Перспективные решения Cisco в области информационной безопасности

Василий Томилин
Инженер-консультант
security-request@cisco.com, vtomilin@cisco.com

Предпосылки и план разговора

- Наверное, вы (как-то) представляете себе набор решений Cisco #поИБ
- Возможно, вы слышали о Before/During/After
- Вероятно, вы слышали про открытость и интеграцию, всяческие интерфейсы и т.п. (хотя я напомню)
- Что мы уже сделали - вехи?
- Несколько продуктов, на которых я бы хотел сконцентрировать ваше внимание
- Что мы будем делать?

Ландшафт угроз

Какие решения по ИБ есть у Cisco?

МСЭ и NGFW

- Cisco ASA / ASA-SM
- Cisco IOS Firewall
- Cisco ASAv
- Cisco FirePOWER
- FTD/FTDv

IPS и NGIPS

- Cisco FirePOWER
- Cisco ASA with FirePOWER
- Cisco FirePOWER for ISR
- Cisco wIPS
- Cisco vNGIPS

Advanced Malware Protection

- AMP для Endpoint
- AMP для Network
- AMP для Content
- Threat Grid

Интернет-безопасность

- Cisco WSA / vWSA
- Cisco Umbrella
- Threat Awareness Service

Безопасность электронной почты

- Cisco ESA / vESA
- Cisco Cloud Email Security

NAC + Identity Services

- Cisco ISE / vISE

VPN

- Cisco AnyConnect
- Cisco ASA
- Cisco ISR / RVPN

UTM

- Meraki MX
- ASA with FirePOWER
- Firepower

Объективный контроль

- Cisco Stealthwatch

Сегментация/доступ

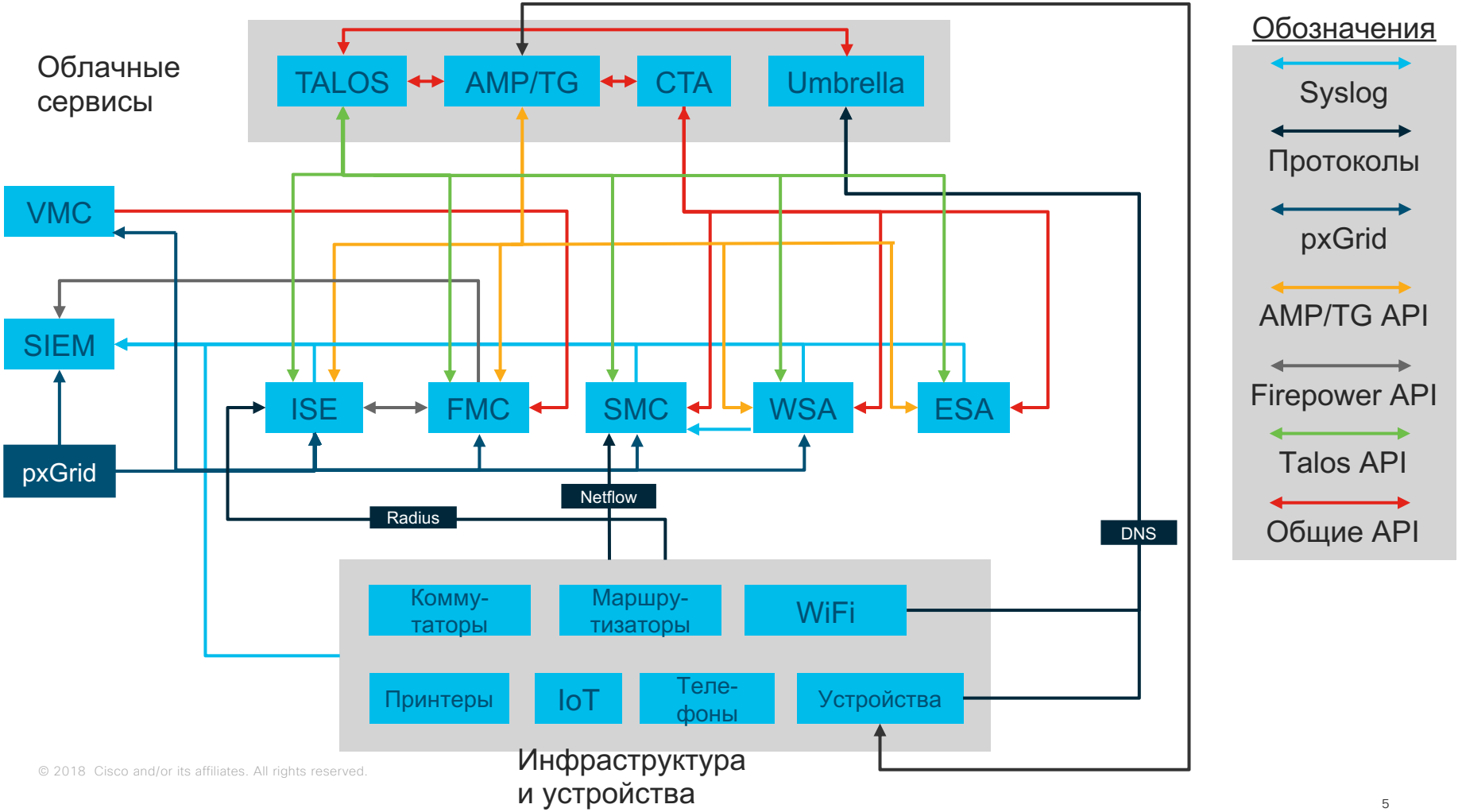
- Cisco TrustSec
- Cisco ISE

Защита ЦОД

- Cisco ASA / 1000v / ASAv / FTDv
- Cisco TrustSec

Контроль приложений

- Cisco ASA NGFW / AVC
- Cisco IOS AVC / NBAR
- FirePOWER NGFW



Cisco Security 2019

Да, всего много… а что списано?

https://www.cisco.com/c/en/us/products/eos-eol-listing.html

Быстрая проверка, по каким продуктам (и их версиям) объявлено окончание продаж и поддержки

End-of-Sale and End-of-Life Products

These products are no longer being sold and might not be supported.
Click on the product link, when available, for more information.

Please see the **End-of-Life Policy** for more details.

Products End-of-Sale and End-of-Life RSS

Analytics and Automation Software

Cisco ServiceGrid

Application Networking Services

Cisco ACE 4700 Series Application Control Engine Appliances

- Cisco ACE 4710 Application Control Engine

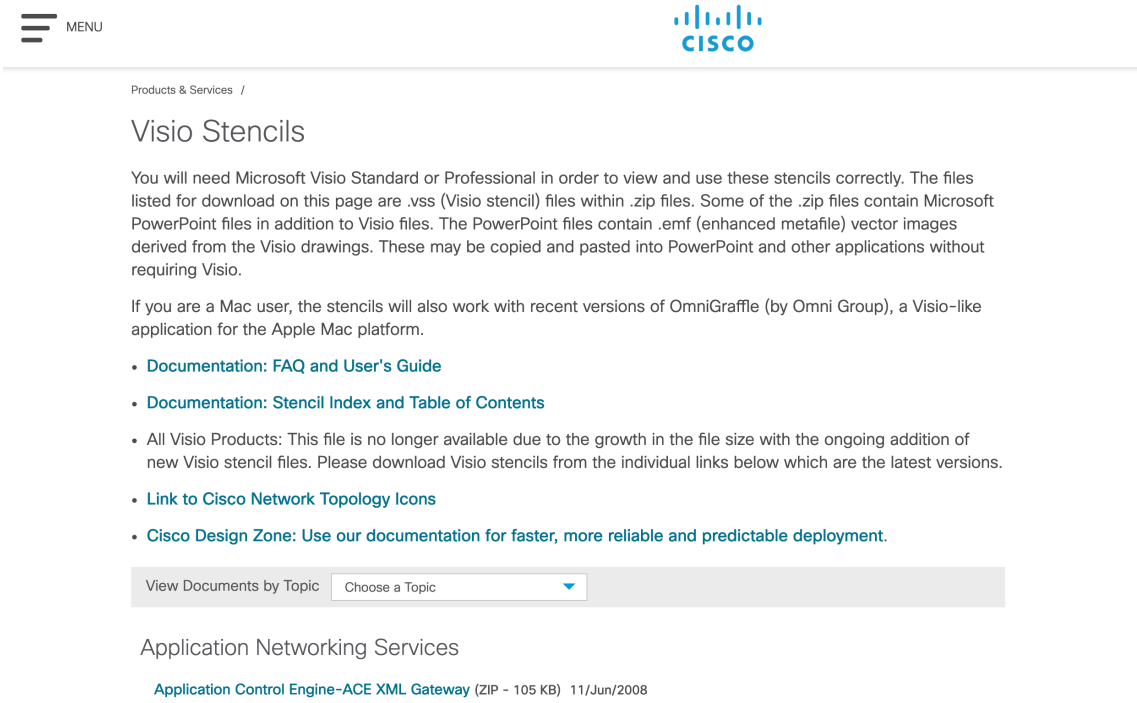
Cisco ACE GSS 4400 Series Global Site Selector Appliances

- Cisco GSS 4492R Global Site Selector

А как нарисовать схему умному заказчику?

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

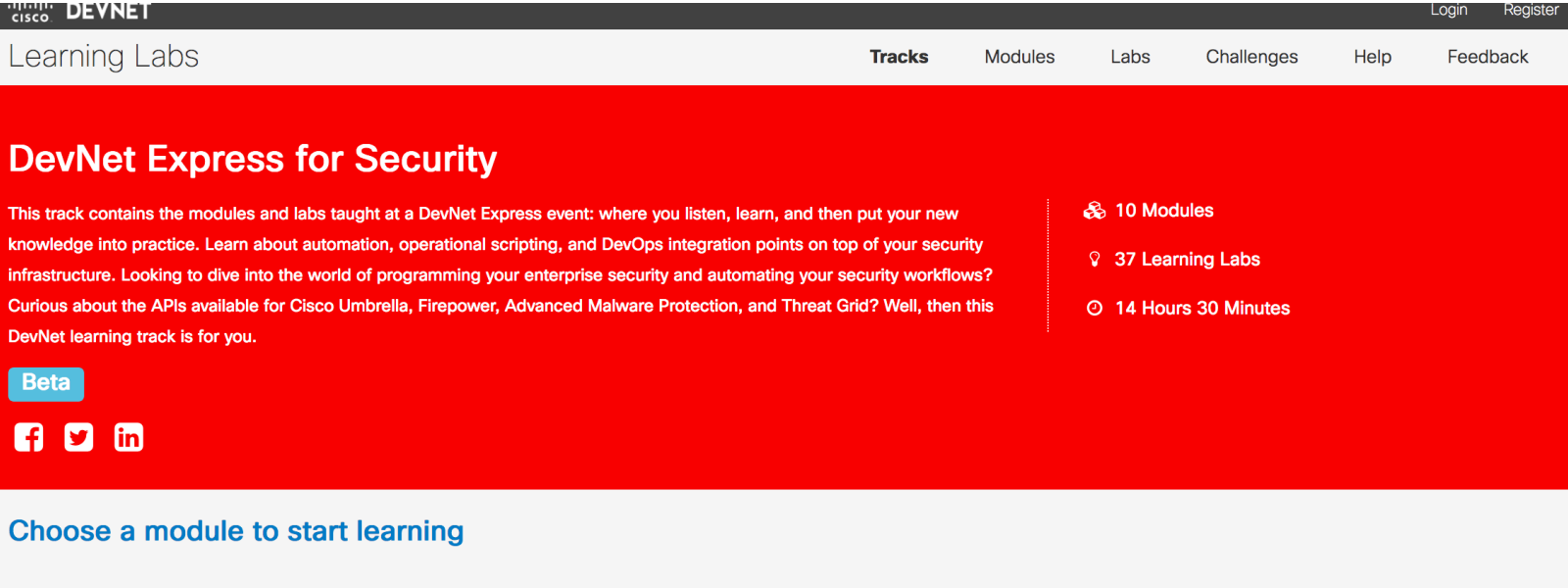
Ресурс, позволяющий найти иконки продуктов Cisco для использования их в MS Visio



Все для интеграции: Cisco DevNet

- Developer.cisco.com – единая точка входа.
  Множество API для решения самых разных задач.
- Learninglabs.cisco.com – практические лабораторные работы для освоения представленного материала
  (уроки для инженеров)

