Claude Mythos

Infopercept | INVINSENSE

Mythos-Ready Security with Invinsense

Building Control in the Age of AI-Driven Vulnerability Storms

Executive Summary

AI systems like Mythos have fundamentally altered cybersecurity.

- Vulnerabilities can now be discovered autonomously
- Exploits can be generated instantly
- Attacks can be executed at machine speed

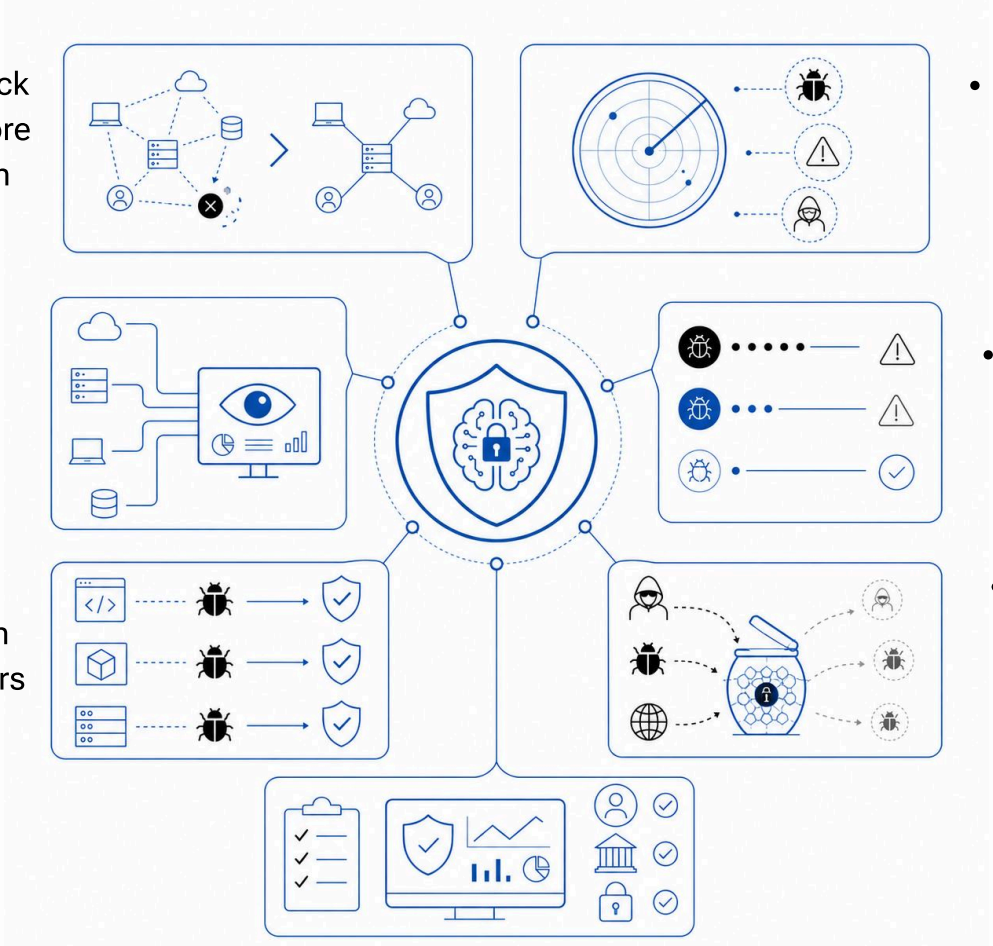
This creates a continuous exposure reality, where organizations face:

- Infinite vulnerabilities
- Compressed response timelines
- Overwhelming remediation cycles

However, the real challenge is not visibility—it is control.

This whitepaper introduces a Mythos-ready security architecture powered by Invinsense, enabling organizations to:

- Reduce attack surface before amplification
- Discover exposures proactively using offensive-first security
- Centralize exposure visibility
- Prioritize via CTEM
- Execute remediation across layers
- Contain risk through deception



- Align detection and compliance into one platform

The AI Vulnerability Storm

Mythos represents a structural shift:

- Autonomous vulnerability discovery at scale
- Chained exploits across systems
- Near-zero time to weaponization

Organizations are

no longer dealing with incidents

—they are dealing with:

Continuous Exposure

Why Traditional Security Fails

Traditional models:

