Veracity Web Threat Protection Battle card – July 2024

Target Market	Website Threat Protection (WTP) is a solution that can be used by any business that operates a website. It blocks a wide range of bot attacks, which helps to preserve website performance and optimize infrastructure costs and security resources. It is important for businesses that want to protect their data, clients, reputation, and future. This is especially relevant for small and medium-sized businesses that may have budget or knowledge constraints but are just as vulnerable to fraudulent activity as larger enterprises. Businesses that handle sensitive customer information, such as legal firms, e-commerce sites, insurance and financial institutions are at the highest risk of being targeted by malicious bots. Online marketplaces, travel and hospitality companies, gaming websites, healthcare organizations & the public sector are also vulnerable to bot attacks. They are likely to have valuable data such as personal & financial information that can be used for fraudulent purposes and are therefore prime targets of automated bot attacks designed to steal data or disrupt their services. WTP is suitable for businesses of all sizes that have an online presence and want to protect their website from automated attacks. It is particularly useful for businesses that rely on their website for revenue generation and customer engagement. The personas that would look to purchase WTP include IT managers, security professionals, and business owners. IT managers would be interested in WTP because it can help them minimize vulnerabilities and defend against threats while ensuring a friction-free customer experience. Security professionals would be interested in WTP because it can help them prevent loss and protect their organization's brand reputation. Business owners would be interested in WTP because it can help them safeguard online revenue and maintain a competitive edge.

Elevator Pitch	Veracity Trust Network safeguards organisations from the threat of bot attacks on their public-facing digital platforms. Protect your business from bot attacks and preserve website performance with Website Threat Protection (WTP) 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 organizations increases. From client-side attacks that steal sensitive data from compromised third-party JavaScript to bots that leverage it to commit fraud, you need protection from these threats. Veracity's Website Threat Protection (WTP) is a machine-learning bot detection solution that protects websites from automated attacks. It addresses the twin challenges of security and fraud by minimising vulnerabilities and defending against threats while preventing loss and ensuring a friction-free customer experience. Bots can also significantly affect operational costs and contaminate business analytics with false data, which can lead to flawed decision-making.
How does WTP work? / Positioning	Automated bots are likely generating over 50% of the traffic to websites. 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 affect businesses by committing online fraud through, for example, account takeover or competitive price scraping. Reduce the adverse business impact and gain visibility and control over human, good bot, and bad bot traffic without imposing friction on legitimate users. These bots try to take over users' accounts, scrape content and pricing, abuse payment services, and manipulate inventory.

	Our Website Threat Protection (WTP) prevents fraud before it's committed and reduces exposure to fraud and limits the risk to your business. WTP stops bots and helps companies maintain brand reputation, avoid costs and losses associated with security issues. WTP reduces the threat of fraud and is there to maintain your customer's confidence, loyalty, and trust. There is a better customer experience because WTP detects bots without unnecessary friction on legitimate consumers, leading to improved conversion rates. Please Note that – Other solutions and Products focusing on DDoS protection (Distributed Denial of Service), WAF protection (Web Application Firewall), Malware and Anti-virus protection do NOT prevent 'bad bots'. • WAF (blocking specific IP addresses or ports) and scanning for XSS or SQL injections – are all valid but will not detect general bot activity for the things we talk about. • DDoS – nothing to do with bot protection. • CDN (Content Delivery Network) – nothing to do with cybersecurity at all, this is about better performance. Bots pose many threats to websites, including: • Performance degradation: Large numbers of bots can slow down website performance, increase hosting costs and in extreme situations, cause it to crash. • Data scraping: Bots can scrape sensitive data from websites, such as personal information, financial fraud, and manipulation: Bots can be used to manipulate online transactions and inflate website traffic, leading to misleading analytics and business decisions. • Spam and misinformation: Bots can spread spam and misinformation on websites, harming a company's reputation and user trust.

	• Security breaches: Bots can exploit vulnerabilities in a website's code, leading to security breaches, reputational impact, and loss of sensitive data. 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 as the protection around more traditional targets gets stronger and therefore harder to break. This attention by attackers has resulted in an increased focus on protecting websites from bot-related threats, leading to the development of specialized software solutions to help identify and block bots while also improving the overall security of the website.
Why Veracity? The Marker Relevance Our MLM machine-learning model tech	Veracity Trust Network was born from a digital agency wanting to deliver accurate data and better marketing campaign results to its clients. Founders, Nigel Bridges, Mike Townend and Stewart Boutcher, developed a solution which combines ad fraud prevention with accurate marketing campaign data. Veracity's Ad Fraud Prevention solution is recognised in the industry for championing transparent and accurate marketing data and reducing ad spend waste. It saves wasted budget and makes campaigns far more effective can improve advertisers' results by up to 50%. Veracity Trust Network has taken our core IP – the ability to distinguish between humans and 'bots accurately' – and turned that into a solution applicable to all business sectors where it is important that 'bad bots' are not entering and interfering with websites. This product is known as Veracity Website Threat Protection (WTP).

