



Иновации Cisco Security

Что нового в продуктах безопасности

Pavel Rodionov

CSE Security

14 ноября 2017

Иновации Firepower NGFW

Firepower NGFW: эволюция

2016

- Анонс Firepower Threat Defense

- Критический функционал Enterprise Edge

- Перенос ASA функционала

2017

- Новые платформы, RA VPN

6.2.3

- Улучшения работы системы , FDM расширения

Предыдущие релизы

МАЙ 2017

Firepower 6.2.1

- Анонс Firepower 2100
- Remote Access VPN (SSL и IPsec) для 2100



СЕНТЯБРЬ 2017

Firepower 6.2.2

- Remote Access VPN для остальных платформ
- Threat Intelligence Director
- FDM для VMware NGFWv



ASA 9.8.1

- MOBIKE (Mobile IKEv2)
- VTI
- ASA v50



ASA 9.8.2

- ASA для Firepower 2100



На всех устройствах Firepower может быть запущен ASA



2100 серия

Хорошее отношение
цена/качество
NGFW дл Internet Edge,
10 GbE подключение



4100 серия

Высокопроизводительный 1RU
NGFW для ЦОД
40 GbE интерфейсы



9300 серия

Операторский класс
NGFW дл кампуса и SP
Подключения до 100 Gbps

На всех может работать как Firepower Threat Defence,
так и ASA

Cisco Threat Intelligence Director (CTID)



Управление NGFW

Расширение возможностей локального менеджера

Предназначен



- Для создания простой, но эффективной системы безопасности
- Клиентам с устройствами 5506-X-5555-X/2100

UX
переработка

Управление
процессом

Простая
безопасность

- Снижение количества ложных срабатываний
- Первая линия обороны с Cisco Security Intelligence
- Расширенная инспекция зашифрованного трафика с SSL Decryption
- Простая миграция ASA → FTD с Flexconfig/SmartCLI
- Упрощение troubleshooting с CLI Console
- Управление NGFWv на VMware и KVM с FDM
- API для автоматизации/оркестрации

Настройка IPS сигнатур

Intrusion Event ---- Dropped Thu 05 Oct 2017, 3:17 PM

Message: PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt

SOURCE		DESTINATION		TRAFFIC	
Source IP	10.89.130.23	Destination IP	192.168.45.47	Ingress Security Zone	outside_zone
Source Country and Continent	not available	Destination Country and Continent	not available	Egress Security Zone	inside_zone
Source Port Itype	53	Destination Port Itype	53		
User	Special Identities/No Authentication Required	HTTP Response			

IPS

Priority	1
Inline Result	Dropped
IDS Classification	Attempted User Privilege Gain
Generator Id	3
Signature Id	19187
View IPS Rule	

POLICY

Intrusion Policy	Maximum Detection
Firewall Rule	Inside_Outside_Rule

Application Business Relevance Very High

Security Policies

Navigation: SSL Decryption → Identity → Security Intelligence → NAT → Access Control → **Intrusion**

Connectivity Over Security | Balanced Security and Connectivity | Security Over Connectivity | **Maximum Detection**

GID	SID	ACTION	STATUS	MESSAGE
>	3 19187	Drop		PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt

Action

- ALERT
- DROP (DEFAULT)**
- DISABLED

Search

GID	<input type="text"/>
SID	<input type="text"/>
Action	<input type="text" value="Any"/>
<input type="button" value="SEARCH"/> <input type="button" value="Cancel"/>	

Поддержка Security Intelligence Feeds

Monitoring Policies Objects Device

SSL Decryption Identity Security Intelligence NAT Access Control Intrusion

Security Intelligence

Network URL

Security Intelligence Feature Description

The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. Any allowed connections are still evaluated by access control policies and might eventually be dropped. You must enable the Threat license to use Security Intelligence.

How Security Intelligence Works

INCOMING PACKETS → [BLACKLIST / DO NOT BLOCK] → DROP / OTHER POLICIES

Blacklist (Block/Drop)

Filter: Network Feed Network Object

- attackers
- bogon
- bots
- cnc
- dga

CANCEL OK

Security Intelligence Feeds

Configure

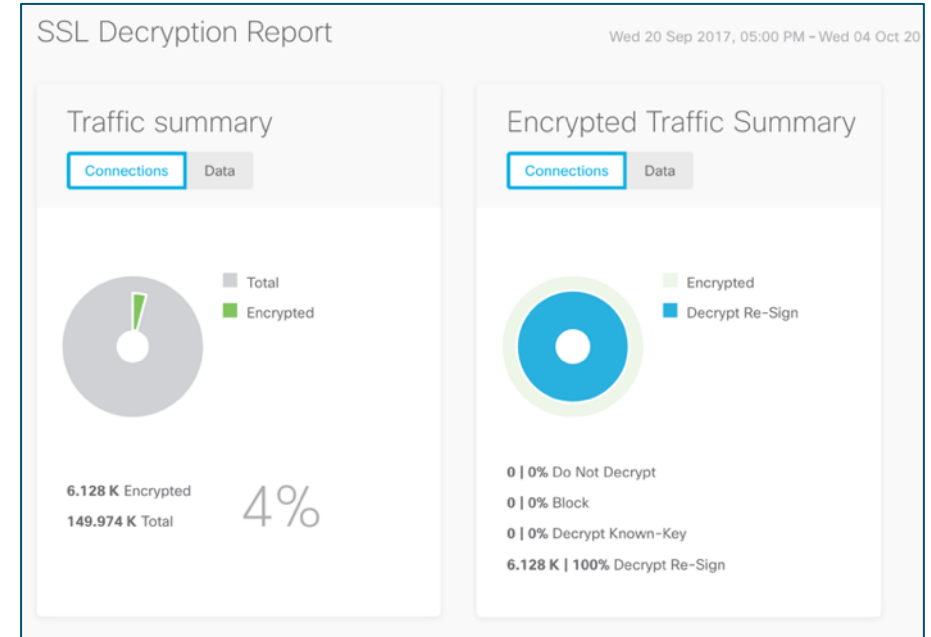
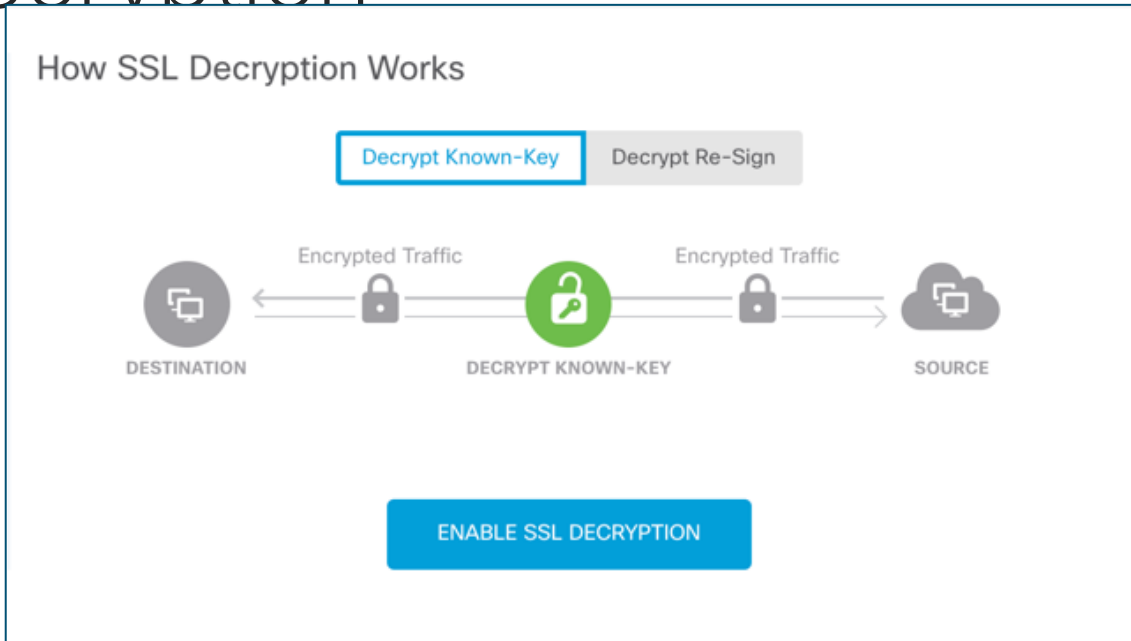
Set recurring Security Intelligence Feeds updates

UPDATE NOW



- Поддержка Cisco SI Feeds
- Включение whitelist/Blacklist

Расширенная инспекция трафика с помощью SSL Decryption

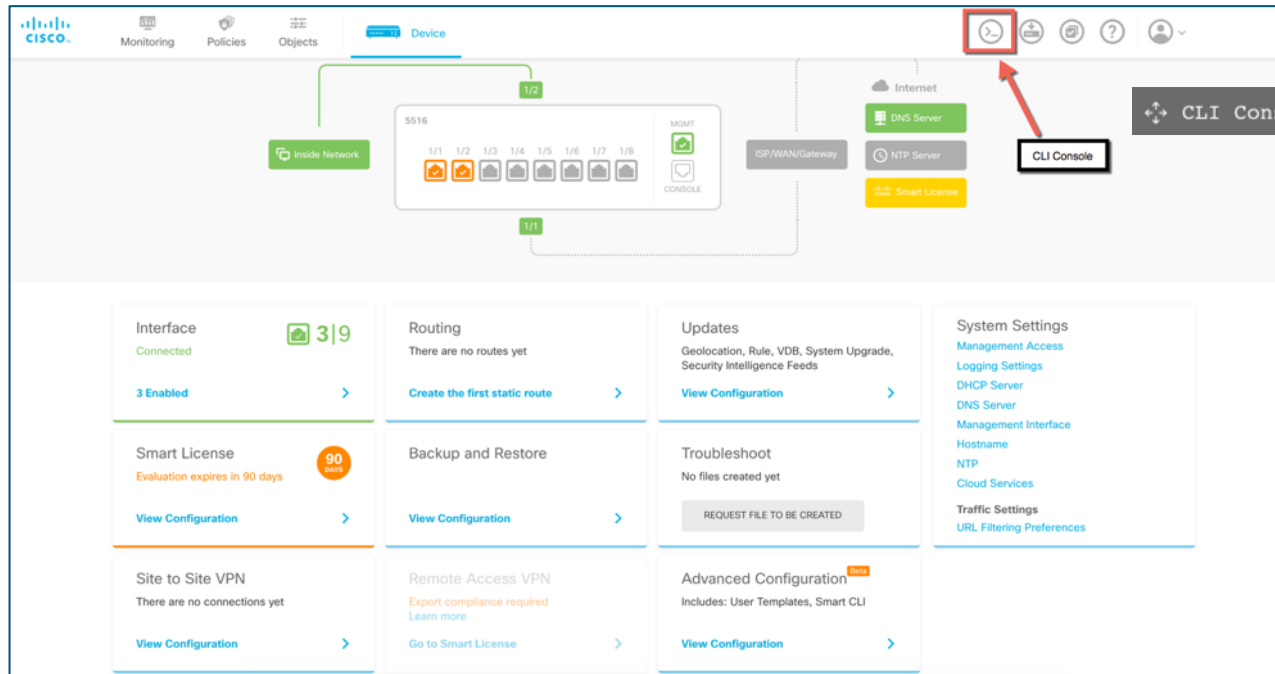


SSL Decryption 1 rule

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTOCOLS				
SSL Native Rules												
> 1	Sensitive_data	No Decrypt	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Financial Services Health and Medicine	ANY	

