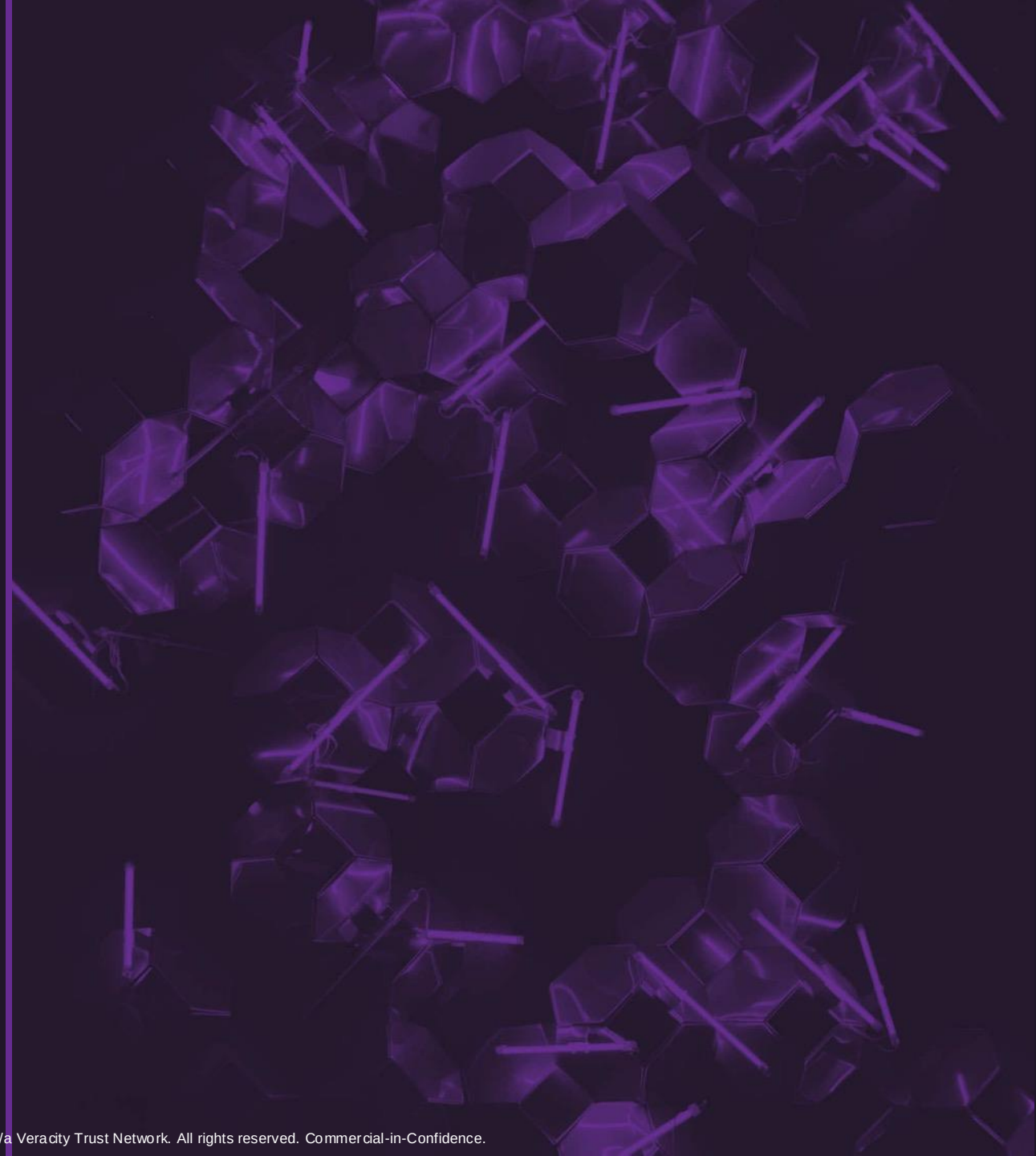
Veracity Trust Network

Partner Onboarding

www.veracitytrustnetwork.com

Who We Are



Our Mission

Malicious bots are constantly evolving, and so are we. Our patent pending, machine-learning bot protection lives on your digital estate, analysing micro-behaviours, to identify and block threats in real-time. Put simply — **we block what others don’t.**

Sales Stack

Global presence

We’re headquartered in the UK, with a subsidiary company in Singapore. We’re also highly active in the UK, Asia Pacific, and the GCC. With clients in the US & EU as well.

Advanced behavioural protection

Our patent pending, machine-learning protection goes beyond basic behaviours to block even the most complex AI threats.

Bot threats we stop

Data theft. Fake account creation. Data scraping. Account takeovers. Attack scouting. Basket blocking. Data contamination. Ad abuse. Budget waste.

What we protect

Abbi (our machine-learning model) protects digital ads (Ad Fraud Prevention) and websites or web apps (Web Threat Protection) from sophisticated bots.

Our Audience

Organisations vulnerable to the growing threat of sophisticated malicious bots on their website and looking to protect their ad budget from fraudulent bot clicks.

Why we’re different

We’re the only bot defence platform that sits Beyond the Edge to utilise real-time behavioural analysis to detect and block even the most complex bots.

Award-winning protection

Regional Winner
Tech Nation Rising Stars Awards 2020

Best Martech Innovation Winner
Prolific North Tech Awards 2021

Cyber Award Winner
Tech Nation Rising Stars 3.0 Awards 2021

Best Marketing Tool Winner
B2B Marketing Expo Innovation Awards 2021

Innovation of the Year Winner
Digital City Award 2022

Innovation in Cyber Award Finalist
The National Cyber Awards 2022

Emerging Technology of the Year Finalist
UK IT Industry Awards 2022

Best Innovation Winner
Best Business Awards 2022

Best Digital Tool or Software Finalist
Northern Digital Awards 2022

Tech Entrepreneur of the Year, Stewart Boutcher, Finalist
Global Business Tech Awards 2023

AI-Enabled Data Solution of the Year Finalist
Data IQ Awards 2023

Tech Innovation of the Year Winner
Leeds Digital Festival Awards 2023

Cyber Security Company of the Year Finalist
UK Business Tech Awards 2023

Best Use of AI - Highly Commended
Prolific North Tech Awards 2023

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

The Innovation Award Finalist
Lloyds Bank British Business Excellence Awards 2024

Proud alumni of the UK Government Cyber Runway 2023 Cohort, for leading UK cyber companies.

