Veracity Web Threat Protection

Veracity Trust Network

A key & missing part of your cyber protection suite

We complement your other security systems

Malicious bot detection is an important part of your holistic security strategy. No doubt you have DDoS and WAF protection in place already, along with AV & Malware protection for yourself and your team. Veracity WTP adds a vital layer of defense by detecting and removing malicious bots that get through.

DDOS (Distributed Denial of Service) is a form of attack whereby lots of fake connections are made, overwhelming the target website, or system, and preventing it from responding to genuine traffic which often results in system crash. DDOS prevention systems act before the website but are specific solutions that don't detect bots.

WAF (Web Application Firewalls) is a hardware or software solution that prevent visitors to a website carrying out certain forms of attacks, such as cross-site scripting (XSS), SQL injection or cookie poisoning. WAFs will catch malicious activity by humans and many also use blacklists to block known bot sources, but malicious bots that are pretending to be human, and which regularly change where they come from, will not be detected by WAF.

Veracity Web Threat Protection

Veracity Web Threat Protection is a point solution that focuses on stopping sophisticated malicious bots. Many of the current solutions have a weakness in this capability, and as bots become more sophisticated and AI-driven this area of vulnerability grows. Bots like these are looking for potential ways to break in to your website, or for potential vulnerabilities that can be exploited later. They may also be attempting to set-up fake accounts, blocking items from purchase by genuine users on ecommerce websites, or scraping data. Veracity WTP is focused 100% on stopping these things happening.

> **"Detecting bots is difficult because the sophisticated ones try to appear human and evade detection. Your bot management solution must protect from every OWASP automated threat and be accurate in detecting the difference between human and bot traffic on your website, mobile apps, and APIs.**
>
> Open Web Application Security Project
> (https://owasp.org)

OWASP®

Why this is important?

Data breaches cost upwards of US$160k (£130k) to fix according to the UK National Cyber Security Centre and 60% of small and medium companies go out of business within six months of falling victim to a data breach or cyber-attack.

Research by HSBC on NASDAQ listed firms that suffered a data breach showed share price underperformance of 15.6% over the following 3 years.

64% of consumers are put off using a business that has been the victim of a compromise or breach, according to Experian.

In 2022, Lloyds of London moved to limit systemic risk from cyber-attacks by requesting that insurance policies written in the market have an exemption for state-backed attacks, due in part to attacks from Russian backed or associated hacking groups increasing by 300% since the start of the Ukrainian invasion. Mario Greco, CEO of Zurich Insurance, was reported in the Financial Times on Dec 26th 2022 to say cyberattacks would become uninsurable. **It's down to you to protect your organisation.**

GDPR in the EU & UK, the California Privacy Rights Act in the US and other similar acts impose a duty of responsibility on business owners and staff to secure private data. Malicious bots are already active on your website – we guarantee it – in the event of a data breach, failure to take all reasonable steps to protect your website could be very costly and result in substantial, long-term reputational damage.

Easy to deploy & easy to use

- Veracity Web Threat Protection is a simple deploy solution with no integration overhead – a single piece of JavaScript on your website or websites and we take care of the rest.
- Protects against OWASP attack classifications 7–10 and 12–13 (Automated Bot Attacks and Supply Chain Attacks) where existing technologies do not operate.
- Ultra-fast and ultra-accurate (after the initial 3–month learning phase), with low false positives.
- Control how aggressive or cautious our bot detection engine is for your exact purposes.
- Automatically get notified of which parts of your website are most attacked.
- Works alongside your existing cyber protection, including DDoS and WAF, with no configuration needed.
- No operational overhead and no management overhead.
- Try before you buy – 2–week analysis in "watch-only" mode, producing a report of what bots are already active on your website and what they are doing. No obligation.
- Applicable to the smallest SME through to the largest Enterprise.

We are specialists in what we do

This is what we do: we look for and stop malicious bots on your websites. This is a highly specialist skill and one that requires our full-time attention. Malicious bots change all the time to evade detection, so we work hard to stay ahead and we don't allow ourselves to be distracted!

We are fully transparent and work in your way

It's your website and it's your data, so you can access whatever you need when you need it; whether that be through our reporting dashboard, through our API for integration into your own systems, or by exporting the data so that your own data team can add the data to your BI processes. Whatever, we are there to support you along the way.

veracitytrustnetwork.com
hello@vtn.live
UK +44 (0) 5603 861 037
US +1 (833) 286 6284

VeracityTrust
in veracitytrustnetwork

Veracity
Trust Network