- Detection-centric
- Reactive
- Tool-fragmented

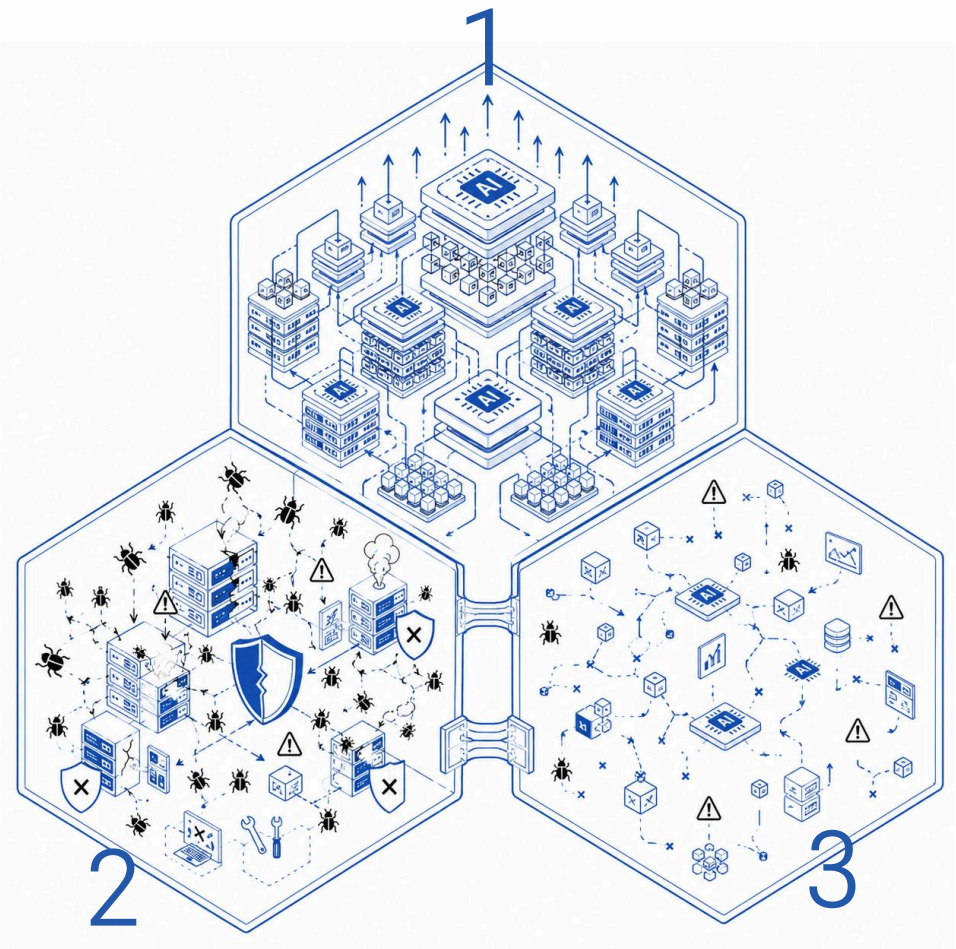
But exposure now spans:

- Infrastructure
- Cloud
- Identity
- Applications
- APIs
- Supply chain

Invinsense identifies this gap:

"Reactive detection alone is not enough for managing threat exposure."

The Mythos Constraint



1. Cost Explosion

   Running AI like Mythos across full environments is not sustainable

2. Operational Collapse

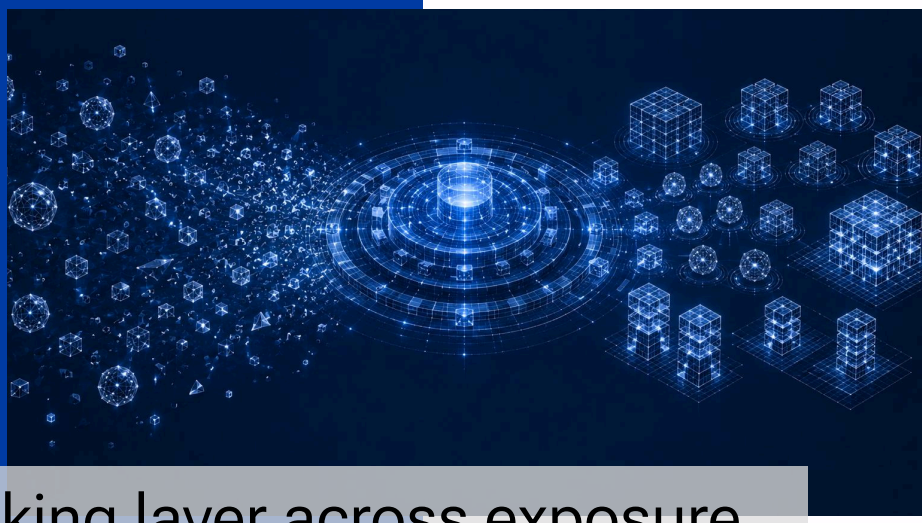
   Too many vulnerabilities → not enough remediation

3. Lack of Context

   Generic vulnerability lists lack business prioritization

Introducing the Missing Layer – Regiment AI

Regiment AI is not another AI tool.



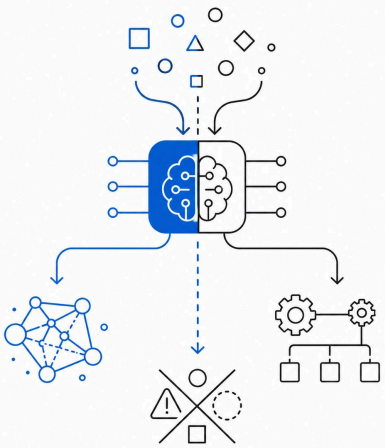
It is:

A decision-making layer across exposure, detection, and compliance

What Regiment AI Does

It continuously evaluates:

- What needs AI
- What needs deterministic execution
- What should be ignored



Output:

