TREACLE TECHNOLOGIES i-MIRAGE DECEPTION & RESPONSE PLATFORM

In the art of war, deception is often the greatest weapon
Deception. Autonomous Protection.

Treacle Tech
Security, Trust, Assurance

ABOUT

Treacle Technologies features an AI-Based Proactive Deception System that detects, disguise, and deceives the adversaries.. Our flagship platform, i-Mirage , uses Artificial Intelligence to deploy decoys that engages the adversaries with precision. By introducing pro-active defense mechanism in the network, i-Mirage allows organizations to uncover threats at a very early stage of the cyber kill chain and respond with actionable intelligence.

With a focus on innovation and quantifiable outcomes, Treacle has earned recognition through national-level programs and has been adopted by leaders across different sectors. The platform empowers the organization to know the unknown, reduce response time, and strengthen cyber resilience.

WHY i-MIRAGE

Treacle Tech
Security, Trust, Assurance

CYBER DEFENSE FOR THE DIGITAL AGE

Domain	Capabilities
Identity & Access	Active Directory decoys, Decoy-docs
Data Security	Lure files, fake databases (SQL, NoSQL), data exfiltration
Customized Threat Intelligence	Real-time IOC extraction, Attack replays, IP reputation scoring, Targetted Malware Capture
Infrastructure Security	IoT, SCADA, legacy system deception for hybrid networks
Incident Response	Threat attribution, timeline visualization, forensic replay
Automation & Orchestration & Recommendation Engine	Risk-weighted IP blocking, automated decoy tuning

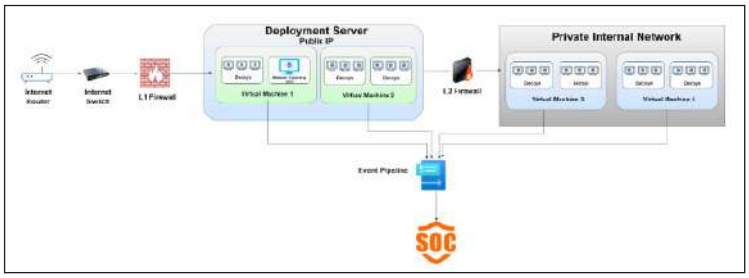
KEY ARCHITECTURAL COMPONENTS

i-Mirage™ Deception Engine

Includes an extensive suite of high-interaction decoys such as HTTP, FTP, SSH, RDP, VPN, SQLi, LFI, XSS, Active Directory, Printer, DNS, LDAP, SMTP, SMB, Modbus, Database, OT/ICS systems, specialized Malware Capturing Decoy (Octopus) and Reverse Shell environments. Each decoy mimics real services and assets to lure, engage, and analyze adversaries without exposing production systems.

Distributed Event Streaming Platform

Streams real-time telemetry data from all decoy zones, including DMZ, internal networks, and operational technology (OT) environments. Ensures continuous logging, alerting, and data synchronization across the platform for unified threat visibility



Self-Restoration and Containment Engine

Automatically restores compromised decoys to a clean state while preserving full forensic records of adversary's actions. Enables uninterrupted engagement and immediate deception surface recovery during active threats

AI-Guided Deployment and Customization Engine

Learns from adversary's dwell time, lateral movement patterns, and TTPs (tactics, techniques, and procedures) to dynamically update decoy configurations and increase adversary interaction depth

Specialized Malware Capture Decoy

Isolate, records, and analyzes tools, scripts, and malware deployed by adversaries. Extract actionable Indicators of Compromise (IoCs) for threat intelligence feeds, supporting early detection of novel threats and zero-day exploits

TRUSTED BY

Treacle Technologies currently serves organizations across the following sectors:

A leading higher education institute

A major state law enforcement department

One of India's busiest international airports

A global engineering and defense technology company

A key state government department

These clients operate in high-risk environments and rely on i-Mirage™ for continuous **threat detection, proactive defense, and deception-led resilience.**

Backed By Innovation and National Recognition

Treacle Technologies currently serves organizations across the following sectors:

Selected for government-backed innovation grants from the Ministry of Electronics and IT, Department of Telecommunications, and Department of Science and Technology, Government of India.
Winner of the AWS Campus Fund Grand Challenge, receiving international cloud credits and support. Selected among top Indian startups to represent the country at the Dubai Expo under the Startup India initiative.
Supported by leading deep-tech incubators and institutional partners including C3iHub and SIIC at IIT Kanpur.
Backed by leading angel investors.

