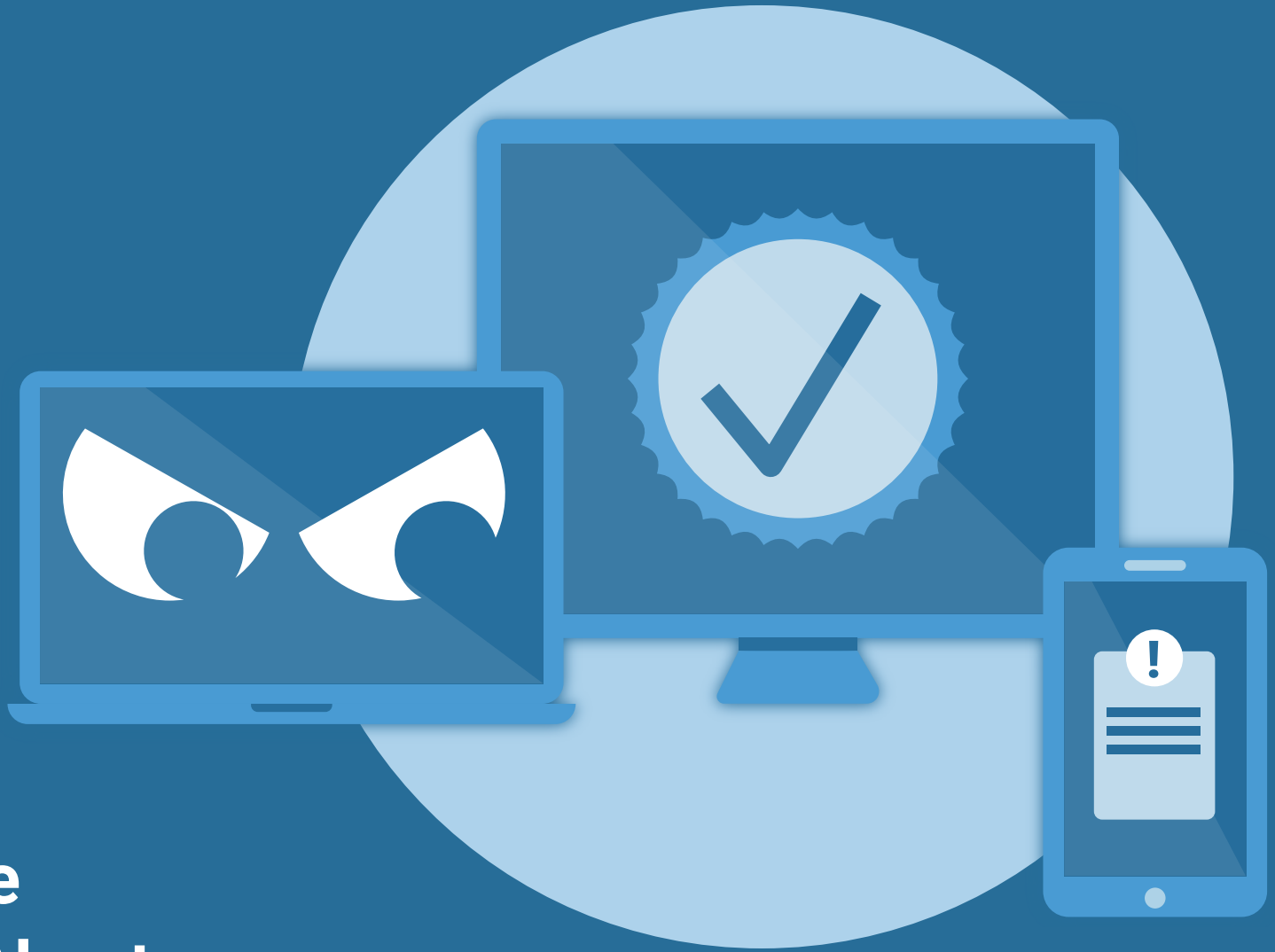


Debunking the Top 5 Myths About Malicious Bots

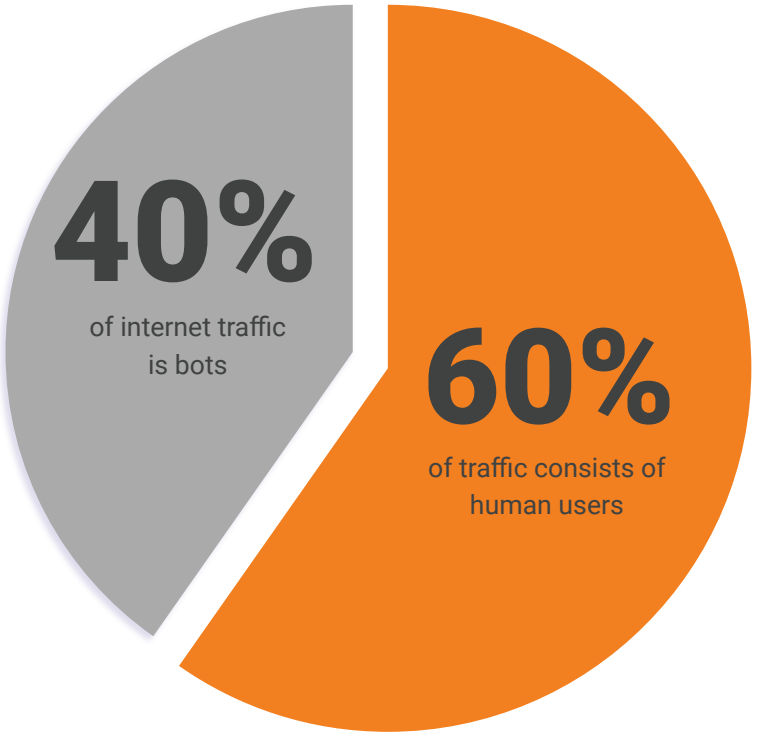
1-888-99-FLARE | enterprise@cloudflare.com | www.cloudflare.com

CLOUDFLARE®

Table of Contents

CLOUDFLARE

Myths About Malicious Bot Traffic

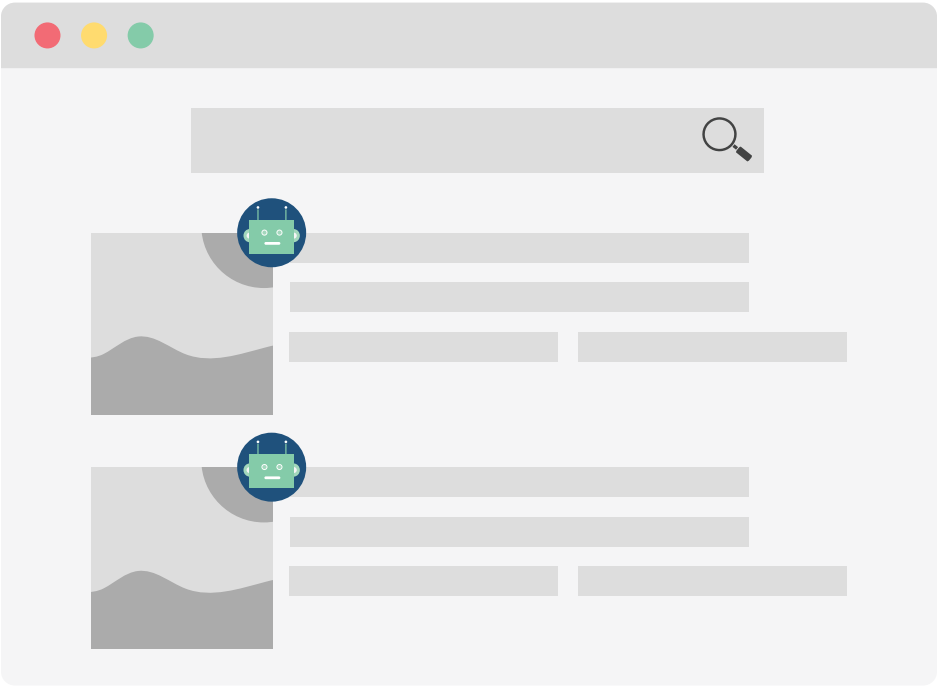


Today, as much as 40% of all Internet traffic consists of bots: non-human users of websites and apps.[1] Unfortunately, much of this bot traffic is malicious. And as malicious bots become more prevalent and sophisticated, truth and fiction sometimes blur together, making it difficult to understand how bad bots can impact your organization — and what you can do to prevent them.

Let's take a closer look at some of the most common false assumptions about bad bots — and how your organization can stay bot-free by taking a more informed approach to defense.

MYTH #1

All bots are bad



Although malicious bots tend to get the most attention, good bots are almost as prevalent.

Good bots play crucial roles in keeping digital business flowing. For example, bots help companies like Google, Bing and Baidu index billions of sites that show up in your search results. And every time you run a travel search on Expedia or Priceline, a team of partner bots "scrape" (i.e., run searches on) the websites of companies like Delta and American Airlines, then return with a list of flight times and prices that match your search terms.

