VAPTOR AI

TECHNICAL WHITEPAPER · VERSION
1.4.0 · 2026

VAPTOR
AI Pentest GPT

Autonomous Vulnerability Assessments, Penetration Testing & Cybersecurity Compliance. Managed Pentest Service for MSSPs, MSPs, SMEs & SMBs.



Cyber Watchdogs (Pty) Ltd
Reg. 2018/097508/07 · sales@vaptgpt.com · vaptgpt.com

PUBLIC · 2026

Continuous security assessment, at the speed of threats.

VAPTOR AI deploys inside your network as a dedicated appliance and autonomously runs a complete, multi-phase security assessment — discovery, vulnerability enumeration, exploit verification, web scanning, traffic analysis, and AI-enriched reporting — with no operator intervention once initiated.

8+	13+	99%	4+
INTEGRATED SCAN PHASES	INDUSTRY-STANDARD TOOLS	INTELLIGENCE STORAGE REDUCTION	AI PROVIDERS WITH AUTOMATIC FALLBACK

Key Differentiators

Internal Vantage Point

Deployed inside the network, VAPTOR sees what an attacker already inside sees — not just the perimeter. Misconfigurations, lateral movement paths, and internal service weaknesses that external scanners miss are surfaced automatically.

Fully Autonomous Pipeline

Eight sequential scan phases — each writing verified, artifact-first outputs — run end-to-end without operator intervention. A partial scan still produces usable findings from completed phases.

AI-Enriched Intelligence

Every finding is cross-referenced against NVD, GitHub Advisories, ExploitDB, and the MITRE ATT&CK knowledge base, then synthesised by GPT-4o, Claude, or VaptorAI into executive-ready narratives with prioritised remediation guidance.

Hardware-Bound Security

Deploy keys bind permanently to the first MAC address that uses them. A stolen key without the original hardware is useless. Revocation propagates to the device on the next 24-hour heartbeat.

MSSP-Ready Architecture

Multi-tenant Control Panel supports unlimited client organisations, per-org Service Portal access, and fleet-wide update delivery. Clients see only their own data.

Compliance Reporting

Signed compliance certificates (PDF), board-level executive reports, and per-device risk scoring (A–F grade) are generated directly from scan data — no manual assembly required.

The gap between threats and testing.

Adversaries operate continuously. Security assessments don't. Organisations face a structural mismatch between how fast attackers move and how infrequently they can run meaningful security tests.

EXTERNAL SAAS SCANNERS

Scan the perimeter from the internet. Miss internal vulnerabilities, lateral movement paths, weak internal service authentication, and misconfigurations visible only from inside.

SIEM & XDR PLATFORMS

Aggregate and alert on events but do not actively probe for exploitable weaknesses. They detect incidents after the fact — they don't prevent them by finding the attack surface first.

MANUAL PEN TESTING

Provides the deepest coverage but is expensive and slow. Most organisations afford one or two engagements per year, leaving months-long windows of unassessed exposure.

VAPTOR's Answer

VAPTOR bridges this gap by deploying a persistent, autonomous security assessment device inside the customer network — running on demand or on schedule, delivering findings equivalent in scope and depth to a junior-to-mid-level penetration test, enriched by AI analysis that surfaces the prioritisation a senior analyst would apply.

THE VAPTOR DIFFERENCE

Unlike external scanners, VAPTOR sits **inside the network** at the same vantage point as an internal threat actor. Unlike SIEM platforms, it actively probes for vulnerabilities. Unlike annual pen tests, it runs continuously — finding new exposures as they appear, not months later.

Who VAPTOR is for

Enterprise IT & Security Teams

Continuous internal network assessment without scaling a full pen-test team. Results integrate into existing SIEM and ticketing workflows.

Managed Security Service Providers

Multi-tenant fleet management. Deploy one device per client, manage all from a single Control Panel, deliver findings via the client-facing Service Portal.

Compliance-Driven Organisations

Automated compliance certificates with risk grading, executive reports for board submission, and framework-mapped findings for audit evidence packages.

Resource-Constrained Mid-Market

Scales from enterprise servers to Raspberry Pi. Free tier allows evaluation. AI enrichment available from Starter tier upward — no large security team required.

A complete scan engine in a single appliance.

VAPTOR is a four-layer system: the on-premises device, the scan engine backend, the cloud control infrastructure, and the AI enrichment pipeline. Each layer has a single, well-defined responsibility.

ON-PREMISES DEVICE

Kali Linux · Python 3.12 · PostgreSQL 18
PyQt6 desktop UI · Flask web UI (JWT + RBAC)
Runs fully offline — cloud sync is heartbeat only.

