Cisco Firepower NGFW

Как предупредить, заблокировать и отреагировать на атаку

Pavel Rodionov

Cisco CSE Security

prodiono@cisco.com

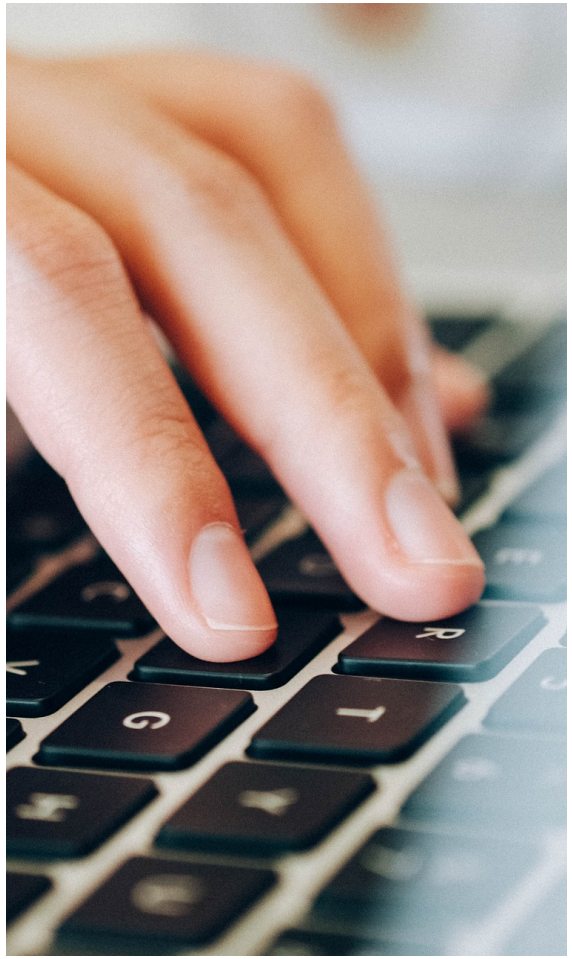
У вас есть задача построить и защить сеть, которая использует новейшие технологии

- Мобильный доступ
- Социальное взаимодействие
- Публичные и частные гибридные облака
- Облачные приложения

IT помогает достичь желаемого

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Сегодня инновации требуют цифровой транформации



UBER

$62.5B

Оценка на декабрь 2015

Source: Forbes

Информатизация создает ценность

Но это должно делаться безопасно

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

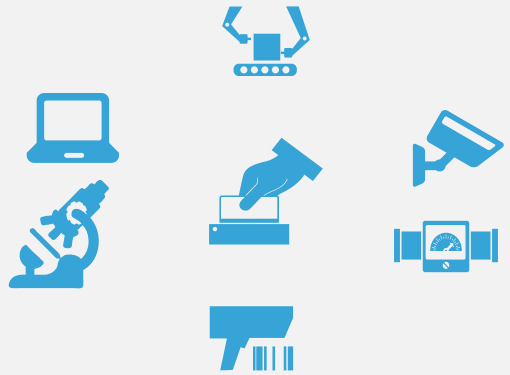
Которая резко расширяется, что заставляет беспокоиться

Новые требования

- Глобальное взаимодействие
- Доступ отовсюду
- BYOD

Сложно управлять доступом

Больше вещей



Видимость стала ускользать

Целевые угрозы

30% Фишинг сообщений открываются целями во время проведения кампаний

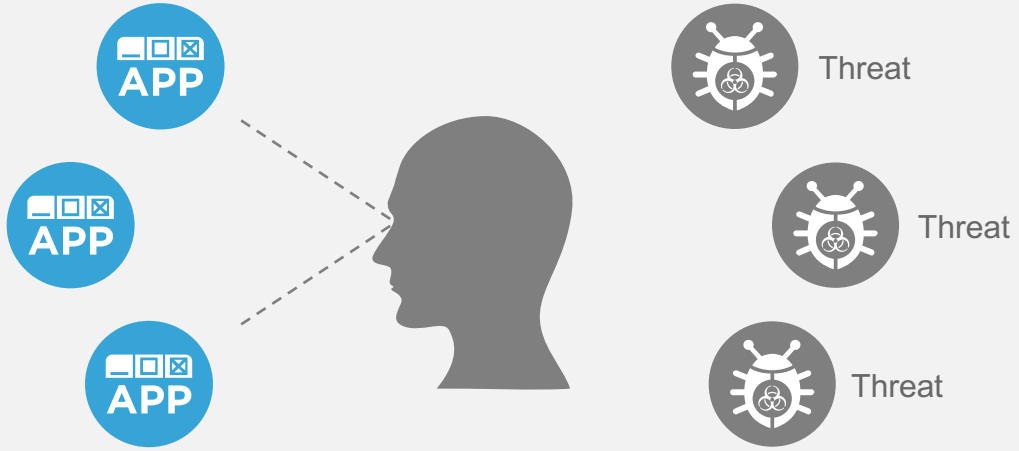
Source: 2016 Verizon Data Breach Investigations Report

Угрозы сложно остановить

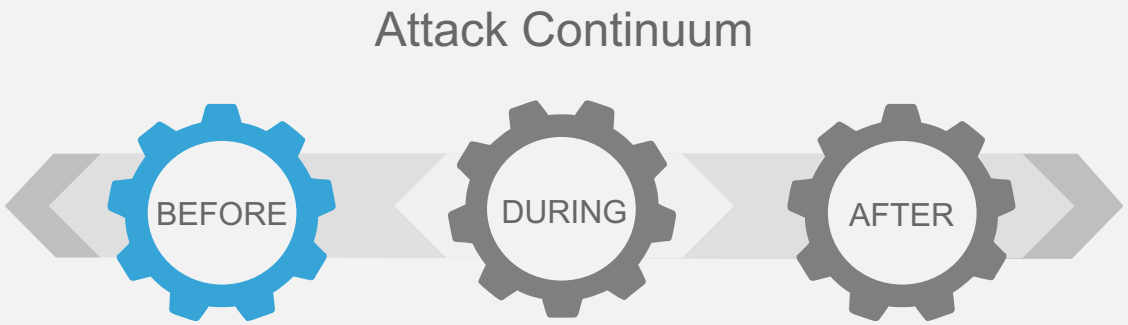
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Другие межсетевые экраные “нового поколения” решают одни проблемы но создают другие

Они сфокусированые на приложениях…



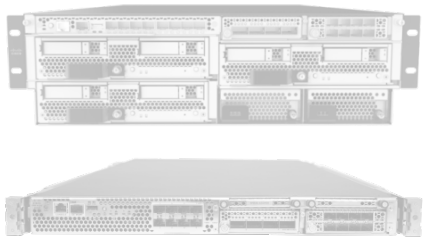
Они не помогут вам, если ваша сеть уже скомпрометирована…



Есть и другие области для управления

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Полное решение – это Cisco Firepower NGFW



Cisco Firepower™ NGFW

Остановить
больше угроз

Получить
Больше информации

Обнаружить
раньше и быстрее

Снизить
сложность

Получите большую
отдачу от вашей сети

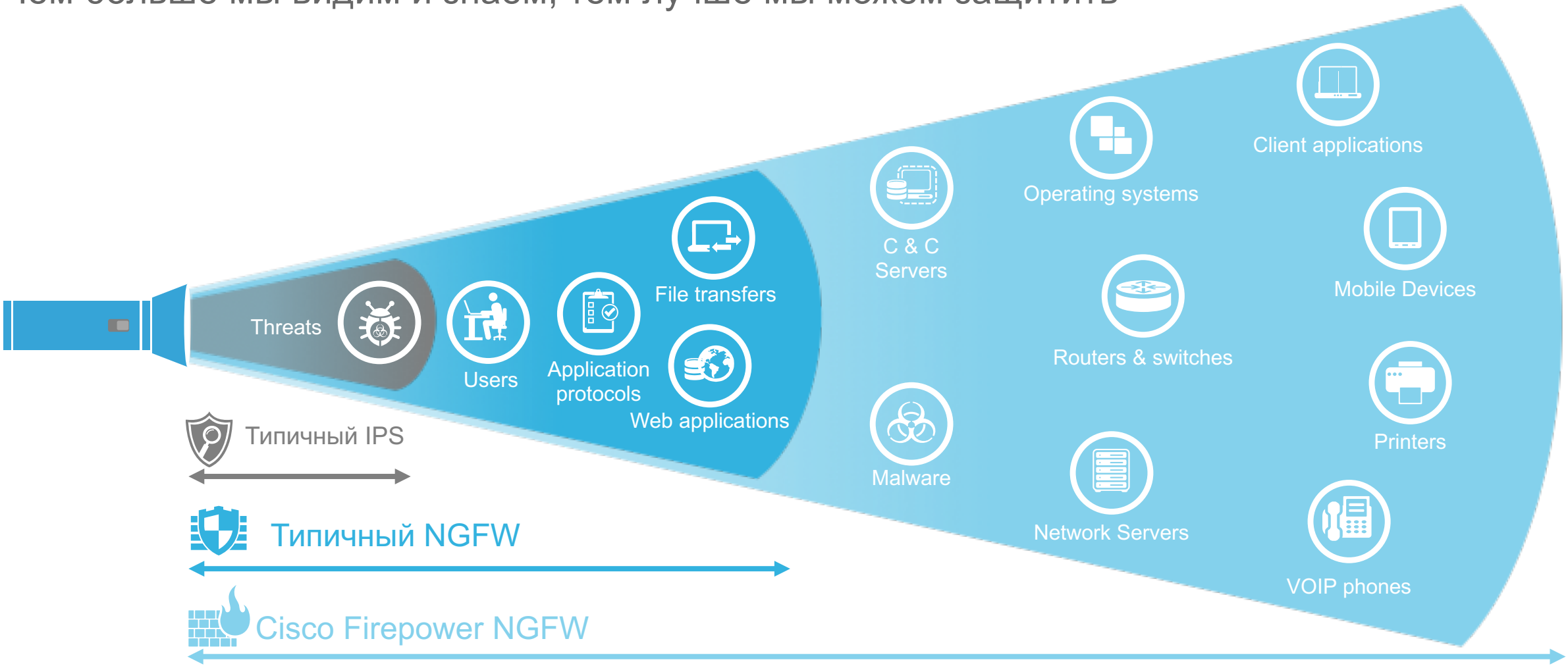
Сфокусирован на угрозах

Полностью интегрирован

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

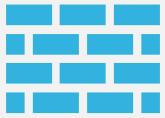
Предлагает расширенную видимость контекста

Чем больше мы видим и знаем, тем лучше мы можем защитить



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

С восемью основными вариантами использования



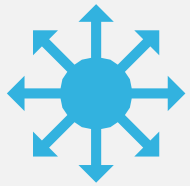
Капмусный NGFW

Граница сети

Граница облачного ЦОД

Граница локального ЦОД

Правила использования



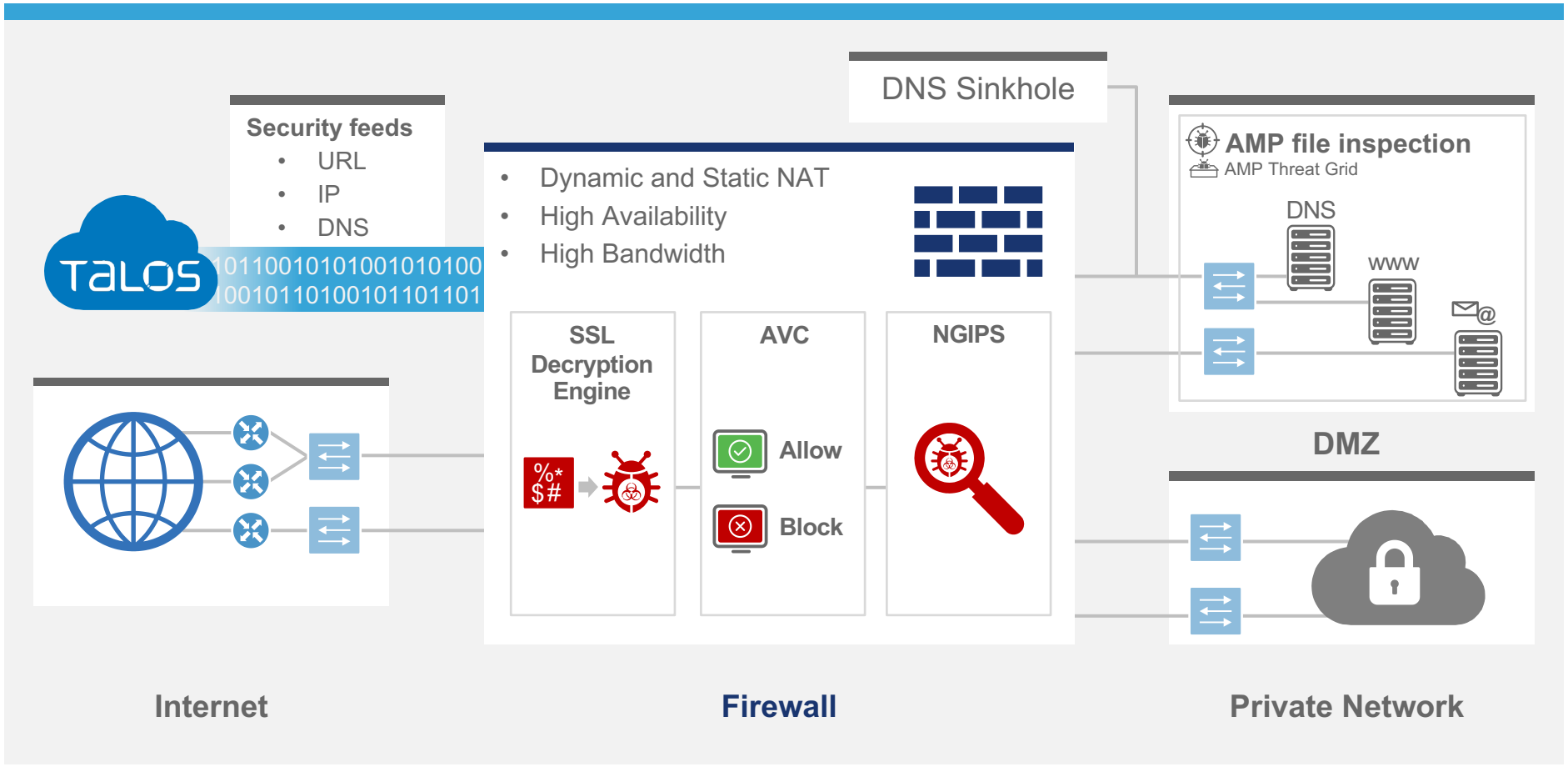
ACI интеграция

Сложный удаленный доступ

Быстрое сдерживание угроз

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Защитите границу Internet в вашей компании



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Защитите ваш облачный ЦОД

Подготовка | Защита | Политики | Обнаружить угрозы | Реагирование | Исправление

Security feeds
URL | IP | DNS

TALOS

1011001010100101010010001100101110100101101101

HR

Finance

DevOps

TrustSec

- High Availability
- High Bandwidth

SSL Decryption Engine

AVC

Allow

Block

NGIPS

AMP file inspection
AMP Threat Grid

Financial data

HR data

In-house app

Граница ЦОД

Virtual Firewall

Облачный ЦОД

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Защитите границу локального ЦОД

Подготовка | Защита | Политики | Обнаружение угроз | Реагирование | Исправление

Security feeds
URL | IP | DNS

TALOS

1011001010100101010010001100101110100101101101

HR

Finance

DevOps

TrustSec

- High Availability
- High Bandwidth

SSL Decryption Engine

%*
$#

AVC

Allow

Block

NGIPS

AMP file inspection
AMP Threat Grid

- Кластеризация
- Поддержка трафика North-South и East-West

Financial data

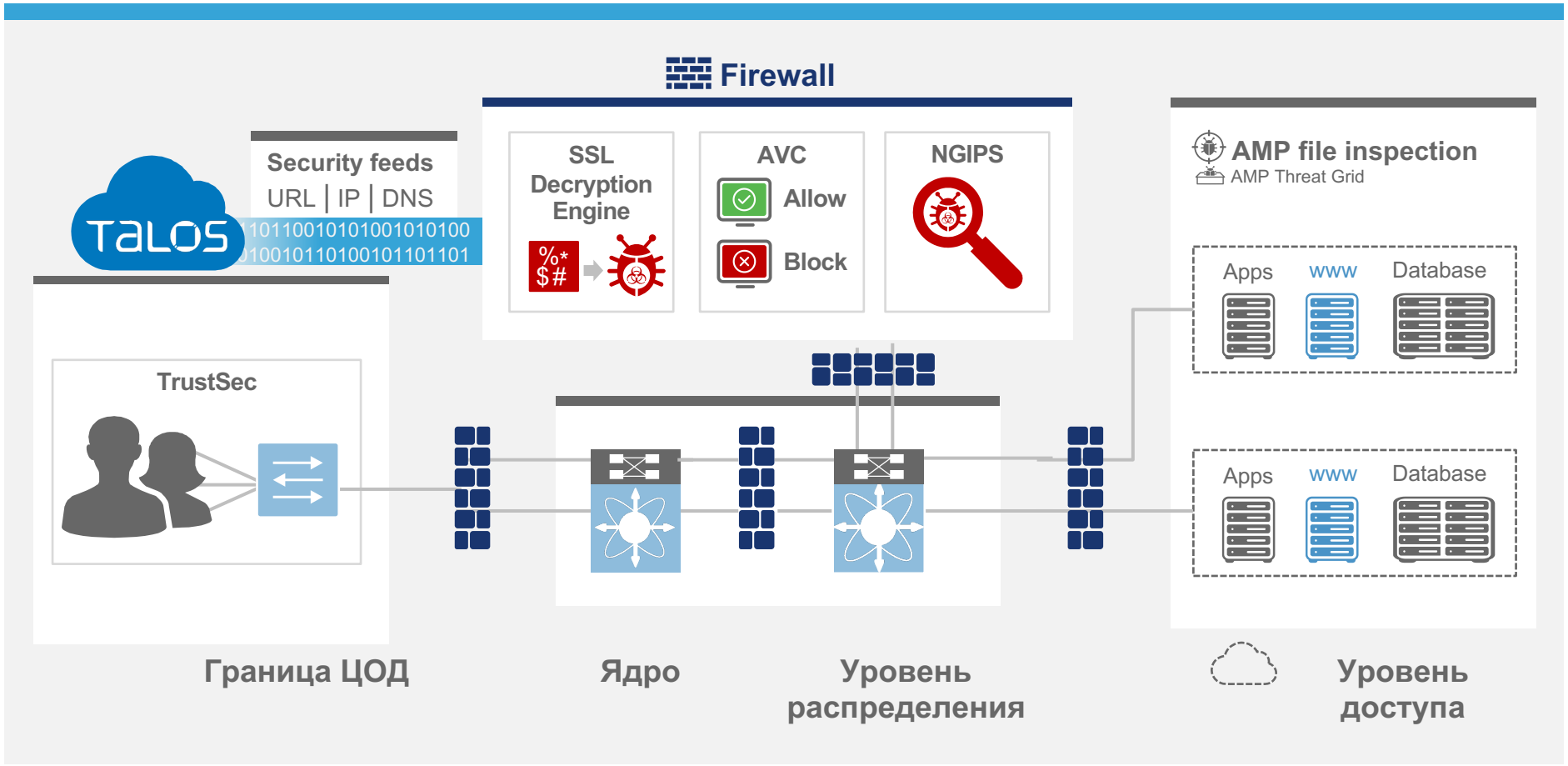
HR data

In-house app

Граница ЦОД | **Firewall** | **Сеть ЦОД**

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Не допустите угрозы в кампусную сеть



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Применение политик использования во всей организации

Reputation scoring

www

4000+ web and **in-house** applications

…and additional **custom applications**

Gambling Application

www

Фильтрация нежелательных URL

SSL Decryption Engine

%* $# → www | Decrypt

Partial Block

Allow

Block

Определение политик доступа

Firewall

Приоритетный трафик

1

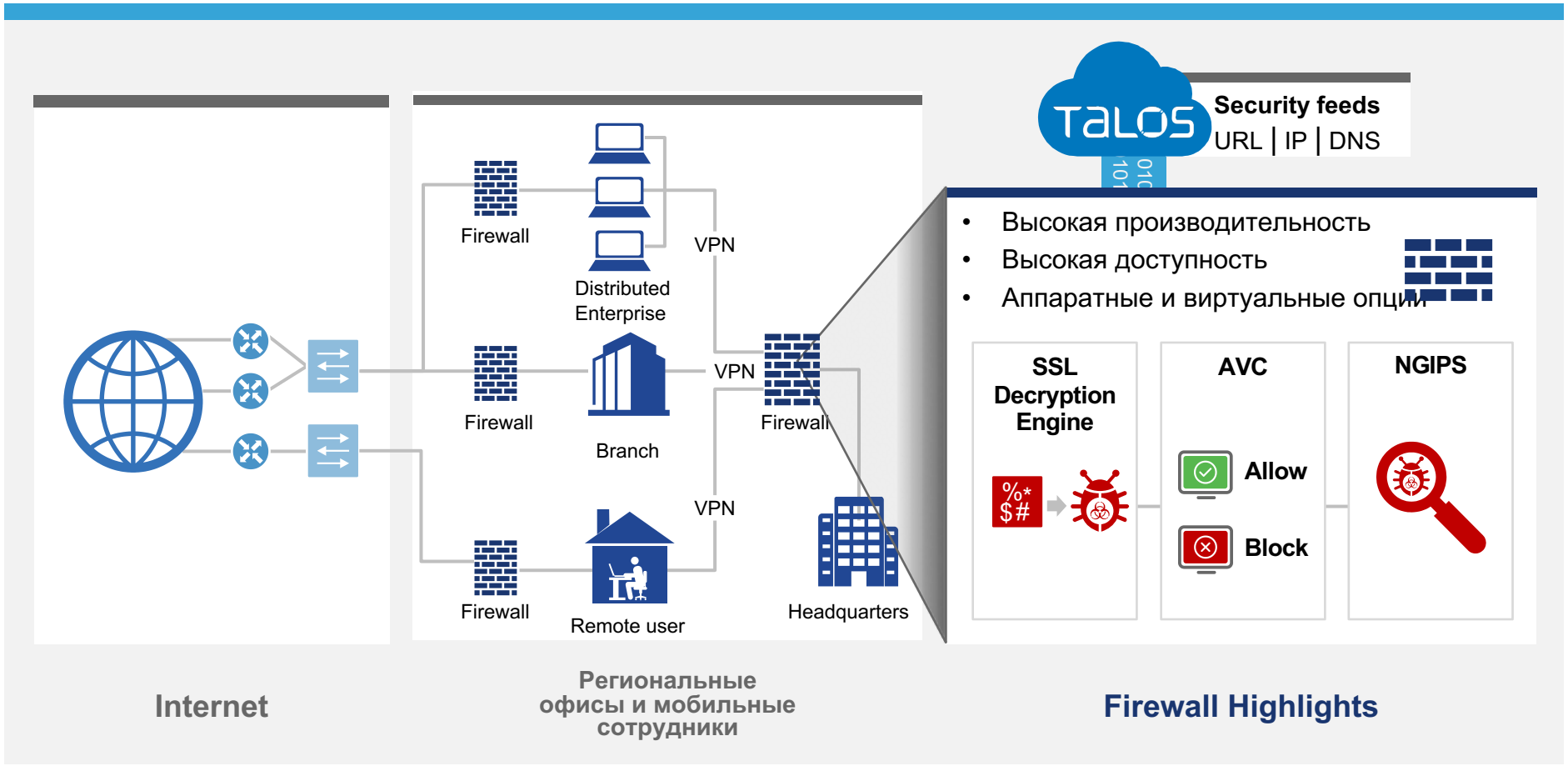
2

Идентификация

Сеть

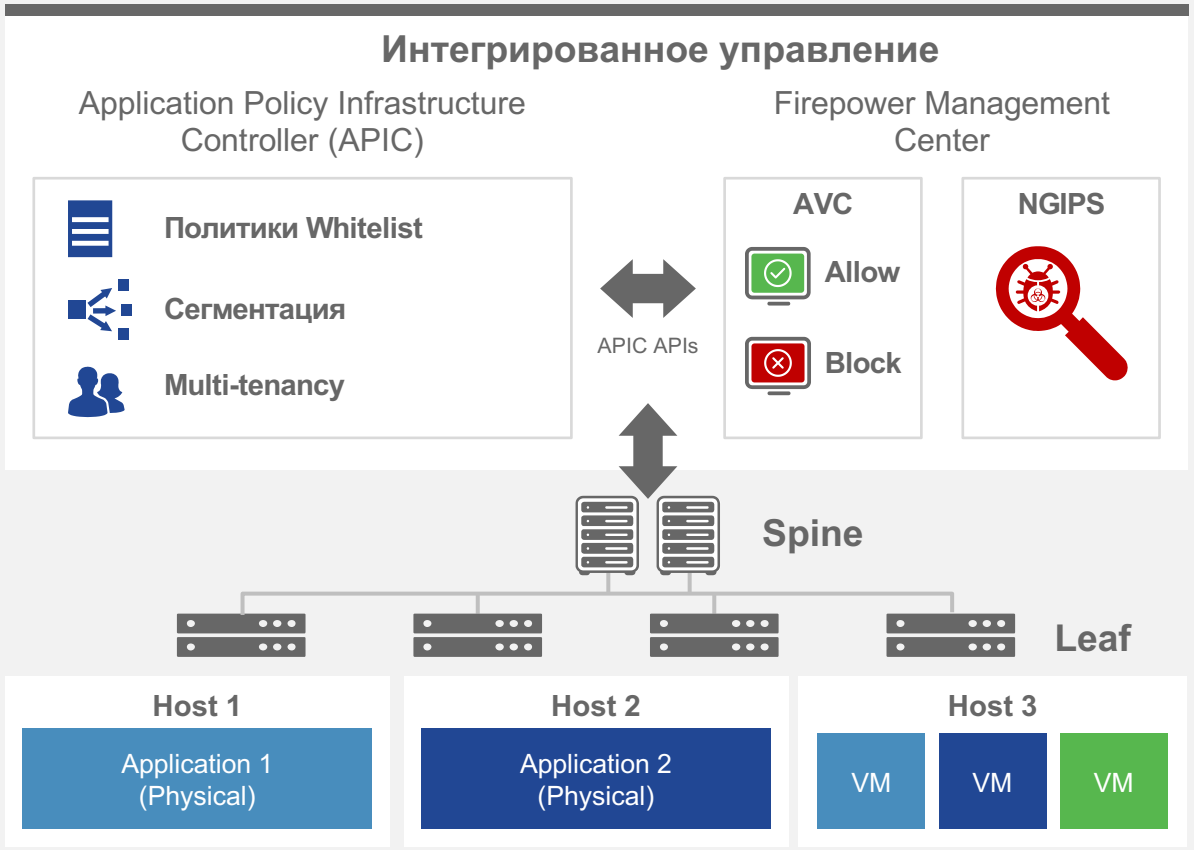
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Расширить безопасный доступ на другие локации



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Улучшить масштабируемость и управление с ACI



Обнаружить угрозы с NGIPS с помощью ACI fabric visibility

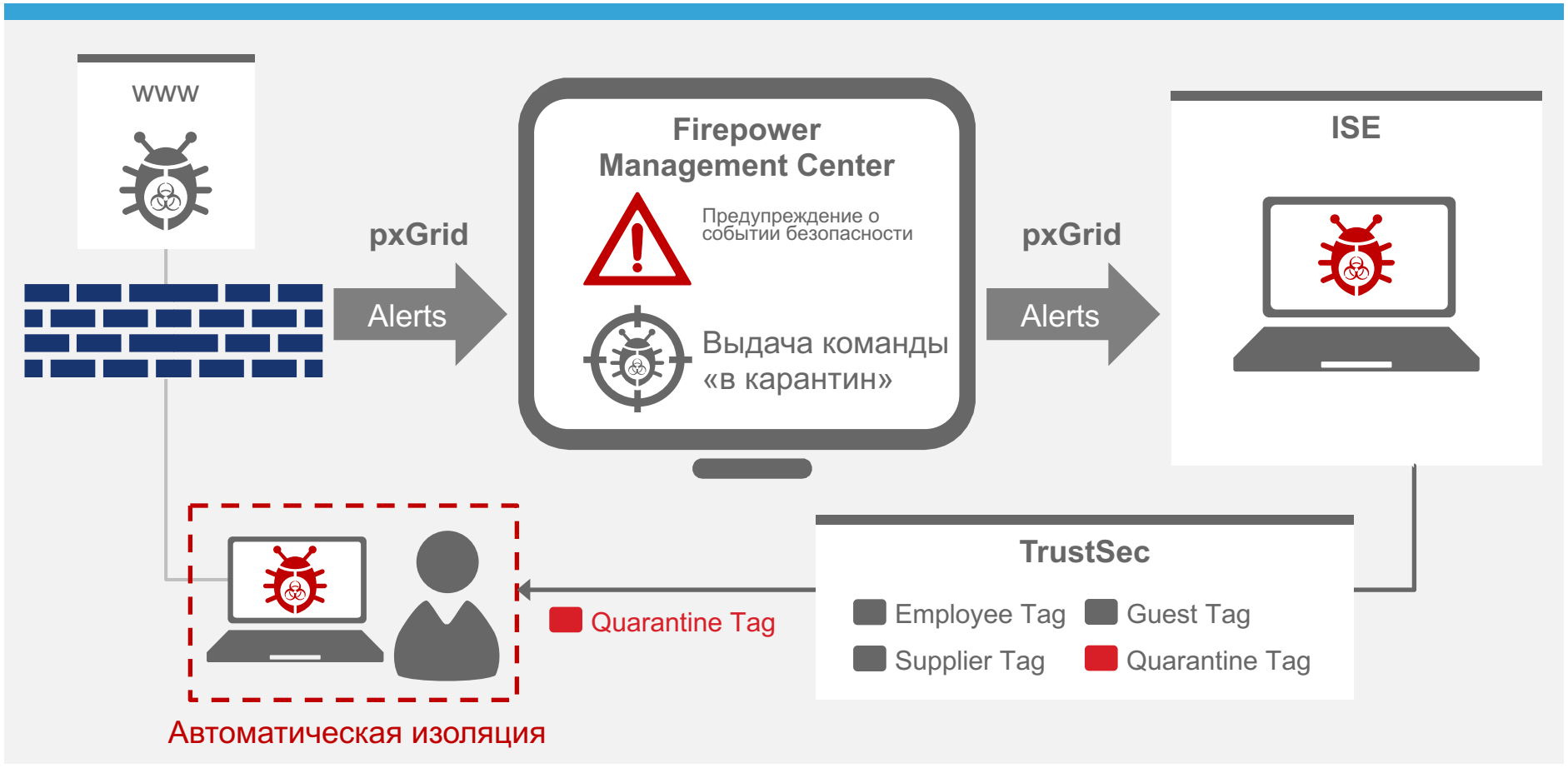
Настройка политик с помощью интегрированного интерфайса управления

Пересмотр политик с помощью анализа активности

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Защита сети с помощью Rapid Threat Containment

Быстрое сдерживание угроз



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Функционал:

Firewall и AVC
Защита от угроз
Управление
Интеграция

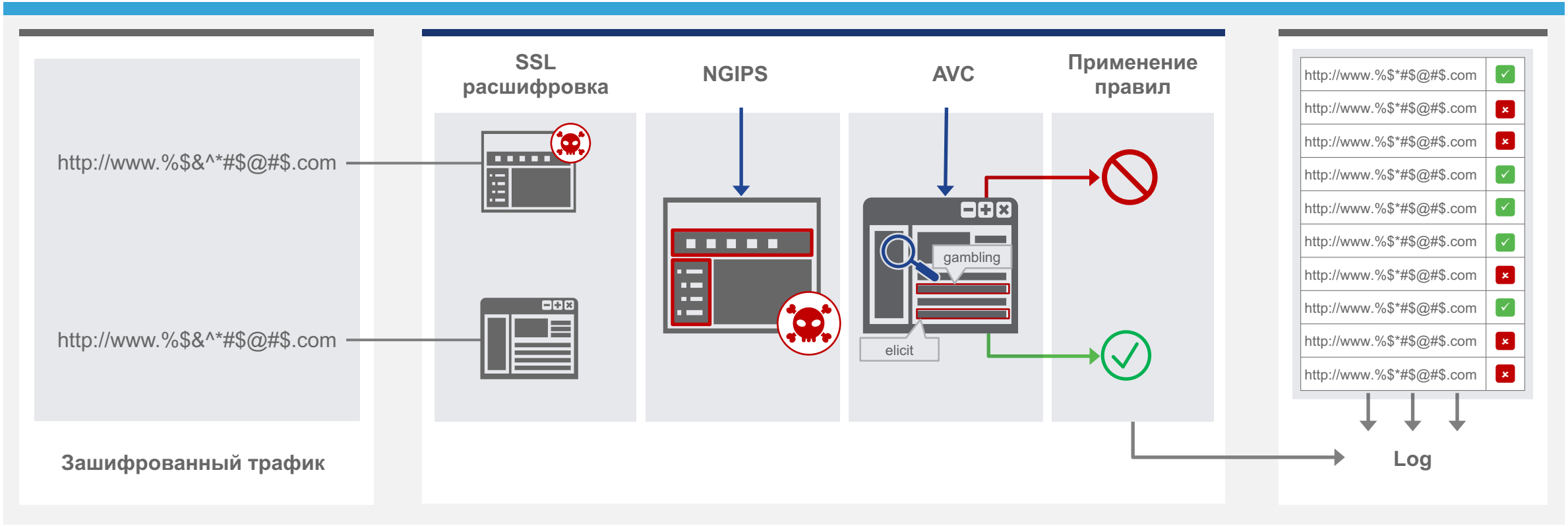
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firewall и AVC

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Найдите скрытые угрозы

Механизм расшифровки SSL



Расшифровка **3.5 Gbps** трафика с более чем 5 млн одновременных потоков

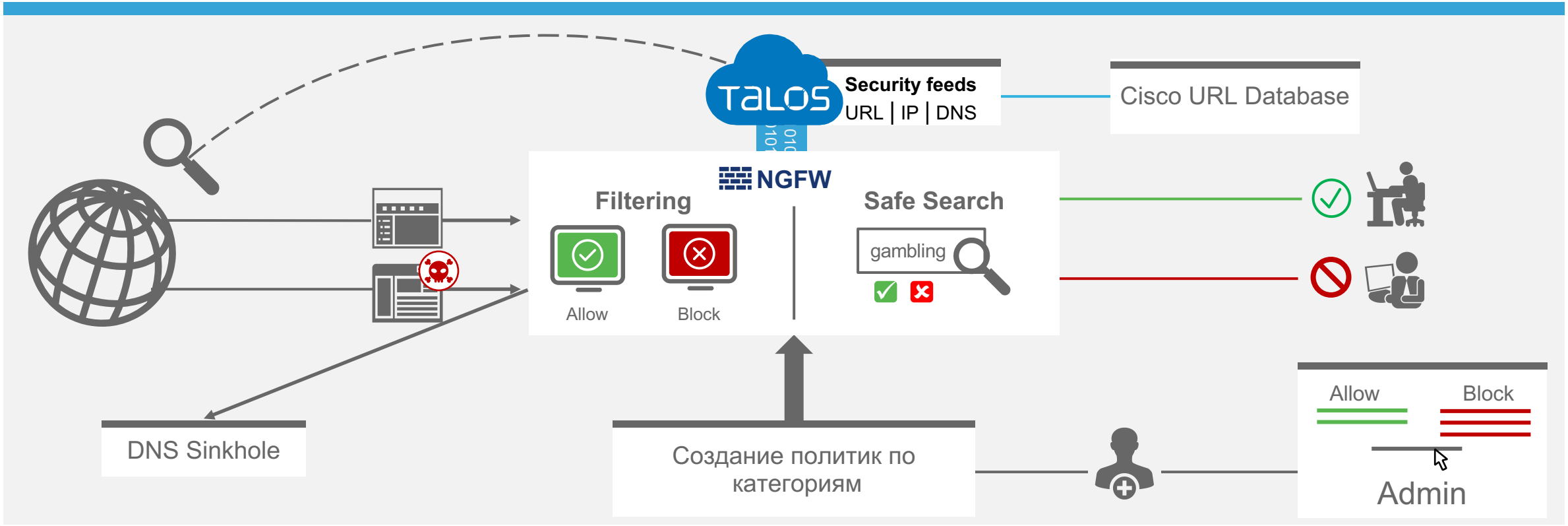
Инспекция расшифрованных пакетов

Отслеживание и учет SSL сессий

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Контроль доступа к URL и доменам

Web контроль

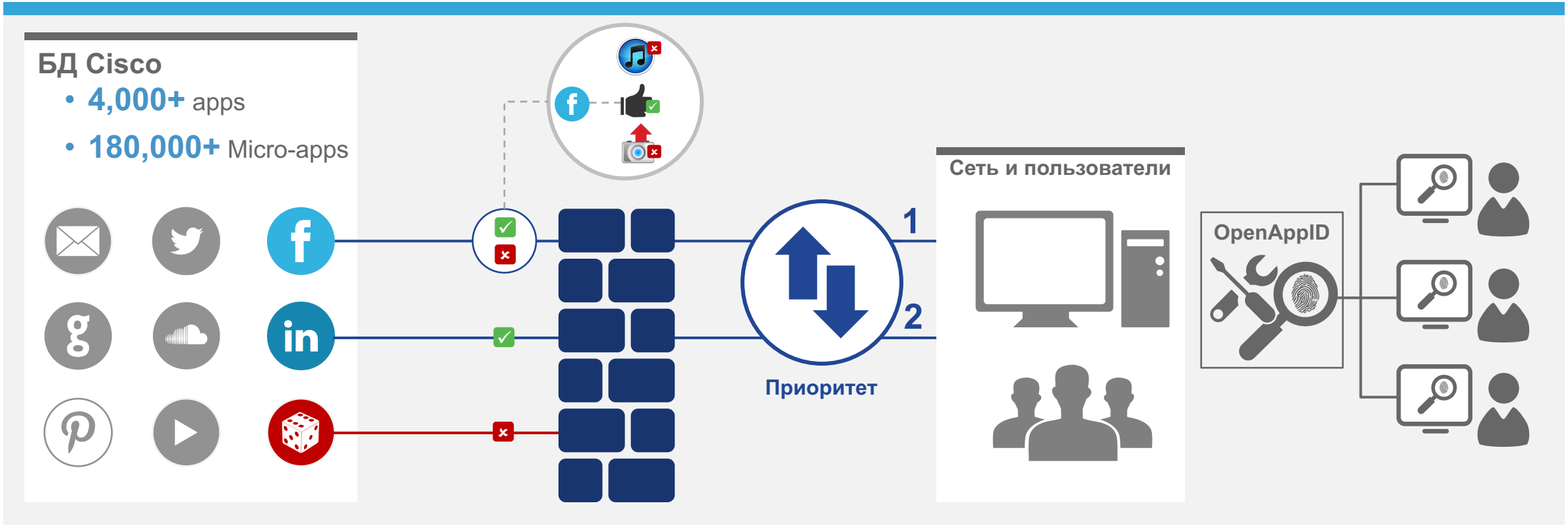


Классификация **280M+** URLs	Фильтрация по **80+** категориям	Простое управление списками Allow/Block	Блокирование вредоносных URL

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Видимость работы приложений нового поколения

Application Visibility & Control



Видеть и понимать риски	Применение детального контроля доступа	Приоритет по трафику и ограничение полосы	Создание детекторов для своих приложений

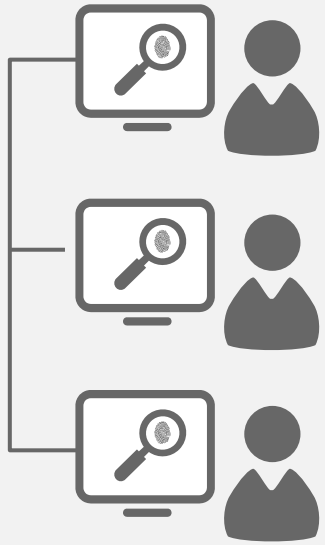
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Расширение AVC на проприетарные и пользовательские приложения

OpenAppID

Самообслуживание

Open-Source

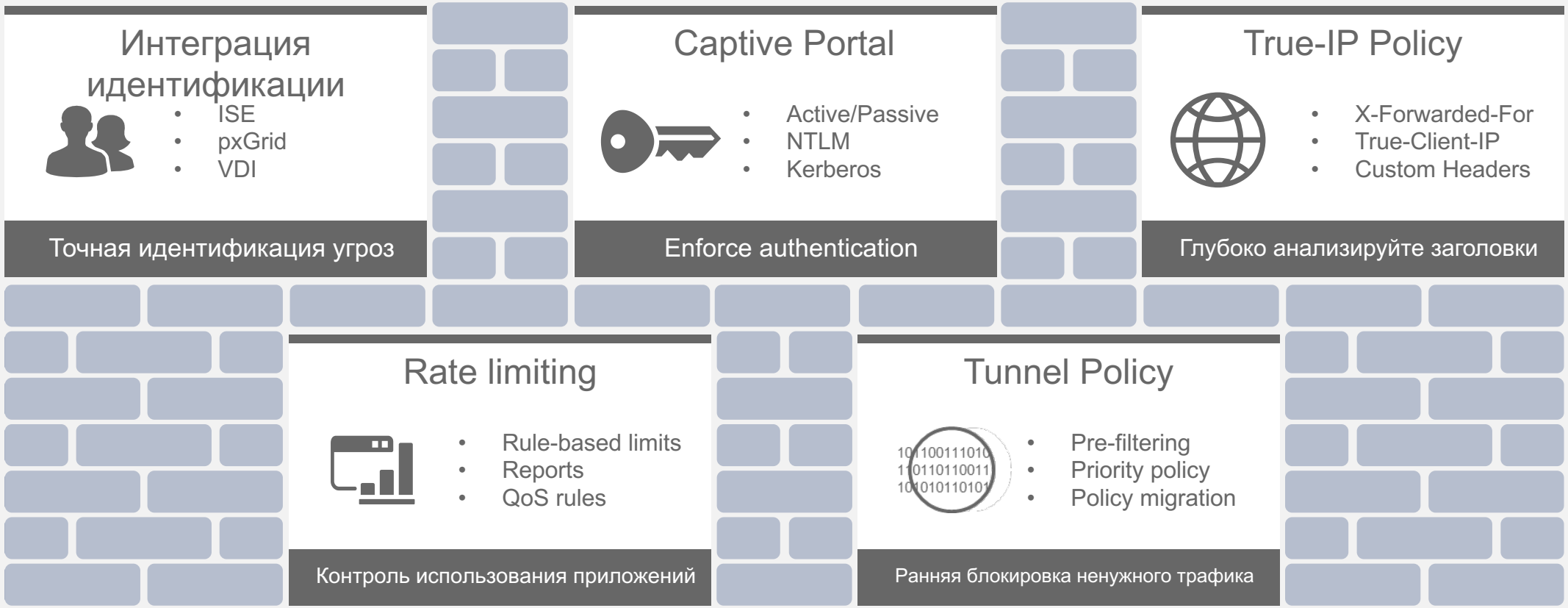


Простая кастомизация детектора прилоежний	Обнаружение пропиретарных и пользовательских приложений	Поделитесь детекторами с другими пользователями

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Усовершенствование контроля над трафиком с помощью набора функций

Дополнительные функции Firewall



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Разные режимы развертывания

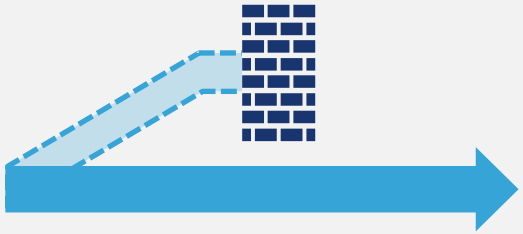
Режимы развертывания Firewall

Inline или Passive

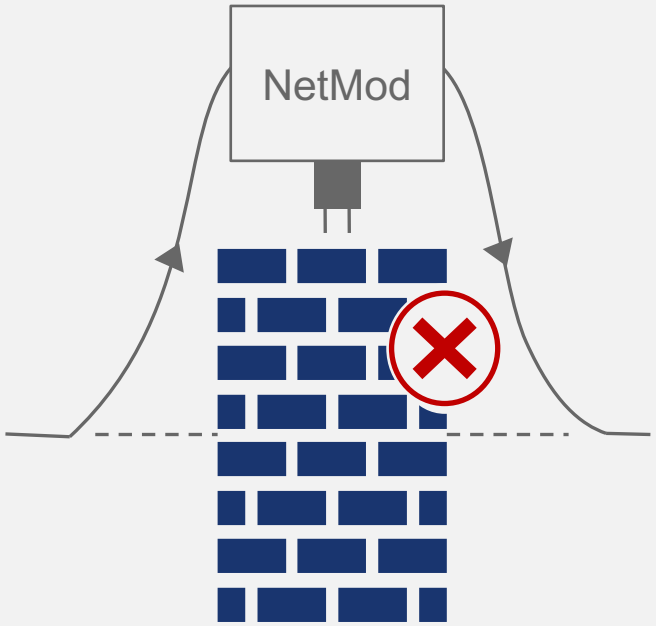
Inline

Inline Tap

Passive

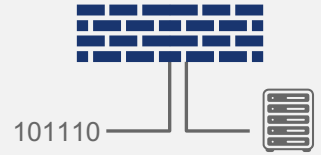


Fail-to-wire NetMods

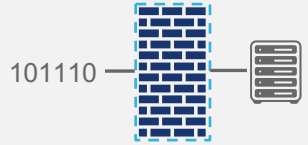


Дополнительные опции

Routed



Transparent



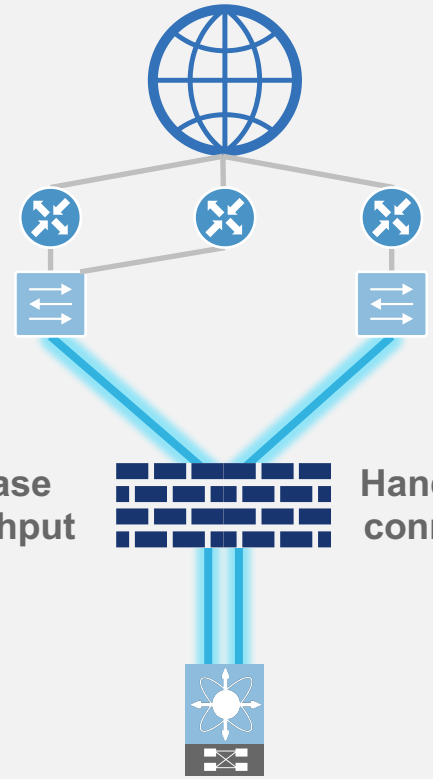
Виртуальный или физический

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Масштабируемая производительность на несколько локаций

Кластеризация

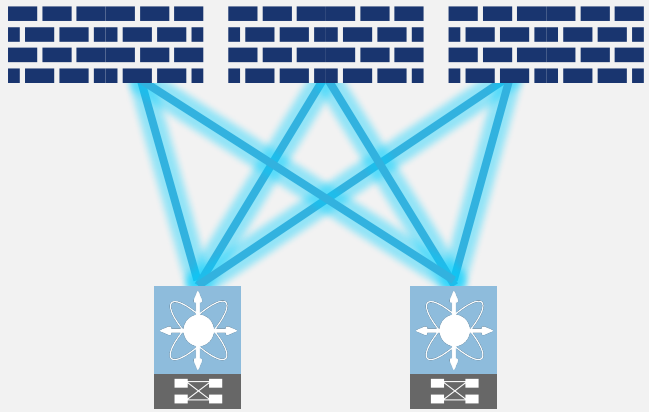
Масштабируемость линков



Increase throughput

Handle more connections

Распределение

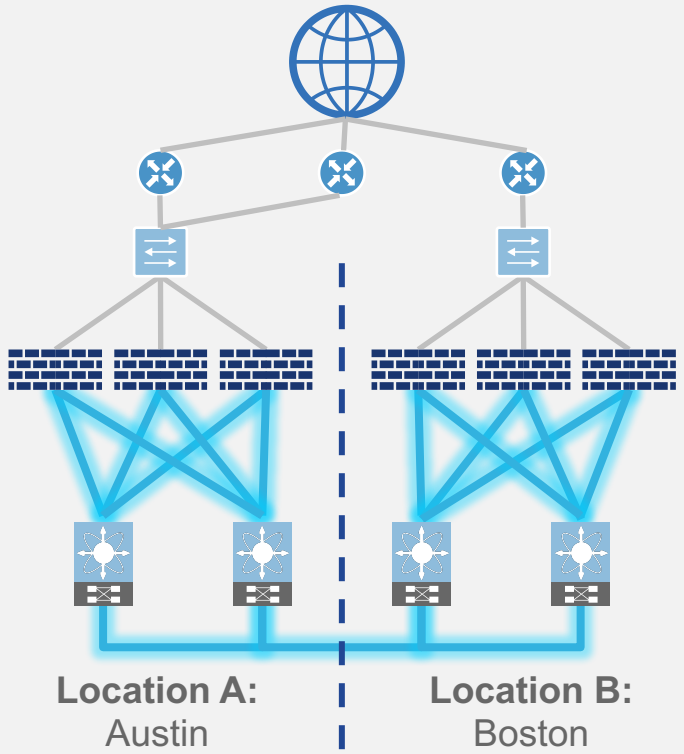


Работайте с

16

Индивидуальными устройствами

Inter-site Clustering



Location A: Austin

Location B: Boston

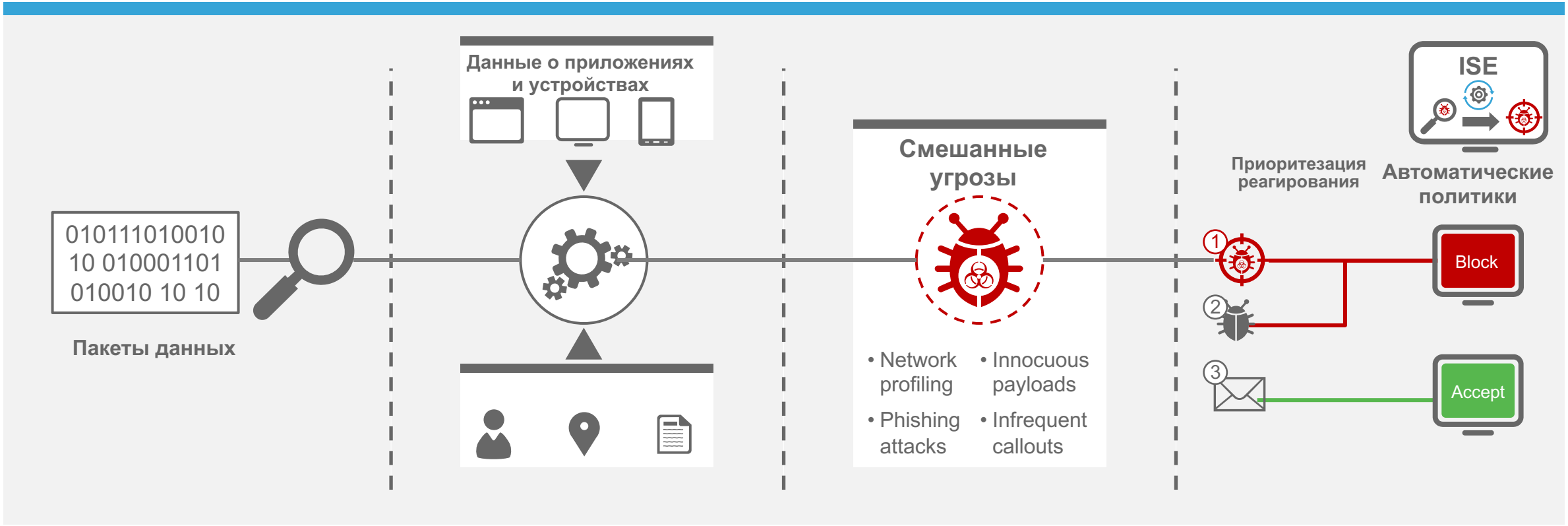
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Защита от угроз

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Понять детали угрозы и быстро отреагировать

Next-Generation Intrusion Prevention System (NGIPS)



Сканирование трафика сети	Корреляция данных	Обнаружение скрытых угроз	Реагирование в зависимости от приоритета

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Найти скрытые угрозы в среде

Advanced Malware Protection (AMP)

Заблокировать известный malware	Безопасное исследование файлов	Обнаружение новых угроз	Реагирование на предупреждения

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Остановите от проникновения скрытые угрозы

Security Intelligence

TALOS

На базе URL

Заблокируйте рискованные веб-узлы с помощью нашей базы из

270 million+

Известных URL

На базе IP

Отфильтруйте плохие IP с помощью нашей базы из

70,000+

Известных IP

На базе DNS

Получите защиту в реальном времени с помощью информации о

80 млрд+

Ежедневных запросов DNS

Понимание рисков с помощью репутации

Увидеть больше

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Защита в реальном времени от глобальных угроз

Talos

TALOS

Threat Intelligence

1.5 млн экземпляров malware в день

600 млрд почтовых сообщений в день

16 млрд веб запросов в день

Покрытие безопасности

Endpoints

Web

Networks

NGIPS

Devices

Исследование

250+
исследователей

24 x 7 x 365
Operations

Идентификация сложных атак	Получение специфической информации	Остановите скрытые угрозы	Оставайтесь защищенными с обновлениями

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Управление

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Простое управление NGFW в нескольких узлах

Firepower Management Center

Централизованное управление для распределенной сети

- Мультидоменное управление
- Role-based access control
- Высокая доступность
- API и pxGrid интеграция
- Firewall & AVC
- NGIPS
- AMP
- Информация безопасности

…Доступна в опции физического и виртуального устройства

Управление в нескольких узлах	Управление доступом и политиками	Расследование инцидентов	Приоритет опций реагирования

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Простое управление индивидуальными NGFW

Firepower Device Manager

Integrated on-box option for single instance deployment

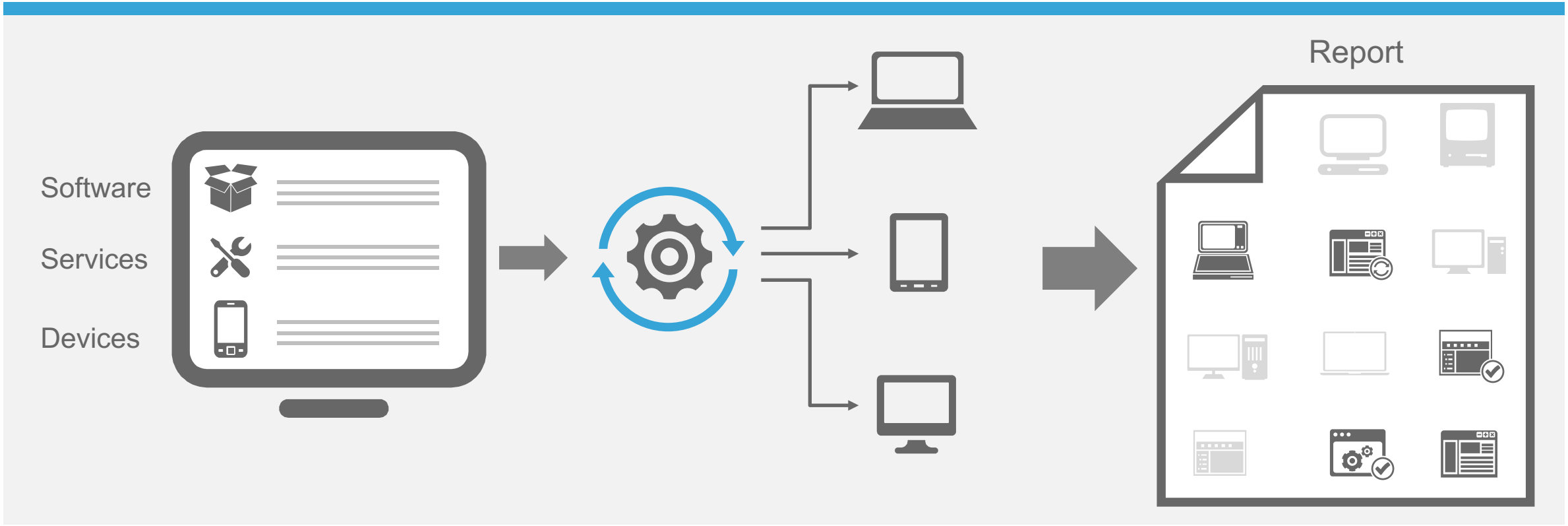
- Простая установка
- Ролевой доступ
- Высокая доступность
- Физическое устройство
- NAT и Routing
- Intrusion and Malware prevention
- Мониторинг
- VPN поддержка

Простая установка	Контроль доступа и политики	Расследование инцидентов	Приоритет реагирования

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Know what and when you need to update

Smart Licensing



View software, services, and devices in one easy to use portal	Activate software automatically	Extend licenses automatically	Track software usage with regular reports to Cisco

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Помощь в миграции на Firepower

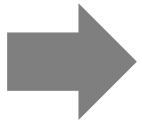
Инструмент миграции

Предыдущее устройство ASA

Политики

Настройки

Группы



Firepower NGFW

Политики

Настройки

Группы

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Передовая автоматизация Cisco NGFW

Он совсем не похож на то, что используют другие!

Использование контекста

Создание профилей узлов, ISE pxgrid, интеграция со сканерами уязвимостей

Автоматизированная настройка

Автоматическое создание политик безопасности на основании профиля сети

Оценка уровня влияния и IoC

Корреляция угроз уменьшает количество событий, которые требуют реакции на 99%

Идентификация приложений, которой вы можете доверять

OpenAppID

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Исполняемое обнаружение

Ваши события релевантны?

Флаг влияния коррелирует

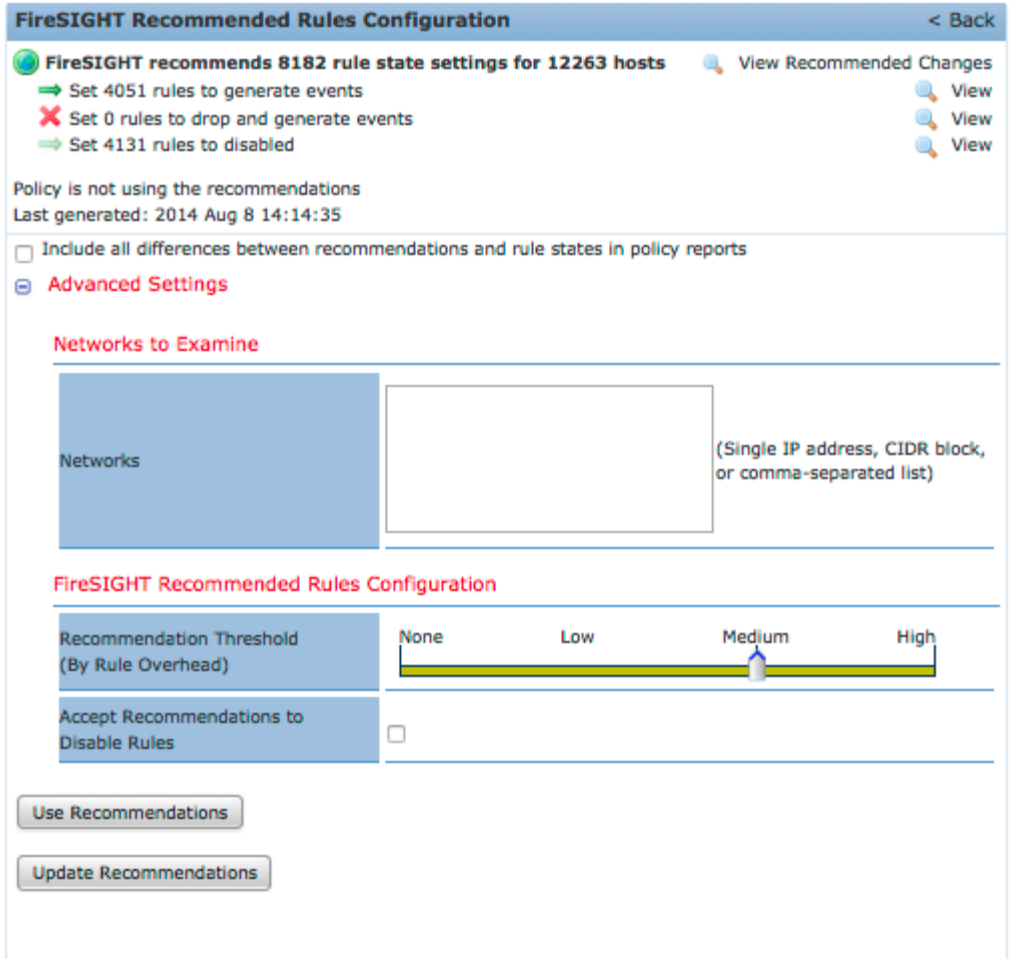
- Профиль узла
- События безопасности
- Сканеры уязвимостей

IMPACT FLAG	ADMINISTRATOR ACTION	HOW
	Act Immediately, Vulnerable	Host vulnerable to attack or showing an IOC
	Investigate, Potentially Vulnerable	Relevant port or protocol in use but no vuln mapped
	Good to Know, Currently Not Vulnerable	Relevant port not in use
	Good to Know, Unknown Target	Monitored network, but unknown host
	Good to Know, Unknown Network	Unmonitored network

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Простая настройка

- Мы всегда сможем увидеть атаку, чтобы ее заблокировать
- Контекст позволяет «автонастройку» для вашей сети



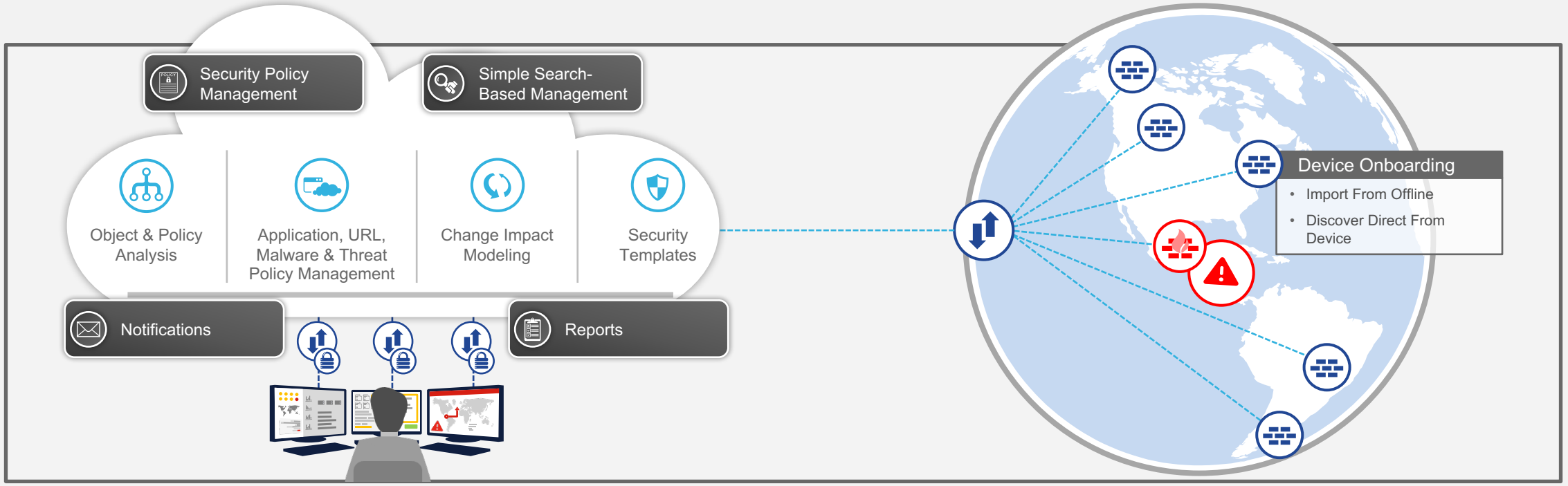
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Интеграция

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Применение согласованных политиках во всех локациях

Cisco Defense Orchestrator



Упростить управление политиками в облаке с помощью Cisco Defense Orchestrator Security

Планирование и моделирование изменений в политиках безопасности перед их применением в облке

