Veracity Trust Network

The Bot Protection Market

# Veracity and the Bot Mitigation Landscape

About Veracity

We use AI behavioural analysis to stop malicious human mimicking bots.

Our mission is to identify and block unwelcome bots on web & mobile platforms, in real-time; providing detailed insights into the source of these threats — whether they originate from competitors, foreign actors, or other malicious entities, ensuring organisations are mitigating active bot activity as well as addressing the root causes, strengthening their defences holistically.

We are a multi award-winning bot defence platform, alumni of the UK Government Cyber Runway programme and validated by the Singaporean Government with our 2024 award of the Cyber Security Agency of Singapore CyberCall Innovation Award Winner.

We use advanced machine learning to analyse human and bot behaviour, stopping malicious bots at the browser for highest accuracy.
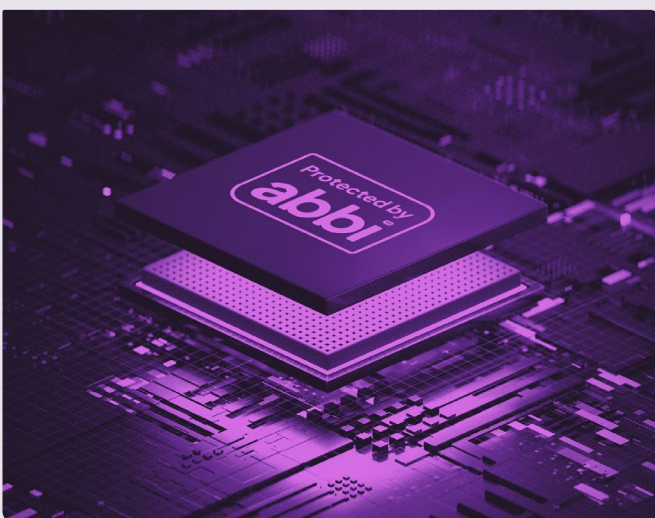
How we use AI to strengthen your cyber defence against bot attacks

Our platform is an AI-based User and Entity Behaviour Analytics (UEBA) cybersecurity solution that can detect non-humans quickly and accurately using micro-behavioural analytics.
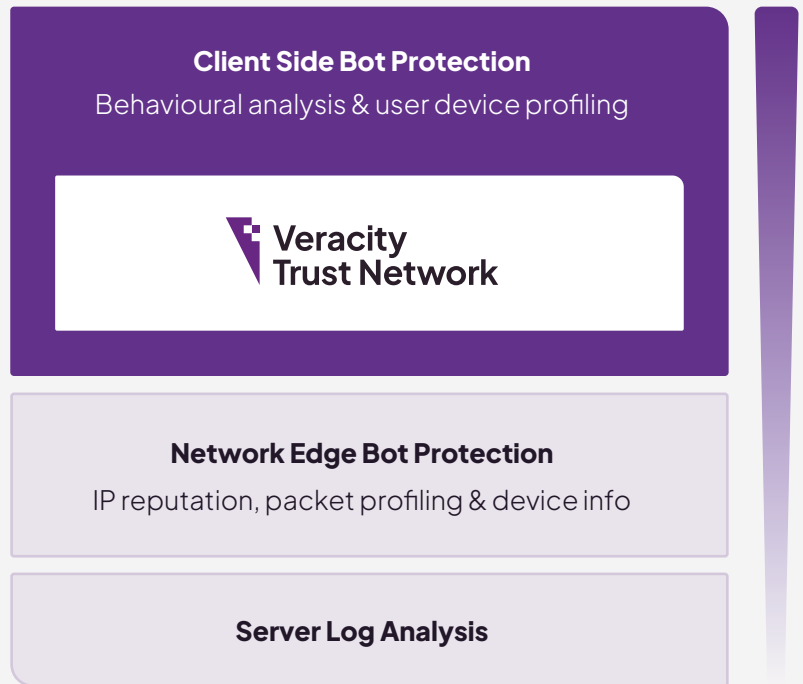
Classifying user journeys as a malicious bot or a human is a task well-suited to Supervised Machine Learning models as this is a binary (two-class) classification problem. Our model is based on the XGBoost (Extreme Gradient Boosting) algorithm due to its high efficiency, flexibility, and performance in supervised learning tasks, particularly tabular classification problems.

How we beat other "bot protection" tools

Many other cybersecurity solutions use the term "bot protection" but they don't mean what we mean, and they don't provide any genuine protection against sophisticated human-mimicking bots.

Veracity works by capturing behavioural patterns directly where the user - or bot - is: directly in the browser or the mobile app. This is the only place where user behaviours are available.

Bot protection tools that operate at the Network Edge or by analysing server logs do not have access to user behaviours which are the only way to tell the difference between a human or a sophisticated, often AI powered, malicious attack bot.

Client Side Bot Protection
Behavioural analysis & user device profiling

Veracity Trust Network

Network Edge Bot Protection
IP reputation, packet profiling & device info

Server Log Analysis

Increased bot protection

> "
> **Implementing Veracity was a real awakening. It highlighted, that even while using a Content Delivery Network (CDN) claiming bot detection capabilities, malicious bot activity was still a substantial concern.**
> Head of Marketing, Insurance Provider

Why Veracity is the best bot protection available

In-browser behaviours

A point solution focused on bot detection where the behaviours needed to detect bots are found: directly in the browser or the mobile app.

This is the only place where the user behaviours, needed to tell the difference between humans and bots, are available.

Sector-specific protection

The only bot protection platform to giving sector-specific bot protection. Bots working on breaking into ecommerce website are different from those trying to scrape content from an online gaming app. Our technology automatically deploys the best defence against the bots that affect you.

Seamless integration

Our platform integrates seamlessly with your security stack and is tailored to your exact requirements

Out-of-the-box, the platform provides an automatic detect & block service (in the DOM). It can also integrate to your SIEM providing real-time threat intelligence on bot activity on your website or mobile app, or provide 'bot detection on demand' through a secure API, for your existing security tools to action.