0
Рейтинг

InlyIT

Для старательного нет ничего невозможного

InlyIT
31 мая 2024 в 07:23

Cloudflare положил наш сайт после того, как мы отказались выплатить 120 000 $ в течение 24 часов

9 мин 131K

Блог компании InlyIT, Администрирование доменных имен*, Облачные сервисы*

Перевод

Автор оригинала: Robin Dev

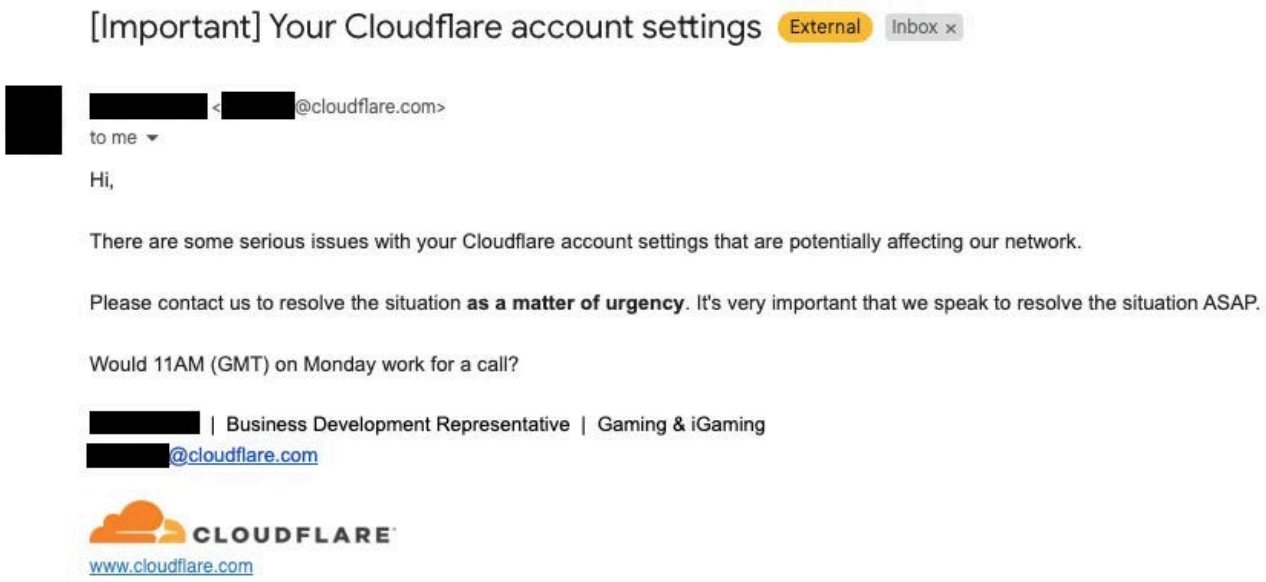
Я работаю системным оператором в довольно крупном онлайн-казино (мне представляется, что материал статьи может быть полезен читателям вне зависимости от их позиции касательно этичности казино в целом – упоминаю об этом просто для контекста). У нас около четырех миллионов активных пользователей в месяц. С Cloudflare мы охотно сотрудничаем с 2018 года по тарифу «Бизнес», который стоит 250 $ в месяц и предоставляет неплохие возможности, включая безлимитный трафик.

Нужно признать, 250 $ — невеликие деньги за те объемы трафика, которые мы прогоняли через Cloudflare. В основном мы используем Cloudflare для CDN (кэшируем весь свой статический контент) и для защиты от DDOS-атак – с этими задачами сервис хорошо справляется. Работать с ним просто, и обычно ни о чем не приходится особенно задумываться.

Я читал несколько статей на Hacker News, где рассказывалось, как в какой-то момент Cloudflare связывается с компаниями и начинает агрессивно навязывать корпоративный тариф на персональных условиях. Но я не ожидал, что всё будет настолько плохо.

19 апреля 2024 года

В апреле мы получили от Cloudflare вот такое письмо:



[Important] Your Cloudflare account settings External Inbox ×

[redacted] <[redacted]@cloudflare.com>
to me

Hi,

There are some serious issues with your Cloudflare account settings that are potentially affecting our network.

