CISCO UMBRELLA FAQ

Последнее обновление: 23 Января 2018 г.

1. **Почему время отклика Вашего сервиса на порядок больше родных провайдерских и публичных альтернатив? В среднем XXмс против 3мс.**

   Время отклика DNS Umbrella будет ожидаемо выше чем у локального провайдера, поскольку локального хостинга центров обработки данных в РФ у Umbrella пока нет, тем не менее ЦОДы Umbrella по всему миру имеют прямой пиринг с более чем 500+ провайдерами и располагаются на основных точках обмена трафика, чтобы гарантировать предсказуемое время отклика и 100% доступность по кратчайшему возможному маршруту, используя ANYCAST для анонсирования маршрута до своих DNS 208.67.222.222 и 208.67.222.220.

2. **Каковы модели использования сервиса, в чем их преимущество от бесплатных OpenDNS?**

   Модели использования сервиса предполагают:

   a. Защита инфраструктуры при обращении к внешним ресурсам с интеграцией в инфраструктуру как внешний DNSForwarder;
   b. Возможность установки виртуальной машины OpenDNS, что даст возможность писать политики полагаясь на внутренние адреса (private address space) кампусной сети
   c. Возможность установки виртуальной машины OpenDNS с последующей интеграцией в AD, что даст возможность писать политики фильтрации оперируя членством в группах AD и именами пользователей
   d. Защита оконечных пользователей, покидающих периметр корпоративной сети (мобильные сотрудники, командировки и тд), агент, установленный на ПК будет продолжать защищать пользователя даже при отсутствии VPN соединения в центральный офис.
   e. Фильтрация запросов на базе категорий URL;
   f. Фильтрация запросов по различным категориям вредоносных запросов;
   g. Интеграция с корпоративными средствами защиты через готовые или интегрируемые API интерфейсы для возможность централизованной блокировки вредоносных запросов по результатам обнаружения внутри сторонних средств защиты.
   h. Единая политика фильтрации, логирования, отчетности на всех офисах, узлах сети и мобильных пользователях.
   i. Защита по динамическим IP черным спискам, выгружаемым на сторону хостового клиента с опцией туннелирования и инспекции трафика.
   j. Возможность контентной фильтрации через механизм Intelligent Proxy с проверкой антивирусными движками и средствами защиты от вредоносного кода Cisco AMP передаваемых файлов, от ресурсов, которые нельзя однозначно определить в BlackList.
   k. Возможность интеграции в WLC (Беспроводные контроллеры Cisco) и маршрутизаторы серии ISR4k с Umbrella через готовый встроенный

коннектор, который автоматически будет перенаправлять запросы в облако Umbrella и через API интегрируется с Вашим аккаунтом.

l. Возможность расследования инцидентов и получения централизованного источника информации по инфраструктуре, контекстным данным, историческим изменениям активности, эволюцию и взаимосвязи доменов, IP, сетей, связанных запросов, активностям malware по запрашиваемым доменам и IP адресам через инструментарий Investigate.

m. В бесплатной версии Вы получаете самую базовую защиту от вредоносных категорий и фильтрацию по категориям сайтов, защита только на уровне DNS без какой-либо отчетности и мониторинга.

3. **Как лицензируются подписки, и сколько это стоит?**

a. Лицензирование идет по подписке и по соответствующему пакету функционала:

Umbrella опции заказа

		Branch	Roaming	Wireless LAN	Professional	Insights	Platform
		Работает с специфичными решениями Cisco и интеграцией, ограниченный функционал			Работает самостоятельно и в интеграции с Cisco		
Покрытие	On-Network (Любое устройство)	(ISR только)		(LAN только)	✓	✓	✓
	Off-Network (Ноутбуки)		✓		✓	✓	✓
Детальность политик и отчетности	По сети и хосту	(Сеть только)	(Только Хост)	(Сеть только)	✓	✓	✓
	По подсети и пользователю					✓	✓
Фильтрация глубина и покрытие	DNS Layer (domains+IPs)	✓	✓	✓	✓	✓	✓
	IPv4 Layer (non-DNS IPs)					✓	✓
	Proxy (security+IWF URLs)	(IWF только)		✓		✓	✓
	API-Based Integrations						✓
Видимость и интеллект угроз	Basic Logging & Reports	✓	✓	✓	✓	✓	✓
	Advanced Reporting					✓	✓
	Log Management via S3					✓	✓
	Investigate Console						✓

b. Umbrella состоит из трех основных типов подписки: **Professional/Insight/Platform**, все они дают защиту от угроз Интернета в любых сайтах развертывания, для устройств и мобильных хостов с подключенным и отключенным VPN.

