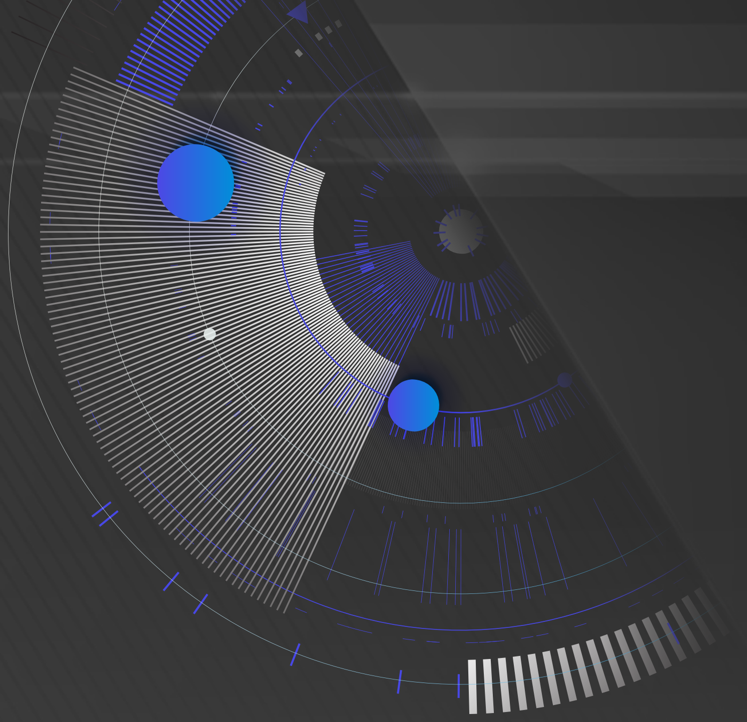
kasada



2021

STATE OF BOT MITIGATION

Introduction

It’s well-known that bots are detrimental to your business; however, no one has explored the effectiveness of bot mitigation solutions after they have been deployed in various organizations - not until now, that is.

Conducted by an independent research firm, this first of its kind survey covers the state of bot mitigation *exclusively* from the perspective of organizations already using anti-bot solutions from over 200 respondents.

The 2021 State of Bot Mitigation survey finds that despite spending up to millions of dollars on bot mitigation and bot management solutions, companies are struggling to stay ahead in the fight against malicious bot attacks.

Research Methodolgy:
Kasada commissioned Atomik Research to conduct an online survey of 204 U.S. security and technology professionals responsible for mitigating bots. Sample participants work within IT departments of organizations that employ 250 or more people. All organizations surveyed currently have bot mitigation solutions in place. The survey was conducted in August 2021. Atomik Research, a part of 4media group, is an independent market research agency.

Despite Having Implemented Bot Mitigation, Companies are Losing the **WAR AGAINST BAD BOTS**

100% of the survey respondents are security or tech professionals that work at an organization which has invested in an anti-bot solution.

A quarter of respondents say that on average a single bot attack costs their organization **$500,000** or more.

76% say they are either playing a game of cat and mouse or feel like it's an impossible balancing act to keep up with evolving bot threats.

Bad Bots Cost Organizations Hundreds of Thousands to Millions of Dollars

83%

83% say that their company has experienced one or more bot attacks within the past year.

Of those who experienced at least one bot attack within the 12 months:

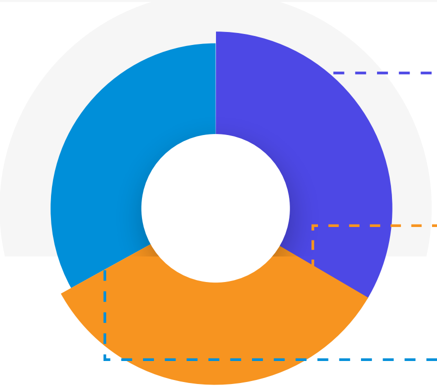
- **77%** say they lost **6%** or more of revenue due to bot attacks
- **39%** say they lost **10%** or more of revenue

77% of companies spent $250,000 or more on mitigating bot attacks within the past year, while more than one in four (27%) spent **$1 million** or more.

$1M

Buyer Beware: High Total Cost of Ownership

A resounding **66%** of the total funds necessary to fight bot attacks are attributed to the ongoing management, maintenance, and post-event remediation of their bot mitigation solution - as opposed to the cost of the solution itself.



34% **An anti-bot solution**

Respondents report that their organization allocated 34% of their funds to an anti-bot solution within the past year.

34% **Ongoing management and maintenance**

34% of their funds were allocated to the ongoing management and maintenance of fighting bot attacks.

32% **Post-event remediation**

32% of their funds were allocated to post-event remediation.

Stopping Bot Attacks is a C-Level Imperative, Companies Plan on Spending Even More Next Year

80%

4 in 5 (**80%**) respondents say their executive team asked about automated and bot attacks within the last six months.

87%

The vast majority **(87%)** of tech and security pros see effective bot mitigation as a competitive advantage.

