Infopercept

INSINSENSE

A Platform Led Managed Security Services *(Real MDR)* Operating Platform

Cybersecurity with an attacker's mind and a defender's brain - delivered as a platform, operated as **Real MDR.**

Invinsense is a platform led managed security services operating platform built by Infopercept to help enterprises continuously reduce cyber risk, simplify security operations, and stay within budget.

Invinsense Real MDR is not a module.

It is the **operating model** through which the entire Invinsense platform is delivered — combining technology, intelligence, and 24×7 managed services across

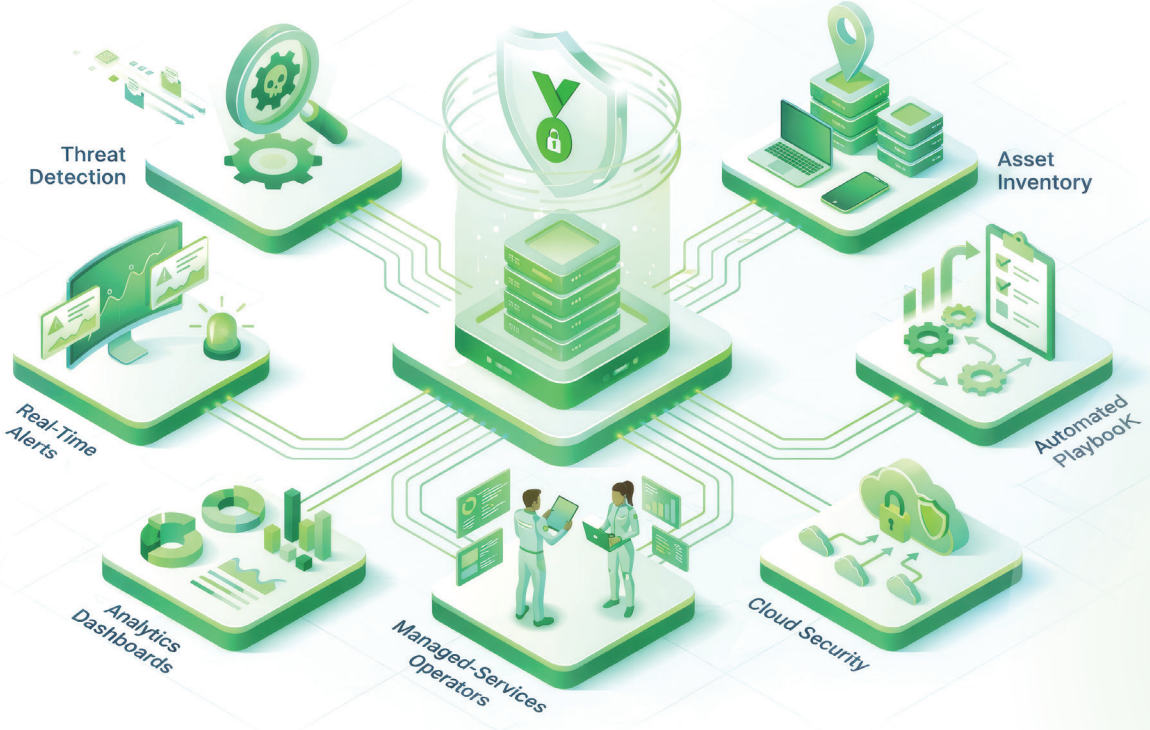
Detection & Response

Exposure Management

Security Compliance

Instead of managing disconnected tools or outsourcing security to black box MDR vendors, organizations get:

- A **deep, unified cybersecurity platform**, and
- **Outcome driven managed services** operated on that same platform



Why **Invinsense** Exists

Modern cyberattacks are:

- Identity driven
- API centric
- Cloud native
- Data theft first
- Silent and persistent

Yet most security programs remain:

- Tool heavy but risk blind
- Alert driven instead of outcome driven
- Expensive yet hard to justify to boards

Invinsense exists to change the operating model of cybersecurity.

