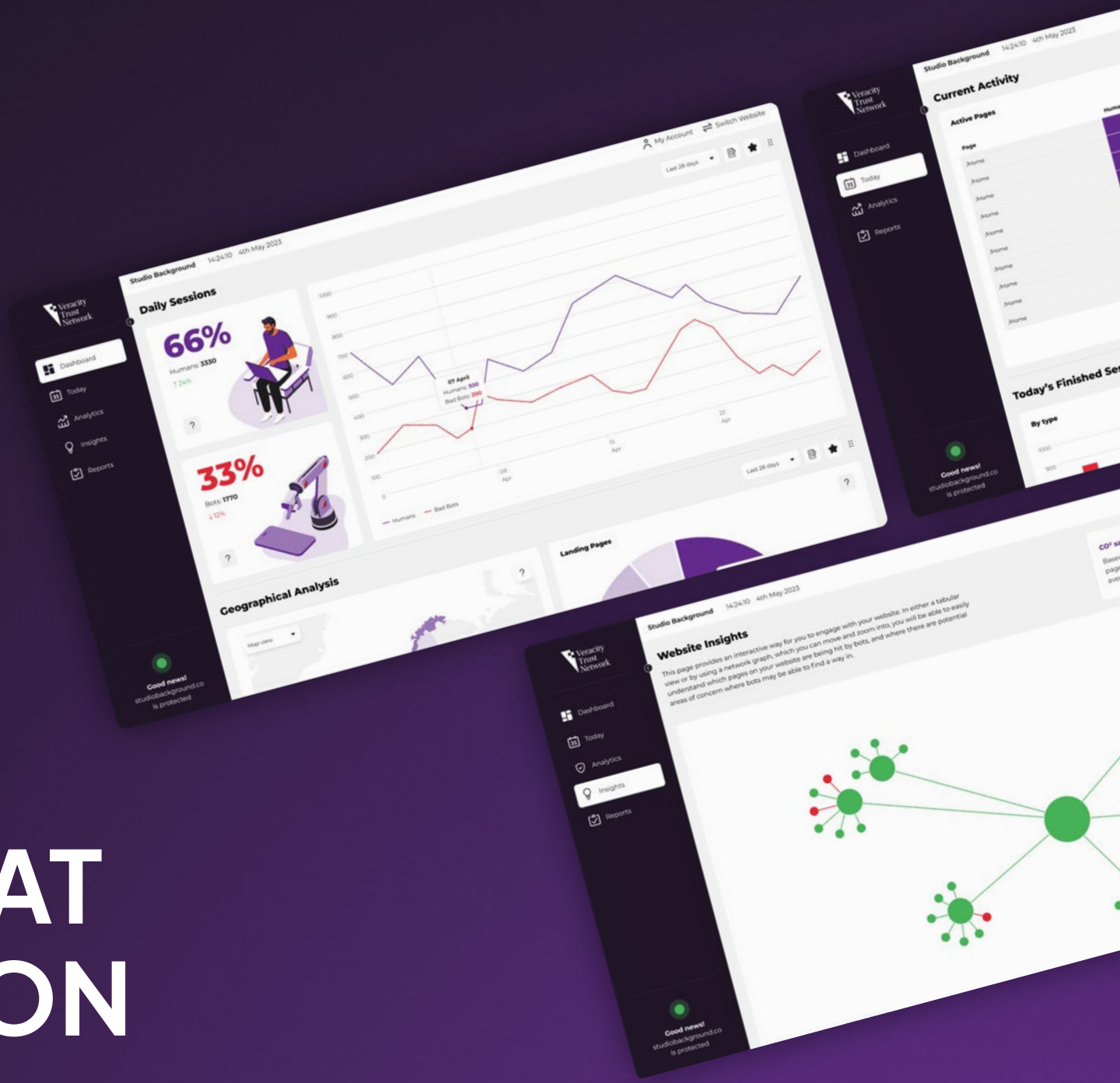
Veracity Trust Network



WEB THREAT PROTECTION

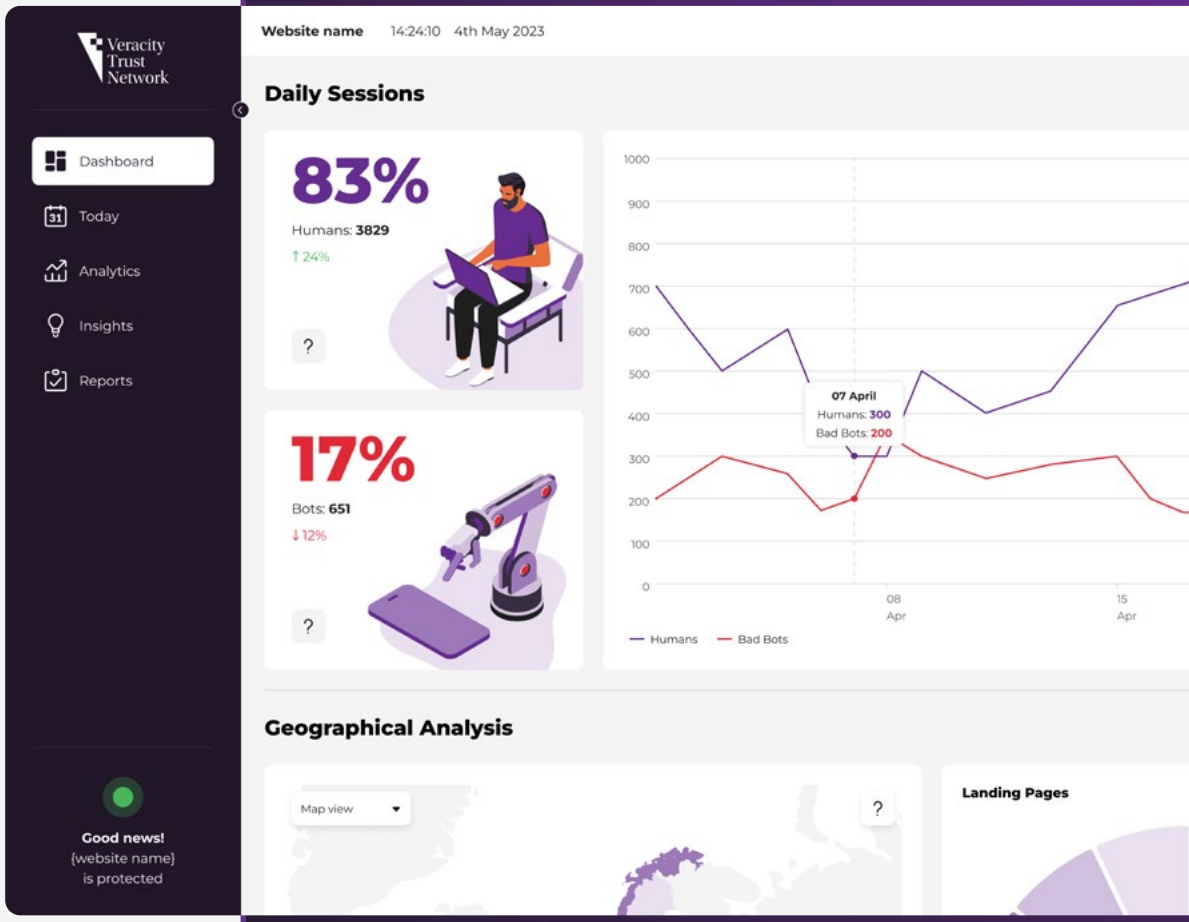
What are the threats?

It's extremely likely that automated bots are generating between 30 and 50% of the traffic to your website.

While some bots are legitimate, such as search engine crawlers, most of this automated traffic comes from malicious bots that continue to increase and evolve.

These bots try to take over your users' accounts, scrape your content and pricing, abuse your payment services, and manipulate inventory.

As well as posing a security threat, bots can also significantly affect operational costs and contaminate your business analytics with false data which can lead to flawed decision making.



This is what a bot problem would look like; as you can see above, Veracity has blocked 651 bad bots from this website in the past month.

What is Web Threat Protection?

Veracity's Web Threat Protection is a bot detection solution that protects your websites from automated attacks. This protection safeguards your:

Online revenue

Competitive edge

Brand reputation

This is done by addressing security and fraud challenges to minimise vulnerabilities, prevent loss, and ensure an efficient customer experience.