Default Action: Do Not Decrypt

Простой Troubleshooting



```
CLI Console > show running-config
: Saved

:
: Serial Number: JAD19390578
: Hardware: ASA5516, 8192 MB RAM, CPU Atom C2000 series 2416 MHz, 1 CPU (8 cores)
:
NGFW Version 6.2.3
!
hostname firepower
enable password $sha512$5000$5trbYYP14J83TjuAopta5w==$06/ysP0+oKjHQ022m5RV4w== pbkdf2
strong-encryption-disable
names

!
interface GigabitEthernet1/1
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address dhcp setroute
 ipv6 address autoconfig
 ipv6 enable
!
interface GigabitEthernet1/2
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

- Быстрый доступ к CLI командам
 - show, ping, traceroute, packet tracer

Автоматизация/оркестрация

Новый API

API Explorer

The following is a list of resources you can use for programmatic access to the device using the Firepower Device Manager REST API. The resources are organized into groups of related resources. Click a group name to see the available methods and resources. Click a method/resource within a group to see detailed information. Within a method/resource, click the **Model** link under **Response Class** to see documentation for the resource.

You can test the various methods and resources through this page. When you fill in parameters and click the **Try it Out!** button, you interact directly with the system. GET calls retrieve real information. POST calls create real objects. PUT calls modify existing objects. DELETE calls remove real objects. However, most changes do not become active until you deploy them using the POST /operational/deploy resource in the DeploymentStatus group. Although some changes, such as to the management IP address and other system-level changes, do not require deployment, it is safer to do a deployment after you make configuration any changes.

The REST API uses OAuth 2.0 to validate access. Use the resources under the Token group to get a password-granted or custom access token, to refresh a token, or to revoke a token. You must include a valid access token in the Authorization: Bearer header on any HTTPS request from your API client.

NOTE: The purpose of the API Explorer is to help you learn the API. Testing calls through the API Explorer requires the creation of access locks that might interfere with regular operation. We recommend that you use the API Explorer on a non-production device.

SystemInformation

Show/Hide | List Operations | Expand Operations

CommandAutoComplete

Show/Hide | List Operations | Expand Operations

FeatureInformation

Telemetry

HTTPAccessList

SSHAccessList

DataInterfaceManagementAccess

DeviceHostname

CloudCommunicationSettings

SystemInformation

Show/Hide | List Operations | Expand Operations

GET /operational/systeminfo/{objId}

Response Class (Status 200)

Model	Example Value
-------	---------------

SystemInformationTopLevel {

description: An object that specifies the System Information, ip address, software version, vdb and last rule update date.

version (*string*): A unique string version assigned by the system when the object is created or modified. No assumption can be made on the format or content of this identifier. The identifier must be provided whenever attempting to modify/delete an existing object. As the version will change every time the object is modified, the value provided in this identifier must match exactly what is present in the system or the request will be rejected.,

ipv4 (*string*): A string specifying the IPv4 address of the system.,

ipv6 (*string*): A string specifying the IPv6 address of the system.,

softwareVersion (*string*): A string which specifies the version of the software running in the system.,

vdbVersion (*VDBVersion*): An object which specifies the current VDB version, last success date, current build and release date.,

sruVersion (*SRUVersion*): An object which specifies the current SRU version and last success date.,

platformModel (*string*): A string which specifies the platform model of the system.,

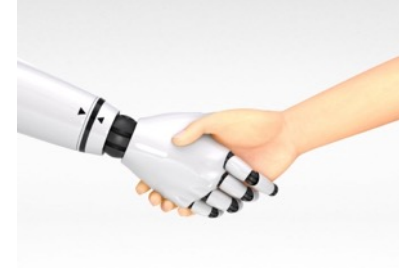
- Направление на оркестрацию
- Позволяет легко автоматизировать процессы

Фаза 1

- Автоматизация прямо на устройстве
- Не нужен FMC
- Весь поддерживаемый функционал GUI
- <https://<hostname>/#/api-explorer>

Новый API FMC

- Выгоды
 - Быстрая и тесная интеграция с инструментами 3-х компаний
 - Ускоряет процесс настройки
 - Миграция ASA → FTD



EtherChannel/PortChannel Interface	CRUD
Redundant Interface	CRUD
NAT Policies, NAT Rules	CRUD, Bulk Post for Manual & Auto NAT
Interface Groups	CRUD
Security Zones	R
Ipv4 and Ipv6 Static Routing	CRUD, Bulk Post
FTD HA	CRUD (except Monitoring Intf, MAC Addr)

Улучшения использования

FDM



- Новая система мониторинга
- Новый Dashboard Web Application
- Отслеживание IP/пользователей

FMC



- Быстрое создание НА
- Аудит изменений, Просмотр CLI после развертывания
- Увеличенное окно политик
- Возможность создавать групповые объекты в правиле
- Copy/Paste конфигурации

Meraki MX

Новые устройства MX250 & MX450

Расширение портфолио MX новыми высокопроизводительными моделями



High Throughput



Flexible Interface types



Modular redundant power



Новые устройства MX250 & MX450

MX250



MX450



Интерфейсы

WAN



2 x 10G SFP+

LAN



8 x 1G RJ45



8 x 1G SFP



8 x 10G SFP+



2 x 10G SFP+



8 x 1G RJ45



8 x 1G SFP



8 x 10G SFP+

Пропускная способность

4 Gbps

6 Gbps

Количество клиентов

2,000

10,000

VPN производительность

1 Gbps

2 Gbps

Спецификация не окончательная

Представляем vMX100 для Azure

Virtual MX доступен для Microsoft Azure

- 500 Mbps VPN
- Доступен в Azure Marketplace
- Полные возможности SD-WAN
- Та же модель лицензирования



MX портофолио – осень 2017

Teleworker



Z1

~5 users

802.11ac Wireless & PoE

FW throughput: 50-100 Mbps



Z3

Small Branch



MX64

~50 users

802.11ac wireless & PoE

FW throughput: 250 Mbps



MX65

Medium Branch



MX84

~200 users

FW throughput: 500 Mbps



MX100

~500 users

FW throughput: 750 Mbps

Large Branch, Campus or Concentrator



MX250

~2,000 users

FW throughput: 4 Gbps



MX400

~2,000 users

FW throughput: 1 Gbps



MX450

~10,000 users

FW throughput: 6 Gbps



MX600

~10,000 users

FW throughput: 1 Gbps

Virtual



vMX100 for AWS & Azure

FW throughput: 750 Mbps

VPN & SD-WAN features

Новый MX Firmware – Функции безопасности

MX 13.24 ()

- Threat Grid
- Правила firewall FQDN/hostname
- Syslog экспорт для событий AMP
- DNS-based Google safesearch и Youtube ограничения
- URL фильтрация по списку для HTTPS запросов на основе запроса сертификатов



Облачная безопасность

Cisco Umbrella и CloudLock

Обзор решений

- Umbrella – безопасный доступ к Internet для любого пользователя в любой сети с любого устройства через DNS
Функционал SIG, обновление категорий, отчетность, мобильные и роуминг клиенты.
- Cloudlock – безопасность санкционированных SaaS приложений
Обновления Office 365, ServiceNow, App Discovery, и Cisco Spark.
- Полная видимость и защита в облаке



Cisco Umbrella

«Разумный» прокси (вышел)

▼ ADVANCED SETTINGS



Enable Intelligent Proxy

Gain visibility into threats, content, or apps by proxying web connections for risky domains.

Клиенты могут увидеть риски и угрозы с помощью проксирования трафика на порты 80/443.

- По умолчанию включен для новых политик
- Трафик проксируется если он в "Grey List" Umbrella. Серый список – это набор доменов, которые являются «подозрительными», но не блокируются. Это управляется командой Umbrella.
- Трафик автоматически проксируется через нашу инфраструктуру если это включено в политике.

Инспекция файлов с помощью AMP и AV



Inspect Files

Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.

- Автоматически инспектирует файлы через прокси
- Инспекция с более чем ~200 расширениями
- Использование как AMP, так и AV для блокирования файлов
- Файл будет заблокирован при позитивном срабатывании

Блокирование URL

A list of bad URLs

Destinations on this list will be **BLOCKED**

Enter a Domain or CIDR IP Range [ADD TO LIST](#)