CLOUD INFRASTRUCTURE

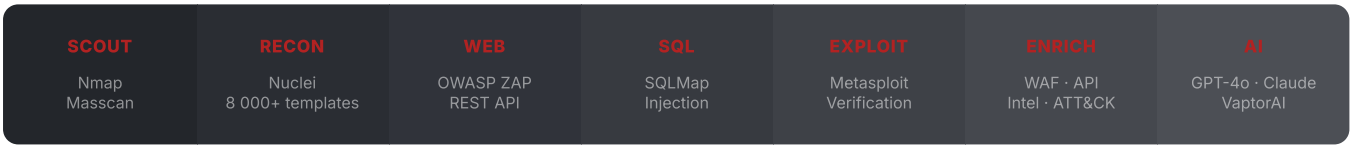
Control Panel — fleet management, licensing, updates
Service Portal — client-facing reporting portal
Receives only aggregated scan summaries.

AI LAYER

OpenAI GPT-4o (primary)
Anthropic Claude (supported)
VaptorAI Cloud (automatic fallback)
Azure OpenAI (enterprise option)

The Scan Pipeline

Every scan runs the same sequence of phases. Each phase writes its findings as structured JSON artifacts before the next phase begins. The **artifact-first design** means reports are reproducible and a scan interrupted at any phase still produces results from completed phases.



Post-Scan Modules

MODULE	TOOL	WHAT IT CAPTURES
VAPTORSHARK	mitmproxy · tshark	Live packet capture, MITM credential exposure, protocol analysis
VAPTORFW	Suricata	IDS/firewall rule hits, anomalous traffic patterns
VAPTORDAST	Nuclei DAST	Dynamic application security testing against discovered web endpoints
VAPTORSAST	Bandit · gitleaks · Bearer	Source code vulnerability scanning, secret detection in repositories
VAPTORVAS	GVM / OpenVAS	Full CVE-based vulnerability assessment for comprehensive coverage
VAPTORAGENT	WinRM · SSH · SMB	Endpoint security log collection and AI analysis on Windows/Linux/macOS

Adversary Technique Mapping

MITRE ATT&CK® INTEGRATION — V20

Every reportable finding is mapped to the MITRE ATT&CK techniques an attacker could use against it, across the Enterprise, Mobile, and ICS matrices. Reports carry per-finding **technique chips** and a tactics-coverage summary, and each scan exports a **Navigator layer** for interactive heatmap review. The technique catalogue is refreshed on demand during an Intelligence Update.

From raw findings to board-ready intelligence.

VAPTOR's AI layer operates at two levels: per-finding CVE enrichment with exploit availability and remediation guidance, and a full-scan executive synthesis that translates technical findings into risk narrative appropriate for senior leadership.

Live Threat Intelligence Feeds

SOURCE	CONTENT	METHOD	STORAGE
NVD (NIST)	CRITICAL/HIGH CVEs with CVSS scores	Incremental REST API, 119-day window	~3 MB
GitHub Advisories	Dependency & package vulnerabilities	GraphQL API, incremental cursor	~10 MB
ExploitDB	Exploit code availability & references	CSV metadata sync	~10 MB
Metasploit	Local exploit module database	In-DB, updated with Metasploit	In-DB
MITRE ATT&CK v20	Adversary techniques — Enterprise · Mobile · ICS	STIX 2.1 bundles, fetched on Intel Update	~6 MB

99% STORAGE REDUCTION

VAPTOR uses a **metadata-only** approach — structured vulnerability metadata, not full advisory text or exploit code. This reduces storage from ~3.5 GB (full git clones) to ~29 MB. Incremental cursors with automatic gap-recovery ensure no advisory data is silently missed between update runs.

AI Enrichment Flow

① Structured Context Assembly

Discovery artifacts, vulnerability findings, and service fingerprints are assembled into `ai_ready_summary.json` — a provider-agnostic prompt context combining network topology, CVE IDs, and scan metadata.

② LLM Enrichment

Each finding is enriched with contextual CVE analysis. The full scan receives an executive summary prompt. A provider abstraction layer supports OpenAI GPT-4o, Anthropic Claude, and VaptorAI — with automatic failover and exponential backoff retry between providers.

③ Prioritised Output

`vaptorgpt.json` contains per-finding AI assessments, severity justification, exploit availability, and remediation priority. AI-derived vulnerabilities are upserted to the local database for trend tracking.

④ Risk Grading

A weighted risk score (0–100) is computed from severity distribution and mapped to a letter grade (A–F). Grades appear in compliance certificates, executive reports, and the Service Portal dashboard.

Built secure from the ground up.

