BI&I

2020 Bot Landscape & Impact Report

Kount®
Identity Trust Platform

Table of Contents

Executive Summary

Bots are a permanent and growing part of the internet. Estimated at 40% of all internet traffic, they perform a variety of both critical and criminal operations. And increasingly, the ability to identify and manage these bots is essential for businesses. But the sophistication of emerging bots is creating problems for traditional detection tools.

To uncover the current state of bots and their impact on business, Kount commissioned Atomik Research to conduct a survey of online retail and eCommerce business employees in the United States. Respondents had full-time roles related to fraud prevention, customer experience, payments, and management. Fielding took place between September 1 and September 16 of 2020.

Bots Can Be Good, Bad, or Questionable

Survey results reveal that while 96% of businesses depend on good bots, 80% have lost revenue to bad bots. The tension between these numbers is affecting the industry response to bot detection. Businesses eager to reduce eCommerce friction for customers and automate internal operations are also wary of attacks that target and disrupt those same systems.

Companies Are Responding, But Slowly

93% of businesses surveyed report plans to implement tools within 12 months. One possible reason is that responsibility for defensive tools often falls on IT and cybersecurity teams. These teams typically focus on infrastructure protection, and have less visibility into bot attacks on payments, brand reputation, and inventory.

WAFs & CDNs Don't Address eCommerce Bot Needs

The needs of bot protection are growing beyond perimeter safety, and penetrating further into eCommerce operations. WAFs and CDNs are ineffective at identifying sophisticated bots at points within the customer journey, and businesses are urgently seeking tools that detect and manage different bot types without disrupting customer experiences.

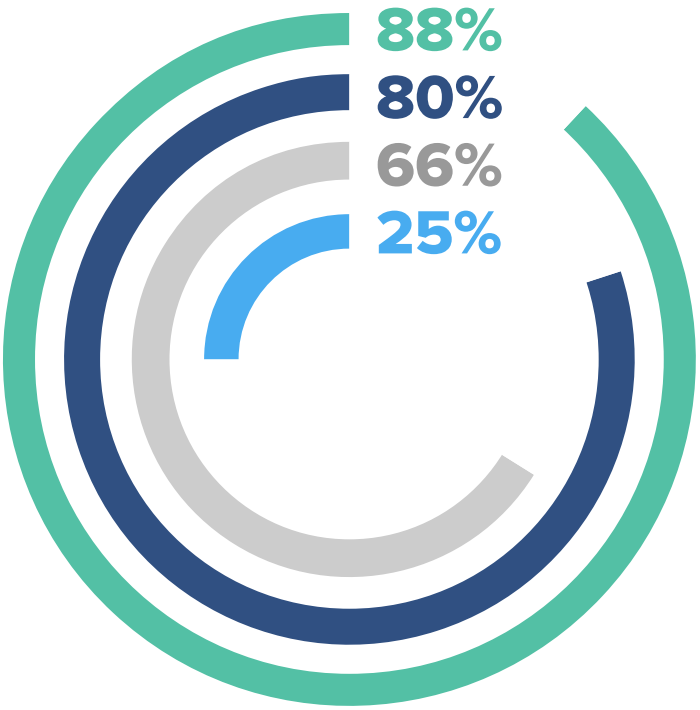
Top Stats

88% of organizations say complex, malicious bots are becoming more difficult for their security tools to detect.

80% say increasingly sophisticated bot attacks have resulted in increased financial losses.

Two thirds say a single malicious bot attack costs their company **$100k or more in lost revenue.**

One in four report a single malicious **bot attack costs their organization over $500k.**



96% say good bots are important to the success of their organization's eCommerce.

81% say they often or very often deal with issues related to malicious bots, and more than half **encountered at least 50 bot attacks in the last 12 months.**

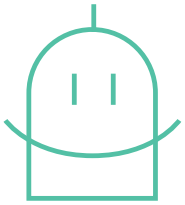
50+ **Attacks**

Businesses most often report encountering:

- social media bots **60%**
- spam bots **52%**
- hacker bots **50%**
- scraper bots **45%**

Good, Malicious, and Questionable Bots

Is a bot good, bad, or somewhere in between? The answer may depend on the business, or even department. A bot that is harmless to cybersecurity can hurt ecommerce or customer experience. Many organizations allow bots for automated purchases, quotes, and virtual assistants. But sophisticated bots can mimic human behavior, bypassing traditional perimeter defenses to launch card testing and card cracking attacks, and retail arbitrage such as inventory depletion or denial of inventory.