Cont'd Next >>

The Role of Good Bots

This distinction matters because good bots are so essential to today's Internet that it is impractical to stop bad bots simply by blocking all non-human users.

Attackers are well aware of this fact — which is why they deliberately design their malicious bots to mimic the behavior of the good bots that can benefit your organization. Scraper bots, for example, can grab original content from your site and repost it on fraudulent sites without your permission. But if you block all scrapers, you might prevent well-intentioned partners — e.g. a distribution partner or a review site — from accessing the information they need to promote your organization legitimately.

> *Before using Cloudflare we were simply in the dark, we had no idea about the percentage of bots our infrastructure was receiving or if we needed to take action to protect our publisher partners' interests against malicious traffic."*

Romeo Ju President

Sulvo

MYTH #2

Bots target only certain industries – ecommerce, travel and finance

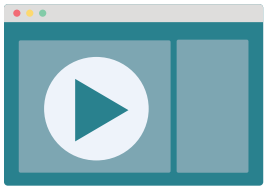
While many high-profile bot attacks have targeted banks, airlines, hotels, and e-commerce companies, malicious bots increasingly target numerous industries. Over the past several years, Cloudflare has seen bots prey on healthcare facilities, ticketing providers, educational institutions, gaming companies, advertising and marketing firms, publishing houses, and even government agencies.

The tactics of bot operators vary widely from one of these verticals to another. In fact, many bot attacks are uniquely targeted to exploit vulnerabilities in a specific organization's business logic. For example, a website that serves content to millions of external users may fall victim to a content scraping or inventory hoarding attack, while a facility that stores sensitive internal data may become a target for brute force password cracking.

The truth is that any website with a customer-facing login page can present an attractive target for bad bots. What's more, any enterprise-scale organization that provides marketing, IT, web design, or other digital services can appear every bit as tempting as a cash-filled bank vault from the perspective of a malicious bot operator.

MYTH #3

Bot attacks are most prevalent during the holiday shopping season



It's certainly true that we see a large number of bot attacks during the holidays.[2] But it's equally true that bot attacks can strike at any time of the year — sometimes driven by a major event like a product launch, other times incited by factors much harder to predict.

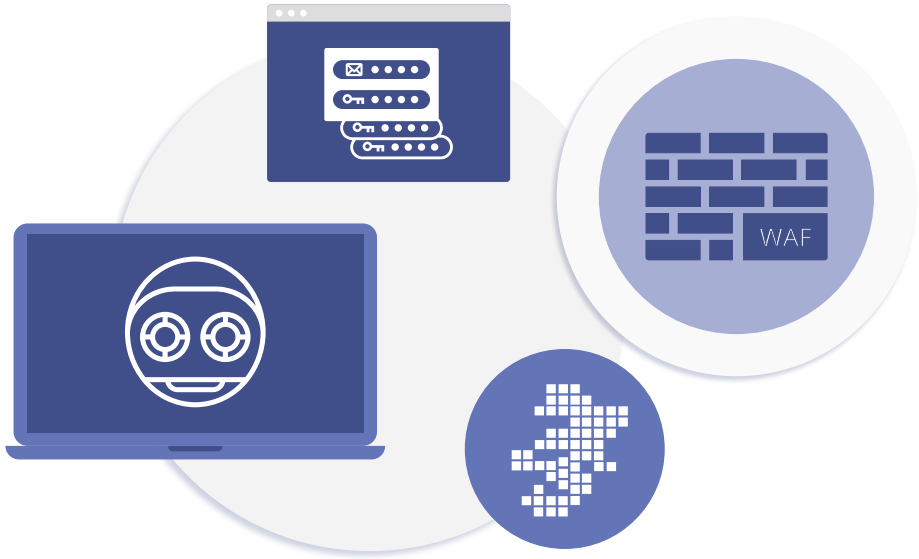
Bot attacks happen year-round

For example, an infamous bot attack targeted Disney in November 2019, coinciding with the launch of the new Disney+ content streaming service.[3] Bots used credential stuffing to target customer accounts during the launch of the service, and thousands of those compromised accounts appeared for sale on the dark web. Criminals who purchased these cracked accounts could potentially gain access to users' banking details, along with login info for many other sites and apps.

And while the Disney attack remains one of the largest bot-related disasters in recent memory, numerous smaller attacks take place throughout every month of the year. In fact, the sheer unpredictability of bot activity such as J.Crew credential stuffing attack in April 2019,[4] represents one of the strongest arguments for adopting a multifaceted bot defense solution.