c. Помимо основных подписок есть еще подписки начального уровня: **Roaming/Branch/Wireless LAN**, которые рассчитаны на продажу совместно с соответствующим оборудованием Cisco и позволяют проихводить их интеграцию в облако Umbrella.

d. Стоит отметить, что пользователи приобретающие основные подписки могут использовать и подписки начального уровня для интеграции устройств Cisco.

e. Также если Вы выбираете опции защиты оконечных хостов с установкой агента Umbrella, являющегося модулем Cisco AnyConnect клиента, то необходимо включить в заказ лицензии на агент AnyConnect по количеству устройств.

i. **Roaming** – дает возможность установки клиента Umbrella или модуля Anyconnect Umbrella на хостовую машину и его использование как мобильного агента.
ii. **Branch** – дает возможность интеграции Umbrella с ISR4k маршрутизаторами.
iii. **Wireless LAN** – дает возможность интеграции с контроллерами БЛВС Cisco 2504, 5508, 5520, 8510 и 8540, а также с Wireless Services Module 2 (WiSM2)

f. Опционально можно докупать пакет **Investigate Console** для получения доступа к консоли расследования инцидентов Investigate, а также пакет **Investigate API** для доступа к программному интерфейсу Investigate базы для интеграции с SIEM и другой автоматизации. Лицензируется Investigate по количеству получающих к нему на доступ пользователей, а для API по количеству запросов.
g. Лицензирование ведется по подписке, каждый заказчик имеет одну подписку, куда может входить необходимое количество лицензий. Подписка существует на 12 месяцев или на 3 года.
h. Лицензирование основано на двух моделях:
    i. **по количеству пользователей:**
        1. Пакеты **Cisco Umbrella Professional, Insights, Platform,** и **Roaming** лицензируются по количеству пользователей (рабочих мест). Рабочее место определяется как уникальное рабочее место имеющее подключение к Интернет. В лицензию Roaming, как и другие лицензии Umbrella не входит лицензирование самого агента AnyConnect.
    ii. **по количеству устройств:**
        1. Пакет **Branch** лицензируется по количеству маршрутизаторов ISR4k и не зависит от количества защищаемых устройств. Поддерживаются модели ISR4k: 4221, 4321, 4331, 4351, 4431 и 4451.
        2. Пакет **Wireless LAN** лицензируется по количеству точек доступа и не зависит от количества защищаемых пользователей

i. Также можно свести в таблицу вводные по лицензированию:

Table 5. Cisco Umbrella Licensing Summary

Licensing Model Element	Professional / Insights / Roaming	Platform	Branch / WLAN
License type	Subscription	Subscription	Subscription
Licensing unit	Seat	Seat	Device
Minimum units	10 seats	500 seats	1
Licensing terms	12- or 36-month	12- or 36-month	12- or 36-month
Renewal terms	12 months	12 months	12 months
Renewal type	Automatic renewal	Automatic renewal	Automatic renewal
Support model	Basic Support included; Premium Support available for purchase	Basic Support included; Premium Support available for purchase	Basic Support included; Premium Support available for purchase
Endpoint client	Umbrella endpoint footprint for Windows and Mac OS X. AnyConnect licenses must be purchased separately	Umbrella endpoint footprint for Windows and Mac OS X. AnyConnect licenses must be purchased separately	-

Table 6. Cisco Umbrella Investigate Licensing Summary

Licensing Model Element	Investigate Console	Investigate API
License type	Subscription	Subscription
Licensing unit	User	API license
Minimum units	3	1
Licensing terms	12- or 36-month	12- or 36-month
Renewal terms	12 months	12 months
Renewal type	Automatic renewal	Automatic renewal
Support model	Basic Support included; Premium Support available for purchase	Basic Support included; Premium Support available for purchase
Endpoint client	-	-

Вам просто нужно выбрать интересующий пакет лицензирования и количество пользователей (или устройств по соответствующим подпискам), время контракта 12 или 36 месяцев.

