	Meraki MX
Основные варианты использования	Клиенты хотят унифицированное устройство безопасности, которое обеспечивает функции FW, IPS, веб-фильтрации и отчетности и управления	Клиенты с очень большими объемами web трафика, котором требуется глубокая инспекция и управление	Клиенты с существующими системами безопасности, которые ищут варианты дополнения и/или расширения их за пределы своих корпоративных систем	Клиенты с большим количеством маленьких отделений или со скромными IT бюджетами
Решение уникальных проблем заказчика	Объединение системы сетевой безопасности и некоторых возможностей по веб-безопасности. Обеспечение единого решения, которое масштабируется от уровня границы сети до ЦОД с возможностью фильтрации по всем портам и протоколам	Может проксировать очень большие объемы web трафика (зашифрованного и нет). Прокси терминирует клиентские подключения таким образом, как и конечный сервер. Это позволяет реализовать механизмы детального контроля, инспекции и кеширования web контента.	Самый простой вариант для развертывания. Простое дополнение существующих on-premise механизмов безопасности (NGFW, Web Proxy, etc.). Простое расширение механизмов безопасности на устройства, которые находятся за пределами корпоративной сети	Просто для развертывания и управления в очень распределенной офисной среде. Единая панель управления для безопасности и сетевых функций упрощает администрирование
Технологический дифференциатор	Полнофункциональный Next Generation Firewall с Next Generation IPS и защитой от malware (Advanced Malware Protection, AMP). Не проксирует Web трафик, но может деалть URL фильтрацию, Web репутацию и имеет функционал контроля приложений (AVC)	Многофункциональный web прокси, который обеспечивает очень глубокий уровень инспекции и контроля web трафика. Несколько уровней Web безопасности и механизмов сканирования. (3xAV, Web Reputation, DLP и т.д.). Дополнительные механизмы AMP и CTA обеспечивают защиту от malware и обнаружение malware, которое уже попало в сеть. Оптимизировано для портов 80 и 443.	Применение безопасности на уровне DNS, перед организацией подключения TCP/IP для любого приложения, порта или протокола. Информация об угрозах, которая основывается на глобальной сети, обслуживающей более 80 млрд DNS запросов ежедневно	Unified Threat Management (UTM) – Firewall, IPS, site to site VPN, и web фильтрация.
Другое	Цена на устройство, не зависит от кол-ва пользователей. Во многих случаях клиенты приобретают ASA с FP для NGFW и NGIPS. Можно добавить функционал URL фильтрации и AMP. Сфокусировано на on-premise сетевой безопасности	Возможность гибкого выбора вариантов развертывания (Облачный CWS, локальный физический или виртуальный WSA, гибридный). Для всех вариантов поддерживается построение унифицированных отчетов и унифицированные наборы политик (скоро)	OpenDNS Umbrella — это SaaS. Перспективные клиенты могут получить полное тестирование и развернуть его за 30 минут. Доступен API, интеграция с ThreatGrid, FireEye и др.	Цена за устройство — не зависит от кол-ва пользователей. Meraki предлагает полный набор решений, которые включают MDM, Wireless, Switching, Routing и Security
Относительная стоимость	$$	$$$	$$	$
Основные конкуренты	PAN, Checkpoint, Fortinet	Bluecoat, Zscaler, Websense	Infoblox (DNS), Bluecoat, Zscaler, Websense (SWG)	Fortinet, SonicWall

Требования клиентов	ASA FirePOWER	WSA/CWS	OpenDNS Umbrella	Meraki MX
Качество URL фильтрации			 Domain Name	
Advanced Malware Protection	 Full Tunnel VPN + AMP	 Cognitive Threat Analytics + AMP	 API Driven – e.g. FireEye Integration	 AMP скоро
Next Generation IPS				
Роуминг/защита вне сетевых пользователей				
Web использование и compliance				
Web/HR отчетность				
Унифицированная платформа (UTM/NGFW)				
Облако		 CWS		
Облачное управление		 CWS		
Простота развертывания				

