kasada

# 2022 State of Bot Mitigation

## ANNUAL REPORT

## Introduction

The **2022 State of Bot Mitigation** annual report reveals the state of bot management and mitigation solely from organizations that have invested in one or more solutions in attempt to solve their automated threat and bot problems.

Conducted by an independent research firm, this year's report finds that the majority of companies using anti-bot solutions continue to struggle to stay ahead of threat actors despite spending up to millions of dollars fighting malicious bot attacks, largely due to the manual effort required to maintain and manage their expensive solutions.

The failure of these solutions to effectively detect and stop bots forces companies to spend an increasing amount of time, money, and resources to keep pace with the innovation and speed of motivated attackers.

---

**Research Methodolgy:**
Kasada commissioned Atomik Research to conduct a survey of 202 U.S. security and IT professionals responsible for mitigating bots. All organizations surveyed currently have anti-bot solutions in place. Fieldwork took place between August 18th and August 29th of 2022. Atomik Research, a part of 4media group, is an independent market research agency.

# Executive Summary

## Bots are Thriving, Companies are Losing

Bots continue to evolve and thrive at the expense of businesses. IT and security professionals at the frontlines of bot detection paint a troubling portrait of organizations' battles against malicious automation.

Automated threats, bot attacks, and online fraud contribute to revenue loss for organizations. Most companies surveyed report that they have lost revenue as a direct result of account fraud and malicious web scraping.

## Wasted Time, Money, and Resources Due to Bot Attacks

Bot attacks have become more advanced and difficult to combat.

Respondents cite a higher spend toward managing and mitigating bot attacks, and more anticipate their organization to increase spending toward bot detection and prevention compared to last year.

In addition, companies are still spending the majority of their anti-bot budget on the maintenance, management, and remediation of their solution, rather than on the solution itself.

---

# Key Findings

All of the survey respondents are security or IT professionals who work at an organization which has invested in at least one anti-bot solution.

**83%** of companies say bots are becoming more sophisticated and difficult for their security tools to detect.

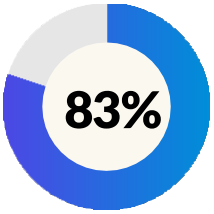
**69%** report that they lost more than **6%** of their revenue due to account fraud in the past 12 months.

**62%** have spent more than **$500,000** fighting bot attacks in the past year.

---

# Bots are Evolving to Evade Detection

**83%** of companies say bots are becoming more sophisticated and difficult for their security tools to detect, up from **80%** last year.




# The Most Difficult Types of Bots to Stop

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

# The Impact of Bots on Online Businesses

**45%** said bot attacks resulted in more **website and IT crashes.**

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

**33%** said bot attacks resulted in an **increase in infrastructure costs.**

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

**32%** said bot attacks resulted in a **poor customer experience.**

*The Most Difficult Types of Bots to Stop and the Impact of Bots on Online Businesses is based on data from the 2021 State of Bot Mitigation Report.*

# Lost Revenue Due to Account Fraud

In 2021, only **5%** of companies reported losing **10% or more of revenue** due to account fraud. This year, the number soared to **40%** of companies.


**69%**

lost over 6% of their revenue due to account fraud.

**40%**

lost 10% or more of revenue due to account fraud.

# Lost Revenue Due to Web Scraping

Last year, only **7%** of companies had **revenue loss of 10% or more** due to web scraping. In 2022, **39%** of companies lost that amount in revenue.

**54%**

lost over 6% of their revenue due to web scraping.