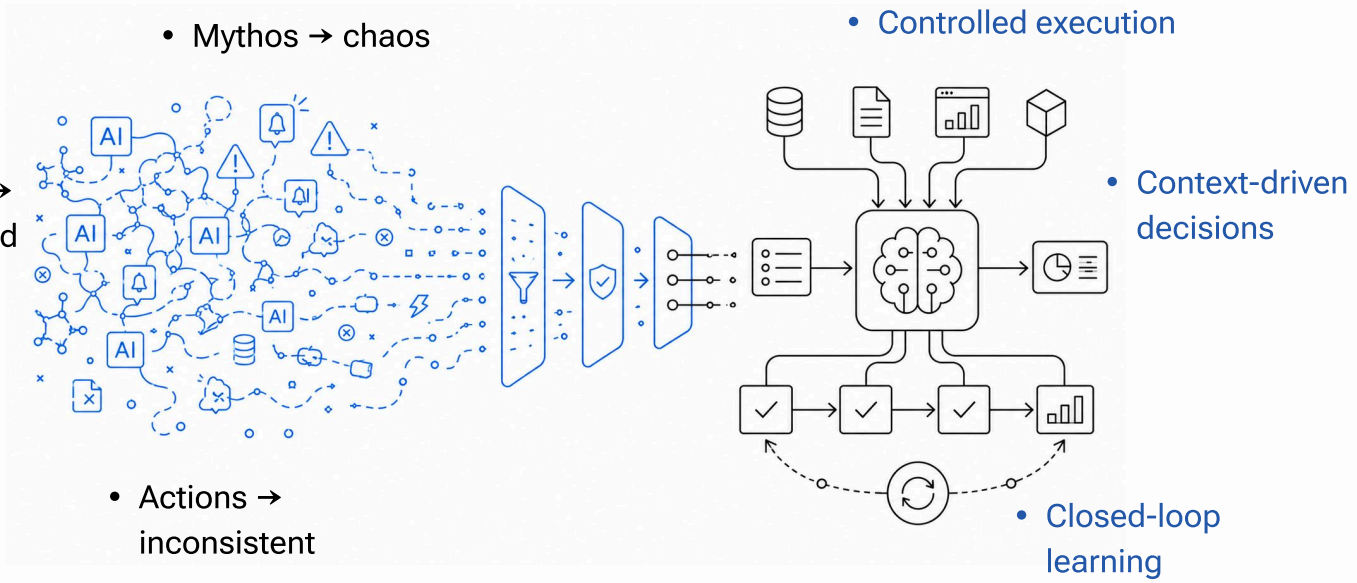
- Structured intelligence
- Not raw AI noise

Key Principle

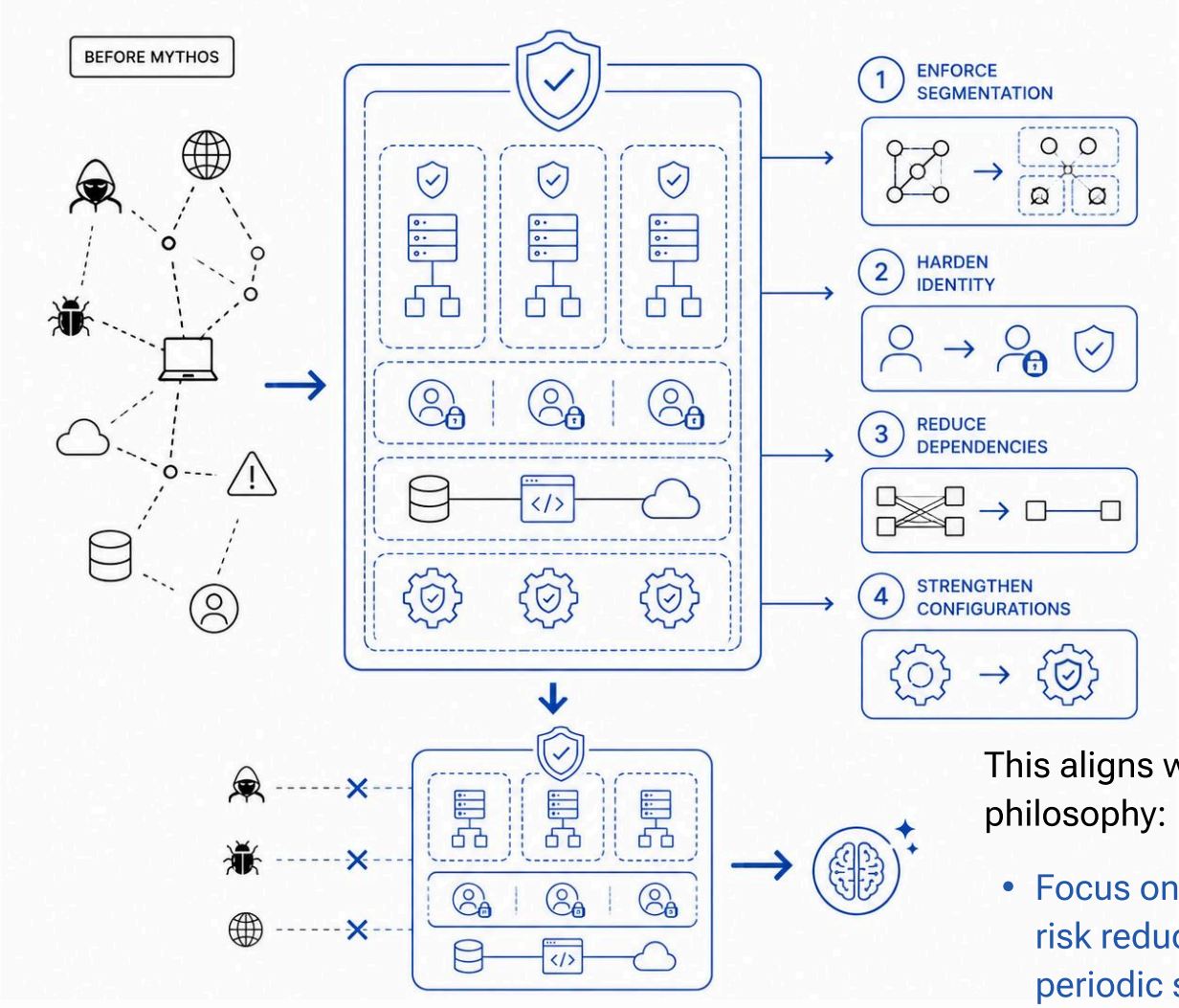
AI should not be everywhere.
It should be exactly where it matters