If a destination exists in both a blocked and allowed list, allowed destinations take precedence.

Destination	Type	Comments	
example.com/malware.php	URL	Add a comment	

Позволяет заблокировать определенные URL путем перенаправления на прокси

- Клиенты могут блокировать любые URL, запрещенные в организации
- Добавление URL также блокирует любые «дочерние» URL, если они есть

SafeSearch (через DNS)

Позволяет организациям, которые хотят заблокировать контент к нежелательному контенту заблокировать его в результатах поиска

- Google
- Bing
- YouTube

▼ ADVANCED SETTINGS



Enforce SafeSearch

Enforce SafeSearch for queries sent to supported search engines. [Learn More](#)

Коннекторы

AnyConnect

- Интеграция с Anyconnect на Windows и Mac
 - Защищает Anyconnect пользователей вне корпоративной сети

Роуминг-клиент

- Клиенты имеют возможность проксировать и защищать на IP ehjdyt yf Windows и MacCustomer ability to proxy and enforce at the IP Layer with the Windows and Mac Roaming Client (Released)
- Поддержка Active Directory (в работе)

Policy Tester (Released)

Enables administrators to understand whether or not a particular identity is blocked or allowed to go to a particular domain.

Administrators can now test the end state across all the policies they have configured to ensure their policies are working

Policy Tester

Test whether a destination will be allowed or blocked for an identity. If you receive results you don't expect or want, reorder or refine your policies and run the test again.

Identities

Ex: Roaming Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)

Destination

Note: Currently URLs are not supported

RESET

RUN TEST

Поддержка IPv6

Планируемая полная поддержка IPv6 в Umbrella

- Сейчас работает резолвинг адресов IPv6, но не политики

Блокирование приложений с помощью DNS

Возможность для Umbrella блокировать приложения с помощью DNS

- Позволит организациям заблокировать определенные приложения через DNS
- Блокирование на основе политик
- Организации не надо будет знать все потенциальные домены для приложения. Umbrella использует свою базу данных для ассоциации доменов










Cisco Cloudlock

Cloudlock Apps Firewall

Последние улучшения

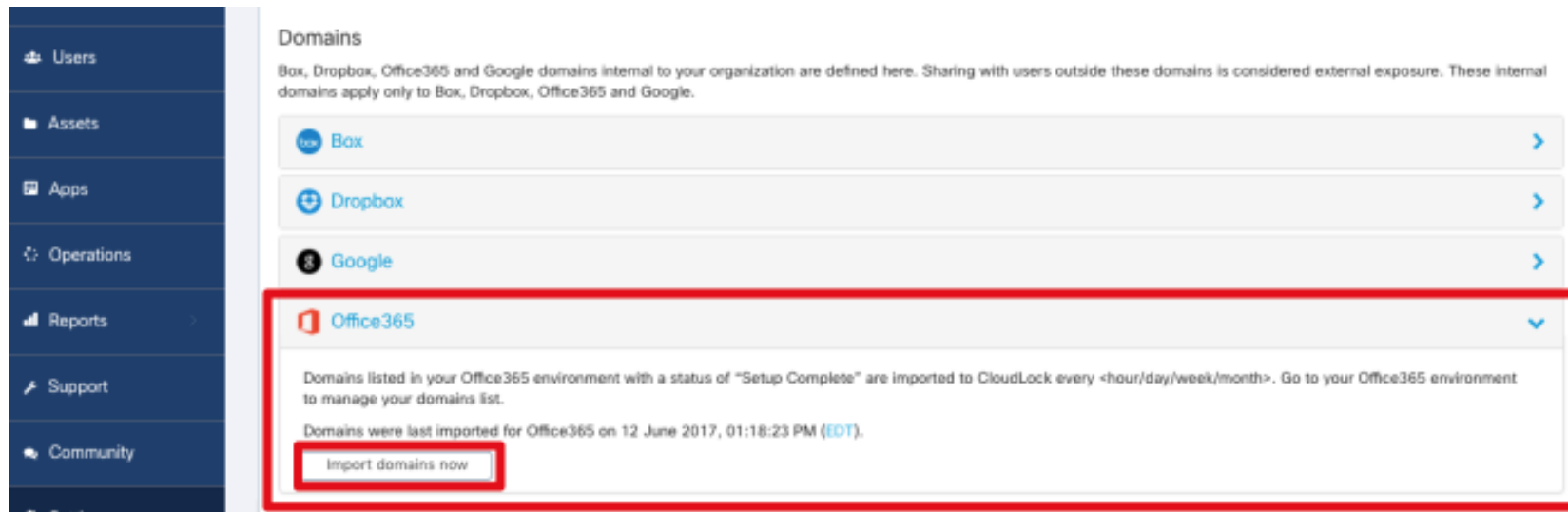
- Улучшили время обнаружения
- Черный список приложений

<input type="checkbox"/>	Flocabulary	 Blacklisted 	No users
<input type="checkbox"/>	GeoGebra <i>Education</i>	 Blacklisted 	No users
<input type="checkbox"/>	OAuth Risk Assess	<div data-bbox="1123 875 2303 1096"> This application has been identified as cloud malware, and access has been revoked. More details</div>	
<input type="checkbox"/>	DocHub	 Blacklisted 	No users

Cloudlock для Office 365

Последние улучшения

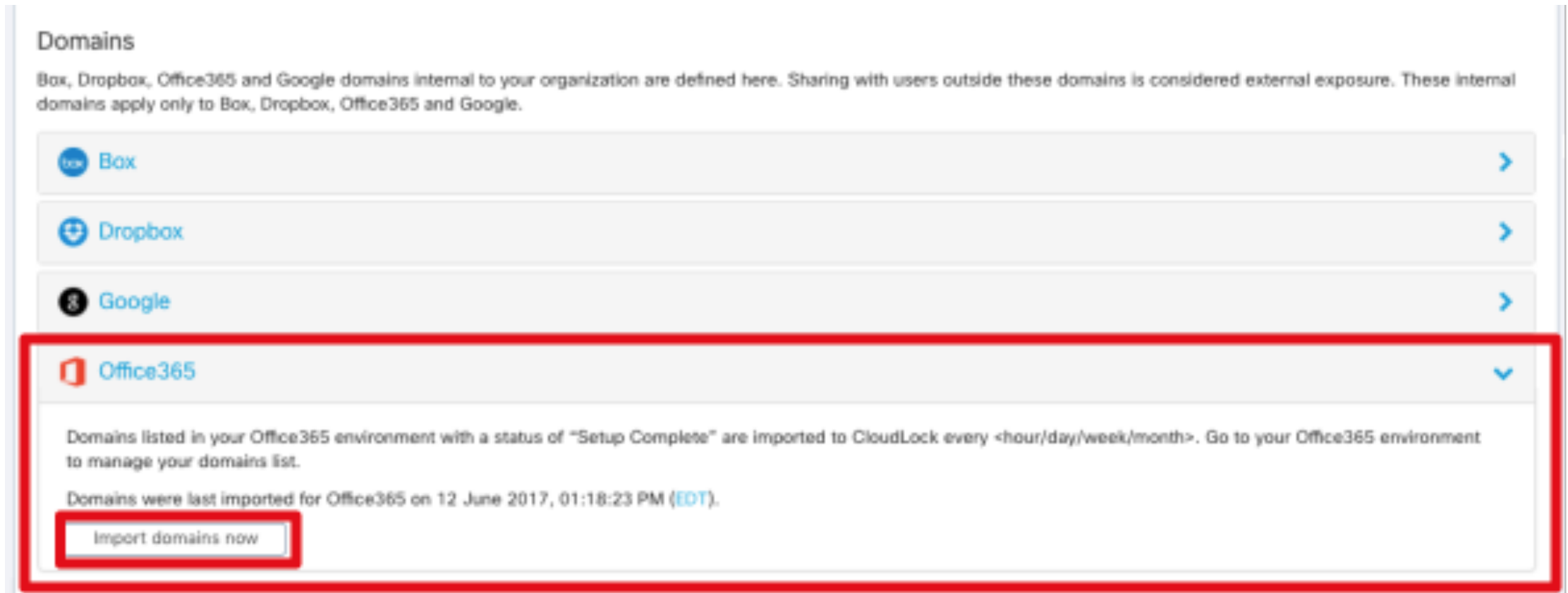
- Улучшенный процесс авторизации, больше не требуются права глобального админа для получения доступа к OneDrive и Sharepoint Online
- Возможность мониторинга или исключения определенных пользователей и групп



Cloudlock for Office 365 Improvements

Recent Improvements

- Available domains automatically listed in platform configuration



The screenshot shows the 'Domains' configuration page in Cloudlock. It lists four domain categories: Box, Dropbox, Google, and Office365. The Office365 section is highlighted with a red border and contains a detailed description of how domains are imported from the Office365 environment, including a timestamp and an 'Import domains now' button.

Domains

Box, Dropbox, Office365 and Google domains internal to your organization are defined here. Sharing with users outside these domains is considered external exposure. These internal domains apply only to Box, Dropbox, Office365 and Google.

- Box
- Dropbox
- Google
- Office365**

Domains listed in your Office365 environment with a status of "Setup Complete" are imported to CloudLock every <hour/day/week/month>. Go to your Office365 environment to manage your domains list.

Domains were last imported for Office365 on 12 June 2017, 01:18:23 PM (EDT).

[Import domains now](#)

Cloudlock App Discovery (Shadow IT)

Сейчас в ВЕТА

Dashboard Save page to PDF

83 unreviewed apps in the last 7 days

137 apps under audit in the last 7 days

826 apps not approved in the last 7 days

985 apps approved in the last 7 days

Traffic by App Risk

Showing a total of 675 GB over 350 shadow IT apps from the last 7 days

39 GB total traffic

June 14, 2017
Apps included: Unreviewed, Not Approved, Under Audit, Approved

7.5 GB very high **7.3 GB low**
6.2 GB high **6.6 GB very low**
11.4 GB medium

Very low risk

Filter: Show All Traffic, From All Geographies, All Log Sources

Recent Unreviewed Apps

Showing the 10 most recently discovered apps out of 83 total shadow IT apps that have not been evaluated as approved, not approved or will be placed under audit, will be left as unreviewed.

Filter Risk: Very High risk, High risk, Medium risk, Low risk, Very low risk

Discovered	Application	Vendor	Weighted Risk	30 Day # of Source IPs	30 Day Traffic	Approve?
Today	Last Pass Computer Security	LastPass	High	22	9,485 GB total traffic 6,780 GB 2,705 GB	Evaluate
Today	Zoho Accounts Account Management	Zoho Corp	Medium	211	31,473 GB total traffic 7,350 GB 24,123 GB	Evaluate
Yesterday	Lucidchart Data Manipulation & Analysis	Lucid Software, Inc.	Low	15	458 GB total traffic 0 GB 458 GB	Evaluate
2 days ago	Conceptboard Collaboration	Digital Republic Media Group GmbH	Very High	5,351	9,485 GB total traffic 6,780 GB 2,705 GB	Evaluate
2 days ago	HelloSign Editing/Authoring	JN PROJECTS Inc.	Very High	269	16,278 GB total traffic 12,325 GB 4,283 GB	Evaluate

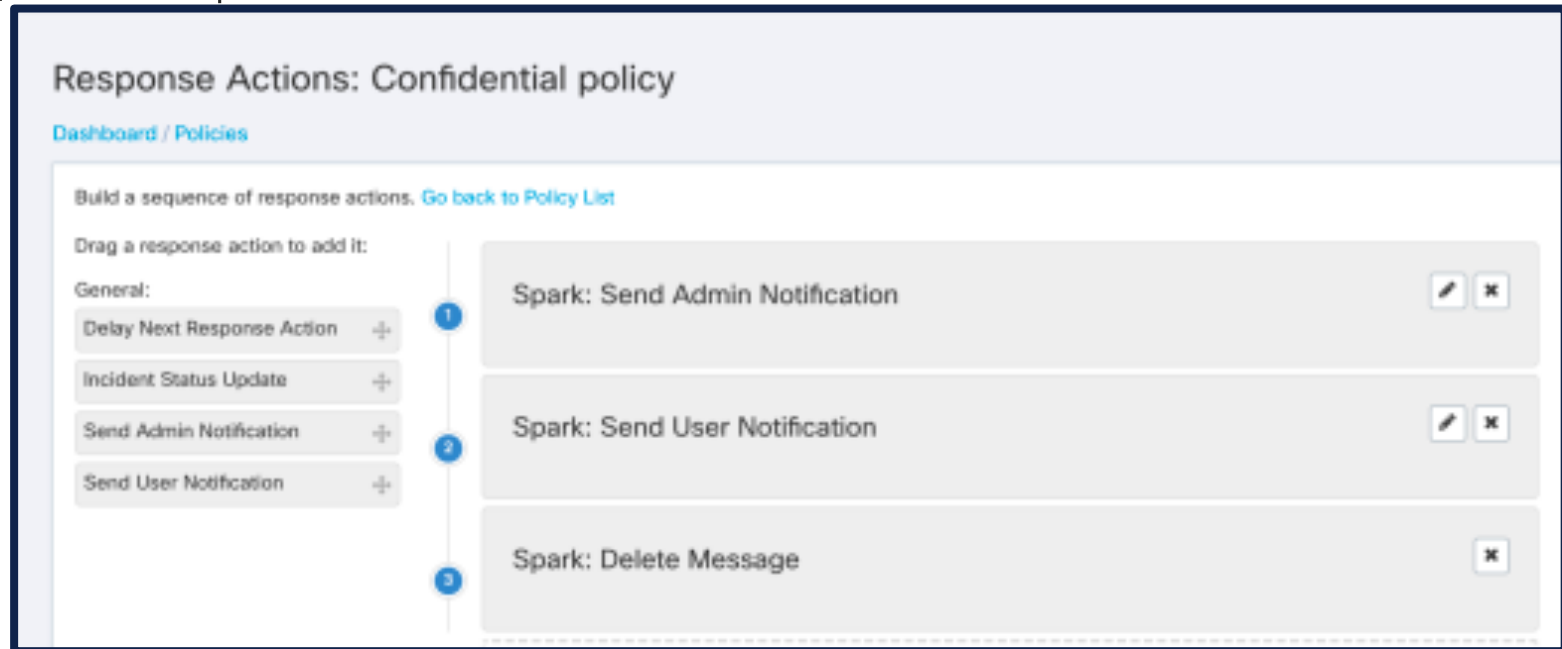
76% inbound traffic

Approve, Don't Approve, Put Under Audit, View Details

Cloudlock для Cisco Spark

Сейчас в ВЕТА

- Идентификация чувствительной информации, которая существует в Spark spaces и загруженных файлах
- Нотификация о нарушениях политик на Spark
- Удаление сообщений и файлов



Email Security

- Email Security 11.0 и дальше

Email Security: ключевые фазы развития

Улучшение безопасности

- Улучшенная эффективность анти-спам, фишинг, спуфинг
- Интеграция
- Advanced Threat Detection

Гибкость платформы

- Образы для частных и публичных облаков
- Поддержка большого количества физических и виртуальных платформ

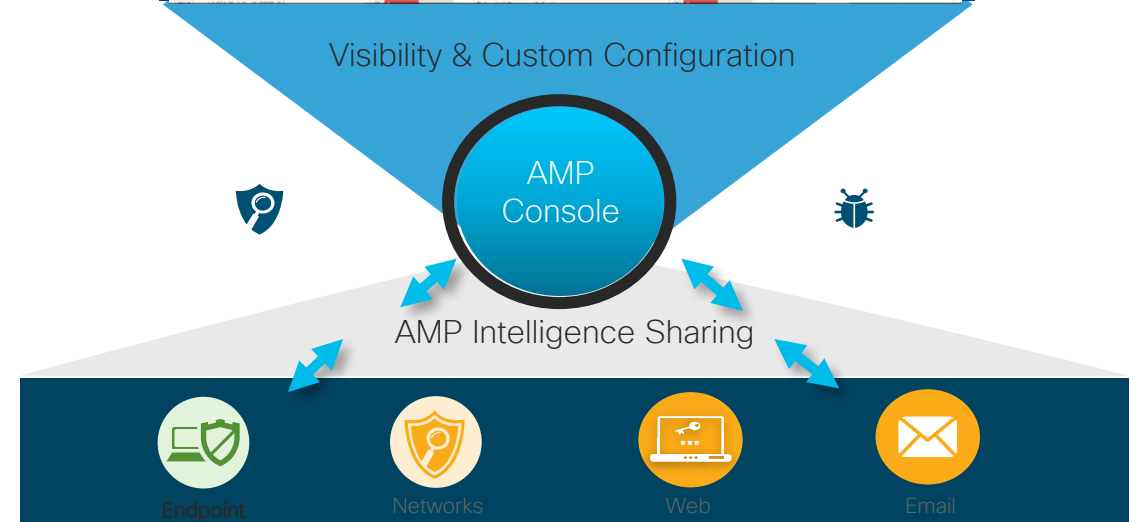
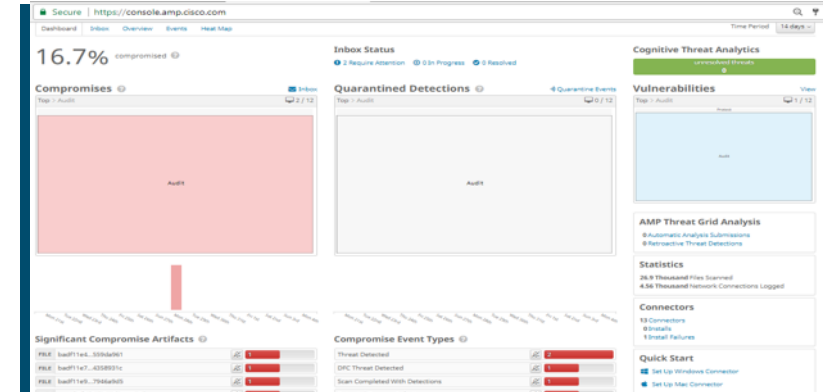
Улучшение UE

- Фокус на предоставлении улучшенных данных и инструментов для администраторов и аналитиков
- Выравнивание функционала CLI и GUI
- Соответствие с остальным портфолио Cisco

Email Gateway интегрируется в AMP консоль

Видимость и контроль вредоносных файлов

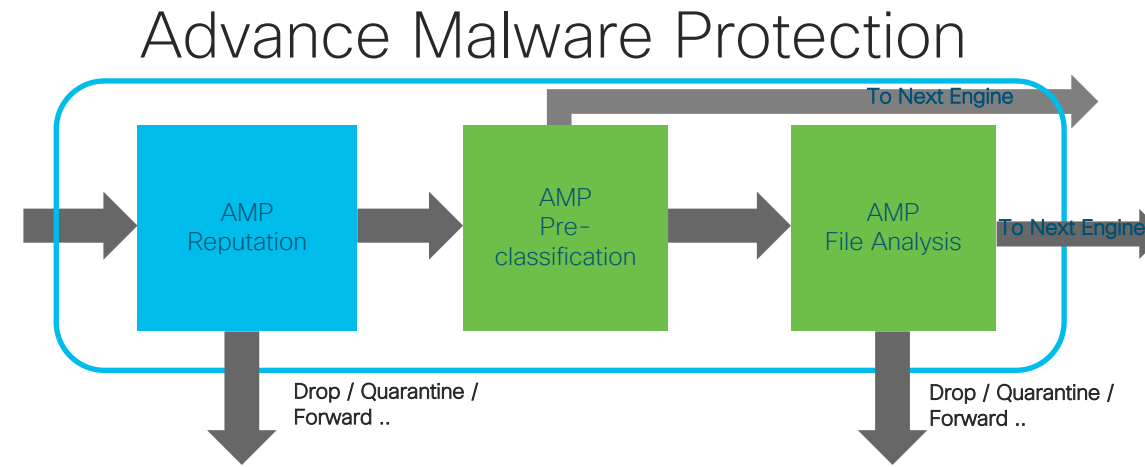
- Indicators of Compromise (IoC), File Trajectory
- несколько устройств (Email Gateways, End Points, Firewalls) и общая политика
- Whitelist, blacklist файловых хешей SHA через устройства



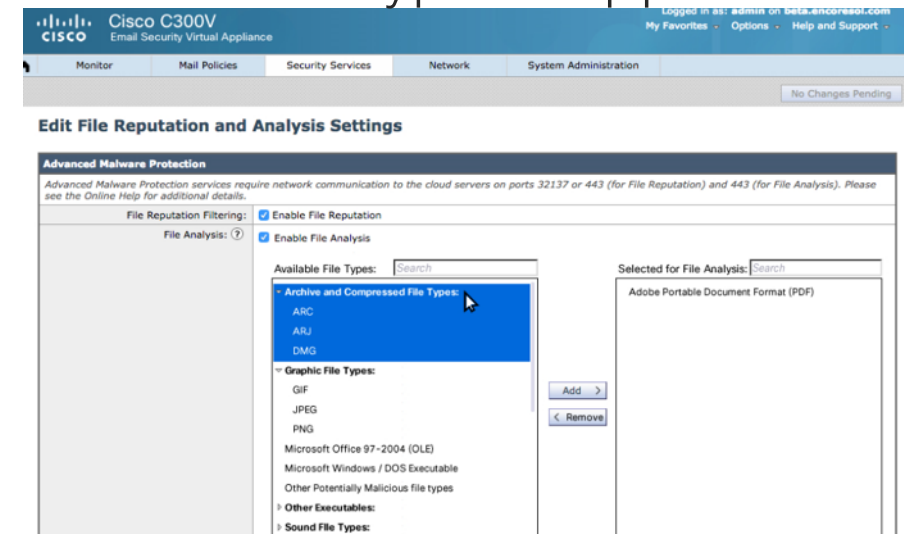
Улучшенные возможности AMP

Больше типов файлов и возможностей

1. Расширение механизма классификации для детектирования файлов
2. Дополнение списка действий для подозрительных файлов
3. Поддержка всех типов файлов в AMP/TG
4. Возможность заблокировать ретро-предупреждения для файлов не в почтовом ящике пользователя



More File types supported

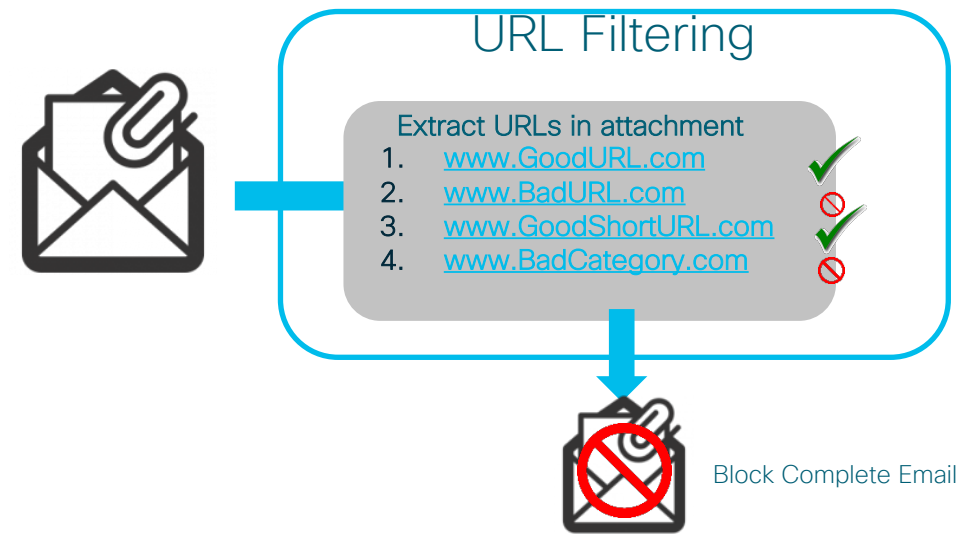
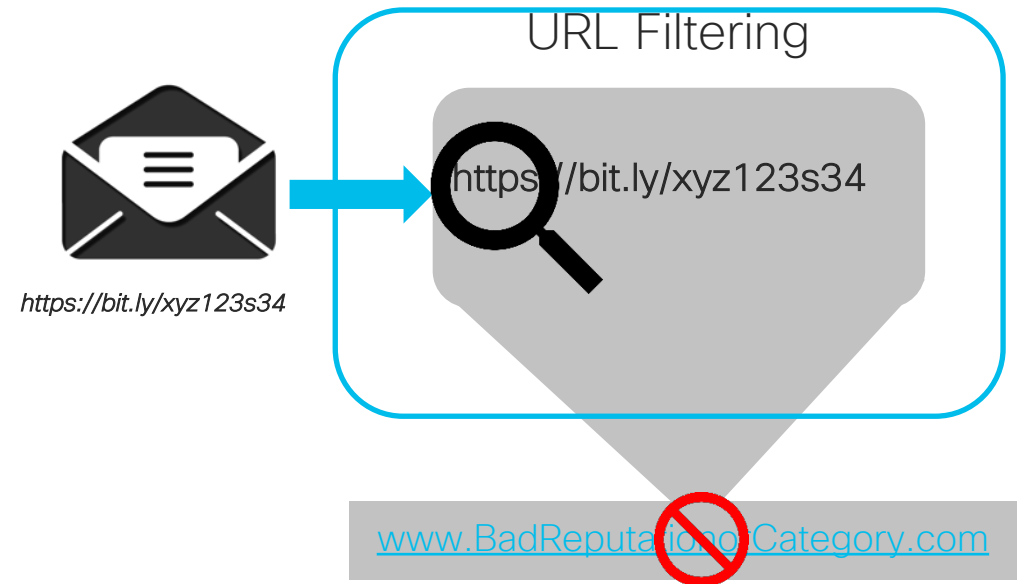


Augmented in 11.1

Улучшенная фильтрация URL

Защита от обфусцированных URL

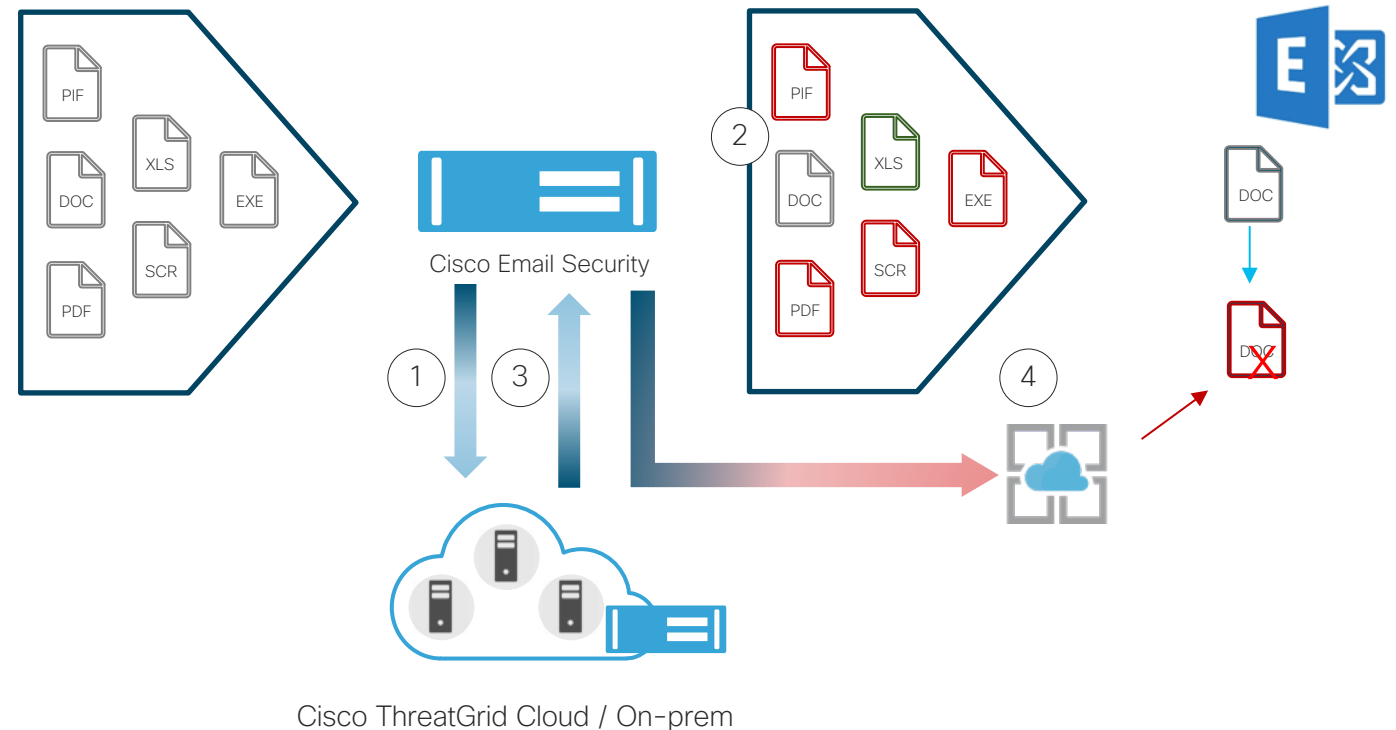
- Обнаружение актуальных URL за сокращенными ссылками
- Обнаружение URL в присоединенных файлах



Mailbox Auto Remediation – MS Exchange

Уменьшайте время на реагирование

1. Аттач проанализирован
2. Аттач имеет неизвестное состояние и отправлен пользователю
3. Случилось ретроспективное событие и аттач оказался вредоносным
4. Автоматизированный вызов API позволяет удалить письмо из ящика пользователя



Forged Email Detection V2

Защита от спуфинг-атак / Business Email Compromise (BEC)



Pre-processing



From: Chuck
<chuck.robbins@mail.com>

Subject: [URGENT] Need help
transferring funds

Inspects the SMTP envelope address:

