kasada

2023 State of Bot Mitigation

ANNUAL REPORT

Conducted by an independent research firm, this is the 3rd annual survey that covers the state of bot mitigation exclusively from the perspective of CISOs, CTOs, and technology professionals who are already using anti-bot solutions at their companies.

The findings in this report shed light on the pressing need for effective bot mitigation strategies. The 2023 report explores the challenges companies are facing with bot attacks and automated fraud, including the financial and reputational impact and gaps in existing defenses.

Research Methodology

Kasada commissioned Atomik Research to conduct the 2023 State of Bot Mitigation study in August and September 2023. The survey involved **206 U.S. security, fraud, risk, engineering, IT ops, and technology professionals** responsible for mitigating bots. Atomik Research, a part of 4media group, is an independent market research agency. The participants were selected from organizations with 250 or more employees, all of whom have existing bot mitigation solutions in place.

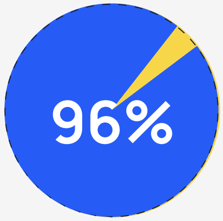
Executive Summary

Despite substantial investments, companies continue to spend more money and time to mitigate automated threats and malicious bots. Over the past year, an alarming 63% of organizations experienced bot attacks. This number is expected to rise, with 76% anticipating increased spending on bot mitigation in the coming year. Half of respondents suffered revenue losses of over 10% due to account fraud.

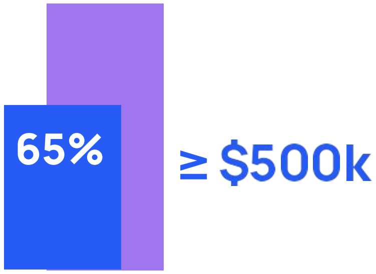
The 2023 findings emphasize the urgency for a paradigm shift in bot mitigation strategies, urging organizations to adopt more efficient and proactive approaches to not only protect their financial interests but also ensure a seamless and secure digital environment for their customers.

Key Findings

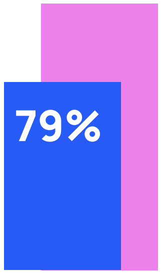
All of the survey respondents are CISOs, CTOs, security, IT, fraud, engineering, or technology professionals who have invested in at least one anti-bot solution.



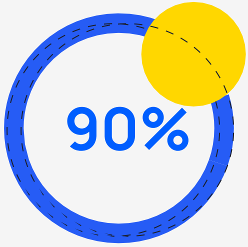
96% of companies using bot management solutions reported revenue losses due to bot attacks.



65% of organizations spent **$500,000** or more in the past year to mitigate bot attacks.



79% say bots are becoming more sophisticated and challenging for their security tools to detect.



90% of respondents say their executive team is concerned about bot attacks and AI-driven fraud.

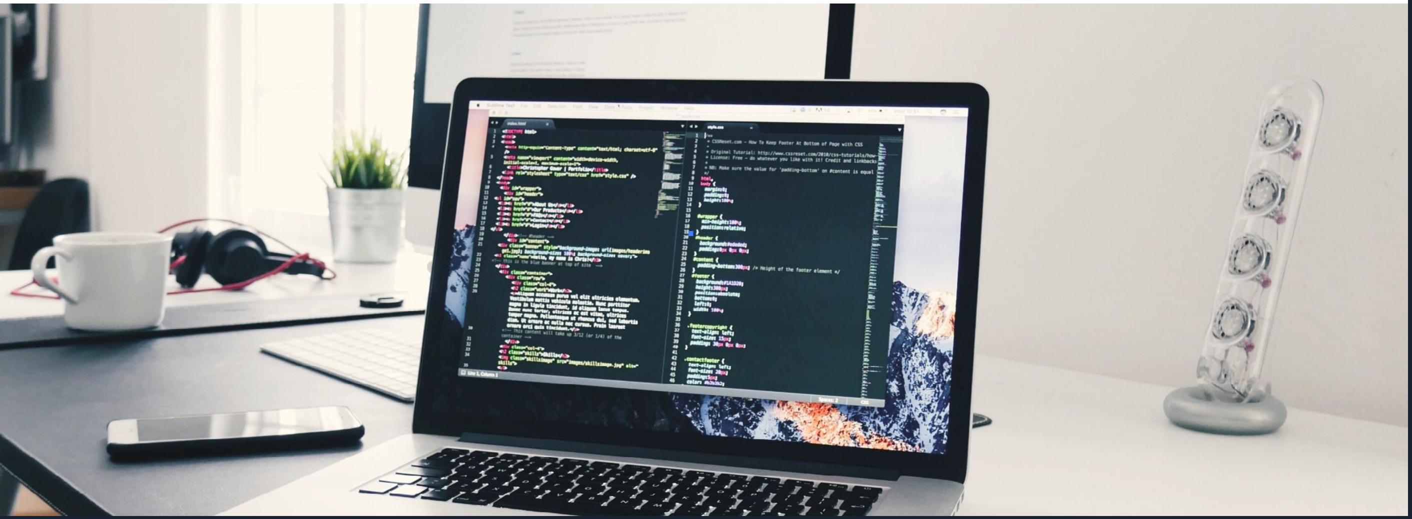
Companies Struggle to Keep Up with Increasing Adversary Sophistication

