Краткий обзор решения Cisco Umbrella

Раньше и компьютеры, и бизнес-приложения, и критически важная инфраструктура – все находились за межсетевым экраном. Сегодня все больше процессов происходит вне внутренней сети организации. Стало больше пользователей в роуминге. Больше корпоративных ноутбуков, подключающихся к Интернету из других сетей. Больше облачных приложений, для работы с которыми пользователям не требуется доступ к корпоративной сети. И больше филиалов, подключенных к Интернету напрямую.

По прогнозам Gartner, к 2021 году 25% корпоративного трафика среднестатистической компании будет передаваться в обход периметра сети. Когда пользователь находится вне корпоративной сети, он становится более уязвимым, и возможности организации по контролю и защиты от угроз снижаются. Одной лишь защиты периметра теперь недостаточно. Бреши в системе безопасности открывают доступ вредоносному ПО, программам-вымогателям и другим угрозам.

Первая линия обороны

Защищенный интернет-шлюз Cisco Umbrella служит первой линией обороны от интернет-угроз независимо от местонахождения пользователей. Umbrella обеспечивает полную прозрачность действий в Интернете всех пользователей на всех устройствах в любой точке и блокирует угрозы еще до того, как они проникнут в сеть или на оконечные устройства. Umbrella – это открытая облачная платформа, которая легко интегрируется с существующим стеком решений безопасности и предоставляет актуальную аналитику текущих и новых угроз.

Анализируя шаблоны интернет-трафика, Umbrella автоматически выявляет инфраструктуру злоумышленников, подготовленную для атак, и заранее блокирует запросы к вредоносным узлам до установления соединения. При этом никаких дополнительных задержек в сети не возникает.

Umbrella останавливает фишинговые атаки и заражение вредоносным ПО на ранних стадиях, быстро обнаруживает уже зараженные устройства и предотвращает утечку данных.

Безопасность, которая обеспечивается из самого Интернета

Система доменных имен (DNS) – базовый компонент Интернета, сопоставляющий доменные имена с IP-адресами. Когда пользователь переходит по ссылке или вводит URL-адрес, DNS-запрос инициирует подключение устройства к Интернету. Umbrella использует DNS в качестве одного из главных механизмов для передачи трафика на нашу облачную платформу, а также для применения политик безопасности.

Получив DNS-запрос, Umbrella оценивает его на основе данных аналитики как безопасный, вредоносный или сопряженный с риском (когда домен содержит и вредоносный, и легитимный контент). Безопасные запросы передаются как обычно, вредоносные блокируются, а сопряженные с риском перенаправляются на наш облачный прокси-сервер для углубленного анализа. Прокси-сервер Umbrella использует данные Cisco Talos о репутации веб-ресурсов и другие сторонние каналы для проверки URL-адреса. С помощью антивирусных систем и решения Cisco для защиты от сложного вредоносного ПО (AMP) наш прокси-сервер также анализирует файлы, которые пользователи пытались загрузить с сомнительных веб-сайтов. По результатам анализа подключение разрешается или блокируется.