4. **Какие существуют методы защиты настроек от обхода серверов через файлы hosts, локальные политики, запросы к альтернативным DNS?**

    a. При защите инфраструктуры, то есть пользователей внутри кампуса существует несколько методик.
        i. GPO с защитой доступа к смене настроек сетевого интерфейса;
        ii. Отсутствие прав локального админа у пользователей для редактирования системных файлов типа hosts. (это в принципе хорошая практика, крайне рекомендуемая)
        iii. Закрыть на МСЭ для внутренних сетей доступ к сторонним DNS; (самое очевидное)
    b. При защите мобильных хостов, работают как два первых совета предыдущего пункта, так и мобильный клиент AnyConnect работает на уровне ядра ОС и перехватывает все DNS запросы на уровне ядра.

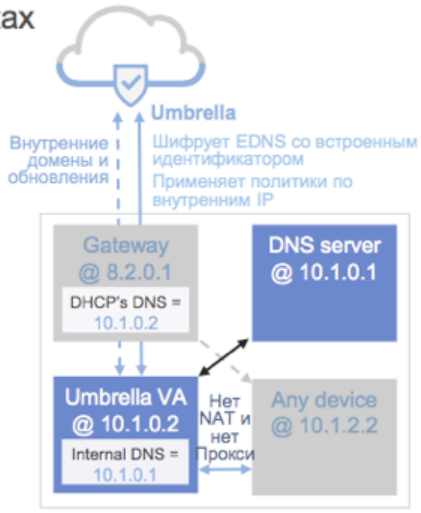
5. **Какова глубина детализации статистики? Сейчас видно только наши внешние адреса. Возможно ли углубиться до хоста, сделавшего данный запрос?**

    a. для этого нужно установить виртуальную машину Umbrella и использовать её/их (поставить две для отказоустойчивости) для разрешения имен локальными службами и пользователями, локальные запросы на внутренние домены будут пересылаться на локальный корпоративный DNS, а внешние в облако Umbrella.
    b. Следующие иллюстрации на тему:

Защита внутри сети

Umbrella Virtual Appliance – Для локаций требующих использования внутренних IP в политиках

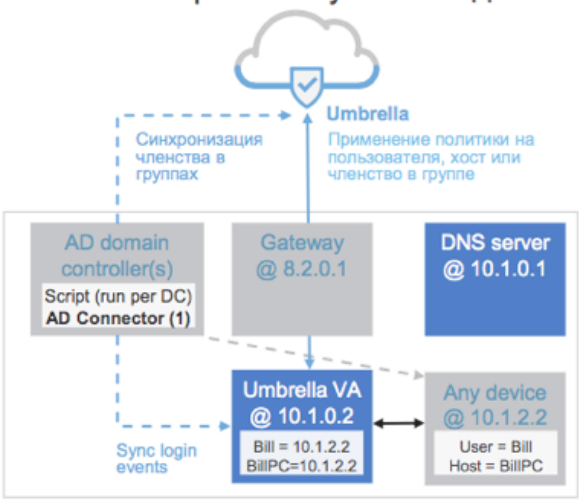
- Поддерживается для VMware и Hyper-V
- Внутренние/Внешние запросы отсылаются в VA
- Внутренние запросы разрешаются локально
- VA упаковывает внутренний IP с использованием RFC-совместимого расширения в DNS



Защита внутри сети

Virtual Appliance + AD Connector – Для детального контроля и глубокой видимости

- Домен-Контроллеры регистрируются на Umbrella
- Сервис коннектора устанавливается на DC/Контроллере:
  1. Синхронизирует членство в группах пользователей и компьютеров в Umbrella
  2. Отсылает соответствие IP->USER на Виртуальные Аплаенсы
- Виртуальный Аплаенс инкапсулирует уникальные идентификаторы, которые Umbrella использует в политиках и отчетах



6. **В TOP Domains появились наши внутренние адреса, почему они форвардятся наружу? Это означает, что клиент не получит правильного адреса?**

   Если Вы указывали Umbrella DNS как Forwarder на Вашем внутреннем DNS сервере, то Ваш DNS отсылает на разрешение имен только внешние запросы, иначе я бы проверил настройку корпоративного DNS сервера, настройку делегирования и зон.