Web Threat Protection is applicable to any business operating a website and it:

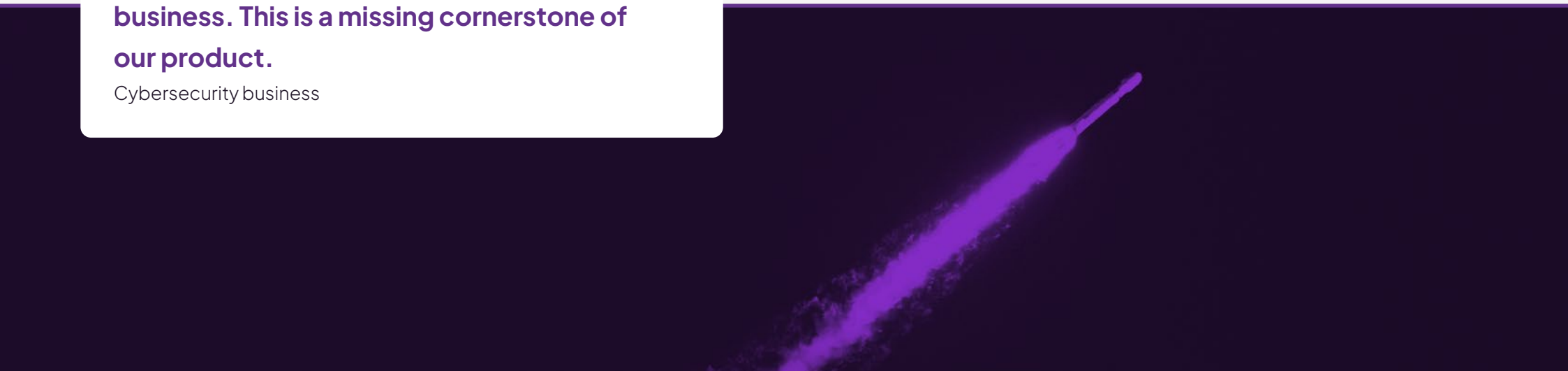
- blocks a wide range of bot attacks
- preserves website performance
- optimising infrastructure costs and security resources.

Our AI-powered bot detection engine detects and blocks automated threats in real time, protecting customer data and reducing the risk of a data breach, without you having to think about it.

Online businesses tell us that they are switching to specialised bot mitigation solutions like Web Threat Protection because existing WAF (Web Application Firewalls) / in-house solutions have severe limitations that advanced bots can bypass, such as:

- not protecting all endpoints, including mobile apps
- failing to prevent malicious JavaScript calls
- being incompatible with and not integrating well with multi-cloud and multi-CDN setups
- requiring all customers to solve CAPTCHA because bot detection facilities are inadequate

> **Veracity has the potential to be such a valuable piece of technology for our business. This is a missing cornerstone of our product.**
>
> Cybersecurity business



A market-leading global proven solution.

We safeguard organisations from the threat of bot attacks, through our deep tech machine-learning solutions which address Security, Fraud and Advertising Technology.

Veracity Trust Network offers numerous benefits to companies in terms of detecting and preventing bot attacks, reducing click fraud, enhancing security, improving website performance, and providing peace of mind.