Global AWS Technology Partners.

Corporate partner of the Association of Information Security Professionals (AiSP) in SE Asia.

AiSP
Advance Connect Excel

Clients

UK & Europe

CaspianInsurance

CHATTER
making people matter

Genpower

iDACS
WORKING SMARTER

moneypenny

NAVIMA

Recognition

VIDRATE
Enhanced Hydration

Asia Pacific

Asteria
VISIONS

BitCyber
Securing Your Business

custom media

DD2 MEDIA

dex

QV

webcada

zen8labs

United States

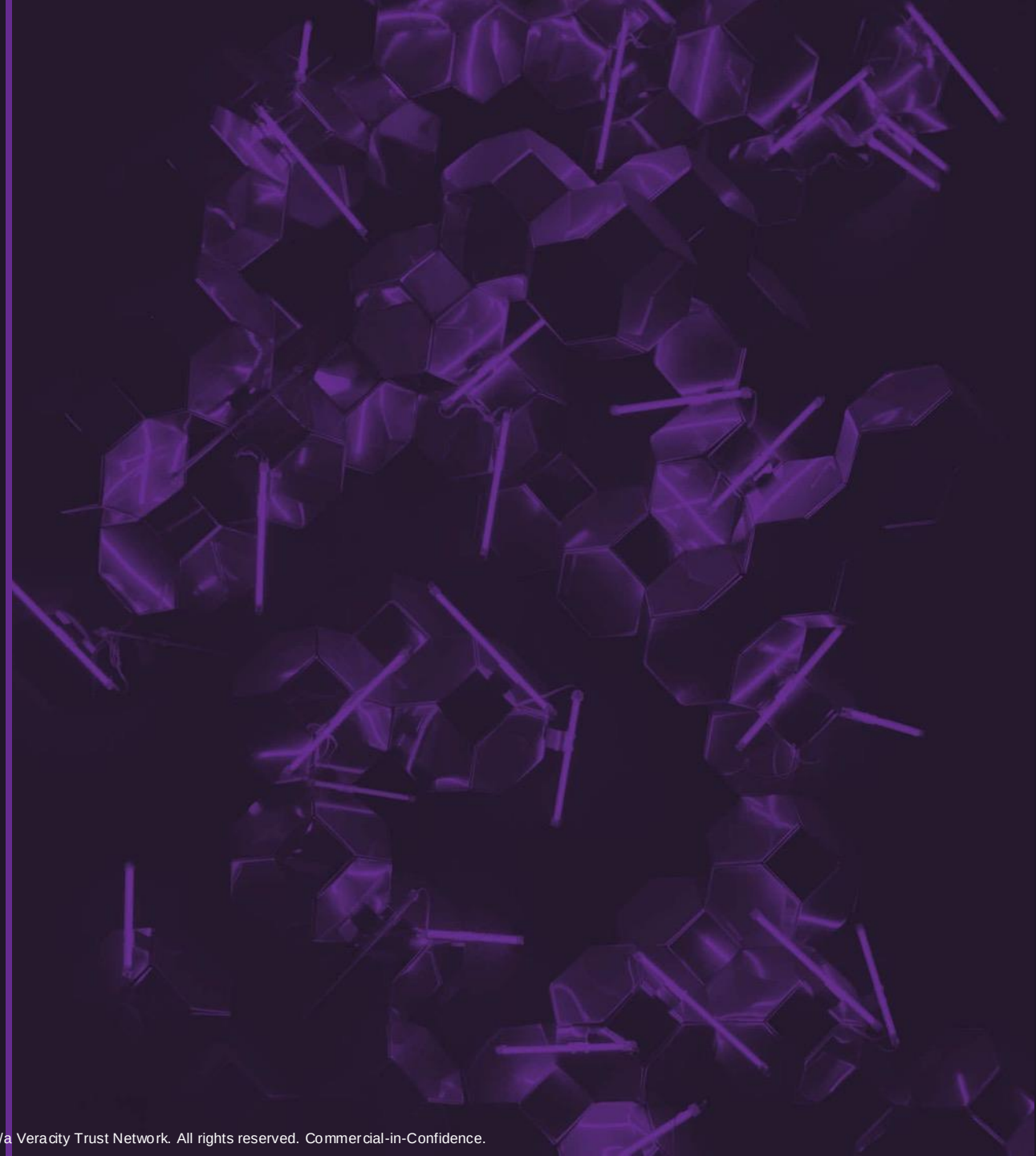
fbcomms.

PlayStar

RESORTS
CASINO.COM

Island Jay
10 Years

The Bot Problem



The scale of the problem

30%

of all traffic to websites is from sophisticated malicious bots

$4.45m

the global average cost of a data breach*

11%

of UK businesses and 8% of charities experienced cybercrime in the last 12 months**