```
$ telnet mail-smtp-in.l.mail.com 25
Trying 74.125.206.26...
Connected to mail-smtp-in.l.mail.com.
Escape character is '^]'.
220 mx.mail.com ESMTP i11si22058766wmh.67 - gsmt
HELO mail.outside.com
250 mx.mail.com at your service
MAIL FROM:<adam@outside.com>
250 2.1.0 OK i11si22058766wmh.67 - gsmt
RCPT TO:<alan@mail.com>
250 2.1.5 OK i11si22058766wmh.67 - gsmt
Data
```

Recipient Domain

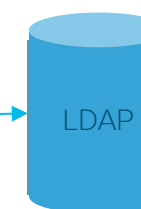
Sending Domain

Actual Sender

SMTP Envelope



Recipient



Sending Domain



Cousin / Look Alike

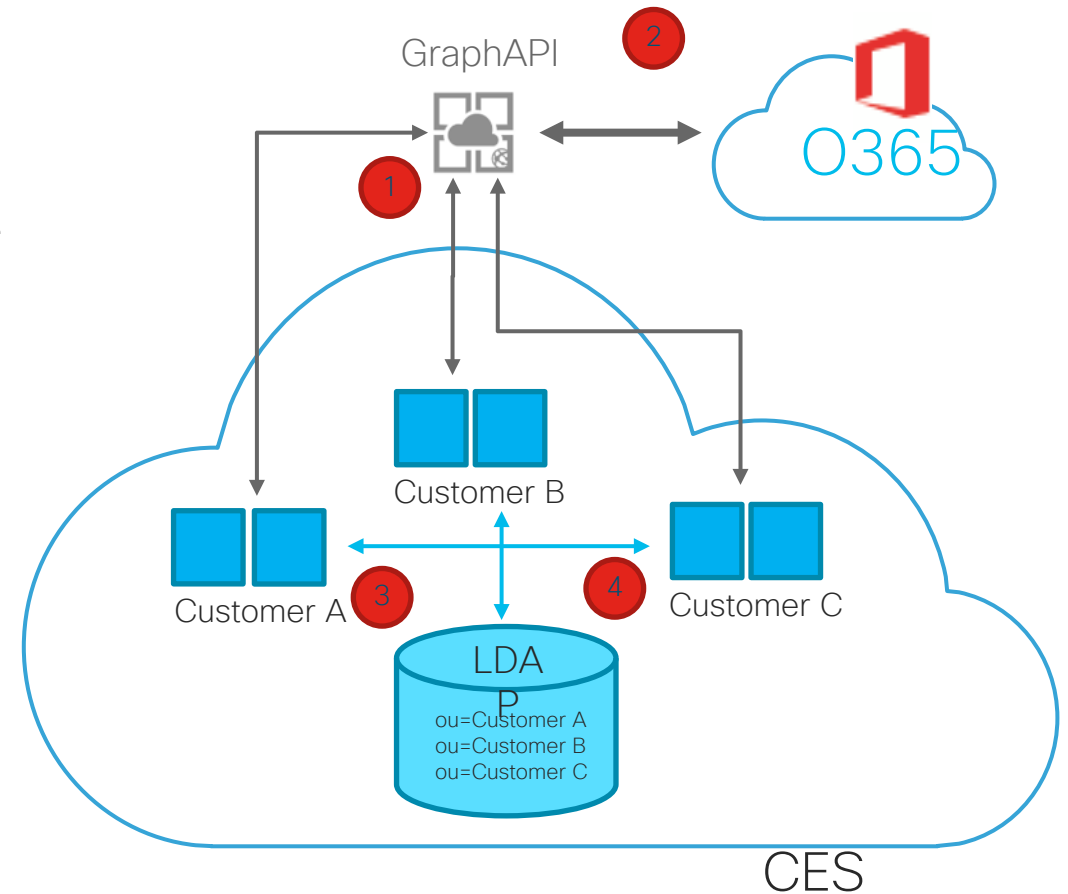
Inspect SMTP envelope
for True sender address

Match sender address against
company directory

O365 Connector



- Native LDAP and Mailbox Access functionality in CES with Azure
- Sync recipient and group information inside Azure AD with CES LDAP server
- Read-only access to the directory to review and verify records

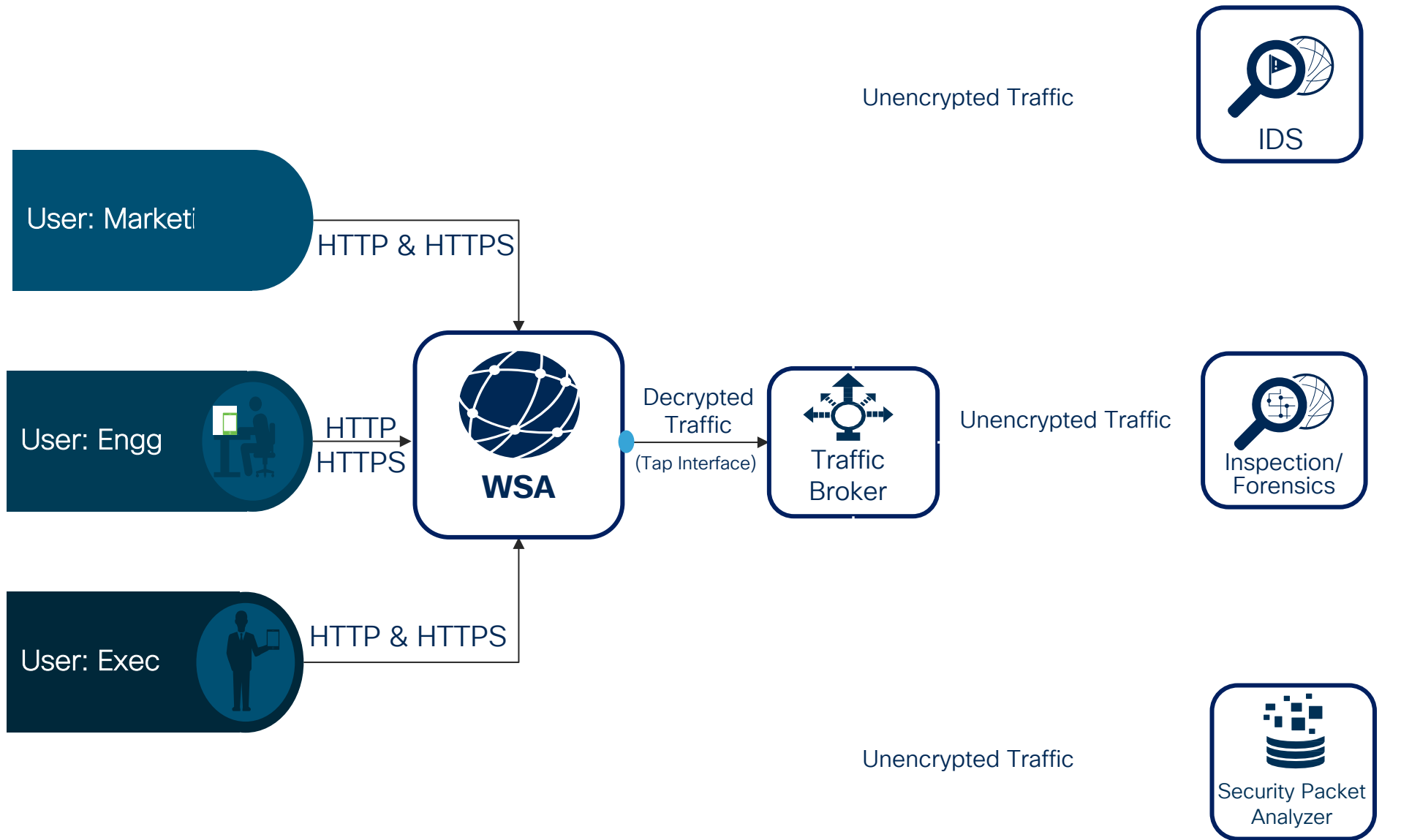


Web Security Appliance



Web Traffic Tap

11.5



- High Performance SSL Decryption
- SSL Decryption only once for Network
- No Dedicated SSL Appliance Required
- Malware protection on SSL Traffic

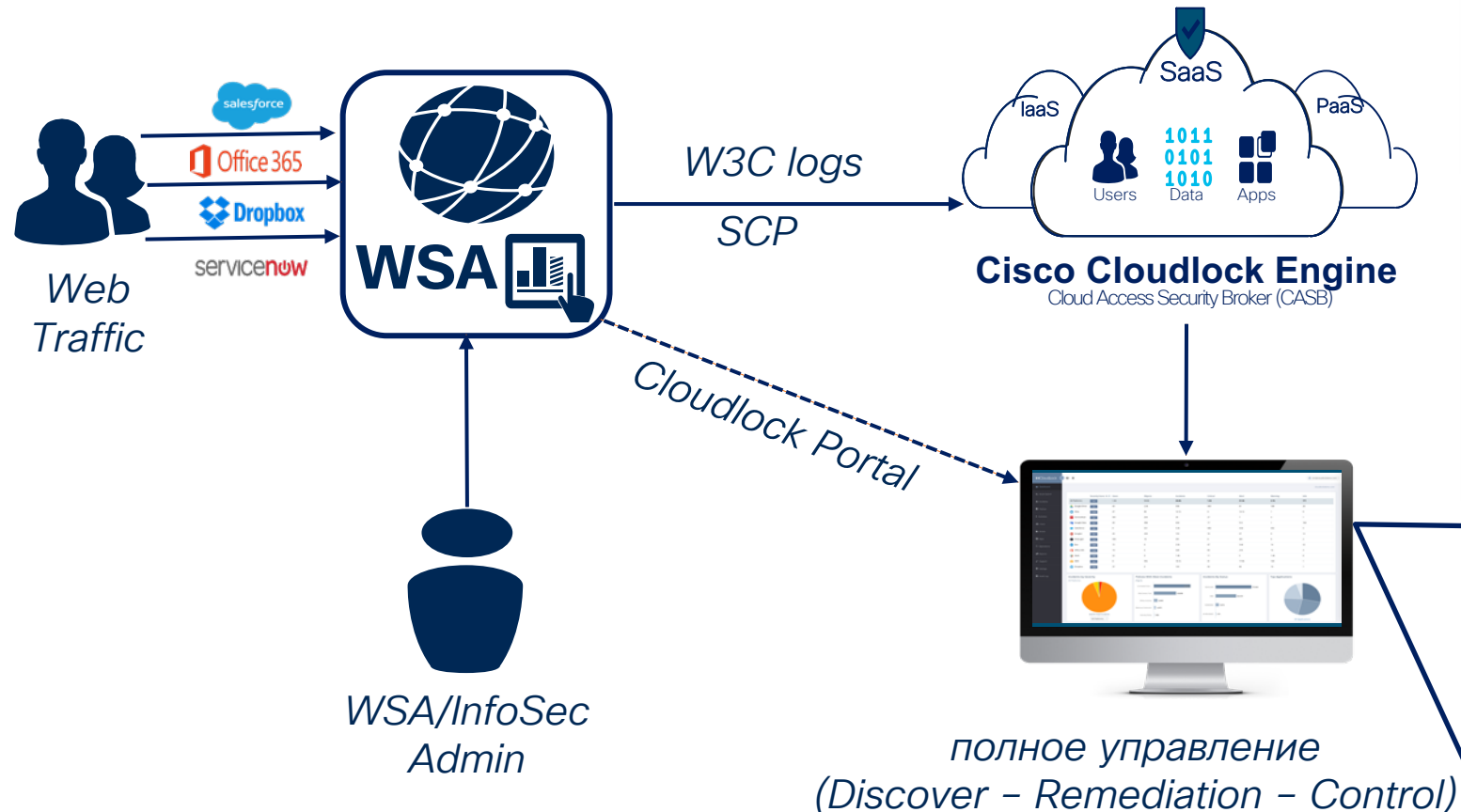




Cisco Cloudlock интеграция

11.5

App Discovery



полное управление
(Discover – Remediation – Control)

Dashboard
SHADOW IT RISK
We found 968 total apps for the last 30 days.

- PaaS**: 211.57 MB / 1% of traffic
- IaaS**: 36.03 GB / 40% of traffic
- SaaS**: 54.78 GB / 61% of traffic

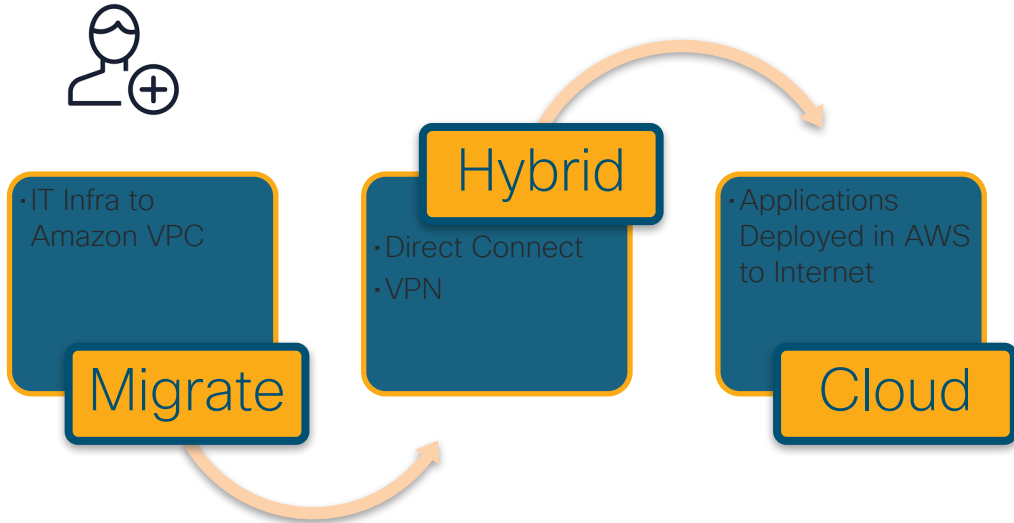
Top 10 Risky Apps

App	Risk	Vendor	App URL	App type	Source IPs	Traffic (MB)
Janrain Security	Critical	Janrain	www.janrain.com	SaaS	153	13,943,393
Last.fm Media	Low	Last.fm	www.last.fm	SaaS	2	1,174,388
LogmeOnce Security	Very Low	LogmeOnce	www.logmeonce.com	SaaS	1	15,367
Powerinbox Marketing & Sales	High	Powerinbox	powerinbox.com	SaaS	1	5,788
Kruix Marketing & Sales	Very Low	Kruix Digital	www.kruix.com	SaaS	806	84,918,783
1&1 Hosting Services	Low	1&1	www.1and1.com/web-hosting...	IaaS	2	347,790
LimeLight CDN Content Delivery Network	Medium	LimeLight Networks	www.lime-light.com/delivery	IaaS	13	1,616,678
Sequoia E-Commerce	Very Low	Sequoia	www.sequoiainc.com/products	SaaS	1	377,303
Napster Media	High	CISA control	www.napster.com	SaaS	3	9,934,616
iPage Hosting Services	Medium		www.ipage.com	IaaS	2	201,315

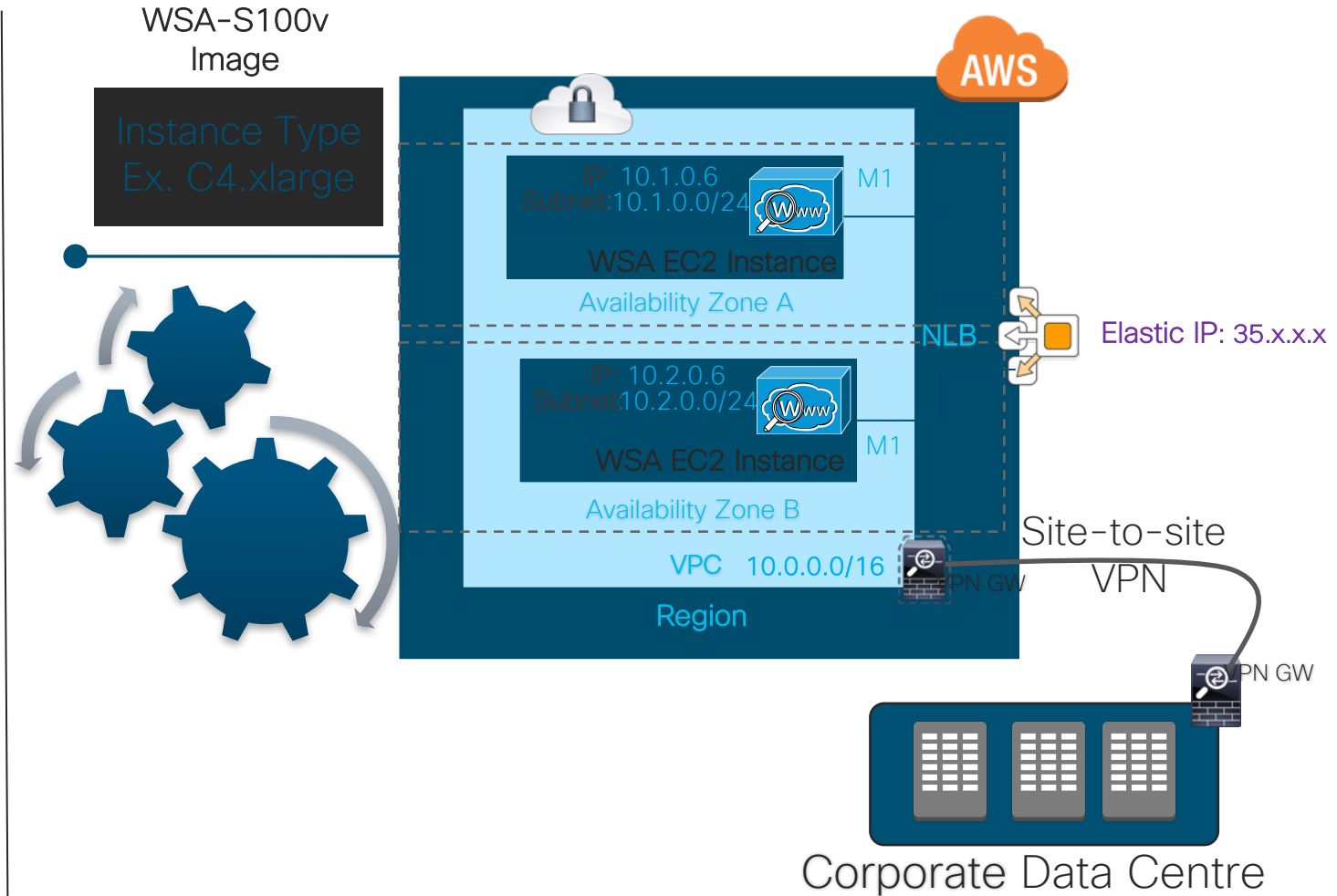
968 Apps found

App	Risk	Status	Vendor	Source	Source IPs	Total Traffic	First Detected (UTC)	Last Detected (UTC)
1&1 Hosting Services	Low	✘ Unsactioned	1&1	wsa	2 source IPs	339.64 KB	May 15, 2017 12:00:00 AM	May 15, 2017 12:00:00 AM
iPage Hosting Services	Medium	✘ Unsactioned	iPage	wsa	2 source IPs	196.6 KB	May 14, 2017 12:00:00 AM	May 16, 2017 12:00:00 AM
Janrain Security	Critical	✘ Unsactioned	Janrain	wsa	153 source IPs	12.96 MB	May 13, 2017 12:00:00 AM	May 16, 2017 12:00:00 AM
LogmeOnce Security	Very Low	✘ Unsactioned	LogmeOnce	wsa	1 source IP	15.01 KB	May 15, 2017 12:00:00 AM	May 15, 2017 12:00:00 AM
Napster Media	High	✘ Unsactioned	Napster	wsa	3 source IPs	9.47 MB	May 15, 2017 12:00:00 AM	May 16, 2017 12:00:00 AM
Powerinbox Marketing & Sales	High	✘ Unsactioned	Powerinbox	wsa	1 source IP	5.65 KB	May 15, 2017 12:00:00 AM	May 15, 2017 12:00:00 AM
Kruix Marketing & Sales	Very Low	✘ Unsactioned	Kruix Digital	wsa	806 source IPs	80.98 MB	May 13, 2017 12:00:00 AM	May 16, 2017 12:00:00 AM
Last.fm Media	Low	✘ Unsactioned	Last.fm	wsa	2 source IPs	1.12 MB	May 15, 2017 12:00:00 AM	May 15, 2017 12:00:00 AM
Sequoia E-Commerce	Very Low	✘ Unsactioned	Sequoia	wsa	1 source IP	368.46 KB	May 15, 2017 12:00:00 AM	May 15, 2017 12:00:00 AM

WSAv на Amazon Web Services



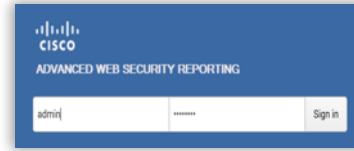
Virtual Image	AWS Instance Type
s100v	C4-xlarge
s300v	C4-2xlarge
s600v	C4-4xlarge



Ключевые возможности интеграции WSA



Advance Web Security Reporting v6.2

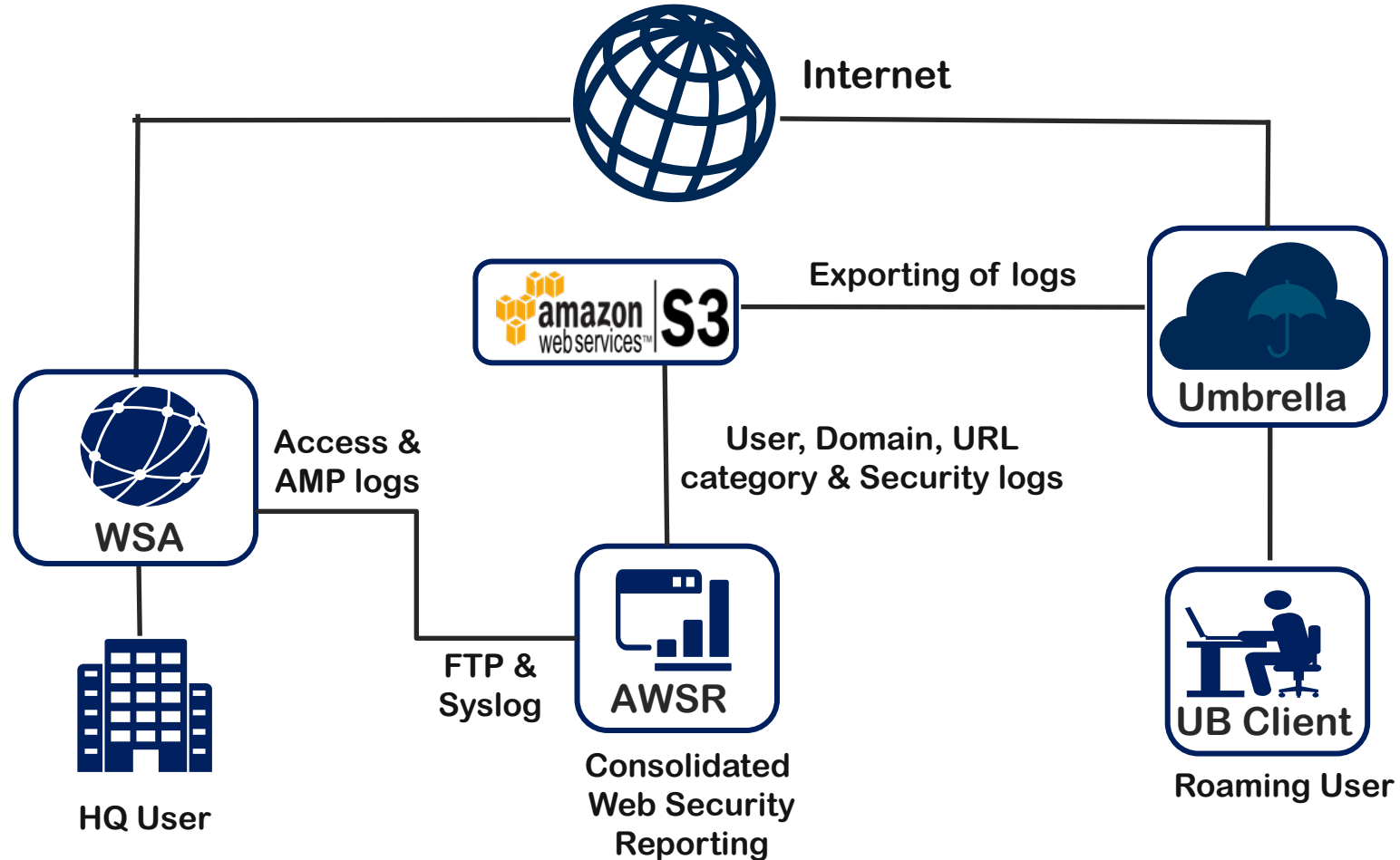


Один механизм просмотра Web Security

Настраиваемые отчеты

Сохранение логов для расследований

Групповые отчеты





Video Caching Solution



Saving Bandwidth

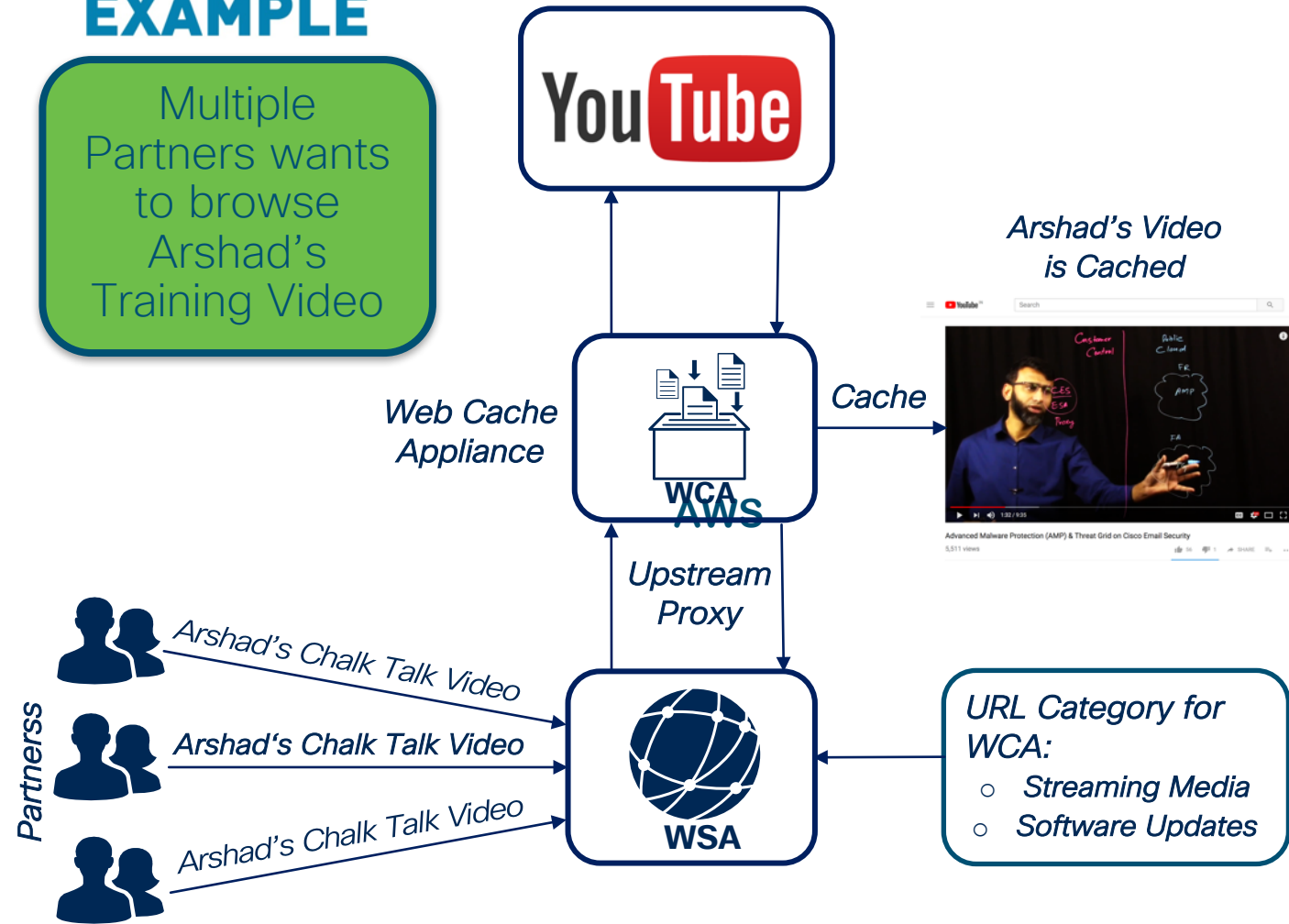
Caching Video & Software Updates

Blocking Adult Video content

Video Resolution locker

Let me give you an
EXAMPLE

Multiple Partners wants to browse Arshad's Training Video



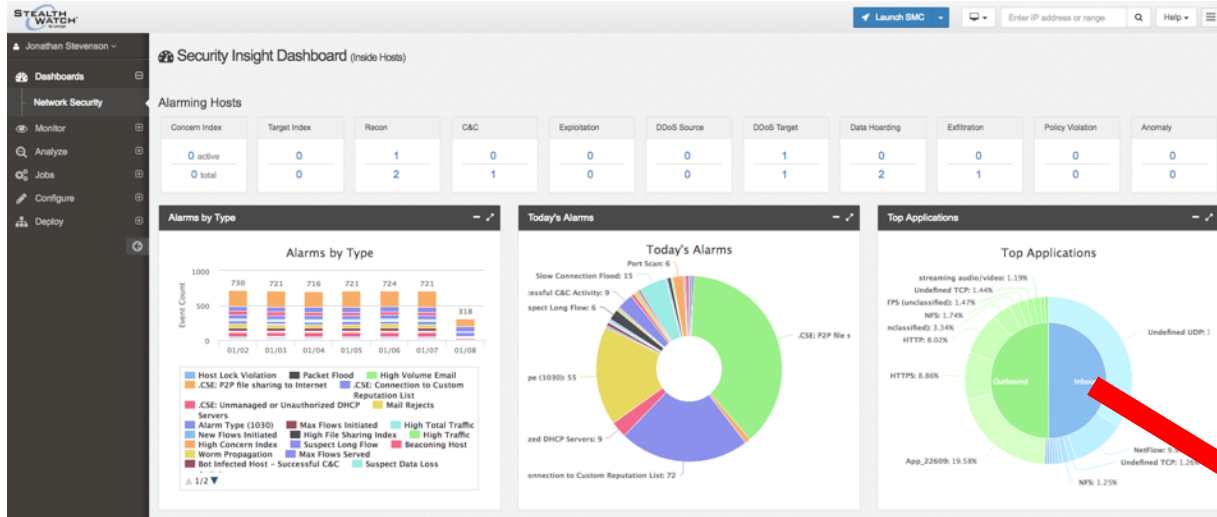


Stealthwatch

Аналитика безопасности для цифрового бизнеса

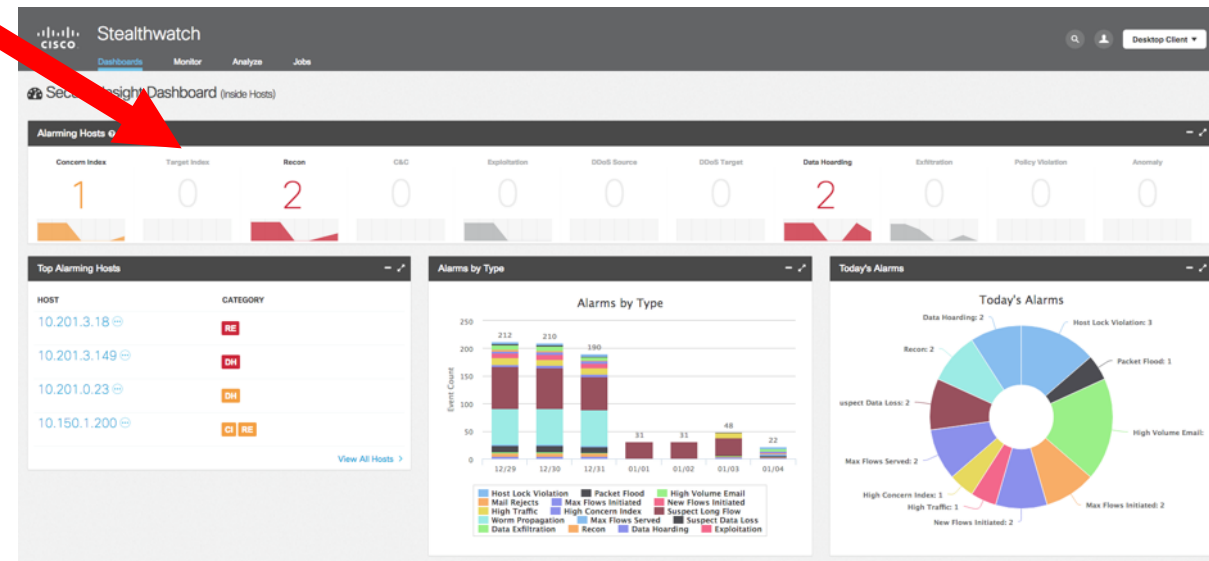
Новое в StealthWatch 6.9!

Существенные улучшения Web UI



SMC 6.8

SMC 6.9



Host Group Reports

The screenshot displays the Cisco Stealthwatch interface for a Host Group Report on 'Inside Hosts'. A red circle highlights the 'Change Host Group' button in the top left. Another red circle highlights a 'Select Host Groups' dialog box on the right side of the screen. The dialog box contains a search bar with 'dmz' entered and a list of host groups. The 'DMZ' group is highlighted in red in the list.

Host Group Report | Inside Hosts

Change Host Group

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration
1	0	2	0	0	0	0	2	0

Summary

Inside Hosts
2 TB total data currently monitored

551 GB In → 1 TB Internal → 50 GB Out

Total Traffic (Last 7 Days)

Category	Value
Inbound	1.2 TB
Outbound	419.8 GB
Internal	8.7 TB

Top Applications (Last 12 Hours)

Select Host Groups

Please select the host group(s) you wish to add to the query

Host Group Selector

Inside Hosts x

dmz

- Inside Hosts
- Blackhole
- Business Units
- By Function
