kasada

# 2024 State of Bot Mitigation

**ANNUAL REPORT**

Conducted by an independent research firm, this is the 4th 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 showcase the extent of challenges companies face from bot attacks and automated fraud, the staggering financial cost, and impact of AI on this evolving threat to companies' revenue, business models, and reputation.

# Executive Summary

Despite substantial investments, companies are struggling to mitigate automated threats and malicious bots. Most have experienced bot attacks even with defenses in place, leading to revenue losses in the millions.

The 2024 findings urgently emphasize the need for a paradigm shift in bot mitigation - CAPTCHAs remain ubiquitous, yet bots solve them better than humans. AI raises the stakes by increasing the scalability and speed of traditional attacks and threatening a company's very existence by stealing intellectual property.

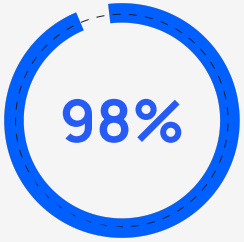
Organizations must adopt proactive, agile defenses that evolve as quickly as adversaries. This is the price of entry to safeguard businesses - and customers - in the years ahead.

# Research Methodology

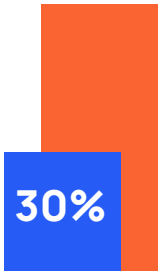
Kasada commissioned Atomik Research to conduct the 2024 State of Bot Mitigation study in June and July 2024. The survey involved **222 U.S. security, fraud, risk, engineering, IT ops, and technology professionals** responsible for mitigating bots. Atomik Research, a part of 4media group, is an independent market research agency. The participants were selected from organizations with 250 or more employees, all of whom have existing bot mitigation solutions in place.

# Key Findings

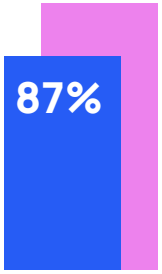
All companies surveyed have bot defense yet two-thirds **(63%)** experienced at least one bot attack in the past year - highlighting how quickly defenses can lose efficacy. Costs incurred from bot attacks can substantially cut into revenues.




**98%** of companies who experienced bot attacks lost revenue as a result.




**30% spent $1 million** or more to mitigate bot attacks in the past 12 months.




**87%** say their executive team is concerned about bot attacks and AI-driven fraud.


**Only 20%** report their new bot mitigation solution was still effective **after 12 months.**

# Keeping Up With Automated Threats is Becoming Harder

Nearly **6 in 10 (63%)** companies experienced a bot attack in the past 12 months despite having bot defense in place.

On average, companies used **at least two** bot detection solutions (67% use CDN-based defenses). Only **20%** of these organizations reported their solution was **still effective 12 months after** deployment, indicating that traditional bot defenses aren't agile enough to keep up with evolving threats.

Companies face a diverse threat landscape, with fake account creation and new account fraud being the hardest to stop **(56%)**. Additionally, one-third of companies are increasingly worried about **web scraping** and the abuse of **Large Language Models (LLMs)**, highlighting how quickly these new threats have become a significant and costly issue.

This data highlights the urgent need for proactive and strong bot mitigation strategies to safeguard customer data, protect intellectual property, and reduce operational costs.

## The 7 Most Difficult Bot Attacks to Detect & Stop

Account Takeover/ Credential Stuffing

CAPTCHA Defeat

Distributed Denial of Service (DDoS)

Fake Account Creation

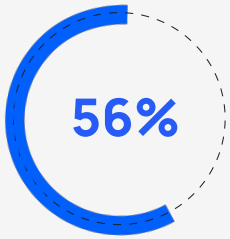
SMS Fraud

Web Recon / Malicious Scanners

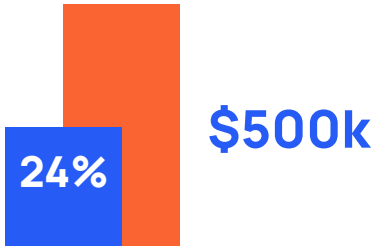
Web & Price Scraping

# The True Cost of Bot Attacks

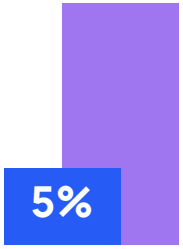
1 in 4 (**24%**) say a **single bot attack costs their organization $500,000 or more.** Worse, recovering from these failures and managing the solution far outweigh the cost of the bot defense itself.



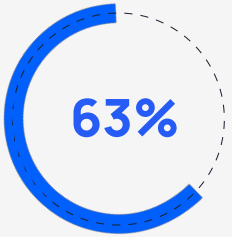

**56% of respondents spent $500,000 or more** mitigating bot attacks over the past 12 months.




**24%** say a single bot attack costs their organization **$500,000** or more.




1/3 report that Account fraud, SMS fraud, and web scraping each cost **5% or more of revenues**.