The Marker Relevance	One of the main challenges is keeping up with the speed at which bots evolve. Over time, bots adapt to evade detection and slip under the radar, where this rapid evolution means that cyber security SaaS firms 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. Historically, the technology works via a rules-based engine, meaning that a defined set of rules is responsible for determining whether the user is a bot or human. This has meant that the rules must be continually retrained with fresh data to stay up to date with bot behaviours and remain effective. Veracity Trust Network has built a machine-learning model that can more accurately detect bots trying to access an organisation's digital platform. The model is trained to detect bots on new datasets and behavioural data points in real time and has a 95% probability of accurately detecting a bot, which is an improvement on the current rules-based model.
Our Unique Selling Points (USPs. Differentiators)	Gartner's current Magic Quadrant for Cloud Web Application and API Protection strategic planning assumptions are: *By 2024, 70% of organizations implementing multi cloud strategies for web applications in production environments will favour cloud web application and API protection platform (WAAP) services over WAAP appliances and IaaS-native WAAP.* *By 2026, 40% of organizations will select a WAAP provider based on its advanced API protections and web application security features — up from less than 15% in 2022.* *By 2026, more than 40% of organizations with consumer-facing applications that initially relied only on a WAAP for bot mitigation will seek additional anomaly detection technology from specialized providers — up from less than 10% in 2022.*

	USPs. Differentiators In summary • Competitive commercial pricing compared to the established and larger organisations such as Akamai and Cloudflare • We specialise in Bot protection and focus all our energy and talent on these aspects as defined by OWASP - Open Web Application Security Project, Attack Classification • We have an advanced machine-learning model that can more accurately detect bots trying to access an organisation's digital platform, which has a 95% probability of accurately detecting a bot. • We are new to the market, with patented technology and an agile and flexible organisation to work with • Very easy to implement – no changes to the 'Customers' stack, adds straight in

Target Buyers & How WTP addresses their challenges

Target Buyers & Job Titles	CEO/Business Owners	IT Manager/ CTO	Security Professional
How WTP addresses their challenges	• Protect their business • Protect their position, as an owner their reputation and that of the business • Safeguard online revenue and maintain a competitive edge	• Ensure systems don't break and data is lost • Will help them minimise vulnerabilities • Defend against threats	• Can help them prevent loss • Protect their organisation's brand reputation
Impact and Consequences	• Attack could cause their business to go under • Irreputable damage to reputation	• Ensuring a friction free customer experience	• Attack could cause the business to go under • Irreputable damage to reputation

WTP Proof Points

Brand Pillars / Buyers	Hiscox Insurance (small businesses)	Hiscox Continued	Zurich	What do the 'experts' say about protecting websites from bots?
Supporting evidence & examples from Innovate, customers etc.	According to Hiscox Insurance cybersecurity issues, including website hacking costs the average small business £27,500 to recover from in terms of direct costs. Plus, indirect costs such as damage to reputation, the impact of losing customers and difficulty attracting future customers. According to the latest Hiscox Cyber Readiness report in 2022, businesses increasingly view cyber challenges as a dominant risk; it is ahead of the pandemic, economic downturn and skill shortages. This comes as the scale of the problem continues to grow	The number of firms facing attacks has risen and cyber attacks are becoming more severe. What's more, small and medium sized businesses are bearing the brunt. Firms with revenues of $100,000 to $500,000 now get as many attacks as those in the $1 million to $9 million bracket	Insurance premiums continue to spiral up as insurers ger more data on how frequent attacks have become and how much damage they cause. Indeed, Mario Greco, Chief Executive at insurer Zurich says that cyber attacks will become uninsurable, particularly those involving state actors (Lloyds of London has announced an exemption for state actors)	Most experts agree that protecting websites from bots is a critical component of a comprehensive cyber security strategy. While there may be different approaches and tools used to protect networks and servers, they are ultimately part of the same overall security posture and underlines the importance of taking a holistic approach to cyber security that incorporates both network and website security