63%

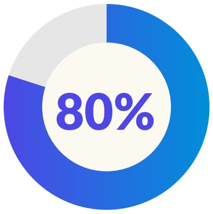
Almost two-thirds (**63%**) expect their company's spending on bot mitigation and prevention to increase over the next 12 months.

Automated Threats are Increasingly Difficult to Detect, Even With Anti-Bot Solutions in Place

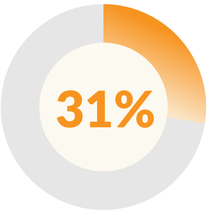
Respondents indicate that the most difficult types of bot attacks to stop are:

- Credential Stuffing/ ATO
- Web Scraping/ Price Scraping
- Denial of Inventory
- CAPTCHA Defeat
- Fake Account Creation
- Application DDoS
- Carding/ Cracking

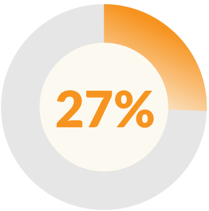
Most Companies Aren't Prepared to Defend Against Sophisticated Bot Attacks



Most respondents **(80%)** say bots are becoming more sophisticated and difficult for their security tools to detect and stop.

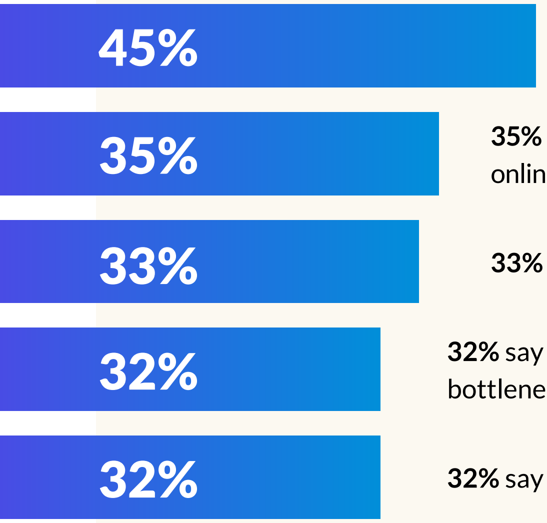


Less than one-third **(31%)** are very confident in their ability to detect new zero-day bots with their current anti-bot solution.



Only **27%** of respondents, who all invested in bot mitigation/bot management solutions, have no problems detecting bot attacks.

The Negative Impact of Bad Bots is Significant Across the Business



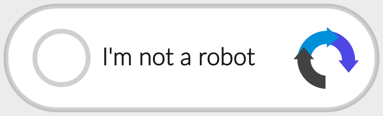
45% say bot attacks resulted in more website, software, and/or IT crashes.

35% say bot attacks resulted in brand or reputational damage, or reduction in online conversions, or more frequent data leaks.

33% say bot attacks resulted in an increase in infrastructure costs.

32% say bot attacks resulted in an increase in operational or logistical bottlenecks.

32% say bot attacks resulted in a poor customer experience.



72% believe the customer experience on websites would be improved by the elimination of CAPTCHAs.

An Enormous Amount of Time and Resources Are Wasted

Configuration

65% say it takes one week or more to configure and optimize their anti-bot solution prior to deployment.

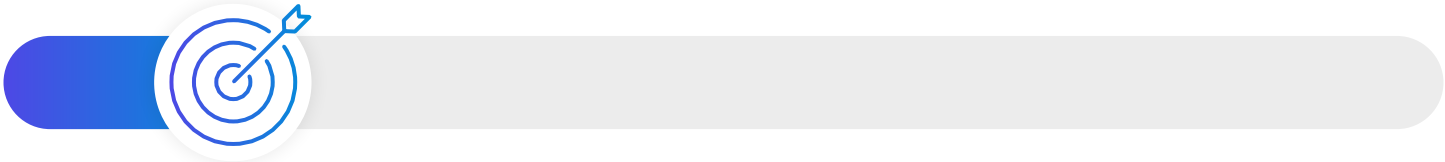
Management

92% say they spend 25 or more hours each month managing and/or maintaining anti-bot rules and policies.

Remediation

63% say it takes one week or more to remediate a successful bot attack across multiple roles or departments.

Even With All of the Time, Resources, and Money Spent, Anti-Bot Solutions Are Not Providing Long-Lasting Protection



15%

Only **15%** of companies report that their bot mitigation or bot management solutions retained effectiveness a year after initial deployment.

Bot Attacks Aren't New **BUT THERE NEEDS TO BE A NEW APPROACH**

Bot mitigation is complex, but your solution shouldn't be.

Automated threats and bot attacks are a huge problem for organizations that's only getting worse - even for those who have invested in anti-bot solutions.

More has changed in the automation and bot ecosystem over the past two years than the prior decade.

There needs to be a simple and more effective way for companies to defend against these modern threats.

85% of our customers were using other bot mitigation providers prior to contacting us.

We stop bot attacks others can't.

Learn how: kasada.io.

kasada