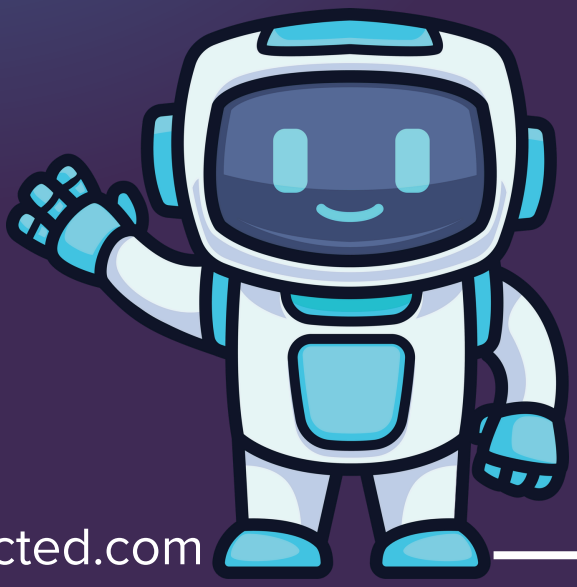
spec

HOW TO TELL GOOD BOTS FROM BAD BOTS



www.specprotected.com

The Changing World of Commerce Requires a New Lens

Commerce is shifting under the surface. For years, “bot traffic” was treated as abuse to be blocked. But with Agentic AI, bots can attack and act like customers. Some are malicious, some are beneficial, and many are simply new kinds of buyers.

Every time a good agent is mistaken for a bad bot, it’s not just a false positive, it’s lost revenue and a lost customer.

The Numbers That Matter:

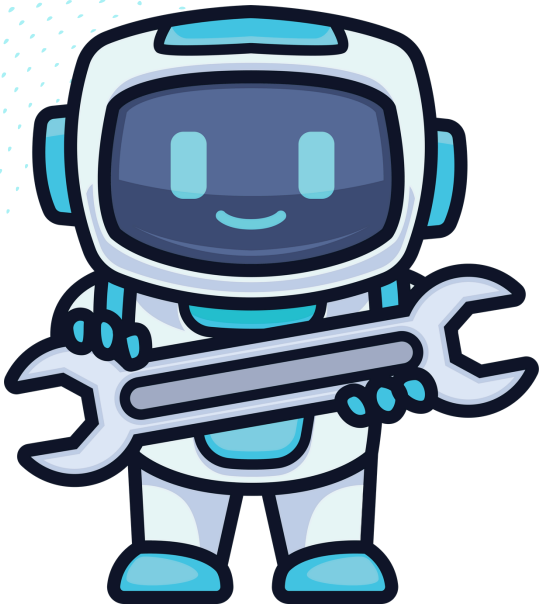
- 0.5-1% of visitors are automated agents making legitimate purchases
- For some merchants, 5-25% of good purchases now come from automated buyers
- Only 2-3% of visitors are humans making legitimate purchases

Most merchants can’t tell the difference between good agents and bad bots. Their tools rely on brittle signals, like device fingerprints, IP addresses, login details, and broad rules. That creates two costly risks:

- **Blocking good agents**: Real customers bounce and buy from competitors
- **Letting bad bots through**: Fraud, abuse, chargebacks, and revenue leakage

Every time a good agent is mistaken for a bad bot, it’s not just a false positive, it’s lost revenue and a lost customer. In a world where switching costs are low, that customer may never return.

Blocking bots is no longer enough. Merchants need to identify intent to know who’s behind every session and act with confidence.



From “Block All Bots” to “Know Who’s Behind the Request”

Not all automated traffic is malicious. Some of it powers your business, some of it represents real buyers, and some of it truly is a threat. The problem is that most merchants can’t tell the difference so they treat it all the same.

Three Types of Automation You See Today:

1. Malicious Automation

- Fraud rings, scalpers, credential stuffing, refund abuse
- Goal: Exploit your systems and extract value

2. Good Automation

- Search crawlers, QA scripts, accessibility tools, partner integrations
- Goal: Support the business, improve performance, or serve customers

