

BLUEWAVE AI · INTRODUCTION

AI security for networks **and** **voice channels**



Two product lines for two different problems: HYDRA spots unusual behaviour inside a network; VoiceGuard flags deception on phone calls, whether the voice is cloned or real.

Separate products, one team, one way of working: customer-controlled processing, traceable results.

Two product lines, **two separate security problems**

HYDRA • NETWORK

Network anomaly detection

Is something inside the network behaving in a way it normally does not?

Learns how a network normally behaves and flags what deviates, with the context an analyst needs to investigate.

FOR

CISOs, SOC and network teams

VOICEGUARD • VOICE

Protection against phone deception

Is this call trying to deceive someone?

Flags synthetic and cloned voices and deceptive conversation patterns, and adds a planned way to verify who is calling.

FOR

Fraud, customer service and security teams; service partners

Separate products and separate engines, built by the same team on Kolmogorov–Arnold Network (KAN) model architectures. Both are designed for customer-controlled processing, with deployment options agreed for each implementation, and return results that can be traced back.

Signatures catch what is already known. **New behaviour needs a baseline.**

KNOWN PATTERNS

Rules and signatures stay essential

An intrusion detection system recognises what has been described before. It has nothing to match against a pattern no one has written down.

UNSEEN BEHAVIOUR

Attacks change faster than rules

A new way of moving data or acting on files may match no written rule, yet still stand out against what is normal on that particular network.

INVESTIGATION

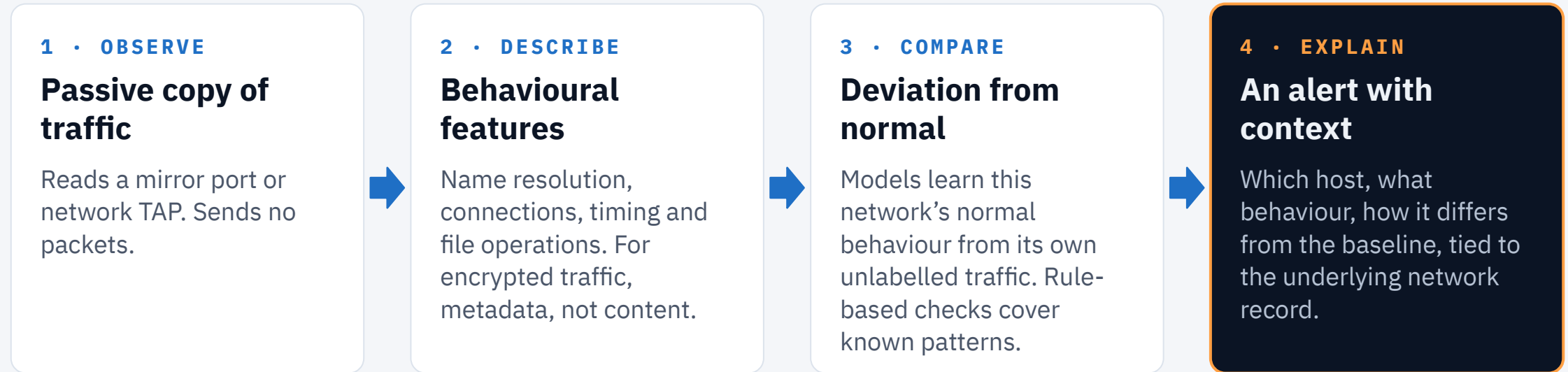
A score alone is not enough

An analyst needs to see which host behaved how, and compared with what, before acting.

241 days

IBM reports a global mean breach lifecycle of 241 days in 2025, from identification to containment and service restoration.

From a copy of traffic to an alert an analyst can inspect



HYDRA is passive: it does not block traffic or change the network. Your team decides what happens next.

Built for sensitive environments, **assessed in yours**

WHERE IT IS RELEVANT

- Mid-sized organisations with limited SOC capacity
- Critical infrastructure and industrial environments
- Financial services and the public sector
- University and research networks
- Managed security service providers

WHY IT SUITS THEM

- Runs on your premises, without cloud connectivity; designed for isolated networks too
- Small models that run on standard CPUs
- The trained model stays with you, and can be handed over on request

IN OUR LAB • RESEARCH PROTOTYPE

On our 15-machine lab cyber range we demonstrate two scenarios: data hidden in DNS queries, and mass encryption of files on a file server over SMB. These are lab demonstrations, not field results; detection validation for the SMB scenario is ongoing.

Voice cloning is only one tool in phone fraud

FAKE VOICE

Cloned or synthetic voice

Asks for money, data or an approval in the voice of a relative, a manager or a member of staff.