~50%

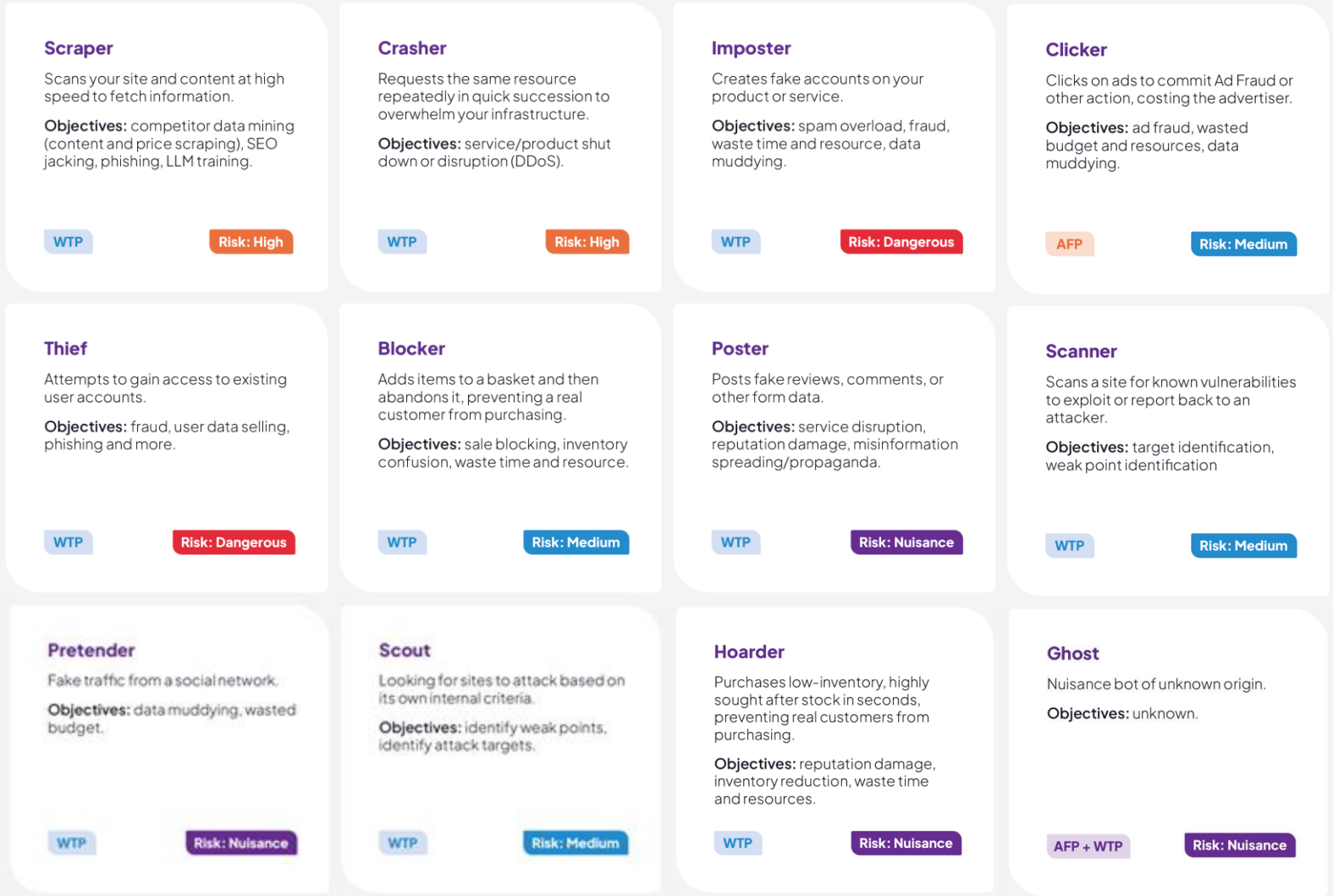
Of consumers said they had stopped doing business with a company known to have experienced data loss through cybercrime***

*Ponemon Institute survey on behalf of IBM. **UK Cyber security breaches survey 2023. ***IBM Report — the Cost of Data Breaches

What are malicious bots doing?

Malicious bots can be classified into 12 types based on what objective they are designed to accomplish.

These range in risk level from **nuisance** through to **dangerous**. And objectives from phishing and DDoS attacks to data theft and wasted budgets.



Industry Breakdown

Automotive
Price scraping, data scraping, inventory checking

Business Services
Attacks on the API layer, data scraping, account takeover

Education
Account takeover for students & course availability, scraping research & data

Entertainment & Arts
Account takeover, price scraping, inventory checking, scalping

Financial Services
Account takeover, card cracking, content scraping

Food & Beverage
Credit card fraud, gift card fraud, account takeover

Gaming & Gambling
Account takeover, odds scraping, account creation for promotion abuse

Government & Public Services
Account takeover, data scraping of business & voter information

Healthcare Services
Account takeover, content scraping, inventory checking, appointments/availability

Information Tech
Account takeover, scraping

Marketing & Agencies
Custom content scraping, ad fraud, denial of service

News & Media
Custom content scraping, ad fraud, comment spam, fake accounts

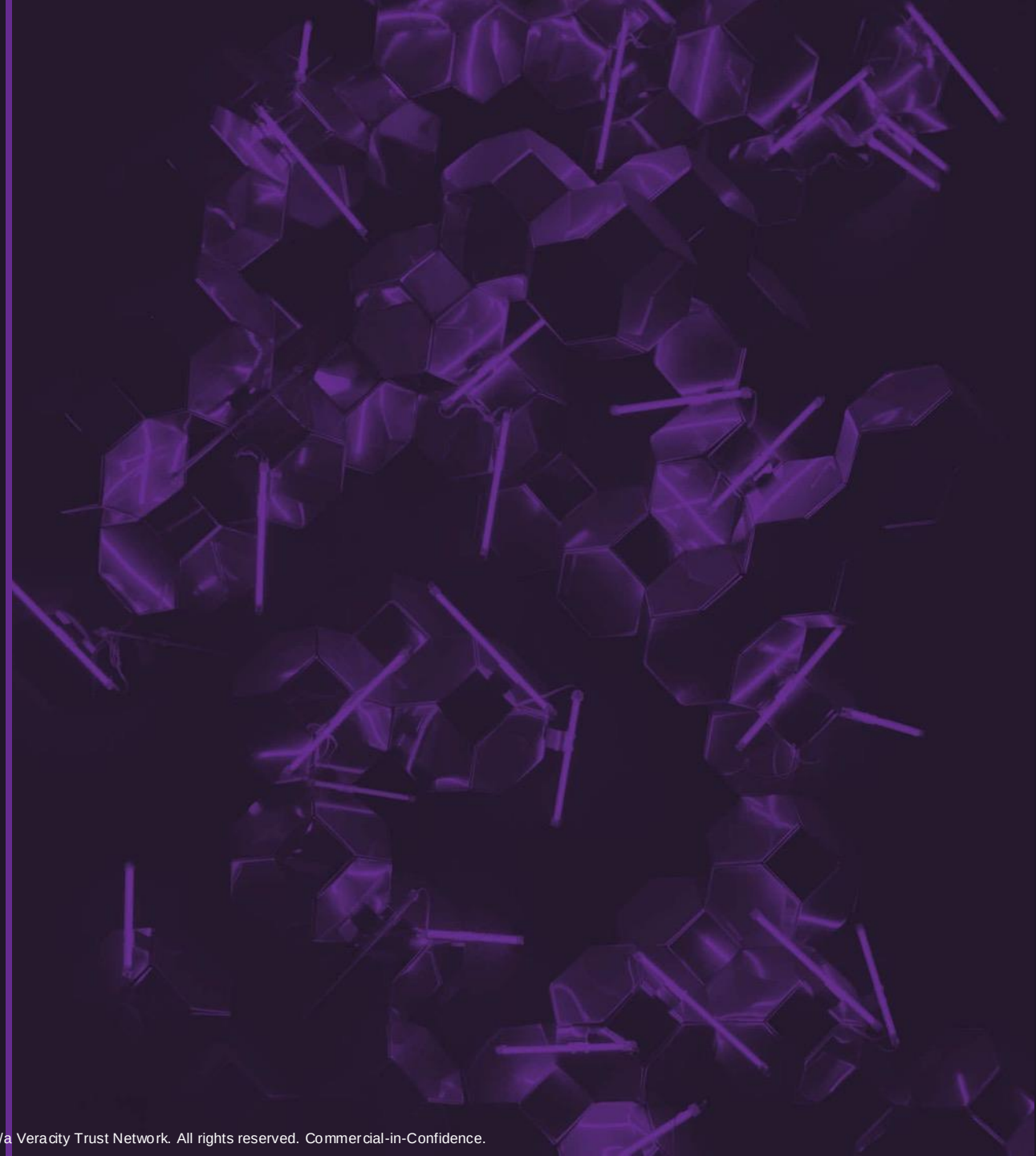
Retail & eCommerce
Denial of inventory, credit card fraud, gift card fraud, account takeover, data and price scraping