It shifts security from:

Alerts	›	Attack paths & business risk
Tools	›	A unified security operating platform
Outsourcing	›	Platform led Real MDR outcomes

Invinsense **Real MDR**

Platform Led Managed Security Services

Real MDR is how Invinsense is delivered. It combines the Invinsense platform with 24×7 managed operations provided by Infopercept's global security teams — covering

Prevention | Detection | Response | Exposure Reduction | Compliance

What **Real MDR** Includes

Managed Detection & Response

- Continuous monitoring using Invinsense XDR & XDR+
- Threat hunting and attacker behavior analysis
- Incident investigation, containment, and response

Managed Exposure Management (CTEM)

- Continuous attack surface discovery
- Validation of exploit-ability using real attack techniques
- Fix validation and regression control

Managed Security Compliance

- Continuous evidence collection
- Control validation mapped to real incidents
- Audit readiness and regulatory reporting

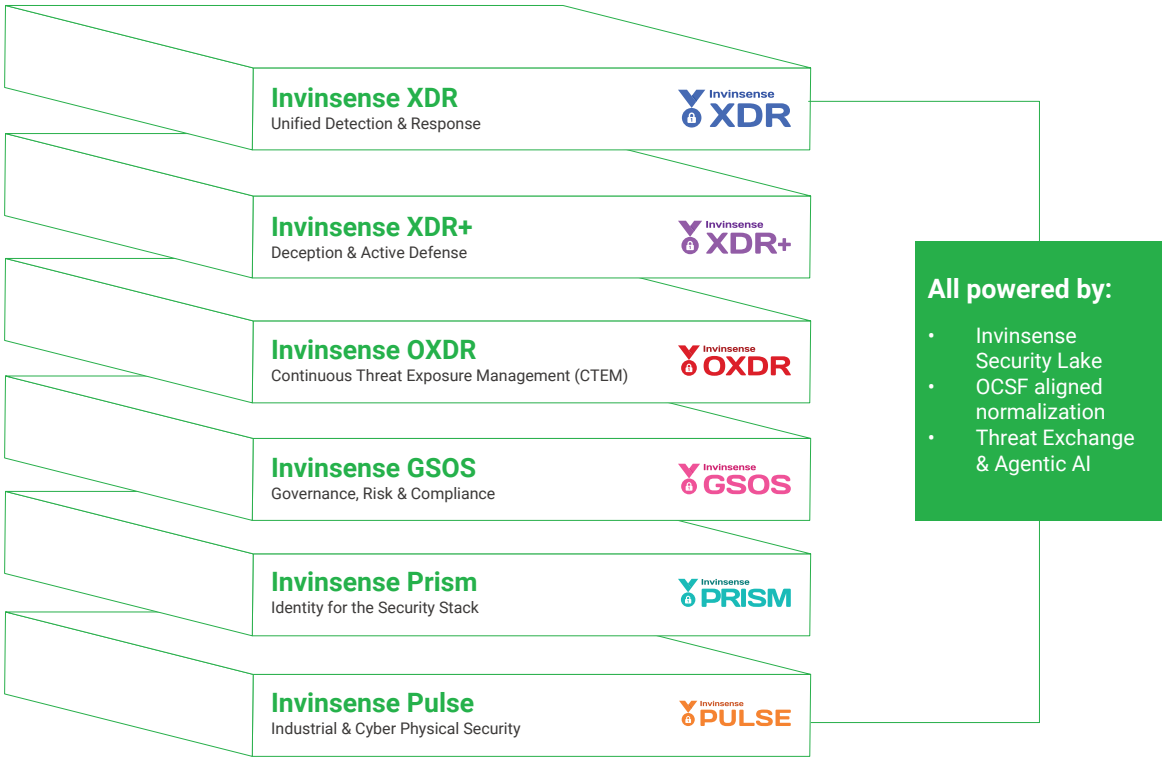
Key **Difference**

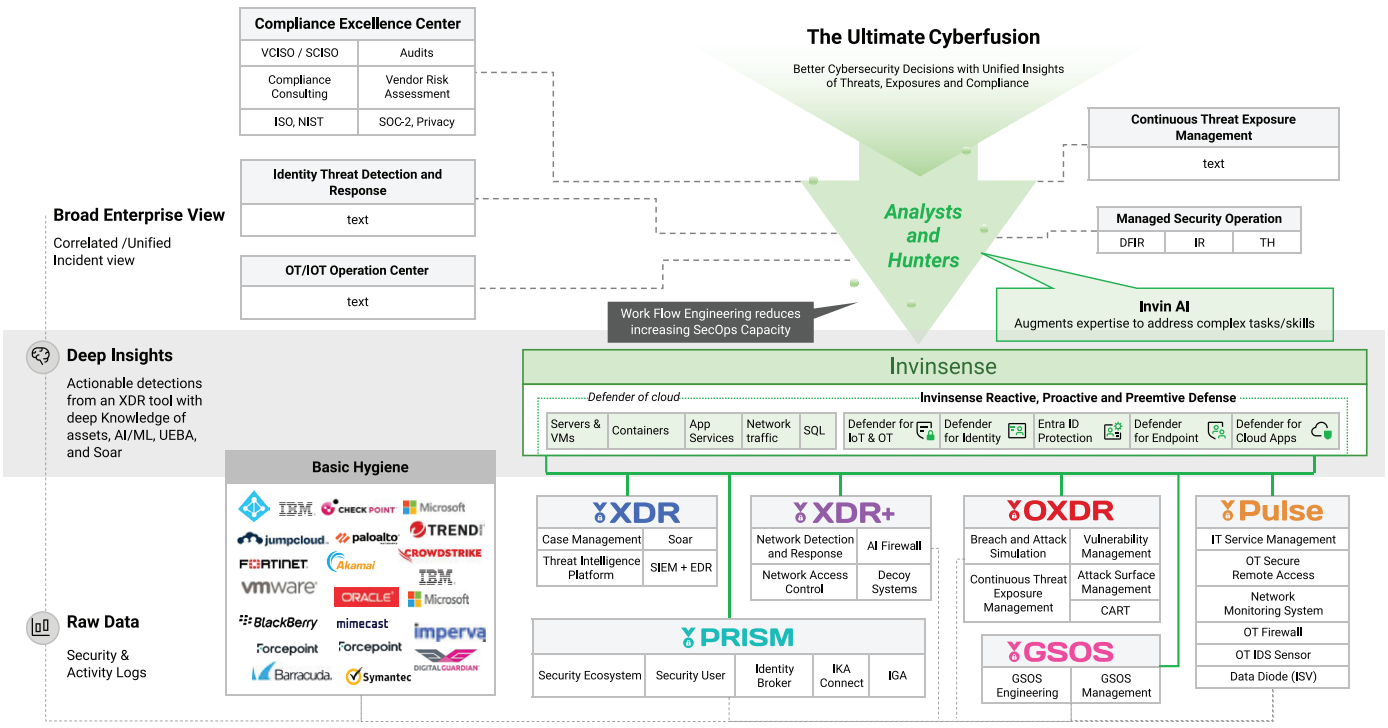
Real MDR is platform operated, not analyst overlay. Security teams act with **full context across XDR, OXDR, GSOS, identity, cloud, and OT** — enabling real response, not recommendations.

One **Platform.** One **Operating System.**

Invinsense unifies detection, exposure management, compliance, identity, OT, and AI security into a single operating platform.

Core Platform Modules





Invinsense **XDR**

Unified Detection, Investigation & Automated Response

Invinsense XDR is the core detection and response layer of the platform, designed to consolidate signals, investigations, and response actions into a single operational view.

XDR Modules

SIEM
Centralized log ingestion, correlation, and analytics

SOAR
Automated and guided response playbooks

EDR
Endpoint detection, containment, and forensics

Threat Exchange
Cross-customer and ecosystem threat intelligence sharing (policy-driven)

Threat Intelligence
Contextual enrichment using internal and external intel feeds

Case Management
End-to-end incident investigation, collaboration, and reporting

Outcomes →

40–60% faster detection	55–70% faster response	Reduced blast radius during incidents	Lower breach impact and recovery cost