REAL-VOICE DECEPTION

Real person, deceptive conversation

Rushes the victim, poses as someone else, demands secrecy or pushes them to skip the usual security step.

The attack is a chain of deception that also works without a synthetic voice. That is why VoiceGuard does not stop at asking whether the voice is real.

Voice, conversation, origin: three separate signals

WHAT IT LOOKS AT	THE QUESTION	CAPABILITY	STATUS
Voice	Could the voice be synthetic or cloned?	VoiceGuard Engine	AVAILABLE
Conversation	Does the conversation show a deceptive pattern?	Vishing and social engineering pattern analysis	DEMONSTRABLE PROTOTYPE, PERFORMANCE VALIDATION UNDERWAY
Origin	Can we verify the call really comes from who it claims to be?	BlueWave Witness	PLANNED PARTNER CAPABILITY

The signals are not merged into a single ‘fraud / not fraud’ verdict. The customer’s or partner’s rules decide the next step: proceed, verify further, suspicious, block or inconclusive.

What may be fake, and what can be verified

VERIFIED

The calling organisation's system signed the call: it really comes from them.

WHAT TO DO

That does not make every request on the call automatically safe.

NOT VERIFIED

No signature. On its own, a missing verification is not a sign of fraud.

WHAT TO DO

Treat as an unknown caller; confirm any money movement on another channel.

FLAGGED

No signature, and detection also fires: a synthetic voice or a deceptive pattern.

WHAT TO DO

Hang up and call back on a known number. Not a legal finding of fraud.

Detection asks what may be fake; Witness asks what can be verified. Together they give a fuller picture: red needs detection, and a missing signature on its own is only grey.

STATUS

Planned partner capability, with a proof of concept on a simulated telephone channel. Not a finished mobile app.

APPLICATIONS

CallCenter Guard and partner applications

CALLCENTER GUARD • VOICEGUARD IN THE CONTACT CENTRE

For banks, insurers, outsourced contact centres, helpdesks and any team that handles requests by phone

- Account recovery and password resets
- New device or phone-number registration
- Phone approvals and customer data changes
- Internal IT helpdesk requests

TODAY • ON RECORDINGS

Synthetic and cloned voice detection runs on recordings: we measure how useful the signal is, at what false-alert rate and review workload.

LATER • LIVE INTEGRATION

Live call connection (SBC/SIPREC) is in development; alerts in the agent or fraud workflow are planned.

PARTNERS

Partner integrations

We work with partners to integrate VoiceGuard capabilities into their existing platforms and services.

Through a partner to end users

Banks, operators or app providers can offer protection to their own customers. CallGuard Mobile is planned.

INTEGRATION AND READINESS

Where each capability **stands today**

HYDRA

Passive: mirror port or TAP, on premises

Network anomaly detection

RESEARCH PROTOTYPE

DNS exfiltration scenario

LAB DEMONSTRATION

SMB file-encryption scenario

DEMONSTRATED IN LAB,
DETECTION VALIDATION ONGOING

SIEM export

PLANNED

Operational anomalies (AIOps)

CONCEPT

VOICEGUARD

API, events, or a file / recording export

Synthetic and cloned voice
detection

AVAILABLE

Vishing and social engineering
patterns

DEMONSTRABLE PROTOTYPE,
PERFORMANCE VALIDATION UNDERWAY

Live call connection
(SBC/SIPREC)

IN DEVELOPMENT

BlueWave Witness

PLANNED PARTNER CAPABILITY

CallGuard Mobile

PLANNED

Readiness differs by capability. A lab demonstration, a measured result, a partner pilot and a production integration are different things, and we label them separately.

A short conversation first, then a scoped assessment

1 • CONVERSATION

Which product line and which situation could be relevant for you or your organisation.

2 • SCOPE

HYDRA: the network segments and traffic sources that can be observed. VoiceGuard: the process and the audio that is lawfully available.

3 • ASSESSMENT

A scoped technical assessment in your environment or on your recordings, with a written report.

4 • DECISION

A joint decision on whether and how to continue, based on the results.

We agree the scope, terms and any fees of an assessment before it starts. If someone else in your organisation owns network security or phone-channel fraud, please feel free to forward this to them.

CONTACT

Let's talk about **one concrete situation**

A short call to see which of our product lines, and which situation, could be relevant for you or your colleagues.

Gergely Vass, CEO

Extensive banking experience across four banks, including project management and vendor selection on the buyer's side. Leads BlueWave AI's sales, business development and strategy.

Gyula Németh, CTO

More than 25 years in systems engineering and IT leadership; designer of the detection engines.

Gergely Vass, CEO · gergely.vass@bluewaveai.co · +36 20 441 5497

Gyula Németh, CTO · gyula.nemeth@bluewaveai.co · +36 30 560 9260