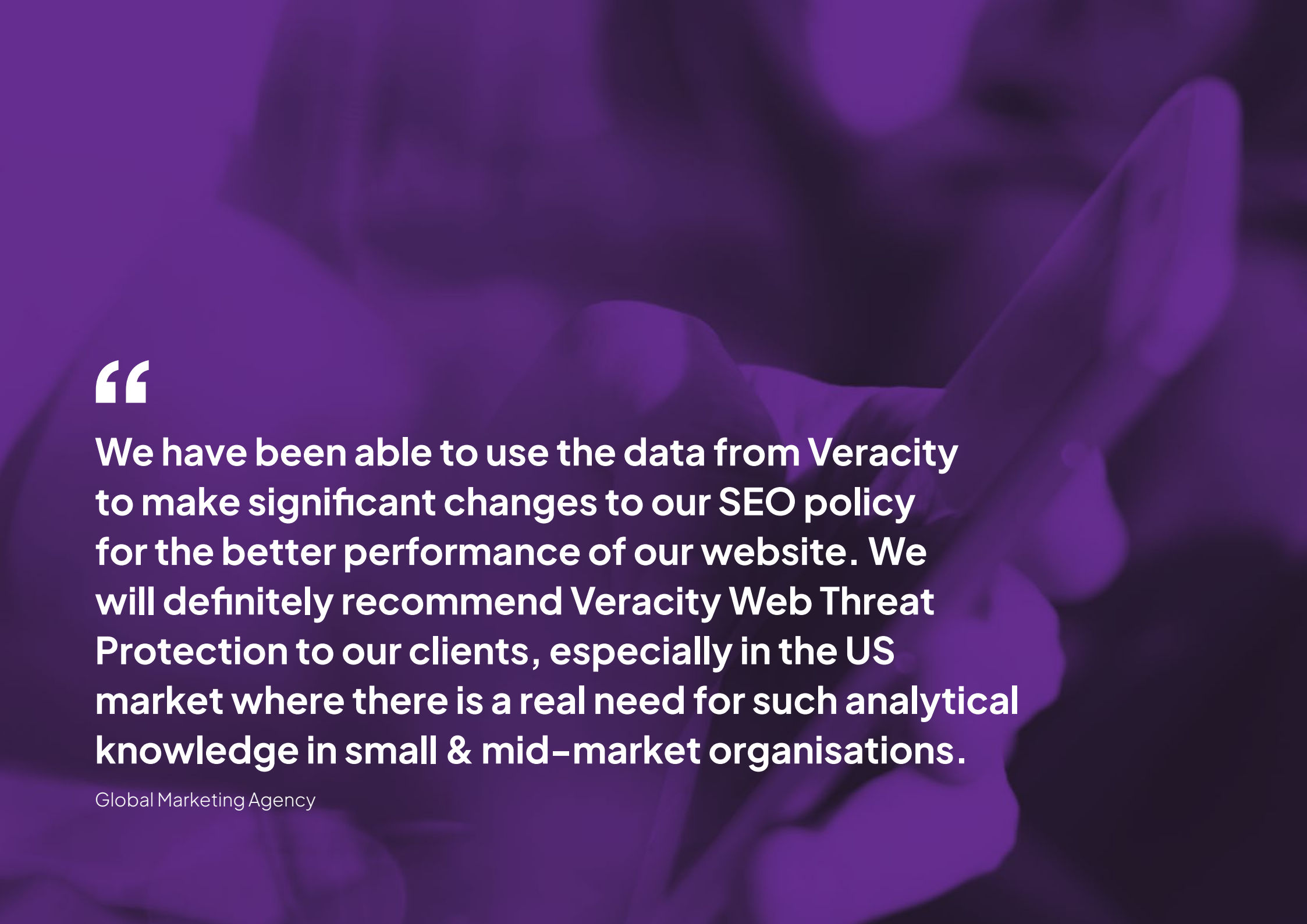
Veracity's Web Threat Protection solution protects website performance, security, and user experience:

Minimise vulnerabilites

Defend from threat of fraud

Prevent loss

Ensure a friction-free customer experience



“

We have been able to use the data from Veracity to make significant changes to our SEO policy for the better performance of our website. We will definitely recommend Veracity Web Threat Protection to our clients, especially in the US market where there is a real need for such analytical knowledge in small & mid-market organisations.

Global Marketing Agency

Veracity Web Threat Protection in detail

Our Veracity Web Threat Protection (WTP) platform is built on sophisticated AI machine learning models that can more accurately detect bots trying to access an organisation's digital presence. The model is trained to detect bots using over 100 behavioural data points in real time and has a greater than 95% probability of accurately detecting a bot on the first page load, which is vast improvement on traditional rules-based models and ML used in older, less sophisticated solutions.

Online fraud has become more sophisticated over the years, making traditional security tools ineffective. As financial incentives grow and attack costs lower, the risk to all organisations increases: from client-side attacks that steal sensitive data by using compromised third-party JavaScript to bots that leverage it to commit fraud, *you need protection from these threats.*

Bots can pose many threats to websites, including performance degradation, data scraping, fraud and manipulation, spam and misinformation, and security breaches. This can have a significant negative impact on a website's performance, security, and user experience, making it important for companies to protect their websites from bots.

Historically, there has been a greater emphasis on protecting networks and servers from cyber threats, but this has shifted as attackers increasingly target web applications and websites, which are less well protected.

This has placed an increased focus on protecting websites, leading to the development of specialised solutions to help identify and block bots while also improving the overall security of the website.

One of the main challenges is keeping up with the speed at which bots evolve. Older solutions are unable to keep up as bots adapt to evade detection. This means that cyber security SaaS firms using AI/machine learning frequently face the risk of 'model drift' - when the accuracy of the data they are using to detect bots declines over time and becomes ineffective at outsmarting bots.

The focus Veracity place on researching how bots behave and evolve, puts us at the forefront of bot detection and prevention solutions, as evidenced by our recent shortlisting as "Cyber Security Company of the Year" at the UK Business Tech Awards 2023 and "AI-enabled Data Solution of the Year" at the dataIQ awards 2023.

Veracity Trust Network

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

VeracityTrust
veracitytrustnetwork