Invinsense **XDR+**

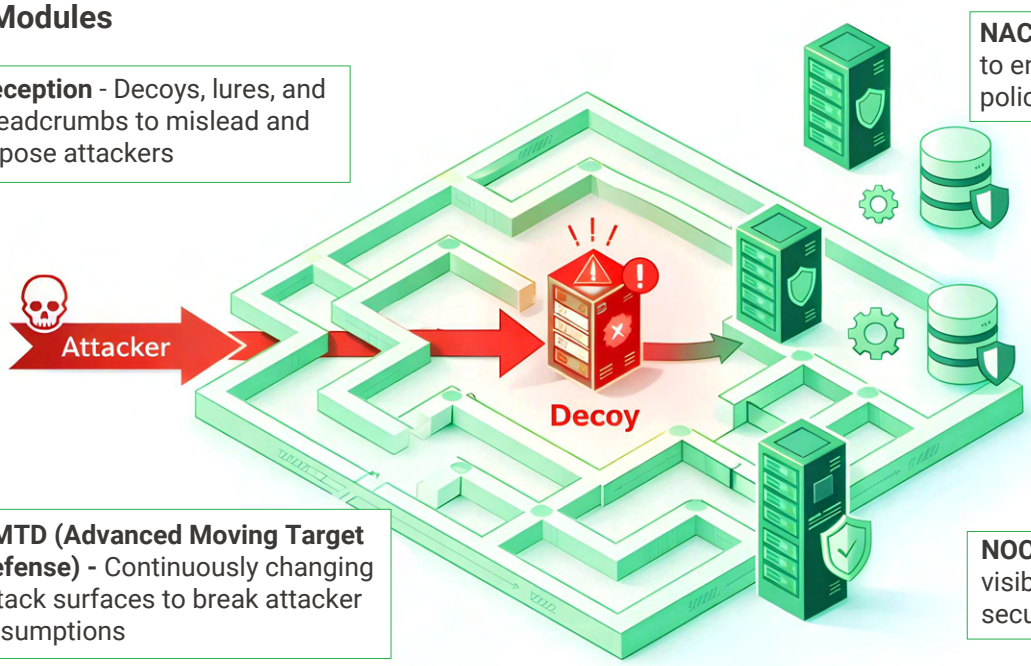
Proactive Defense, Deception & Active Threat Disruption

Invinsense XDR+ extends detection and response into **active defense**, enabling security teams to disrupt attackers before they can cause damage.

XDR+ Modules

Deception - Decoys, lures, and breadcrumbs to mislead and expose attackers

NAC - Network access control to enforce segmentation and policy-based access



AMTD (Advanced Moving Target Defense) - Continuously changing attack surfaces to break attacker assumptions

NOC - Network operations visibility tightly integrated with security signals

NDR - Network detection and response for east–west and north–south traffic visibility

Outcomes →

Near-zero false positives through attacker interaction	Earlier detection of lateral movement and credential misuse	Faster containment by controlling attacker movement

Invinsense **OXDR**

Continuous Threat Exposure Management (CTEM)

OXDR focuses on eliminating attack paths before attackers exploit them.

OXDR Modules

Attack Surface Management (ASM)

Vulnerability Management with business context

Breach & Attack Simulation (BAS)

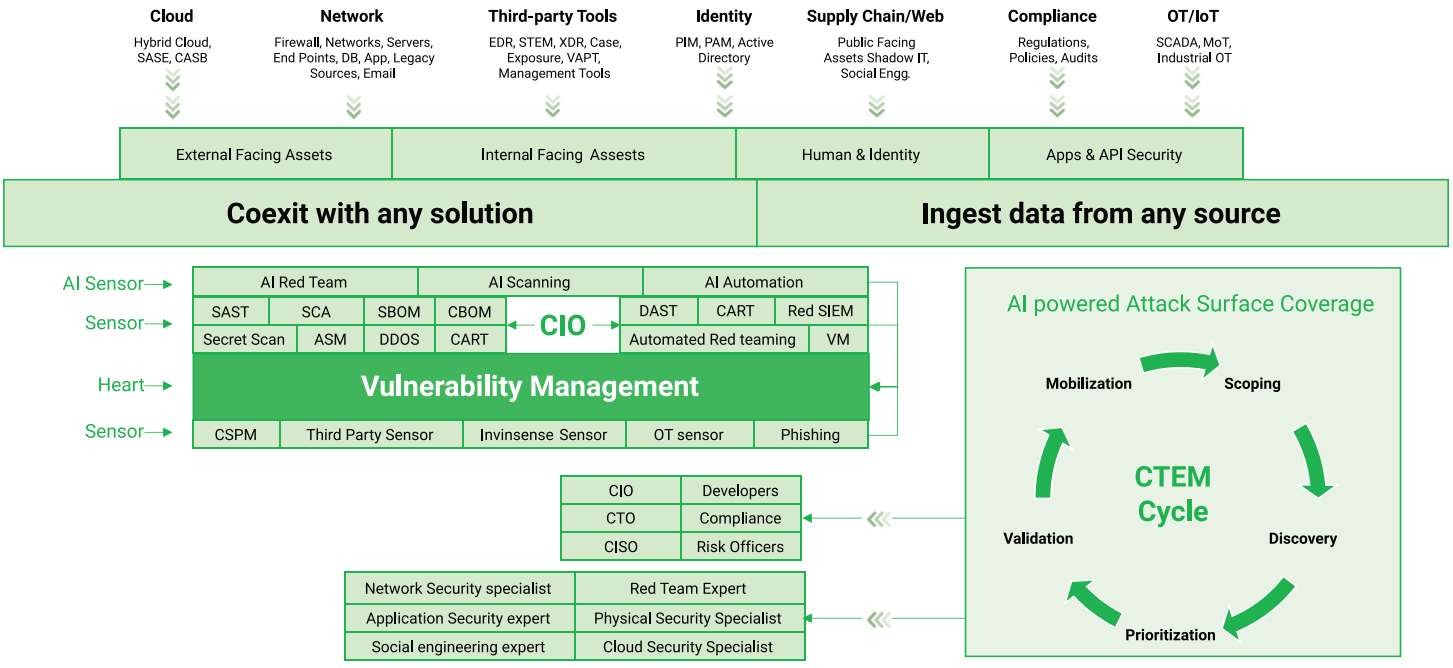
Continuous Automated Red Teaming (CART)