Please contact us to resolve the situation **as a matter of urgency**. It's very important that we speak to resolve the situation ASAP.

Would 11AM (GMT) on Monday work for a call?

[redacted] | Business Development Representative | Gaming & iGaming
[redacted]@cloudflare.com

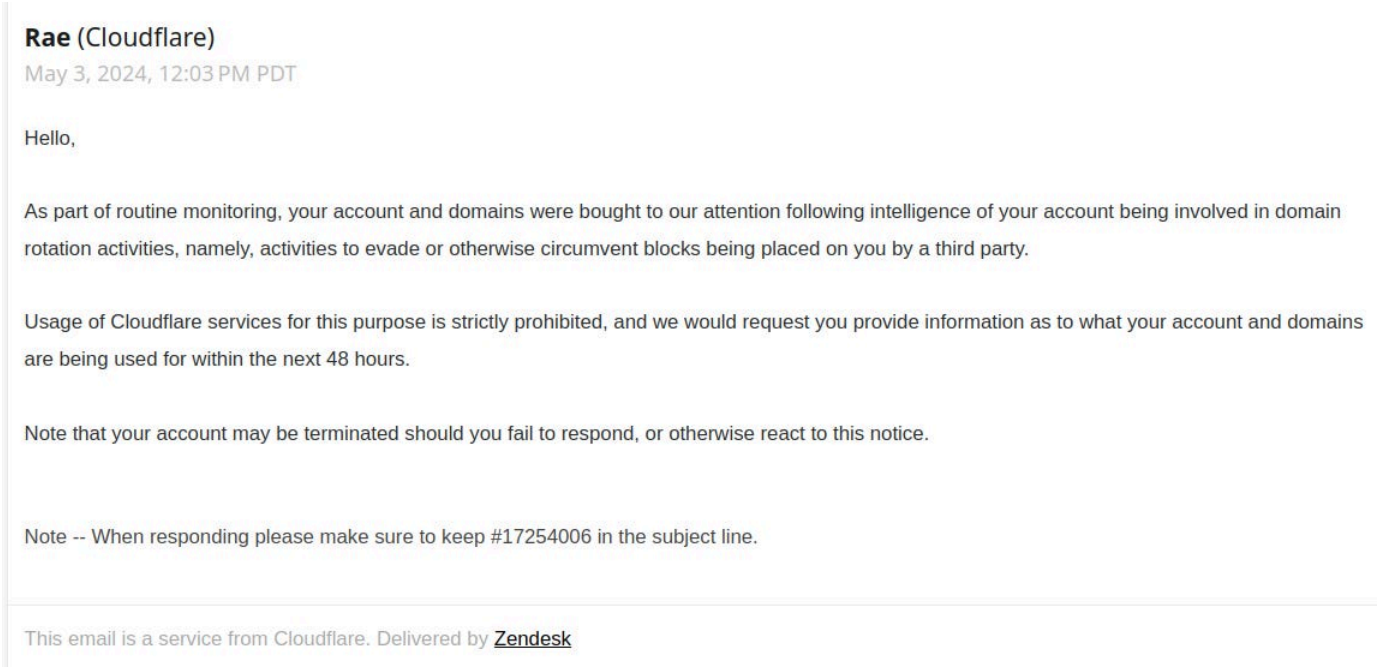
CLOUDFLARE
www.cloudflare.com

Добрый день!
В настройках вашего аккаунта на Cloudflare обнаружены серьезные проблемы, которые могут влиять на работу наших сервисов.
Пожалуйста, свяжитесь с нами, чтобы разрешить этот вопрос, в срочном порядке. Для нас крайне важно решить вопрос как можно скорее.
Удобно ли вам будет созвониться в 11 часов (GMT) в понедельник?