 - Access Points
 - BC Authentication
 - Client IP Ranges (DHCP Range)
 - DMZ**
 - NAT Gateway
 - Network Scanners
 - Other
 - Printers
 - Protected Assets
 - Proxy
 - Servers
 - Users
 - VoIP
 - Watch List
- By Location
 - Catch All
 - Cloud Hosts
 - Compliance Systems
- Outside Hosts
 - Business Partner Networks
 - Countries
 - Custom Reputation List
 - Filtered Internet Hosts

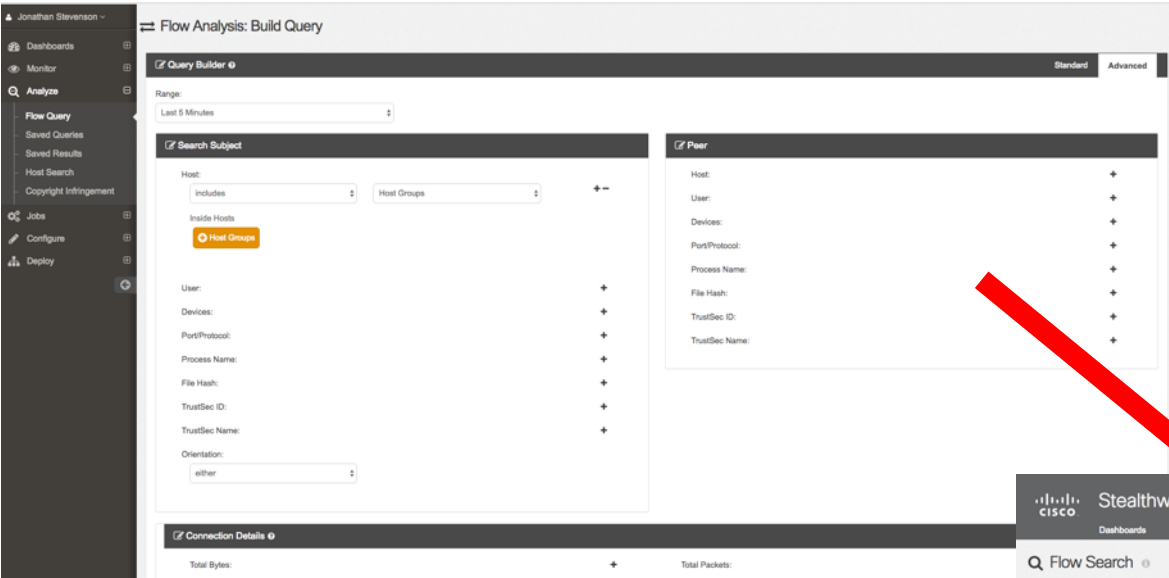
Cancel Select

Поиск в ассоциированных потоках

The screenshot displays the Cisco Stealthwatch 'Hosts' page. The interface includes a top navigation bar with 'Stealthwatch' and 'Cisco' logos, and a search bar. Below the navigation, there are tabs for 'Dashboards', 'Monitor', 'Analyze', and 'Jobs'. The main content area is titled 'Hosts (2000)' and features a 'Current Filters' section on the left, which is currently empty. Below this is a 'Filter Results By:' section with three expandable categories: 'ALARMS', 'HOST GROUPS', and 'LOCATIONS'. The 'ALARMS' section lists various security alerts such as 'Concern Index (820)', 'Recon (4)', and 'Data Hoarding (3)'. The 'HOST GROUPS' section shows 'Inside Hosts (5321)'. The 'LOCATIONS' section lists 'RFC 1918 (1451)', 'United States (521)', and 'Unknown (28)'. The main table displays a list of hosts, sorted by overall severity. The first row is highlighted, and a context menu is open over it, showing options like 'View Flows', 'External Lookup', and 'Top Reports'. The table columns include Host Address, Host Name, First Sent, Last Sent, CI, TI, RC, C&C, EP, DS, DT, DH, EX, PV, AN, Location, and Host Groups. The first row shows a host with address 10.150.1.200, last sent on 1/8/17 at 10:26 AM, and a severity score of 155%.

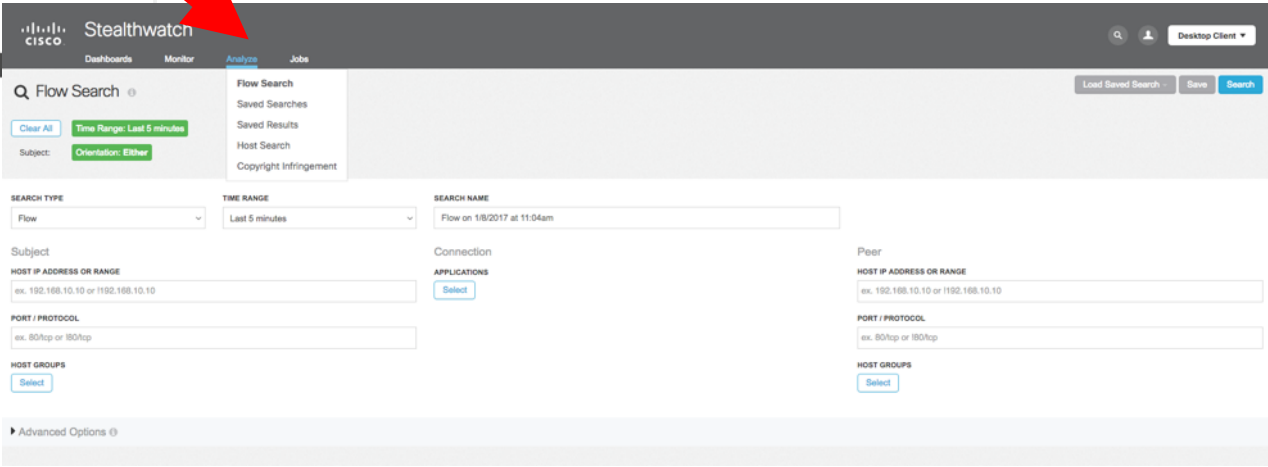
Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
10.150.1.200		11/16/16 11:46 PM	1/8/17 10:26 AM	155%	1%	2,984%					111%				RFC 1918	WebHostedApp
		11/16/16 11:51 PM	1/8/17 10:26 AM	7%		1,846%									RFC 1918	End User Devices Desktops Atlanta Sales and Marketing
		11/16/16 11:35 PM	1/8/17 10:26 AM	2%	1%	60%					529%	2%			RFC 1918	End User Devices Desktops Atlanta Sales and Marketing
		11/14/16 7:54 PM	1/8/17 10:26 AM	4%	1%						485%				RFC 1918	Terminal Servers Atlanta Datacenter
10.201.3.78	workstation-078.	11/14/16 7:54 PM	1/8/17 10:27 AM	13%			4%								RFC 1918	End User Devices Desktops Atlanta Sales and Marketing
209.182.184.2		11/14/16 7:54 PM	1/8/17 10:26 AM	17%	1%										United States	Datacenter
10.10.30.16		11/16/16 9:27 AM	1/8/17 10:26 AM	13%	1%										RFC 1918	End User Devices Desktops New York Domain Controllers DNS Servers
10.201.0.16	server-016.	11/14/16 7:54 PM	1/8/17 10:27 AM	10%	1%										RFC 1918	Domain Controllers Atlanta
10.201.3.83	workstation-083.	11/16/16 8:06 PM	1/8/17 10:26 AM	9%	1%										RFC 1918	End User Devices Desktops Atlanta Sales and Marketing
10.201.0.77	silver-srv-077.	11/14/16 7:54 PM	1/8/17 10:26 AM	6%											RFC 1918	Atlanta BC Authentication
10.10.101.24		11/16/16 8:12 PM	1/8/17 10:18 AM	3%											RFC 1918	End User Devices Desktops New York

Расширенный поиск в потоках

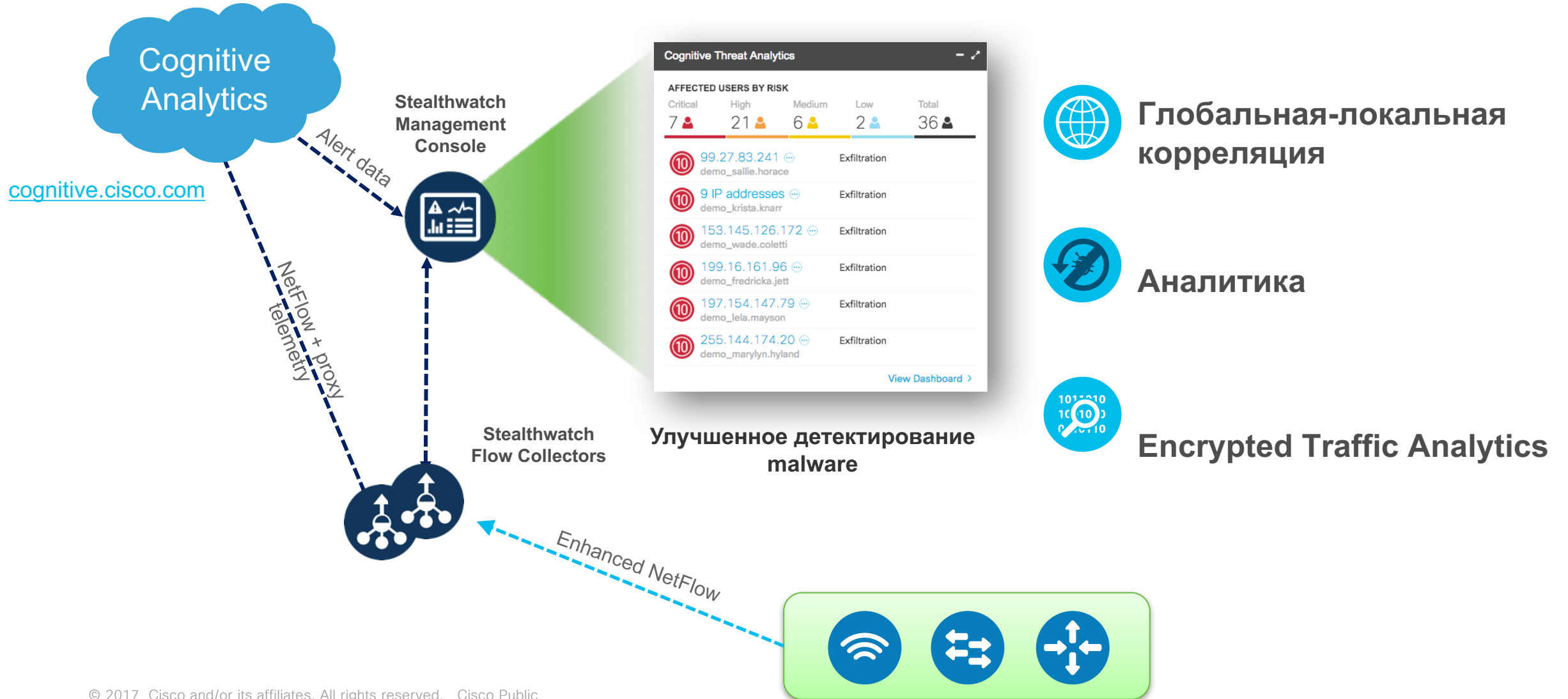


SMC 6.8

SMC 6.9



Stealthwatch и Cognitive Analytics



Stealthwatch ➤ Cognitive – User Flows

СТА виджет в SW

СТА инцидент на консоли SW

СТА в отдельном окне

Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low	Total
7	21	6	2	36

IP Address	Activity
99.27.83.241	Exfiltration
9 IP addresses	Exfiltration
153.145.126.172	Exfiltration
199.16.161.96	Exfiltration
197.154.147.79	Exfiltration
255.144.174.20	Exfiltration

[View Dashboard >](#)

Cognitive Threat Analytics

10 99.27.83.241
demo_sallie.horace
Apr 3 4 hours

Apr 10

10 Exfiltration
#CMST04

Apr 3

- 9 https communication
- 9 https communication
- 9 https communication

10 NEW

[Incident Detail >](#)

DASHBOARD CONFIRMED DETECTED

10 MALWARE
100% confidence, in #CMST04
NEW

AFFECTING
demo_sallie.horace (Windows)
99.27.83.241

OCCURRENCE
4 hours
Apr 3 - Apr 3

ACTIVITIES AND FLOWS

ACTIVITIES (3) DOMAINS (6) IPS (6) AUTONOMOUS SYSTEMS (2)

9 https communication
9 https communication
9 https communication

148.251.80.172
93.190.140.144
136.243.4.69
148.251.80.145
217.23.6.72
136.243.4.68

148.251.80.172
93.190.140.144
136.243.4.69
148.251.80.145
217.23.6.72
136.243.4.68

Herzner Online GmbH
WorldStream

UPLOAD 1.2 KIB DOWNLOAD 8.8 KIB REQUESTS 14 DURATION 7 minutes 36 seconds USER AGENTS 1 NO REFERRER 100% HTTP 0

Client IP	Server IP	URL	SHA	Filter	REFERRER	USER	BYTE	HEJ	HTI	TIMESTAM	DUR	FILENA	CATEG	CONTEI	CLIENT
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	372 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	455 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	365 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	470 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	367 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	124 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	361 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	367 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	364 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	369 ms			unclassified
W	148.251.80.1	https://148.251.80.172/					89	640	X	0	Apr 3, 2017	555 ms			unclassified

Выберите IP

Выберите детали

СТА Dashboard на отдельной странице

Stealthwatch 6.10

Stealthwatch 6.10 – кратко

Расширения Web UI

- Расширенный поиск
 - Параметры запросов и результаты
 - Ограничение результатов запроса