Exposure scoring and CTEM orchestration

Measured Outcomes

- Average 76% reduction in exploitable exposures within three CTEM cycles
- Collapse of identity, API, cloud, and lateral movement attack paths

Invinsense Oxdr-Unified Exposure Management Platform



Invinsense **GSOS**

Governance, Risk & Compliance — Operationalized

GSOS embeds compliance directly into daily security operations.

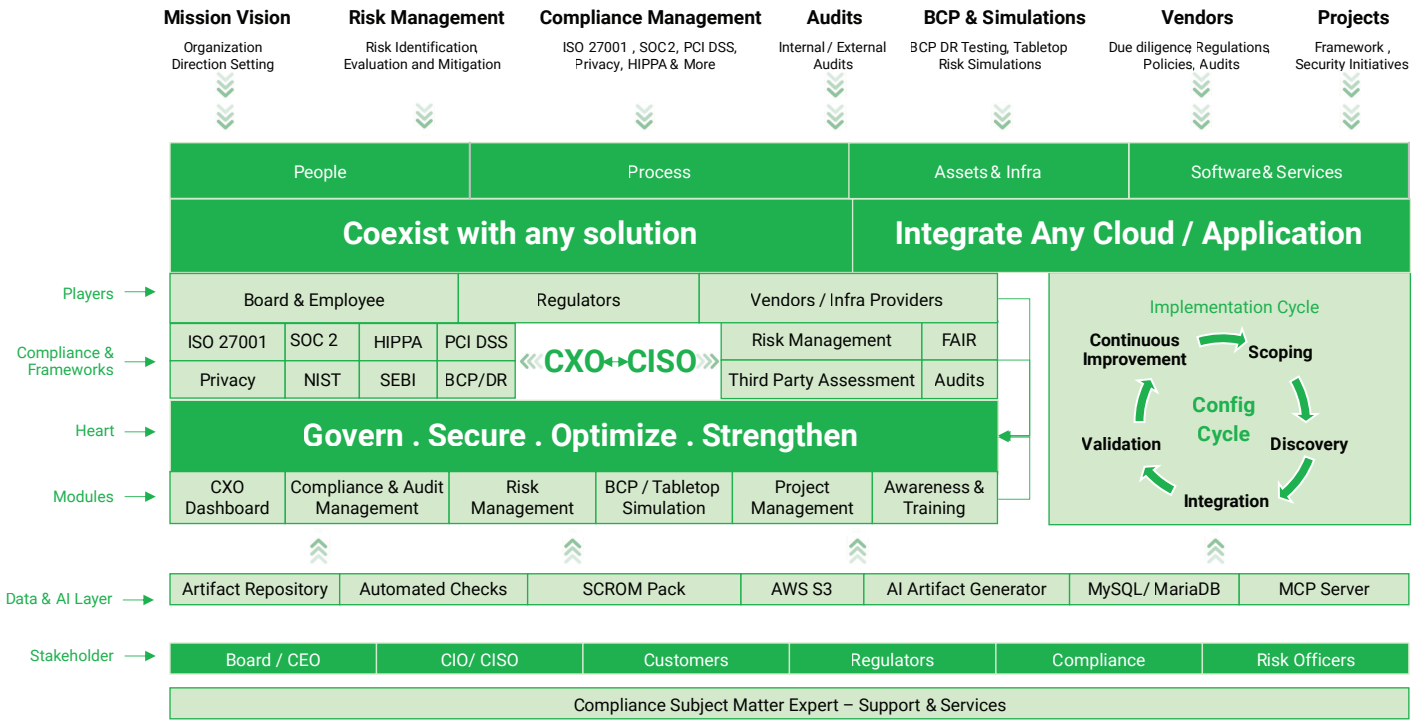
GSOS Modules

Supported Frameworks

ISO 27001 | SOC 2 | PCI DSS | SEBI | RBI

SAMA | HIPAA | NIST | CIS

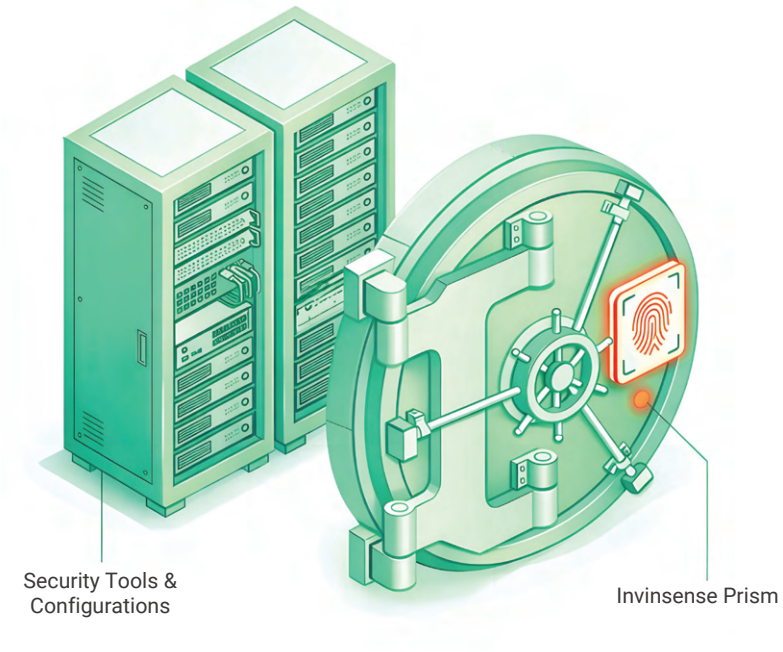
