Castle

# Identity-Aware Bot Detection

## Protecting Against Bot Attacks Requires a New Approach

Bot attacks are growing increasingly more complex by mimicking legitimate user behavior and getting past traditional perimeter solutions. According to the 2019 Data Breach Quickview Security Report, there were more than 7,098 breaches reported in the past year that exposed over 15.1 billion records, most of which were access credentials.

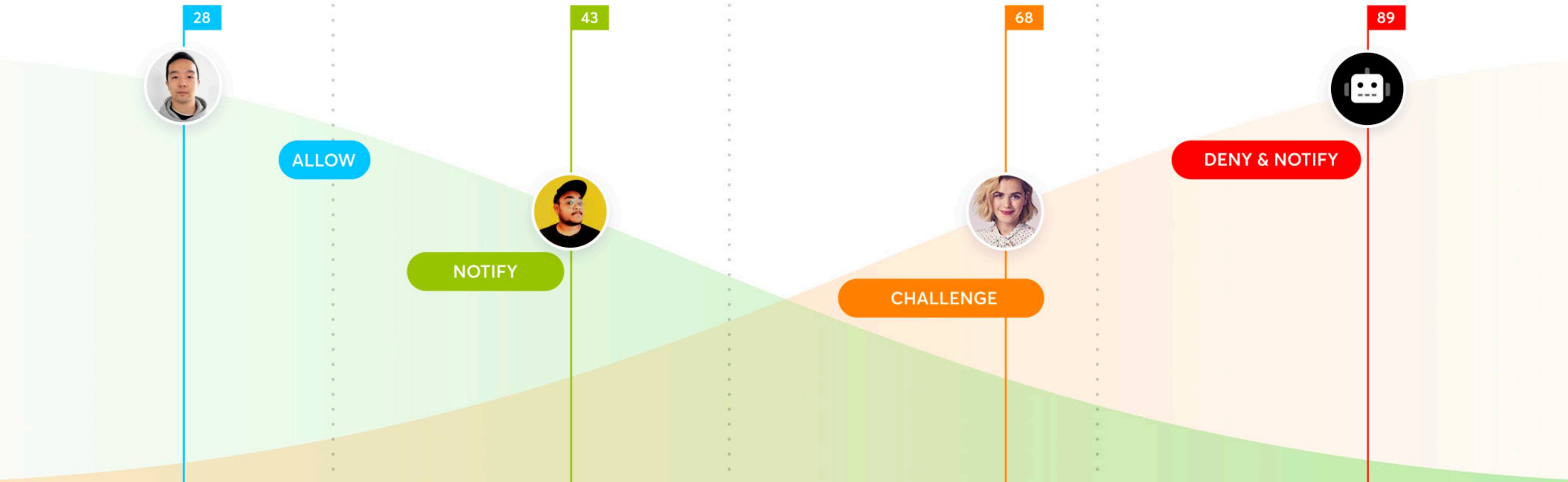
The reason why bot attacks are cleverly targeting user accounts and credentials is because of the wide variety of malicious activities that can be performed, from stealing sensitive PII data to causing financial loss to the user and organization. Bots imitating legitimate user behavior are becoming increasingly indistinguishable from normal human behavior. Organizations need to move beyond traditional bot detection techniques to stop these advanced attacks.

## Stopping Malicious Bot Activity Everywhere: Web, Mobile, or API

Because bot web activity can be indistinguishable from human web activity, organizations need to understand not only a user's identity but also understand that same identity across all platforms: web, mobile, or API. Castle is a cross-platform solution that can stop potential fraud such as fake account creations, credit card stuffing, and account takeovers by tying a user to their device and application activity - everywhere. Castle reduces the number of false positives for all channels of a digital business by dynamically profiling the behavior of a user, no matter what device they are on.

### Protecting User Accounts From

- ✓ Fake Account Creation
- ✓ Carding
- ✓ Account Takeovers
- ✓ Business Logic Abuse
- ✓ Content Spam
- ✓ In-App Scraping
- ✓ Denial of Inventory
- ✓ API Abuse
- ✓ Skewed Analytics



### Castle Redefines Bot Detection by Focusing on Identity

Castle offers a unique approach to protecting organizations against the most advanced bot attacks by layering on the context of a user's identity to traditional bot detection risk signals. While other anti-bot solutions are parsing through web traffic and trying to understand attack tools and traffic origins, Castle offers higher fidelity detection by analyzing Identity behavioral analytics in addition to these traditional risk patterns.

### Traditional Bot Detection Signals

**AUTOMATION TOOLS**

- Sentry MBA
- SNIPR
- Ncrack
- Hydra
- Medusa
- Playwright
- Selenium
- Puppeteer
- Cypress.io
- TestCafe
- PhantomJS
- more

**TRAFFIC ORIGINS**

- Compromised or unknown devices
- Tor Browsers
- Home routers
- Underground VPNs
- Suspicious Internet Service Providers
- Blacklisted IPs
- Malicious Servers and Datacenters
- more

### Castle's Identity Behavioral Analytics

**IDENTITY CONTEXT**

- Suspicious Geolocation
- Language and Time Zone
- Fast Travel
- Device Fingerprinting
- Behavioral Biometrics
- Successful/ Failed Logins
- Non-human Activity
- Inconsistent Event Sequence
- Account Usage Behavior
- Known Compromised Credentials
- more

### Security with The Customer Experience In Mind

Castle contextualizes all user behavior during every digital touchpoint and delivers a consumable verdict both on how to remediate bad behavior and encourage good behavior. With a dynamic risk engine and automated workflows, Castle protects users on any device and safeguards their interactions with web or mobile platforms. The end result is a solution that simultaneously strengthens security while reducing the friction involved with fraud mitigation and identity protection strategies. Castle's new approach to bot detection offers:

- Visibility into user risk from their account, device, and application activity.
- Reduction of fraudulent or risky accounts, yielding lower financial losses.
- Customizable and automated workflows that reduce operational expenses.
- Minimal complexity with easy deployment, management, and administration.
- Optimal end-user experience around registration, account creation, account set up and log in, transactions, resets, and recovery.

From registration to recovery, Castle's identity-aware bot detection is both accurate and actionable, maximizing security without sacrificing user experience.

### About Castle

Castle redefines consumer security by protecting a user's identity from account takeovers, fake account creation, and other types of identity threats throughout their entire journey with your digital business. Instead of focusing exclusively on the threat, Castle puts user experience at the center of the security model by enabling good behavior as well as stopping bad behavior. With risk-based authentication, bot detection, and custom risk policies, Castle offers real-time consumer identity protection that optimizes the customer experience.