kasada

WHITE PAPER

The Business Case for Stopping Malicious Bots: How Better Bot Management Maximizes ROI

Introduction

Whether or not you currently have a bot management solution in place, you might think that the only thing it's good for is protecting your online channels from automated attacks. But you'd be wrong. While it's true that defending against malicious automation is its primary function, an effective bot management solution also addresses the financial impact of bot attacks. That's important, because if you are still serving bot traffic, you are spending money on infrastructure, systems, tools, and personnel you shouldn't have to and you are also losing revenue. This white paper looks at the blight of bot traffic and the dire consequences it has on an organization's costs and competitiveness. We'll also dive into how a superior bot management approach that stops malicious bots from the first request drives down those costs.

The Blight of Bot Traffic

Traffic to your online channels is likely increasing, with everyone working, shopping, and living online these days. But if you look at that traffic, you will see that not all of it is human; in fact, research has shown that less than two-thirds of Internet traffic is generated by actual people—the rest is automation, and not just the good kind like web crawlers, but downright malicious automation. In fact, a whopping quarter of all Internet traffic comes from bad bots.

You are likely aware of the havoc these malicious bots can wreak—account takeover, carding, credential abuse, price scraping, and other types of data, login, and scraping fraud.

That's why many companies today deploy bot management tools to mitigate these kinds of automated attacks. However, because of the way these bot solutions are designed, they aren't entirely effective against stopping bots.

Most bot management solutions look at historical data (such as checking whether traffic is coming from a known bad address) or analyze behavior (for example, acting like a non-human by making more requests per time period than humanly possible). The problem is that attackers change their methods to avoid detection, and most solutions constantly need to adapt by adding new rules based on learnings from the past.

Such rule-dependent approaches operate under the premise that traffic is innocent until proven guilty. This approach is fine until that assessment is incorrect, in which case the damage is already done. Revised attack methods and bots directed from compromised, legitimate devices often circumvent their way around defenses. Would you let an unknown person into your house without knowing whether they were friendly or not? Of course you wouldn't—you would measure them up first to understand whether or not they posed a threat before you ever let them cross the threshold. The result is a frustrating cat-and-mouse game, with inconsistent anomaly detection, short-lived efficacy, and high internal support burden.

Unfortunately, the impact of letting all traffic in has consequences not only for your security posture but also for your budget. You are paying for all that non-human traffic to your online channels—an operational and infrastructure expense that will never yield leads, sales, or real customer engagement. Adding to this cost is the fact that traditional solutions are expensive to install and maintain, and need human oversight, impacting your budget further.

The bottom line is that with ineffective bot management solutions that let in bot traffic, your online channels will likely:

- Experience downtime that costs you revenue
- Suffer from latency that decreases your conversion and engagement rates
- Rack up costs related to operations and infrastructure
- Require expensive personnel to monitor and maintain these solutions

How a Superior Approach to Bot Mitigation Eliminates Bots and Also Drives Down Costs

What if there were a way to stop bot traffic before it ever got through the front door, one that offered superior protection for a low total cost of ownership—and eliminated all the additional costs associated with bad bots? Such an approach would:

- Protect online revenue by eliminating bot-driven latency and downtime
- Reduce unnecessary overhead by rightsizing traffic to authentic human user traffic only
- Eliminate costs associated with other solutions and the human resources needed to maintain them
- Avoid lock-in to products and services, such as CDN, allowing for more flexible terms and negotiation

Let's take a closer look.

Protect Online Revenue

When we look at ways to protect your online revenue from the ravages of bot traffic, it's clear to see that keeping your online channels up and running and providing a positive user experience are two of the most important factors.

KEEPING THE SITE UP AND RUNNING

There is nothing more critical to protecting online revenue than ensuring that its channels remain operational. But bots can overrun servers, causing sites to crash at worst and slowing sites to barely usable at best. What does that kind of impact look like? Here is a hypothetical example: let's say you run a popular e-commerce site that generates $100 million in revenue per year—that's $274K per day. If bots overwhelm your servers and take your site offline for just two days, you have easily lost a minimum of $548K in online revenue. If that same business protects just 50% of its traffic with a bot management solution, that's $50 million the organization can count on and not lose to downtime caused by bots, $137K per day.

ENSURING A POSITIVE USER EXPERIENCE

Bots can slow down sites, which impacts conversion rates. In fact, one popular statistic is that for every 100ms delay, conversion rates drop 7%. Let's say you run the $100 million e-commerce site mentioned above and every day there is a bot-driven delay; that adds up to thousands of dollars in potential lost revenue whose cost over time is almost incalculable. But that's the risk you run by not stopping bots at the front door.

As well, research shows that one out of every 10 users who have a bad experience won't return, whether that's from the site being unavailable or just frustratingly slow. So any online business impacted by bots has likely lost 10% of its future customers, impacting revenue and profits long into the future. But with an effective bot management solution that keeps the site up and running, such a business can look forward to serving all of its customers and reliably delivering on its forecasts from online channels.

Reduce Unnecessary Overhead

Another good way to measure the ROI of an effective bot management solution is to measure the bottom line; that is, to understand how certain costs decrease with the elimination of synthetic traffic. This takes into account how much traffic each of an organization's online channels (web, mobile apps, APIs) receive each month, how much of that traffic is synthetic, and its related costs (operations, infrastructure, personnel), such as bandwidth costs, authentication and credit card authorization charges, and more.

For example, in the hospitality industry, research shows that bad bots can make up 80% of traffic. By offloading bot traffic from hitting infrastructure in the first place, companies can save tens of thousands of dollars per month, easily.

