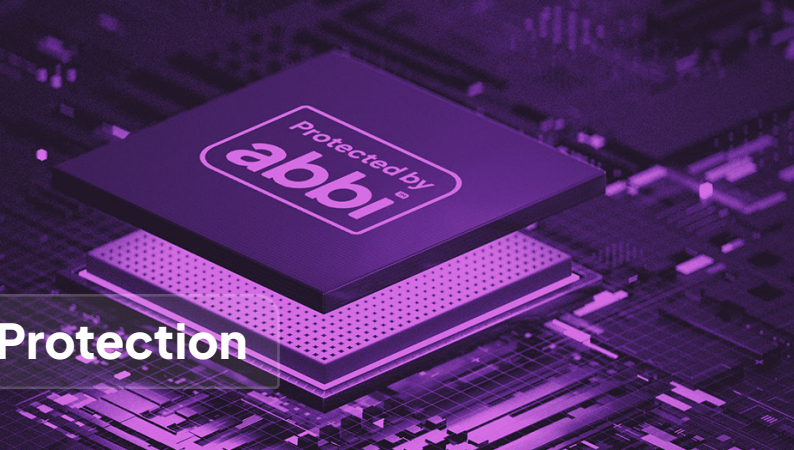


The Bot Protection Market

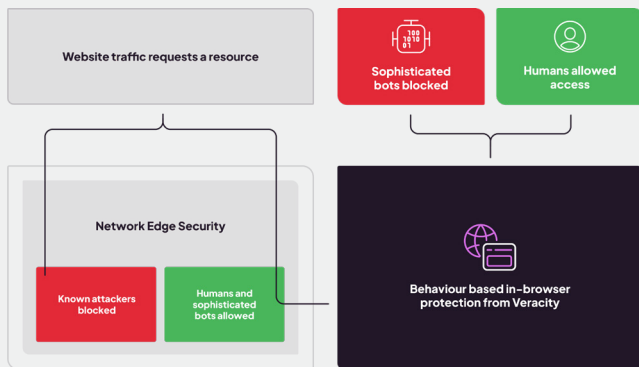
Veracity and Client-Side Bot Protection



Why client-side protection?

Bot networks are increasingly able to bypass network edge and server bot detection tools.

Client-side bot detection tools work by capturing behavioural patterns directly where the user, or bot, is — directly in the browser or mobile app. **This is the only place where such user behaviours are available, making client-side bot detection the only effective way to protect against modern bot threats.**



Adaptive bot blocking intelligence

Our bespoke, patent-pending, bot detection platform — abbi™ — sits at the heart of our defence against bots.

Built on years of data, abbi™ detects the subtle and ever-changing differences between humans and bots, continually adapts as threats evolve to bypass other protection tools, and uses machine learning AI to detect bots with the highest possible level of accuracy.

About Veracity

Veracity is a multi-award winning deep tech cyber company using AI behavioural analysis to stop malicious human mimicking bots.

veracitytrustnetwork.com

Veracity versus other client-side tools



Targeted, sector-specific protection

We automatically deploy the best defence against the bots that affect you. Our targeted, multi-layered & adaptive approach uses a combination of supervised and unsupervised machine learning (ML) models for accurate and tailored bot protection.

Bots scraping content from ecommerce websites are different to those targeting accounts on gambling apps. Our unique bot knowledge allows abbi™ to automatically deploy targeted ML models for specific sectors, geographies, or a combination of both.

abbi™ monitors the success of the deployed model and can fine tune its bot detection capabilities to directly respond to the specific threats in your environment.

In a world where a 2% improvement in bot detection can make the difference between a successful or failed attack, abbi™ can be that difference.

Need an even more tailored model?

We can deploy a specific ML model based on your exact risks and bot threats.



Seamless & bespoke integration

Out-of-the-box, we provide a set and forget detect & block service, in the DOM or on the mobile device.

We can also integrate to your SIEM providing real-time, detailed threat intelligence on malicious bot activity in your existing dashboards. For highly secure platforms, we can provide remote 'bot detection on demand' through a secure API, for your existing security tools to action.