7. **Каким образом и как быстро добавляются Black/White листы?**

   a. - Black/White списки добавляются в разделе политики (**Policies->Policy List-><Имя Вашей политики>)** в разделе Destination Listsможете модифицировать **Global Allow** и **Global Block list**, также можете составлять свои списки.
   b. Белые списки имеют приоритет над всеми другими категориями и туда можно включать ресурсы, которые как Вам кажется ошибочно попали в вредоносную категорию, соответственно добавив ресурс к белому списку Вы восстановите доступ

к ресурсу пока TAC рассматривает заявку на изменение его статуса, без создания проблем для бизнеса.

c. На моем опыте работа списков начинается мгновенно после сохранения измененной политики. (Кэш браузера надо очистить, поскольку продолжает выдавать закэшированный ответ на блокировку. Другой браузер мгновенно открывает страницу.

8. **По поводу отклика, хотелось бы понимать перспективы появления узлов доступа в РФ, в частности в Москве.**

   На текущий момент мы изучаем возможность развертывания инфраструктуры OpenDNS на территории РФ.

9. **На первом этапе мы настроили ForwardDNS, если я правильно понял таблицу, то это Professional подписка, не очень понятно как в таком случае считаются пользователи?**

   Вариант развертывания типа ForwardDNS может быть использован для любого и трех типов корневых подписок Professional, Insights или Platform, разница в том какой набор защитных средств и средств расследования/анализа Вам доступен в зависимости от используемого пакета.
   Umbrella Professional – предоставляет защиту против Malware, Фишинга, вызовов на Command and Control сервера для пользователей находящихся как внутри сети, так и за её пределами, в дополнение к WEB фильтрации и отчетности.
   Umbrella Insights – предоставляет все сервисы пакета Professional и дополнительно включает возможность использования политик защиты с детализацией по пользователям благодаря интеграции с Microsoft Active Directory, фильтрацию URL и IP-уровня, собственные списки фильтрации URL, инспекция файлов на вредоносный контент с использованием Cisco AMP и других антивирусных движков, возможность сохранения логов и расширенная отчетность. Также доступна аналитика использования облачных приложений.
   Umbrella Platform - предоставляет все сервисы пакета Insights и дополнительно включает уже преднастроенные и настраиваемые API механизмы интеграции. Также становится доступна консоль расследования Investigate для 50-для 50-ти рабочих мест операторов, предоставляющих более глубокий контекст для расследования.
   Если рассматривать модель работы из-за NAT, то система полагается на корректность расчета количества пользователей Интернет произведенных оконечным заказчиком, корректность подсчетов в данной модели не проверяется.

10. **В таблице лицензирования для лицензии Insights заявляется фильтрация на уровне IPv4 как она реализована, если мы ограничиваемся только настройкойDNS серверов (не считая разъездных пользователей с AnyConnect?)**

    Фильтрация на базе IP-фильтрации может проводиться через динамически загружаемые IP-фильтры для Umbrella Roaming Client, доступно для платформ MAC и WINDOWS.
    Несколько тысяч IP адресов блок-листа динамически загружаются в агент, установленный на ПК и трафик, адресуемый на данные IP автоматически туннелируется через IPSEC в облако OPENDNS для инспекции либо блокировки при необходимости.
    Для работы функции должны быть открыты следующие порты/протоколы на МСЭ:

a. Protocol 50 (ESP)
b. Protocol 51 (AH)
c. UDP Port 500
d. UDP Port 4500

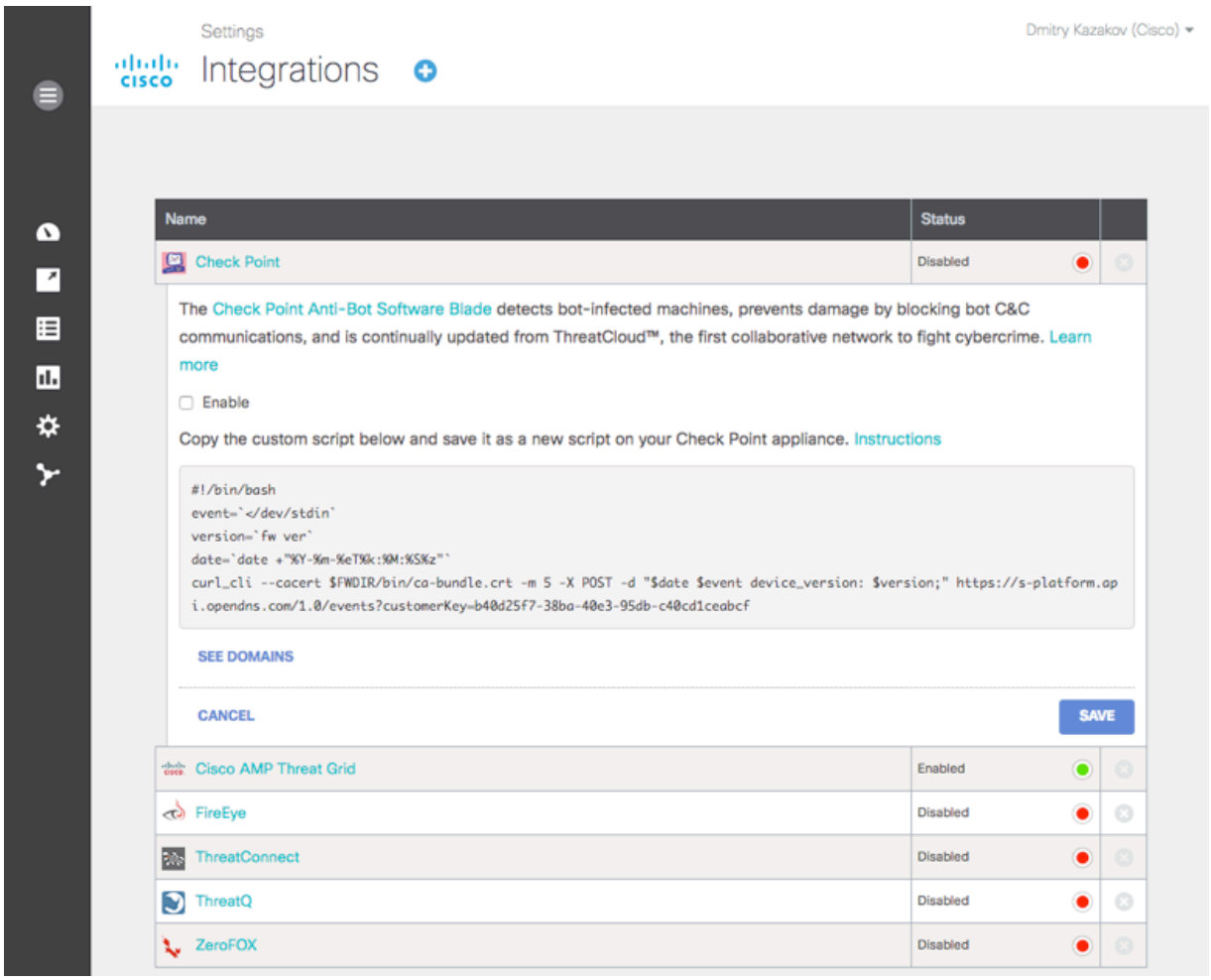
Проверить работает ли активно функция на конкретном ПК можно по ссылке http://ipblock.opendnstest.com/
Если Вы ограничиваетесь настройкой DNS серверов, то IP Enforcement не работает.

11. **Касаемо подписок, хотелось бы немного более подробно понять отличия Между Professional и Insights. (Помимо вышеприведенной таблицы). Так же хотелось бы понять, каким образом осуществляется расширение пакета, в случае появления новых пользователей. (Подписка добавляется к текущему годовому/трехгодовому контракту, или делается новый?) В случае исчерпания «лицензий», каково поведение для новых/текущих пользователей? Не получится ли произвольных блокировок DNS запросов?**

    Описание пакетов я привел в пункте (2), расширение подписок проводится в рамках имеющейся подсписки *(один заказчик = одна подписка)*. Произвольных блокировок не будет. Изменение подписки в процессе её действия происходит по установленному процессу Change-Subscription. Изменения, вносимые в подписку, могут касаться как продуктов, так и количественных характеристик. Срок действия добавленных позиций к подписке будет истекать одновременно с основной подпиской. При планировании появления новых пользователей также проводится заказ позиций изменения подписки и добавляется необходимое количество пользователей.