 - Загрузка результатов запроса
 - Фильтрация результатов
- Расширенные группы событий
 - Host Report Security
 - Детали события безопасности
- Упрощение интерфейса

Отчеты о сети

- Статус и утилизация интерфейсов
- Host Group Traffic Widget

KVM Hypervisor support

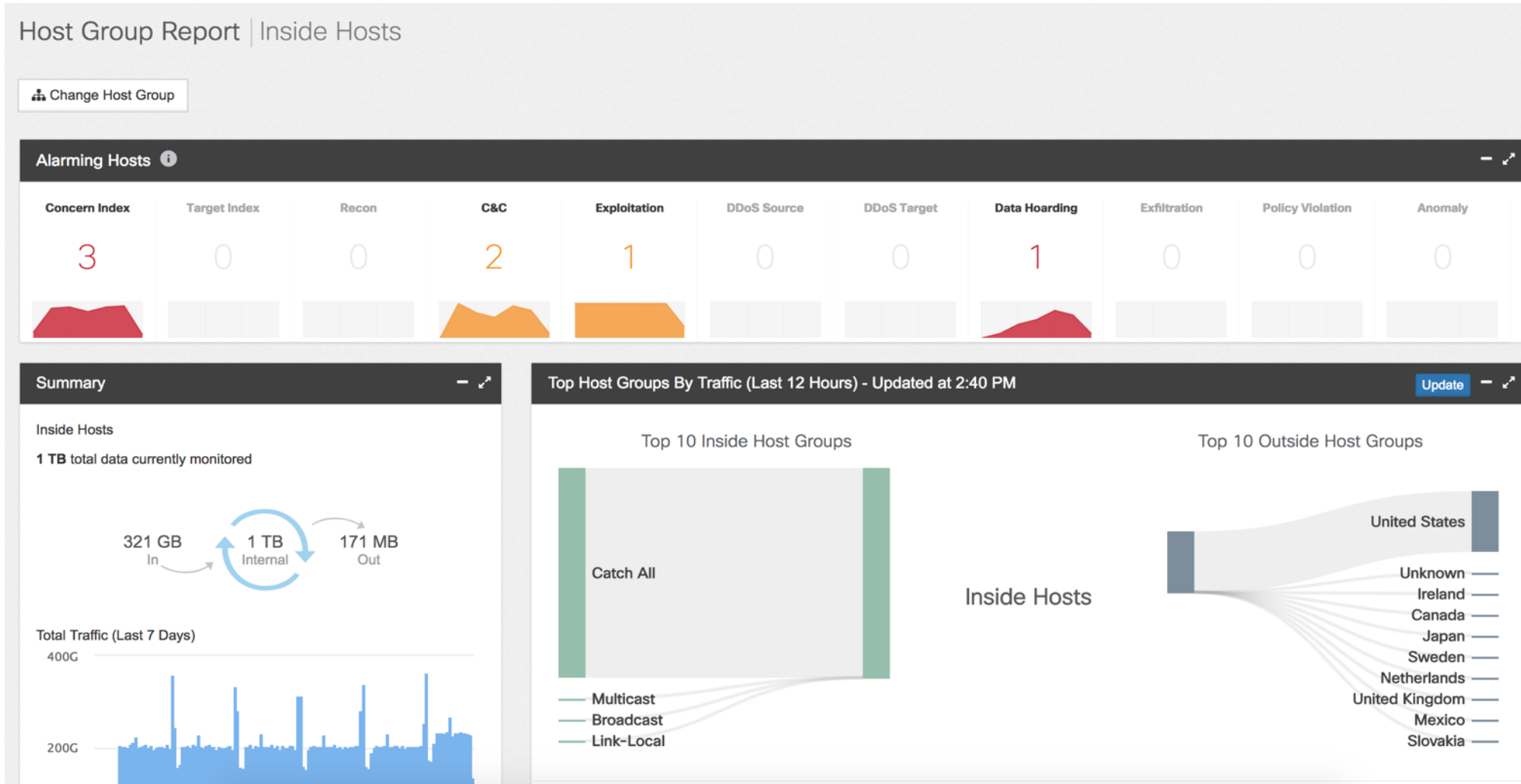
FIPS 140-2 Compliance

API enhancements

- Top reports
- Security events
- Network ops.

Расширения системы обновлений

Host Group Dashboard Traffic Widget



Статус интерфейсов

Stealthwatch Cisco

Search, User, Settings, Desktop Client



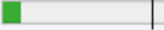
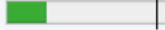
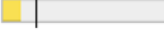
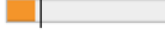
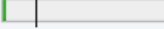
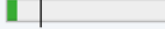
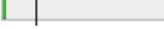
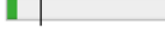
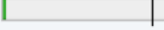
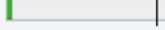
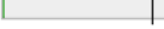
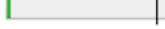
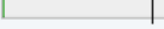
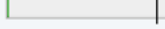
Dashboards **Monitor** Analyze Jobs Configure Deploy

Interfaces (130)

Filter by Device

- Hosts
- Host Groups
- Users
- Interfaces**

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	FLOW COLLECTOR	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
▶ ifIndex-147	10.203.0.1	nflow-691-10-0-44-11...	 41.43%	414.31 mbps	 62.56%	625.56 mbps	INBOUND	1 gbps
▶ ifIndex-1	10.203.17.40	nflow-691-10-0-44-11...	 11.09%	110.91 mbps	 23.41%	234.13 mbps	INBOUND	1 gbps
▶ ifIndex-146	10.203.0.1	nflow-691-10-0-44-11...	 11.02%	110.17 mbps	 17.25%	172.55 mbps	OUTBOUND	1 gbps
▶ ifIndex-146	10.203.0.1	nflow-691-10-0-44-11...	 2.38%	23.83 mbps	 5.76%	57.61 mbps	INBOUND	1 gbps
▶ ifIndex-147	10.203.0.1	nflow-691-10-0-44-11...	 2.36%	23.59 mbps	 5.73%	57.33 mbps	OUTBOUND	1 gbps
▶ ifIndex-4	10.203.0.214	nflow-691-10-0-44-11...	 1.64%	16.36 mbps	 3.02%	30.24 mbps	INBOUND	1 gbps
▶ ifIndex-3	10.203.6.80	nflow-691-10-0-44-11...	 1.16%	11.56 mbps	 2.43%	24.35 mbps	INBOUND	1 gbps
▶ ifIndex-5	10.203.0.208	nflow-691-10-0-44-11...	 0.53%	53.32 mbps	 0.54%	54.26 mbps	INBOUND	10 gbps

Статус интерфейсов

Interfaces (130)

Filter by Device

Interface Status (Since Reset Hour)

INTERFACE	EXPORTER	FLOW COLLECTOR	CURRENT UTILIZATION	CURRENT TRAFFIC	MAXIMUM UTILIZATION	MAX TRAFFIC	DIRECTION	SPEED
ifIndex-147	10.203.0.1	nflow-691-10-0-44-11...	41.43%	414.31 mbps	62.56%	625.56 mbps	INBOUND	1 gbps

Details

Description	--
Total Bytes	1.26 TB
Peak Inbound	625.56 mbps
Peak Outbound	57.33 mbps
Average Packet Rate	43.23 kpps
Current Packet Rate	40.82 kpps
Maximum Packet Rate	62.47 kpps

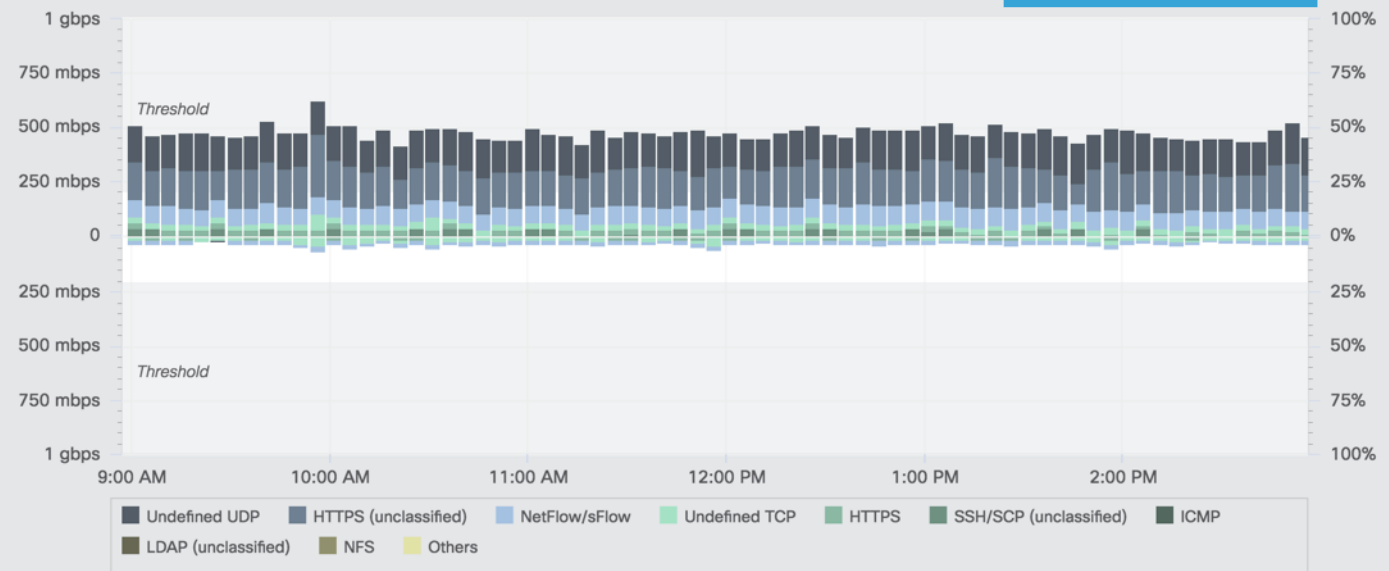
Today's Alarms

- 2 Interface Utilization Exceeded Inbound
- 0 Interface Utilization Exceeded Outbound

Top Application Traffic (bps) Packets (pps)

Utilization

Last 6 Hours



Deselect All Select All



Обновления ISE

Он становится еще лучше!

ISE 2.3

Что вошло в релиз

- За сценой – не функциональные улучшения
- Администратор на чтение
- Логин используя Социальную сеть
- Коннектор Групповых политик
- Улучшения в Оценке состояния
- Изменения движка политик

Click here to do wireless setup and

- Authentication
- Authorization
- Administrators
 - Admin Users
 - Admin Groups
- Settings

Admin Groups > Read Only Admin

Admin Group

Name **Read Only Admin**

Description Access Permission for admin with read-only functionality

Type External

External Identity Source

Name : r1

External Groups

r1.ind/Users/Domain Users +

this is how we map external group of users to Read Only Admin Group

Member Users

Users

+ Add - Delete

<input type="checkbox"/>	Status	Email	Username	First Name	Last Name
<input type="checkbox"/>	Enabled		read-only		

Save Reset

Posture Issues Tackled by ISE 2.4

Customer Challenges

- Need to gracefully deal with end-user posture issues
- Need more flexibility with checks and remediation
- Need to see faster value from an ISE PoV

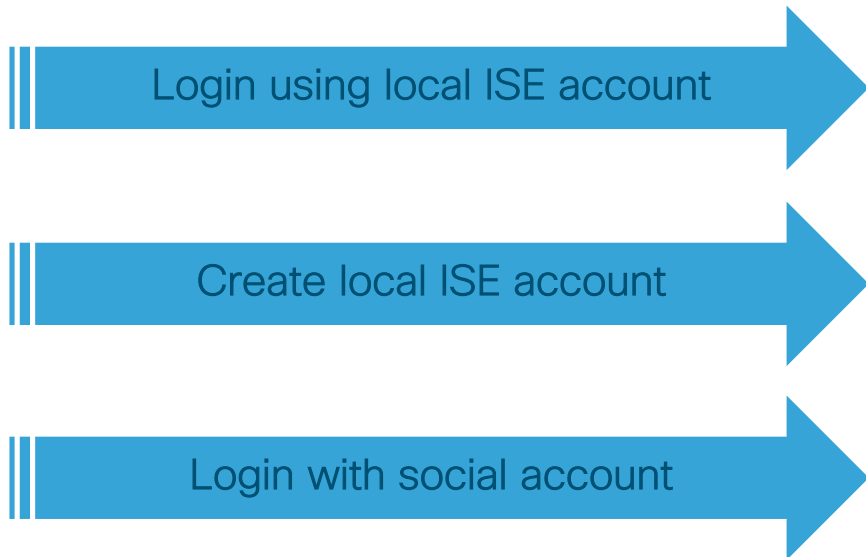
Seller Challenges

- Need to be able to tackle Forescount in their “agentless” story



Логин через социальную
сеть для гостей

Facebook логин для гостей (фаза 1)



CISCO Guest Portal


Sign On
Either enter the username and password provided OR log in with Facebook OR create a guest account.

Username:

Password:

Sign On

OR

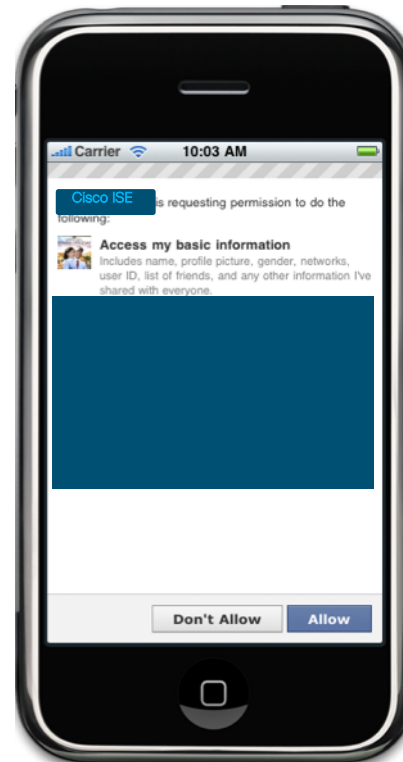
 **Log in With Facebook**

[Don't have an account?](#)

Phase 1 will include Facebook ONLY!!!

Доступ в первый раз

При первом заходе пользователь должен разрешить ISE получать базовые данные из Facebook



Информация в логах

Facebook Имя и идентификатор в Социальной сети

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repeat ...	Identity
Jun 07, 2017 08:09:55.852 PM	✓			jason kunst
Jun 07, 2017 08:00:37.018 PM	✓			tme ise
Jun 07, 2017 07:42:57.327 PM	✓			jason kunst

Identity

Authentication Identity Store FacebookISEApp

Authentication Method PAP_ASCII

Authentication Protocol PAP_ASCII

Other Attributes

ConfigVersionId 79

SocialMediaIdentifier https://www.facebook.com/10213161358285391

IpAddress 10.1.100.6

PortalName Self-Registered Guest Portal (default)

PsnHostName ise-1.demo.local

GuestUserName jason kunst

Улучшения в Policy UI

Пример групп политик – ISE 2.2

Policy Sets

Search policy names & descriptions.



- Summary of Policies**
A list of all your policies