Звучит так, будто с нашим сайтом что-то неладно. Мы назначили время для созвона с их отделом «по развитию бизнеса». В реальности беседу проводил отдел продаж, и ни о какой «серьезной проблеме» они на деле сообщить нам не смогли. Они спросили, не хотим ли мы перейти на корпоративный тариф. Мы вежливо отказались, недоумевая от того, как плохо все это вяжется с тоном письма.

3 мая 2024 года

Спустя две недели мы получили новое письмо.



Rae (Cloudflare)
May 3, 2024, 12:03 PM PDT

Hello,

As part of routine monitoring, your account and domains were bought to our attention following intelligence of your account being involved in domain rotation activities, namely, activities to evade or otherwise circumvent blocks being placed on you by a third party.

Usage of Cloudflare services for this purpose is strictly prohibited, and we would request you provide information as to what your account and domains are being used for within the next 48 hours.

Note that your account may be terminated should you fail to respond, or otherwise react to this notice.

Note -- When responding please make sure to keep #17254006 in the subject line.

This email is a service from Cloudflare. Delivered by Zendesk

Здравствуйте!
В ходе регулярного наблюдения наш внимание привлек ваш аккаунт и домены; поступали сведения, что ваш аккаунт осуществляет действия, связанные с ротацией доменов, если конкретнее, направленные на обход блокировок, выставленных против вас третьей стороной
Использование сервисов Cloudflare в подобных целях строго запрещено, и мы просим вас предоставить информацию о том, для чего используются ваши аккаунт и домены, в течение 48 часов.
Обращаем ваше внимание на то, что ваш аккаунт может быть удален при отсутствии ответа или иной реакции на данное извещение.

Тут нужно привести немного дополнительного контекста, чтобы было понятно, о чем идет речь. У нас действительно несколько доменов, и по большей части они служат зеркалами для основного. На то имеется несколько причин. Первая: так как мы держим казино, нам приходится соблюдать соответствующие нормативные требования, которые отличаются от страны к стране. Например, доступ ко многим играм открыт только для ряда стран. Некоторые страны мы блокируем полностью. Кроме того, мы завели несколько доменов, чтобы отключать на каких-то из них те или иные категории игр или активности – скажем, социальную часть (чаты, персональные донаты, общение между игроками) или букмекерские услуги. Также мы используем домены, чтобы таргетировать разные глобальные группы пользователей и партнеров и отслеживать конверсию на длинных временных отрезках. Помимо прочего это означает, что, если страна накладывает DNS-блокировку на наш основной домен, то доступ к дополнительным может сохраняться. Это с какой-то точки зрения можно рассматривать как нарушение соглашения с Cloudflare, о котором они говорится в письме.

Так или иначе, более 95% нашего трафика идет через основной домен, и это оставалось

неизменным со дня основания компании. Вдобавок мы совершенно не возражали против того, чтобы решить проблему любым способом, включая удаление с Cloudflare всех дополнительных доменов, к которым возникли претензии.

Мы переслали им информацию о доменах и попытались выяснить подробности о проблеме и о том, кого из нашей команды следует привлечь к обсуждению. Но они отказались озвучить что-либо, кроме даты следующего созвона.

7 мая 2014 года

Мы договорились о втором созвоне, на этот раз с отделом «доверия и безопасности». Как потом выяснилось, на самом деле мы снова общались с отделом продаж.

Они сказали, что могут предложить нам отличный тариф с массой замечательных возможностей за 10 000 $ в месяц. Мы попытались разобраться, как именно это связано с нарушением соглашения и что нужно, чтобы его устранить. Мы поинтересовались, какие именно домены задействованы в ротации, которая их беспокоила. Ответов на эти вопросы не последовало.

Тогда мы спросили, какие из возможностей корпоративного тарифа нам действительно необходимо оплатить.

Нам не предложили никаких вариантов, кроме покупки полного набора за 10 000 $ — это якобы магическим образом решит все проблемы. В обсуждении других путей решения сотрудники были не заинтересованы.

Нам дали сутки на подписание контракта, потому что они обязались «передать информацию отделу доверия и безопасности». Мы попросили перевести нас на помесячную оплату. Нам ответили, что мы должны подписать контракт на год и выплатить всю сумму сразу. Это напоминало вымогательство: выкладывайте 120 000 $ к завтрашнему дню, или мы уничтожим ваш бизнес.

