MirrorMire AMaze™ — Corporate Brochure

Proactive Cyber Resilience, Powered by AI · Map · Maneuver · Maze

ABOUT MIRRORMIRE

MirrorMire is a cyber-security company building the next generation of proactive cyber resilience, powered by AI. Our flagship platform, AMaze™, flips the traditional security dynamic. Instead of waiting for alerts after damage is done, AMaze™ actively shapes the adversary's path and turns every intrusion attempt into actionable intelligence.

AMaze™ operates on three principles: **Map**, **Maneuver** and **Maze**. The platform **maps** adversarial behaviour as it unfolds, **maneuvers** adversaries away from production systems and into synthetic environments, and traps them inside a **maze** of decoys that extends engagement time while limiting exposure to real assets.

AMaze™ uses AI to deploy **Synthetic Cognitive Agents (SCAs)** — advanced decoys indistinguishable from production services — and **Neural Echoes** — high-fidelity breadcrumb lures planted across real infrastructure. Embedded directly in the network, AMaze™ detects threats at the earliest stages of the cyber kill chain and arms security teams with actionable intelligence instead of alert fatigue.

The result is an organisation that can reduce time to detect and respond, strengthen cyber resilience across IT, OT, AI and cloud, and convert every intrusion attempt into organisation-specific threat intelligence. SOC analysts spend less time triaging noise; CISOs gain reporting they can take to the board; and adversaries face an environment where the cost of attack keeps climbing.

WHY MIRRORMIRE

Most security tools react. MirrorMire anticipates. The legacy stack was built on the assumption that security teams can detect every attack before it lands — a bar modern adversaries routinely clear by living off the land, weaponising zero-days and dwelling quietly inside networks for months. MirrorMire was founded on a different premise: be proactive.

AMaze™ changes the economics of an attack. Security teams no longer need to be right every time; adversaries must be right at every step. The outcome is resilience that compounds, because every engagement teaches the platform, enriches your threat intelligence and raises the cost of the next attempt.

INSIDE AMAZE™

AMaze™ delivers a full suite of AI-driven capabilities engineered to stay ahead of evolving adversary tactics. Unlike conventional decoys, AMaze™ fields Synthetic Cognitive Agents that mirror the behaviour of real assets, adapt in real time to adversary movement and capture the full spectrum of tactics, techniques and procedures used against your organisation.

Feature	Description
Zero False Positives	Alerts fire only when adversaries engage with SCAs or Neural Echoes — assets a legitimate user has no reason to touch — eliminating noise and ensuring every alert is a high-fidelity, actionable event.
Discovery of Unknown & Zero-Day Threats	Captures malware and payloads unseen by public databases; surfaces novel threats before traditional tooling can detect them; live binary capture, SHA-256 fingerprinting and quarantine.
Self-Healing & Threat Attribution	Compromised SCAs are automatically restored to clean state via the Deployment Planner's lifecycle; full forensic record (session, payloads, command sequences) is preserved for analysis.
Live Capture of Targeted Malware	Collects and preserves adversary tools, scripts and payloads for deep forensic analysis and organisation-specific threat intelligence — published on the *amaze.events.malware* NATS subject.
High-Fidelity AI Cognitive Agents	SCAs across HTTP · SSH · RDP · FTP · MySQL · Redis · IoT · Windows-server (SMB · WinRM · LDAP · AD) · BACnet · Modbus · DNP3 · S7/CIP · IEC 104 · OPC UA, plus malware-capture decoys and reverse-shell environments.
Cognitive Deception for AI	AI-SCAs trap attackers and rogue AI agents probing your AI applications (chatbots · agents · MCP · RAG): an in-product engine shields the AMaze Analyst assistant, and MCP honey-server / LLM proxy / SDK forms protect your own AI. Mapped to OWASP LLM Top-10 / MITRE ATLAS.
AMaze Analyst — AI SOC Assistant	An in-product analyst teammate: ask about tickets and threats in natural language; reconstructs attack campaigns via RAG + safe, read-only text-to-SQL; vendor-neutral / BYOK.
Seamless Ecosystem Integration	Structured JSON output and outbound dispatch (Webhook · Slack · Teams · Generic-HMAC) enable smooth interoperability with monitoring, response, SIEM, SOAR and threat-intelligence platforms already in your stack.
Clear & Concise Reporting	Translates technical findings into HMAC-signed weekly, monthly and quarterly CISO and board reports that decision-makers can understand and act on with confidence — verifiable post-hoc via the platform's *verify* endpoint.