Good Bot Activity

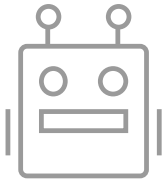
Search Engine Bots

Copyright Bots

Site Monitoring Bots

Commercial Bots

Feed Bots



Questionable Bot Activity

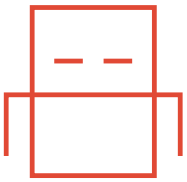
Social Media Bots

Scraper Bots

Quoting Bots

Ticketing Bots

Automated Purchasing Bots



Malicious Bot Activity

Card Testing / Card Cracking Bots

Account Testing Bots

DDoS Bots

Brute Force Bots

Spam Bots

Denial of Inventory Bots

Ad Fraud Bots

Good Bots: Architecture, Automation, Acceleration

Good bots, such as search engine and SEO tools, virtual assistants, and chatbots, help businesses to optimize operations.

Businesses employ these bots primarily to reduce friction across their entire operational landscape, from customer experiences to internal operations.

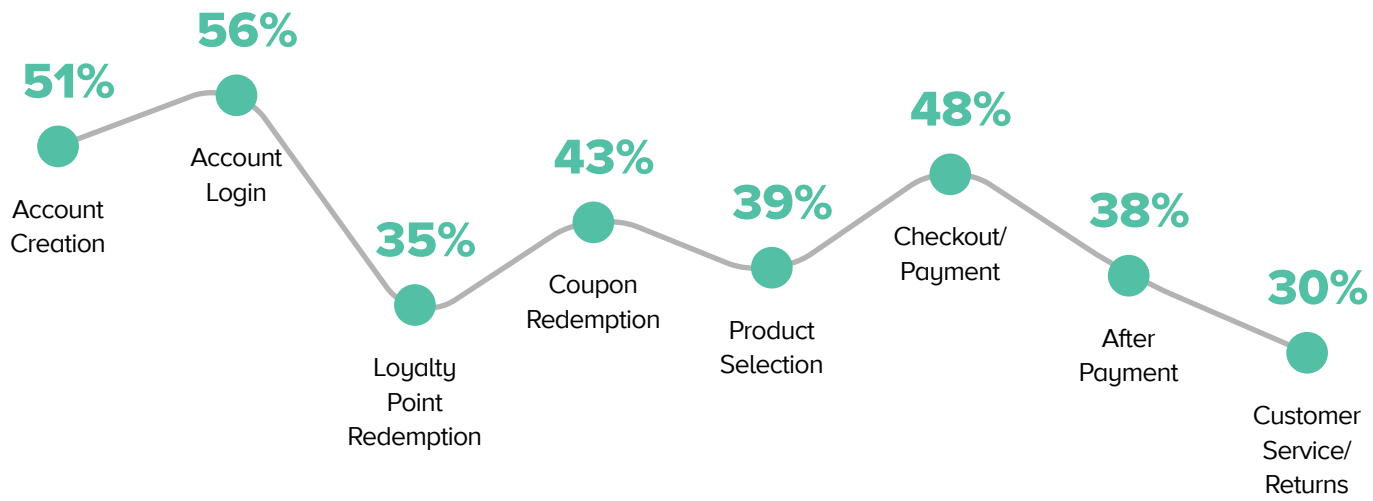
Good bots tend to support one of three goals:

1. Architecture SEO tools detect website problems that can interfere with site visibility or navigation.

2. Automation Virtual assistants can automate common tasks. And bots can help entrepreneurs to scale communications that increase customer loyalty.

3. Acceleration Chatbots can respond immediately to customer inquiries when a human is unavailable.

Percent of Businesses That Use Good Bots At:



Good Bots

Key Impact: Most businesses employ good bots to reduce friction and improve operations.