The Invinsense + Regiment AI Model

This is your architecture:



Steps 1: Reduce Attack Surface



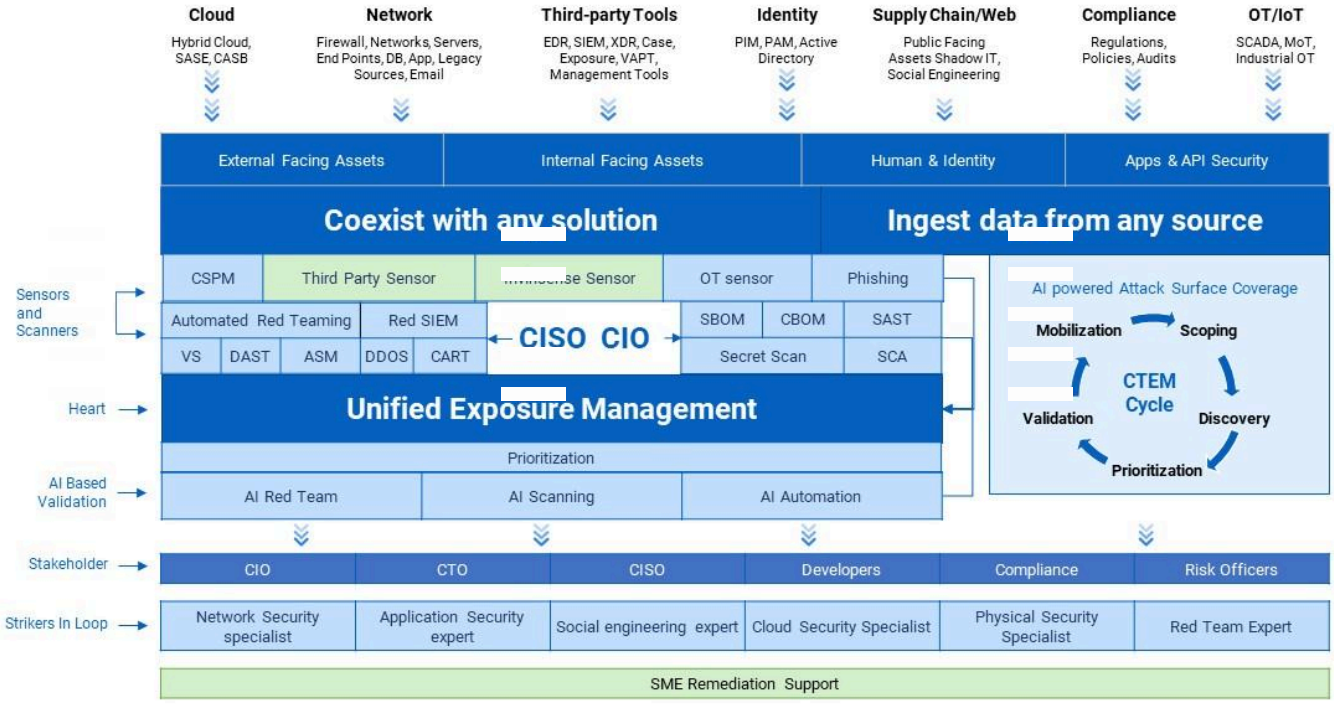
This aligns with CTEM philosophy:

- Focus on continuous risk reduction, not periodic scanning

Step 2 : Offensive-First Security (OXDR)

Invinsense OXDR

Invinsense OXDR-Unified Exposure Management Platform



Invinsense OXDR introduces:

Invinsense OXDR

"Get attacked to prevent breaches."

Core Capabilities:

- Attack Surface Monitoring (ASM)
- Vulnerability Management
- Breach & Attack Simulation (BAS)
- Continuous Automated Red Teaming (CART)
- Adversarial Exposure Validation