CYBER RESILIENCE FOR THE DIGITAL AGE

AMaze™ protects across every critical domain with purpose-built capabilities that address the most advanced cyber threats modern organisations face.

Domain	Capabilities
Identity & Access	Active Directory SCAs and Neural Echoes to catch credential abuse and privilege escalation; SMB · WinRM · LDAP coverage with full session logging.

Domain	Capabilities
Data Security	Echo files, decoy databases (SQL, NoSQL), document-embedded lures and real-time data-exfiltration detection on FIM-watched paths.
Custom Threat Intelligence	Real-time IOC extraction, attack-chain replay, IP-reputation scoring (IPQS · AbuseIPDB · VirusTotal) and targeted malware capture into a tenant-specific intelligence graph.
Infrastructure Security	IoT, SCADA and legacy-system deception engineered for hybrid networks; OT-protocol-correct emulators that never inject traffic into real controllers.
AI / LLM Security	AI-SCAs that trap prompt-injection, jailbreaks and data-exfiltration against your chatbots, agents, MCP servers and RAG pipelines; canary credentials for breach attribution; OWASP LLM Top-10 / MITRE ATLAS.
Incident Response	Threat attribution, timeline visualisation in the Attack Explorer, and forensic replay with full session recording for rapid investigation.
Automation & Orchestration	Risk-weighted IP blocking and automated decoy tuning driven by the Deployment Planner; approval-gated automation with timeout-based auto-rejection.

KEY ARCHITECTURAL COMPONENTS

AMaze™ Deception Engine

An extensive suite of high-interaction Synthetic Cognitive Agents spanning HTTP, FTP, SSH, RDP, VPN, SQLi, LFI, XSS, Active Directory, printer, DNS, LDAP, SMTP, SMB, Modbus, database, IEC 60870-5-104, BACnet/IP, DNP3, S7 / EtherNet-IP CIP and OPC UA, plus specialised malware-capture agents and reverse-shell environments. Each SCA faithfully mimics real services and assets to lure, engage and analyse adversaries without exposing production.

Distributed Event Streaming Platform

NATS JetStream streams real-time telemetry from every SCA zone — DMZ, internal networks and OT environments — delivering continuous logging, alerting and data synchronisation with TimescaleDB-backed time-partitioned storage for unified threat visibility across the enterprise.

Self-Restoration & Containment Engine

Compromised SCAs are automatically restored to clean state via the Deployment Planner's DRAFT → ACTIVE → ROLLBACK state machine while full forensic records of adversary actions are preserved, enabling uninterrupted engagement and immediate surface recovery during active threats.

AI-Guided Deployment & Customisation Engine

Learns from adversary dwell time, lateral movement and TTPs to dynamically update SCA configurations and deepen adversary interaction — your deception posture improves every time it is engaged.

Specialised Malware-Capturing Synthetic Cognitive Agent

Isolates, records and analyses the tools, scripts and malware adversaries deploy. Extracts actionable Indicators of Compromise for your threat-intelligence feeds, supporting early detection of novel threats and zero-day exploits.

BUILT FOR OT — FROM SUBSTATION TO SHOP FLOOR

Operational technology is where deception either earns its place or quietly fails. Real controllers cannot be scanned, real PLCs cannot tolerate injected traffic, and real operator workflows cannot be interrupted by a noisy security tool. AMaze™ was built for this constraint from day one — and ships an OT/ICS fleet that mirrors the real estate rather than approximating it.