 - Global Exceptions**
Rules across entire deployment
 - Oracle-test**
 - CiscoIT_Posture_POC**
 - CiscoIT_Posture_POC_copy**
 - IT Labs**
Posture-MDM Validation
 - Building_SJCN_Wireless_Wired**
NMTG
 - NMTG_3850**
 - Building_SJCM1_Wireless_LWA**
 - Bldg_SJC19_Wireless_Floors2and4**
SJC19 Wireless Access
 - Bldg_SJC19_Wireless_Floors1and3**
SJC19 Wireless Access
- Save Order Reset Order

Access Policy Sets

Summary of the defined policy sets
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description	Conditions
<input checked="" type="checkbox"/>	Oracle-test		Radius:User-Name EQUALS oracle OR Radius:User-Name EQUALS oracle1
<input checked="" type="checkbox"/>	CiscoIT_Posture_POC		NAS_WLC_BDLK OR NAS_WLC_LWR OR NAS_WLC_CSV OR NAS_WLC_STLD1_1 OR NAS_WLC_STLD1_2 OR NAS_WLC_AST_1 OR NAS_WLC_AST_2 OR NAS_WLC_SCJ12 OR NAS_WLC_RTP1
<input type="checkbox"/>	CiscoIT_Posture_POC_copy		Radius:User-Name EQUALS vishirem
<input type="checkbox"/>	IT Labs	Posture-MDM Validation	Radius:NAS-IP-Address EQUALS 10.51.59.5
<input checked="" type="checkbox"/>	Building_SJCN_Wireless_Wired	NMTG	DEVICE:Location EQUALS Location#All Locations#SJC#SJCN1
<input type="checkbox"/>	NMTG_3850		Network Access:Device IP Address EQUALS 172.23.208.121
<input type="checkbox"/>	Building_SJCM1_Wireless_LWA		Radius:Called-Station-ID MATCHES ^.*alpha-lwa\$ AND DEVICE:Location EQUALS Location#All Locations#SJC#SJCM1
<input checked="" type="checkbox"/>	Bldg_SJC19_Wireless_Floors2and4	SJC19 Wireless Access	Wireless_802.1X AND DEVICE:Device Type EQUALS Device Type#All Device Types#Wireless#WLC AND DEVICE:Location EQUALS Location#All Locations#SJC#SJC19#Floors2and4
<input checked="" type="checkbox"/>	Bldg_SJC19_Wireless_Floors1and3	SJC19 Wireless Access	Wireless_802.1X AND DEVICE:Device Type EQUALS Device Type#All Device Types#Wireless#WLC AND DEVICE:Location EQUALS Location#All Locations#SJC#SJC19#Floors1and3

Улучшенный вид – Пример групп политик – ISE 2.3

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	Oracle-test_Default		OR Radius-UserName EQUALS oracle Radius-UserName EQUALS oracle1		0		
	CiscoIT_Posture_POC_Dot1X		AND OR NAS_WLC_BDLK NAS_WLC_LWR NAS_WLC_CSV NAS_WLC_STLD1_1 NAS_WLC_STLD1_2 NAS_WLC_AST_1 NAS_WLC_AST_2 NAS_WLC_SCJ12 NAS_WLC_RTP1 Wireless_802.1X		0		
	CiscoIT_Posture_POC_Default		OR NAS_WLC_BDLK NAS_WLC_LWR NAS_WLC_CSV NAS_WLC_STLD1_1 NAS_WLC_STLD1_2 NAS_WLC_AST_1 NAS_WLC_AST_2		0		

Количество сессий

Reset Save

Переход

- Insert new row above
- Insert new row below
- Duplicate above
- Duplicate below
- Copy rules to this set
- Delete

Добавить policy sets

Логические операторы

Обзор Групп Политик

Policy Sets → Set view

Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	CiscoIT_Posture_POC_Dot1X		AND OR NAS_WLC_BDLK NAS_WLC_LWR NAS_WLC_CSV NAS_WLC_STLD1_1 NAS_WLC_STLD1_2 NAS_WLC_AST_1 NAS_WLC_AST_2 NAS_WLC_SCJ12 NAS_WLC_RTP1 Wireless_802.1X	802.1X	0

- Authentication Policy (1)
- Authorization Policy Global Exceptions (7)
- Authorization Policy Local Exceptions
- Authorization Policy (4)

Студия формирования условий

Добавить атрибуты

Категории

Conditions Studio

Library

Поиск

Search by Name



- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed
- Non_Cisco_Profiling_Phones
- Non_Compliant_Devices
- Switch_Local_Web_Authentication
- Switch_Web_Authentication
- Wired_802.1X
- Wired_MAB
- Wireless_802.1X

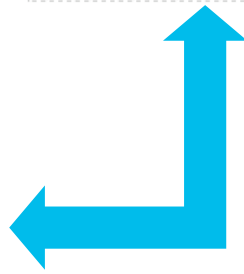
Editor

Click to add an attribute

Equals Attribute value

Drag & Drop

+ AND OR



Преднастроенный список

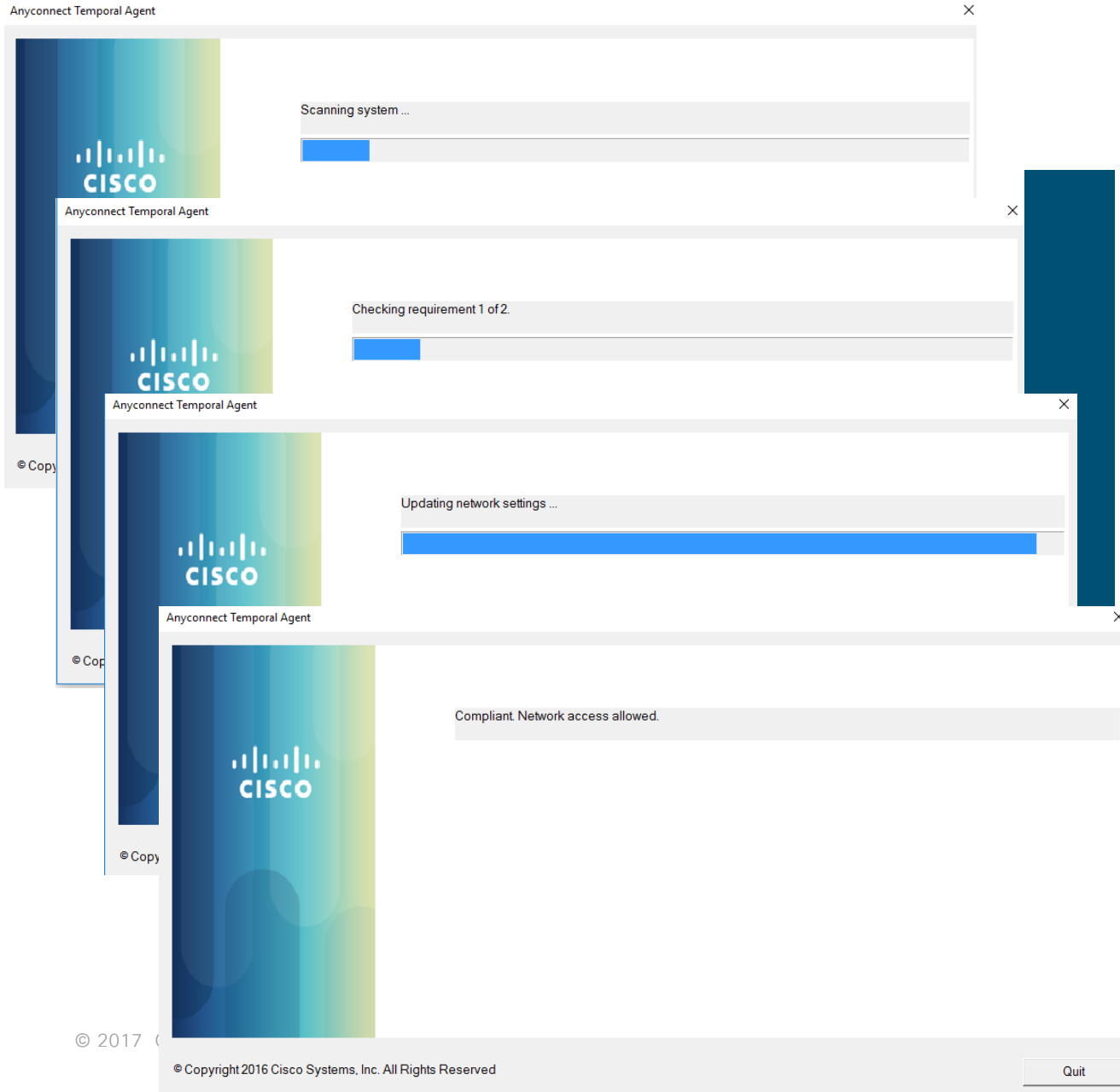
Составление условий политики

The screenshot displays the 'Conditions Studio' application. On the left is the 'Library' pane with a search bar and a list of conditions including IP addresses, AD objects, and device types. The main 'Editor' pane shows a visual rule builder with two conditions: 'WLC_SJC19_Alpha' and 'WLAN_ID_1'. A third condition is being built: 'CiscoAD-manager' with a 'Conta' dropdown set to 'jsmith'. Below this, a 'Network Access-Protocol' condition is being configured with the operator 'Equals' and the value 'RADIUS'. Logical operators 'AND' and 'OR' are visible between the conditions. At the bottom right are 'Close' and 'Use' buttons.

1. Добавление атрибутов
2. Создание условий с операторами (AND или OR)
3. Создание условий по необходимости с комбинациями AND/OR.

Улучшения в оценке СОСТОЯНИЯ

Temporal Agent (ISE 2.3)



Детали

- Замена NAC Web Agent (только Windows) на временный Windows/exe и Mac OS/dmg
- Запускается один раз и удаляется
- Не требует административных привилегий
- Такой же богатый набор проверок что и AnyConnect (также с инвентаризацией ПО, но однократно)
- Только ручное исправление состояния
- Загружается с портала через URL перенаправление, возможно интегрировать с Guest, BYOD, CWA, etc.

Видимость установленных приложений

The screenshot displays the Cisco Identity Services Engine (ISE) interface. At the top, there is a navigation bar with tabs for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below this, there are sub-tabs for Endpoints, Users, Network Devices, and Application. The main content area shows details for an endpoint with MAC address 00:00:00:00:00:E4. A metadata box lists: MAC Address: 00:00:00:00:00:E4, Username: autouserwin7, Endpoint Profile: Microsoft-Workstation, Current IP Address: 19.9.10.124, and Location: Location → All Locations. Below this, there are tabs for Applications, Attributes, Authentication, Threats, and Vulnerabilities. The 'Applications' tab is active, showing a table of installed applications. The table has columns for Application Name, Version, Vendor, Running process, Category, and Install Path. A 'Refresh' button and a 'Policy Actions' dropdown are visible at the top left of the table. A 'Filter' dropdown is at the top right.