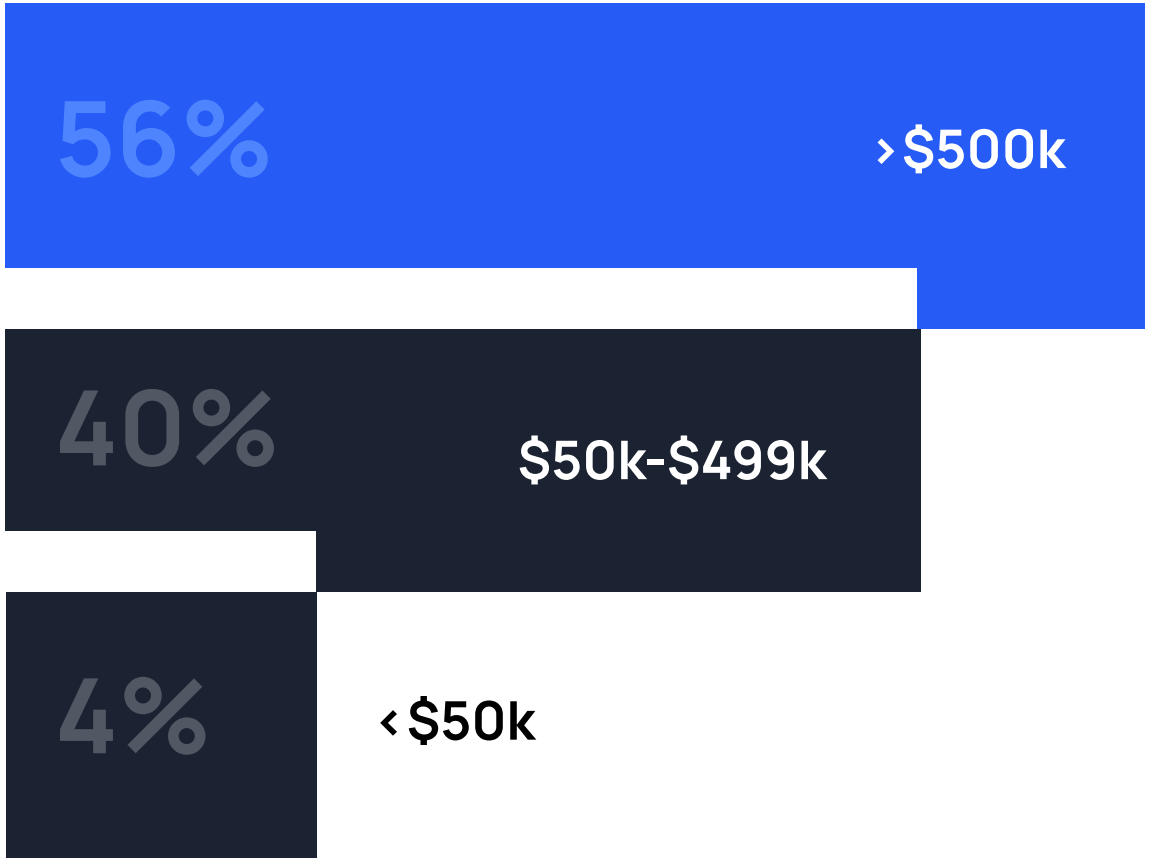



A staggering **63%** of bot management budgets go to solution maintenance and fallout from attacks that get through, dwarfing the 37% spent on the solution itself.

# The True Cost of Bot Attacks

According to the survey, **56% of respondents spent $500,000 or more** mitigating bot attacks over the past 12 months.