Nearly 4 in 5 (79%) respondents say bots are becoming more sophisticated and difficult for their current security tools to detect.

According to the survey results, **the seven most difficult types of bot-driven attacks to detect and stop in 2023** are: account takeover/ credential stuffing, API abuse, CAPTCHA defeat, Distributed Denial of Service (DDoS), fake account creation, SMS fraud, and web scraping.

User profile information (46%), customers' personal identifying information (44%) and employees' personal identifying information (42%) were reported as the **top organizational data stolen by attackers using bots and malicious automation**.

These use cases emphasize the critical need for proactive and robust bot mitigation strategies to protect sensitive data and the integrity of digital operations.



The 7 Most Difficult Bot Attacks to Detect and Stop

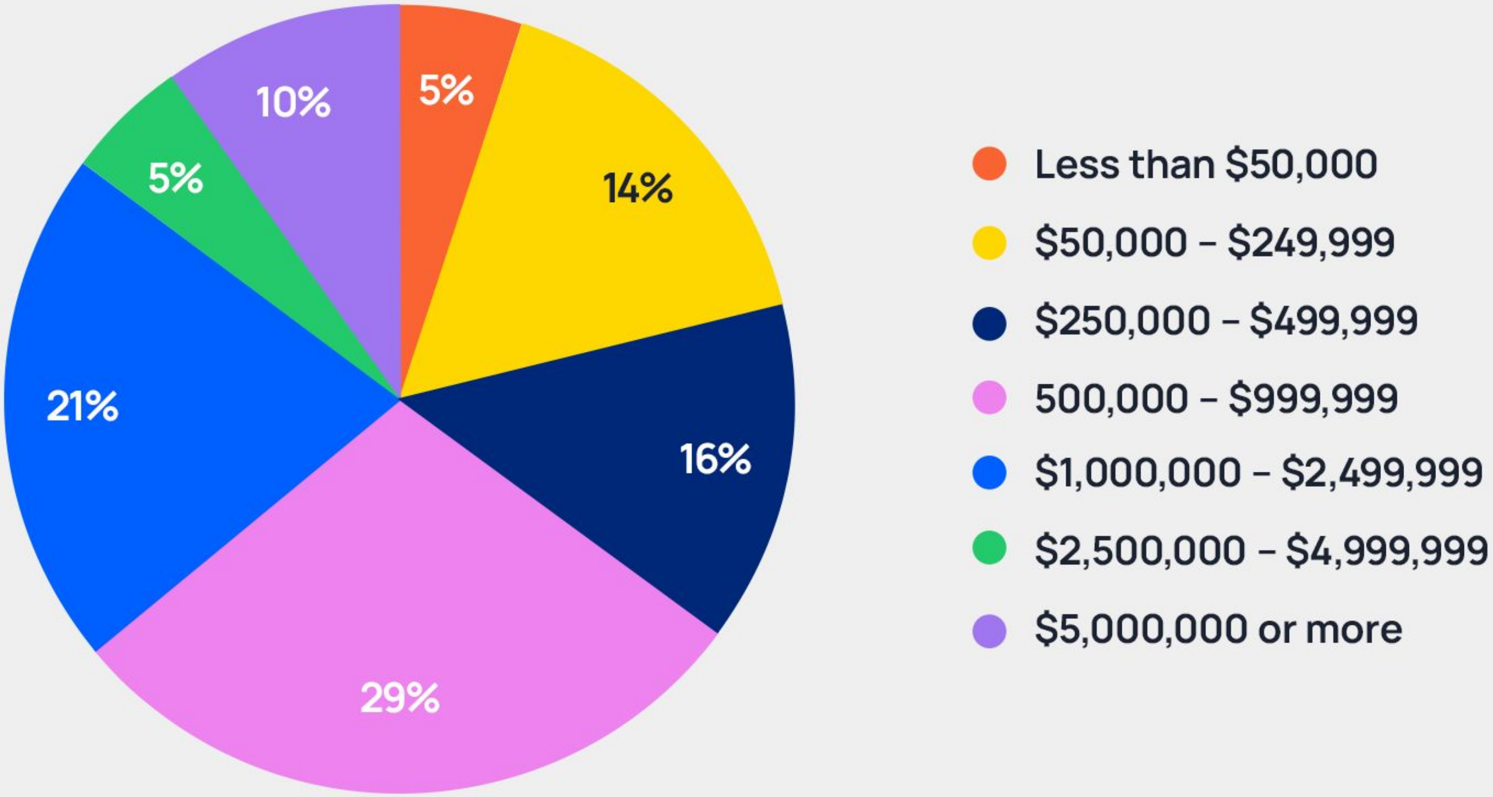
- Account Takeover/ Credential Stuffing
- API Abuse
- CAPTCHA Defeat
- Distributed Denial of Service (DDoS)
- Fake Account Creation
- SMS Fraud
- Web Scraping

