Cisco Umbrella

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Cisco Umbrella: пакет Insights

Защита от интернет-угроз независимо от местонахождения пользователей

Блокирование угроз до того, как они проникнут в вашу сеть или на оконечные устройства

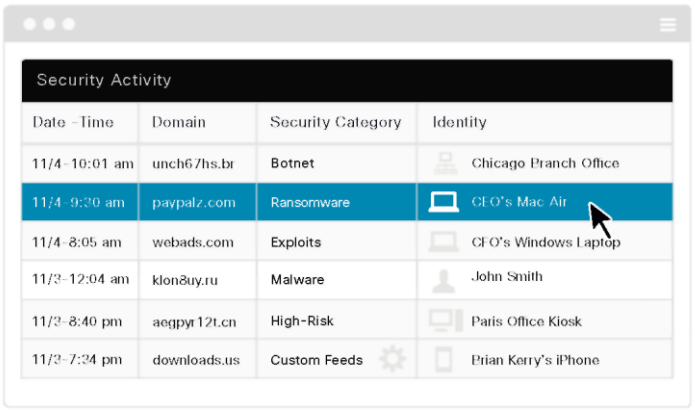
Первая линия обороны от угроз

Cisco Umbrella – это облачная платформа обеспечения безопасности непосредственно из Интернета. Применяя политики безопасности на уровнях DNS и IP, Umbrella блокирует запросы к вредоносным и нежелательным узлам до того, как будет установлено соединение. Это позволяет нейтрализовать угрозы на любом порте и с использованием любого протокола прежде, чем они проникнут в сеть или на оконечные устройства.

Всеобъемлющий мониторинг и защита

Облачный сервис Umbrella обеспечивает мониторинг, необходимый для защищенного доступа к Интернету всех сетевых устройств, офисов и пользователей в роуминге. Все операции в Интернете записываются в журнал и делятся на категории по типу угрозы безопасности или веб-контента, а также по типу выполненного действия (блокирование или разрешение). Эти журналы хранятся настолько долго, насколько это необходимо, и ими легко можно воспользоваться для проведения расследования. Вы можете даже узнать об облачных приложениях и устройствах Интернета вещей (IoT), которые используются в вашей компании.

Cisco Umbrella



Как это работает

Аналитика, позволяющая обнаружить атаки до их начала

Наша глобальная сетевая инфраструктура ежедневно обрабатывает свыше 100 млрд интернет-запросов. Благодаря этому мы получаем уникальную картину отношений между доменами, IP-адресами, сетями и вредоносными программами в Интернете. Подобно тому, как Amazon анализирует модели покупательского поведения для предложения следующего товара, мы изучаем шаблоны интернет-трафика и на их основе автоматически выявляем инфраструктуру злоумышленников, подготовленную для очередной атаки, а затем блокируем доступ пользователей к вредоносным узлам.

Развертывание во всей организации за считанные минуты

Umbrella – самый быстрый и простой способ обеспечить безопасность всех пользователей за считанные минуты. Типичные эксплуатационные сложности для этой мощной и эффективной системы безопасности совершенно не характерны. Все операции выполняются в облаке со стопроцентной отказоустойчивостью, поэтому не нужно устанавливать никакое оборудование и вручную обновлять программное обеспечение.

Преимущества решения Cisco Umbrella

- Сокращение количества заражений вредоносным ПО на 98%
- Снижение количества оповещений от системы предотвращения вторжений, антивирусных программ и системы управления событиями и данными безопасности (SIEM) на 50%
- Сокращение времени восстановления на 20%
- Защита внутри и вне корпоративной сети

Отличительные особенности Umbrella

- **Широчайшее покрытие** вредоносных узлов и файлов
- **Самая точная прогнозная** аналитика для нейтрализации угроз на ранних стадиях
- **Простейшее развертывание** с удобными способами подключения к нашей облачной платформе
- **Самая быстрая и надежная** облачная инфраструктура

Проблемы, которые мы решаем

82% пользователей обходят сеть VPN[1], а 70% филиалов имеют прямой доступ в Интернет[2]

Большинство мобильных и удаленных сотрудников не всегда используют VPN, и большинство филиалов не пропускают весь трафик через транзитную сеть, а следовательно, недостаточно защищены. Менее чем за 30 минут Umbrella может обеспечить глобальную защиту.