Мы запустили модуль по безопасности

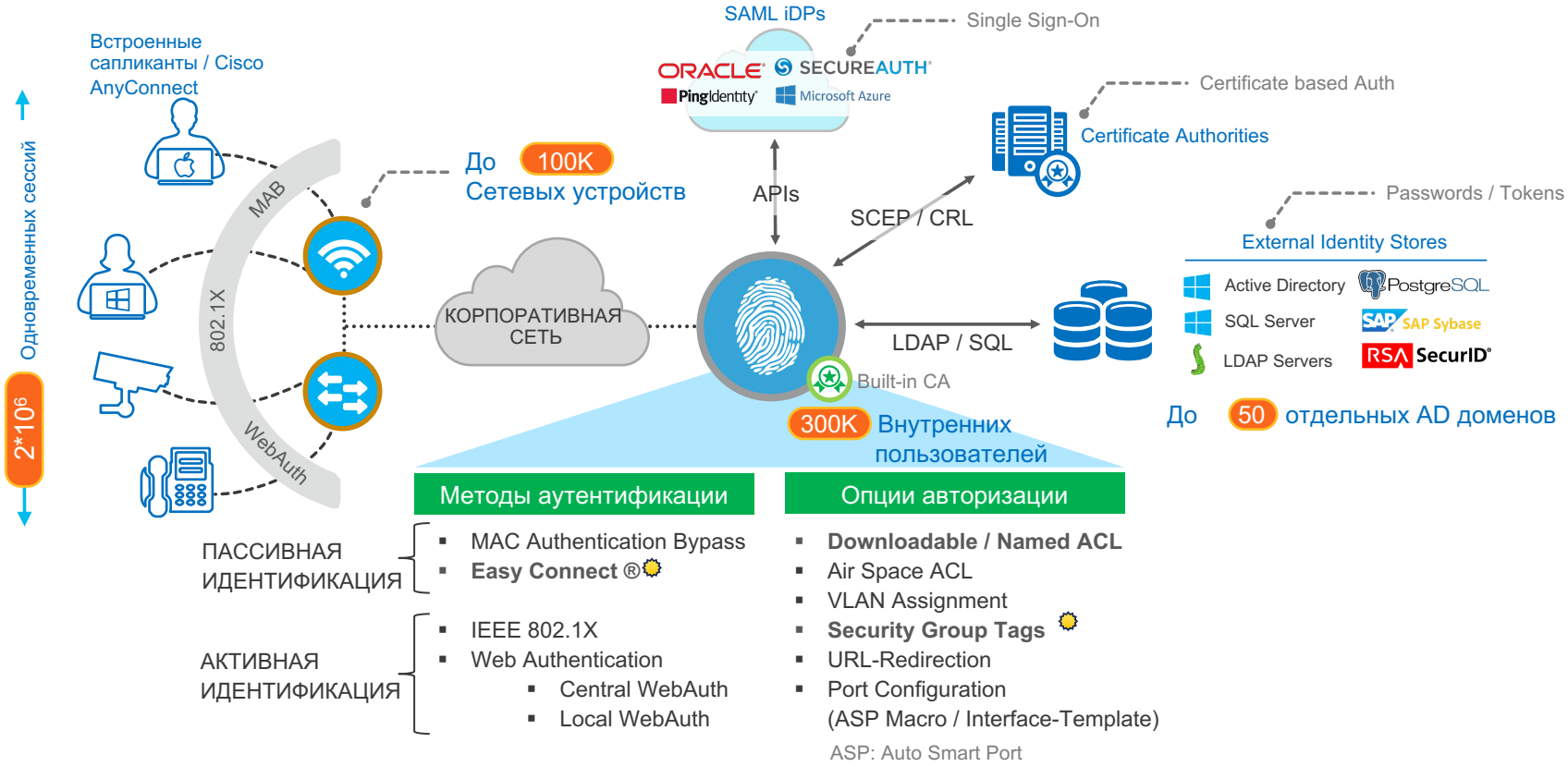


Мы продолжаем развитие

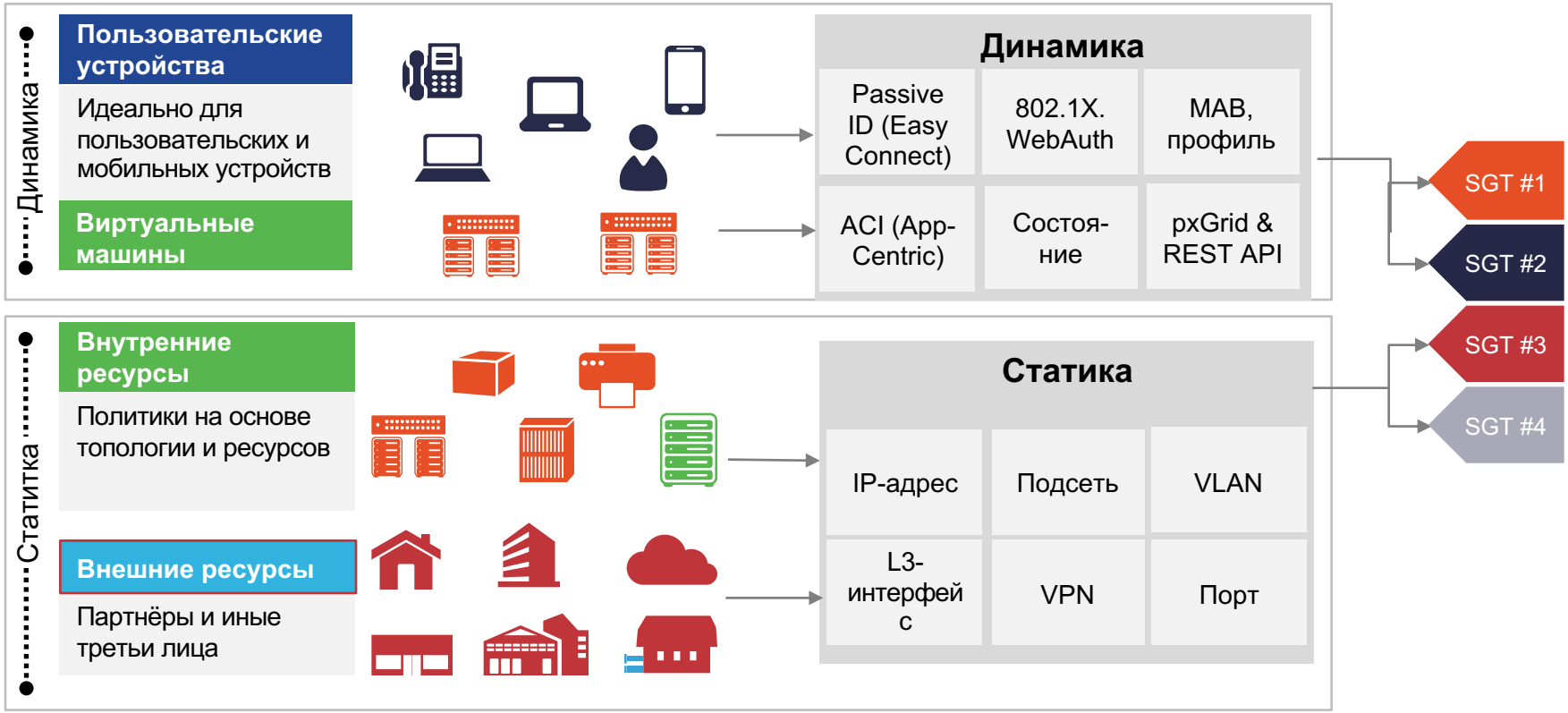
Вы помните про Cisco ISE? Теперь уже 2.6

- Расширение максимального развертывания до $2 * 10^6$ активных одновременных подключений
- Расширение поддержки IPv6 на management
- Поддержка идентификации рабочих станций по UDID, а не MAC-адресу с AnyConnect 4.7 (уже выпущен и работает) – специально для «коворкинга» и «нового стиля работы»
- Более гибкие возможности Grace Period и настраиваемые уведомления (для Posture) с AnyConnect 4.7
- Проверка внесения изменений в инфраструктуру и отчеты после изменения политик TrustSec
- Аутентификация в AD логинов по CLI и REST API
- Поддержка Manufacturer Usage Descriptor (MUD) для создания профилей и автоматического создания устройств IoT

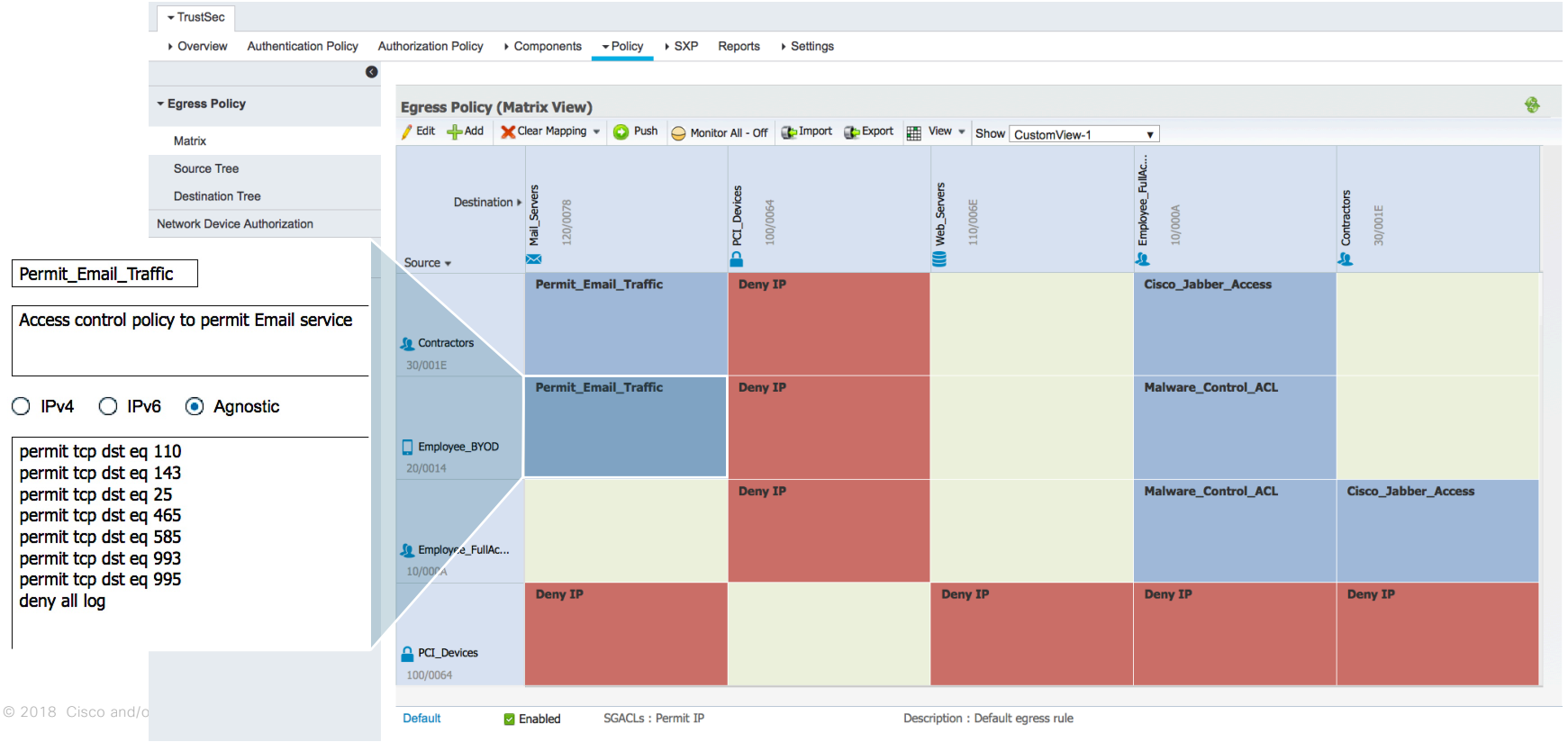
Cisco ISE: поддержка безопасного доступа



Гибкие методы классификации



Будем внимательны с маркетингом: SGACL – это не permit all/deny all



Почему заказчики покупают ISE?

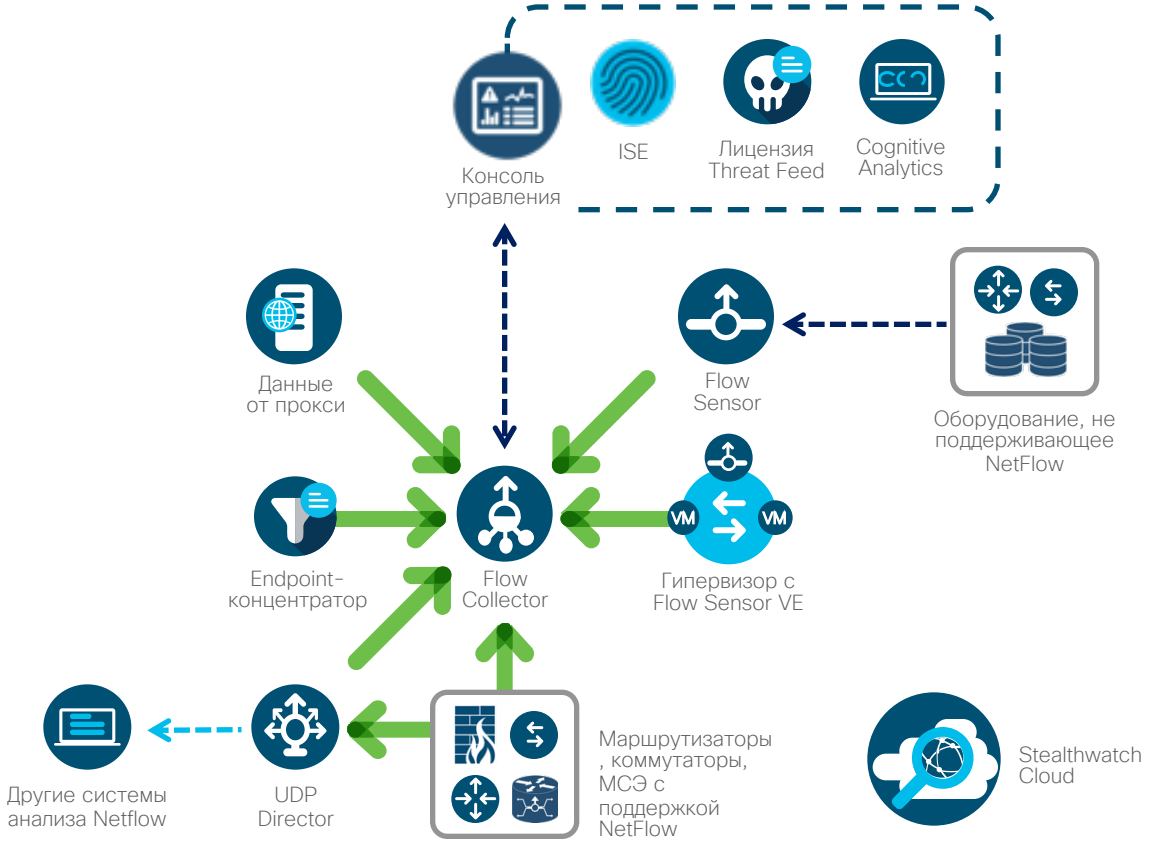
Видимость устройств	Cisco ISE смотрит глубоко на всю сеть и предоставляет непревзойденную видимость того кто и что соединяется к ресурсам.
Контроль доступа	Целостный контроль доступа в проводной, беспроводной и VPN сети.. 802.1X, MAC, WEB-Аутентификация и Easy-connect для контроля доступа
Гостевой доступ	Полностью настраиваемые мобильный и десктоп гостевые порталы с простым визуальным Wizard'ом для простого управления гостевым доступом
BYOD доступ	Упрощенное управление BYOD в строенным CA сервером и поддержкой сторонних MDM интеграций для саморегистрации собственных устройств
Сегментация	Политика топологически-независимой сегментации для сдерживания сетевых угроз с использованием Cisco TrustSec
Контроль угроз	Обмен контекстом с партнерской экосистемой для улучшения их эффективности и уменьшения времени реагирования на инцидент
Доступ администратора	Cisco ISE поддерживает протокол TACACS+ для контроля и аудита конфигурационных изменений на сетевых устройствах.

Вы помните про Cisco Stealthwatch? Уже 7.0

- Существенное расширение функционала веб-интерфейса
- Концепция App-ов
- Модификация API (только REST)
- И многое другое

Система Cisco Stealthwatch

Всеобъемлющий мониторинг **безопасности** и **работы сети**



Обзор преимуществ системы StealthWatch

Угрозы	• Мы обнаруживаем больше, потому что видим больше • Угрозы в сети – это реальность; верить нельзя никому (Stealthwatch можно) • Использование существующей сетевой инфраструктуры для обнаружения и анализа современных угроз
Лучшее решение в своем классе	• Суть: многоуровневые машинное обучение, моделирование, статистический анализ • Единственное решение класса NTA, реализующее ETA • Полная интеграция с другими компонентами подсистемы обеспечения ИБ для ускорения обнаружения и оперативной реакции
Полная видимость	• Полная видимость – основа для обнаружения потенциальных инцидентов • Намного больше, чем классический NetFlow • Критически важна для внедрения и контроля сегментации

Новые возможности и особенности Stealthwatch

Улучшение управления

Security policy manager

Host Group manager

User manager

Упрощение управления

Appliance manager

Update manager

Stealthwatch Apps

Расширение аналитики

Обновления ядра машинного обучения

(Cognitive Intelligence)

Нейтрализация с учётом контекста

Модернизация интеграции с ISE (EPS->ANC)

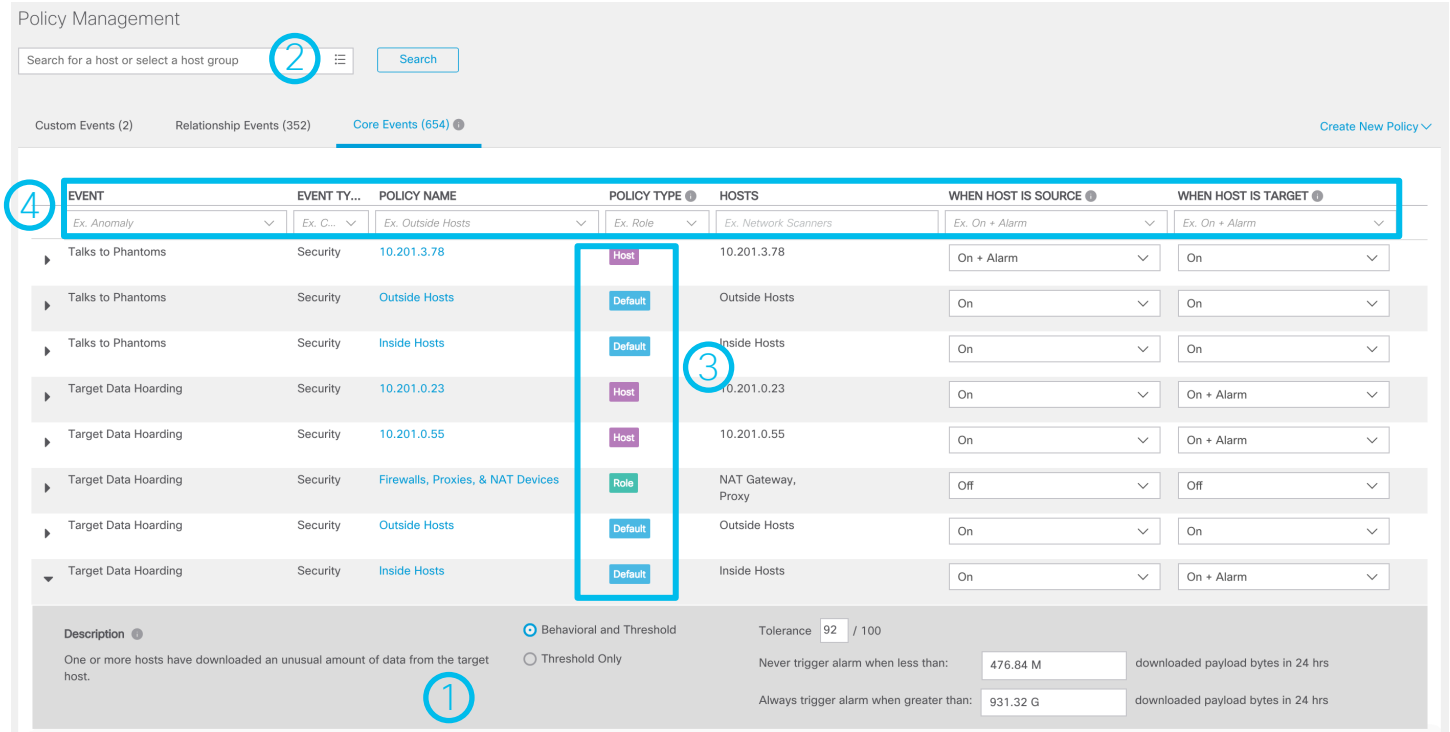
Усовершенствования Policy Manager

- Существенная переработка управления политикой безопасности (чтобы тревоги соответствовали вашей логике)
- Политики Stealthwatch всех трех типов (core, custom и relationship) управляются централизованно с помощью веб-интерфейса
- Простота создания, правки и удаления событий
- Просмотр «эффективной политики» для хоста одним щелчком, простота «проваливания» в тревогу, чтобы настроить параметры события

