Enabling Secure Financial Development: How a Government-Backed Finance Institution Elevated Cyber Resilience and Regulatory Readiness with Invinsense

About the Customer

This government-backed financial institution plays a critical role in promoting and supporting the development of the micro, small, and medium enterprise (MSME) sector. Operating under parliamentary mandate, it provides funding and refinancing services through a network of banking and non-banking financial partners. The institution also facilitates credit guarantee programs and digital lending platforms that serve lakhs of small businesses across the country. With a mission rooted in economic empowerment and national financial inclusion, cybersecurity is essential to protecting public trust, national digital infrastructure, and compliance with evolving financial regulations.

Industry	Development Finance / Public Sector Banking
Challenge	Securing loan enablement platforms and regulatory compliance under RBI and national frameworks
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

As The institution faced mounting cybersecurity and governance pressures tied to its national role and expanding digital reach:

API and web app exposures across public-facing MSME portals and internal lending dashboards	Credential misuse and session hijacking attempts on partner onboarding interfaces	Visibility gaps across hybrid infrastructure supporting grant disbursement, credit assessments, and subsidy distribution
Regulatory obligations under the RBI cybersecurity circulars, CERT-IN guidelines, and national data protection initiatives	Limited validation of patching and control effectiveness across decentralized IT teams • Fraud risks tied to misuse of public funding disbursal mechanisms and subsidy pipelines	

The Invinsense Solution

The institution adopted Invinsense to consolidate threat visibility, reduce exposure, operationalize deception, and meet complex regulatory reporting demands across its public mission infrastructure.

Invinsense XDR: Full-Stack Detection for Lending & Refinance Workflows

XDR integrated data sources from lending APIs, government-facing web portals, citizen dashboards, and core decision engines.

Key Results:

- 69% faster detection of suspicious login behavior and privilege escalation
- 2.6-minute average detection time for privilege misuse anomalies
- 77% improvement in real-time alert correlation across subsidized loan disbursement flows
- Alert triage accuracy improved by 58% across operations and security teams

Invinsense OXDR + CTEM: Exposure Management for Critical Financial Infrastructure

CTEM methodology helped assess and reduce attack surfaces across applications, internal workflows, and mission-critical partner APIs.

Scoping	• Discovered over 6,300 digital assets spanning mobile loan apps, refinance APIs, and department-level portals • Identified dormant endpoints from legacy subsidy tracking systems
Discovery	• Surfaced 224 high-priority vulnerabilities across finance APIs, web form validators, and backend credit rule engines • Exposed inactive admin accounts with full access to audit and disbursal history
Prioritization	• Focused on business-critical risks such as fraudulent claim injection and fund redirection via backend APIs • Quantified attack paths tied to grant routing and PII leak potential
Validation	• Simulated credential escalation via misconfigured user roles • Emulated attacks targeting citizen KYC datasets and subsidy fraud paths
Mobilization	• Resolved 81% of validated exposures within 40 days • Integrated remediation insights into ITSM pipelines across regional teams

Key Result

- 69% faster detection of anomalous activity across digital portals
- 3.7x improvement in vulnerability validation cycles
- 91% coverage of required financial sector cybersecurity controls
- 5.3x increase in early threat identification using deception technology

Executive Insight

"Protecting national development programs requires more than good technology — it requires clarity, accountability, and cyber assurance. Invinsense helped us deliver all three at scale."

CTEM Impact:

- 3.7x faster validation of vulnerabilities
- 71% reduction in lateral movement opportunities across core finance systems
- Reduced average remediation cycle time by 59%

Invinsense XDR+: Deception for Fraud & Policy Abuse Detection

To proactively detect sophisticated fraud and insider manipulation attempts, decoys were deployed across subsidy workflows and internal decision dashboards.

Results:

5.3x increase in early-stage threat identification	Flagged misuse of form upload services mimicking actual KYC documentation	Isolated session hijacking bots targeting grant access credentials	Lowered false positives in fraud alerting by 63% with deception signal scoring

Invinsense GSOS: Regulatory Alignment for Public Sector Financial Systems

GSOS helped align control implementations across:

RBI Cybersecurity Framework for Regulated Entities	CERT-IN incident response and reporting guidelines	Internal audit checkpoints for grant, subsidy, and refinance workflows	Future-readiness for India's Digital Personal Data Protection (DPDP) Act

Compliance Outcomes:

91% control coverage across required RBI and CERT-IN domains	5x faster regulatory audit readiness across IT and data functions	Live dashboards for internal GRC teams tracking all control owners	Automated control mapping to mission-critical public platforms

Quantifiable Impact

Category	Improvement
Threat Detection Speed	↑ 69% faster
Vulnerability Validation	↑ 3.7x faster
Public Portal Exposure Remediation	↑ 59% faster
Deception-Driven Threat Intelligence	↑ 5.3x more accurate
Regulatory Framework Alignment	↑ 91% coverage (RBI, CERT-IN, internal audit)
Compliance Reporting Prep Time	↓ by 5x

Conclusion

For public institutions tasked with funding national growth, cybersecurity must be built for integrity and visibility — not just defense. Invinsense helped this customer reduce risk, accelerate trust, and deliver regulatory confidence across every touchpoint in their mission to empower businesses and citizens.

Infopercept | INVINSENSE

Imprint

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