## Budget spent to mitigate bot attacks in the last year:

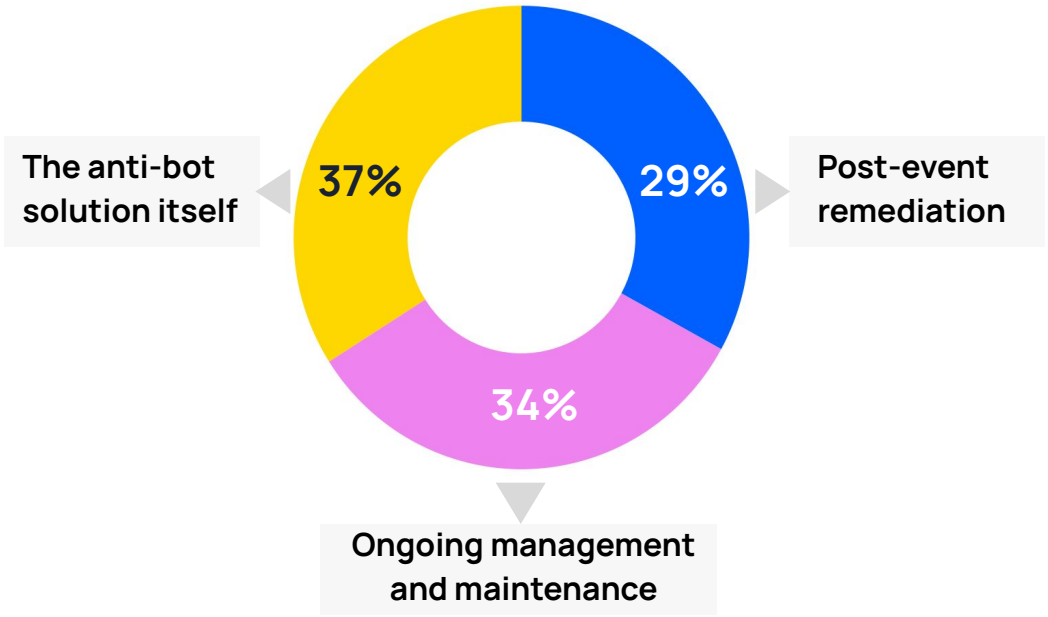



**72% of mid-size businesses** reported costs of $500k or more, highlighting the disproportionate burden for this group.

# Anti-Bot Budget Allocation

Organizations are still allocating a majority of their bot management budget **(63%)** to ongoing management and remediation vs. the cost of their bot management solution itself **(37%)**.

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 considerable resources are deployed after an attack has occurred, most likely due to the limitations and ineffectiveness of their existing bot management solutions.




**30% of companies spent $1M or more to mitigate bot attacks in the past 12 months.**

Breakdown by company size:

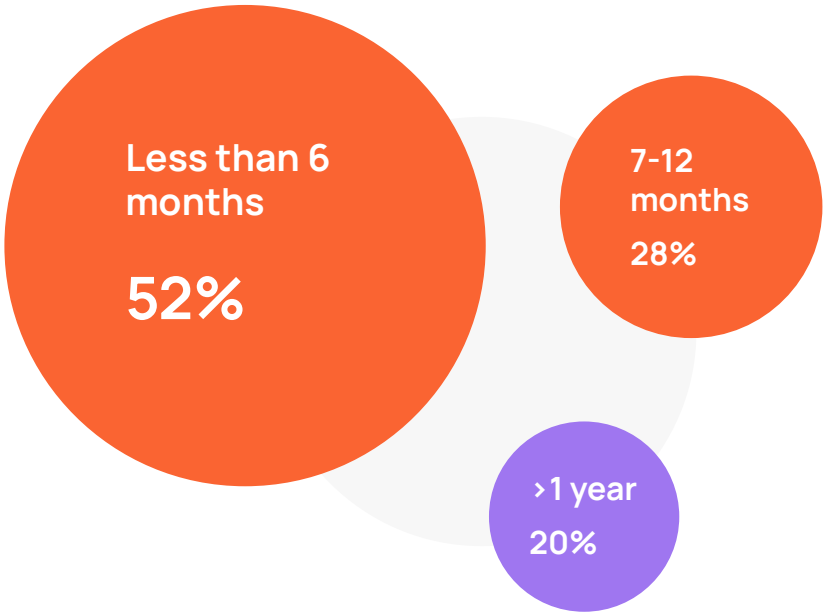
**18%** - Small (250-999 employees)
**39%** - Midsize (1K-4.9K employees)
**36%** - Large (5K+ employees)

# Solution Effectiveness

The fact that only **20% 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.

How long bot mitigation solution remains effective post-deployment:




**79% are likely to switch to a more effective bot mitigation provider, suggesting widespread dissatisfaction with current solutions.**

# Likelihood to Switch Bot Mitigation Providers

Bot mitigation rarely becomes “shelfware” - it has to constantly prove it’s effective. What worked at deployment fails in six months (or sooner!) if the defense has failed to keep up.

This becomes painfully clear when ATOs increase, infrastructure costs rise, website performance suffers, and conversion rates drop - among many other consequences.

**Strong bot mitigation forms the bedrock of solid business performance,** which is why companies are so willing to jump for better efficacy.

