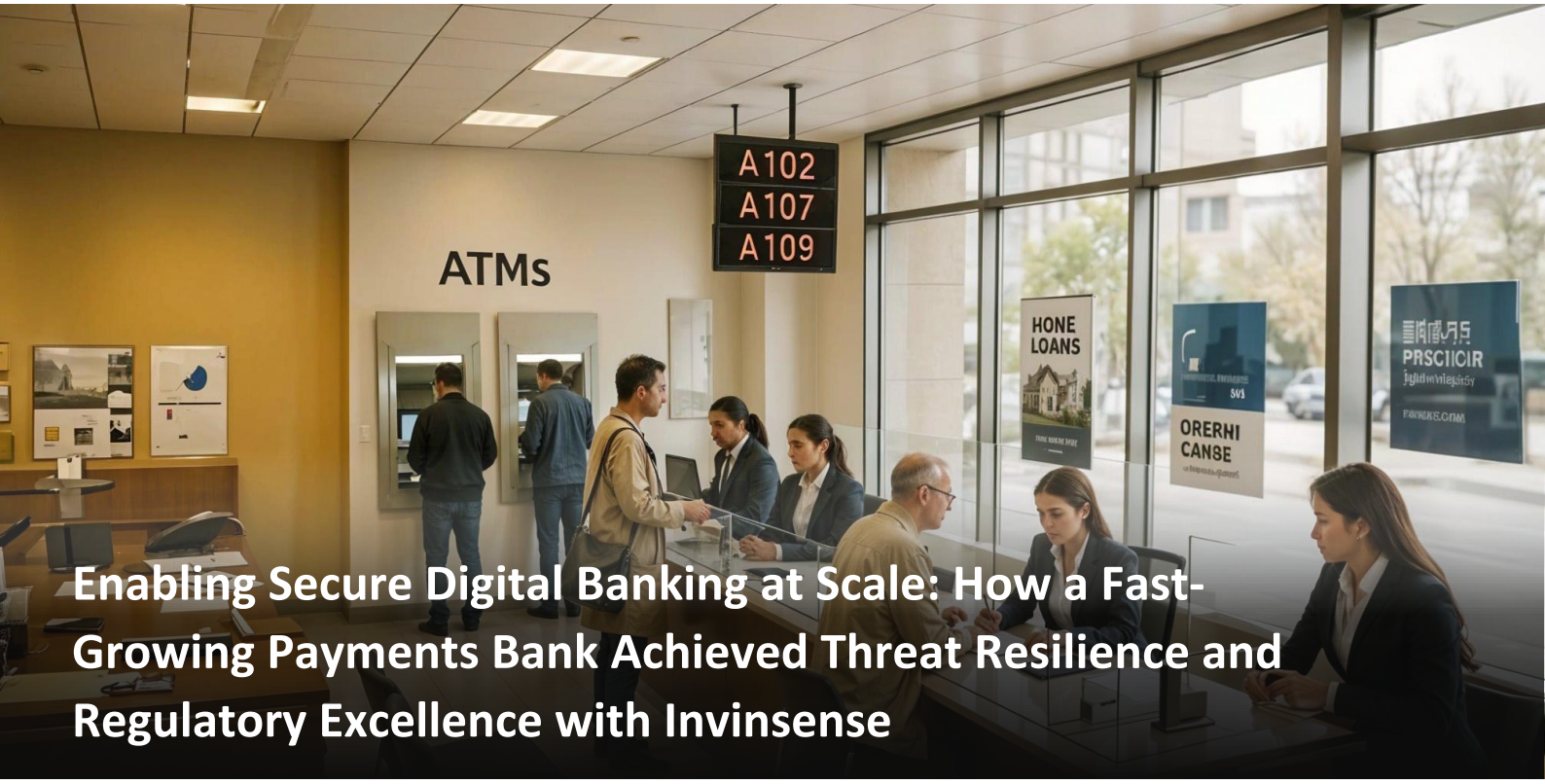

Enabling Secure Digital Banking at Scale: How a Fast-Growing Payments Bank Achieved Threat Resilience and Regulatory Excellence with Invinsense

About the Customer

This digital-first payments bank is part of a diversified business group and serves millions of customers across India with financial inclusion at its core. With offerings including savings accounts, domestic remittance, bill payments, and mobile banking, the bank leverages technology to deliver branchless, paperless, and secure banking services. Operating under strict regulatory oversight, the institution processes high-volume digital transactions across platforms like UPI, IMPS, and AePS, and relies heavily on mobile-first banking experiences.