После созвона нам пришло письмо с описанием тарифа:

As discussed, please find below a summary of the solution needed for your use case as well as the preliminary quote.

Cloudflare Enterprise Plan with:
1. BYOIP (you can lease IPs and we will onboard and advertise them on your behalf)
2. SSL4S (helps you to add/change hostnames/mirrors with 3 sec. propagation and without the need to set up DNS/ CDN/DDoS/WAF/SSL configurations) - this can be done via API too

The **Enterprise Plan** includes the following services:

- Advanced **DDoS** / **WAF** / **CDN** / **DNS** / **Certificates** fully managed
- **Argo Smart Routing** - optimised content delivery via fastest routes (up to 70% latency improvement)
- **Advanced Cache control** (ie. Custom Cache Keys, Cache Purge by Tag and more)
- **Image Resizing** (1m images served per month, included)
- **Workers** (10m included)
- **Zero Trust Access** - 50 seats
- **Raw logs** - detailed HTTP request logs to debug, identify configuration adjustments and create analytics - up to 150 attributes for each request. Additionally direct integration with SIEM tools like Splunk, DataDog, ELS, Azure, GCP, AWS or any S3 compatible storage
- **Site Analytics** resolution (down to 1 minute scope for the last 30 minutes)
- **Priority Support** 24/7/365 via telephone, chat, email
- Assigned Account Manager and Solutions Engineer, Access to Success team for consultation
- Advanced/ proactive notifications on the status of your Cloudflare environment - support for Webhooks and Slack
- **Role Based access -** grant access to Cloudflare based on member's access rights. Additionally full audit log on the activity

BYOIP (leasing companies): *These are some options where you can lease IPs, you can of course use any other provider:*
Larus https://www.larus.net/ip-leasing
Bandwidth Technologies https://www.bandwidth.co.uk/connectivity/ipv4-leasing
IPXO https://www.ipxo.com/lease-ips/
IPV4Market Group https://ipv4marketgroup.com/broker-services/ip-leasing/

Commercials**: $9.940/ month** (with default annual payment), including:

- Enterprise Plan (as per above) - based on 80 TB/ 6B requests
- Your main domains & hostnames for rotation - 2 Top Level Domains & 15 mirror domains
- BYOIP support and onboarding

Happy to walk this through and discuss further technical details tomorrow.

As we have a very short window to report back to the Trust and Safety team, please let me know if you can make time **tomorrow at 13:00 CET.**

Заметьте: из текста письма выходит, что ежемесячные платежи – все же допустимый вариант. Когда мы стали уточнять этот момент, нам снова сказали, что платить мы должны сразу за целый год.

Большинство возможностей, перечисленных в письме, нам не нужно. Просьба подключить BYOIP и снять с компании обязательства по нашим доменам мне понятна, но всё остальное либо совсем нам ни к чему, либо из разряда «ну, можно».

За счет привлечения руководителя компании и технического директора, которые поговорили с Cloudflare лично, мы выторговали себе еще неделю времени. Однако представители компании по-прежнему не желали слышать ни о каких других вариантах решения проблемы и не предлагали альтернативных условий контракта. Отыскать расценки в сети непросто, однако, если приглядеться (для сравнения можно взять этот или этот посты), то 80TB трафика можно уложить во вполне разумный диапазон от 150 $ до 2000 $ в месяц. Отмечу, что 80TB – это та цифра, которую нам называли, за ее точность поручиться не могу, так как нам отрезали доступ к исторической аналитике.

Всё это время мы параллельно вели поиски альтернативы: обратились к Fastly, который выглядел достойным конкурентом, и создали там тестовый домен.