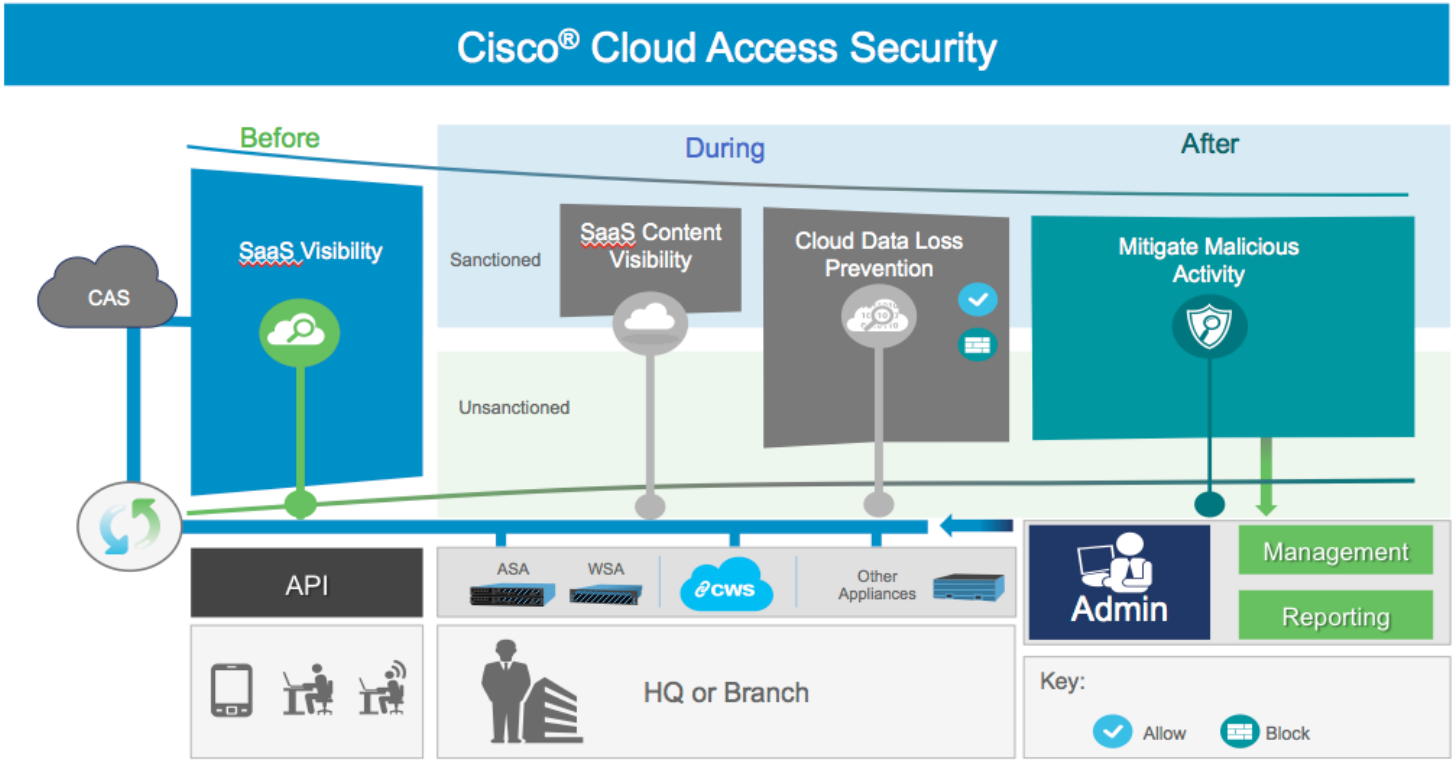
Алгоритм выбора решений по безопасности Web



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Контроль теневых ИТ и облаков

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- **Shadow IT & Data**
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

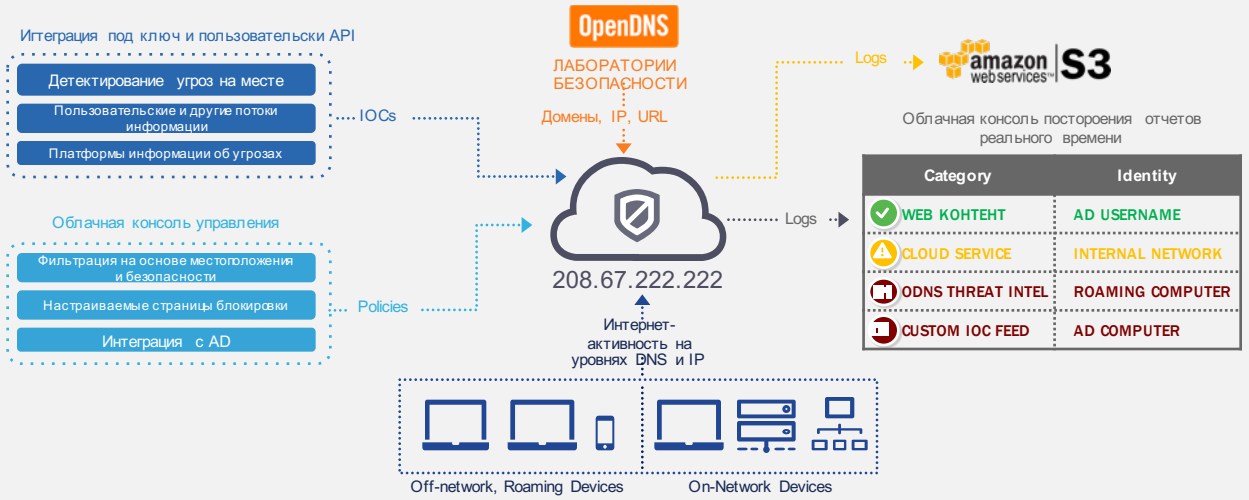


© 2015 Cisco and/or its affiliates. All rights reserved.

Защита вне зависимости от нахождения в периметре или за ним

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- **DNS, IP & BGP**
- Advanced Threats
- Sandboxing
- Anomaly Detection

OpenDNS Umbrella



Глобальная видимость
Блокирование malware, C2 callbacks, & фишинга через любой порт/протокол

Глобальная сеть
Управляет 80B+ DNS запросов ежедневно с 100% uptime

Прогностические технологии
Контроль 2% всей мировой Интернет-активности и возможность долговременного хранения логов

© 2015 Cisco and/or its affiliates. All rights reserved.

Обнаружение существующих и будущих вредоносных доменов и IP

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- **DNS, IP & BGP**
- Advanced Threats
- Sandboxing
- Anomaly Detection

OpenDNS Investigate

Начало

- Имена доменов
- IP адреса
- Автономные системы
- Email адреса

Веб-консоль или API

Зарпрос дополнительного контекста

Простой, скоррелированный источник информации

Обнаружение

- Все ассоциированные домены, IP, и ASN
- Исторические данные DNS
- Данные записей WHOIS
  Значения репутации
- Ассоциированные аномалии (fast flux, DGA's, и т.д.)
- Шаблоны запросов DNS и IP геолокация

Предиктивная информация
Мы применяем статистическую модель к историческим данным и данным реального времени для того, чтобы предсказать вероятно вредоносные домены, которые могут быть использованы в будущих атаках.

