Invinsense: The CISO's Ally in the Boardroom

Translating Security Investments into Business Risk Reduction

1. The Reality: Boards Judge Security as Business Risk, Not Technology

Boards care about one thing:
"How will this protect our money, operations, brand, and compliance?"

But CISOs are often forced to speak in:

- Alerts, CVEs, tool names
- Compliance checkboxes
- Technical metrics without financial meaning

This creates a **communication gap**

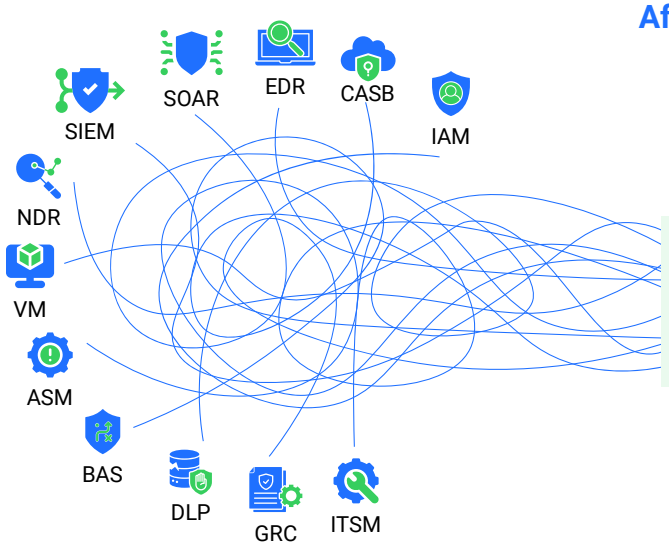
Invinsense closes this gap by turning:

- Complex security telemetry → Business-level risk signals
- Multiple tools → One measurable operating model

2. The Invinsense Advantage for CISOs

A. Better Economic Decision

Before:



After:

Board takeaway:
We eliminate waste and complexity — not add more tools.

INVINSENSE

One platform doing the work of many — **Invinsense**

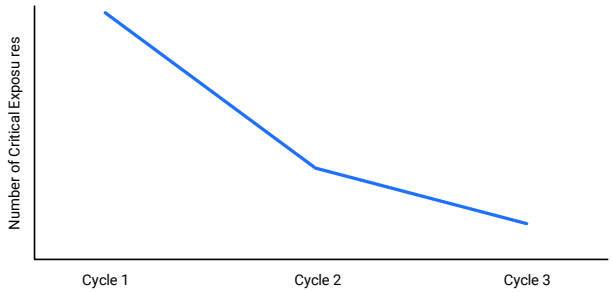
Consolidation outcomes:

Benefit	Why the Board Cares
Lower license & integration cost	Reduced spend without reduced security
Fewer vendors, contracts, audits	Operational simplicity
Fewer analysts needed for tool ops	Cost efficiency + faster outcomes

B. Better Cybersecurity Decision

Invinsense *doesn't just monitor.*
It ***improves*** *security posture — measurably.*

76% Average Reduction in Exploitable Exposures within 3 Cycles



Across CTEM programs last 12 months:

Industry	Exposures: Cycle 1 → Cycle 3	Reduction
Fintech	185 → 41	78% ↓
BFSI	232 → 62	73% ↓
SEBI Entities	121 → 23	81% ↓
Healthcare	203 → 51	75% ↓
Manufacturing	164 → 36	78% ↓

This means:

- *Attack paths closed*
- *Fraud/downtime/data-theft likelihood slashed*

C. Better Business-Language Reporting

Invinsense gives the board the **only three metrics they care about:**

Metric	What it Means
Exposure Trend ↓	Risk is reducing, not stagnating
Attack Path Reduction ↓	Controls are actually working
Response Speed ↑	Business interruption minimized

3. Invinsense Has Three Superpowers the Board Understands

A. Invinsense OXDR — Exposure Management with CTEM

Find → Validate → Fix → Verify — Repeat

Board impact:

Attack surface shrinks every quarter	Real exploitability testing (BAS, CART)	No hidden pivots to critical systems

Board message:
We don't just "have controls".
We ***prove*** *they stop attackers.*

B. Invinsense XDR — Faster Detection & Automated Response

If the attack still comes → We respond before damage.