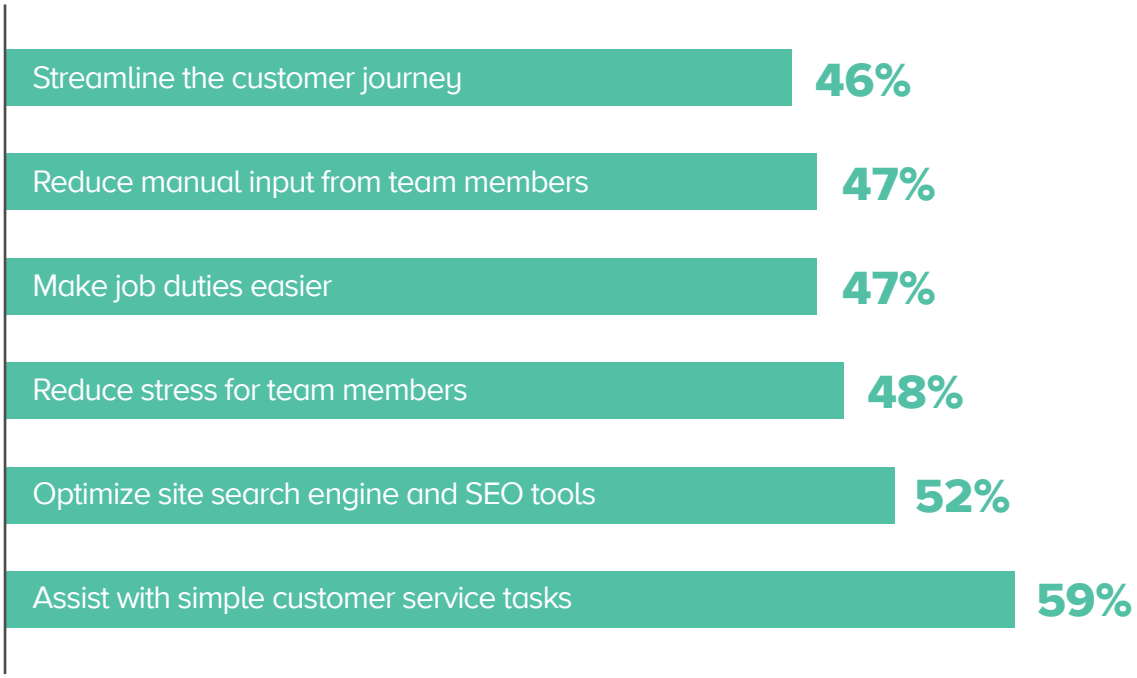
Almost all participants say their organization employs good bots at some point in the customer journey to enhance customer experiences.

99%

96%

An overwhelming majority of respondents report that good bots are important to the success of their organization's eCommerce.

Benefits of Good Bots



The Broad Impact of Malicious Bots

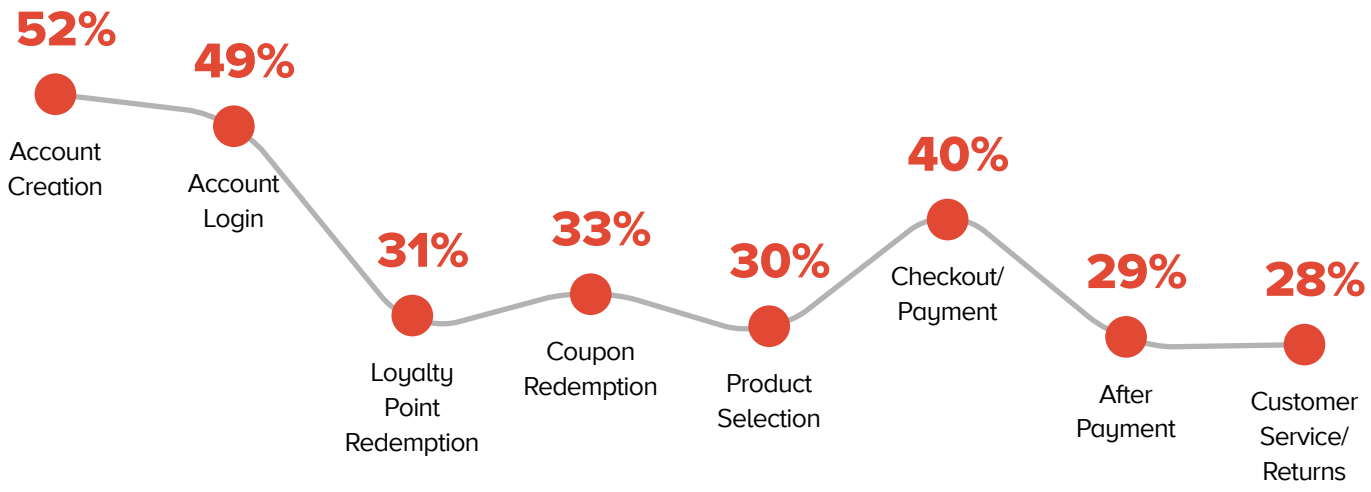
Key Impact: Malicious bot attacks are becoming more complex and sophisticated at every point in the customer journey.

A growing number of sophisticated, malicious bots can target customers at any point in the customer journey to cause significant damage. Emerging bot designs can attack infrastructure to take down digital operations, steal customer information for financial gain, freeze critical inventory, reduce productivity, or disrupt the customer experience to cause severe brand damage.