Прохождение через инфраструктуру атакующего
Видимость, откуда атакующих инициирует атаки и как соединяются домены, IP, ASN и URL

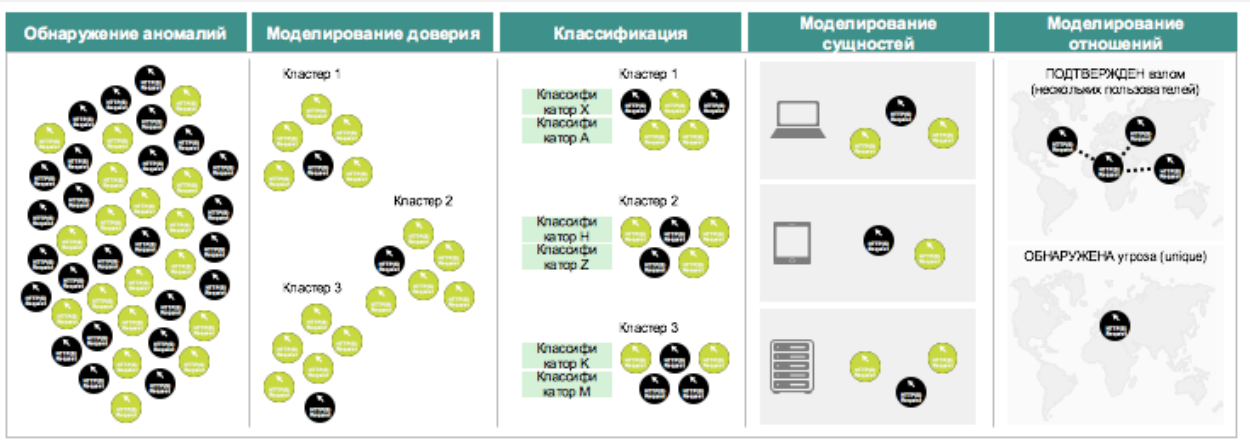
Обзор всего Internet
Обогащение данных безопасности дополнительным контекстом

© 2015 Cisco and/or its affiliates. All rights reserved.

Анализ web-логов от прокси

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

Cognitive Threat Analytics



Мониторинг угроз

Мы применяем статистическую модель к историческим данным и данным реального времени для того, чтобы обнаружить зараженные и скомпрометированные узлы и пользователей в сети

Широкий спектр угроз

Утечки данных, коммуникации с C2-серверами, DGA, эксплойт-киты, туннелирование через HTTP/HTTPS