Управление политикой – Core Events

Configure > Policy Management > Core Events

1. Подробные сведения о тревогах, изменение политик на основании как поведенческих, так и «пороговых» моделей
2. Простота поиска политик, установленных для хоста или группы хостов
3. Просмотр, создание, изменение политик по умолчанию, определение политик для ролей и хостов
4. Фильтрация Core Events по многим параметрам



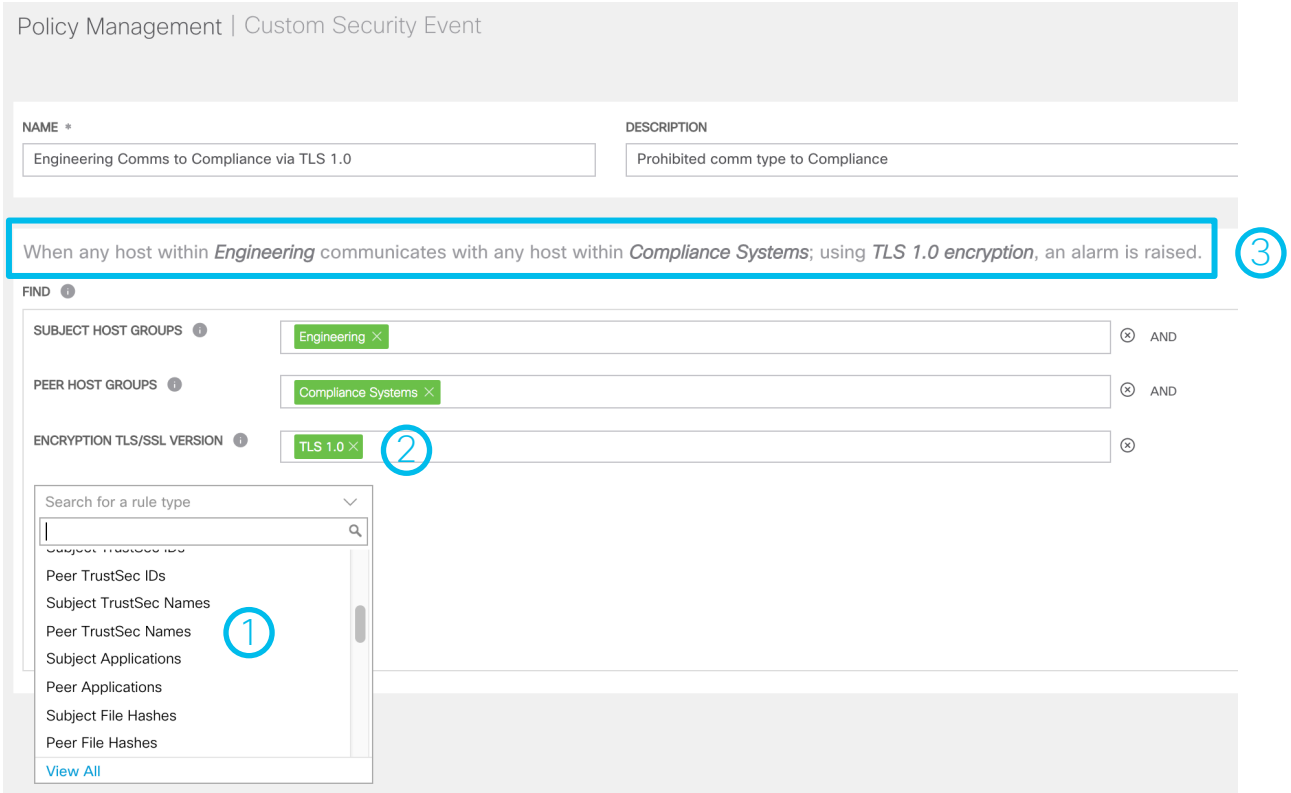
Примечание. Права admin

Управление политикой – Custom Events

Configure > Policy Management > Custom Events

1. Множество параметров для выбора
2. Возможность выбора полей Encrypted Traffic Analytics (ETA) для упрощения криптоаудита
3. Автоматически генерируемое простое, понятное и наглядное изложение правила

Примечание: Custom event'ы в веб-интерфейсе заменяют политики изоляции хостов в Java-клиенте

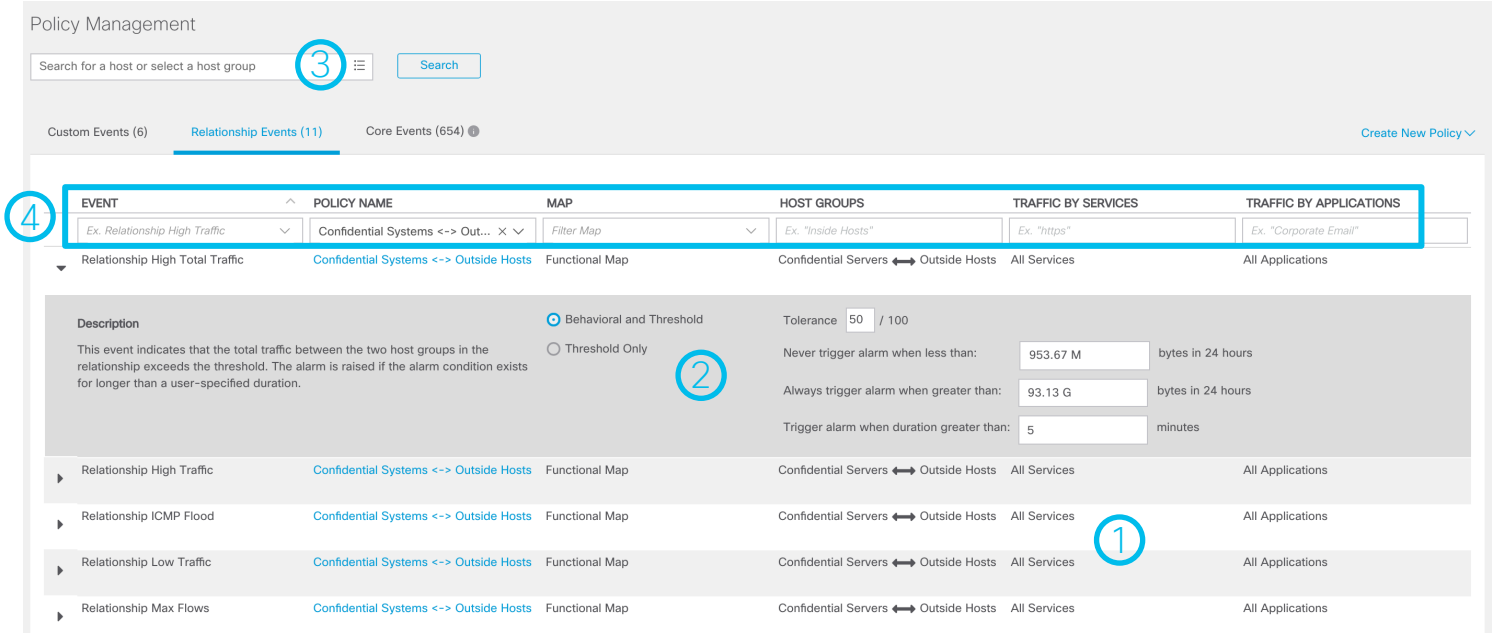


Примечание. Права admin

Управление политикой – Relationship Events

Configure > Policy Management > Relationship Events

1. События «relationship» позволяют контролировать соблюдение политики группами хостов
2. Просмотр и изменение политик на основании поведенческих и «пороговых» метрик
3. Простота поиска политик, заданных для хоста или группы хостов
4. Фильтрация Relationship-событий по многим параметрам



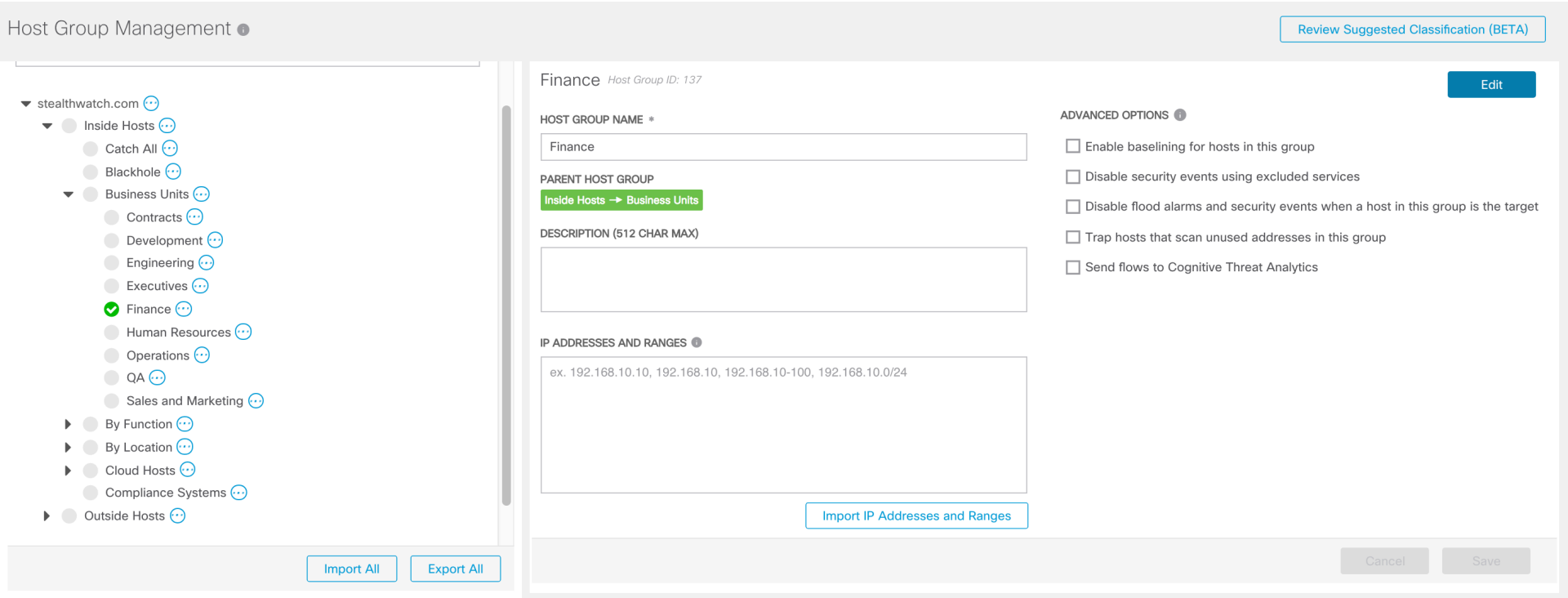
Примечание. Права admin

Усовершенствования User Manager и Host Group Manager

- Добавление пользователей Stealthwatch и настройка их доступа к данным в соответствии с их ролями
- Классификация хостов в Host Groups для повышения эффективности обнаружения аномалий и угроз в соответствии с логикой работы организации

Управление группами хостов

Configure → Host Group Management



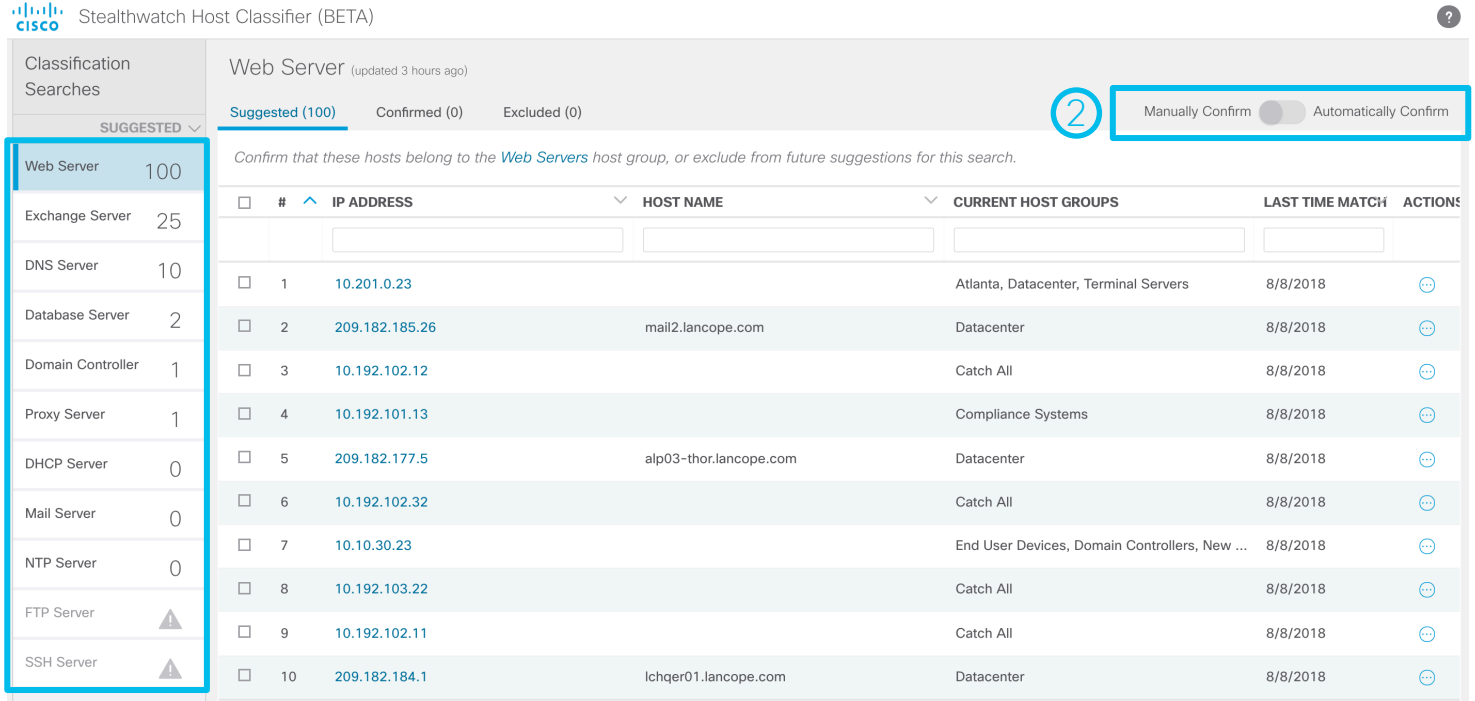
Примечание. Права admin или power analyst

Stealthwatch Host Classifier

(ограниченная доступность, бета)

Configure → Host Group Management → Review Suggested Classification

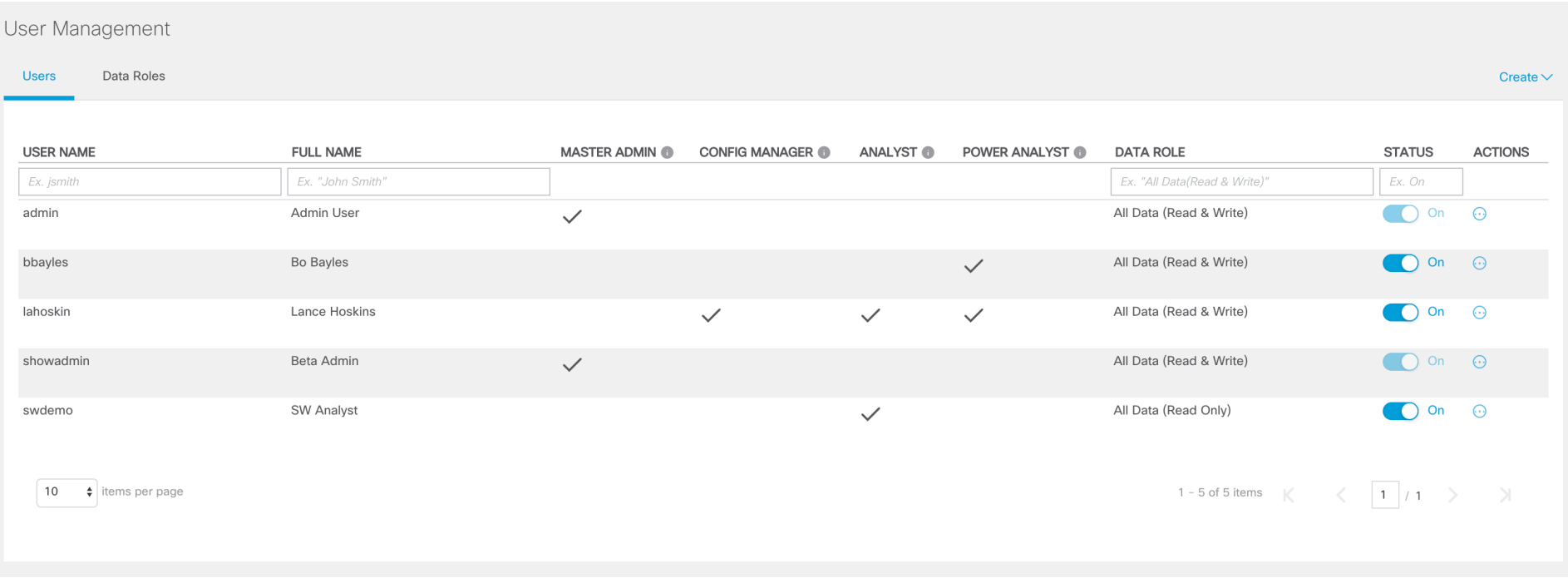
1. Автоматическое распределение хостов по 11 группам
2. Обучение алгоритма классификации по реакции пользователя
3. Анализ выполняется полностью локально, данные не отправляются в облако