70–90% вредоносных программ уникальны для каждой организации[3]

Средства на основе сигнатур, аналитика угроз, обеспечивающая лишь реагирование на атаки, и изолированное применение политик безопасности – все это не позволяет опережать действия киберпреступников. Umbrella обнаруживает и изолирует вдвое больше скомпрометированных систем, чем раньше.

86% ИТ-менеджеров отмечают нехватку квалифицированных специалистов по безопасности[4]

Мы понимаем, что вы испытываете дефицит кадров и нуждаетесь в системе безопасности, которую можно будет легко установить, настроить и использовать. Решением Umbrella не только легко управлять – оно блокирует угрозы на ранней стадии и сокращает число заражений и оповещений, получаемых от других продуктов безопасности.

Сценарии использования

Предотвращение обратных вызовов командных серверов со стороны скомпрометированных систем через Интернет и по другим каналам

Применение и соблюдение политик допустимого использования с 60 категориями контента и вашими собственными списками

Ликвидация невидимой области DNS и бессрочное хранение журналов для более эффективного реагирования на инциденты и соблюдения политик

Передача трафика из сомнительных доменов на прокси-сервер для углубленного анализа URL-адресов и файлов с помощью антивирусных систем и Cisco AMP

Предотвращение скрытой загрузки вредоносного кода и попыток фишинговых атак со стороны вредоносных или мошеннических веб-сайтов

Мониторинг использования облачных сервисов (включая IoT-устройства)

Выявление скомпрометированных систем путем отслеживания событий безопасности в режиме реального времени и обнаружение целенаправленных атак с использованием глобального контекста

У вас множество децентрализованных или разрозненных подразделений?

- Предлагаем вам самое простое решение для централизованного управления безопасностью!
- Принципы его работы можно посмотреть на веб-сайте http://cs.co/umbrellamultiorgconsole

Распространенный вопрос о развертывании

«Насколько клиент Cisco Umbrella Roaming проще и прозрачнее по сравнению с другими средствами защиты оконечных устройств?»

Подробнее: http://cs.co/RoamingClient

Особенности развертывания

- Для предоставления сервисов Umbrella можно использовать любое сетевое устройство (например, маршрутизатор). Для защиты всех устройств, подключенных к сети, нужно внести всего одно изменение в IP-адрес на DHCP-сервере (или в диапазон адресов) или на DNS-сервере. А благодаря интеграции с контроллерами беспроводных локальных сетей Cisco и точками доступа Aruba, Cradlepoint и Aerohive для защиты всех устройств, подключенных к сети Wi-Fi, достаточно просто установить флажок.
- Защита устройств с операционными системами Windows и Mac OS X, не подключенных к сети. Если вы уже используете клиент Cisco AnyConnect для Windows или Mac, никаких дополнительных агентов устанавливать не нужно! Просто выполните обновление до версии 4.3 или более поздней и активируйте модуль защиты в роуминге. Либо разверните клиент Umbrella Roaming с помощью объекта групповой политики Windows или приложения Apple Remote Desktop.
- Детальный контроль устройств, подключенных к сети, с использованием удостоверений внутренней сети или Active Directory, поддерживает VMware и Hyper-V.
- Пассивная идентификация Active Directory поддерживает контроллеры домена в Windows Server.

Источники данных
1. http://cs.co/IDG-survey
2. http://cs.co/Forrester-BranchOffices
3. Отчет Verizon об утечках данных за 2015 г.
4. Отчет Ассоциации аудита и контроля информационных систем (ISACA) о глобальном состоянии информационной безопасности за 2015 г.

Cisco Umbrella