The True Cost of Bot Attacks

According to the survey, 65% of respondents spent $500,000 or more mitigating bot attacks over the past 12 months.

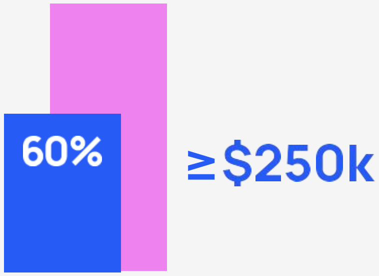
The vast majority (76%) expect their company's spending on bot mitigation to increase over the next year.

Breakdown of How Much Bot Attacks Cost Companies (Past 12 Months)

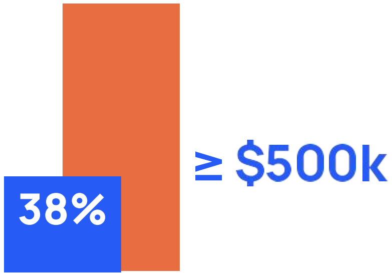


The True Cost of Bot Attacks

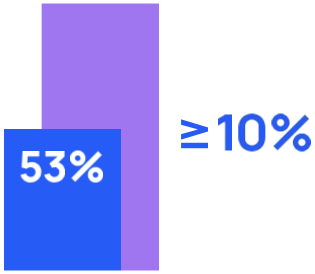
Nearly two-thirds (63%) say their companies experienced at least one bot attack in the past year, with 3 in 5 (60%) saying a single bot attack costs their organization $250,000 or more.



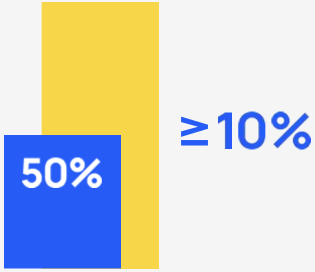
60% say a single bot attack costs their organization **$250,000** or more, up from 44% in 2021.



38% say a single bot attack costs their organization **$500,000** or more, up from 25% in 2021.



53% of organizations lost **10%** or more of revenue due to web scraping within the last 12 months, up from only 7% of orgs in 2021.