Примечание. Права admin

Управление пользователями

Global Settings → User Management



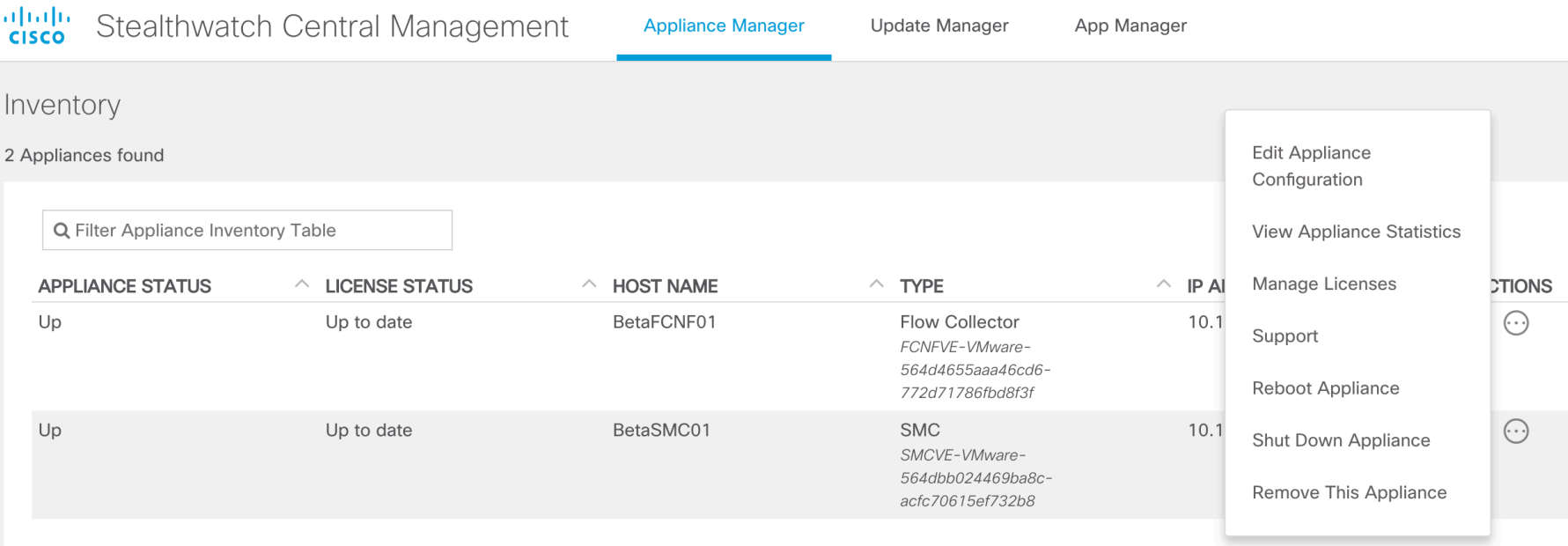
Note: admin access required

Централизованное управление устройствами и обновлениями

- Поддержание системы в актуальном состоянии не должно отвлекать вас от обеспечения ИБ!
- Предприняты меры для упрощения управления и обновления компонентов платформы Stealthwatch (SMC, Flow Collector, …).

Appliance Manager

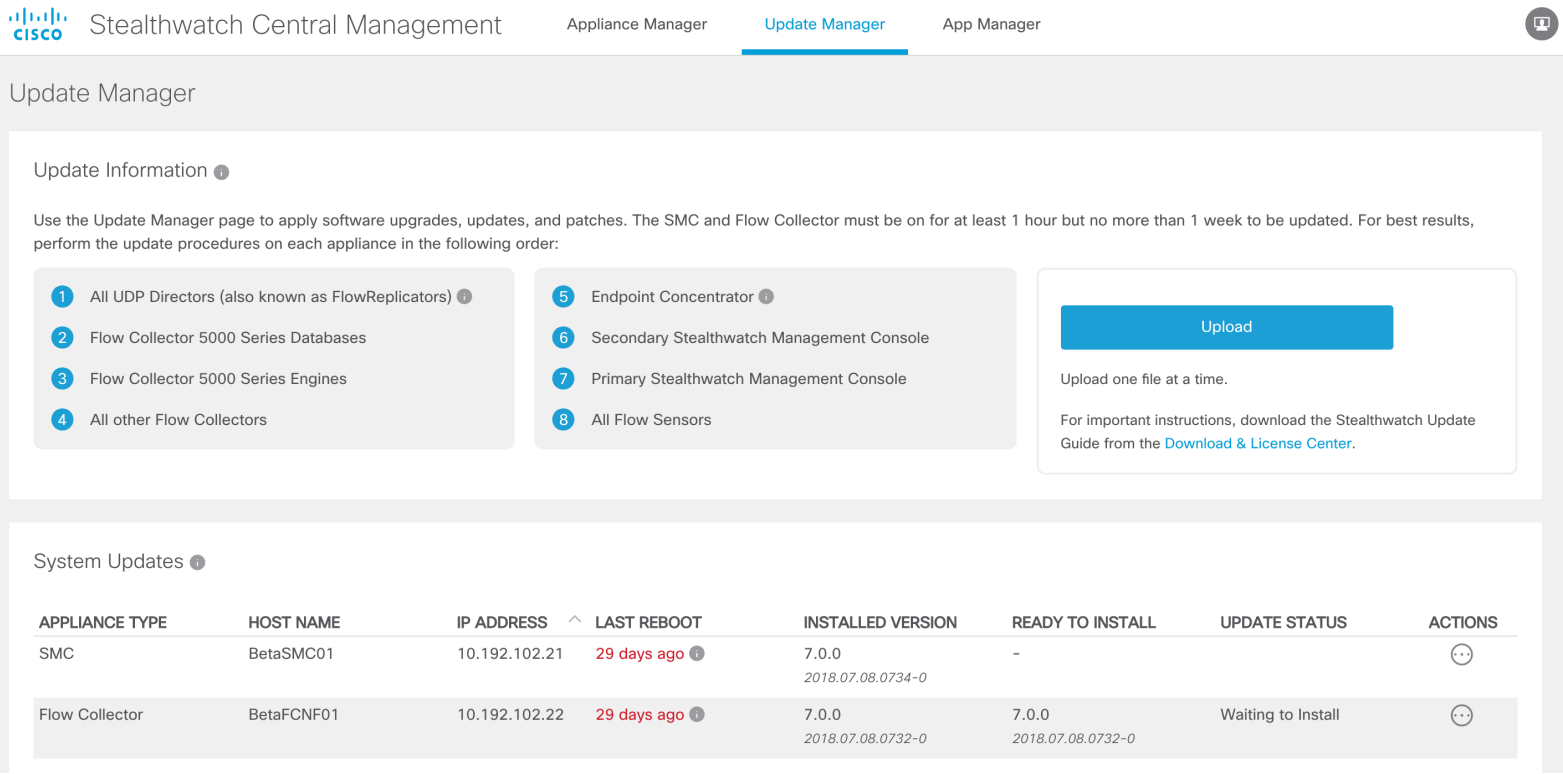
Global Settings > Central Management > Appliance Manager



Примечание. Права admin

Update Manager

Global Settings > Central Management > Update Manager



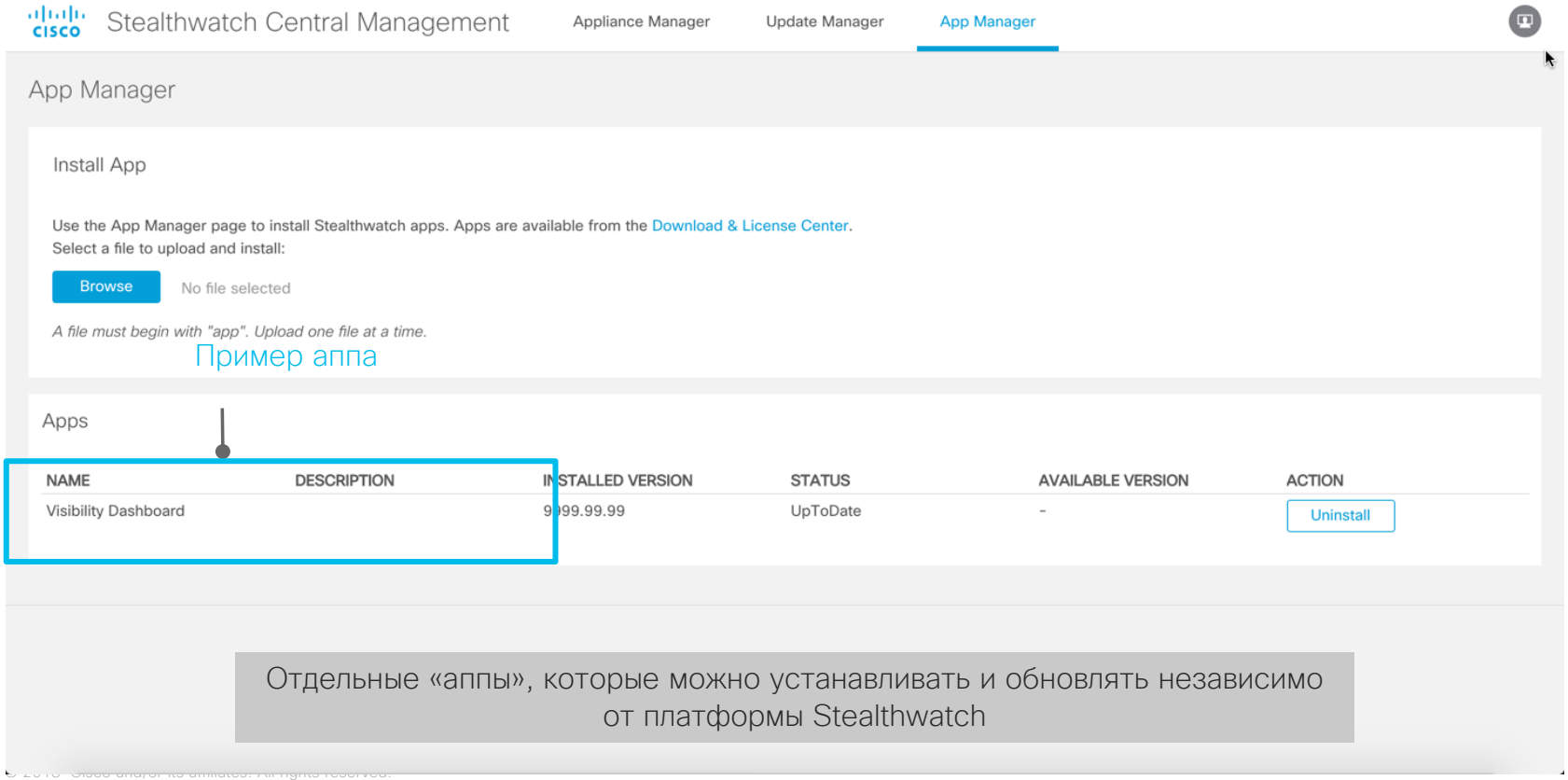
Примечание. Права admin

Stealthwatch Apps

- Как быстро модифицировать функционал, не обновляя систему? Конечно, аппы!
- Два аппа первой волны:
  - Stealthwatch Visibility Assessment – упрощение пилотов, создание «отчётов для руководства» в существующих развёртываниях Stealthwatch
  - Stealthwatch Host Classifier – экономия времени и сил (и простота масштабирования) за счет динамического обнаружения и классификации основных ресурсов в сети (текущий статус: beta)

Stealthwatch Apps

Global Settings > Central Management > App Manager

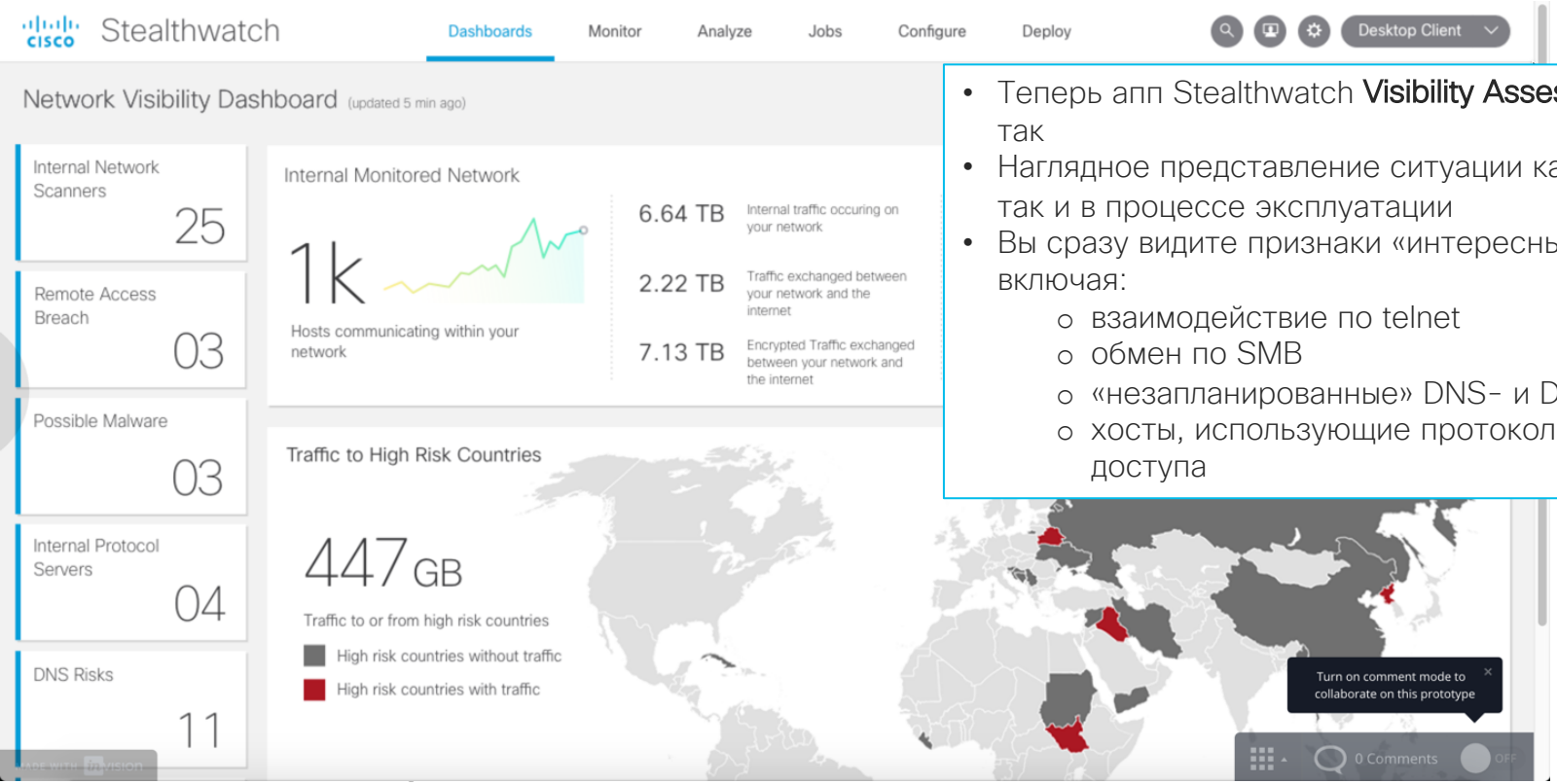


Отдельные «аппы», которые можно устанавливать и обновлять независимо от платформы Stealthwatch