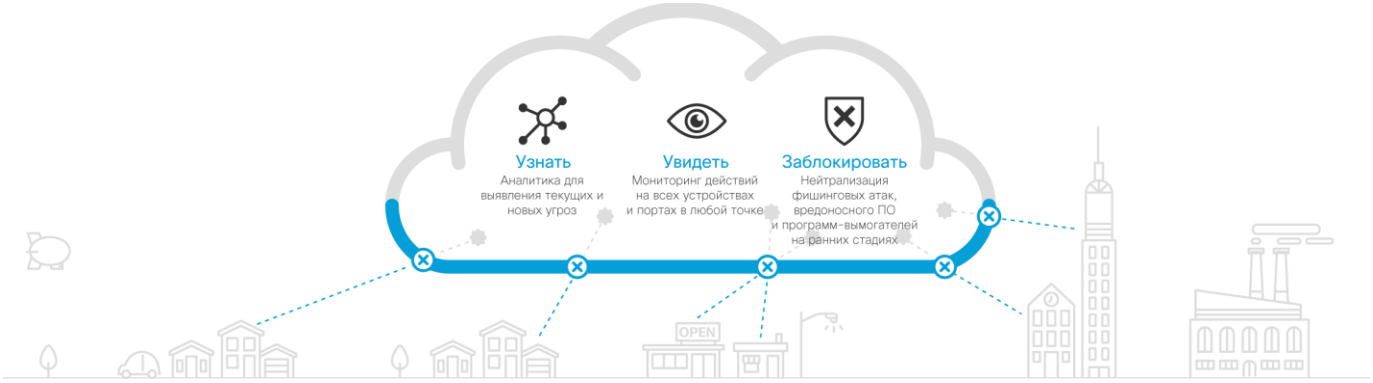
Преимущества

Снижение затрат на восстановление и ущерба в результате нарушения безопасности.
Так как Cisco Umbrella – это первая линия обороны, сокращается число заражений вредоносным ПО, требующих устранения, и угрозы удается нейтрализовать до того, как они нанесут ущерб.

Ускорение обнаружения и сдерживания угроз.
Cisco Umbrella блокирует обратные вызовы командных серверов через любой порт и протокол и предоставляет отчеты об этих действиях в режиме реального времени.

Улучшение мониторинга интернет-трафика для всех пользователей в любой точке.
Cisco Umbrella обеспечивает мониторинг, столь необходимый для оперативного реагирования на инциденты, и дает уверенность в полном контроле над обстановкой.

Выявление облачных приложений, используемых в компании.
Cisco Umbrella позволяет контролировать разрешенные и неразрешенные облачные сервисы, используемые на предприятии: можно понять, какие новые сервисы и кем используются, а также связанный с этим потенциальный риск.



Аналитика, позволяющая блокировать атаки до их начала

Глобальная сеть Umbrella, на основе которой построена наша служба рекурсивных DNS-запросов, ежедневно обрабатывает миллиарды интернет-запросов от миллионов пользователей по всему миру. Мы анализируем этот огромный объем данных, чтобы выявить шаблоны и обнаружить инфраструктуру злоумышленников.

Все данные об интернет-трафике, полученные через нашу глобальную сеть, в режиме реального времени передаются в графовую базу данных и затем непрерывно пропускаются через модели на основе статистических методов и машинного обучения. Эту информацию также постоянно изучают аналитики по безопасности Umbrella, дополняя ее сведениями от группы Cisco Talos. Успешно сочетая опыт наших специалистов с машинным обучением, мы выявляем вредоносные сайты (домены, IP-адреса или URL-адреса) по всему Интернету.

Совместимость с другими решениями

Umbrella интегрируется с существующим стеком решений безопасности, включая устройства защиты, аналитические платформы и брокеры безопасного доступа к облачной инфраструктуре (CASB, Cloud Access Security Broker). Umbrella может передавать данные журналов об интернет-трафике в системы управления событиями и данными безопасности (SIEM) или системы управления журналами. Используя наш API-интерфейс, можно запрограммировать отправку вредоносных доменов в Umbrella для блокирования. Это позволяет усилить имеющиеся средства обеспечения безопасности и легко расширить комплексную защиту.

Развертывание во всей организации за считанные минуты

Umbrella – самый быстрый и простой способ обеспечить безопасность всех пользователей за считанные минуты. Так как это облачное решение, не нужно устанавливать никакое оборудование и вручную обновлять программное обеспечение. Вы можете быстро инициализировать все устройства внутри сети, включая личные устройства сотрудников и устройства Интернета вещей, и использовать существующие решения Cisco – AnyConnect, маршрутизаторы с интегрированными сервисами (ISR) серии 4000 и контроллеры беспроводных локальных сетей моделей 5520 и 8540 – для оперативной подготовки тысяч устройств, покидающих сеть, и ноутбуков в роуминге.

Последующие действия

Чтобы обсудить, как решение Cisco Umbrella поможет защитить вашу мобильную, подключенную к облаку организацию от сложных угроз, обратитесь к торговому представителю или партнеру Cisco. Для получения дополнительной информации посетите наш веб-сайт umbrella.cisco.com.

Основные характеристики

- Всеобъемлющий мониторинг и защита
- Аналитика для раннего обнаружения атак
- Простота развертывания и управления
- Открытая платформа для интеграции
- Быстрая и надежная облачная инфраструктура

Основные цифры

- 100 млрд интернет-запросов ежедневно
- 65 млн пользователей
- 25 центров обработки данных по всему миру
- Более 7 млн вредоносных узлов назначения одновременно блокируется на уровне DNS