

Cisco Umbrella: пакет Professional

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 уровне DNS, 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).

Cisco Umbrella

Security Activity			
Date - Time	Domain	Security Category	Identity
11/4 - 10:01 am	unch67hs.br	Botnet	Chicago Branch Office
11/4 - 9:30 am	paypalz.com	Ransomware	CEO's Mac Air
11/4 - 8:05 am	webads.com	Exploits	CI O's Windows Laptop
11/3 - 12:04 am	klon8uy.ru	Malware	John Smith
11/3 - 8:40 pm	aegpyj121.cn	High-Risk	Paris Office Kiosk
11/3 - 7:34 pm	downloads.us	Custom Feeds	Prian Kerry's iPhone



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. Запланированные отчеты автоматически отправляются в вашу папку входящих сообщений.

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%
- Применение политик допустимого использования для более чем 60 категорий контента

Отличительные особенности Umbrella

- **Предотвращение угроз:** Umbrella не только обнаруживает угрозы, но и помогает избежать их
- **Защита устройств внутри и вне сети:** защита Umbrella не ограничивается устройствами, пересылающими трафик по локальной инфраструктуре
- **Регулярное обновление:** не требуется обратная связь устройств с локальным сервером по VPN-сети для получения обновлений

Проблемы, которые мы решаем

82% пользователей обходят сеть VPN¹, а 70% филиалов имеют прямой доступ в Интернет²

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 организации³

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 безопасности⁴

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



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



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



Выявление скомпрометированных систем путем отслеживания событий безопасности в режиме реального времени

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 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.

Распространенный вопрос о развертывании

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

Подробнее:
<http://cs.co/RoamingClient>

Источники данных

- <http://cs.co/perimeter>
- <http://cs.co/branchoffices>
- Отчет Verizon об утечках данных за 2015 г.
- Отчет Ассоциации аудита и контроля информационных систем (ISACA) о глобальном состоянии информационной безопасности за 2015 г.