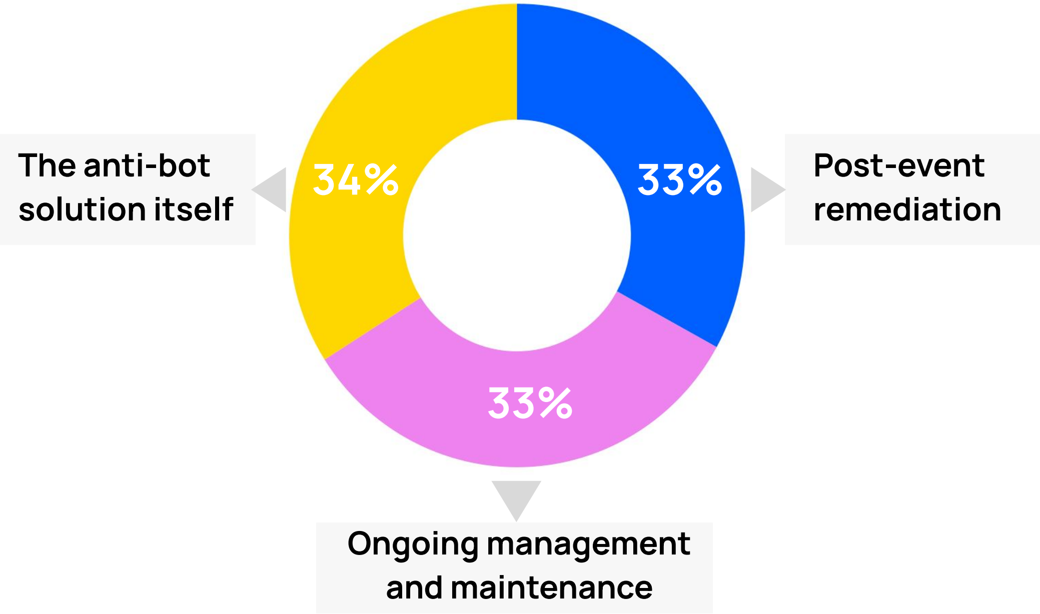


50% of organizations lost **10%** or more of revenue due to account fraud within the last 12 months, up from only 6% of orgs in 2021.

Anti-Bot Budget Allocation

Organizations are still allocating a majority of their bot management budget (66%) to ongoing management and remediation vs. the cost for their bot management solution itself (34%).

Allocating a significant portion of the bot management budget to ongoing maintenance and remediation indicates a reactive approach to dealing with bot attacks. This suggests that a considerable amount of resources are being used after an attack has occurred, most likely due to limitations and ineffectiveness of their existing bot management solutions.



Only 19% of respondents say their bot mitigation solution retained its effectiveness for 1 year or more after initial deployment.

Response Times

The statistics about the time taken to mitigate and resolve a successful bot attack are concerning. A majority (55%) of companies report that it takes more than 7 days to respond effectively to a bot attack. One-third (34%) take over 10 days to address and mitigate a bot attack.

This delay in response could lead to substantial damage, including financial losses, compromised data, and reputational harm.

Solution Effectiveness

The fact that only 19% of respondents believe their bot mitigation solution retains its effectiveness for a year or more after initial deployment raises questions about the longevity and adaptability of their current solutions. It highlights the need for more robust, flexible, and future-proof bot defense that can evolve and effectively counter the changing tactics of bots over time.

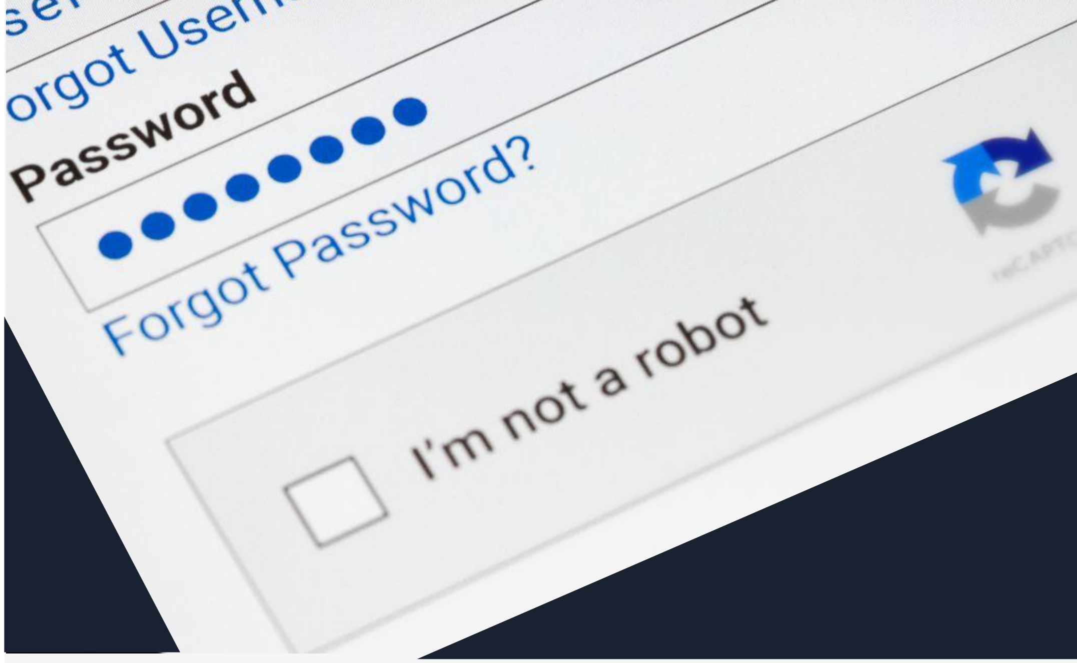
The CAPTCHA Conundrum: Striking a Balance Between Security and User Experience