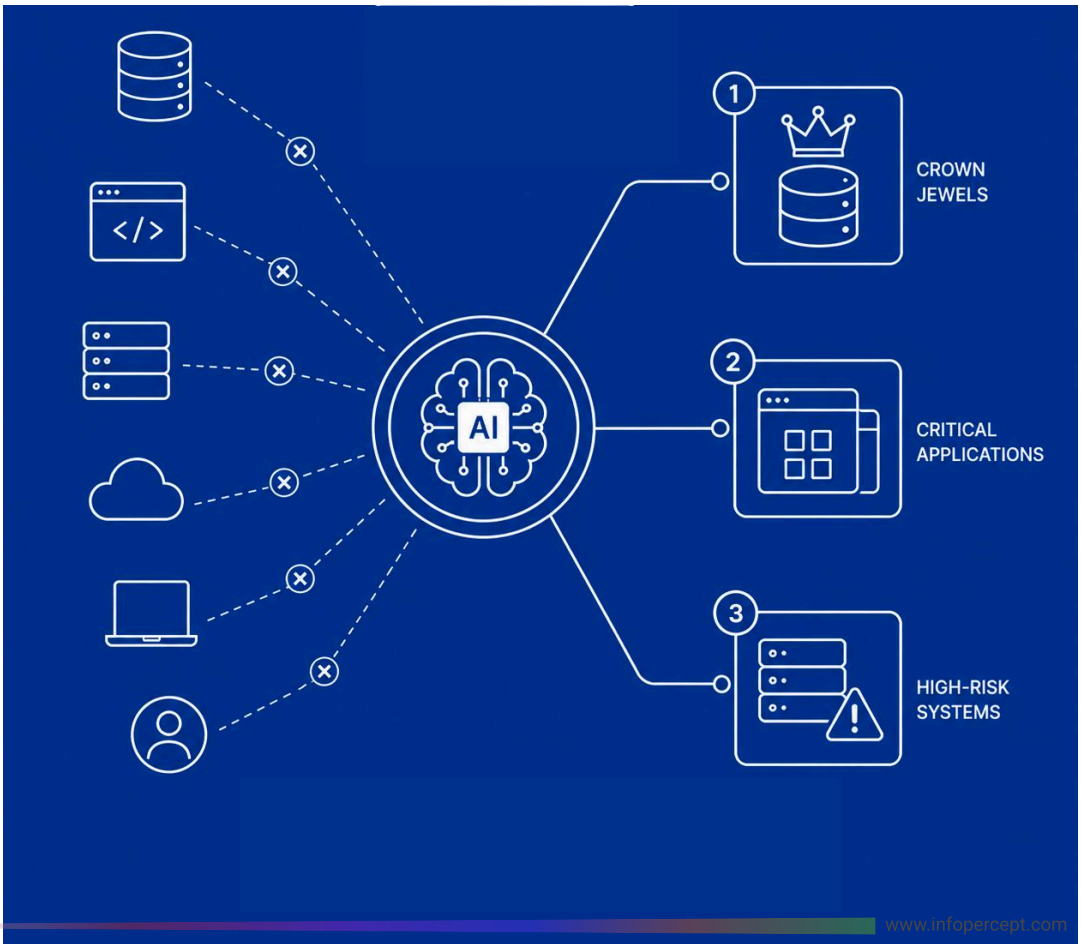
Outcome:

Continuous exposure discovery	Business-context prioritization	Alignment of DevSecOps + security

Step 3: Controlled Use of Mythos

Instead of scanning everything:
Use Mythos on:

- Crown jewels
- Critical applications
- High-risk systems



Step 4: Unified Exposure Management (UEMP)

Invinsense OXDR acts as: Single source of truth for all exposures

Infra | Cloud | Identity | Applications | APIs

Step 5: CTEM as the Core Engine

CTEM enables:

- Continuous identification
- Risk-based prioritization
- Business-aligned remediation

Outcomes include:

- Better risk prioritization
- Attack surface visibility
- Cross-team collaboration

Step 6: Exposure Remediation (3H Model)

