curator.pro

CURATOR

Curator.AntiDDoS

Защита сайтов от DDoS-атак

Curator.AntiDDoS

Curator Availability Network позволяет малым и крупным предприятиям защитить свои приложения от всех типов DDoS-атак, вне зависимости от их полосы и сложности.

Собственная уникальная георасределенная сеть фильтрации Curator, построенная на базе единой архитектуры BGP Anycast, обеспечивает надежную защиту приложений от любых сетевых атак, приводящих к недоступности веб-ресурсов.

Расширяем возможности бизнеса с облачным решением для защиты от DDoS-атак, обеспечивая постоянную доступность сети и повышая лояльность клиентов.

16 центров очистки трафика обеспечивают отличную связность сети с пропускной способностью свыше 4 Тбит/с. Центры фильтрации Curator расположены в мировых точках концентрации интернет-трафика, подключены к мировым TIER1 провайдерам и ведущим региональным магистральным интернет-провайдерам.

Ключевые преимущества Curator.AntiDDoS

Нейтрализация атак на всех уровнях сетевой модели ISO OSI, включая уровень приложений (L7).

Полный набор инструментов защиты для клиентов любого масштаба и для всех тарифных планов.

99,95% — самый высокий в отрасли уровень SLA по доступности инфраструктуры заказчика

В случае несоответствия решения качеству, заявленному в договоре, заказчик за нее не платит.

Уникальная архитектура BGP-Anycast

BGP-Anycast гарантирует географически распределенную, отказоустойчивую сеть для защиты приложений с высокой степенью связности. Отказ любого узла фильтрации не окажет влияния на качество обслуживания и производительность приложений клиентов благодаря балансировке трафика между ведущими поставщиками интернет-услуг

Легкость подключения

Несколько вариантов подключения, включая DNS и BGP

Always-on защита в автоматическом режиме 24/7

Не требует привлечения квалифицированных специалистов и ручной настройки системы для защиты от сложных DDoS-атак.

Простая интеграция с мобильными приложениями и API

API Curator дает доступ ко множеству функций управления системой, включая интеграцию с корпоративной системой аутентификации, базами данных или службами мониторинга.

Прозрачность для легитимных пользователей

Мы не используем CAPTCHA и другие системы проверки, раздражающие пользователей.

Техническая поддержка 24/7/365

Клиенты могут рассчитывать на помощь высококвалифицированных инженеров Curator по различным каналам связи, включая систему онлайн-тикетов, поддержку по телефону, электронной почте и в чате. Время реакции на каждый запрос клиента не превышает 15 минут.

Secure Sockets Layer (SSL) – фильтрация HTTPS без раскрытия ключей (PCI DSS ready)

Уникальная технология позволяет анализировать и фильтровать HTTPS-трафик без раскрытия ключей шифрования, не нарушая политики безопасности клиента.

Не оказывает влияния на SEO

Улучшает SEO веб-сайта за счет сокращения времени загрузки страницы и повышения уровня безопасности.

Балансировка трафика между IP-адресами и веб-серверами клиента

Мы распределяем трафик между основными и резервными web-серверами сайта клиента. В зависимости от пожеланий, мы можем реализовать индивидуальные алгоритмы обращения к резервным серверам.

3 уровня фильтрации трафика

1 Перенаправление трафика защищаемого приложения в сеть Curator.

Анализ трафика проводится на всех уровнях стека протоколов, включая уровень приложений (седьмой уровень модели OSI). Трафик атак уровня приложения максимально походит на активность обычных пользователей, что делает атаки нетривиальными в обнаружении и очень сложными в нейтрализации.