Outcomes → Reduced audit fatigue | Faster regulatory response | Stronger legal defensibility



Invinsense **Prism**

Identity & Access Management for the Security Stack

Prism governs who can access every security tool.



- Central IAM for security platforms
- Vendor-agnostic
- Integrates with existing IDPs and IGA tools

Outcomes

Least-privilege access across the entire security ecosystem.

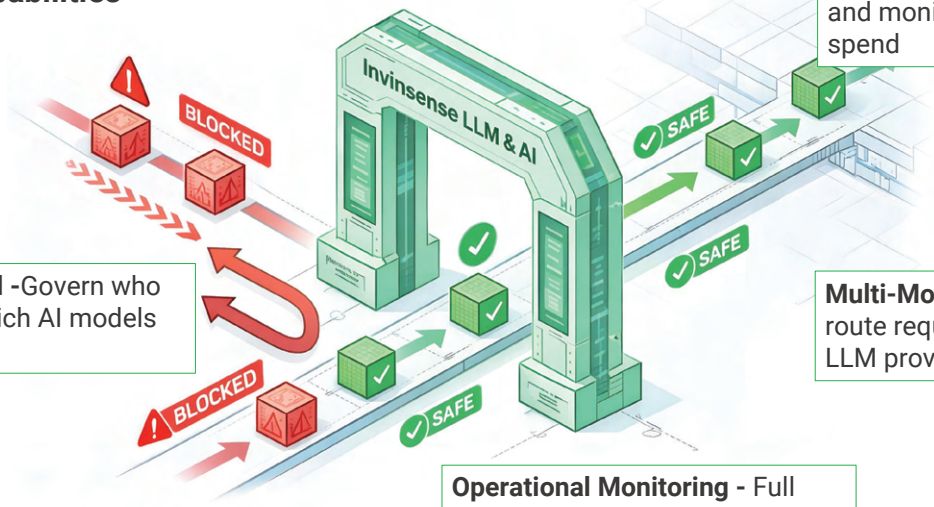
Security of **AI**

Invinsense LLM & AI Gateway

As organizations rapidly adopt generative AI and LLMs, AI itself becomes a new attack surface — for data leakage, abuse, uncontrolled access, and runaway cost.