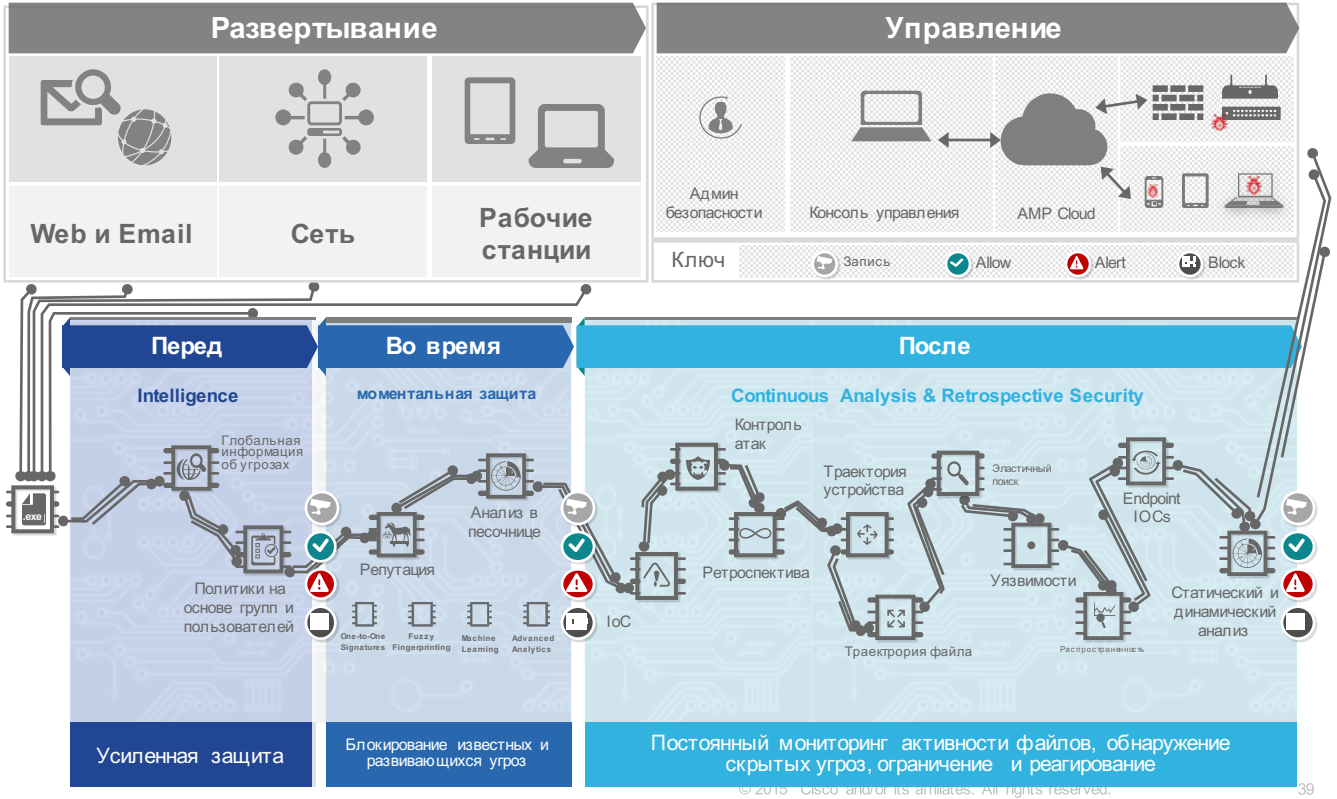
Интеграция

Интеграция с Cisco ISE, Cisco AMP for Endpoint, Cisco AMP for Networks и SIEM для блокирования и анализаугроз

© 2015 Cisco and/or its affiliates. All rights reserved.

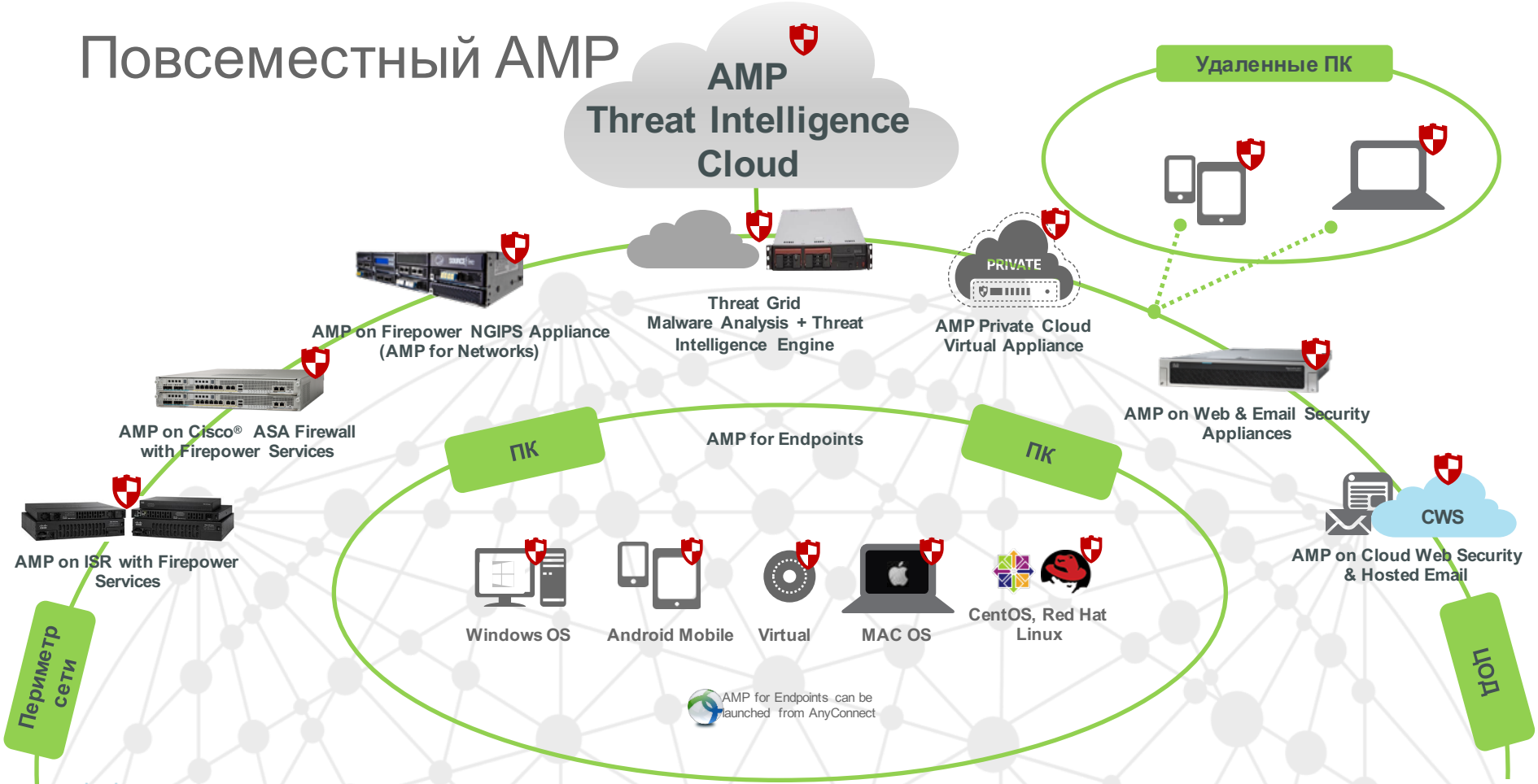
Сокращение времени на обнаружение и снижение влияния

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- **Advanced Threats**
- Sandboxing
- Anomaly Detection



© 2015 Cisco and/or its affiliates. All rights reserved.