A penetration testing platform has a heightened obligation to protect the data it collects. VAPTOR applies the same rigour to its own security that it applies to scanning customer infrastructure — defence in depth at every layer.

Fail-Open on Network Errors

A VAPTOR device is never permanently bricked by a Control Panel outage. All cloud checks fall back to the last cached status if the network call fails — an 8-second timeout prevents startup hangs on unreachable networks.

Least Privilege

Destructive operations (`scan:run`, `exploit:run`) are gated behind explicit role assignments. The `admin` permissions are immutable — they cannot be removed via the RBAC editor, preventing self-lockout.

No Secrets in Git

Control Panel configuration, database DSNs, and bootstrap passwords are never stored in the repository. Runtime secrets are environment-injected. Portal directories are permanently excluded from version control.

Defence in Depth

Multiple independent layers protect the same assets: MAC binding ties deploy keys to hardware, industry-standard adaptive hashing protects passwords, TLS validates every Control Panel API call, RBAC restricts every web endpoint, and log sanitisation prevents credential leakage.

Threat Model Coverage

THREAT	MITIGATION
Stolen deploy key reused from another machine	Key is permanently MAC-bound on first use — a stolen key without the original hardware is useless
Device theft or resale	Admin revokes key in the Control Panel; device blocked on next 24-hour heartbeat
Unauthenticated web API access	JWT bearer token required on every endpoint, validated per-request
Privilege escalation via web RBAC	Permissions enforced server-side per request; admin permissions are immutable at the API layer
Credential leakage in log files	`vaptorsanitize.py` strips passwords, API keys, tokens from all log output
Plaintext passwords in database	Industry-standard adaptive hashing exceeding OWASP 2024 minimum requirements; per-user random salt; constant-time comparison
SQL injection	All DB access uses parameterised queries — no string interpolation of user data into SQL
MITM-observed credentials stored in plaintext	Only masked username (first char + ***) and SHA-256 hash are stored; password always `[REDACTED]`

One platform, three dedicated portals.

VAPTOR's cloud layer provides three purpose-built portals — each scoped to a specific audience, with strict data segregation ensuring no cross-org data leakage at any tier.

Control Panel

Cyber Watchdogs only
Full fleet administration

- Device fleet management
- Deploy key lifecycle
- License tier assignment
- Release & update push
- MSP account management
- Append-only audit log

Service Portal

End clients
Read-only per-org view

- Device status & last scan
- Vulnerability severity breakdown
- Full scan reports (CVE refs)
- Compliance certificates (A–F)
- Executive security reports

MSP Portal

MSPs & MSSPs
Multi-org management view

- All linked orgs at a glance
- Device fleet across clients
- Device Panel direct link
- Update-available alerts
- Update request ticketing
- Read-only license & billing
- Mandatory TOTP · Audit log

DATA SCOPE — WHAT REACHES THE CLOUD

All portals receive only **aggregated scan summary counts** (severity totals, target count, device version). Full vulnerability data, raw scan artifacts, and CVE details **never leave the VAPTOR device**. The cloud layer is a fleet management and reporting coordination layer — not a data store.

Compliance Certificate Engine

Formal compliance certificates generated from live scan data — signed, versioned, downloadable as print-quality PDF.

FIELD	VALUE
Serial format	`CW-{YYYYMM}-{ORG4}-{SEQ4}` (e.g. CW-202606-AMCE-0001)
Validity	30 days from issue date
Risk grade	A–F computed from severity-weighted score
Device identification	Device ID including MAC (audit-grade traceability)
Scope	Selectable devices, date range, vulnerability counts by severity

Deploy anywhere.
From enterprise to edge.

VAPTOR runs on any Kali Linux-capable hardware — x86_64 servers, ARM64 Raspberry Pi 5, or 32-bit ARMv7 devices. A single installer handles tool provisioning, database initialisation, and cloud registration in one pass.

Technology Stack

COMPONENT	TECHNOLOGY
Operating System	Kali Linux (rolling)
Python Runtime	CPython 3.12+ · 3.13 compatible
Database	PostgreSQL 18
DB Driver	psycopg3 · SERIALIZABLE isolation
Desktop UI	PyQt6
Web UI	Flask · JWT (HS256) · RBAC
Report Templates	Jinja2 · WeasyPrint (PDF)
Remote Access	Tailscale zero-trust mesh
Update Auth	ed25519 SSH (no interactive prompts)
Schema Management	Boot-time idempotent reconcile

Multi-Architecture Support

ARCHITECTURE	TARGET
x86_64	Servers, workstations, VMs
aarch64	Raspberry Pi 5, ARM64 servers
armv7l	Raspberry Pi 3/4 (32-bit)

Hardware Requirements

COMPONENT	MINIMUM	RECOMMENDED
CPU	4 cores	8 cores (x86_64)
RAM	4 GB	16 GB
Storage	64 GB	256 GB
Network	100 Mbps	1 Gbps

Performance Characteristics

SHA-256 DEDUPLICATION

Every vulnerability upsert includes a SHA-256 fingerprint. Duplicate findings from multiple scanners on the same CVE are merged — preventing inflated counts. **154× faster** than naive insert-and-check patterns.