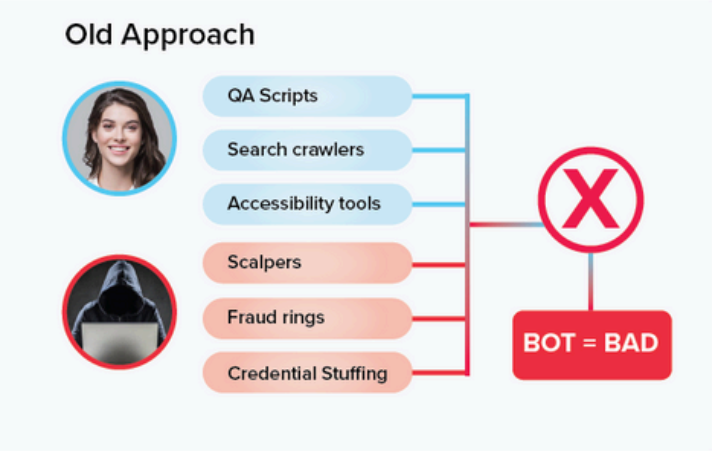
3. Agentic Commerce

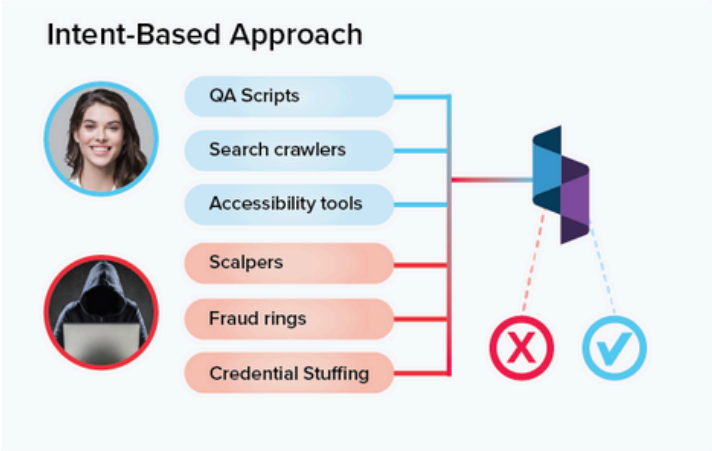
- AI agents acting on behalf of real customers (e.g., buying resale inventory, booking travel, auto-ordering retail stock)
- Goal: Complete legitimate purchases faster than a human could

The Blind Spots That Make Rules-Based Detection Ineffective

The problem isn't just the rise of new types of automation, it's that most detection systems weren't built for it. Tools that rely on static rules or surface signals can't adapt when agents behave like people. What slips through looks normal, and what gets blocked often includes good buyers. Here's why the old approach breaks down:

- **Rules don't scale**: Agentic AI doesn't trip obvious thresholds; it adapts
- **Static signals are brittle**: Device fingerprints, IPs, and emails rotate or spoof
- **Snapshots miss context:** Tools that only check login or checkout can't see the journey leading up to it





The real job is to recognize intent and act accordingly by keeping the right traffic moving and stopping the wrong traffic before damage is done.

Persistent Identity for Every Session, Human or Agent

Legacy tools were designed for obvious bots. They miss what blends in. Spec ID was built for this new era where automation looks like a person and intent is what matters.

How Spec ID Works:

- **Links behavior across sessions** even if devices, IPs, or accounts change.
- **Creates a behavioral fingerprint** that persists beyond logins or surface signals
- **Captures before, between, and beyond API calls**, giving visibility into the full journey, not just snapshots.

This is a business shift. By tying sessions together and revealing intent, Spec ID changes how teams make decisions. Instead of reacting to signals in isolation, you can act with confidence on the full picture of who's behind the activity.

Agentic AI means bots can act like people. Spec ID means you still know who is who.

Spec ID gives you the precision to tell good from bad. The result: fewer false positives, fewer misses, and faster approvals for the customers you actually want.

Stop the Bad. Keep the Good. Grow With Confidence.

Intent detection is about stopping fraud and unlocking growth. By separating good agents from bad bots, Spec ID helps you capture sales competitors lose, protect your brand from abuse, and keep the customer experience friction-free.

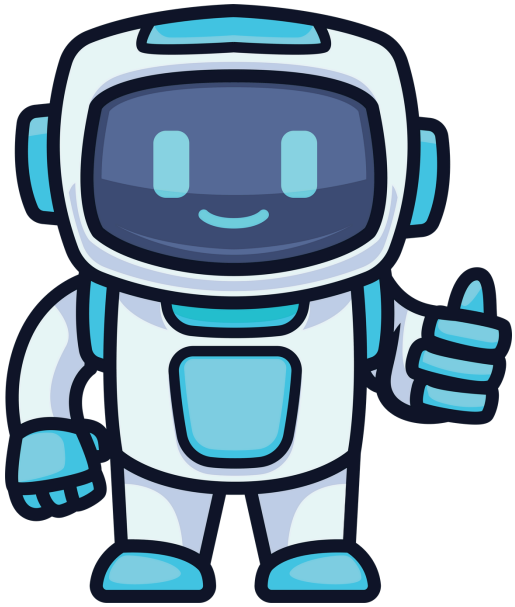
The Outcomes You Can Expect:

More Revenue
Capture purchases from trusted AI agents that competitors block by mistake.

Less Risk
Stop malicious bots and fraud rings before they cash out.

Better Experience
Keep checkout fast and simple for real customers and trusted automation.

Aligned Teams
Give Fraud, CX, and Product a shared truth about intent, not conflicting reports.

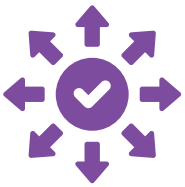


Next Steps

Intent detection delivers results quickly when you start small and build momentum. The path forward isn't about a massive overhaul, it's about applying Spec ID in the right places, proving value, and then expanding. Here's how to begin:

1. Audit

Assess how much legitimate automated traffic you're currently blocking.



2. Pilot

Apply Spec ID to a high-impact flow (checkout, promo abuse, booking) to measure results.

3. Measure

Track conversion lift, reduction in false positives, and fraud loss prevented.

4. Scale

Expand cross-session linking to persist identity across all journeys

Spec ID helps you know every bot, stop the bad ones, and keep the good ones buying.

See intent in action. Speak with a Spec fraud expert to learn more.

REQUEST A DEMO

ABOUT SPEC

We’re reinventing customer security from the ground up.

Led by a team that’s protected some of the most attacked businesses on the planet, we're on a mission to help organizations secure their customer journeys from ever-evolving threats. By creating a real-time defense layer, our platform enables businesses to effortlessly detect and block threats, ensuring they can deliver trusted customer experiences.

Discover more at specprotected.com.