Примечание. Права admin

Stealthwatch Visibility Assessment

Dashboard > Visibility Assessment



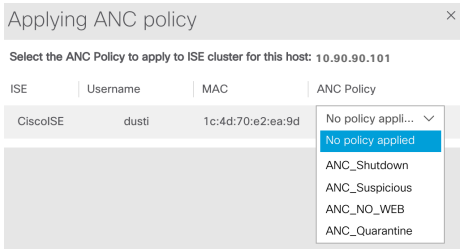
- Теперь апп Stealthwatch **Visibility Assessment** выглядит так
- Наглядное представление ситуации как в рамках пилота, так и в процессе эксплуатации
- Вы сразу видите признаки «интересных» действий, включая:
  - взаимодействие по telnet
  - обмен по SMB
  - «незапланированные» DNS- и DHCP-серверы
  - хосты, использующие протоколы удаленного доступа

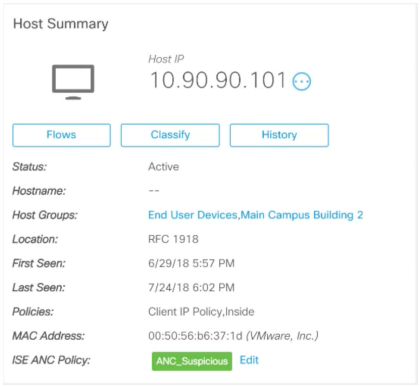
Интеграция с Identity Services Engine (ISE)

- Stealthwatch интегрируется с ISE для получения дополнительных данных о пользователях и контексте взаимодействия
- Теперь мы можем осуществлять более тонкую нейтрализацию с помощью ANC-политик ISE
- Естественно, метки SGT также могут сослужить большую пользу

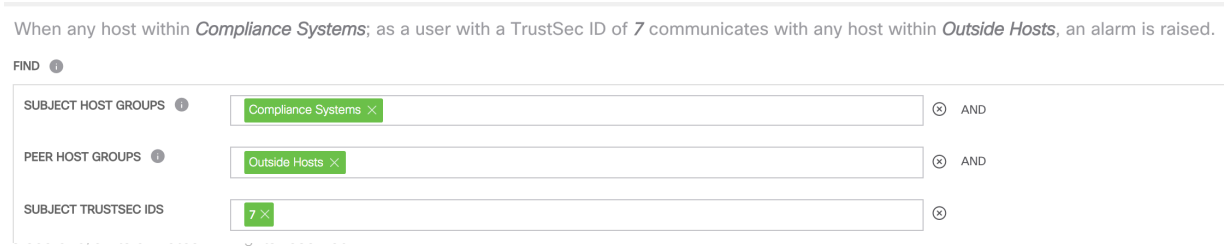
Усовершенствования интеграции с ISE

1. Быстрая нейтрализация с помощью ANC-политик ISE – например, от уровня угрозы





2. Метки SGT, которые считываются с ISE, теперь можно использовать в CSE совместно с IP-адресами (может быть полезно и при SDA)



3. Усовершенствования производительности и поддержка нескольких кластеров ISE

Классический периметр

Периметр: набор апробированных решений

- Web Security Appliance – апробированная платформа очистки веб-трафика
- Email Security Appliance –признанный в отрасли анти-спам
  Помните про возможность перезаписи URL и отслеживания кликов!!!
  Помним про вычистку ящика в Office365 по данным AMP в ESA 10.0
- Cloud Web Security (exScanSafe)/Open DNS
- Cloud Email Security/….
- Современные межсетевые экраны/системы предотвращения вторжений
- Платформа Cisco AMP – не только периметр (включая ThreatGrid)

На чем фокусироваться?

Совсем новое

Duo MFA

Duo Security is
now part of Cisco.

Duo – обзор

Мультифакторная аутентификация (MFA)

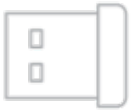
Самый широкий спектр вариантов


Push

Soft Token

SMS


Звонок

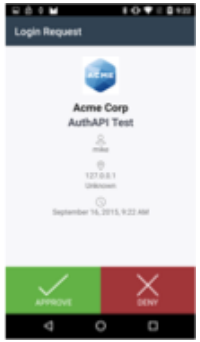

U2F

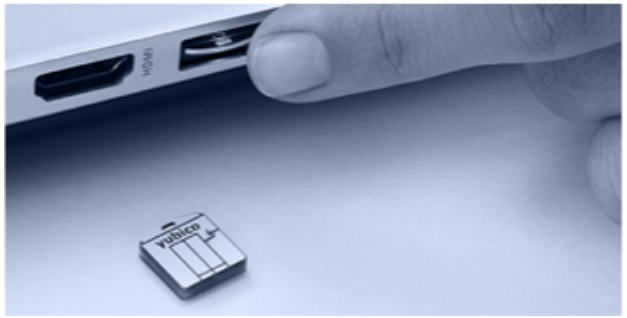

И это!!!

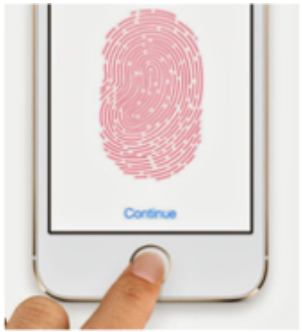

Biometrics

HW Tokens

Одна «галочка»

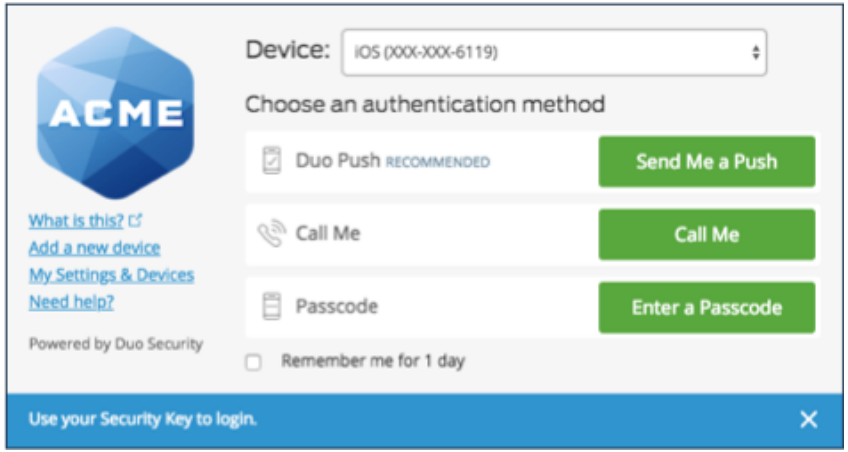


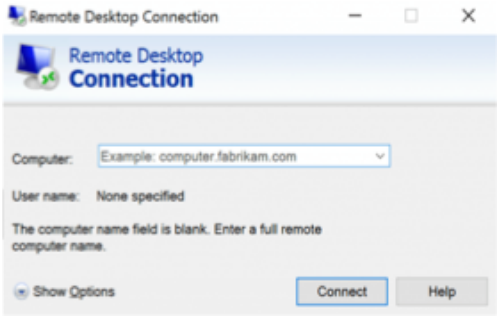




Что мы предлагаем

- Простое повышение уровня защищенности
- Защита доступа к конкретным системам
- Защита доступа, если вы используете RADIUS/LDAP
- Защита доступа к облачным приложениям
- Защита доступа к внутренним приложениям
- И даже немного posturing-а



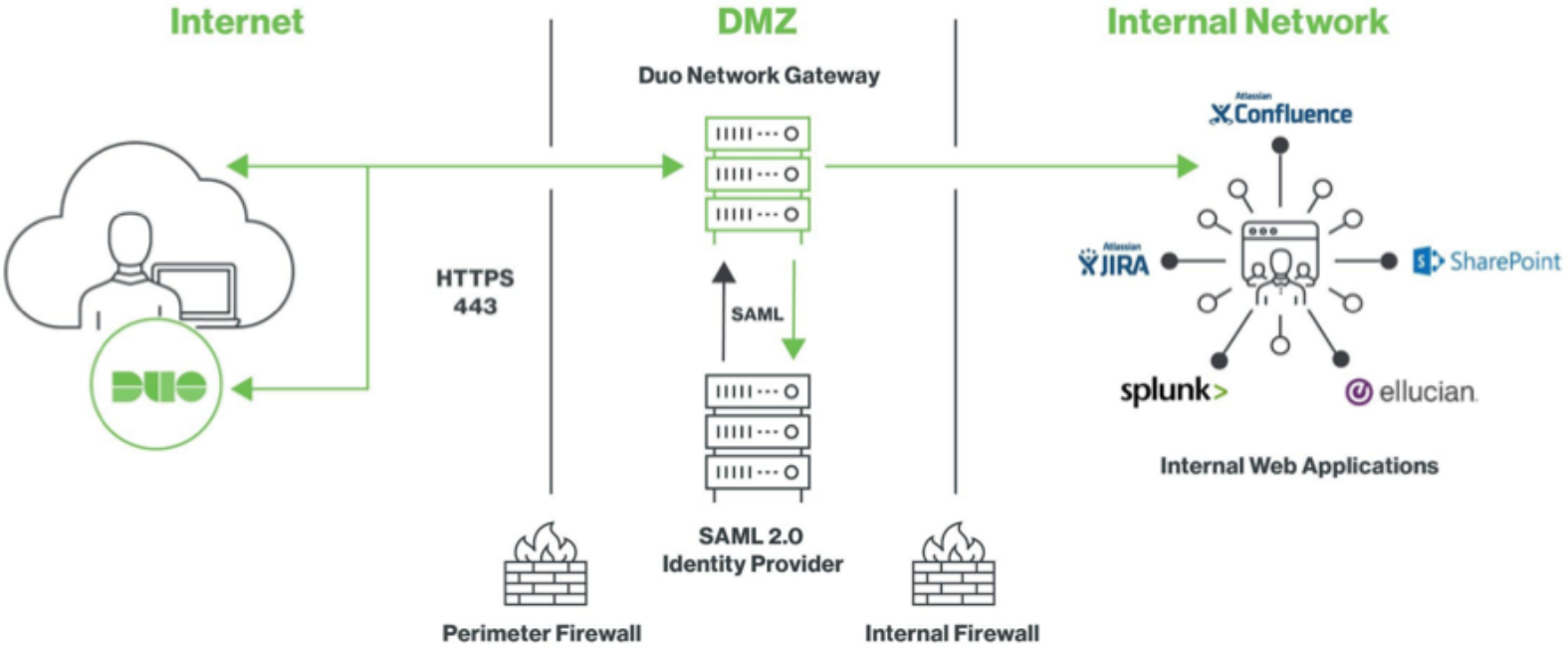


Более 60 SAML-приложений "из коробки"!

- Adobe Document Cloud
- Amazon Web Services
- Asana
- BambooHR
- BlueJeans
- Bomgar
- Bonusly
- Box
- Canvas
- Cisco WebEx
- Clarizen
- CloudLock
- Confluence
- CrashPlan
- Datadog
- Desk
- DocuSign
- Dropbox
- Egnyte
- Evernote
- Expensify
- Freshdesk
- G Suite
- GitHub Enterprise
- GoToMeeting
- Greenhouse
- HackerOne
- Heroku
- Intacct
- JIRA
- Jamf Pro
- Jitbit
- Looker
- Marketo
- Meraki
- Namely
- New Relic
- Office 365
- OpenDNS
- PagerDuty
- Remedyforce
- RingCentral
- Robin
- Salesforce
- Samanage
- Sauce Labs
- ShareFile
- Signal Sciences
- Slack
- Smartsheet
- Splunk
- StatusPage.io
- SugarCRM
- Sumo Logic
- Syncplicity
- Tableau
- Tableau Online
- Udemy
- UserVoice
- Workplace by Facebook
- Zendesk
- Zoom

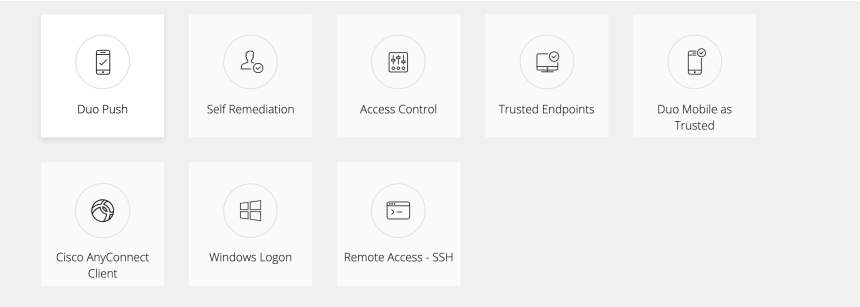
И другие

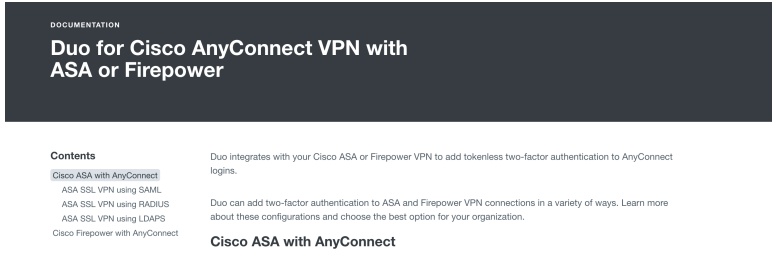
Всё ещё строите VPN для доступа к web-приложениям? Мы можем помочь и с VPN, но:

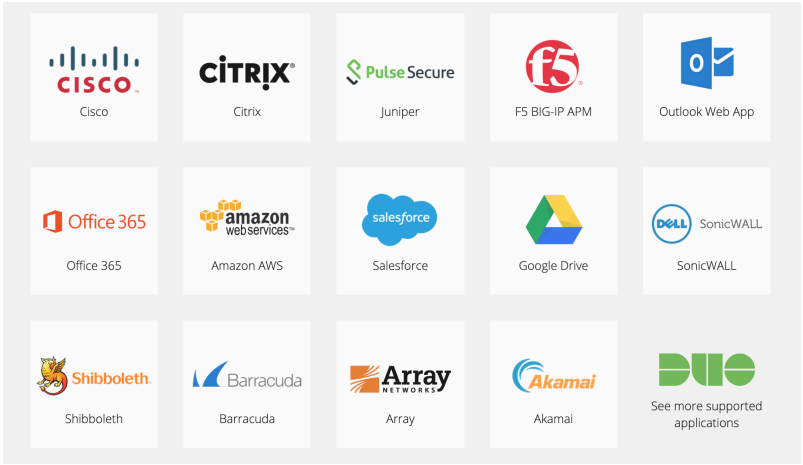


«Потрогать» бы?

- https://demo.duo.com/
- Телефон Ваш, а стенды наши – реалистичные сценарии

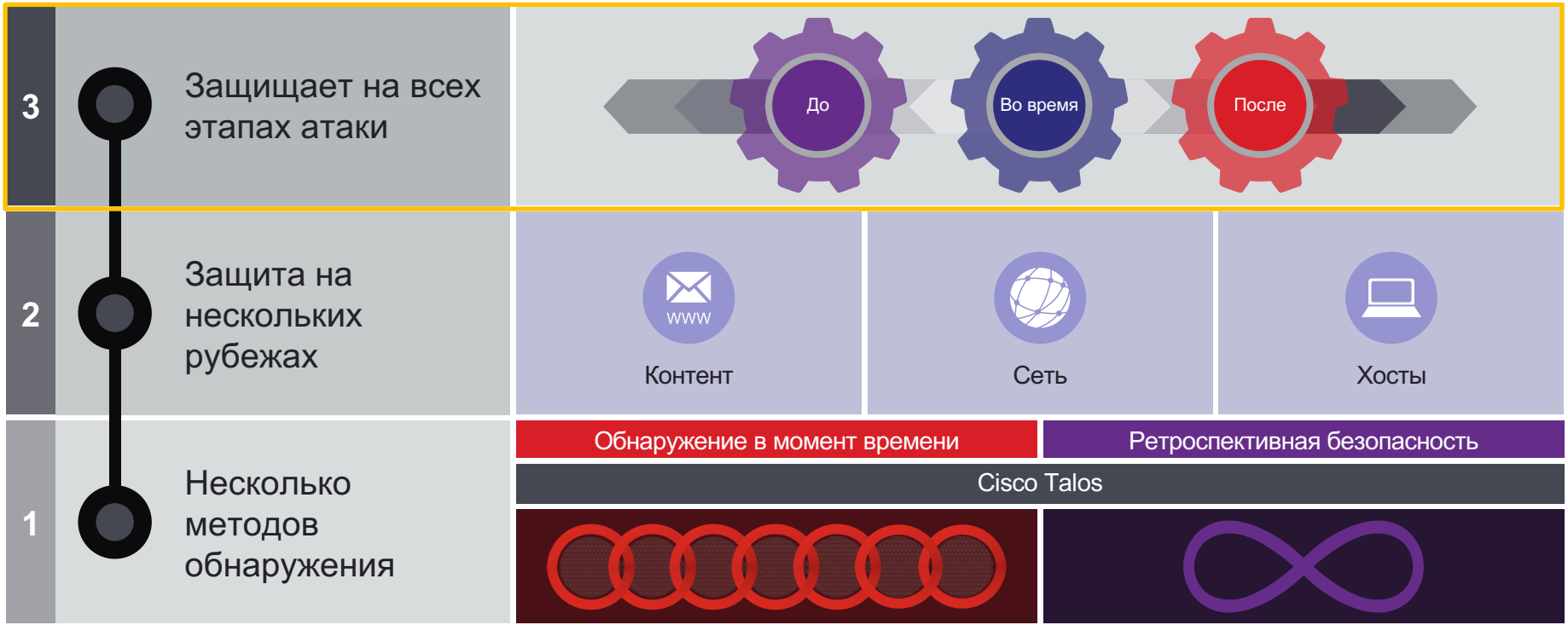






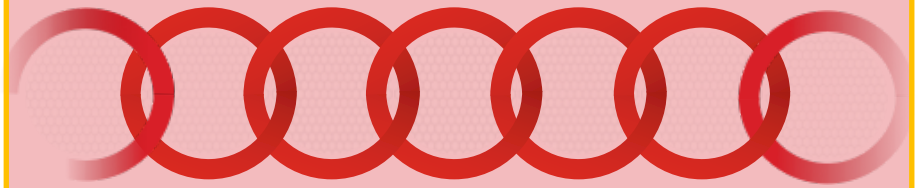
Cisco AMP (4E и не только)

3 преимущества Cisco AMP



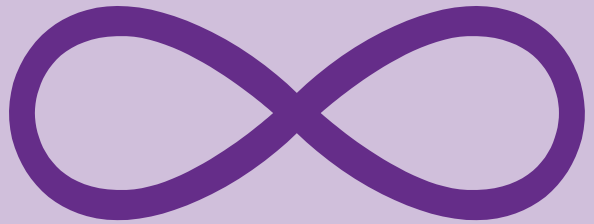
В Cisco AMP учтен как план А, так и план Б

Обнаружение в момент времени



Репутация и поведенческий анализ

Ретроспективная безопасность

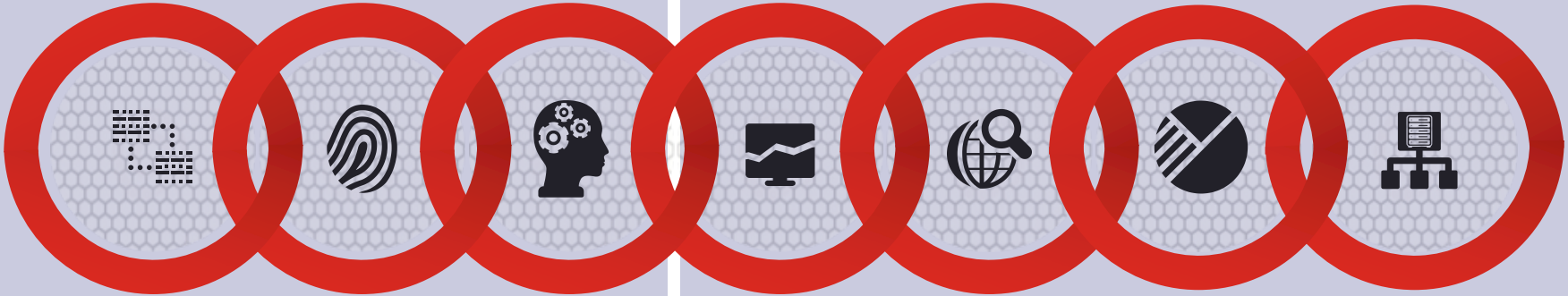


Непрерывная защита

Cisco AMP защищает с помощью репутационной фильтрации и поведенческого анализа файлов

Фильтрация по репутации

Поведенческое обнаружение



Идентичная сигнатура

Нечеткие идентифицирующие метки

Машинное обучение

Признаки компрометации

Динамический анализ

Расширенная аналитика

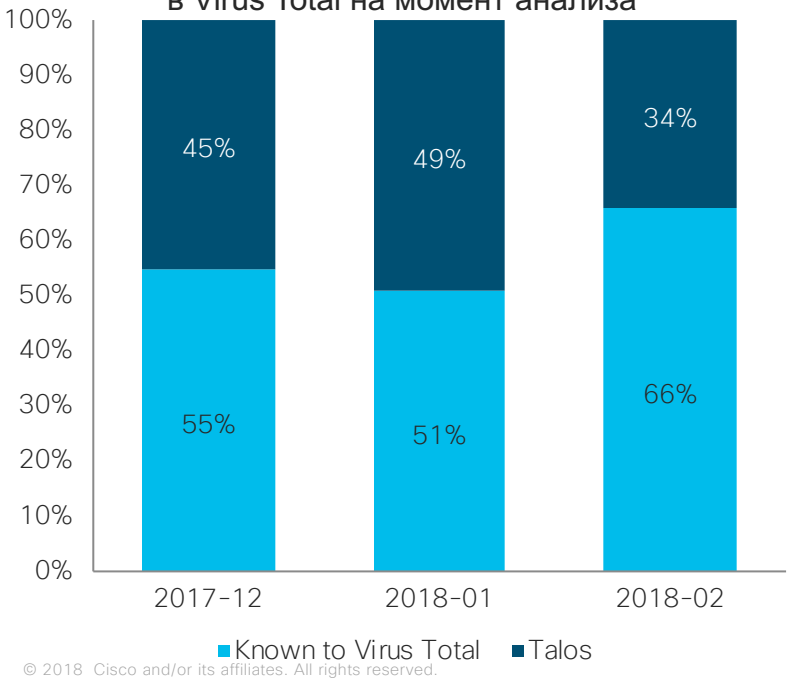
Сопоставление потоков устройств

Talos

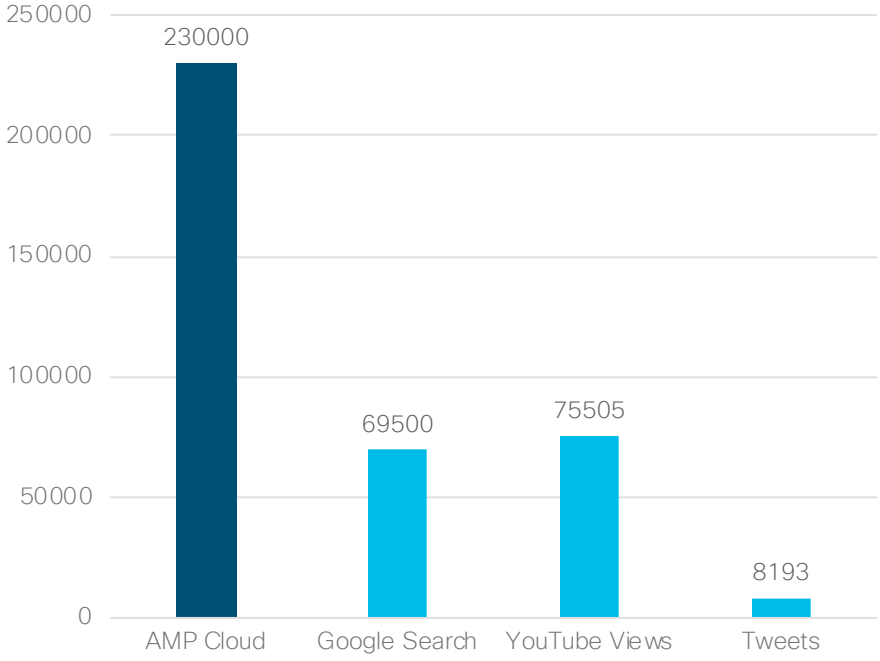
cisco

AMP for Endpoints

Более 34% файлов, признанных вредоносными **Talos**, не считались таковыми в Virus Total на момент анализа

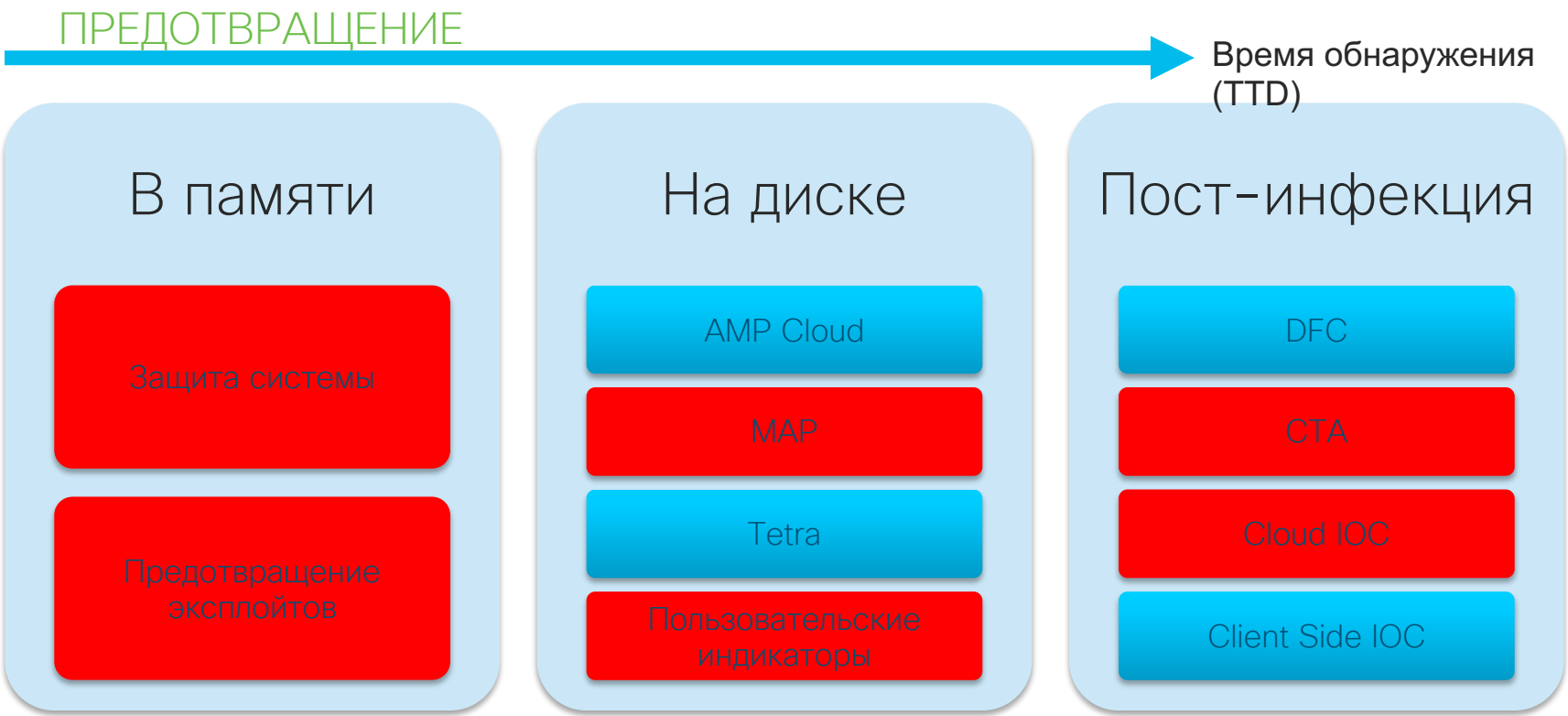


Обращения к облаку: пик 230K QPS в 2018



Источник: AMP Cloud and http://www.internetlivestats.com

А также...



И ещё одна платформа

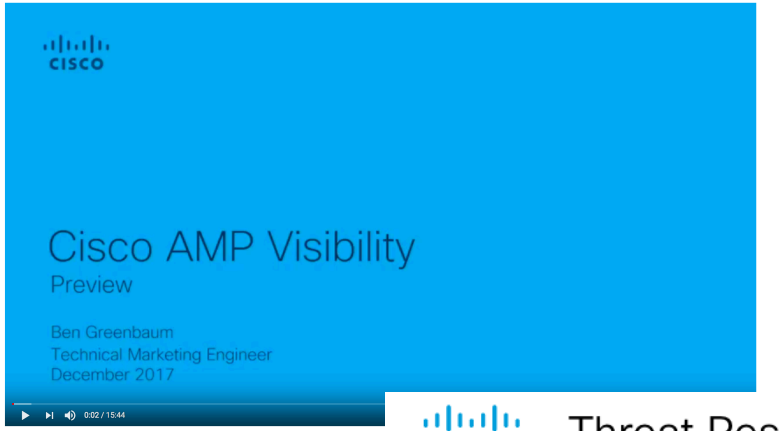
Cisco AMP Visibility

=

Cisco Visibility

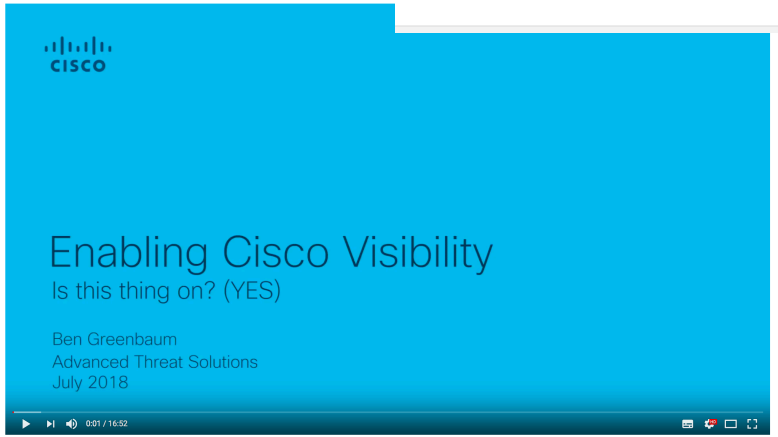
=

Cisco Threat Response*



Introducing AMP Visibility (Beta Preview) (Now Cisco Threat Response)

cisco Threat Response



How to Enable Cisco Threat Response

https://visibility.amp.cisco.com/
https://visibility.eu.amp.cisco.com/

Cisco Threat Response

- Ключевой элемент интегрированной архитектуры Cisco
- Обеспечивает локализацию глобальных данных threat intelligence в контекст безопасности инфраструктуры организации
- Снижает сложность за счет
  - обогащения сведений о *наблюдаемых объектах* автоматически из нескольких источников (ускорение понимания)
  - представления результатов в интуитивно понятной форме в рамках одной системы (ускорение осознания)
- Помогает выделить вредоносные *наблюдаемые объекты* и ускорить реагирование на инциденты
- Помогает специалистам по расследованию инцидентов лучше понимать ситуацию в их инфраструктуре, собирая и комбинируя threat intelligence, доступную от Cisco и сторонних организаций

Основные термины и идеи Threat Response

- Modules (Модули)
- Observables (Наблюдаемые объекты)
- Investigate UI (Графический интерфейс специалиста по расследованию)
- Judgements (Суждения)
- Verdicts (Вердикты)
- Sightings (Обнаружение)
- Indicators (Индикаторы)
- Targets (Цели)
- Snapshots (Моментальный снимок)
- Casebooks (Справочники)

