2020 Bot Landscape & Impact Report
# Table of Contents

- Executive Summary 03
- Top Stats 04
- Good, Malicious, and Questionable Bots 05
- Good Bots: Architecture, Automation, Acceleration 06
- The Broad Impact of Malicious Bots 08
- Questionable Bots 11
- Bot Identification 13
- Managing Bots 14
- Evolution of Bot Detection 15
- Conclusion and Recommendations 16
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.
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.

Businesses most often report encountering:

- Social media bots 60%
- Spam bots 52%
- Hacker bots 50%
- Scraper bots 45%

50+ Attacks
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 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:

- **Account Creation**: 51%
- **Account Login**: 56%
- **Coupon Redemption**: 43%
- **Product Selection**: 39%
- **Checkout/ Payment**: 48%
- **After Payment**: 38%
- **Customer Service/ Returns**: 30%
- **Loyalty Point Redemption**: 35%

---

2020 BL&I Good Bots: Architecture, Automation, Acceleration
**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.

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

### Benefits of Good Bots

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streamline the customer journey</td>
<td>46%</td>
</tr>
<tr>
<td>Reduce manual input from team members</td>
<td>47%</td>
</tr>
<tr>
<td>Make job duties easier</td>
<td>47%</td>
</tr>
<tr>
<td>Reduce stress for team members</td>
<td>48%</td>
</tr>
<tr>
<td>Optimize site search engine and SEO tools</td>
<td>52%</td>
</tr>
<tr>
<td>Assist with simple customer service tasks</td>
<td>59%</td>
</tr>
</tbody>
</table>
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?

![Diagram showing percentages of malicious bot occurrences at different stages of the customer journey.](image-url)
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.

- 23% 6-12 hours
- 4% 13-18 hours
- 3% 19-24 hours
- 4% More than a day
- 11% Less than 1 hour
- 25% 1-2 hours
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?

- 59% Crashed website
- 46% Compromised customer information
- 46% Influx of fake customer/user accounts
- 44% Frozen inventory
- 38% User/Customer account hacks
- 29% Halted order fulfillment
- 12% Proprietary information leaks
- 1% Other

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

What were the impacts of bot-related attacks?

- 59% Loss of partners
- 41% Diminished brand reputation
- 42% Damaged Infrastructure
- 54% Reduction in productivity due to increased security
- 56% Financial loss

41% say bad bots have caused brand reputation damage.
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.

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

<table>
<thead>
<tr>
<th>Bot Type</th>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Media Bots</td>
<td>60%</td>
<td>Automated social media accounts. Some are helpful, others are used for manipulative purposes like inflating KPIs.</td>
</tr>
<tr>
<td>Spam Bots</td>
<td>52%</td>
<td>Assist in the sending of spam.</td>
</tr>
<tr>
<td>Hacker Bots</td>
<td>50%</td>
<td>Distribute malware, deceive individual people, attack websites and/or networks.</td>
</tr>
<tr>
<td>Scraper Bots</td>
<td>45%</td>
<td>Collect data such as proprietary content, pricing information, and creative content from a website for aggregation.</td>
</tr>
<tr>
<td>Spider Bots</td>
<td>39%</td>
<td>Web crawler, spider, or search engine bots that download and index content from all over the internet.</td>
</tr>
<tr>
<td>Ticketing Bots</td>
<td>36%</td>
<td>Scrape ticket pricing details, check for newly released seats, or reserve mass amounts of inventory without completing purchase.</td>
</tr>
<tr>
<td>Insurance Quote Bots</td>
<td>35%</td>
<td>Submit illegitimate bulk quotes to open fake policies by using consumer information purchased or stolen from lead generators or brokers’ books.</td>
</tr>
</tbody>
</table>
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.

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

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

- In-house tools **31%**
- Uncertain **7%**
- Third party tool **54%**
- Already have bot tools **4%**
- Unsure **3%**
- No plans **1%**
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?

- 64% Web Access Firewall (WAF)
- 57% Content Delivery Network (CDN)
- 48% Dedicated bot vendors
- 41% Fraud vendors
- 1% Other
- 1% None

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

- 80% IT/Information
- 51% Cybersecurity
- 30% Fraud Teams
- 29% Web
- 20% Financial Services
- 20% Operations
- 20% Customer Service
- 18% Optimization
- 17% Analytics
Evolution of Bot Detection

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

1. **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.

2. **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.

3. **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

- Account Creation
- Account Login
- Loyalty Redemption
- Coupon Redemption
- Gift Card Redemption
- Add to Basket
- Make Payment

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.
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.

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

Contact Kount at:
sales@kount.com
+1.866.233.9943