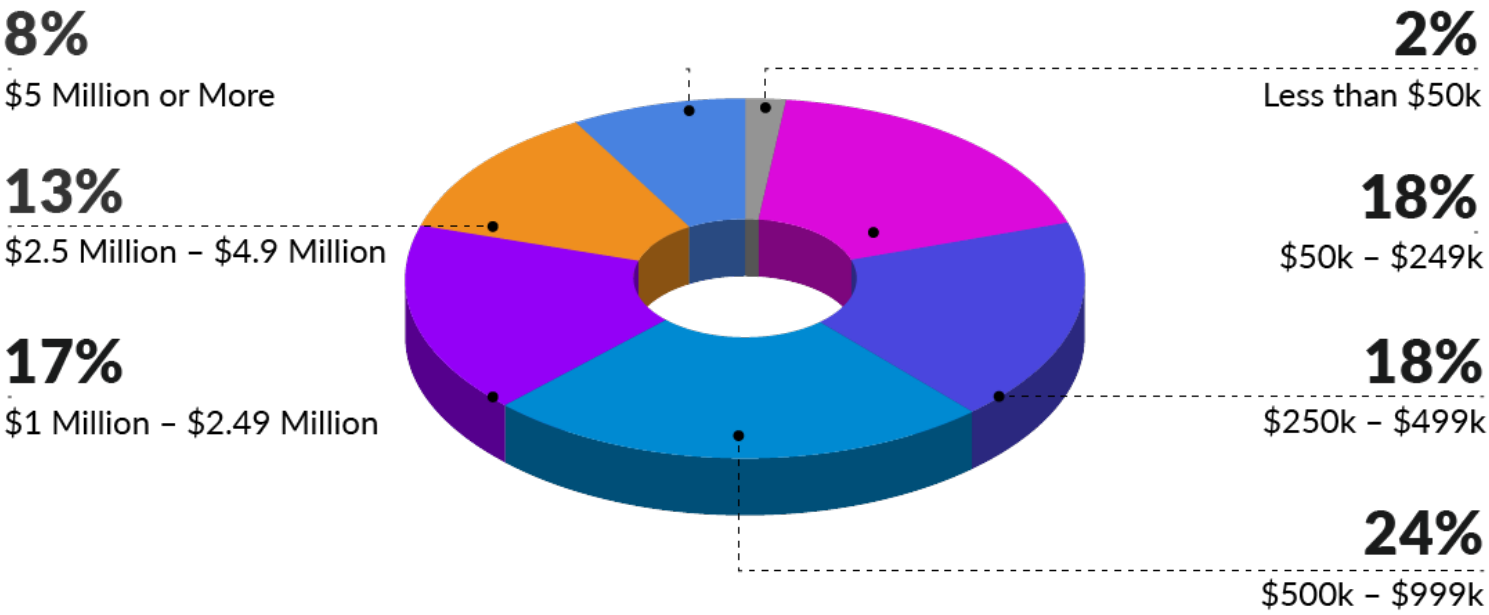
**39%**

lost 10% or more of revenue due to web scraping.

# The Cost of Bot Attacks is Rising

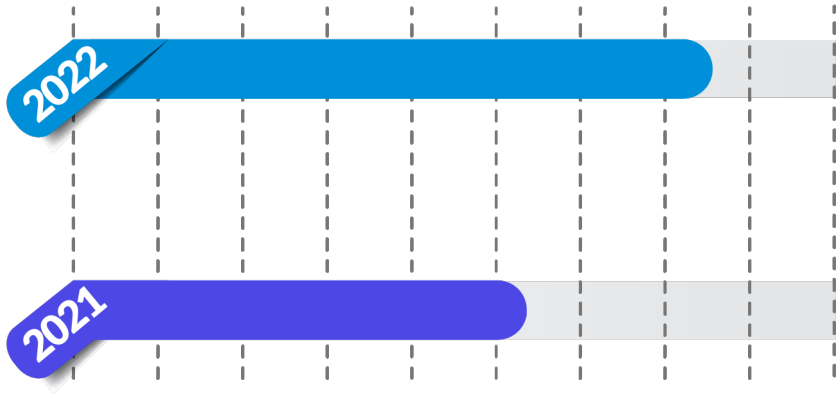
**62%** of companies have spent more than **$500,000** fighting bots within the past year due to inefficient anti-bot solutions, up from **48%** in 2021.

**21%** of companies have spent **$2.5 Million** or more in the past year.




# Spending is Expected to Increase

**85%** of companies expect to spend more next year on bot management and bot mitigation, compared to **63%** in the previous year's report.



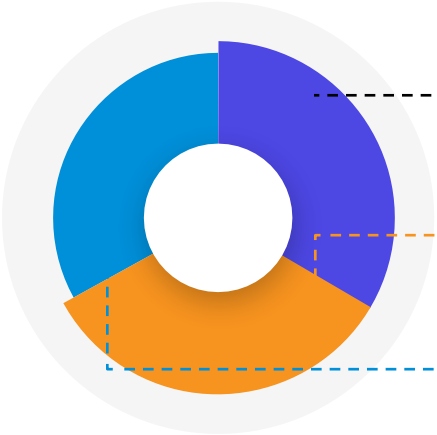

**85%**
expect to spend more fighting bots in the next year.

**VS.**

**63%**
expected to spend more.

# How Budget is Being Spent to Fight Bots

Two-thirds **(66%)** of total funds are spent on ongoing bot management, maintenance, and post-event remediation vs. the anti-bot solution itself.



**34%** The anti-bot solution itself

**33%** Ongoing management and maintenance

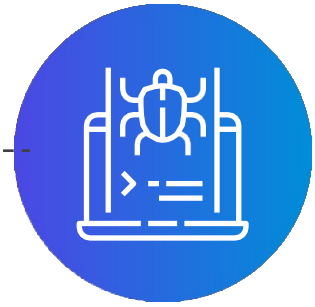
**33%** Post-event remediation

---

# Increase Your Revenue and ROI with Kasada

Kasada enables companies to increase their return on investment (ROI) and reduce their total cost of ownership (TCO) with the most effective and easiest to use bot mitigation platform – with no rules, no ongoing management, and no headaches.

Our proactive, dynamic platform adapts as fast as attackers do, making automated attacks unviable.



Unlike legacy rule-based solutions, Kasada is easy-to-use and offers long-lasting protection from bot attacks across web, mobile, and API channels.

Our invisible defenses eliminate the need for CAPTCHAs, ensuring a frictionless user experience throughout their digital journey.

**85%** of our customers were using other anti-bot providers prior to contacting us.

Learn how you can save time and money while protecting your revenue, customers, and brand at kasada.io.

kasada

Stop bad bots, for good.