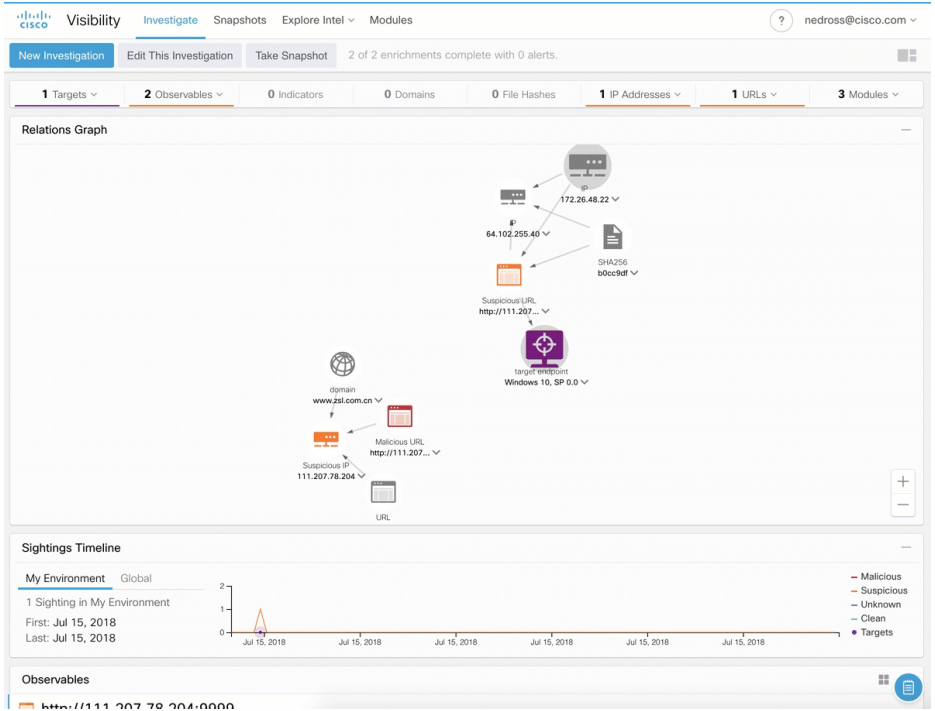
Использование Cisco Threat Response

Я – заказчик Cisco, использующий Cisco Threat Response

Моя команда может

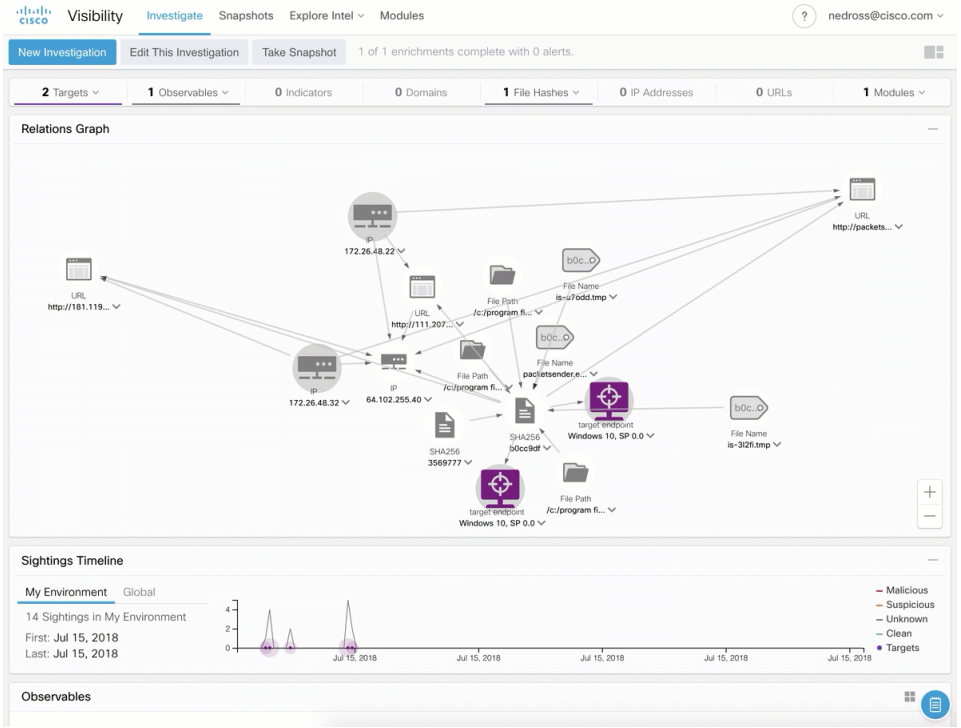
- оперативно оценивать наблюдаемые объекты
- блокировать и разблокировать домены из Cisco Threat Response
- блокировать и разблокировать исполнение файлов из Cisco Threat Response
- анализировать следы, ассоциированные с известными кампаниями, и немедленно оценивать воздействие кампании на организацию
- сохранить моментальные снимки расследований для дальнейшего анализа
- документировать результаты работы над инцидентом с помощью журналов
- легко интегрировать Cisco Threat Response в существующие процессы и собственные инструменты

Оперативная оценка наблюдаемых объектов



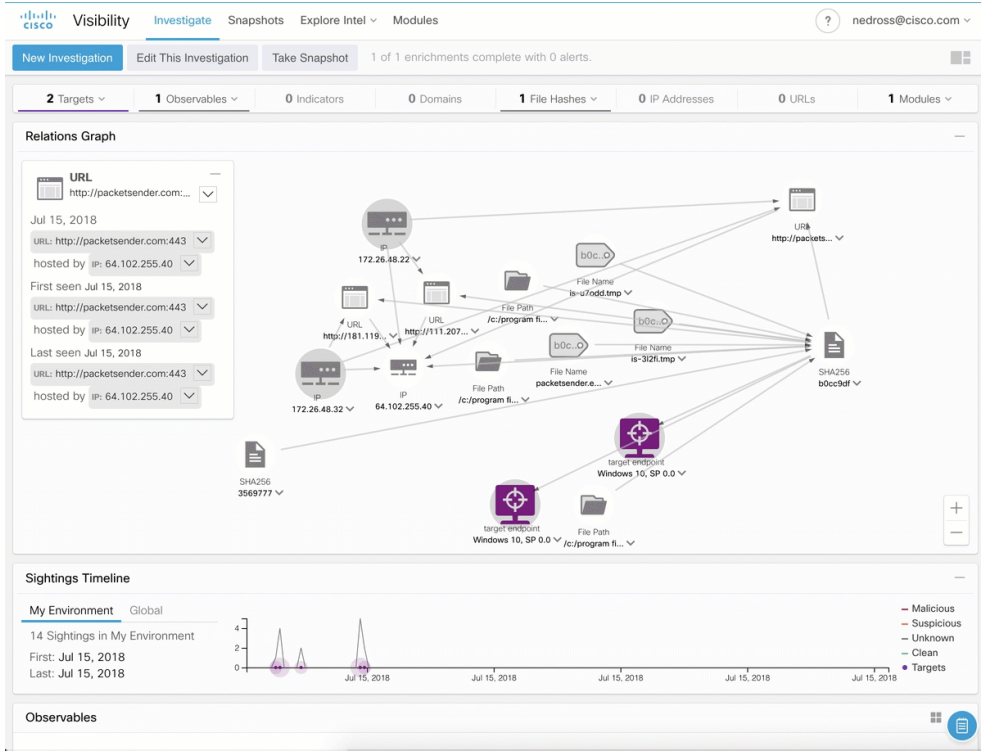
- Неизвестная диспозиция
- (почти) Моментальное представление воздействия на организацию
- Сведения о запуске кода и взаимодействиях

Моя команда может блокировать и разблокировать домены



- Реализовать блокирование из Cisco Threat Response
- Блокировать через Cisco Umbrella
- Интеграционный API для блокирования и разблокирования

Моя команда может блокировать и разблокировать исполнение файлов

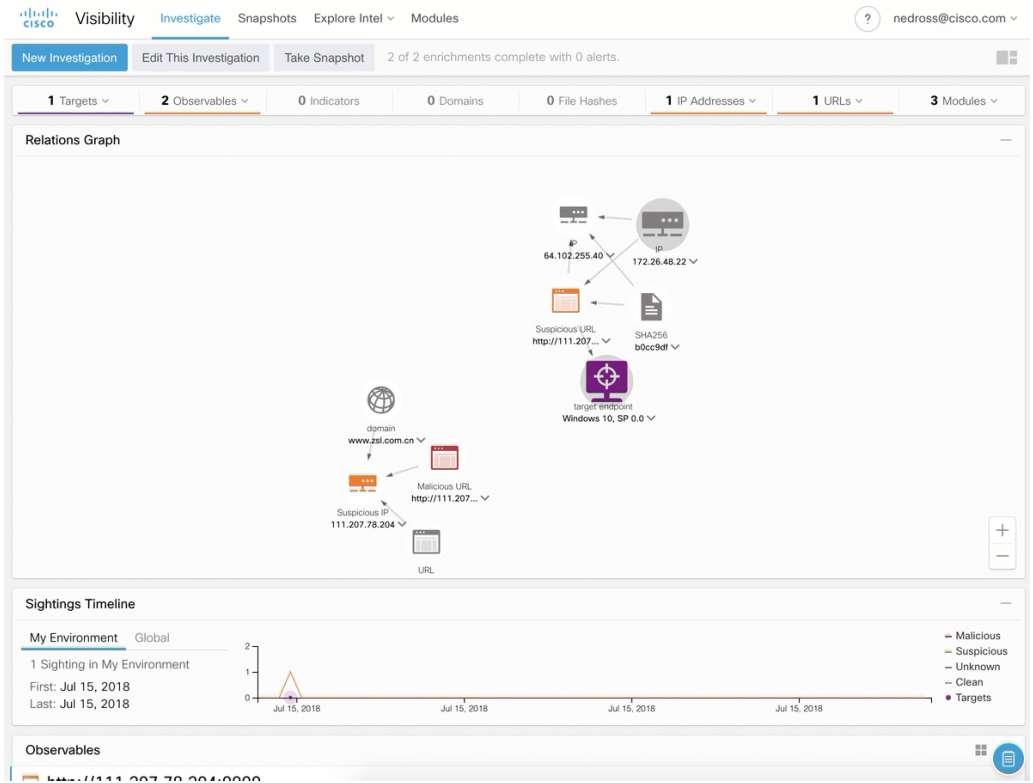


- Блокирование реализуется через Cisco Threat Response.
- Блокирование обеспечивается Cisco AMP for Endpoints.
  - и через AMP Unity в NGFW, WSA, ESA и т.д.
- Интеграционный API для блокирования и разблокирования

Анализ следов, ассоциированных с известными кампаниями, и оценка воздействия

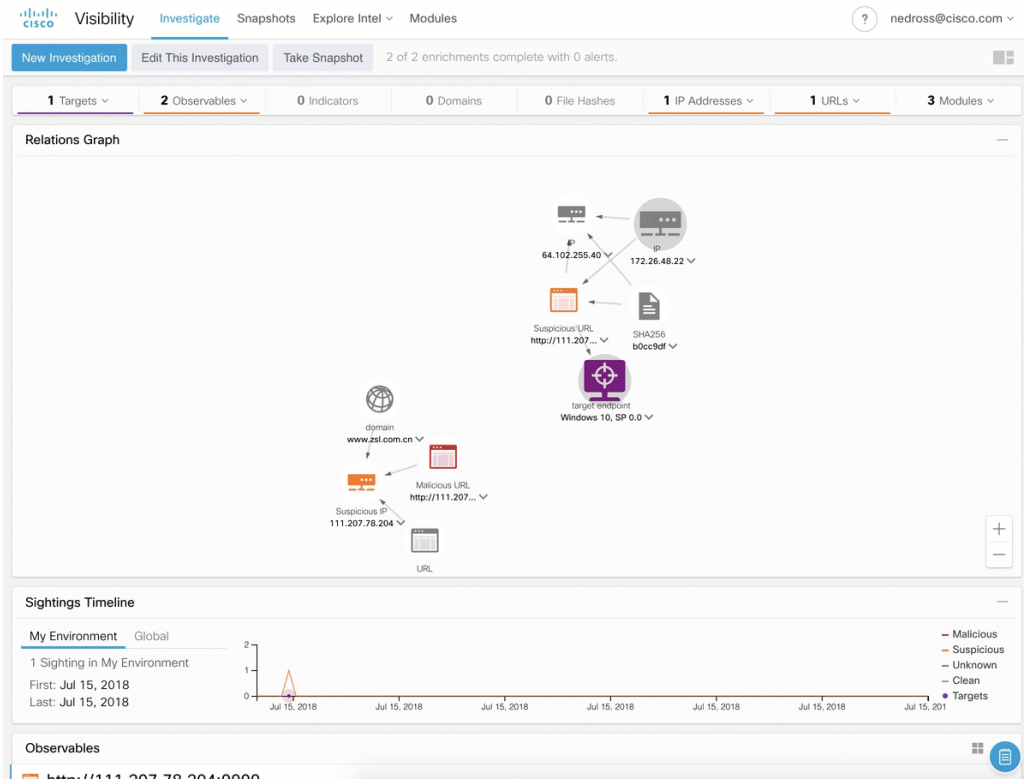
- Пострадавшие (цели)
- Дополнительные IP-адреса
- Ассоциированные программы

Моя команда может сохранять моментальные снимки расследований



- В определенное время
- Ссылка
- Возможность дальнейших расследований

Моя команда может документировать результаты анализа



Журналы работы над кейсами

- Доступны из множества продуктов
  - Официально интегрированные продукты
  - Неинтегрированные, но доступные через web продукты
- Записи и наблюдения для непрерывности процесса
- Немедленный доступ к
  - Вердиктам
  - Операциям реагирования

Моя команда может интегрировать Cisco Threat Response в существующие процессы

Cisco Threat Response разработан для интеграции с другими продуктами по ИБ через URL, который позволяет вам выстраивать эффективные процессы.
Примеры ниже исходят из того, что Cisco Threat Response располагается по адресу: https://visibility.amp.cisco.com

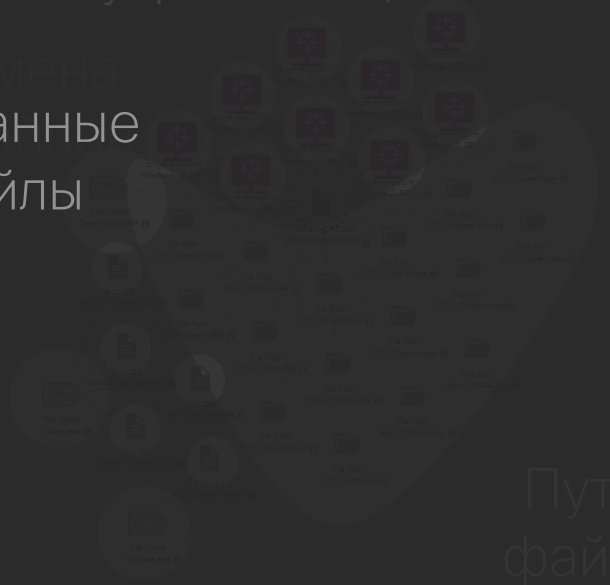
Вы можете выполнить расследование, передавая поисковую строку через параметр q, который идет после фрагмента #/investigate в URL.
Разрешено использовать несколько поисковых элементов, просто разделяя их пробелом.
Убедитесь, что URL правильно использует все параметры.
https://visibility.amp.cisco.com/#/investigate?q=domain.com
https://visibility.amp.cisco.com/#/investigate?q=google.com%0A8.8.8.8%0A6732417baa49b873d72747c0ef46f8d1

Вы можете искать индикаторы, суждения (Judgements) и факты обнаружения (Sightings) на странице Explore. Аналогично странице Investigate, передайте поисковый запрос после параметра q для поиска интересующих угроз:
https://visibility.amp.cisco.com/#/explore/indicators?q=rat
https://visibility.amp.cisco.com/#/explore/judgements?q=rat%20ip
https://visibility.amp.cisco.com/#/explore/sightings?q=662472b8378274eda5cc848536cba2db1d27f8ad

Внутренние цели

Имена

Связанные файлы



Пути файла

Локальное обнаружение

Глобальные данные

Резюме

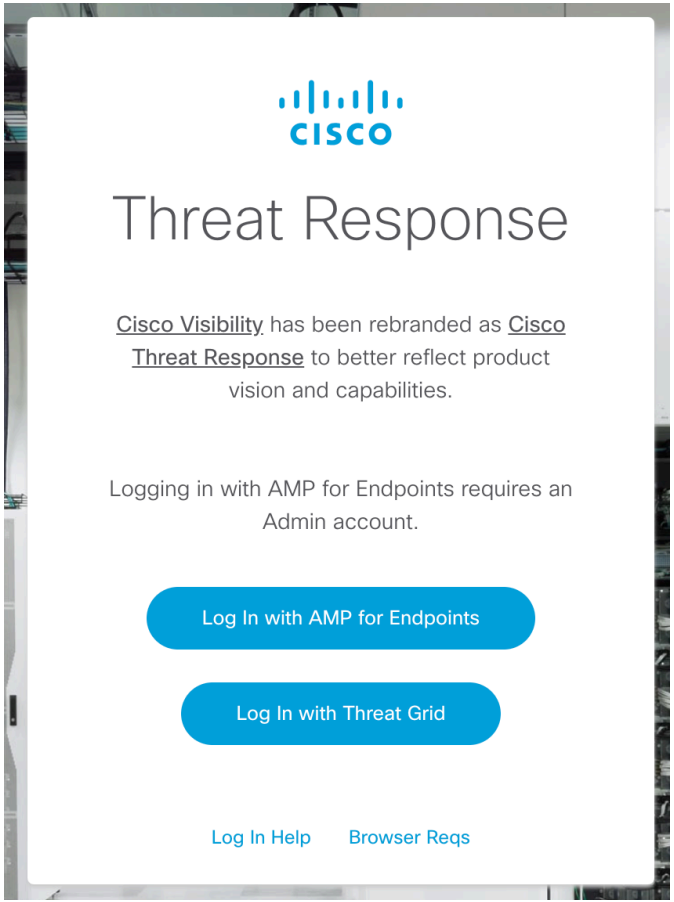
Cisco Threat Response снижает сложность растущего числа инструментов для расследования

- Соединяет внешние данные threat intelligence с внутренними данными логов
- Комбинирует данные из множества источников – Cisco и сторонних организаций
- Единое окно для многих задач по реагированию на инциденты
- До, во время и после атаки
- Снижает время расследования, приоритезации и реагирования

Сколько это стоит?