Some of most common attacks are:

- **Brute force or credential stuffing** attacks that take over a legitimate customer's account
- **Card testing** to identify usable stolen credit cards
- **Price or content scraping** for a competitive advantage
- **Social campaigns** designed to mislead or inflame users
- **Distributed denial of service** (DDoS) to disrupt or take down a website or digital service

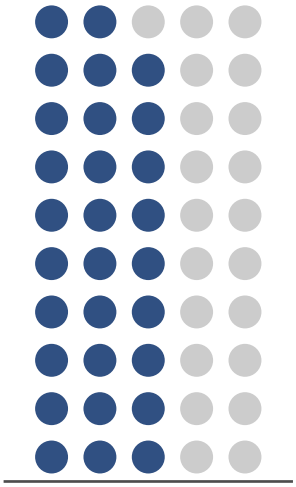
Where Do Malicious Bots Occur in the Customer Journey?



The Cost of Frequent Malicious Bot Attacks

Key Impact: Bot attacks are happening more frequently, costing more money, and taking too long to detect for many businesses.

More than half (58%) of businesses encountered **more than 50 bot attacks in the last 12 months.**

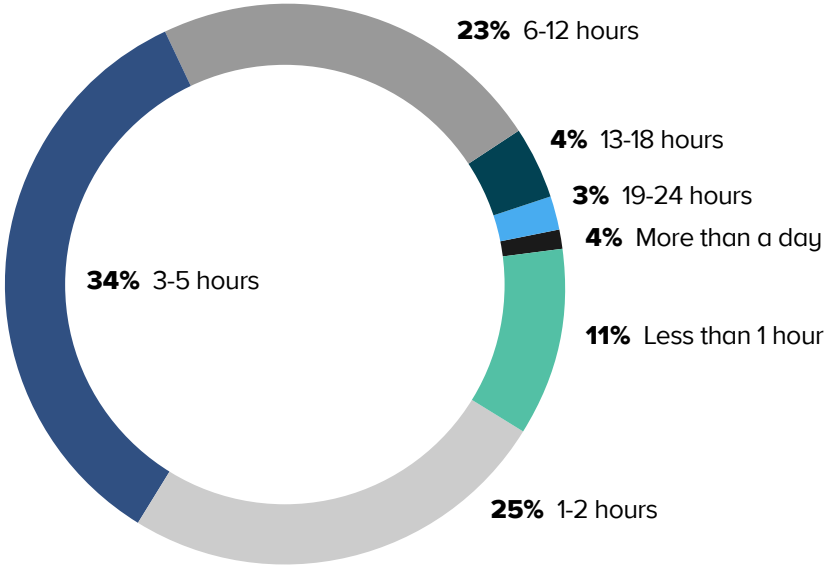


Two thirds say a single malicious bot attack costs their company **$100k or more in lost revenue.**

One in four report a single malicious bot attack costs their organization over **$500k.**

How Long Does It Take to Detect?

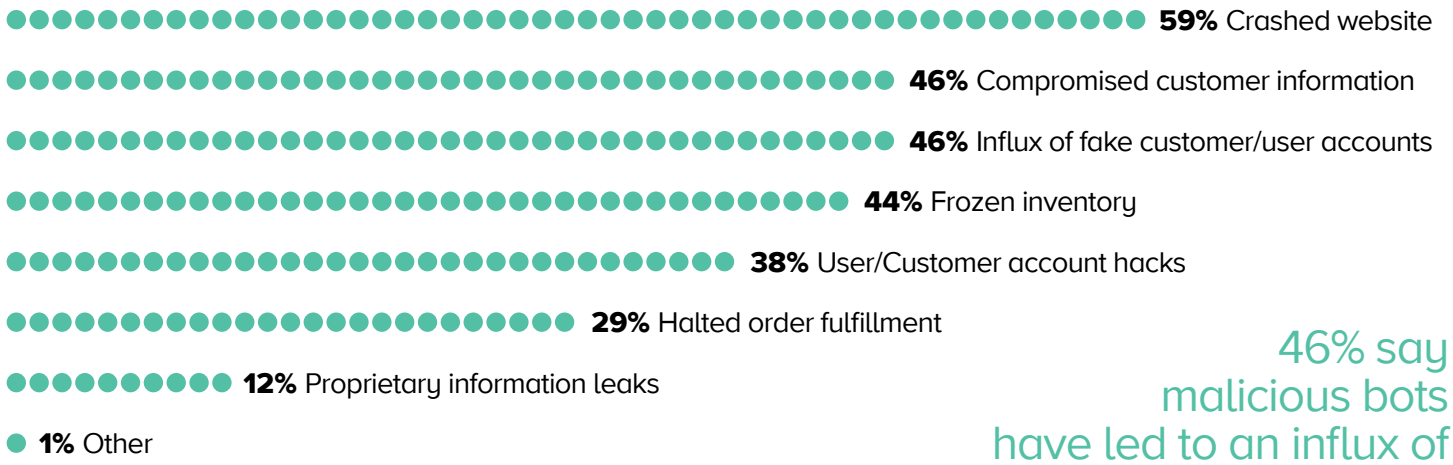
A lot can happen in a matter of hours — the longer it takes to identify and neutralize malicious bot attacks, the more time malicious programs have to cause serious damage.