MYTH #4

My organization can stop all malicious bots with a single tool



It may seem like DDoS mitigation, rate limiting, a web application firewall (WAF), multi-factor authentication, captcha or other single-method tactics will single-handedly meet an organization's bot management needs. But bot attacks are getting sophisticated and are able to bypass individual defenses by mimicking human behavior. The reality is, organizations need a comprehensive bot management solution.

Cont'd Next >>

My organization can stop all malicious bots with a single tool, cont'd

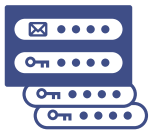
DDoS mitigation can be effective against volumetric attacks, in which a botnet tries to disrupt a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. But DDoS mitigation is much less adept at detecting individual bots that imitate human user behavior.

WAFs can defend against SQL injections, cross-sitescripting (XSS), and zero-day attacks by enforcing policies that prevent access from specific IP address ranges or geographic locations. But today's bot operators can rotate through millions of IPs in hundreds of countries.

CAPTCHAs can serve as an effective component of bot prevention by catching obvious bad bots. But some of the latest bots can now solve CAPTCHAs—and in any case, CAPTCHAs negatively impact your user experience by adding unnecessary friction to your login or purchase journey.

Rate limiting can block simplistic bot attacks that make excessive numbers of requests. But sophisticated bots can avoid detection by simply reducing their request rate. Many of today's bad bots go "low and slow" — performing an action only as often as a human user would.

JavaScript bot detection can prevent access from illegitimate browsers. However, JavaScript bot challenges slow down site performance because the app has to verify each request at the vendor's origin, leading to a poor end user experience. It's also a deployment headache for your IT and security teams, who have to manage and secure third-party JavaScript libraries.



Multi-factor authentication (MFA) can help protect against unauthorized logins when bots attempt to use legitimate user credentials. However, it simply doesn't work for the majority of bot use cases — and it also adds friction to your user experience.

MYTH #5

Since bot attacks are so varied, I should build my own bot management tools.

In view of the sophistication of today's bots, and of the precise individualized targeting of many bot attacks, a purpose-built bot management solution might appear to be the wisest choice. But while an internally developed solution may prove highly effective in the immediate term, it will require costly maintenance and tedious upgrades from in-house experts in order to remain effective.

Additionally, bad bots continue to evolve in response to every thwarted attack, modifying their attack patterns, refining their mimicry of human users, and learning to evade today's most intricate security tools. That means your purpose-built bot solution would require constant fine-tuning of rules and policies to stay ahead of tomorrow's bot threats.

And ultimately, even the most elaborate in-house bot solution would have to stand alone. You would be limited to predicting bot attacks based on your own internal data and analyzing suspicious activity patterns using outdated algorithms. As a result, your purpose-built solution would register many false positives, negatively impacting your legitimate users' on-site experience.

Conclusion: Attributes of the ideal bot management solution

An effective bot management solution should combine the best attributes of all the tools and approaches listed above. It should leverage global threat intelligence at scale and use machine learning to perform real-time behavior analysis of site traffic, blocking bad bots while learning to recognize them even more rapidly in the future.

On a practical level, an ideal bot solution should be easy to deploy and manage, without demanding in-house expertise, costly maintenance, or ongoing manual adjustments. It should generate low false positives, accurately blocking bad bots without negatively impacting real users or helpful bots. On the whole, it should proactively improve and streamline your on-site experience.

Cloudflare Bot Management delivers on all these specifications. It leverages threat intelligence from over 25 million online properties to analyze user behavior, along with machine learning trained on a curated subset of hundreds of billions of requests per day, and fingerprinting collected from millions of sites and apps. This enables Cloudflare to proactively detect anomalies in user traffic and accurately score every request's likelihood of coming from a bad bot — safeguarding your users' experience while keeping your site bot-free.

Visit www.cloudflare.com to learn how to accelerate and protect your website.

Footnotes

[1] Cloudflare, "What Is Bot Traffic?", Cloudflare Learning Center, Accessed March 4, 2020

[2] Cloudflare, 5 BEST PRACTICES: Preparing Your Ecommerce Site for Maximum Holiday Success

[3] Barrett, Brian, "The Likely Reason Disney+ Accounts Are Getting Hacked," Wired.com, November 20, 2019:gg g -z vz

[4] Alina Bizga, "U.S. retailer J.Crew reveals 2019 security incident to customers," Security Boulevard.