Driving Secure Growth: How a Leading Digital Finance Platform Fortified Risk, Resilience, and Regulatory Confidence with Invinsense

About the Customer

This digital-first financial services provider, part of a major retail conglomerate, offers an integrated ecosystem of offerings including loans, insurance, payments, and investments. With a flagship finance app and a suite of merchant-oriented platforms, the firm is committed to financial inclusion and accessibility at scale. As an RBI-registered NBFC, it operates at the intersection of fintech innovation and regulatory accountability, leveraging technology to deliver seamless financial experiences across consumer and merchant segments in India.

Industry	Digital Finance / NBFC
Challenge	Securing proprietary platforms, scaling threat defense, achieving RBI-aligned compliance
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

As the company expanded its footprint nationwide, its cybersecurity team faced mounting pressure from multiple fronts:

Proprietary consumer and merchant platforms handling sensitive KYC and financial data	High-volume user interactions across mobile, cloud, and third-party integrations	Regulatory scrutiny under RBI guidelines, ISO 27001, and PCI DSS frameworks
Limited centralized visibility into threat activity and response	Accumulating security debt from rapid feature releases and agile development cycles	

The existing toolsets were fragmented, lacked exposure validation, and did not provide a measurable roadmap to proactive remediation or compliance tracking.

The Invinsense Solution

The company partnered with Infopercept to implement the full Invinsense cybersecurity stack, ensuring both operational resilience and regulatory alignment.

Invinsense XDR: Unified Detection & Response

Invinsense XDR integrated telemetry from the mobile app, cloud workloads, APIs, and user endpoints into a centralized detection and response layer—enriched with real-time threat intelligence.

Key Results:

- 57% reduction in threat containment time (from 14 hours to 6 hours)
- 66% drop in false positives due to contextual behavioral analytics
- 3x faster triage via automated case enrichment
- 81% detection coverage across MITRE ATT&CK, with custom rules for cloud and

Key Result

- 57% reduction in threat containment time
- 3.6x improvement in exposure validation through CTEM
- 91% compliance control coverage achieved across RBI & ISO frameworks
- 5x increase in attacker engagement via deception

Executive Insight

"Invinsense helped us shift from reactive detection to a continuous, validated approach to risk management. With exposure visibility, smart deception, and compliance automation in one platform, we've built security into the core of our growth and trust model."

Invinsense OXDR + CTEM Framework for Exposure Management

The OXDR module enabled the company to implement Continuous Threat Exposure Management (CTEM)—turning detection gaps into verified and prioritized action items.

Scoping	• Identified 2,800+ externally exposed assets, including cloud microservices, mobile APIs, and vendor connections • Discovered 31% more assets than previously documented, including test environments in production
Discovery	• Hybrid assessments revealed 212 high-risk exposures • 47% tied to weak configurations and logic flaws in customer onboarding and payment flows
Prioritization	• Business risk-based ranking led to the identification of 22 critical risks • These included misconfigured access controls and exposed APIs accepting unvalidated inputs
Validation	• Breach & Attack Simulations showed that 40% of identified issues could lead to PII or financial data compromise • 18 paths to compromise internal admin and reporting interfaces were uncovered
Mobilization	• Coordinated action between DevOps and Cloud teams patched 76% of critical risks in the first 30 days • Custom remediation playbooks accelerated collaboration and patch validation

CTEM Outcomes:

- 3.6x improvement in exposure validation
- 52% of validated issues neutralized before exploitation
- Reduced remediation cycle from 17 days to 6.5 days

Invinsense XDR+: Deception for Proactive Threat Detection

To combat sophisticated threat actors, the company deployed deception assets mimicking sensitive transaction flows and customer service workflows.

Results:

5x increase in attacker engagement through decoy services	Average attacker dwell time in decoys: 19 minutes	No real customer data impacted during threat investigations

Invinsense GSOS: Compliance Automation at Scale

With increasing compliance obligations from RBI, ISO, and PCI, the GSOS platform provided a unified control mapping, automation, and audit management framework.

Compliance Metrics:

91% coverage of controls across three major frameworks	89% automation of evidence collection and reporting	Internal audit readiness time dropped from 3 weeks to 4 days	Dashboards allowed real-time accountability across control owners

Quantifiable Impact

Category	Improvement
Threat Containment	↓ 57% (14h → 6h)
Exposure Validation Accuracy	↑ 3.6x
Critical Vulnerability Fix Time	↓ from 17 to 6.5 days
Deception Engagement	↑ 5x attacker interaction with decoys
Compliance Control Coverage	↑ 91% across RBI, PCI DSS, ISO 27001
Audit Prep Time	↓ from 21 days to 4 days

Conclusion

Digital finance players operating at national scale face the dual burden of innovation and regulation. By implementing Invinsense across detection, exposure management, deception, and compliance, this organization not only reduced its risk but transformed its security posture into a competitive advantage.

Infopercept | INVINSENSE

Imprint

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy