Veracity Trust Network

Web Threat Protection and EDGE Solutions

Why EDGE solutions are losing the arms race

Website traffic

Known attackers

Humans

Sophisticated bots

Session requests a web resource

Network Edge Security
Firewall-as-a-Service (FWaaS)
Network-as-a-Service (NaaS)
Secure Access Service Edge (SASE)
Secure Service Edge (SSE)
Zero Trust Edge (ZTE)
DNS Filters
Distributed Denial of Service (DDoS)

Known attackers blocked

Humans and sophisticated bots allowed

Behaviour based in-browser protection from Veracity
Our machine-learning protection sits in the browser. Allowing us to analyse advanced behaviour to detect and block even the most sophisticated human-spoofing bots.

Sophisticated bots blocked
Our client-side behavioural analysis detects and blocks even the most sophisticated, AI-driven malicious bots.

Humans allowed access
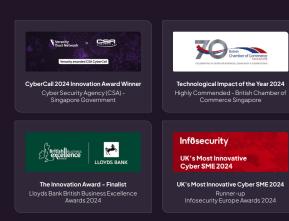Verified human traffic is allowed access to the website or web app.

A key and complementary part of your cyber security stack

In-browser sophisticated malicious bot detection is a crucial part of your security stack to combat the rise in AI-driven malcious attacks. Veracity's Web Threat Protection adds a vital layer of defense, utilising advanced behavioural bot analysis that isn't available to solutions that sit within the EDGE.

Network EDGE technology
Traditional protection methods relying on device/browser fingerprinting, IP blacklisting, and reputational blocking, which detect known attackers and simple bots. But are unable to protect against AI-driven sophisticated malicious bots.

CyberCall 2024 Innovation Award Winner
Cyber Security Agency (CSA) - Singapore Government

Technological Impact of the Year 2024
Highly Commended - British Chamber of Commerce Singapore

The Innovation Award – Finalist
Lloyds Bank British Business Excellence Awards 2024

UK's Most Innovative Cyber SME 2024
Runner-up
Infosecurity Europe Awards 2024

Get protected today

veracitytrustnetwork.com
hello@vtn.live
UK +44 (0) 5603 861 037