Sports
Sports updates, news, live score services data scraping (live scores, odds, etc)

Telco
Account takeover, competitive price scraping

Travel & Airlines
Price & data scraping, skewing of look-to-book ratio, denial of service, price scraping, account takeover

The Veracity Protection Platform

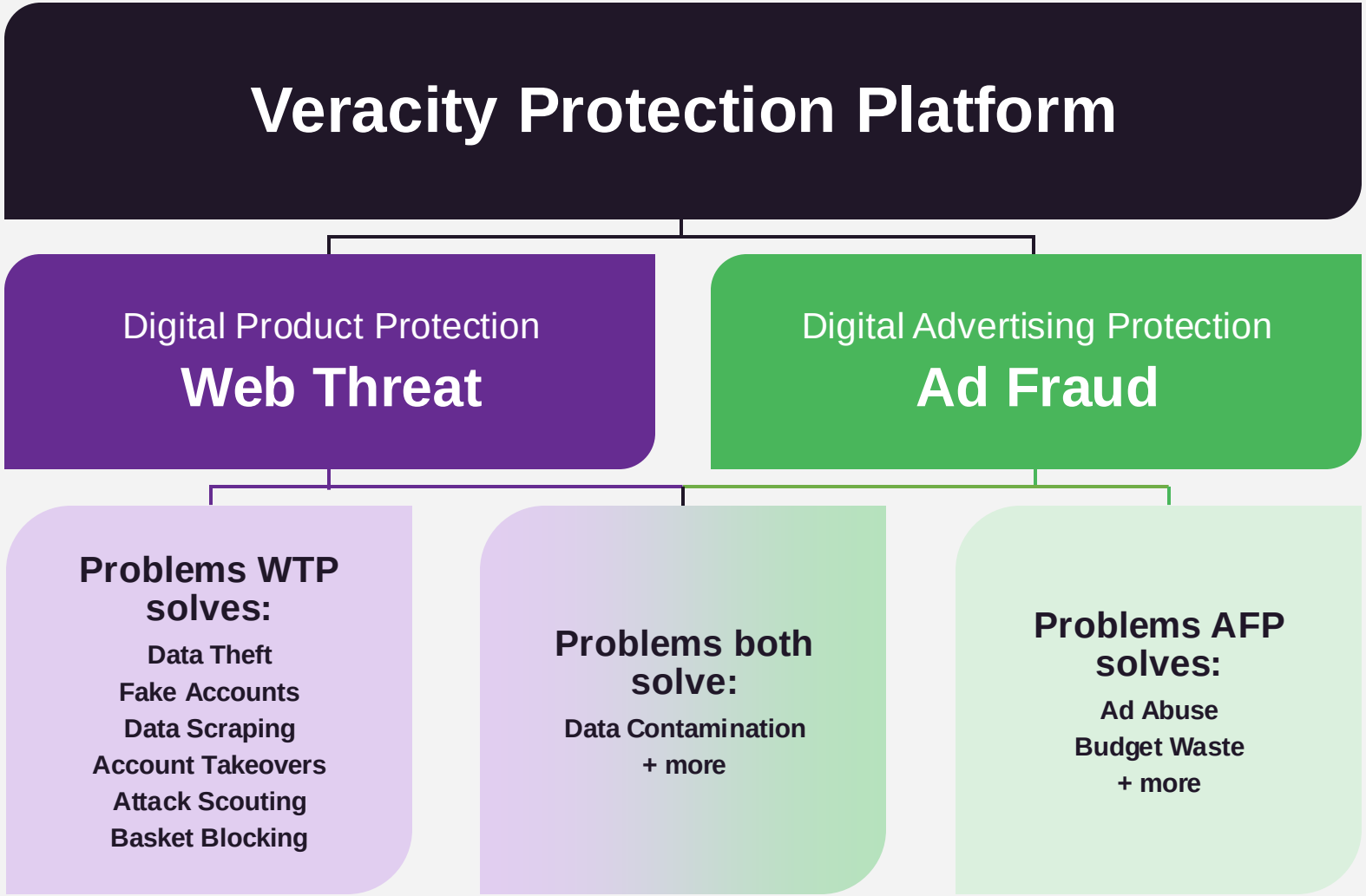


The Veracity Protection Platform

The Veracity Protection Platform defends your digital ads and products from sophisticated bots.

Our modular platform includes Ad Fraud Prevent (for organisations running ads) and Web Threat Protection (for organisations with a website, web app, or mobile app). Both products are powered by Abbi, and benefit from the same machine-learning, behavioural analysis to detect and block bots.

And better still, both products are visible in one dashboard, so all the data is at your fingertips.



Ad Fraud Prevention

Block bot clicks and cut digital ad budget waste by up to 66%.

For organisations running digital ads

Bot detection solutions that protect your online advertising from automated attacks. Ad Fraud protection safeguards your marketing budget, empowers marketers to accurately measure results, and reduces ad budget waste by up to 66% for brands and agencies.

Web Threat Protection

Stop malicious bot attacks against your websites — or your clients'.