Invinsense secures AI usage through a dedicated LLM & AI Gateway, purpose-built for enterprise environments.

Security of AI Capabilities



Cost Management - Control and monitor AI usage and spend

Access Control -Govern who can access which AI models and use cases

Multi-Model Routing - Safely route requests across multiple LLM providers

Operational Monitoring - Full visibility into prompts, responses, latency, and failures

Security Enforcement - Prevent sensitive data leakage and policy violations

Outcomes →

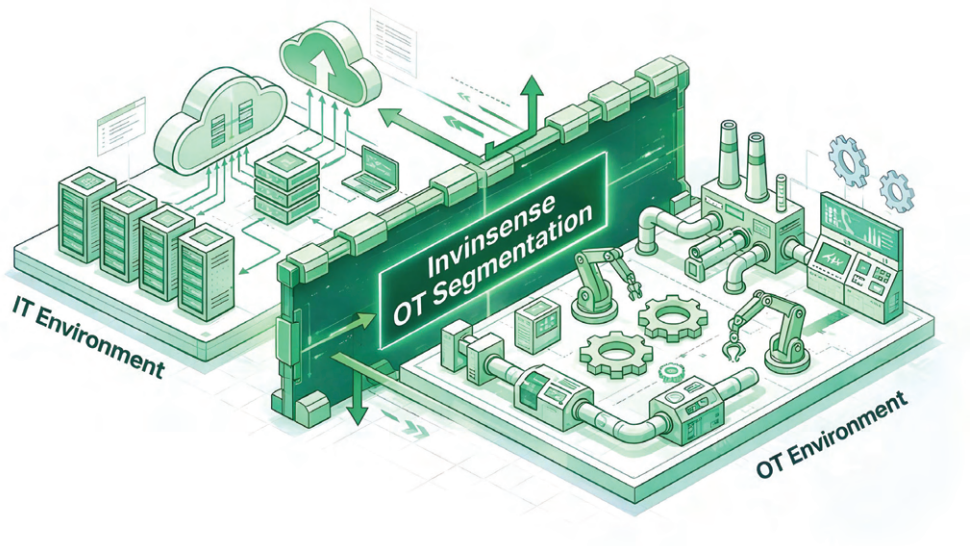
Organizations can adopt AI confidently - without sacrificing data security, governance, or budget control.

Invinsense **OT**

Industrial & Cyber-Physical Security

Invinsense OT secures manufacturing, utilities, energy, and critical infrastructure environments.

- OT-aware monitoring and detection
- Ransomware and lateral-movement prevention
- Remote access and segmentation validation



Outcomes → Reduced downtime and elimination of IT-to-OT attack paths.

Security with **AI**

Security Lake, OCSF & Agentic Intelligence

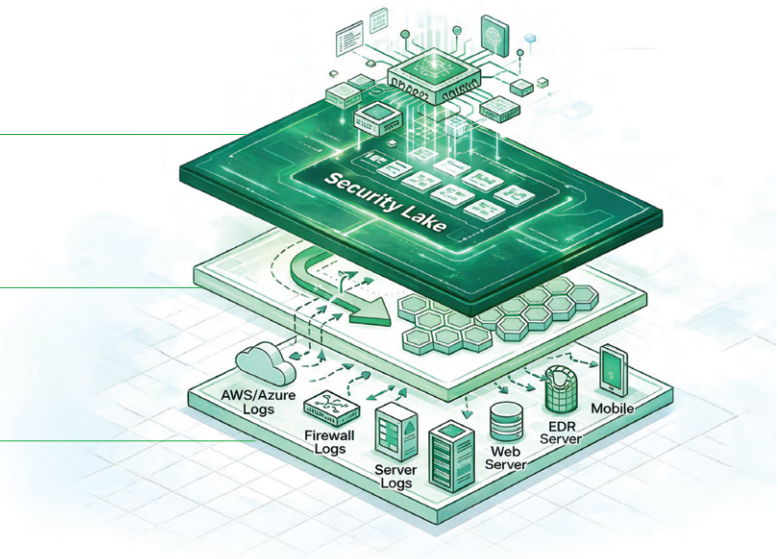
Invinsense uses AI to power security itself — not as a bolt-on, but as a foundational capability.