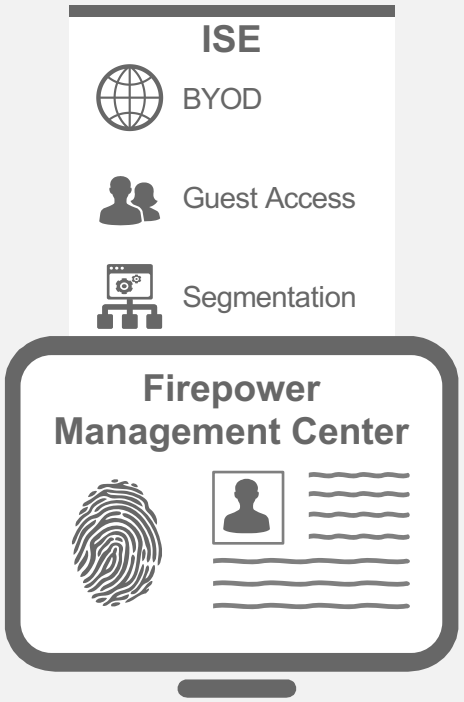
Внедрение изменений в виртуальных средах в реальном времени или offline

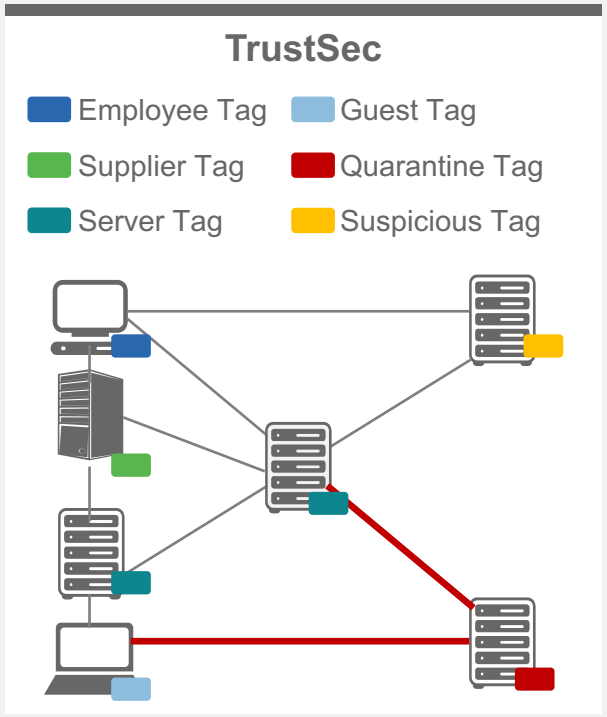
Получение уведомлений о любых незапланированных изменениях в политиках безопасности и объектах

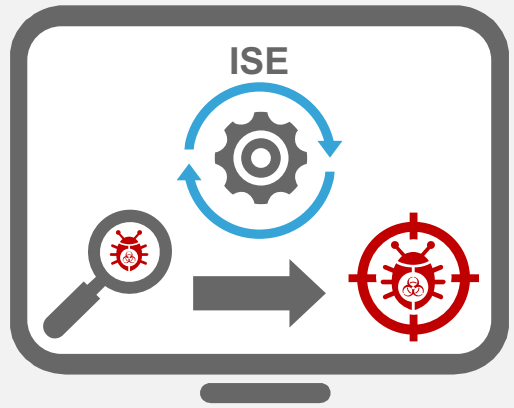
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Гарантировать соответствие перед предоставлением доступа

Identity Services Engine (ISE)







Автоматизация политик

Установка политик доступа	Распространение правил и контекста	Создать безопасную сеть	Немедленноая коррекция брешей

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Построено на открытой платформе

REST API и интеграция с другими вендорами

Дополнительный функционал

- Authentication tokens
- Access control
- Virtual switch

Другие решения

- Radware DDoS
- VDI identity
- VPN возможности

APIs

Firepower Management Center

API Explorer

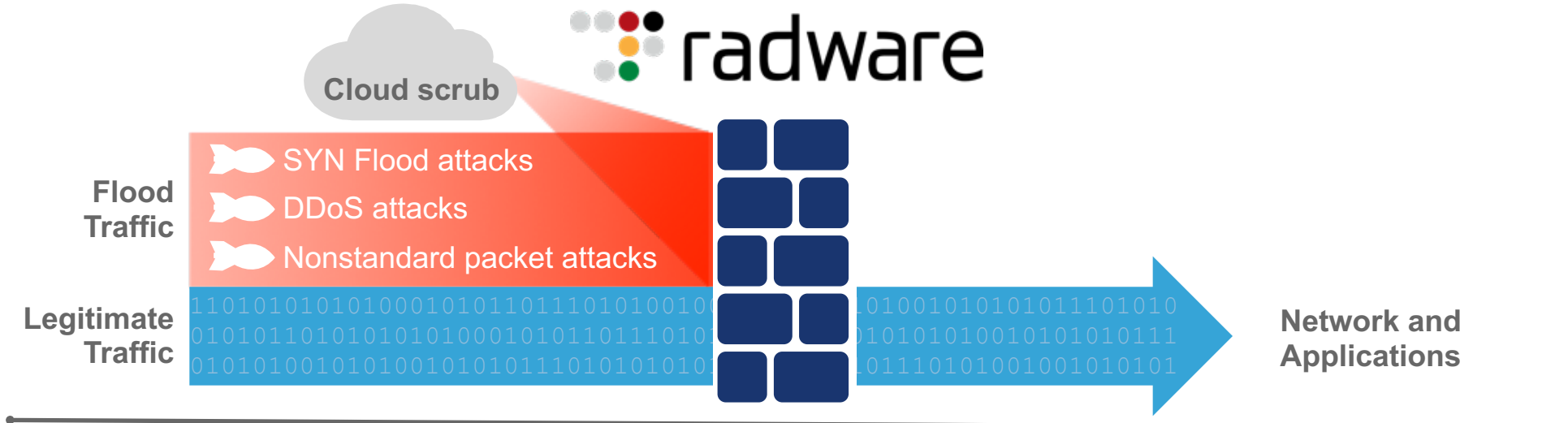
Дополнение функциональности с помощью других решений

Интеграция пользовательских возможностей

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Предотвратить отказ сети и приложений

Radware DDoS vDP



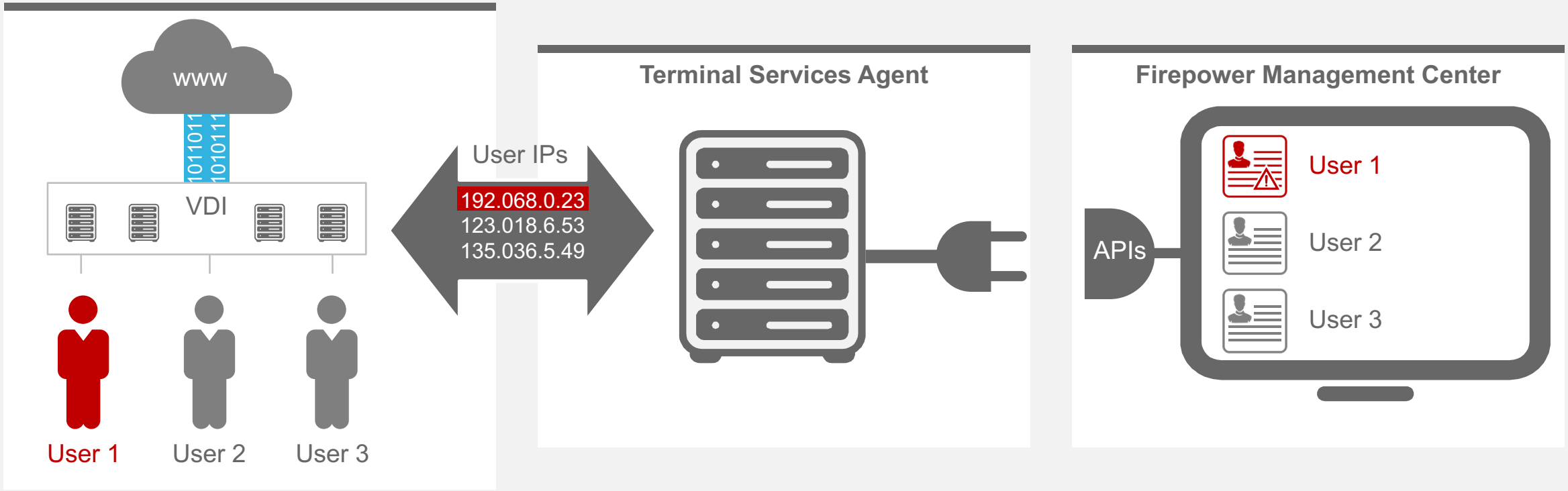
Остановить атаки в течение секунд после обнаружения

Автоматическое блокирование и разрешение трафика

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Идентификация угроз скрытых за виртуализацией

Virtual Desktop Infrastructure (VDI) Identity



Направляет пользовательскую информацию из Terminal Services

Собирает информация с помощью API

Определяет рискованное поведение

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Увидеть веб-атаки перед тем, как они достигнут вашей сети

Cisco Umbrella

65 млн

Ежедневных активных пользователей

80 млрд

DNS запросов в день

160+

стран

Уникальный подход

- Теория графов
- Машинное обучение
- Искусственный интеллект
- 3D визуализация

Опытная команда

- Ученые
- Инженеры
- Математики
- Исследователи безопасности

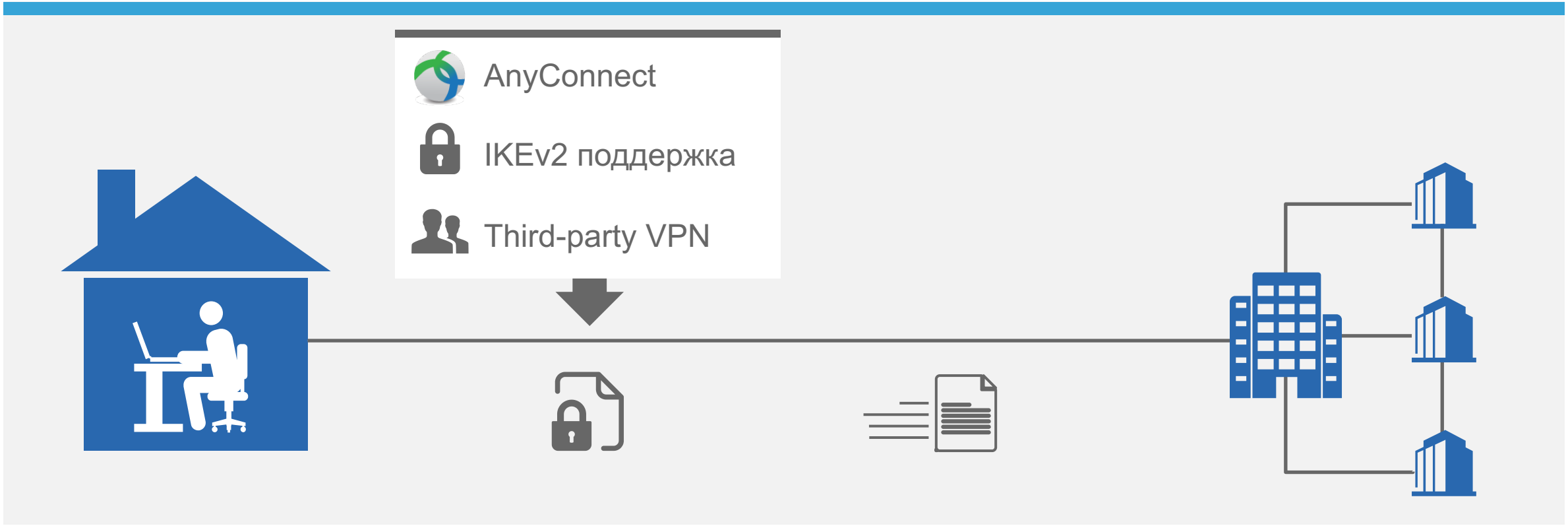
Получить информацию из большой базы данных