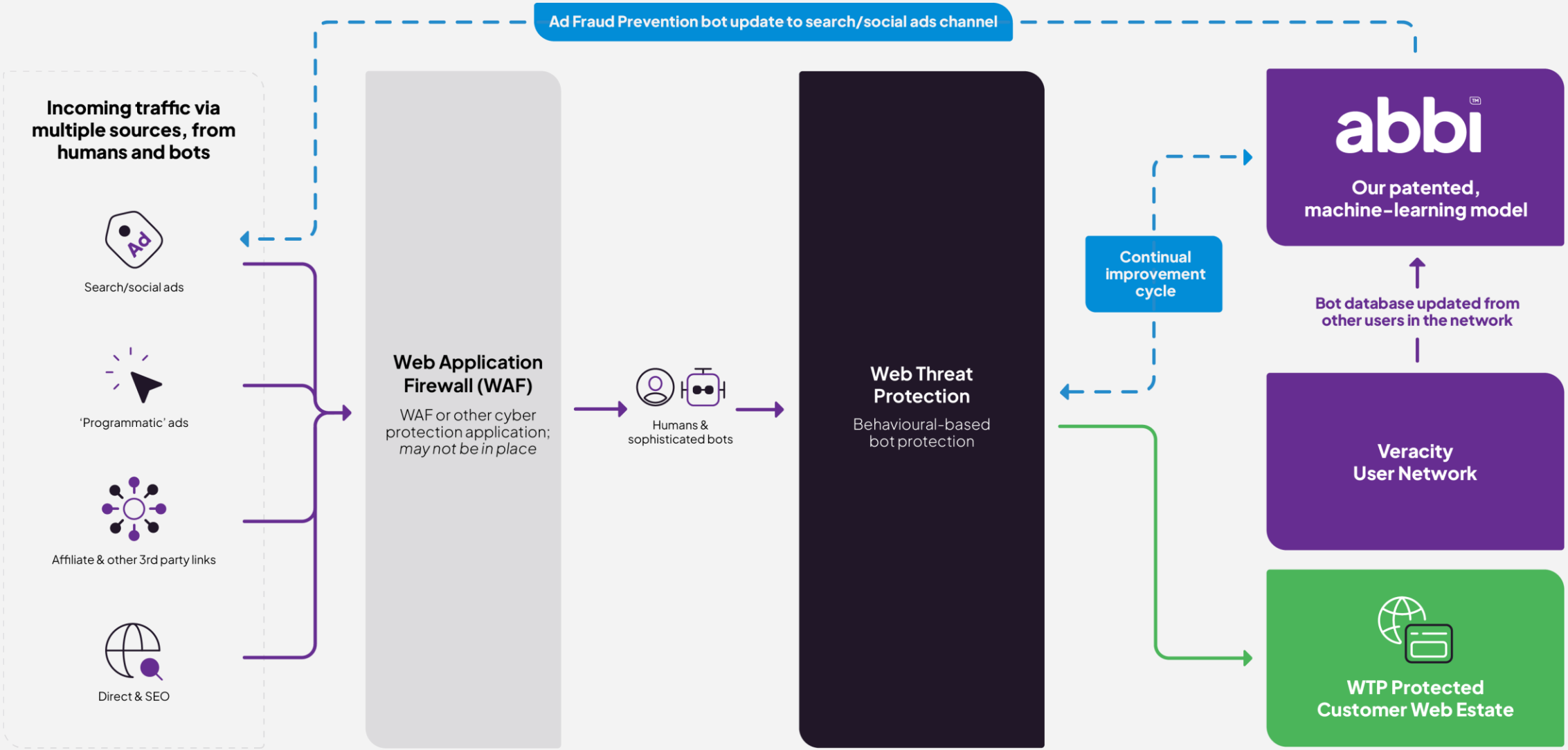
For organisations with a website or webapp

Bot detection solutions that protect your websites from automated attacks. Safeguarding your online revenue, competitive edge, and brand reputation by addressing security and fraud challenges to minimise vulnerabilities, prevent loss, and ensure an efficient customer experience.