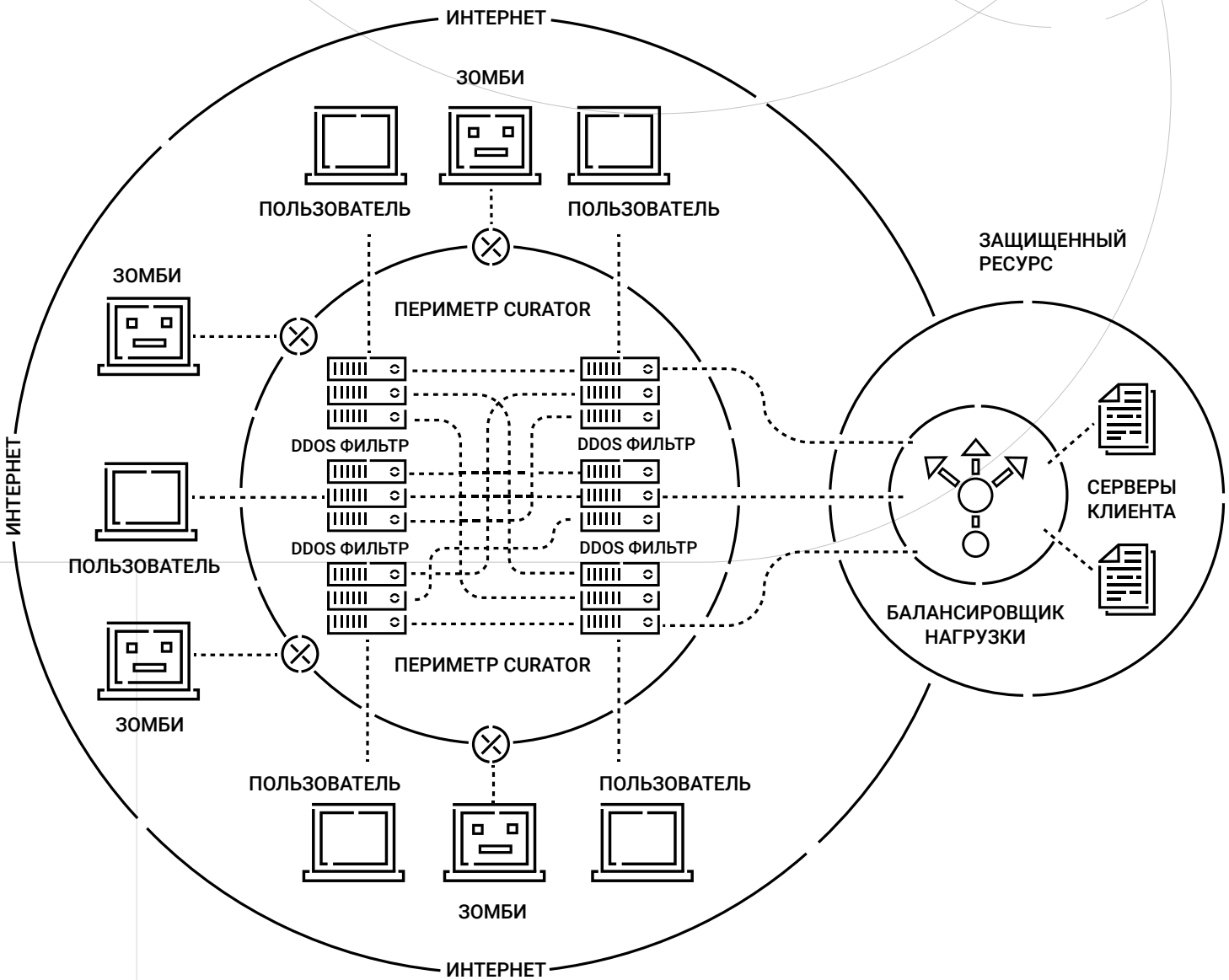
2 Многоуровневая фильтрация трафика с использованием поведенческих, эвристических и сигнатурных алгоритмов.

Постоянно изучая структуру трафика вне зависимости от наличия DDoS-атаки, Curator улучшает алгоритмы и на лету производит донастройку имеющихся методов фильтрации, что позволяет выявлять любые аномалии и немедленно реагировать на DDoS-атаки.

3 Направление чистого трафика на защищаемое приложение.

Отфильтрованный трафик отправляется к защищаемому приложению либо через публичную сеть Интернет, либо через специально организованный L2 VPN. Трафик DDoS-атак блокируется на периметре сети Curator, не достигая ресурсов клиента. Работа сети Curator полностью незаметна как для самого бизнеса, так и для пользователей его приложения, и о факте атаке клиенты Curator узнают только из отчетов в личном кабинете.

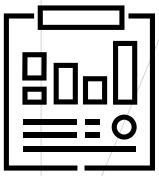
Как работает Curator.AntiDDoS



SLA 100% для платформы Curator

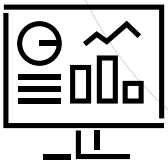
Бесплатный тестовый период – 7 дней

7 дней – если приложение не под воздействием DDoS-атаки. В противном случае, тестовый период составляет одни сутки.



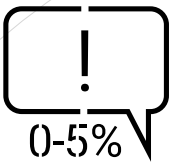
Наглядная отчетность в личном кабинете

Анализ трафика приложения за любой период оказания решения доступен в online-режиме. Используя API, можно подключить существующую у вас систему мониторинга (Nagios, Zabbix и т.д.) к Curator и получать уведомления об инцидентах.



Интеграция с системами мониторинга

Используя API, вы можете подключить к сети Curator свой SOC / систему мониторинга / SIEM и получать оповещения об инцидентах в удобном для вас формате.



Минимальное количество ложных срабатываний: не более 5% в случае атаки

Алгоритмы Curator позволяют определить, чем вызван всплеск посещаемости ресурса – DDoS-атакой или повышением интереса посетителей.

Время реакции сети Curator на DDoS-атаку — до 30 секунд для 97% векторов атак

4 простых шага подключения защиты от DDoS-атак за 15 минут

1. **Зарегистрируйтесь в личном кабинете**
2. **Получите Curator IP**
3. **Установите цепочку сертификатов SSL**
4. **Перенаправьте свой трафик на IP-адрес Curator**

curator.pro
sales@curator.pro
8-800-333-35-22

CURATOR