Повсеместный AMP



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

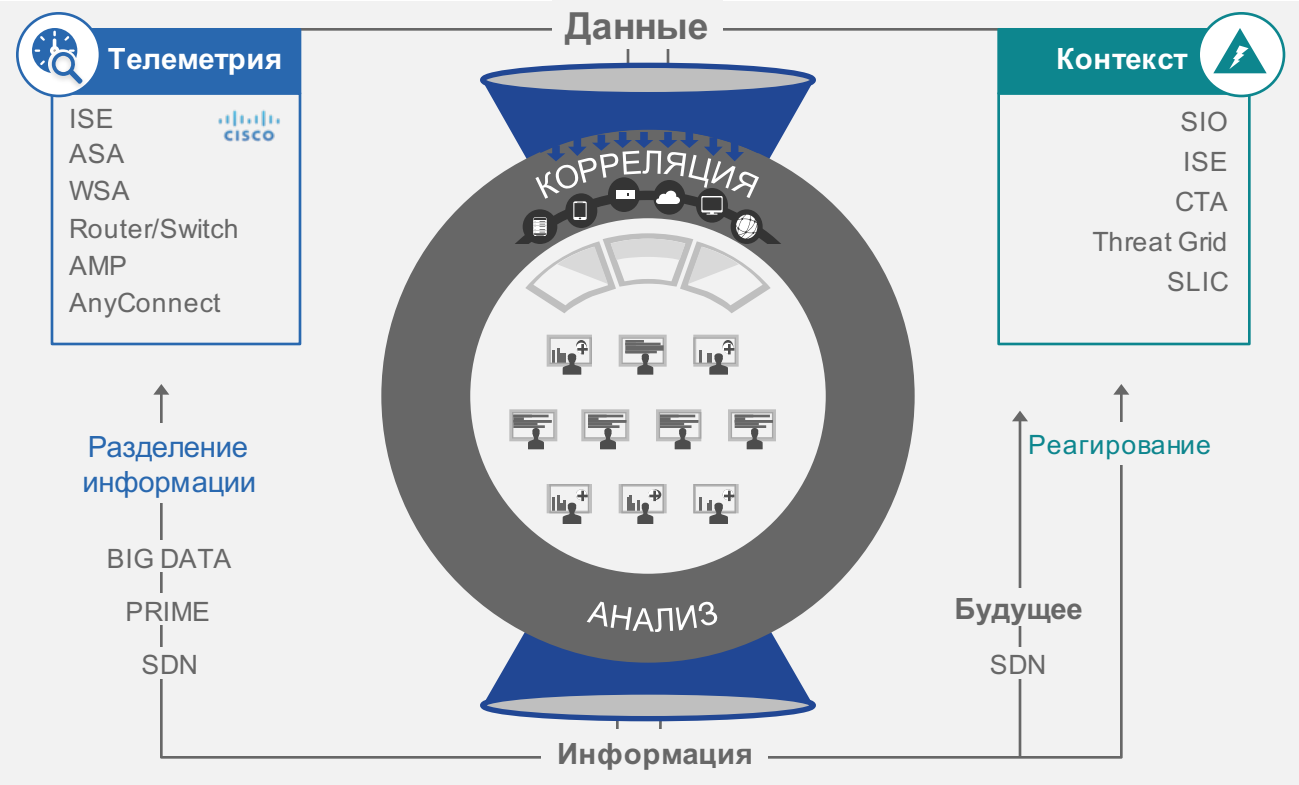
Интегрированный анализ malware и информация об угрозах

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- **Sandboxing**
- Anomaly Detection

© 2015 Cisco and/or its affiliates. All rights reserved.

Превратите вашу сеть в сенсор обнаружения угроз

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection



© 2015 Cisco and/or its affiliates. All rights reserved.

Мобильные пользователи тоже нуждаются в защите

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

Cisco AnyConnect

- VPN-клиент на базе DTLS
- Роуминг между сетями и выбор оптимального шлюза
- Идентификация пользователей и устройств
- Оценка соответствия узлов
- Интегрированная безопасность Web
- Интеграция с защитой от вредоносного кода
- Перенаправление всего трафика на периметр сети
- Выборочное туннелирование
- Обнаружения аномалий
- Поддержка Apple IOS, Android, Blackberry, Windows Phone, Windows 7/8/10, MAC, Linux, ChromeOS
- Локализация на русский язык

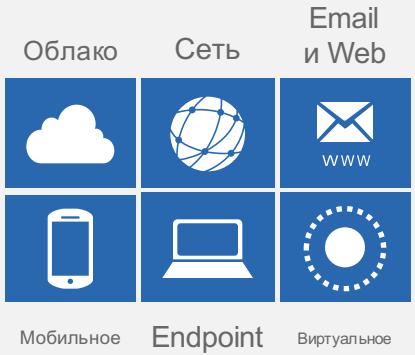
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 43

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Интегрированная защита от угроз – это единственный путь заблокировать продвинутые угрозы

- Global Intelligence
- NGIPS & NGFW
- Identity & Access Control
- Email
- Web
- Shadow IT & Data
- DNS, IP & BGP
- Advanced Threats
- Sandboxing
- Anomaly Detection