Industry	Digital Banking / Payments Bank
Challenge	Real-time transaction security, and compliance with RBI & NPCI norms
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

As a regulated payments bank offering real-time digital services at national scale, the institution faced pressing challenges:

Protecting customer identity and biometric data integrated with Aadhaar	Maintaining compliance with RBI's IT framework, NPCI circulars, and internal audit standards	Limited visibility across hybrid environments, including mobile apps, third-party APIs, and core banking systems
Agility pressure from fast product rollouts (e.g., merchant app, agent onboarding platform) without full security validation	Lack of continuous risk posture tracking in a rapidly evolving threat landscape	

The Invinsense Solution

The bank deployed the full Invinsense cybersecurity suite to elevate security maturity, validate risks in real time, and automate compliance operations.

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:

- 71% drop in alert fatigue from false positives
- 87% rule match coverage across MITRE ATT&CK TTPs

Invinsense OXDR + CTEM for Continuous Risk Validation

To reduce unknown exposures and validate the effectiveness of controls, the bank operationalized the CTEM framework using OXDR.

Scoping	• Identified 3,400+ digital assets, including APIs in onboarding portals, agent KYC systems, and transaction processors • Shadow assets (old APK builds, test UPI environments) accounted for 22% of total attack surface
Discovery	• Discovered 185 high-impact vulnerabilities across cloud and internal assets • 39% of exposures linked to expired tokens, misconfigured access policies, or weak server-side validation
Prioritization	• Ranked 17 risks as critical to customer data and transaction integrity • Most critical: unsecured fallback APIs and insufficient access controls in agent management platform
Validation	• Simulated attacks validated 38 exploitable paths, including elevation via internal APIs • 21% of tested paths reached sensitive zones without triggering alerts in the prior setup
Mobilization	• Coordinated patching across IT and dev teams remediated 73% of issues in under 2 weeks • Custom SOAR playbooks triggered remediation workflows linked to internal ticketing systems

Key Result

- 4.1x improvement in validated exposure coverage
- 93% control alignment with RBI Master Directions
- 6x increase in early threat interception via deception

Executive Insight

"We operate in a world where digital trust is our currency. Invinsense gave us not just better visibility into threats, but the tools to act on them decisively—with proof of control across every audit checkpoint."

CTEM Metrics:

- 4.1x improvement in validated exposure insights
- 67% reduction in time to validate and patch
- 85% of validated risks neutralized within 15 days

Invinsense XDR+: Deception for Proactive Threat Hunting

Deceptive assets were deployed across the transaction layer to lure adversaries, credential stuffing attempts, and unauthorized admin access attempts.

Results:

6x increase in attacker engagement via merchant and customer decoys	71% detection of threats before reaching actual data stores	Deception helped isolate two previously undetected botnets targeting KYC APIs	Increased adversary dwell time to 24+ minutes, enabling full trace capture

Invinsense GSOS: Automated Regulatory Compliance and Audit Management

To keep pace with RBI Master Directions and NPCI mandates, GSOS enabled end-to-end compliance orchestration and audit readiness.

Compliance Outcomes:

93% alignment with RBI IT Framework controls	92% automation of policy control verification and reporting	Reduced internal audit preparation time from 18 days to just 5	Role-based dashboards enabled accountability for all control owners

Quantifiable Impact

Area	Improvement
Fraud Detection Speed	↑ 49% faster (Avg. 3.5 minutes detection)
Exposure Validation Accuracy	↑ 4.1x
Risk Remediation Time	↓ from 21 days to 9 days
Deception Engagement	↑ 6x attacker interaction with decoys
Regulatory Control Coverage	↑ 93%
Audit Prep Time	↓ from 18 to 5 days

Conclusion

As digital banks face rising pressure to balance real-time services with zero-trust expectations, this organization leveraged Invinsense to build a measurable, scalable, and regulator-ready cybersecurity foundation. The outcome: reduced risk, faster threat response, and deeper resilience across customer and infrastructure layers.

Infopercept | INVINSENSE

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

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