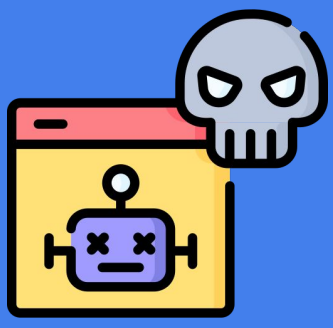
transmit security

SERVICE BRIEF

# Advanced Bot Detection to Prevent Unwanted Automated Activity



Leverage **machine learning** with **multi-method detection** to detect evasive bots designed to elude existing solutions.

Bots are constantly evolving to bypass detection, and powerful automation frameworks like OpenBullet 2.0 are making it easier than ever for them to launch evasive attacks at unprecedented scale. These frameworks are changing the game for bot mitigation, rendering network-level bot detection tools obsolete.

## Challenge

### Evasive bots circumvent controls by mimicking human activity

Innovative bad bots dubbed "evasive bots" use modified web browsers, regularly change IP addresses, imitate human mouse activity and time requests to appear more like legitimate users.

### Criminals leverage automation frameworks for sophisticated attacks

Open-source automation frameworks are becoming popular tools for attackers to leverage credential stuffing attacks that bypass detection by making distributed requests with IP proxies, manipulating headers and cookies and using dedicated services to solve CAPTCHA challenges.

### Blunt controls block good bots and create friction for trusted users

Blocking all bot-like behavior disrupts sessions for trusted users who leverage automation tools and web crawlers used to catalogue content in search engines.

## Solution

### Multi-method detection with machine learning (ML) analysis

Bots designed to obfuscate risk indicators and mimic human activity can make it difficult to identify traffic anomalies that indicate malicious bots. Our approach pinpoints anomalies using broader data collection and advanced ML.

- **Multi-method detection** uses a broad range of telemetry across multiple detection frameworks — including behavioral biometrics, device fingerprinting and user activity patterns — to identify evasive bot attacks.
- **ML analysis** based on PU (positive-unlabeled) learning — a semi-supervised approach that not only enables detection of known bad bots, but new and unknown bots, based on behavioral, device, network & velocity features.

## Bot-Based Attacks

### Web scraping

Automated data harvesting that is used for content reselling, price undercutting and other malicious purposes.

### New account fraud

Using stolen or synthetic identities to rapidly create accounts used for phishing, promotional fraud, loan fraud and more.

### Inventory scalping

Bots used to outpace customers in purchasing sought-after items like concert tickets in order to resell them at a profit.

### Inventory hoarding

Artificially depleting retail inventory by repeatedly adding high-demand or limited-supply items to shopping carts without making purchases.

### Credential stuffing

Automated injection of stolen credential lists into login forms, used by attackers to fraudulently gain access to trusted users' accounts.

# Real-Time Bot Detection with Risk, Trust, Fraud, Bots & Behavior Analysis

Bot detection is part of our Detection and Response service, a fraud prevention SaaS that gives transparent, contextual recommendations that can be used as action triggers to block unwanted automated activity while welcoming trusted users and good bots.

- **Dynamic adaptation to risk and trust signals** leverages cloud-native, microservice architecture to deploy frequent, ongoing updates that support trust lists of good bots and enable detection of new bad bots.
- **Behavioral biometrics** analyze input methods, mouse movements and other user actions to compare trusted users' actions with their historical behavior and detect bad bots even before user profiles are available — enabling the best possible accuracy with the shortest time to value.
- **Out-of-the-box decisioning orchestration** eliminates the need for complex data integrations across multiple siloed tools like WAAP and behavioral analytics.

## Backed by the Transmit Security Research Lab

Benefit from the expertise of our security researchers who leverage threat intelligence and bot attack tools, like those used for credential stuffing, device emulation and headless browser testing, to reverse-engineer sophisticated attacks and uncover features that can be used to identify bad bots, such as suspicious device attributes or mousing patterns. They apply their findings to optimize frameworks used in statistical detection models and train and tune ML algorithms—resulting in continuous improvement and always up-to-date protection.

> **Transmit Security Named 'Overall Leader'**
> in three ranking reports: Fraud Reduction Intelligence, Passwordless Authentication and CIAM Platforms.

## Risk Indicators

**Behavioral biometrics**
- Concentrated mouse clicks
- Touchscreen anomalies
- Ultra-fast typing speed
- Abnormal movements
- Sudden change in input method

**Activity analysis**
- Low session duration
- Abnormal user journeys
- Short time spent on page

**IP/Proxy reputation**
- Use of proxies
- Known malicious IPs
- High rate of fresh IPs
- IP geolocation anomalies

**Velocity checks**
- Repetitive user actions
- Repetitive device actions
- Repetitive orders
- High-velocity IPs

**Device reputation**
- Identical cookies
- Identical headers
- Use of device emulator
- Use of automation frameworks

Evasive bots were responsible for almost two-thirds of all ATO in 2022, which increased 148% from 2021, according to Imperva's 2022 Bad Bot Report.[1]

[1] Imperva

## About Transmit Security

Transmit Security gives businesses the modern tools they need to build secure, trusted and end-to-end digital identity journeys to innovate and grow. CX-focused, cybersecurity-conscious leaders rely on Transmit Security's CIAM platform to provide their customers with smooth experiences protected from fraud across all channels and devices. Transmit Security serves many of the world's largest banks, insurers, retailers, and other leading brands, collectively responsible for more than $1.3 trillion in annual commerce. For more information, please visit **www.transmitsecurity.com**.