Application Name	Version	Vendor	Running process	Category	Install Path
Gatekeeper	9.9.5	Apple Inc.		AntMalware	/System/Library/Prefere...
Cisco AnyConnect Secure Mobil...	3.4.01054	Cisco Systems, Inc.	1	VPNClient	/Applications/Cisco/Cis...
FileVault	9.9.5	Apple Inc.		DiskEncryption	/System/Library/Prefere...
Software Update	2.3	Apple Inc.		PatchManagement	/Applications/App Store...
vpndownloader	3.4.01054	__MyCompanyName__, 2006		Unclassified	/opt/cisco/anyconnect/b...
Firefox	49.0	Mozilla Corporation	2	AntPhishing_Browser	/Applications/Firefox.app
Mac OS X Built-in Firewall	9.9.5	Apple Inc.		FireWall	/System/Library/Prefere...
Messages	7.0	Apple Inc.	1	InstantMessenger	/Applications/Message...
iCloud	5.0	Apple Inc.		CloudStorage	/System/Library/Prefere...
Time Machine	2.3	Apple Inc.		BackupClient	/Applications/Time Mac...
Adobe Flash Player	17.0.0.194	Adobe Systems Inc.		Unclassified	/Applications/Utilities/Ad...
QuickTime Player	9.3	Apple Inc.		Unclassified	/Applications/QuickTim...
Safari	8.1.3	Apple Inc.		AntPhishing_Browser	/Applications/Safari.app

Новая инвентаризация приложений в ISE 2.3

Новый Summary вид внутри Context Directory

Наведите

Множественный выбор

Улучшенная фильтрация

The screenshot displays the Cisco Identity Services Engine (ISE) 2.3 interface. The top navigation bar includes 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area is titled 'APPLICATION CATEGORIES' and features a bar chart showing application counts. A tooltip for 'Messenger' indicates '3 applications' and '8 endpoints'. Below the chart, there are tabs for 'All applications', 'Windows', and 'Mac OSX', and a 'Summary' view. A table lists application categories with columns for 'Application name', 'Version', 'Vendor', 'Category', and 'Endpoints with this software'. A filter is applied to the table, showing results for 'filevault', 'gatekeeper', and 'mac os x builtin firewall'. A blue arrow points to the 'Summary' view, and another blue arrow points to the 'Multiple selection' feature in the table.

Application name	Version	Vendor	Category	Endpoints with this software
filevault	9.9.5	Apple Inc.	DiskEncryption	5
gatekeeper	9.9.5	Apple Inc.	AntiMalware	5
mac os x builtin firewall	9.9.5	Apple Inc.	FireWall	5

Новая аппаратная инвентаризация в ISE 2.3

The screenshot displays the Cisco Identity Services Engine (ISE) 2.3 interface for hardware inventory. The main content area is divided into two sections: 'MANUFACTURERS' and 'ENDPOINT UTILIZATIONS'. The 'MANUFACTURERS' section shows two donut charts: one for 'hewlett-packard' (50%) and 'apple, inc.' (50%), and another for 'cpu' (50%) and 'total' (50%). The 'ENDPOINT UTILIZATIONS' section has tabs for 'CPU', 'Memory', and 'HD', with a filter for 'Devices with over [] % CPU usage'. Below these is a table of endpoint data with columns for MAC Address, Manufacture, Model, Serial Number, Attached devices, CPU Name, CPU Type, CPU Speed (GHz), CPU Usage (%), and Number of devices. The table shows two rows of data: one for a Hewlett-Packard HP 620 and one for an Apple Macmini6,1. The interface also includes a 'Column order' sidebar on the right with a list of columns and checkboxes for selection. Annotations in Russian highlight specific features: 'Богатый контекст' (Rich context) points to the table columns, 'Фильтры загрузки' (Load filters) points to the CPU usage filter, and 'Фильтр по производителям' (Filter by manufacturer) points to the donut charts.

Богатый контекст

Фильтры загрузки

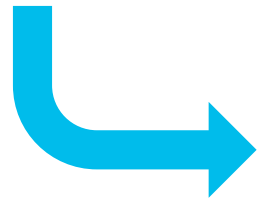
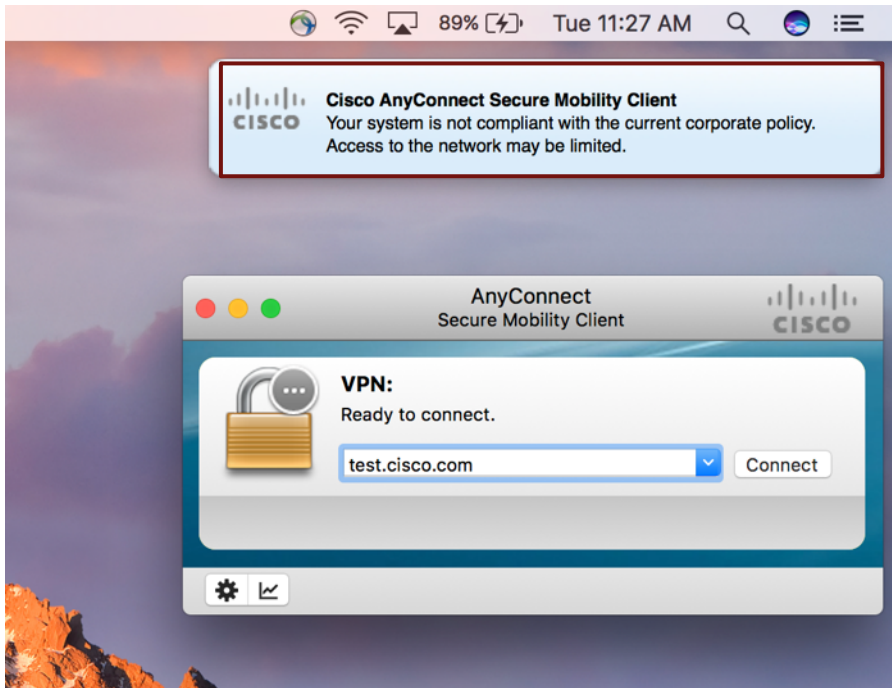
Фильтр по производителям

MAC Address	Manufacture	Model	Serial Number	Attached devices	CPU Name	CPU Type	CPU Speed (GHz)	CPU Usage (%)	Number
70:F1:A1:E5:C2:15	Hewlett-Packard	HP 620	CNU03119WM	5	Intel(R) Core(TM)2 Duo CPU T6...		2.101000		2
A8:86:DD:A7:AA:71	Apple, Inc.	Macmini6,1	C07M2BMNDWYL	7	Intel Core i5		2.500000	15.033408	2

Гибкие настройки уведомлений

Детали

- ✓ Использование системных уведомлений Windows и Mac OS
- ✓ Фокус на проблемах политик и ошибках связи
- ✓ Режимы агента (Full, Stealth, Stealth with Notification)



Agent Behavior

Parameter	Value	Notes
Enable debug log	No	
Operate on non-802.1X wireless	No	
Enable signature check	No	OSX: N/A
Log file size	5 MB	
Remediation timer	4 mins	The default global setting is
Agent Mode	Full	



Advanced Threat

AMP – ВЫШЛО В 2017

- Command line capture
- Переделанный Dashboard
- Поддержка SAML
- Advanced Custom Detections для Mac и Linux Connectors
- Расширение поддержки Linux
- Поддержка инкрементальных обновлений сигнатур
- PCI compliance



Вышло в 2017 – Threat Grid

- Windows 10 поддержка
- Meraki MX интеграция
- Single Sign-on – AMP / TG
- Отслеживание источника отправки
- Sample packs

AMP

Расширенные возможности обнаружения

- Новый механизм эвристики
Детектирование и блокирование ИОС на Endpoints в режиме реального времени
Windows Connector 6.0.x
- Защита от эксплоитов
Windows Connector 6.0.x
- Бета доступна для всех пользователей (в том числе и POV)

AMP Everywhere AMP Unity



Blacklist



AMP for Endpoints
Console