This foundation of public and private sector support reflects Treacle's strength as a research-led and commercially validated

Treacle Tech
Security, Trust, Assurance

USE CASES ACROSS SECTORS

Banking/Finance
Ransomware, Credential Reuse, Lateral Movement, Targetted Malware, Early Response to Attacks

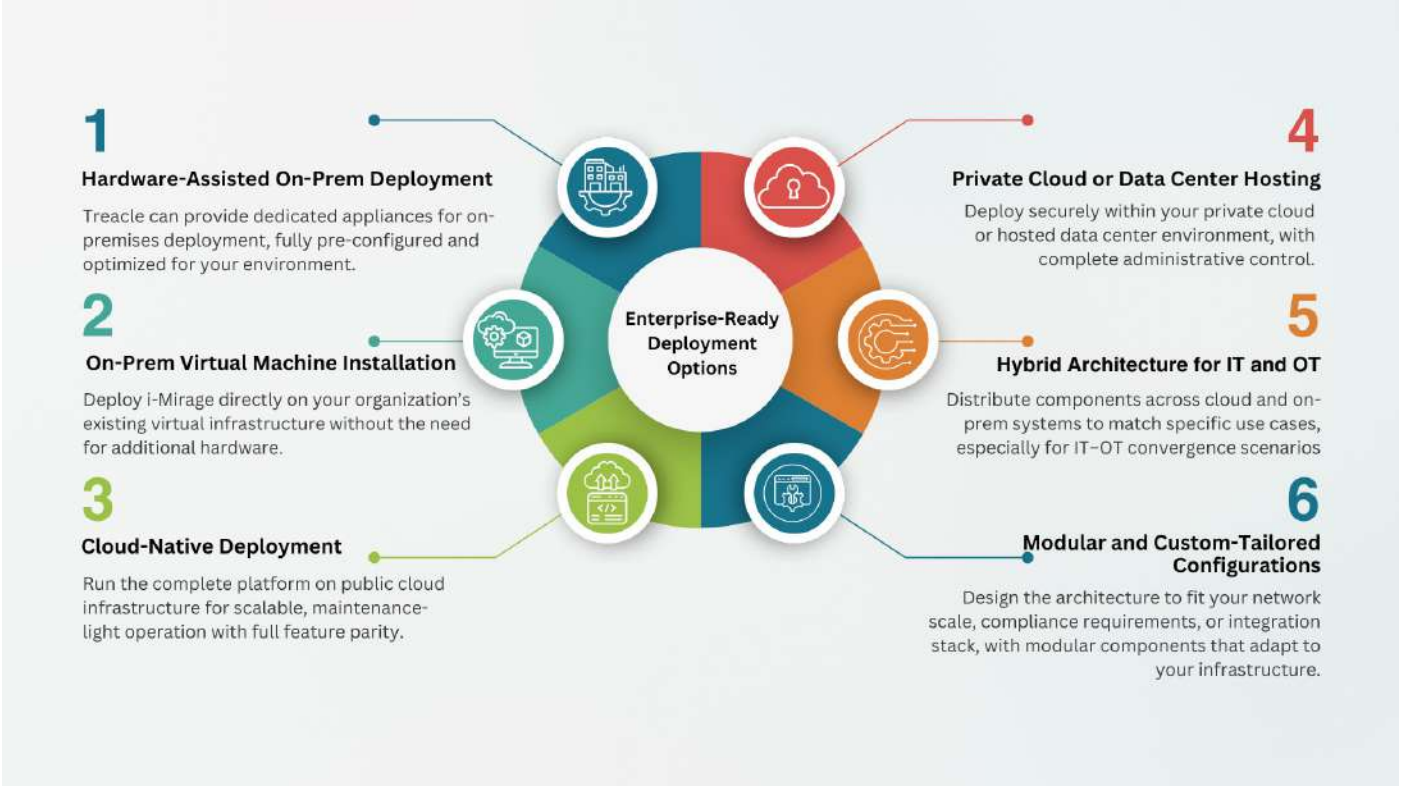
Government
Zero-day protection, APT detection, SOC optimization