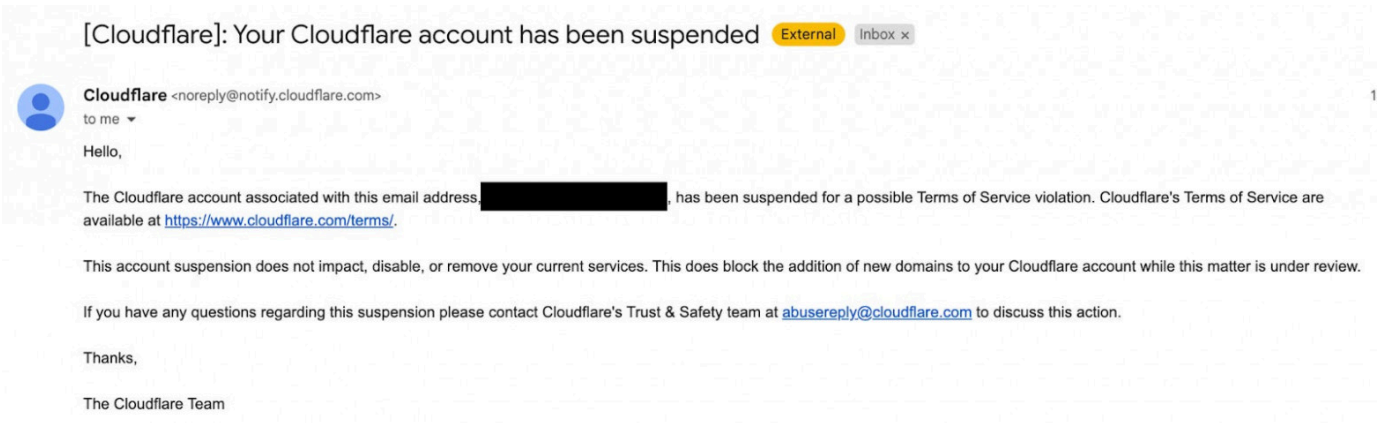
16 мая 2024 года

Во время очередного созвона в попытках добиться более приемлемых для нас условий контракта наш руководитель сообщил отделу продаж Cloudflare, что мы ведем переговоры с их конкурентами. По-моему, это и так понятно, кто бы не пошел искать план Б, когда ему выкатывают счет на 120 000 $? Но через несколько часов после этого разговора произошло следующее:

Date	Action	User	Domain
May 16, 2024	Purge	Cloudflare	[redacted]
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	

Cloudflare внезапно удалили все наши домены. Все DNS-записи, настройки кэширования, ограничения скорости, белые списки – подчистую. Наш публичный вебсайт, наши входящие письма (включая запросы в техподдержку от пользователей), наша внутренняя инфраструктура, наши настройки авторизации на Cloudflare Access – упало всё.

И еще нам пришло письмо:


[Cloudflare]: Your Cloudflare account has been suspended External Inbox ×

Cloudflare <noreply@notify.cloudflare.com>
to me

Hello,

The Cloudflare account associated with this email address, [redacted], has been suspended for a possible Terms of Service violation. Cloudflare's Terms of Service are available at https://www.cloudflare.com/terms/.

This account suspension does not impact, disable, or remove your current services. This does block the addition of new domains to your Cloudflare account while this matter is under review.

If you have any questions regarding this suspension please contact Cloudflare's Trust & Safety team at abusereply@cloudflare.com to discuss this action.