Среднее время обнаружения с Cisco: **46 часов**

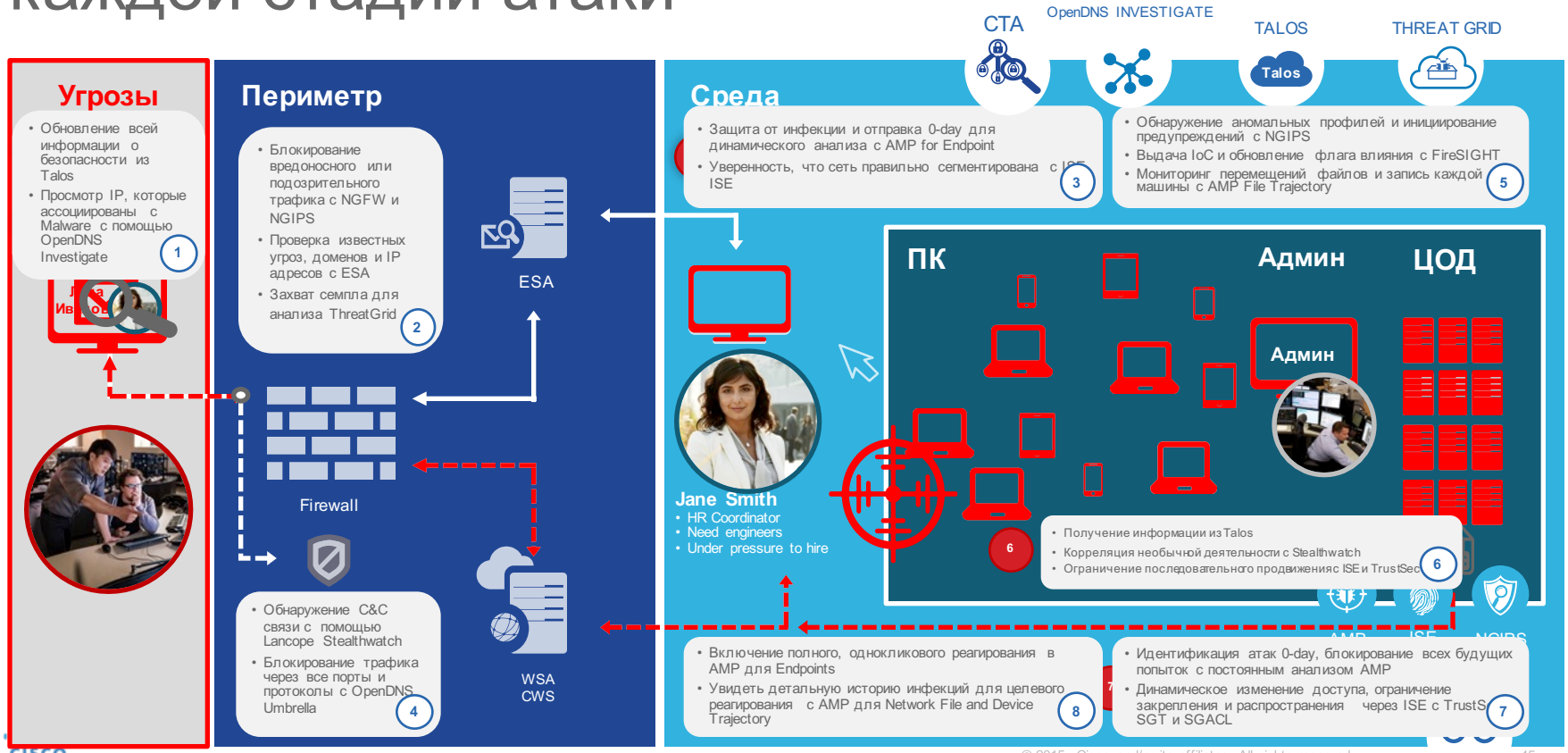


Среднее время обнаружения без Cisco: **200 дней**

© 2015 Cisco and/or its affiliates. All rights reserved.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Интегрированная защита работает на каждой стадии атаки



© 2015 Cisco and/or its affiliates. All rights reserved.

Только Cisco защищает на протяжении всего цикла атаки

ДО	ВО ВРЕМЯ	ПОСЛЕ
ASA NGFW	FirePOWER NGIPS и WIPS	Lancope Stealthwatch
ISE & TrustSec	WSA и CWS	Threat Grid
AnyConnect	ESA	Cognitive Threat Analytics
OpenDNS Investigate	Cloud Access Security	OpenDNS Investigate и CTA
	Advanced Malware Protection	
OpenDNS Umbrella		
Talos		

Запомните этот адрес:

dcloud.cisco.com

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

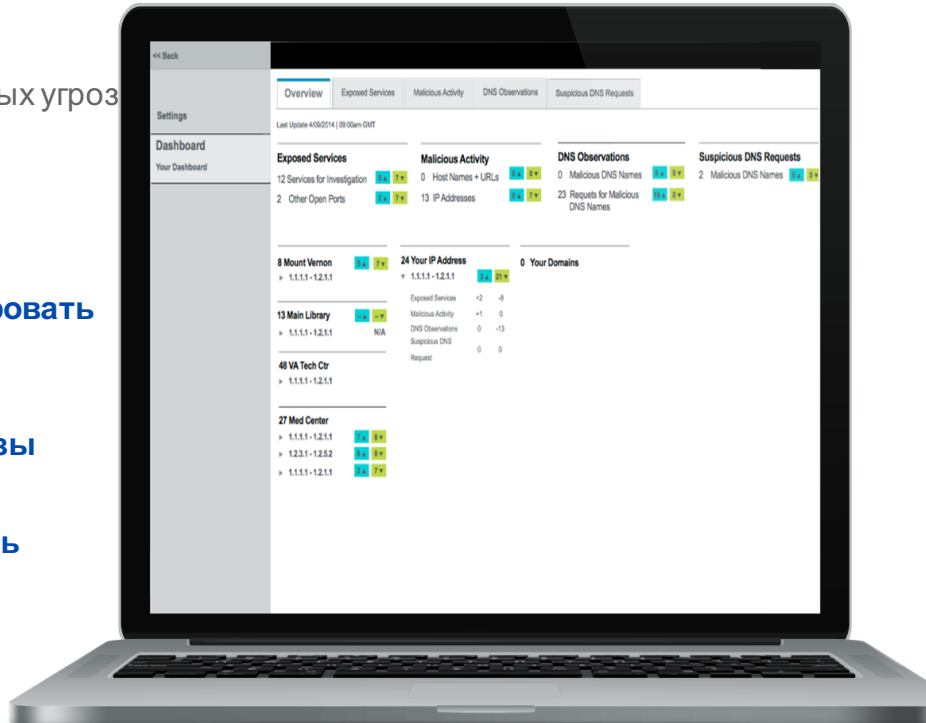
Наша основная задача – в перспективе – интегрировать между собой все решения Cisco, дав им доступ друг к другу и к единому источнику информации об угрозах!