Losing More Than Money: Impacts and Consequences of Malicious Bots

Key Impact: Bot attacks pose risks including crashed websites, bad customer experiences, frozen inventory, and brand damage.

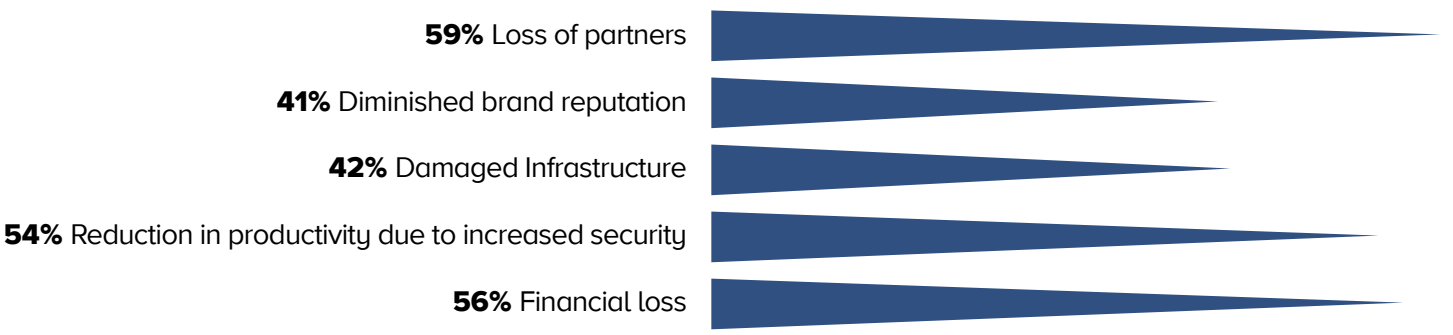
What were the consequences of the bot-related attacks?



46% say malicious bots have led to an influx of fake customer accounts

What were the impacts of bot-related attacks?

41% say bad bots have caused brand reputation damage

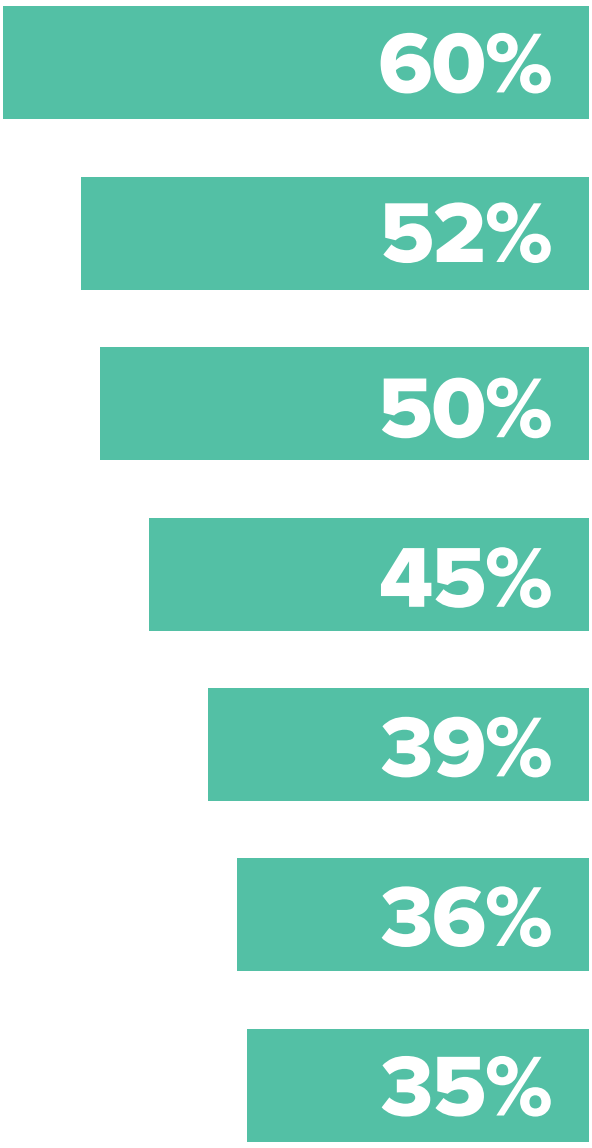


Questionable Bots

Questionable bots are good, bad, or neutral depending on business goals or department perspectives. For example, Scraper Bots/Web Scrapers collect content from websites, such as product reviews, breaking news, product pricing information and catalogs, user generated content on community forums, and so on. For some businesses, this activity is beneficial and increases their exposure on multiple sites frequented by high-value customers. For others, it can divert visitors to a third-party website which reduces advertising and upsell opportunities or hurts the customer experience.