- Вы приобретаете AMP for Endpoints? Бесплатно!
- Вы приобретаете Cisco Threat Grid? Бесплатно!
- В ближайшем будущем WSA, ESA, Firepower…

Вы уже пользуетесь одним из этих решений?
У вас уже есть доступ!



Слайды и пара сценариев… но речь же про IR

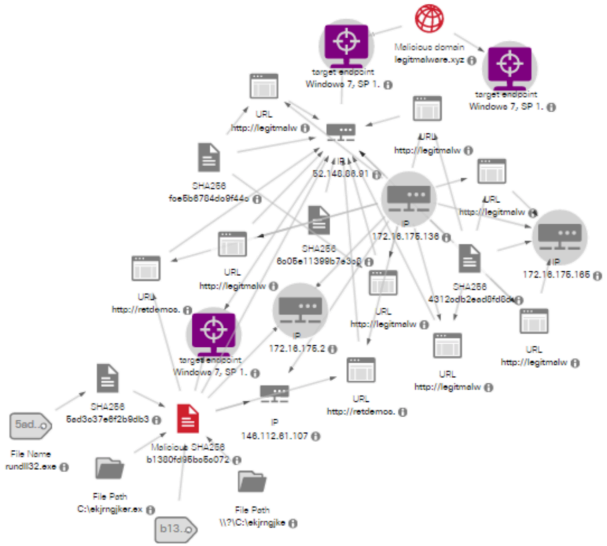
Российская команда Cisco Security регулярно проводит бесплатные Threat Hunting Workshop-ы, помогая партнёрам и заказчикам получить опыт работы с Cisco Threat Response (и другими продуктами Cisco).

Следите за новостями, регистрируйтесь и участвуйте.

Если у вас есть группа специалистов, которым целесообразно посетить такой семинар, напишите нам на security-request@cisco.com!

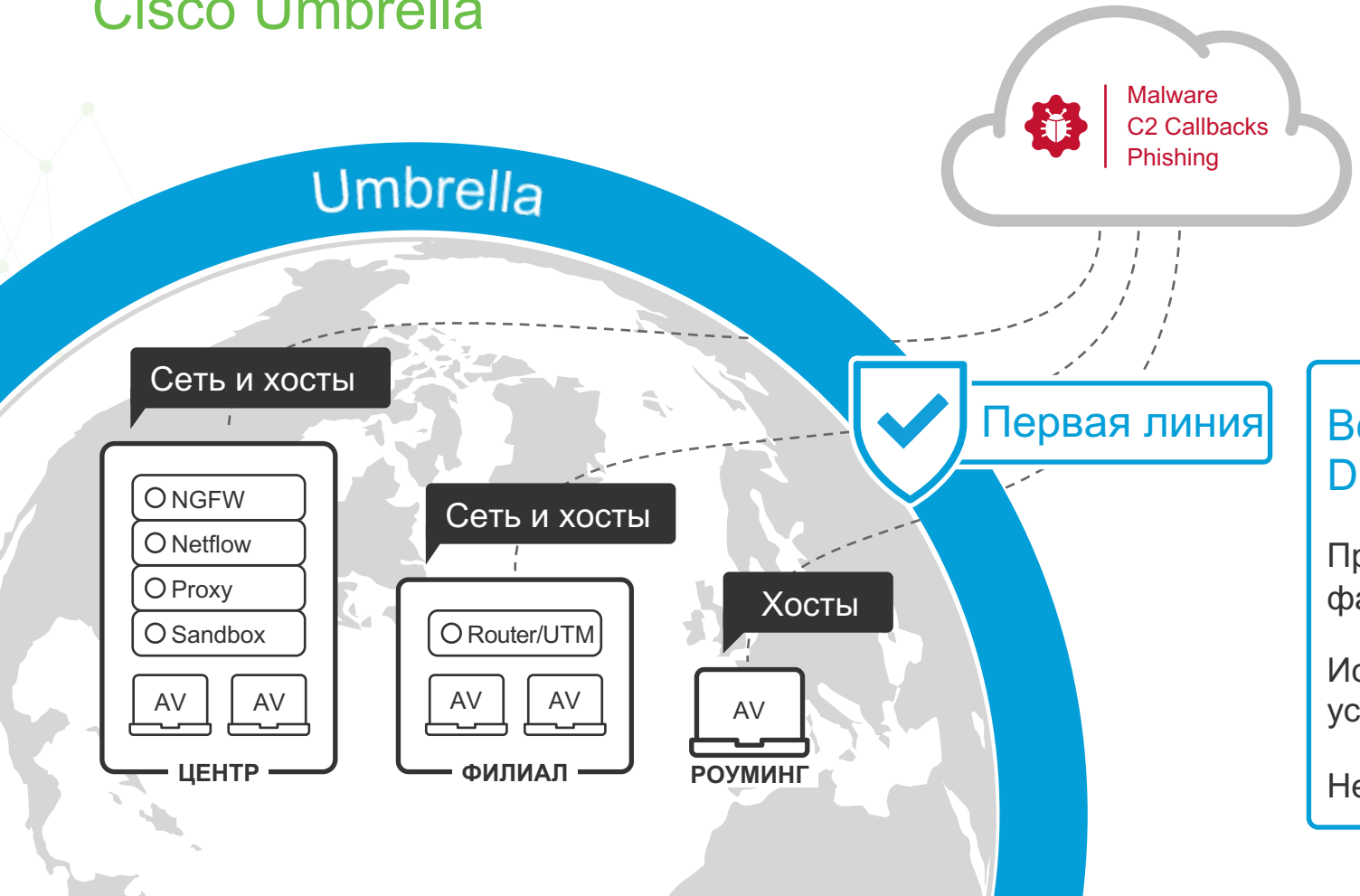
Threat Hunting Workshop

Hands On with Cisco Security Products



Umbrella

Cisco Umbrella



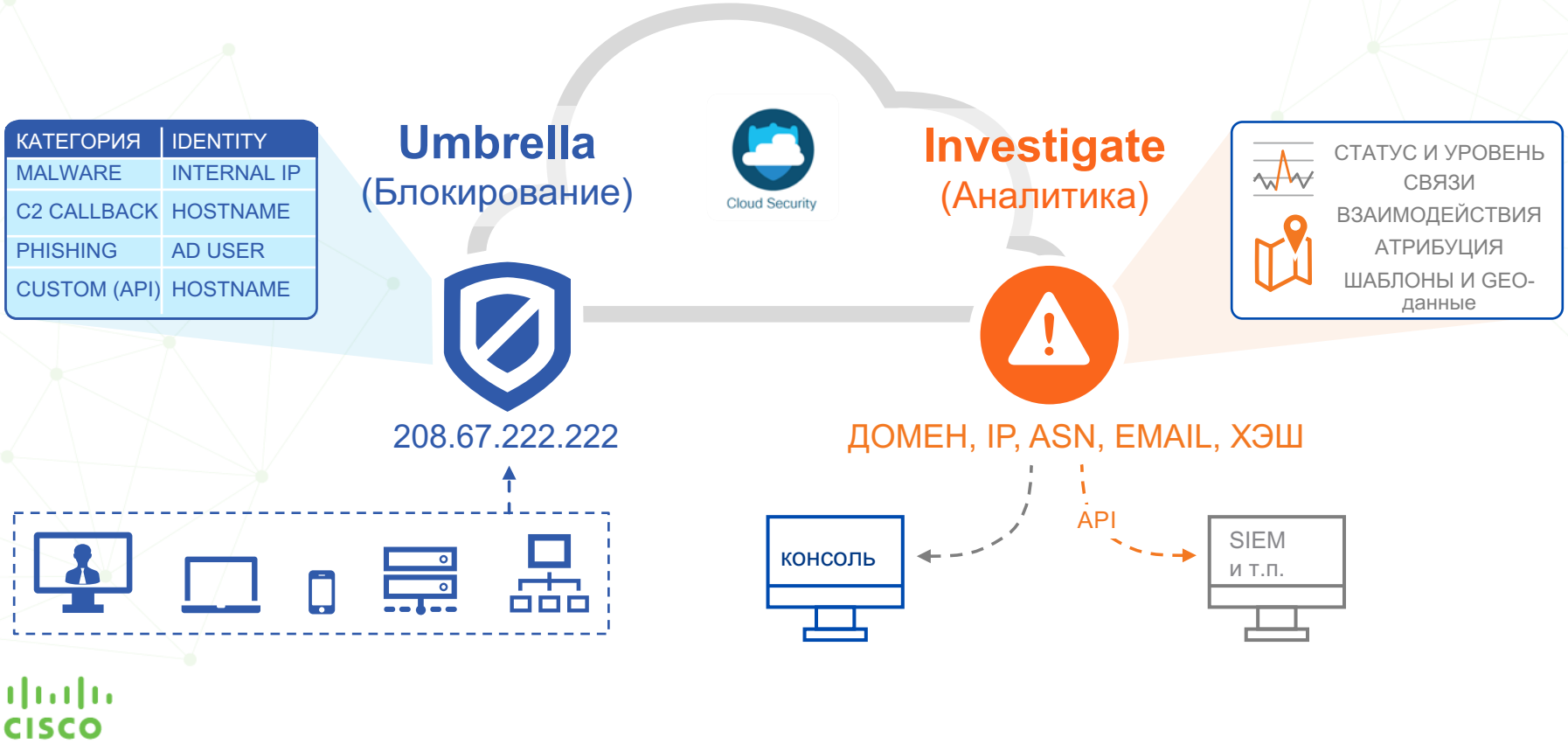
Всё начинается с DNS

Предвосхищает открытие файлов и IP-соединение

Используется всеми устройствами

Не зависит от порта

Архитектура Cisco Umbrella



Umbrella Resolver: обработка запросов

Результат

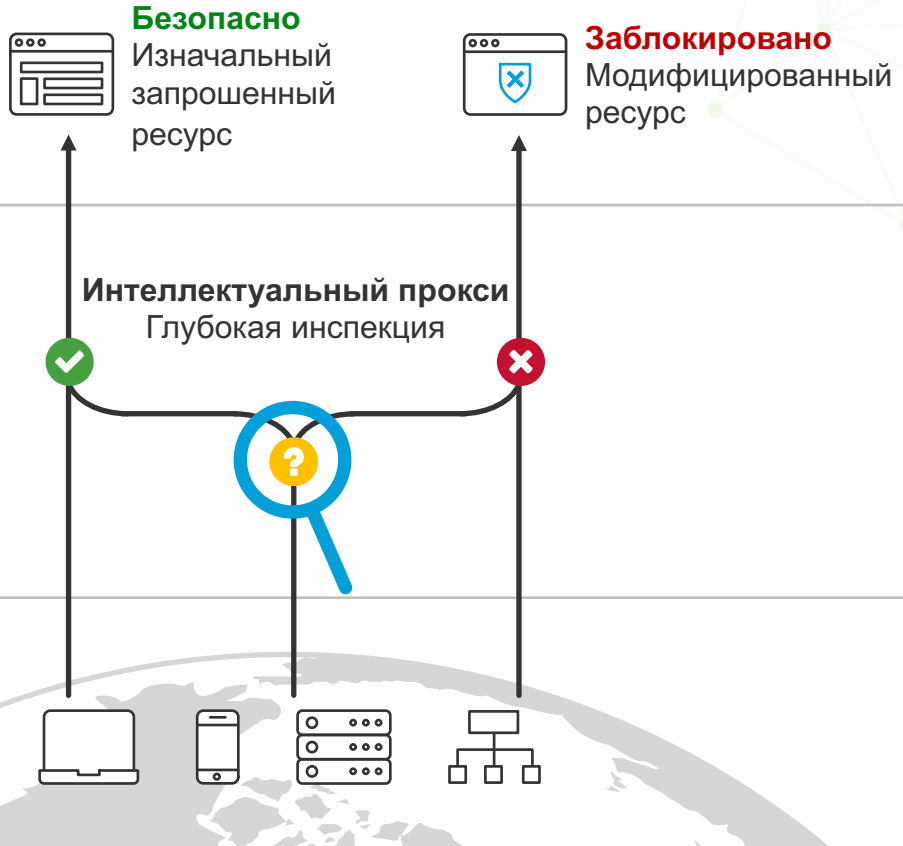
Изначально запрошенный ресурс или страница блокировки

Контроль безопасности

- DNS- и IP-фильтрация
- Инспекция подозрительных доменов через прокси
- SSL-decryption доступен

Интернет-трафик

Внутри сети и за её пределами

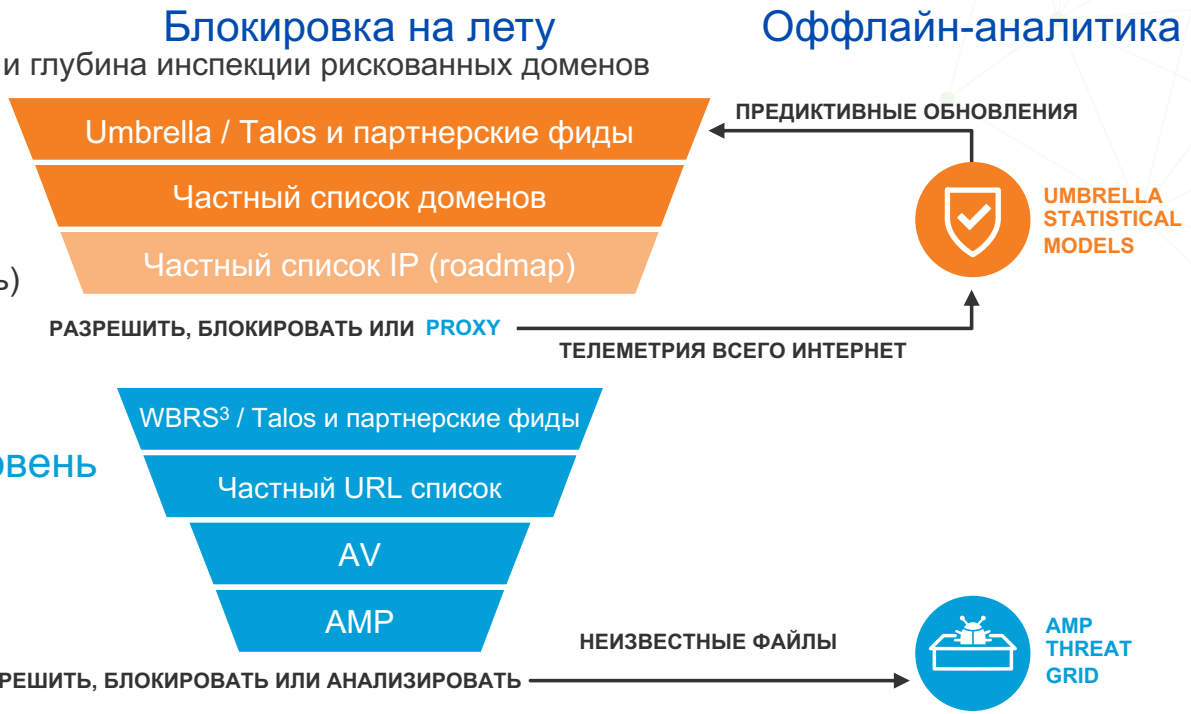


Блокировка на лету - аналитика офлайн

- Широта покрытия всех портов и глубина инспекции рискованных доменов

DNS- и IP-уровень

- Запрос Домена
- IP ответ (DNS-уровень)
  или соединение (IP-уровень)



HTTP/S уровень

- URL запрос
- Хэш файла

Зачем заказчику проводить пилоты Umbrella?

- ✓ Легкий способ попробовать Umbrella
- ✓ Не требует поставки оборудования или поддержки софта
- ✓ Внедрение менее чем за 30 минут, немедленные результаты
- ✓ Демонстрация пользы: немедленное блокирование ВПО
- ✓ Реальные результаты, которые легко проверить – и хотя бы наведение порядка за счет пилота!


Безопасность доступа к облачным ресурсам и сервисам (CAS)
Cisco Threat Intelligence
Cisco Threat Response
Cisco Platform Exchange
Безопасность электронной почты
EMM-решения
Безопасный доступ в интернет (SIG)
Защищенные сети SD-WAN / маршрутизаторы
Борьба со сложными угрозами
Контроль доступа к сети/идентификация и аутентификация
Системы обеспечения безопасности web-трафика
Коммутаторы и точки доступа
Threat Intel/активная защита
Полный объективный контроль
Автоматизация управления политиками
Осведомленность о контексте
Современные МСЭ/СПВ
Защита облачных нагрузок
Системы анализа трафика
Мы продолжаем развитие!


CISCO