Protocol-correct OT/ICS coverage out of the box

Protocol	Real-world devices AMaze™ emulates
BACnet/IP	Building-management-system controllers — HVAC, lighting, access control
Modbus TCP	Gas analysers, power monitors, battery-management gateways, pumps, generic RTUs
DNP3 over TCP	SCADA Master / RTU / IED — utility, water, oil & gas
Siemens S7Comm	Siemens PLCs — anomalous tag read/write, recovery suppression
EtherNet/IP CIP	Allen-Bradley / Rockwell ControlLogix family — DIGESTER (CompactLogix 1769-L33ER) · COMPRESSOR (5069-L320ERS2) · CONTROLLOGIX_HP (1756-L85E)
IEC 60870-5-104	Power-transmission SCADA, substation RTUs
OPC UA	Industrial gateways, sensor aggregators, modern OPC servers

BYOT — Build Your Own Trap: emulate *any* OT device

When the customer's estate contains a proprietary PLC, a regional protocol variant, an unusual battery gateway or any device a vendor would charge a custom-engineering fee for, AMaze™'s BYOT framework gives the answer: a single JSON file declares the protocol, port, device model, register/tag map and TTP-rule list — and the decoy is live in minutes.

What you get	Detail
JSON-defined personas	Protocol · port · model · register/tag map · TTP rules — one file per decoy
Seven protocol handlers shipped	Modbus · EtherNet/IP CIP · Siemens S7Comm · DNP3 · BACnet/IP · IEC 60870-5-104 · OPC UA
Substation-grade examples bundled	DNP3 IED · IEC 104 RTU · Modbus battery monitor · S7 auxiliary control · OPC UA sensor gateway
Per-register MITRE ICS-ATT&CK TTPs	e.g. T0831 manipulation of control · T0855 unauthorised command · T0827 parameter modification
Additive, zero-disruption runtime	BYOT runs in its own process tree; existing SCAs are never disrupted
Full platform integration on day one	Same scoring, attack-chain correlation, outbound dispatch and signed reporting as every other SCA

The result: AMaze™ does not just "support OT." It can be made to mimic the specific OT estate of any customer — substation, plant floor, water utility, oil & gas, data-centre BMS, hospital plant — without platform-side

engineering and without disturbing a single real controller.

DECEPTION FOR THE AI ERA

As enterprises rush AI into production, the attack surface shifts from ports to prompts. AMaze™ is the first deception platform to fight AI attacks *with* AI deception — extending the same instrument-the-attacker's-path model to the AI layer. Where a network SCA traps a port scan, an AI-SCA traps a *thought*: it baits any attacker — human or autonomous AI agent — probing your AI for jailbreaks, secrets or tool abuse.

Form	Deploy for · what it does
In-product engine	Ships inside AMaze™ to shield the AMaze Analyst assistant — refuses jailbreaks, serves tracked honey credentials on exfil attempts, tarpits hostile agents; gated so real analysts never trip it.
MCP honey-server	Drop among the customer's real MCP servers — advertises honey tools/resources; any call is hostile and returns canary data.
LLM proxy-sidecar	Sits in front of any chatbot / OpenAI-compatible endpoint — traps exfil prompts, refuses jailbreaks, scans responses for canary echoes.
Embeddable SDK	Wire deception into the customer's own agent — guard() / scan_response() / honey_tools().

Every honey credential is a **canary** — its reuse anywhere (a SIEM, an auth log, a paste site) is confirmed exfiltration with attribution to the exact AI session. **AI Neural Echoes** (a honey MCP-tool reference, a canary-seeded RAG document) lure an attacker's AI toward the trap. Every trip is OWASP-LLM-Top-10 / MITRE-ATLAS-mapped and joins the same unified attack chain as the IT and OT decoys — one console, one story.

USE CASES ACROSS SECTORS

AMaze™ adapts its deception architecture to the specific threat landscape of each industry vertical, delivering targeted protection where it matters most.

Sector	Threat Scenarios Addressed
Banking & Finance	Mirrored Workload — a zero-production-touch, graduated entry point for risk-averse boards — plus ransomware detection, credential-reuse traps, lateral-movement monitoring, targeted malware capture, and early response to financially-motivated attacks.
Government	Zero-day protection, Advanced Persistent Threat (APT) detection, and SOC-workflow optimisation for sensitive environments.
Manufacturing & OT	ICS-protocol SCAs (Modbus, DNP3, S7/CIP), SCADA lateral-movement detection, and coverage for IT/OT-convergence scenarios.
Telecom	Early attack detection and rogue base-station identification across distributed infrastructure.
Healthcare	Patient-data lure traps and medical-device mimicry to build resilience for IoMT environments.
Critical Infrastructure	Air-gapped deployment, OT-native SCAs, and forensic-grade attack capture for energy, utilities and transport.