Manufacturing/OT
ICS protocol decoys, SCADA lateral movement

Telecom
Early Attack Detection, rogue base station detection

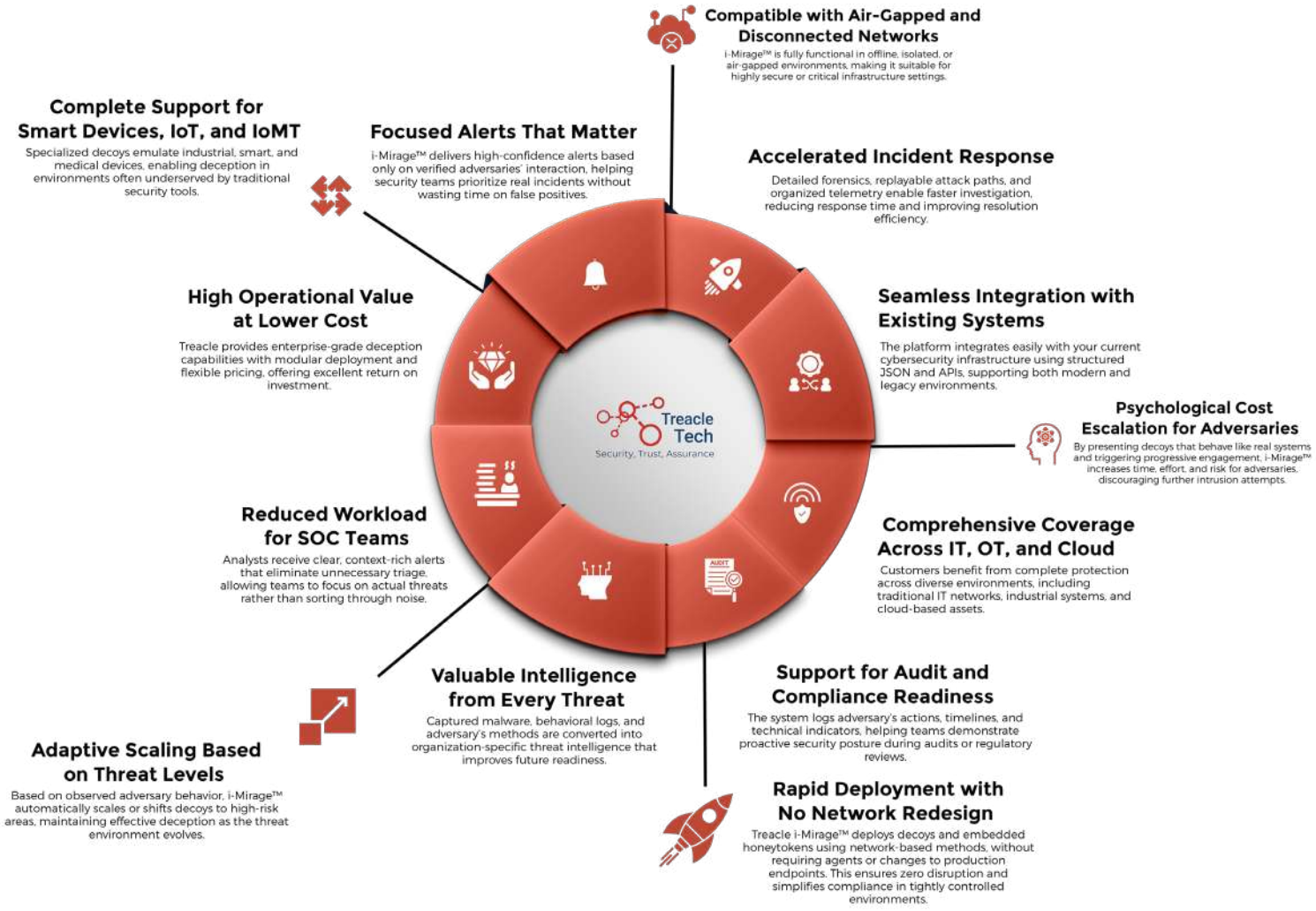
Healthcare
Patient data lure traps, medical device mimicry

Enterprise-Ready Deployment Options



Treacle Tech
Security, Trust, Assurance

USER BENEFITS



CONTACT TREACLE

www.treacletech.com | contact@treacletech.com | IIT Kanpur & Gurugram | +91 8420407686