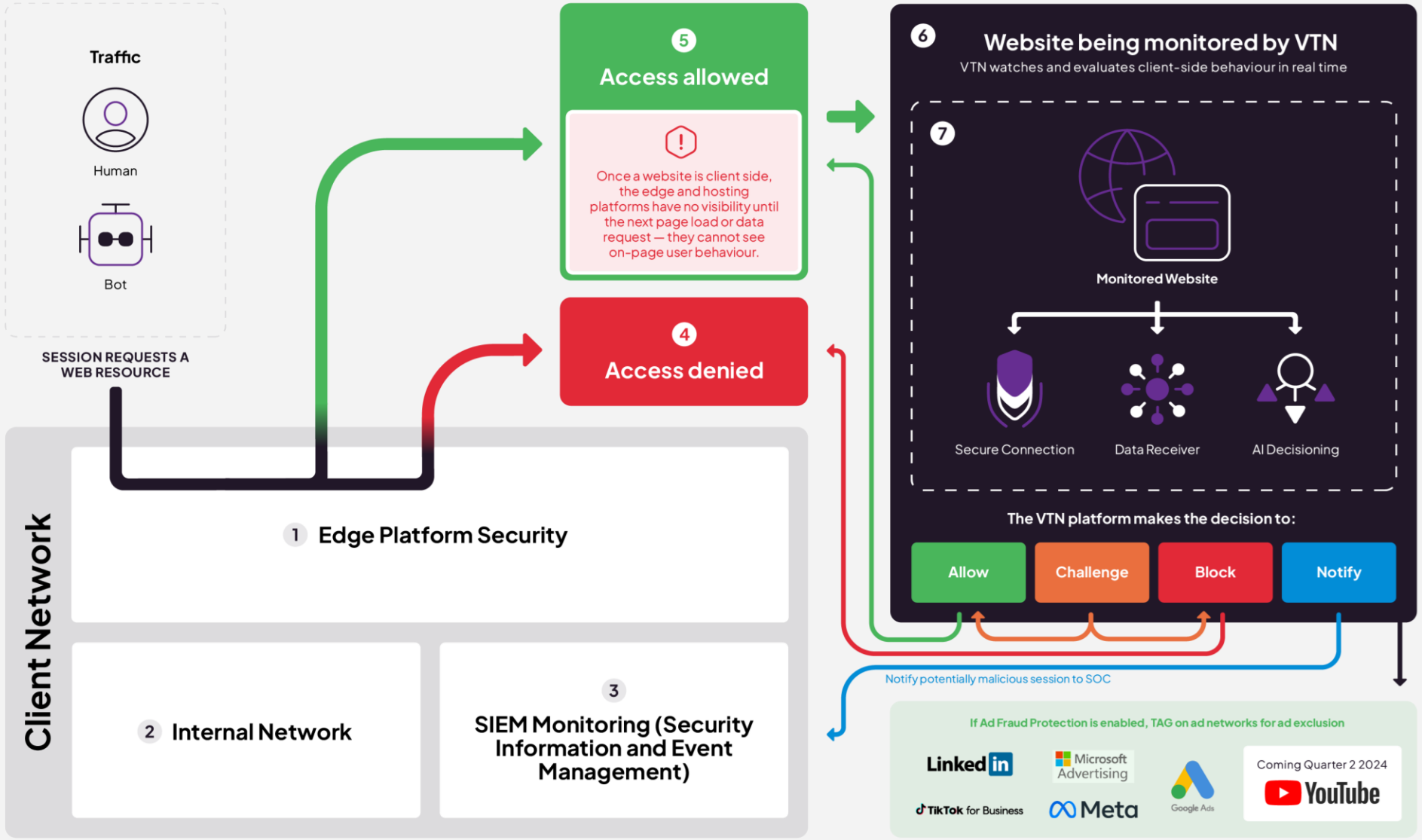
Introducing abbi

abbi (adaptive bot blocking intelligence), our patent pending, machine-learning model, thinks differently. Going beyond basic behaviours to block even the most complex AI threats.

How Veracity Works



Client-side bot protection: reference architecture



Overview

Client-Side Bot Protection usually gets overlooked, is applied inconsistently or incorrectly focused. This leaves you vulnerable to malicious bot attacks on or through your web platforms; leading to data breaches, loss of revenue and with a substantial risk to brand value.

Veracity Trust Network solutions instantly protect your website, digital ads, reputation, customer data and traffic insights from bots.

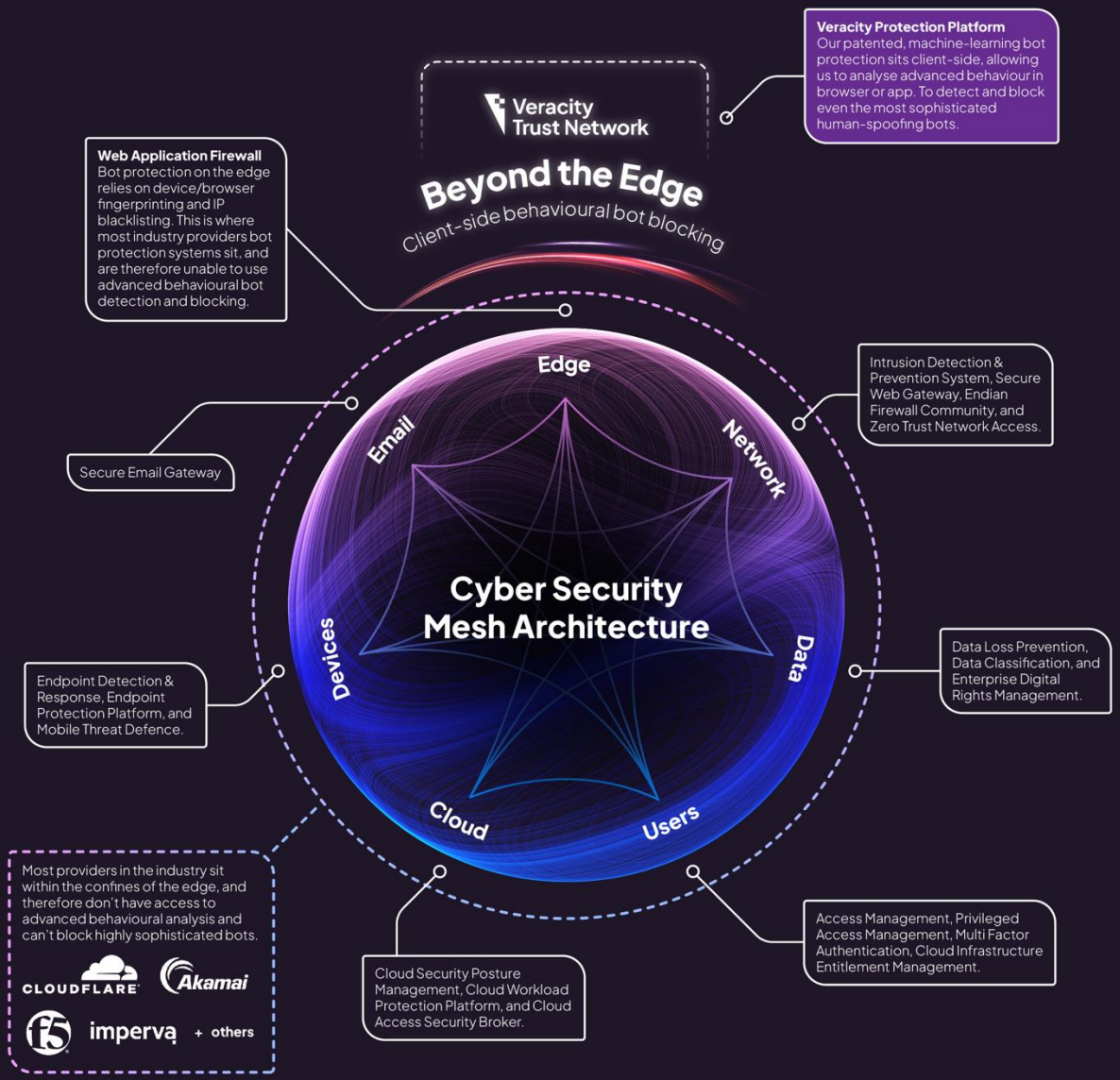
Our patented, AI-powered bot detection engine identifies the risk of client-side malicious bot activity and takes it out of the equation.