Thanks,

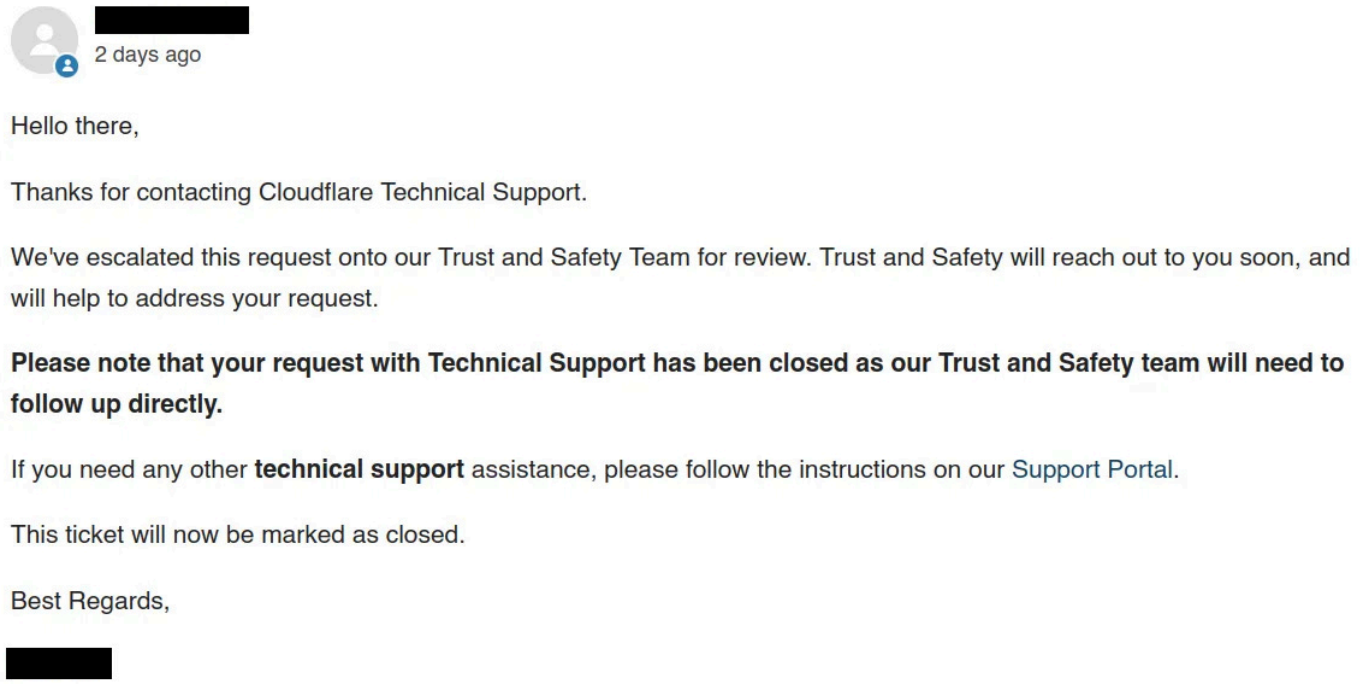
The Cloudflare Team

Здравствуйте!
Аккаунт на Cloudflare, привязанный к электронной почте <….>, заморожен из-за возможного нарушения условий соглашения. Условия соглашения Cloudflare доступны по адресу <…>
Заморозка аккаунта никак не влияет на оказание текущих услуг, не отключает их и не удаляет. В ходе рассмотрения данного вопроса возможность добавлять новые домены на Cloudflare не блокируется.

Если у вас есть какие-то вопросы касательно заморозки, пожалуйста, обратитесь в отдел доверия и безопасности по адресу <….> для их обсуждения.

В письме говорится, что принятые меры «не влияют на оказание текущих услуг», так что мы лихорадочно отправили запрос в техподдержку, но ответа не получили. Поэтому пришлось собирать команду системных операторов и переносить основной сайт на Fastly. С основным справились за несколько часов, но, как выяснилось, сложно предсказать, сколько времени займет даже перенесение изменения в записи доменного имени – от часа до двух суток. Нам до сих пор аукаются последствия.

В конце концов мы получили от Cloudflare ответ по своему запросу в техподдержку:



[redacted]
2 days ago

Hello there,

Thanks for contacting Cloudflare Technical Support.

We've escalated this request onto our Trust and Safety Team for review. Trust and Safety will reach out to you soon, and will help to address your request.

Please note that your request with Technical Support has been closed as our Trust and Safety team will need to follow up directly.

If you need any other **technical support** assistance, please follow the instructions on our Support Portal.

This ticket will now be marked as closed.