CONNECTION POOL

psycopg3 connection pool with SERIALIZABLE isolation and exponential backoff retry. Stable under concurrent scan + web UI + report generation workloads.

ARCHIVE & DATA CONTINUITY

Previous scan artifacts are archived before each new scan with push-confirmed markers and pending-push stubs — ensuring portal data is never lost even if the device reboots mid-scan.

ZERO-TOUCH SCHEMA MIGRATION

Database-structure changes ship with the update and reconcile automatically on next boot — the device re-applies the idempotent schema with no reinstall or manual migration. A failed apply is non-fatal and leaves the existing schema intact.

Three tiers.
One platform for every organisation.

Every tier includes the VAPTOR Watchdog base, the pentesting framework, compliance mapping (MITRE ATT&CK, ISO, NIST, HIPAA, POPIA, PCI-DSS & SOC2) and a managed service. AI Assessment is available as an option on every tier.

STARTER
For small teams getting started

ESSENTIAL

- ✓ Managed service
- ✓ Monthly scans
- ✓ Local intelligence · weekly updates

Up to 50
Scan Assets

PROFESSIONAL
Most popular for growing orgs

RECOMMENDED

- ✓ Managed service
- ✓ Weekly / monthly scans
- ✓ Local intelligence · daily or weekly

Up to 100
Scan Assets

ENTERPRISE
For large networks & MSSPs

FLEET & MSSP

- ✓ Weekly / monthly scans
- ✓ Multi-organisation support
- ✓ Fleet management portal
- ✓ Local intelligence · daily or weekly

100+
Scan Assets

Roadmap

MITRE ATT&CK® Mapping — Phase 1
Shipped · v1.4.0
Deterministic finding→technique mapping across the Enterprise, Mobile, and ICS matrices; per-finding technique chips, tactics-coverage summary, and an exported Navigator layer for interactive heatmap review.

Boot-Time Schema Reconcile
Shipped · v1.4.0
Zero-touch database migrations across the fleet — structure changes reconcile automatically on next boot, with no reinstall. Combined with push-confirmed scan-archive continuity.

MSP Management Portal · Compliance & Executive Report Engine
Shipped
Multi-org MSSP fleet management with mandatory TOTP; signed PDF compliance certificates with A–F risk grading and board-level executive reports generated from live scan data.

MITRE ATT&CK® Mapping — Phase 2
In Progress
In-report technique heatmap, attack-chain narrative, and fleet-wide ATT&CK coverage aggregation across the Control Panel and MSP portals.

VAPTORSHARK — Network Packet Analysis
In Progress
Deep MITM packet capture integration for protocol-level traffic analysis and credential exposure detection.

VAPTORWIFI (802.11) · VAPTORMAST (Mobile App Security) · Remediation Workflows
Planned
Wireless network assessment; mobile application security testing; integrated remediation ticketing with SOAR trigger support.

Cloud Agent Logs · Active Directory Posture · Container Security
Planned
AWS/Azure/GCP log collection; AD/Azure AD posture assessment; Kubernetes and container security scanning.

GET STARTED WITH VAPTOR AI

Ready to see what's really inside your network?

VAPTOR AI deploys in minutes, scans autonomously, and delivers board-ready security intelligence from day one. Contact us to schedule a live demonstration or request a proof-of-concept deployment.

EMAIL

sales@vaptgpt.com

Sales enquiries & demonstrations

WEB

vaptgpt.com

Product information & documentation

MSP PORTAL

MSSP Fleet Management

Multi-org device visibility, update requests & billing

SERVICE PORTAL

Client Reporting & Certificates

Per-organisation findings, reports & compliance PDFs

8+	13+	4+	99%	260K
SCAN PHASES	INTEGRATED TOOLS	AI PROVIDERS	INTEL STORAGE SAVING	PBKDF2 ITERATIONS

Cyber Watchdogs (Pty) Ltd · Reg. 2018/097508/07
VAPTOR AI v1.4.0 · © 2026 All rights reserved
This document contains technical and commercial information proprietary to Cyber Watchdogs.

PUBLIC · 2026