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

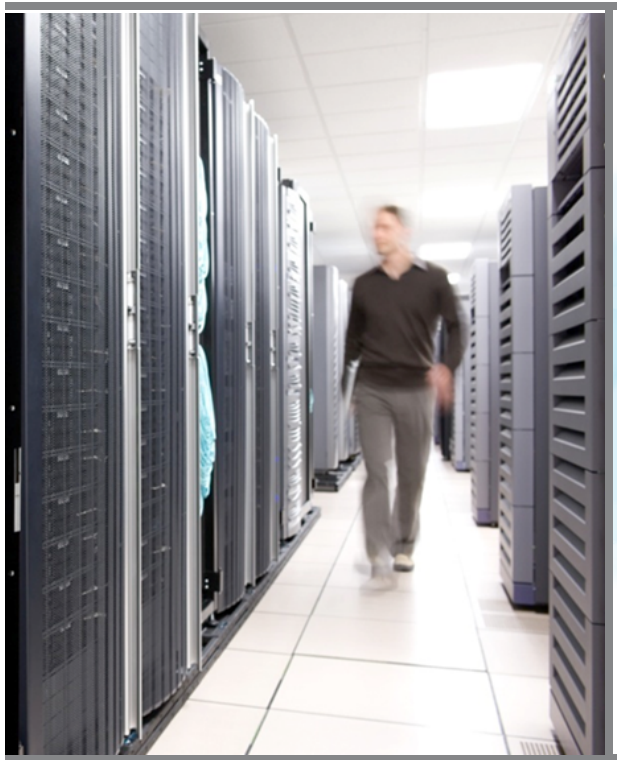
Cisco Threat Awareness Service

Cisco® Threat Awareness Service это **портальный**, сервис анализа угроз, который расширяет **видимость угроз** и является доступным **24-часа-в-сутки**.

- Использование одной из лучших в мире баз данных угроз
  - Оперативное **обнаружение вредоносной активности**
- Идентификация скомпрометированных сетей и подозрительного поведения
  - Помогает компаниям быстро **идентифицировать** скомпрометированные **системы**
- Обеспечение рекомендаций
  - Помогает ИТ/ИБ **идентифицировать угрозы**
- Анализирует сетевой, исходящий из организации
  - Позволяет улучшить **общую защищенность**



Cisco Threat Awareness Service



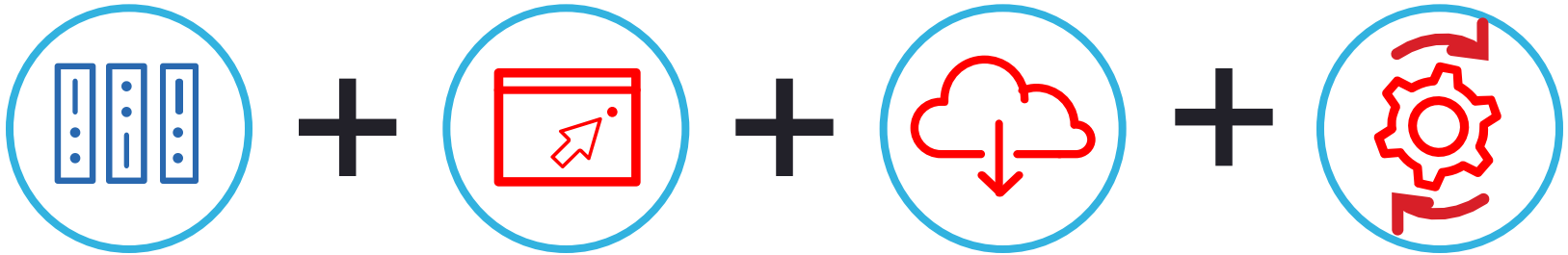
Базируясь на технологиях Cisco, сервис Threat Awareness Service **не требует**:

- Капитальных вложений
- Изменений конфигурации
- Сетевых инструментов
- Новых внедрений ПО
- Сенсоров в сети заказчика
- Дополнительных людских ресурсов

Снижение времени внедрения, сложности,
и цены с ростом эффективности threat intelligence

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Не забывайте про новые возможности



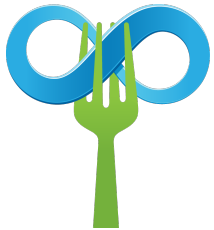
Железо | Обновления | Сервисы/ подписки | Продления подписок