12. **Хотелось бы более подробно узнать об интеграции с сторонними системами контроля доступа (Checkpoint в частности). Это Investigate API, или такая интеграция доступна в рамках основного пакета?**

    Для интеграции с сторонними продуктами Umbrella используется API, не путайте с API для Investigate. Данная функция доступна в панели меню Settings->Integrations, для Checkpoint уже есть готовый модуль интеграции, подробные инструкции по ссылке (https://support.umbrella.com/hc/en-us/articles/231248788):



13. **Какие уровни сервисной поддержки есть у Umbrella, сервис DNS очень критичен.**

Хочу отметить что уровни поддержки имеются трех типов Базовая/Золотая/Платиновая. Золотая и Платиновая относятся к Premium классификации.

a. В **Базовую (Basic)** входит доступ к поддержке в по электронной почте, доступ к онлайн ресурсам база знаний/форумы/документация/портал заведения кейсов и уведомления.
b. В **Золотую (Gold)** входит:
    i. 24x7 доступ по телефону для кейсов уровня P1 (отказ/недоступность сервиса) время реакции 30 минут (2 часа для Basic поддержки);
    ii. 24x5 доступ по телефону для кейсов уровня P2 (техническая проблема – время реакции 1 день) и P3 (Информационные запросы – время реакции 2 дня);
    iii. Доступ к онлайн ресурсам база знаний/форумы/документация/портал заведения кейсов и уведомления.
c. В **Платиновую (Platinum)** входит:
    i. Выделенный технический аккаунт менеджер (TAM);
    ii. 24x7 доступ по телефону для кейсов уровня P1 (отказ/недоступность сервиса) время реакции 30 минут (2 часа для Basic поддержки);
    iii. 24x5 доступ по телефону для кейсов уровня P2 (техническая проблема – время реакции 1 день) и P3 (Информационные запросы – время реакции 2 дня);

iv. Доступ к онлайн ресурсам база знаний/форумы/документация/портал заведения кейсов и уведомления.

14. **Мне пришла ссылка на активацию триальной версии Umbrella, что делать дальше: Вам уже пришло письмо с активацией аккаунта Umbrella на 60 дней.**

    После того как Вы зайдете и установите пароль учетной записи проследовав по соответствующей ссылке в письме, я предлагаю Вам пройтись по краткой видео-инструкции (5 минут), которую я снял для того чтобы Вы могли быстро запустить в работу данное решение: http://www.youtube.com/watch?v=lILRHsKpY5U

    Инструкция для прописывания DNSForwarder доступна по ссылке: https://www.cisco.com/c/dam/en/us/td/docs/security/opendns/opendns-solution-guide-isr-g2.pdf

15. **Я вижу в списках активностей домены наших контрагентов, помеченные как Newly Seen, хотя они зарегистрированы много лет, корректно ли такое поведение Umbrella?**

    Отдельно по категории **Newly Seen Domains** это категория безопасности, которая идентифицирует домены, которые запрашивались впервые за последние несколько дней.
    Когда домен впервые видится пользователем Umbrella, домен помечается как «Newly Seen» для всех последующих пользователей на последующие несколько дней.

    С данной категорией работают соответствующие алгоритмы аналитики, призванные свести к минимуму количество возможных FalsePositives. Категория призвана бороться с угрозами, связанными с DGA инфраструктурой и фишинговыми компаниями (содержащими лексические изменения в именах доменах популярных компаний).

    Newly Seen Domains это категория безопасности, которая работает путем проверки DNS логов на наличие запросов к данному домену в прошлом. Мы фиксируем запрос от клиента, проверяем резолвится ли имя на адрес и помечаем это имя как «Newly Seen» если оно является новым для наших DNS lookup. В некоторых случаях домен не будет резолвиться, но будет опрашиваться Malware на проверку наличия нового появившегося контента. Данная категория “Newly Seen Domains” помогает бороться с таковыми активностями по заранее «зашитым» доменам в Malware.

    Как только домен попадает в категорию «Newly Seen Domains» **он попадает в список, в котором его членство со временем истекает и он уже больше не будет категоризоваться как «Newly Seen Domains»**. Время истечения пребывания домена в данном списке зависит от характеристик домена верхнего уровня и поддоменов, инфраструктуры и её репутационных составляющих (некоторые инфраструктуры часто хостят Malware), другие же известны как надежные поставщики CDN. Хорошие поставщики будут уходить из списка значительно быстрее.
    Обычно домены находятся в данном списке от одного до трех дней.

    По умолчанию сайты категории Newly Seen Domains **не блокируются**.

Отдельно хочу отметить, что как только домен пропадает из списка Newly Seen в консолях Investigate и Activity Search пропадает соответствующая категоризация.
Мы понимаем, что значительная часть доменов категории “Newly Seen Domains” будет хостить абсолютно легитимное содержимое, поэтому для хорошо известных сетей раздачи контента CDN, таких как например AKAMAI, Facebook, CloudFront которые генерируют случайные субдомены для обслуживания контента делаются исключения.