Best Regards,

[redacted]

Здравствуйте!
Спасибо, что обратились в техническую поддержку Cloudflare.
Мы передали ваш запрос на рассмотрение выше, в отдел доверия и безопасности. С вами скоро свяжутся оттуда, чтобы решить проблему.
Пожалуйста, имейте в виду, что ваш запрос в техническую поддержку закрыт, так как отделу доверия и безопасности нужно будет вести с вами обсуждение напрямую.
Если вам нужна еще какая-либо помощь по техническим вопросам, пожалуйста, следуйте указаниям на нашем Портале поддержки
Тикет мы на данном этапе маркируем как закрытый.

Отдел «доверия и безопасности» так с нами и не связался, а аккаунт остается заблокированным.

Советы для тех, кому написали из Cloudflare

Начну с поздравлений: вероятно, ваш бизнес стал весьма успешным! Но по какой же именно причине в Cloudflare решили «попросить» вас перейти на корпоративный тариф? Возможно, дело в том, что вы достигли трафика в 10TB в месяц, или астральные тела в их лавовых лампах сложились определенным образом, или глава отдела продаж увидел, что норма за квартал еще не выполнена.

В общем, никому это не известно. Cloudflare не дает никакой информации о том, в какой момент начнет выпихивать вас на персональную тарификацию. Но если они вдруг возгорелись желанием «срочно» с вами поговорить, то вряд ли вам удастся соскочить без подписания контракта на особых аппетитных условиях. Не случайно они нигде у себя открыто не говорят об ограничениях по тарифам и ценах на корпоративное обслуживание. Их отдел продаж воспользуется любым поводом (например, наличием нескольких доменов), чтобы заставить вас целиком перевести аккаунт на корпоративный тариф, и неважно, что этот повод можно было бы легко устранить.

Цена, которую вам назовут, будет рассчитываться исключительно на основании того, сколько вы, по их предположению, готовы заплатить, а не на измеримых показателях или наборах возможностей.

Мы пытались узнать, как повлияет на цену снижение объемов трафика (у нас большая доля обратного трафика, который использует белые списки IP, ему проходить через CDN вообще не обязательно, просто мы не тратили время на оптимизацию, раз уж нам по тарифу положен безлимитный трафик). Но нам отказали в любых пояснениях, кроме того, что учитывалась цифра 80TB.

Мы пытались возражать, что из 14 возможностей, которые включает тариф, нам не нужна ни одна. Нам сказали, что все эти головокружительные возможности будут входить в набор, нужны они нам или нет.

Данные, которые мы нашли на Hacker News (ссылке приведены выше), позволяют заключить, что цены, которые обычно выставляют за те же услуги, отличаются как минимум на порядок.
Мы пытались донести, что не для всех наших доменов требуется корпоративное обслуживание. Нам сказали, что на корпоративный тариф аккаунт переводится целиком.

Если им покажется, что вы недостаточно лояльны (или, возможно, что у вас есть альтернативы), они выставят нереально сжатые сроки и попытаются продавить вас на оплату за год вперед.
Они воспользуются любым предлогом, чтобы доказать, что вам остро стал нужен корпоративный тариф, даже если до сих пор вы отлично себя чувствовали и на «Бизнесе».

Мы не единственные, чей бизнес оказался под угрозой из-за агрессивной тактики продаж Cloudflare.

Не думайте, что, раз вы платите 250 $ в месяц, то заслуживаете какой-то вежливости или вообще любой реакции (кроме предложений от отдела продаж) на ваши запросы в поддержку. Судя по всему единственный способ ее добиться – устроить скандал в публичном поле.

Подготовьтесь к тому, чтобы за 24 часа переехать с Cloudflare.

- Ни в коем случае не регистрируйте домены непосредственно на Cloudflare. Если вы это сделаете и вас заблокируют, понятия не имею, как вы сможете их вызволить в какие-то разумные сроки. Нам повезло, у нас только доменные имена были не так связаны с CF, так что в ходе переезда для большинства пользователей сайт пролежал от 3 до 24 часов.
- Не используйте никаких кастомных правил кэширования на Cloudflare. Сервис по умолчанию игнорирует многие, если не все, заголовки хэширования в HTTP, за исключением произвольного списка расширений, и подталкивает вас к тому, чтобы создавать кастомные правила. Вместо этого проставьте «Cache: Always» (на самом деле не всегда) и «Respect Origin Headers». Так правила будут работать и на других кэширующих прокси-серверах.
- Не используйте никаких продуктов Cloudflare вроде Zero Access или Workers. Мы активно использовали Zero Access для авторизации во внутренних продуктах, и теперь приходится с нуля выстраивать всю эту инфраструктуру с длительными периодами простоя. Прибегайте к их технологиям только при условии совместимости со сторонними стандартами.