Good	Bot Type	Malicious
Automate social media campaigns, reshare essential content	**Social Media Bots**	Disseminate malicious content, manipulate audiences
Aggregate content to share on revenue-producing 3rd party channels	**Scraper Bots**	Assist in harmful content-reselling, price undercutting, promotional abuse, etc.
Download and index sites to improve site architecture and SEO	**Spider Bots**	Search for site vulnerabilities or proprietary content, slow site operations
Assist consumers in identifying and pricing available, hard-to-find tickets	**Ticketing Bots**	Reserve large quantities of inventory to manipulate prices or for reselling purposes
Deliver multiple quotes from 3rd parties to help consumers price options	**Insurance Quote Bots**	Submit illegitimate bulk quotes to open fakes policies with stolen information

Most Common Bots Encountered



Social Media Bots
Automated social media accounts. Some are helpful, others are used for manipulative purposes like inflating KPIs.

Spam Bots
Assist in the sending of spam.

Hacker Bots
Distribute malware, deceive individual people, attack websites and/or networks.

Scraper Bots
Collect data such as proprietary content, pricing information, and creative content from a website for aggregation.

Spider Bots
Web crawler, spider, or search engine bots that download and index content from all over the internet.

Ticketing Bots
Scrape ticket pricing details, check for newly released seats, or reserve mass amounts of inventory without completing purchase.

Insurance Quote Bots
Submit illegitimate bulk quotes to open fake policies by using consumer information purchased or stolen from lead generators or brokers' books.

The Problem of Bot Identification Is Hindering Protection

Key Impact: Early generation bot detection solutions aren't enough for businesses dealing with complex attacks.

The vast majority of respondents say their business plans to deploy a tool or solution specific to bot mitigation in the next 12 months.

Existing Web Access Firewall (WAF) and Content Delivery Network (CDN) defenses that protect the perimeter are no longer effective as stand alone solutions, as the mission of malicious bots has turned to dodging perimeter protections to penetrate deeper into an organization.

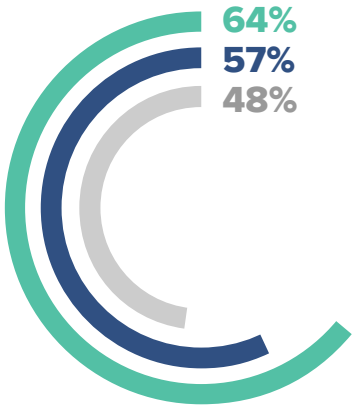
Current solutions identify bots at the front door, but they can't determine a bot's level of risk to the business. This gap in knowledge represents a critical need for businesses that want to detect and mitigate bots across the customer journey.

Nearly 9 in 10

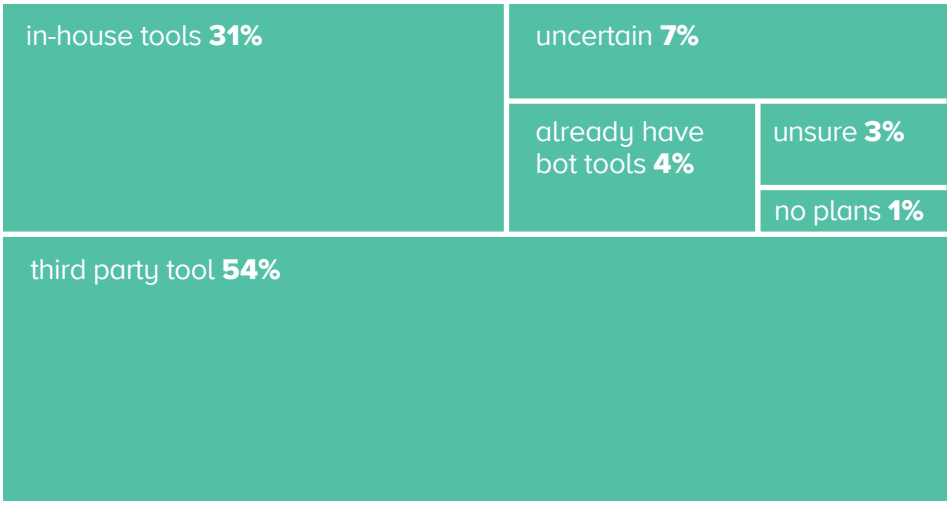
businesses say increasingly complex, malicious bots are becoming more difficult for their security tools to detect

Organizations currently use:

- Web Access Firewalls (WAFs): **64%**
- Content Delivery Networks (CDNs): **57%**
- Dedicated bot vendors: **48%**



93% say they plan to deploy a specific bot mitigation tool within the next 12 months.