Увидитель больше угроз

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Распространить безопаность на удаленных пользователей и региональные офисы

Remote и site-to-site VPN

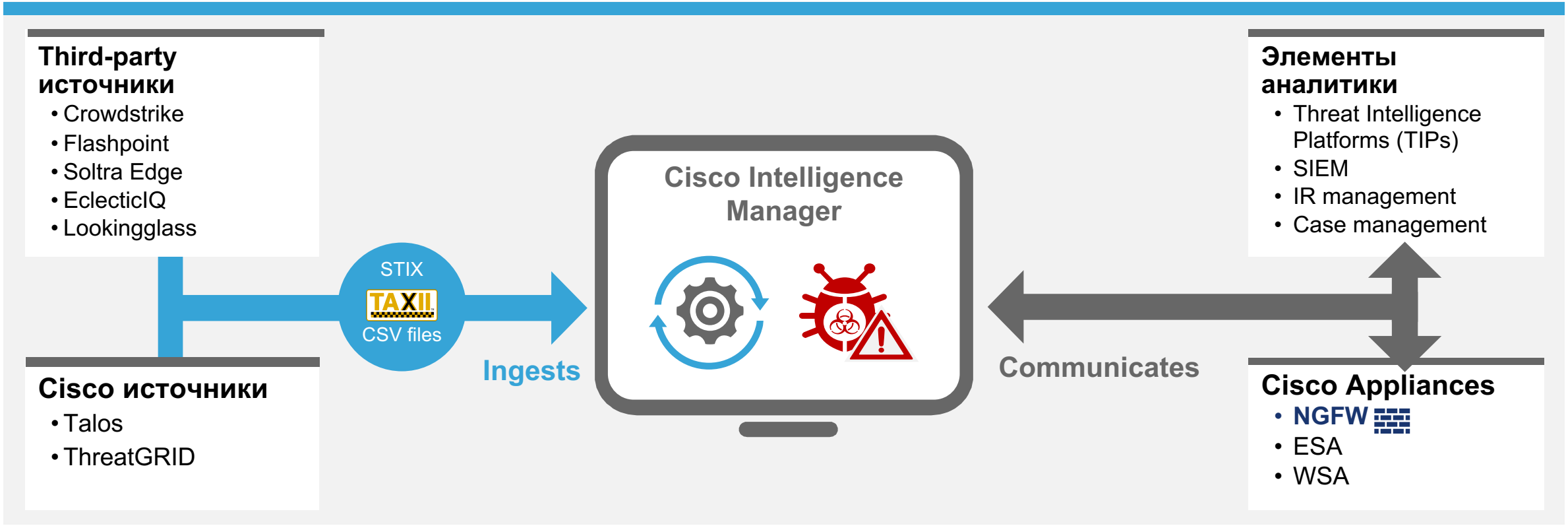


Удаленноый доступ	Защита важных данных	Сохранить производительность приложений	Подержка нескольких точек

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Интегрировать другую информацию о безопасности

Cisco Intelligence Manager



Анализ информации о безопасности	Корреляция наблюдений	Генерация отчетов об инцидентах	Пересмотр анализа безопасности

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Доступна в нескольких форм-факторах

Физический, виртуальный, облако

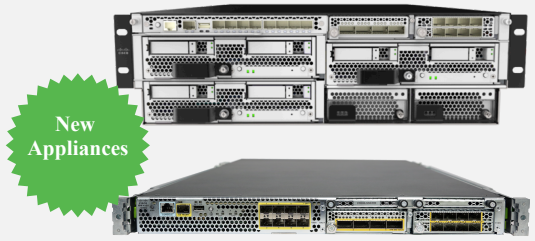
- AWS
- Azure

Также как отдельные решения

NGIPS only

Dedicated AMP

И высокопроизводительные устройства…



Cisco Firepower™ 4100 Series и 9300

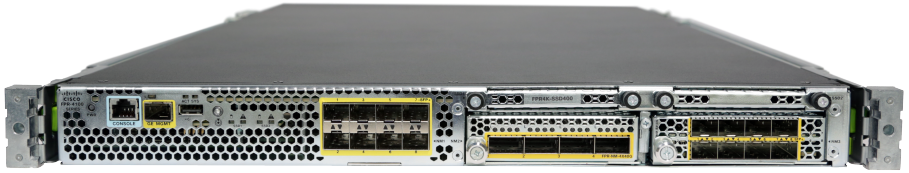
Cisco Firepower Threat Defense на ASA 5500-X

Cisco FirePOWER™ сервисы на ASA 5585-X

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Firepower 4100 Series

Представляем новые высокопроизводительные модели!



Оптимизация для производительности и плотности

- 10-Gbps и 40-Gbps интерфейсы
- До 80-Gbps производительность
- 1-rack-unit (RU) форм-фактор
- Низкая задержка (5 мкс)

Мультисервисная безопасность

- Интегрированные механизмы инспекции FW, NGIPS, Application Visibility and Control (AVC), URL, Cisco Advanced Malware Protection (AMP)
- Radware DefensePro DDoS
- ASA и другие в будущем

Унифицированное управление

- Простой интерфейс управления с Firepower Threat Defense
- Унифицированные политики с наследованием
- Выбор опций развертывания

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Firepower 9300 Platform

Высокая скорость, масштабируемая безопасность

Модульный

Выгоды
- Стандарты и взаимодействие
- Гибкая архитектура

Функции
- Безопасность по шаблонам
- RESTful/JSON API
- Оркестрация и управление

Мультисервисная безопасность

Выгоды
- Интеграция лучшей безопасности
- Динамическое объединение сервисов

Функции*
- Cisco® ASA контйнер
- Cisco Firepower™ Threat Defense контейнеры:
  - NGIPS, AMP, URL, AVC
- Другие контейнеры:
  - Radware DDoS
  - Экосистемные партнеры

Операторский класс

Выгоды
- Производительность:
  - Свыше 1 Тб
  - Высочайшая плотность портов

Функции
- Компактный , 3RU
- 10-Gbps/40-Gbps I/O; 100 Gbps
- Терабитный backplane
- Низкая задержка, быстрые маршруты
- Network Equipment-Building System (NEBS)

* Contact Cisco for services availability

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Добавить огня к уже установленным ASA

Межсетевой экран ASA 5585-X

FirePower-модуль

SSD-диск

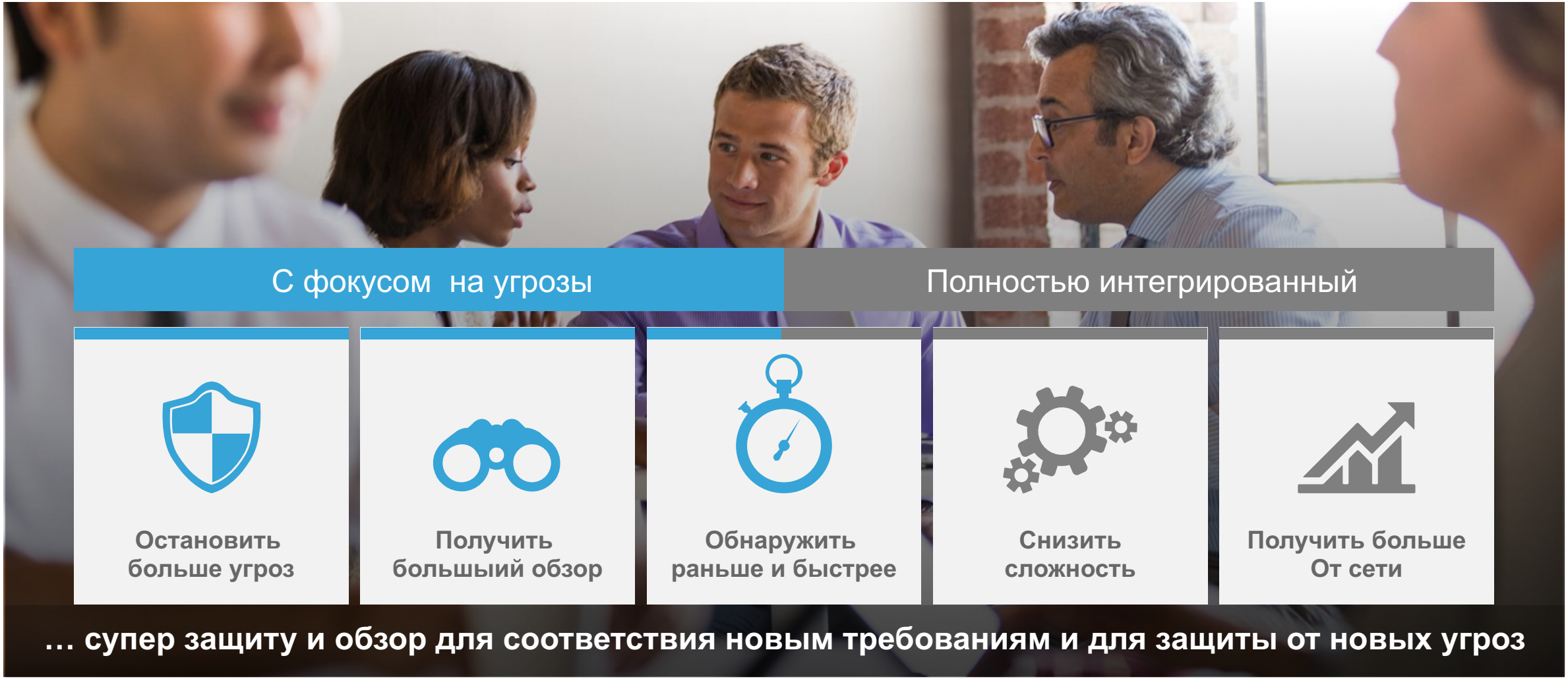
Межсетевой экран ASA 5500-X

ПО Firepower

1. **Бесплатный базовый функционал NGFW (Firewall – AVC), дополнительно подписки на IPS, AMP, URL)**
2. **Trade-in** для старых ASA 5500, модулей CX/IPS в 5585 и продуктов конкурентов

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Только Cisco предоставляет…



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Результат говорит сам для себя

17.5 часов

Среднее время обнаружения угрозы с Cisco

100 дней

Среднее время обнаружения угрозы по индустрии

Source: Cisco Annual Security Report 2016

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Следующие шаги

1 **Узнать больше** о том, что для вас может сделать Firepower NGFW

2 **Договоритесь о демо** сегодня для непосредственного опыта

3 **Запросите тестирования** чтобы увидеть, как мы можем улучшить вашу сеть

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TOMORROW starts here.