Key outcomes (average among customers):

 **MTTD reduced** by 40–60%	 **MTTR reduced** by 55–70%	 Auto-isolation of compromised device/service	 Auto-revocation of stolen access tokens	 Reduced breach **impact** through early containment

Board impact:

Downtime avoided	Fraud losses prevented	Incident handling costs minimized

Board message:
Attacks may not stop —
*but **business disruption does.***

C. Invinsense GSOS — Governance, Compliance & Confidence

The Board's insurance against legal & regulatory chaos

Outcomes:

 Evidence collection **automated**	 Audit readiness **continuous**	 Policy control tied to **actual detections**	 Regulatory mapping (RBI/SEBI/IRDAI/GDPR/HIPAA etc.)

Board impact:

Compliance fines avoided	Faster regulatory reporting	Proof of due care documented in real time

Board message:
*We can show the regulator **what happened,***
***when we acted,** and **why we're safe**.*

4. Reframing the Toughest Board Questions

(Invinsense-driven answers written in business voice)

01

Why do we need more budget for cybersecurity?

We're not buying another tool.
We're replacing **many** tools with **one platform** — reducing overall spend.
At the same time, we're cutting our exploitable exposures by ~76% in 12 months.
Better economics + better security = smarter investment.

02

Are we secure?

No one can promise 100% security —
But I can show you **risk is falling:**
• 185 → 41 exposures in fintech
• 232 → 62 in BFSI
• 203 → 51 in healthcare
That's measurable progress — not assumptions.

03

What's the ROI?

A typical breach costs $4–5M+
(downtime, ransom, legal/regulatory, brand loss).
Invinsense costs **a fraction** of that —
and reduces the majority of that risk.
In business terms:
*We reduce **probability and impact** of a multi-million loss event.*

04

Why consolidate into Invinsense?

Because today we have too many tools delivering too little clarity.
Invinsense is **one narrative, one dashboard, one risk model**
exactly what boards expect from modern cyber investments.

05

How do we know our defenses actually work?

We run weekly attack simulations
and automated red-team validations.
Attack paths are shrinking quarter-on-quarter.
Not an opinion - **tested proof**.

06

Tell me the top 3 business risks… only three.

Risk Scenario	Invinsense Outcome
Ransomware stopping operations	Pivot paths removed via CTEM, fast response via XDR
Customer/regulated data stolen	Data exfil routes reduced by ~75%
Fraud via identity/API abuse	Blast radius dropped by ~80%

Simple story: **fewer paths to money & disruption.**

07

Are we compliant and defensible legally?

GSOS automatically collects evidence every time XDR detects and responds.
Compliance isn't manual anymore — it's continuous.
We can prove due care in hours, not weeks.

08

If you (the CISO) leave tomorrow… what happens?

Invinsense runs our security **as a repeatable system,** not tribal knowledge.
Playbooks, detections, risk metrics — all standardized.
This security program **outlives individuals.**

5. The Board's Decision Matrix

One Line Summary:
Invinsense is both a better cybersecurity decision and a better economic decision.

Value Category	Without Invinsense	With Invinsense
Security Maturity	Vulnerability counts	Risk reduction numbers
Attack Surface	Static	↓76% in 3 cycles
Incident Impact	High	Fast containment via XDR
Compliance	Manual & reactive	Automated evidence via GSOS
Costs & Tools	Fragmented & duplicative	Unified & optimized

Consolidation outcomes:

Fewer attacks succeed

Faster incident closure

Better audit posture

Higher operational resilience

6. Closing Message for the Board

Cybersecurity used to be a **cost to tolerate.**
Invinsense turns it into a **risk-reduction investment.**

Invinsense empowers CISOs to say:

CISO Statement	What the Board Hears
We reduced exploitable exposures by 76% this year.	Our breach risk dropped by 76%.
We consolidated 10+ tools into one.	We cut waste and complexity.
Our defenses are tested weekly.	We aren't relying on assumptions.
Our audits are automated.	We are regulator-proof.

Invinsense — Cybersecurity with an attacker's mind and a defender's brain… translated into board results.

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Infopercept Consulting Pvt. Ltd.

Publisher Address

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

Contact

sos@infopercept.com
www.infopercept.com