ENTERPRISE-READY DEPLOYMENT OPTIONS

AMaze™ supports six flexible deployment models, letting organisations choose the architecture that best fits their infrastructure, compliance requirements and operational needs.

#	Deployment Option	Description
1	Hardware-Assisted On-Prem	MirrorMire-provided dedicated appliances for on-premises deployment, fully pre-configured and tuned for your environment.
2	On-Prem Virtual Machine	Deploy AMaze™ on existing virtual infrastructure (VMware, Hyper-V) with no additional hardware required.
3	Cloud-Native	Run the complete platform on public cloud (AWS · Azure · GCP) for scalable, maintenance-light operation with full feature parity.
4	Private Cloud / Data Centre	Deploy within your private cloud or hosted data centre with complete administrative control.
5	Hybrid IT + OT	Distribute components across cloud and on-prem systems, purpose-built for IT/OT-convergence.
6	Modular & Custom	Design the architecture around your network scale, compliance requirements or integration stack with modular components that adapt to your infrastructure.

USER BENEFITS

AMaze™ delivers measurable value to every stakeholder, from SOC analysts to CISOs, through a comprehensive set of operational, strategic and tactical benefits.

Benefit	Description
Focused Alerts That Matter	High-confidence alerts based only on verified adversary interaction, so teams prioritise real incidents without chasing false positives.
Reduced SOC Workload	Analysts receive clear, context-rich alerts that eliminate unnecessary triage, freeing teams to focus on actual threats instead of noise.
Intelligence From Every Threat	Captured malware, behavioural logs and adversary methods convert into organisation-specific threat intelligence that compounds over time.
High Operational Value, Lower Cost	Enterprise-grade cyber resilience with modular deployment and flexible pricing, delivering excellent return on investment.
Adaptive Scaling to Threat Levels	AMaze™ automatically scales or shifts SCAs to high-risk areas based on adversary behaviour, staying effective as the threat environment evolves.
Accelerated Incident Response	Detailed forensics, attack paths and organised telemetry shorten investigation and resolution times.
Seamless Integration	Integrates easily with your existing cyber-security stack using structured JSON and APIs, supporting both modern and legacy environments.
Psychological Cost Escalation for Adversaries	SCAs that behave like real systems increase the time, effort and risk of every intrusion, discouraging further attempts.

Benefit	Description
Air-Gapped & Disconnected Networks	Fully functional in offline, isolated and air-gapped environments — suitable for the most sensitive infrastructure.
Full IoT & IoMT Support	Specialised SCAs emulate industrial, smart and medical devices, enabling resilience in environments under-served by traditional security tools.
Coverage Across IT, OT, AI & Cloud	Unified protection across traditional IT networks, industrial systems, AI applications and cloud-based assets from a single platform.
AI Application & Agent Security	Traps attackers and rogue AI agents probing your chatbots, ai_analysts, agents and RAG — the newest attack surface, watched in the same console as the rest of the estate.
Audit & Compliance Readiness	Detailed logging of adversary actions, timelines and technical indicators supports a demonstrable, proactive security posture during audits.
Deploy Without Network Redesign	Network-based SCAs and embedded Neural Echoes — no endpoint agents, no production changes, minimal disruption, simplified compliance.
Proactive, Not Reactive	AMaze™ shapes the adversary's path before damage occurs, moving your security posture from detection-and-response to anticipation-and-control.

SEE AMAZE™ IN ACTION

The organisations that thrive in this threat landscape are the ones that stop reacting on the adversary's terms. Let us show you what proactive cyber resilience looks like inside your environment, with a tailored demonstration of AMaze™ built around your network, your compliance needs and the threats your sector faces.

Request a demo: info@mirrormire.ai

CONTACT MIRRORMIRE

www.mirrormire.ai | info@mirrormire.com | +1 (650) 504-3863