1. Your in-situ Edge Platform Security takes care of network level suspicious behaviour detection, allowing humans and human-mimicking malicious bots through.
2. The Internal Network serves up the requested content, in the case of a website: the DOM, CSS, JavaScript and references to media. Veracity's bot protection is injected at this point.
3. SIEM Monitoring may be present for oversight of all website operations and the opportunity for SOC team action.
4. Reputation-based decisioning, IP blocks and network level suspicious behaviours are denied by the Edge Platform Security.
5. Human traffic and malicious traffic that is mimicking human behaviour and patterns is allowed access.
6. Veracity monitors and evaluates all session behaviours in near real-time, looking for malicious bot activity.
7. Once a session is determined to potentially be from a bot, Veracity can optionally challenge it, immediately block it, or refer the decision to the SOC team, depending on your exact requirements.

Security Mesh Position

While most providers in the industry sit in the edge to block bots using more traditional methods, we sit client-side – Beyond the Edge.

This allows us to use advanced behavioural-analysis, directly in browser or app, to block even the most sophisticated human-spoofing bots.



Product Benefits

Tomorrow's protection, today

Our patent pending, machine-learning protection goes beyond basic behaviours to block even the most complex AI threats. And evolves just as quickly as they do.

Superfast and supersmart

Our revolutionary behaviour-based protection blocks human-spoofing bots before you can say data theft.

Effortless integration

Combines seamlessly with your existing security stack, and DDoS & WAF solutions, to block the ones they let through.

We block what others don't

Our patent pending, machine-learning model – Abbi – thinks differently. Going beyond basic behaviours to block even the most complex AI threats.

<0.01% false positives

Block bots not humans with an incident rate of less than 0.01%. Any higher and we wouldn't be doing our jobs.

Website. WebApp. Wi-Fi Fridge.

With just one line of JavaScript you can protect all your products. Better yet, see all your platforms in one simple dash.

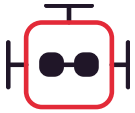
Planet protection included

Try our CO^2 calculator

Malicious bots use energy just like we do. Cut your carbon with adaptive protection that works for you, and Mother Nature.