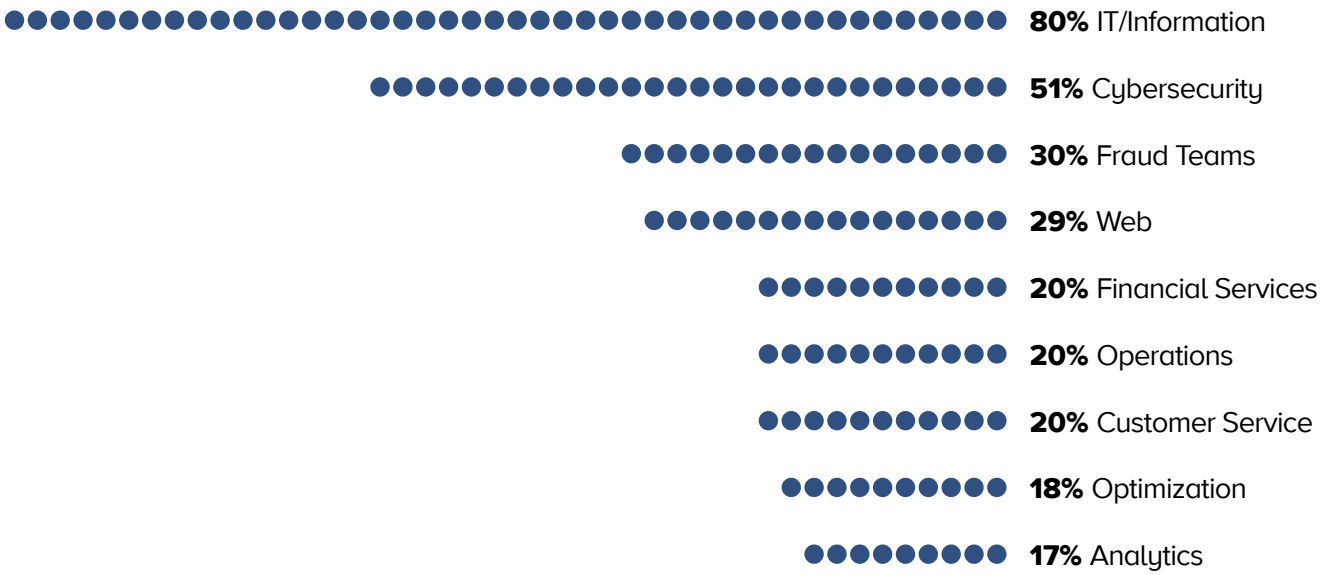


Managing Bots

Key Impact: IT and Infrastructure teams are generally in charge of protecting against bots, but other roles and detection tools are also becoming critical to security.

What bot mitigation solutions does your organization use?

Which team or teams are typically in charge of protecting against malicious bots?



Evolution of Bot Detection

Key Impact: Bot detection has evolved from perimeter defenses to networked data and behavioral analysis.

The first generation of bot detection solutions provided perimeter defenses, protecting websites or systems from melting down when overwhelmed by requests. Web Access Firewalls (WAFs) and Content Delivery Networks (CDNs) were able to stop Distributed Denial of Service (DDoS) and other brute force attacks.

Eventually, malicious bots began dodging WAFs, penetrating deeper into an organization's processes to cause financial harm.

In response, the second generation of bot detection moved to the cloud to better detect bots and protect against different aspects of digital commerce fraud. Rather than an exclusive problem for infosec, departments responsible for customer experience began looking for tools beyond WAFs.

The new generation in bot detection is event-based protection. Because sophisticated bots can mimic human interactions, tools can't always differentiate between human and bot. However, by embedding protection within the business workflow, modern bot protection compares network, device, and behavioral characteristics with identity trust signals to assess risk in real time. In this way, event-based solutions protect the complete customer journey, from account creation, to login, to payment and checkout.