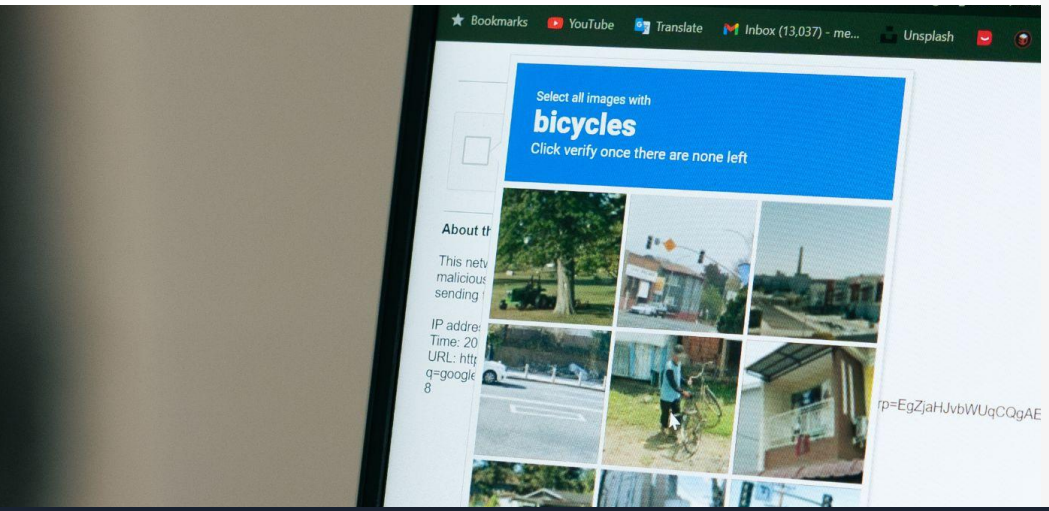
In choosing a new solution, companies should look for a vendor with **flexible integration options that acts as an extension of their team.** Responsiveness and willingness to stay “in the trenches” long after the contract is signed is key to long-term success.

# Despite Doubts, CAPTCHAs Hang On

While a significant portion of organizations (**77%**) use a CAPTCHA, **73%** simultaneously believe the user experience would be improved if these were gone.

Nearly half (**45%**) also find CAPTCHA defeat to be a challenging attack to stop. Therefore, despite being widely used to tell bots from humans, CAPTCHAs **have trouble preventing sophisticated bot attacks.**

Signaling trouble ahead, over half (**57%**)are worried about increasingly sophisticated **bots using AI to bypass CAPTCHAs** - making an already difficult problem worse.




**73% of respondents believe the user experience would be improved if CAPTCHAs were gone.**

# Why CAPTCHAs Don't Work

Besides irritating customers, **CAPTCHAs lower conversion rates** as frustrated customers abandon the buy flow, hurt website UX, and tarnish a brand.

They also do a poor job of telling humans from bots:

- Research shows bots are actually better than people at solving CAPTCHAs
- CAPTCHA solver services are cheap and readily available online - to literally anyone
- CAPTCHAs give attackers an "out." Once they solve it, they are labeled legitimate
- Bots are masters of disguise, faking behavior (like mouse clicks) to appear human and fool defenses

# AI Fuels a New Generation of Sophisticated Attacks

AI increases the speed, velocity, and ease with which attacks are carried out. It's no surprise that **99%** of companies are concerned about AI-driven threats, such as data breaches due to LLM prompt injection increased frequency of majorly disruptive attacks.

AI is also becoming central to business operations. As it embeds in processes and customer-facing applications, it will be critical for companies to **protect their AI functionality and APIs** from abuse.

Finally, AI-supported defenses can be effective, but Kasada cautions against treating AI is as a silver bullet because it can be tricked with data poisoning. **Ensuring AI is acting on authentic, trusted data** - and is combined with human insight - is key to maximizing its potential.

"We've been in the trenches learning how to **protect our AI workloads from abuse,** such as denial of wallet attacks and prompt injection… AI APIs are orders of magnitude more expensive per request than your traditional APIs, and so abuse can be much more costly."

*-Kasada customer Malte Ubl, CTO, Vercel*


## AI-driven threats businesses are most worried about

**57%** Sophisticated bots developing ability to bypass CAPTCHAs.

**57%** Generative AI enabling criminals to pull-off complex attacks with more ease.

**56%** Increased frequency of advanced attacks majorly disrupting our organization.

**54%** Data breach due to a successful LLM (Large Language Model) prompt injection attack.

**52%** Generative AI democratizing the use and ease of creating sophisticated bots.

**49%** Scammers leveraging deepfakes to gain access to sensitive information.

**45%** Fake accounts becoming harder to differentiate from real user accounts.

“Security teams seeking a customer-obsessed partner should look at Kasada.”

**Forrester Wave for Bot Management Software, Q3 2024**

FORRESTER®

# Get Started with Kasada

The growing sophistication of bots, combined with AI fueling more numerous and complex attacks, demand agility in stopping automated threats at speed and scale.

With an effective and user-friendly approach, Kasada’s proactive platform adapts as quickly as attackers do. Kasada received a **Strong Performer ranking in the Forrester Wave for Bot Management Software, Q3 2024 report.**

Its approach is a paradigm shift, 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 detection methods, Kasada requires no management and dynamically updates its defenses for enduring protection across websites, APIs, and mobile - all with a frictionless digital experience free of CAPTCHAs.

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.

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