“Раз и готово” не надо

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Акцент на продажи ПО

Минимальные обязательства → Высокие обязательства

Начало 2016 (пилот)	Доступно с ноября 2015	Доступно (не всем) с ноября 2015	Скоро в России
			
Cisco ONE Advanced Security “Commit to Domain”	**Software Volume Purchasing** ”Commit to Technologies”	**Advantage – Security offer** “Commit to Budget”	**Security ELA** ”Commit to Architecture”
Все организации 1+ devices и/или 100+ users	Все организации 100-100,000 users	Средние/крупные орг-ии $200K+ USD	Крупные организации $400K+ USD и/или >1,000 users
▪ Фиксированные бандлы security software и WAN, ЦОД, ЛВС ▪ Расширение за счет Advanced Security	▪ Три и более решений по ИБ со скидкой в 10% ▪ Доступен в GPL	▪ Гарантированно выделенный бюджет на безопасность на определенный период времени (обычно 3 года) дает дополнительную скидку	▪ Каталог ПО по безопасности с неограниченным числом лицензий на 3-5 лет ▪ Предсказуемые инвестиции

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Дополнительная информация по ИБ Cisco


Сценарий для партнеров

Каким должен быть межсетевой экран нового поколения

В чем суть кампании?

Официальный документ

Требования к межсетевому экрану нового поколения для предприятий малого и среднего бизнеса и географически распределенных предприятий

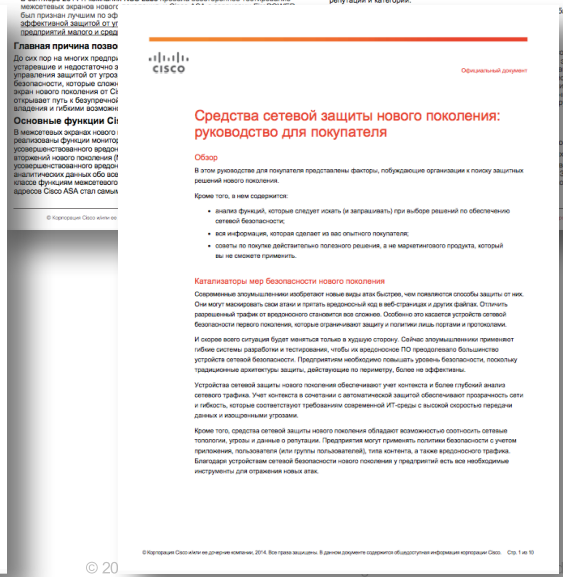
Аргументы в пользу внедрения межсетевого экрана нового поколения на предприятиях малого и среднего бизнеса


Официальный документ

Выбор межсетевого экрана нового поколения: 10 важнейших факторов

Без чего не обойтись предприятиям среднего бизнеса

Обзор


Официальный документ

Средства сетевой защиты нового поколения: руководство для покупателя

Обзор

Катализаторы мер безопасности нового поколения

Cisco ASA с сервисами FirePOWER для предприятий малого и среднего бизнеса и компаний с филиалами
Руководство по проведению телефонных переговоров

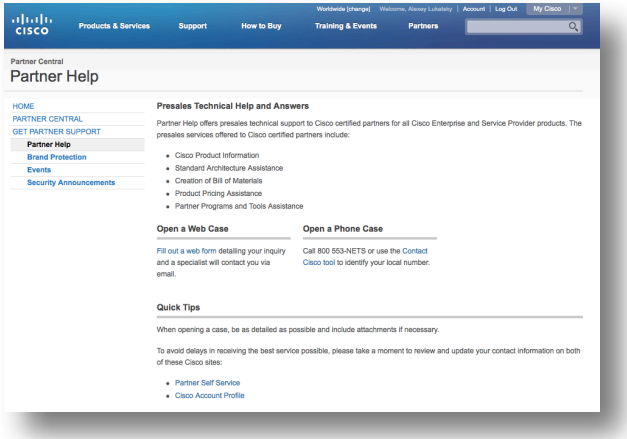
Руководство по проведению телефонных переговоров: Cisco ASA с сервисами FirePOWER для предприятий малого и среднего бизнеса и компаний с филиалами

Три основные причины позвонить заказчикам с установленным оборудованием

Функции (AVC — стандартная функция, остальные предоставляются по подписке)

Проверка и уточнение функциональности продукта

- Сервис Partner Help в рамках которого инженеры службы технической поддержки продаж Global Virtual Engineering (GVE) смогут проверить и уточнить функциональность решений Cisco в области ИБ, выдать презентации, проверить и составить спеки, сгенерить ключи для триалов, выдать ПО, получить сравнения с конкурентами и т.п.



https://www.cisco.com/go/ph

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Где вы можете узнать больше?

Пишите на security-request@cisco.com

Быть в курсе всех последних новостей вам помогут:

- http://www.facebook.com/CiscoRu
- http://twitter.com/CiscoRussia
- http://www.youtube.com/CiscoRussiaMedia
- http://www.flickr.com/photos/CiscoRussia
- http://vkontakte.ru/Cisco
- http://blogs.cisco.ru/
- http://habrahabr.ru/company/cisco
- http://linkedin.com/groups/Cisco-Russia-3798428
- http://slideshare.net/CiscoRu
- https://plus.google.com/106603907471961036146/posts
- http://www.cisco.ru/

© 2015 Cisco and/or its affiliates.

TOMORROW starts here.