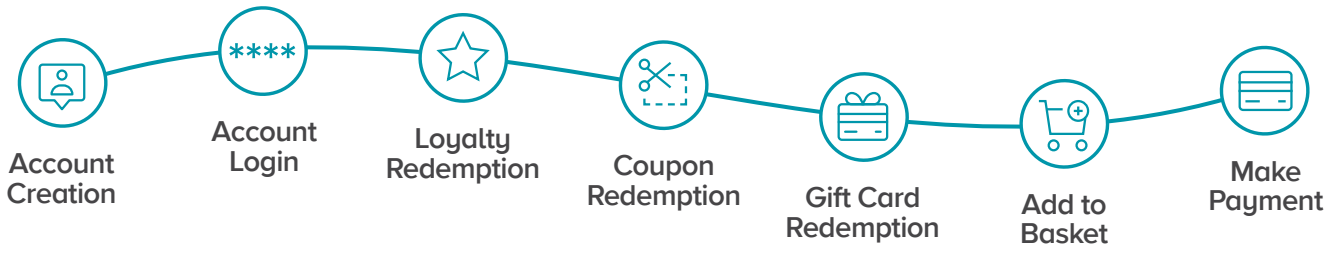
Conclusions & Recommendations

Key Impact: Companies need to detect and distinguish between good, questionable, and malicious bots. Quick, adaptive responses are key to protecting customers, the brand, and revenue.

Top Needs for Sophisticated Bot Protection

Detect Bots	Analyze signals across the customer journey, connecting and linking identifiers in real time to identify bot-like behavior.
Classify Good vs. Malicious Bots	Evaluate user behavior, device, and network anomalies, along with signals from a robust data network, to classify bots as good, malicious, or questionable.
Block Malicious Bots	Provide the intelligence necessary to identify and block emerging malicious bots while protecting the experience of legitimate users and authorized bots.
Adapt Response to Questionable Bots	Allow quick, customized responses to bots, blocking or challenging the interaction based on the bot's behavior and the desired business outcomes.
Remove Friction for Good Bots and Legitimate Customers	Stop fraud without adding unwanted friction for good bots and legitimate customers.
Gain Visibility	Access data and analytics for visibility into how bots are impacting business. Uncover hard to detect fraud, customer behaviors after purchase, and bot trends.

Customer Journey Protection

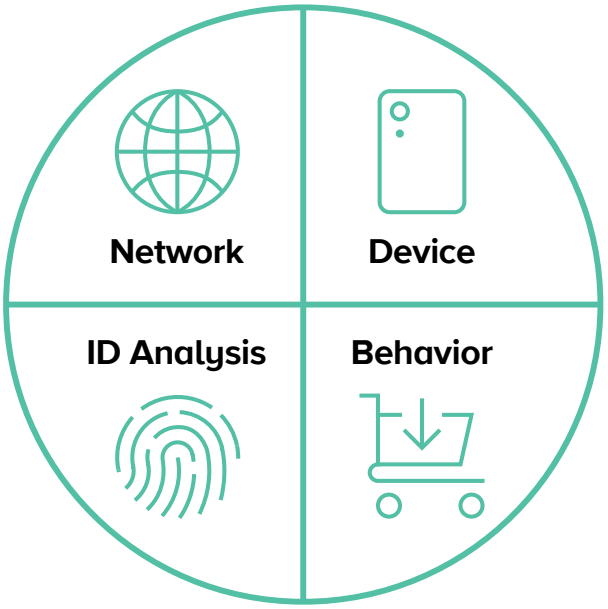


Kount's Event-Based Bot Detection

Kount's Identity Trust Platform, built on the Identity Trust Global Network, is the leader in AI-driven fraud prevention.

Kount's next-generation, Event-Based Bot Detection applies a layered approach to accurately identify and segment good, malicious, and questionable bots.

Kount links network, device, and behavioral characteristics to billions of trust and risk signals in order to assess risk in real time, and in the context of the attack. Businesses gain fine-tuned control over bots throughout the digital journey.



Kount's Identity Trust Global Network Linked by Adaptive AI

- 9,000+ Brands
- 32B+ Annual Interactions
- 250+ Geographies
- 2.7B Fraud Signals
- 1B+ Unique Payment Tokens
- 75+ Verticals
- 600M+ Unique Names
- 600M+ Unique Email Addresses
- 300M+ Unique Phone Numbers

Benefits of Kount's Event-Based Bot Detection Solution

Segment bots based on unique business objectives and risk thresholds

Gain visibility into what bots are doing to your business

Identify fraudulent accounts and abusive behavior before it negatively impacts revenue

Block or challenge suspicious activity without adding friction to the customer experience

Detect bots and stop attacks with event-based bot protection.

SCHEDULE A DEMO

Contact Kount at:
sales@kount.com
+1.866.233.9943

ABOUT KOUNT

Kount's Identity Trust Global Network™ delivers real-time fraud prevention, account protection, and enables personalized customer experiences for more than 9,000 leading brands and payment providers. Linked by Kount's award-winning AI, the Identity Trust Global Network analyzes signals from 32 billion annual interactions in order to personalize user experiences across the spectrum of trust—from frictionless experiences to blocking fraud. Quick and accurate identity trust decisions deliver safe payment, account creation, and login events, while reducing digital fraud, chargebacks, false positives, and manual reviews. **www.kount.com/bots**