Делайте бэкапы своих конфигураций на Cloudflare. Воссоздавать их оказалось неожиданно тягомотным делом, учитывая, что туда входят сервисы для рассылки писем (SPF, DKIM, …), записи DNS по верификации сайтов, списки ip, правила ограничения скорости и так далее.

Прочувствуйте бизнес-модель Cloudflare и ее влияние на ваш бизнес: либо вы наживаетесь на Cloudflare (бесплатный и бизнес-тарифы), либо они на вас (корпоративный тариф с непрозрачными условиями). Промежуточных вариантов нет, и рано или поздно придет время переключаться с первого на второе.

И наконец: подумайте, так ли вам вообще нужен Cloudflare. У нас он справлялся только с

DDOS-атаками довольно крупных масштабов. Если у вас есть поверхности атаки, которые чуть более уязвимы (например, некэшированный неавторизованный API-запрос, который съедает до 100мс процессорного времени, а значит, ресурсы ядер можно исчерпать всего 10-100 запросами в секунду), Cloudflare ничего там даже не обнаружит. Отдельно следует учесть, что все более-менее профессиональные пользователи «DDOS-атаками как услугой», похоже прицельно специализируются на сервисах с Cloudflare, предусматривают обходные пути для Under Attack Mode и так далее.

Теги: cloudflare, домены, dns

Хабы: Блог компании InlyIT, Администрирование доменных имен, Облачные сервисы

+249 141 400

InlyIT

Для старательного нет ничего невозможного

Сайт

253 Карма 0 Рейтинг

InlyIT @InlyIT

Пользователь

Подписаться

Комментарии 400

saga111a
31 мая 2024 в 08:23

> 7 мая 2014 года

Эхх, хорошее время.

Еще один пример когда завязывание инфраструктуры на аутсорс имеет степень угрозы как бандитизм.

Ответить

Wesha
31 мая 2024 в 20:52

Ещё одно напоминание, что всё, что *лично я* не контролирую — оно *не моё.*

Как-то так

Ответить

in_heb
1 июн 2024 в 01:02

ну это по сути ничем не отличается от вендор-лока проприетарного ПО.

а с другой стороны понятно, что 250$ никак не окупают их затрат, цена должна быть изначально коммерческой, а не заманухой на попробовать

Ответить

Popadanec
1 июн 2024 в 09:45

Так иначе бы и не попробовали. Любому бизнесу нужно время чтобы раскрутится и в этот период, любая копейка не лишняя. Это даже государство понимает, устанавливая минимальные налоги для тех у кого нет больших оборотов. Выскочил за 60млн в год(патент в РФ), будь добр, плати совсем другие деньги.

Ответить

alpha_man
27 июн 2024 в 08:20

Так цена объективно должна рассчитываться из затрат. В данном случае объемов трафика и доп услуг. Тут же называли цену с потолка прокатит/не прокатит. В тех же облаках всегда понятно за что и когда ты платишь

Ответить

aleksejjjjj
3 июн 2024 в 08:39

Ну а с другой стороны, какие варианты? Собственный сервер держать на балконе, и мужественно отбивать ддос на канале 100мбит? Ой, канал то опять не наш, дому.ру на аутсорс отдали.

По факту пока вы не гугл и не фейсбук у вас всегда будут сторонние решения. Начиная с виртуальных серверов и заканчивая. Да ничем не заканчивая, всё это вам не принадлежит

Ответить

nev3rfail
3 июн 2024 в 17:45

Самопальный беовульф кластер на PS3, так победим!:)