Competitor Analysis

	COMPANY/PRODUCT FOCUS			FUNCTIONALITY				MARKET AND COMMERCIAL POSITIONING			
	Company focus on bot detection	Bot detection stand-alone or part of a suite/service offering	API access available for client own platform integration	Detects bot activity using AI/ML, behaviour metrics, etc	Blocks or notifies about bots when detected	Continual journey evaluation	Cleanses bots from marketing analytics data	Applicable to every website owner (small to enterprise) across all verticals	Easy Deployment	Zero User / UI Impact	Easy to engage freemium SaaS model starting with £0 deploy
Veracity	**Y**	**Standalone**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
reCAPTCHA (Google)	N	Standalone	Y	Y	Y	N	N	Y	Y	N	Y
SEON	Y	Standalone	Y	?	Y	Y	N	N	N	Y	N
DataDome	Y	Suite	Y	?	Y	Y	N	N	N	Y	N
NuData	Y	Standalone	N	Y	Y	Y	N	N	N	Y	N
Behaviosec	N	Suite	N	Y	Y	Y	N	N	N	Y	N
Arkose Labs	Y	Suite	N	Y	Y	N	N	Y	Y	Y	N
Netacea	Y	Suite	Y	N	Y	Y	N	N	N	Y	N
Imperva	Y	Suite	Y	Y	Y	N	N	N	N	Y	N
Radware	Y	Suite	Y	?	Y	Y	N	N	N	Y	N
Human	Y	Suite	Y	Y	Y	Y	N	Y	Y	Y	N
Cloudflare	N	Suite	Y	Y	Y	N	N	N	N	Y	Y
ThreatMetrix	N	Suite	N	Y	Y	Y	N	N	N	Y	N
Kasada	Y	Standalone	N	?	Y	N	N	N	N	Y	N
Anti Virus	N	N	N	N	N	N	N	Y	Y	Y	Y
Anti Malware	N	N	N	N	N	N	N	Y	Y	Y	Y
WAF	N	N	N	N	N	N	N	Y	Y	Y	Y
DDos	N	N	N	N	N	N	N	Y	Y	Y	Y

	How we win: Brand and Market Awareness Collateral for Lead Gen and Sales in place - 1 pager, brochure, case studies etc, and whitepaper(s) New SE and ISR / BDR for WTP Marketing campaigns to specific sectors Focused Lead Generation through personal networks and where we have a strong innovative reference or fit.
Current customers – Case Studies	6LM IDACS Gales Navima Caspian insurance
Company Profiling to uncover (not all in the first call)	Company Profiling to uncover (not all in the first call) • Public-facing digital platforms that hold personal or financial information. • Where their website is the main vehicle for eCommerce and Sales activities • Number of visitors? • Unregulated or regulated industries • HQ in the UK? /If not nature of business in the UK • Scope/opportunity for Veracity WTP • If eCommerce is present, then touch upon AFP if appropriate.
Understand/qualifying /probing questions.	These will be defined alongside initial messaging for outbound lead generation

Objection Handling	Is it proven? Yes I have an in-house solution. No in-house solution can do what we do with our advanced MLM built-in patented technology. I already got a Protection Application. What do you have? Explain why we are different in terms of 1. Our Company 2. Our approach to business and 3. Our solution I don't have a problem. Yet! Quote WTP proof points and Gartner's expansion According to the UK government's Cyber Security Breaches Survey 2022, 39% of UK businesses identified a cyber-attack in the last 12 months[1]. In addition, Check Point reported that UK organisations experienced an average of 788 weekly cyber-attacks across 2022, marking a 77% increase from 2021[2]. Why should I be at risk? Everyone is at risk, previously big companies such as Uber, WH Smiths, and recently BBC, BA and Boots. According to the UK government's Cyber Security Breaches Survey 2022, 39% of UK businesses identified a cyber-attack in the last 12 months[1]. In addition, Check Point reported that UK organisations experienced an average of 788 weekly cyber-attacks across 2022, marking a 77% increase from 2021[2]. Company Background & Financials: Veracity was born from a digital marketing agency in 2016 that wanted to deliver accurate data and better campaign results to its clients. With a lack of transparency in the ad tech industry, and a growing awareness of ad fraud, the founders, Nigel Bridges, Mike Townend and Stewart Boutcher, developed a solution which combines ad fraud protection with accurate marketing campaign data. In H1 2023 we have taken this core IP – the ability to distinguish between humans and 'bots accurately' – and turned that into a solution applicable to all business sectors where it is important that 'bad bots' are not entering and interfering with websites. This product is known as Veracity Website Threat Protection. We are backed by private equity.