Moreover, modern bot management solutions that don't rely on people to oversee their operation, saves on the cost of one or two security personnel FTEs every year, close to $100-150K per year. In addition to those personnel cost savings, companies will also save on help desk costs. By diverting bots that would take over accounts, companies no longer need the headcount for password resets or the charges related to account recovery. If our hypothetical e-commerce business would normally need 3 FTEs at $50K annually, and spend 50 cents per event for 300,000 account recovery events, they would now save $300K. In addition, they don't need personnel to manage chargebacks for bot-generated credit card fraud. If our business normally needs 2 FTEs at $50K per year for that work, that's a savings of another $100K. You can see these savings add up fast!

When traffic is right-sized through the elimination of synthetic traffic, companies will see web traffic decrease to levels that represent actual levels of human traffic and usually gain additional benefits. "In one case, a company that eliminated bad bot traffic saw web traffic decrease by 66%, while their website page speed and performance doubled...," according to Cybersecurity Europe.

The Price of Intangibles

All of these financial impacts can be measured in dollars, but intangible implications cannot. For example, how do you put a price on:

- Your brand reputation, which is diminished in a data breach, sometimes never to be restored
- The potential cost of litigation and fines for not properly securing user information
- The inconvenience and frustration wrought on customers by account takeover and carding and the resulting loss of loyalty to your business
- The value of your intellectual property, whether that be competitive pricing, information, or other content scraped by bots that you can no longer monetize or use for your own advantage
- The relentless drag on your employees as they scramble to hunt down and stop bots

The bottom line? Dealing with bots is expensive for the company, its employees, and customers. There has to be a better way.

ITEM	NOTES	ESTIMATED COST SAVINGS
2 days of downtime annually	$274K per day	$548K
Security personnel to monitor bot solution	1-2 FTEs	$100-150K
Help desk for password reset/account recovery	3 FTE headcount at $50K per year	$150,000
Tech cost for password reset/account recovery	300,000 accounts at $0.50 per account	$150,000
Infrastructure costs	Bandwidth	Reduced by 20-80% depending on amount of bot traffic stopped
Case management for credit card chargebacks	2 FTE headcount at $50K per year	$100K per year
Brand and reputation protection		PRICELESS
TOTAL POTENTIAL SAVINGS		**A minimum of $1,048,000 annually**

Figure 1: Hypothetical Example of a $100 Million E-Commerce Company - Additional Savings Derived from Better Bot Management, Compared to a Legacy Rules-Dependent Approach

Introducing Kasada

Kasada has pioneered a better approach to bot management that flips the bot mitigation approach on its head by assuming all traffic is guilty of being a bot until proven human. Implemented inline behind a CDN of your choice, Kasada can be deployed within minutes and stops bot traffic from the very first request, keeping them busy with an increasingly difficult browser-based proof of work designed to use up compute cycles for malicious bots. This makes attacks impractical to automate at-scale and financially unviable, as the cost of the attack far exceeds the value of the target. Instead of relying on rules based on context from past attacks, Kasada approaches bot management by finding the immutable evidence that's present whenever bots pretending to be humans interact with your applications. Because Kasada removes bot traffic with the highest level of accuracy in the industry, coupled with proprietary obfuscation to appreciably complicate reverse engineering, companies minimize infrastructure costs by rightsizing traffic to actual human users.

Simply put, Kasada is an easy-to-implement, low-cost, low-maintenance solution that unequivocally demonstrates immediate and long-term efficacy on web, mobile, and API channels while offering a frictionless customer experience without requiring CAPTCHAs. This gives companies the best of both worlds: efficacy AND simplicity so companies can quickly and easily protect their digital properties.

Business Benefits of Better Bot Management

Because companies have a better sense of how much traffic they actually need to serve, they can right size their backend servers, as well as preserve server and compute capacity for actual service delivery. In addition, our customers have:

- Reduced the need for manpower on reactive bot mitigation by 70%
- Increased conversion rates by nearly 60%
- Decreased TCO from a FTE to just an hour a week
- Reduced automated quotes from 5-10% of quotes to 1% of whitelisted traffic
- Eliminated payment fraud at the gateway by turning away bot traffic
- Protected pricing IP by foiling reverse-engineered price scrapers
- Increased ROI by reducing unnecessary infrastructure
- Yield more accurate insights for enhanced forecasting and capacity planning
- Reduced latency, improving page speed and increasing time on page

All of this is in addition to stopping unwanted bot traffic, such as account takeover attempts, credential stuffing attacks, price scraping, and more, every day around the world. So not only do customers get better protection with Kasada's approach to bot management, they also reduce infrastructure and other costs while better serving their own customers, leading to improved conversions and loyalty.

In summary, bot management is more than a tool used by security teams. By making bot management more accurate and far easier to benefit from, Kasada is helping business executives grow their revenue, increase operating margins, and improve their competitiveness. Customers see quick ROI—those companies that are new to bot management gain all the benefits of eliminating unwanted bad bot traffic, and those that move from rule-dependent solutions also benefit greatly as a result of Kasada's elegantly simple and superiorly effective approach.

Would you like to see for yourself how the Kasada bot management solution stops bots in their tracks, and delivers value almost immediately with a quick ROI? Please request a demo today.

About Kasada

Kasada provides the only online traffic integrity solution that accurately detects and defends against bot attacks across web, mobile, and API channels. With Kasada, internet control and safety is given back to human beings by foiling even the stealthiest cyber threats, from credential abuse to data scraping. The solution invisibly stops automated threats while inflicting financial damage to attackers, destroying their ROI. With the ability to onboard in minutes, Kasada ensures immediate and long-lasting protection while empowering enterprises with optimal online activity. Kasada is based in New York and Sydney, with offices in Melbourne, San Francisco, and London. For more information, please visit www.kasada.io and follow us on Twitter, LinkedIn, and Facebook.