While a significant portion of organizations (75%) use a CAPTCHA, a substantial number (45%) find CAPTCHA defeat to be a challenging attack to stop. Therefore, despite being widely used for distinguishing bots from humans, CAPTCHAs are not entirely effective in preventing sophisticated bot attacks.

About half (51%) of respondents are worried about the increasing sophistication of bots capable of bypassing CAPTCHAs using AI.

Additionally, over 3 in 4 (77%) agree that eliminating CAPTCHAs would significantly enhance the user experience. This underscores the negative impact of CAPTCHAs for end-users and the need for providing an optimized and more secure customer experience overall.

81% say their customers would have an improved and more fair user experience if they weren't competing against bots.



A majority (89%) of respondents foresee AI-driven fraud as a threat to their organization over the next 12 months. This statistic emphasizes the evolving landscape of cyber threats and the growing concern over the potential use of AI by malicious actors.

As AI-driven fraud and sophisticated bot attacks continue to escalate, organizations must invest in advanced, adaptive bot mitigation solutions that can effectively combat these threats while preserving a seamless and enjoyable user experience.

Striking this balance is pivotal for companies to thrive in the face of evolving cyber threats and ensure brand loyalty in an increasingly digital world.

> Here's an easy way to look at ROI: an attacker gaining access to a single guest account would be unacceptable to us. The first time Kasada prevented an account takeover event, we saw value. We see very regular updates and new features added to the product – indicating Kasada's commitment to continuous improvement – and full transparency on pricing."
>
> - **Benjamin Vaughn**
>   Vice President and CISO
>   Hyatt

Get Started with Kasada

Companies are recognizing the need for dynamic solutions to stay ahead of sophisticated bot-driven attacks in 2023 and beyond. The competitive, complex, and changing digital environment demands agility in stopping automated threats at speed and scale.

With an effective and user-friendly approach, Kasada's proactive platform adapts as rapidly as attackers do. This represents a profound paradigm shift in the industry, rendering automated attacks financially unviable. As a result, **Kasada's customers increase their return on investment (ROI) and dramatically reduce their total cost of ownership (TCO) for bot mitigation.** Unlike traditional static or CAPTCHA-based bot detection methods, Kasada dynamically changes its defenses to provide long-lasting protection across websites, APIs, and mobile apps while ensuring a frictionless digital experience.

85% of Kasada's customers transitioned from other anti-bot providers, highlighting the platform's effectiveness in stopping today's attacks. To discover how you can optimize protection for your revenue, customers, and brand – or to receive an assessment of your bot risk – visit kasada.io.

About Kasada

Kasada has developed a radical approach to defeating automated cyberthreats based on its unmatched understanding of the human minds behind them. The Kasada platform overcomes the shortcomings of traditional bot management to provide immediate and enduring protection for web, mobile, and API channels. Its invisible, dynamic defenses provide a seamless user experience and eliminate the need for ineffective, annoying CAPTCHAs. Our team handles the bots so clients have freedom to focus on growing their businesses, not defending it. Kasada is based in New York and Sydney, with hubs in Melbourne, Boston, San Francisco, and London. For more information, please visit www.kasada.io and follow on LinkedIn, Twitter, and Facebook.

kasada

Contact us:
enquiries@kasada.io
Australia: 1300-768-601
USA: 877-473-5073
kasada.io