1. Harmony of People

   Clear ownership across teams

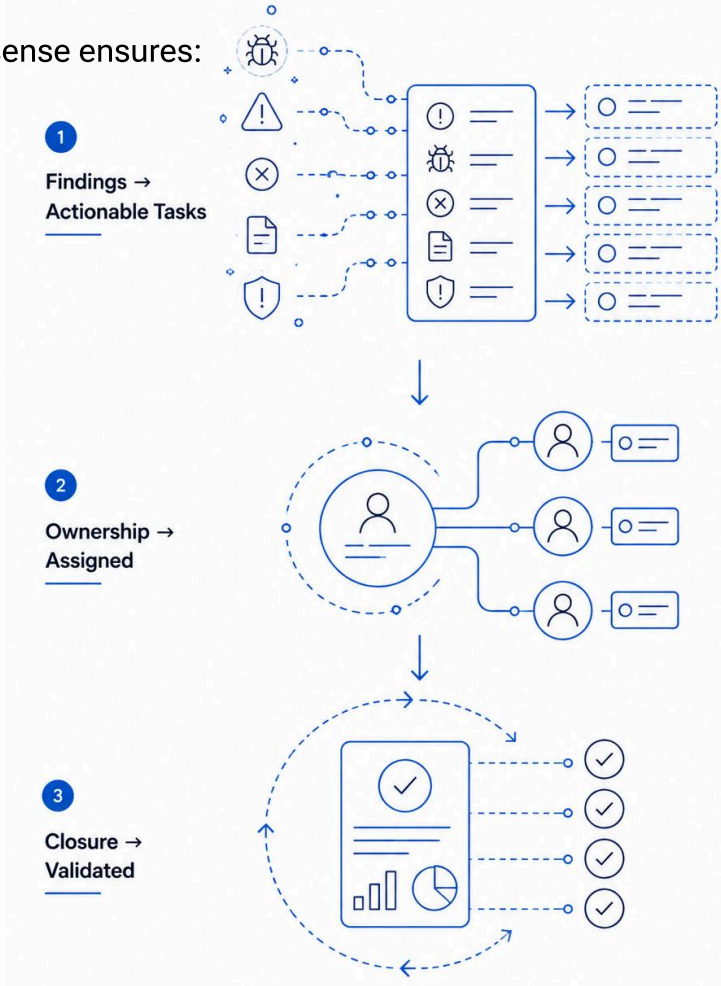
2. Harmony of Platforms

   Unified exposure view

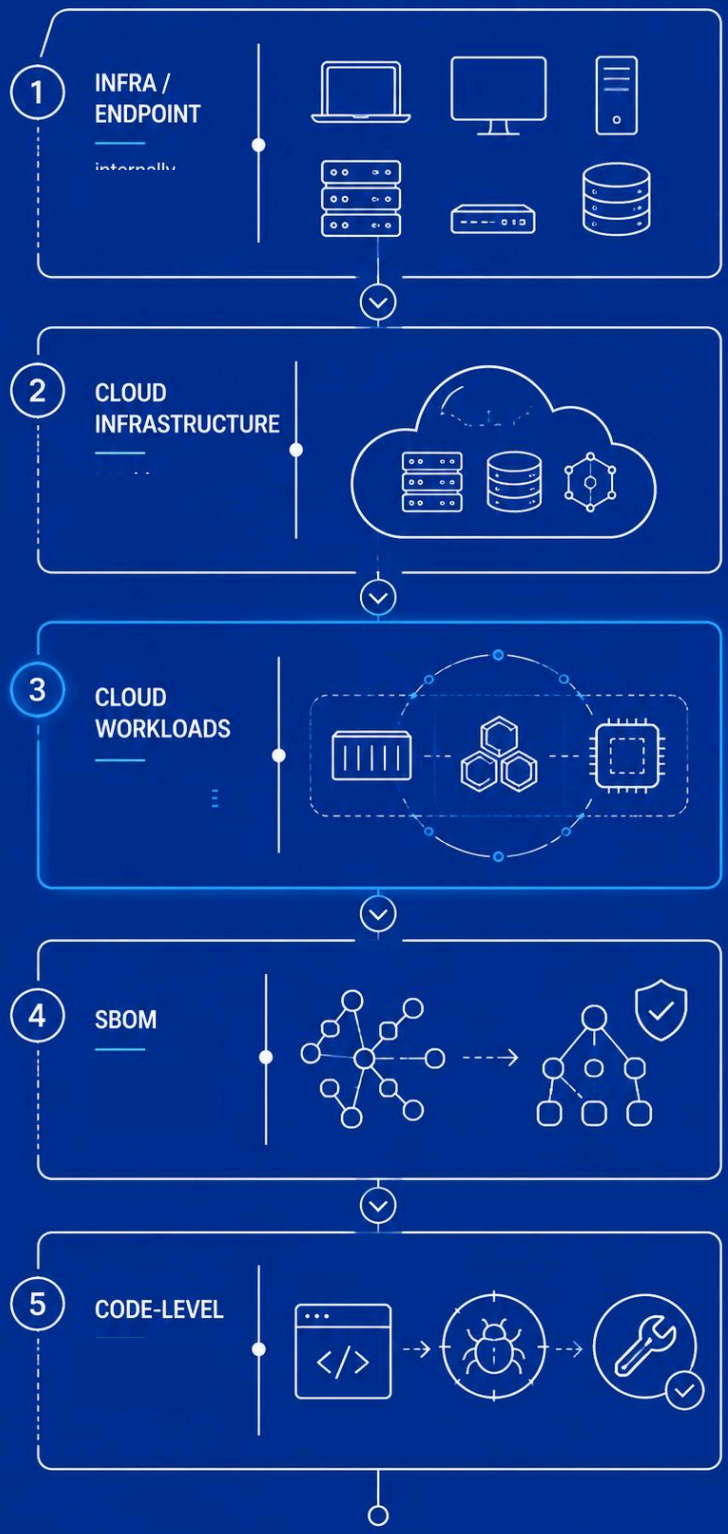
3. Harmony of Partners

   Execution, not advisory

Invinsense ensures:



Step 7: Layered Remediation Model



1. Infra / Endpoint

   Handled internally

2. Cloud Infrastructure

   Handled by provider

3. Cloud Workloads

   Handled with Invinsense

4. SBOM

   Dependency risk reduction

5. Code-Level

   Deep remediation

Invinsense supports:

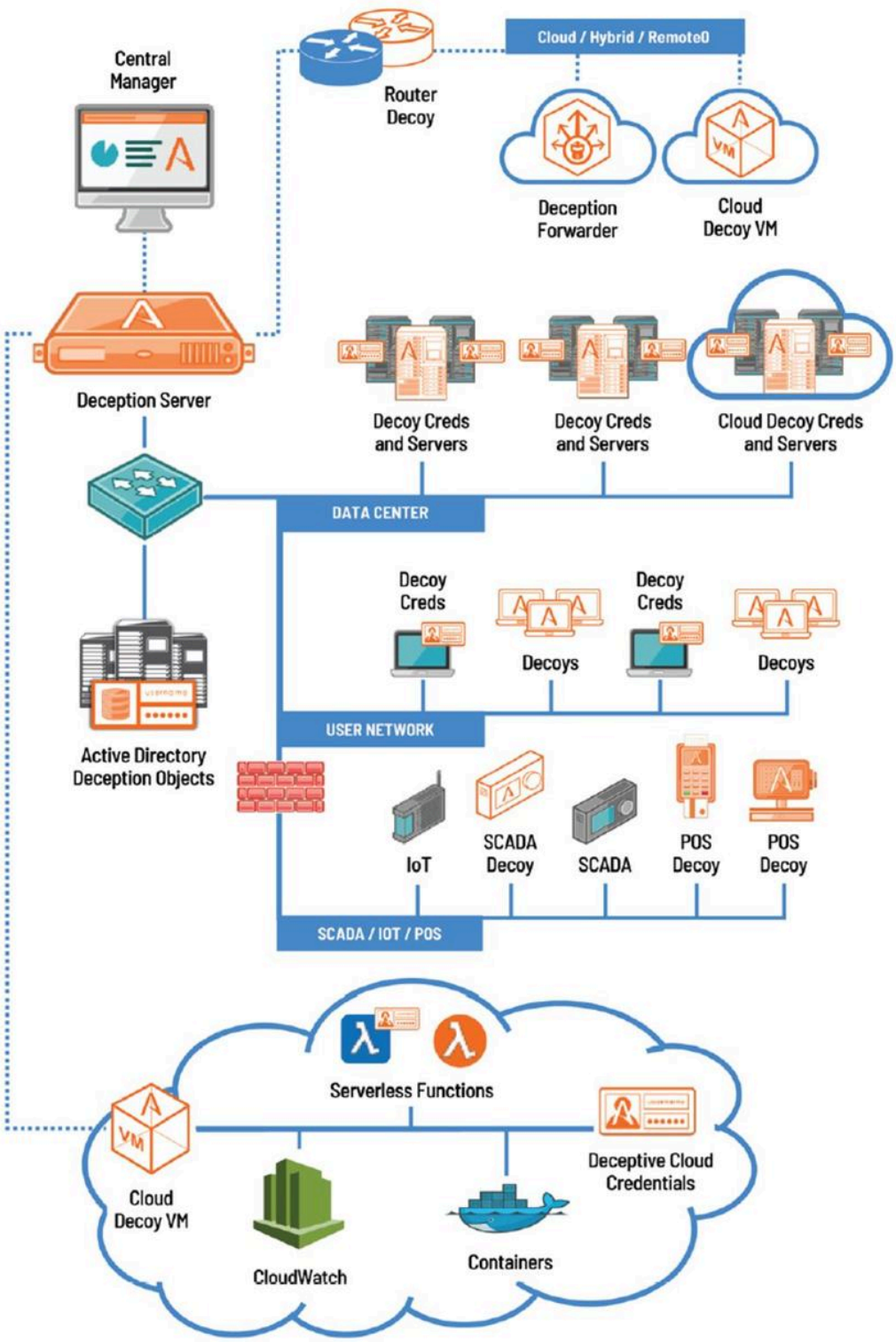
- Manual + automated patching
- Code-level fixes
- DevSecOps integration

Step 8: The Remediation Gap

Reality:

AI finds vulnerabilities instantly
Fixing them takes time

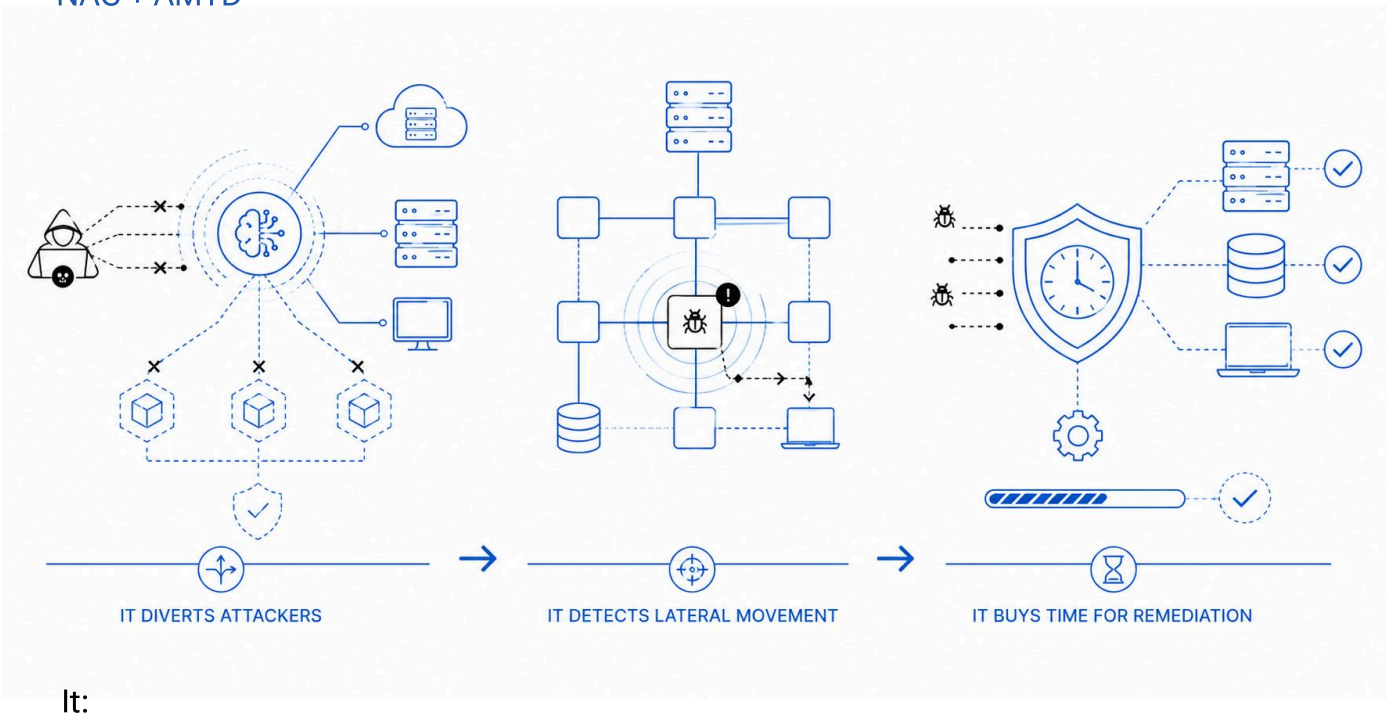
Step 9: Deception with XDR+



Invinsense XDR+

Invinsense XDR+ enables:

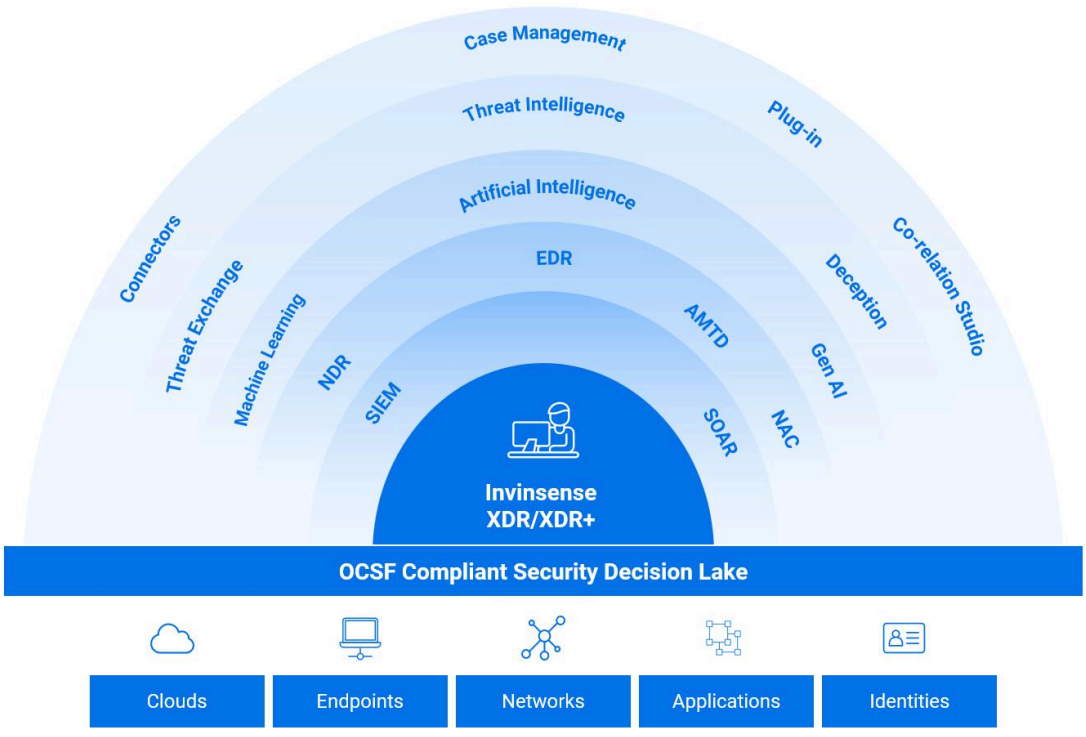
- Deception (honeypots, decoys)
- Network Detection & Response
- NAC + AMTD



It:

- Diverts attackers
- Detects lateral movement
- Buys time for remediation

Invinsense XDR and XDR+



Step 10: Detection (XDR)

Invinsense XDR

- AI-driven threat detection
- Automated response
- Behavioral analysis

Step 11: Governance (GSOS)

Invinsense GSOS provides:

- Compliance-as-code
- Automated audits
- Risk alignment

Moves from:

- Manual GRC → GRC Engineering

Continuous evidence collection

Test to Control Mapping

Audit-ready dashboards

Regulatory confidence

- Privacy & Data Protection Compliance
- Information Security Compliance
- Identity & Access Security Compliance
- Regulatory & Industry Compliance

RBI | SEBI | IRDA | MOP | ISO | NIST | HIPAA | Privacy | Continuity

Key Features of an Effective Compliance Workflow Automation Solution

Regiment AI – The Decision Layer

RegimentAI

Across all steps:

- Prioritization
- Risk scoring
- Execution decisions

Final Architecture

Strategic Advantage

Invinsense delivers:

- Unified platform
- AI + human expertise
- Exposure-to-remediation closure

We don’t stop at detection—we fix.

DETECTED ANALYZED FIXED

Conclusion

Infopercept

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