Example savings

If your average monthly sessions are: **80,000**



Estimated monthly malicious bots

17,760

Estimated CO^2 emissions saved

26.64kg

Equivalent to driving an average petrol-powered car for

57.8 miles

Equivalent to charging a smartphone

1,172 times

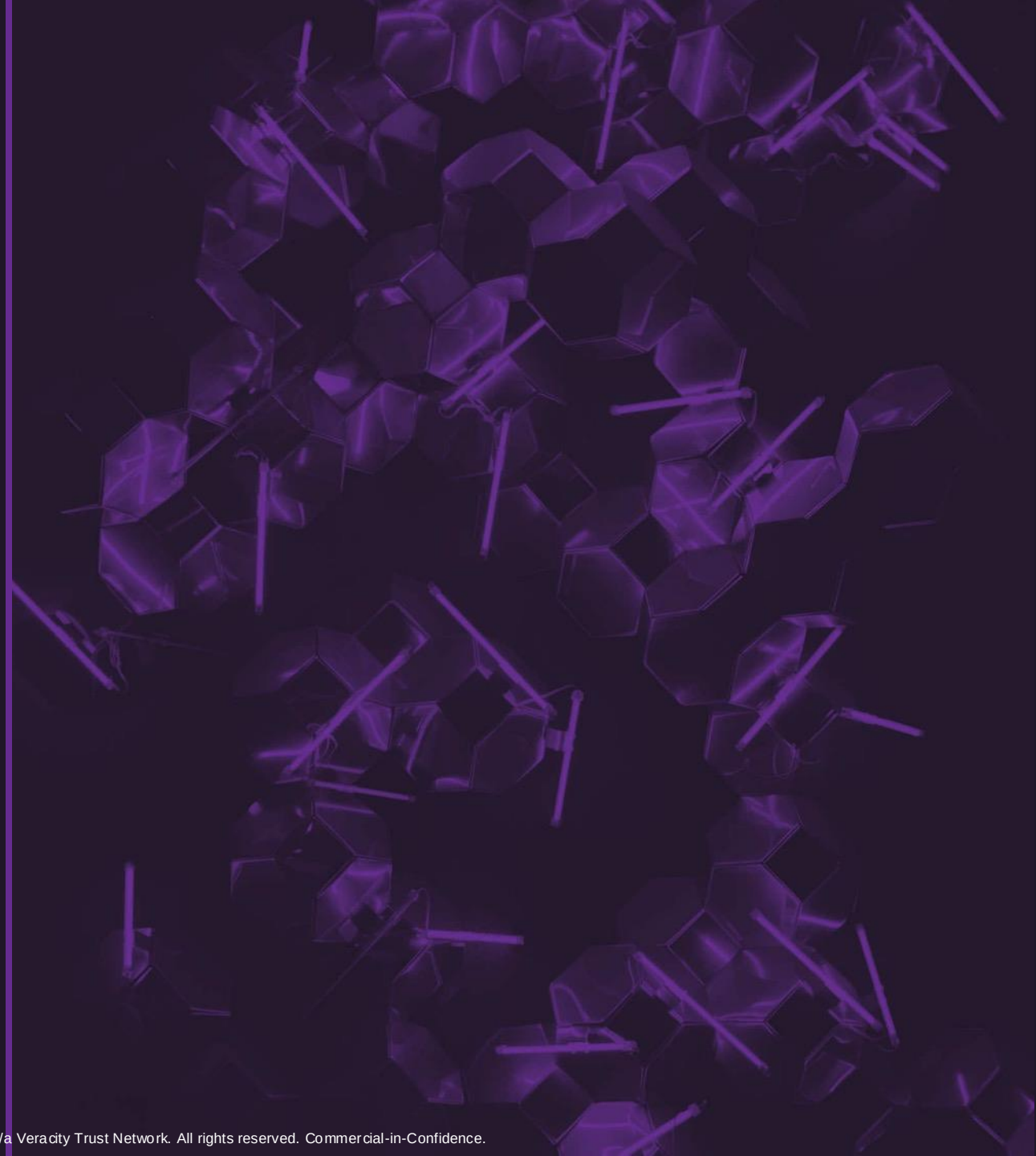
The Web Threat Protection Market

		Veracity	Cloudflare (Bot Management)	Akamai (Bot Manager)	Imperva/Human (Advanced Bot Protection)	F5 (Bot Defence)	Radware	DataDome
Protection	UK Bot activity live feed	✓	✓	✓	✓	✓	✓	✓
	Real-time bot categorisation and reporting	✓						
	Broad bot protection	✓	✓	✓	✓	✓	✓	✓
	Vulnerability scanning protection	✓						
	Digital ads protection	✓						
	Advanced machine learning behavioural analysis	✓		✓	✓			✓
Features	Close to visitor data capture	✓		✓	✓	✓	✓	✓
	Customisable decision engine	✓		✓				
	Device/browser fingerprinting	✓		✓	✓	✓	✓	✓
	Session fingerprint blacklisting	✓		✓	✓	✓	✓	✓
	Good bot whitelisting	✓		✓	✓	✓	✓	✓
	Real-time challenge/block system	✓		✓	✓	✓	✓	✓
	Realtime data feed to SIEM solutions	✓						
	Environmental impact reporting	✓						
Deployment	Security stack integration	✓			✓			
	Agnostic to other security tools	✓			✓			
	Plug and play in under 15 minutes	✓						
	Targeted deployment customisation	✓						
	Flexible pricing options	✓						
Company	Specialists in malicious bot protection	✓			✓			✓
	UK Government accredited	✓						

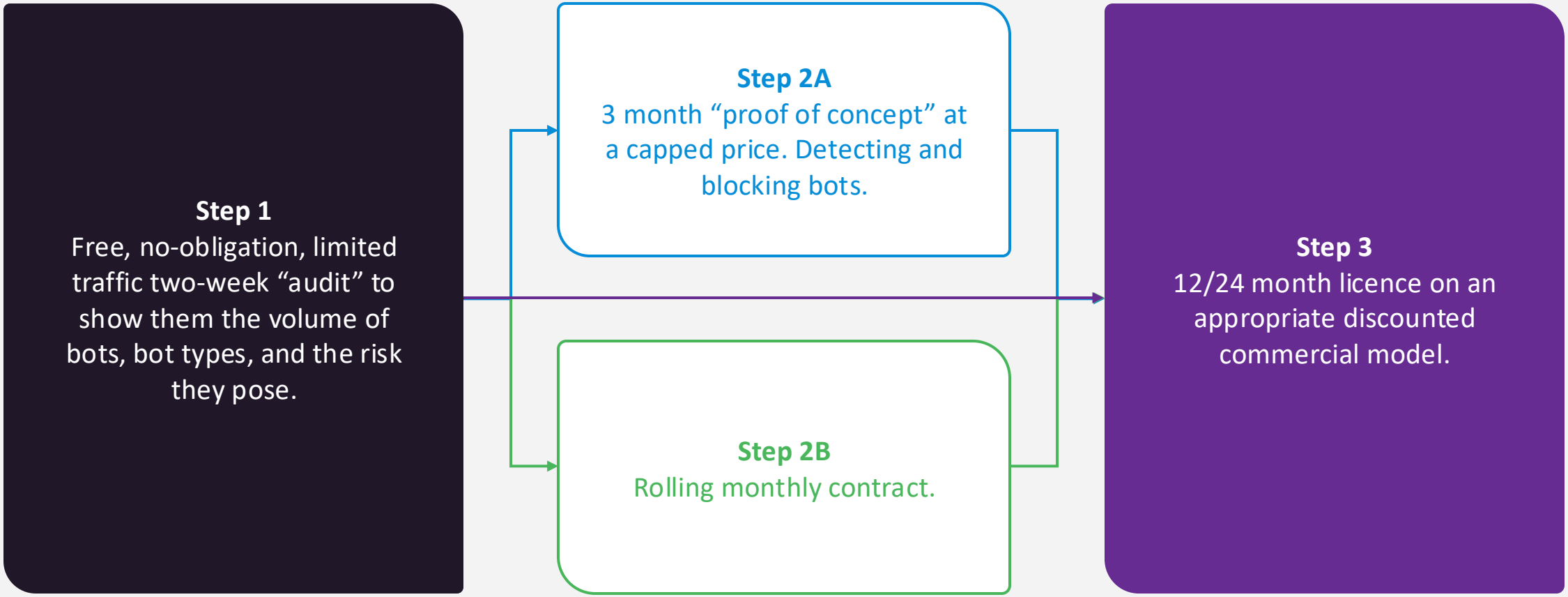
The Ad Fraud Prevention Market

		Veracity	Lunio	CHEQ / Click Cease	IAS	TrafficGuard	Click Guardian	DoubleVerify
Ad Protection	Digital ads protection	✓	✓	✓		✓	✓	
	Device/browser fingerprinting	✓	✓	✓	✓	✓	✓	
	Close to visitor data capture	✓	✓	✓		✓	✓	
	Programmatic platform protection				✓			✓
	Meta and Google Search protection	✓	✓	✓	Limited	✓	✓	Limited
	LinkedIn and TikTok protection	✓	✓		TikTok only			Limited
	Google Audience and YouTube protection	✓				✓		
	Bot impact from affiliate and referral channels reporting	✓				✓		
	Advanced combined machine learning behavioural analysis	✓						
Web Protection	Website bot protection in the same dashboard	✓		Wordpress only			Wordpress only	
	Bot activity live feed	✓					✓	
	Real-time bot categorisation and reporting	✓						
	Broad bot protection	✓		Wordpress and eCommerce only				
	Sophisticated bot protection	✓						
	Vulnerability scanning protection	✓						
	Session fingerprint blacklisting	✓						
	Good bot whitelisting	✓						
	Real-time challenge/block system	✓						
	Environmental impact reporting	✓						
Deployment	Security stack integration	✓						
	Agnostic to other security tools	✓						
	Realtime data feed to SIEM solutions	✓						
	Flexible pricing options	✓						
Company	Specialists in malicious bot protection	✓						
	UK Government accredited	✓						

Commercials



Approach to licence



Potential commercial models

*example pricing only

Option 1
Pay a fixed price per session processed.

Example – pay a small monthly platform fee of $500 up-front, and then pay $0.15 per session in arrears (less the $500 deposit).

Option 2
Pre-purchase a number of sessions and top-up when they are all used.

Example – pre-purchase 10,000 sessions at $0.12 per block; use them until they are all used.

Option 3
Purchase a set number of sessions/month for a longer term, with 5% overage allowance included. Carry forward 15% of unused sessions to next month.

Example – the audit suggests 50k monthly sessions. Customer purchases 50k sessions/month at $0.08/block. This allows overage of 2,500/month. And 7,500/month to be carried forward if unused.

Veracity Trust Network

Any questions?

nick.pomeroy@vtn.live