Core Components

Invinsense Security Lake - A unified, scalable security data lake

OCSF Normalization -Standardizes data from any security tool into a common schema

Agentic AI - Assists analysts with prioritization, investigation narratives, and next-best actions



Why This Matters

Any tool. Any format. One data model.

Faster investigations and correlations

Reduced analyst fatigue

Future-proof analytics across XDR, OXDR, GSOS, OT, and AI security

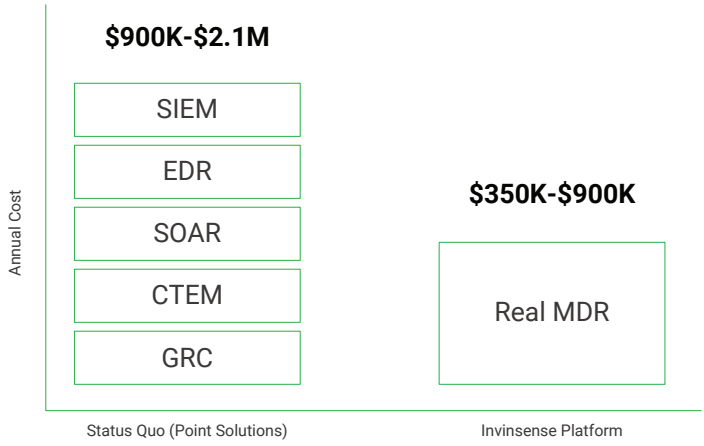
Outcomes → Security teams gain clarity, speed, and consistency — even as environments grow more complex.

Invinsense **Security Lake & OCSF**

One Data Model. One Source of Truth.

All security data is normalized using OCSF, enabling faster investigations, simpler integrations, and future proof analytics.

Built for **Real World Economics**



- One platform
- One operating model
- One managed services layer

Outcomes

- 40–60% lower total cybersecurity spend
- 5×–10× return on security investment

Who Chooses **Invinsense**

Boards - clarity on cyber risk

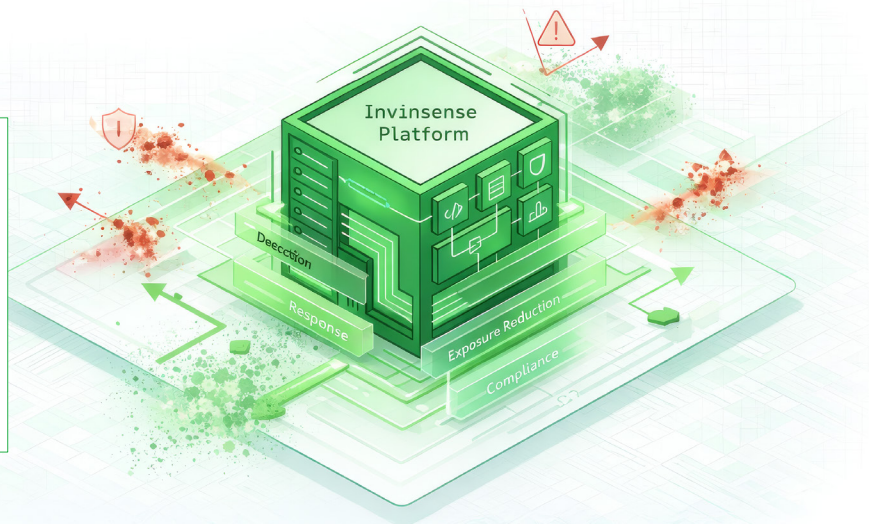
CISOs - measurable risk reduction

CIOs / CTOs - platform simplicity

CFOs - predictable economics

The Invinsense **Promise**

- We don't sell tools. We deliver platform led Real MDR outcomes.
- We don't add noise. We remove attack paths and reduce business risk.
- Invinsense is not just a platform. It is a Real MDR cybersecurity operating system.



Invinsense by *Infopercept*

Built from 12+ years of real world attacks, defenses, and continuous exposure reduction across industries.

Infopercept

INVINSENSE

Office Address

3rd floor, Optionz Complex
Opp. Hotel Regenta,CG Road,
Navrangpura, Ahmedabad -
380009, Gujarat, INDIA

Contact Detail

www.infopercept.com

sos@infopercept.com

+91 9898857117