Fintech Firm Accelerates Threat Detection, Exposure Management, and Compliance Readiness with Invinsense

About the Customer

This fintech company serves as a digital bridge between borrowers and India's leading public and private sector banks. With a platform that enables loan approvals in under an hour, it simplifies access to financial services for MSMEs, individuals, and homebuyers. The firm has built strong partnerships with multiple financial institutions, offering loan products such as MSME loans, personal loans, home loans, and auto loans, with a focus on digitized document collection, AI-based risk profiling, and instant decisioning.

Given their scale, credibility, and commitment to transforming how credit is accessed in India, the organization must uphold strict application security standards and meet robust regulatory mandates from RBI and other financial regulators.

Industry	Fintech
Challenge	Application security & compliance complexity
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

This fast-scaling fintech platform faced increasing cybersecurity pressure. On one side, they needed to secure rapidly evolving APIs and cloud-native applications that interface with regulated banks. On the other, they had to maintain continuous compliance with frameworks like RBI cybersecurity guidelines, PCI DSS, and ISO 27001, while preparing for emerging obligations such as Real-Time Threat Reporting (RTRR).

With a lean internal security team and over a dozen disconnected tools, the CISO needed:

Unified security visibility	Threat exposure management	Compliance mapping and enforcement

The Invinsense Solution

The fintech firm selected Invinsense as its strategic security partner, deploying the platform's full stack across four core modules:

Invinsense XDR

- Integrated SIEM, SOAR, EDR, and threat intelligence into a unified detection and response engine.
- Correlated logs from application layer, API gateway, and infrastructure.

Impact:

- 63% faster mean time to detect and respond (MTTD/MTTR)
- 78% MITRE ATT&CK technique coverage across kill chain
- 41% reduction in alert fatigue using case management automation

Invinsense OXDR & CTEM Execution

Through the Continuous Threat Exposure Management (CTEM) methodology, the firm moved beyond detection toward continuous validation and remediation of exposures:

Scoping	• OXDR mapped all externally exposed assets, shadow APIs, and code vulnerabilities. • Discovered 27% more assets than previously known.
Discovery	• Automated vulnerability scans combined with manual red teaming revealed 164 exploitable paths. • 52% of critical findings were unknown to prior tools.
Prioritization	• Risk scores calibrated using business context, customer data sensitivity, and exploitability. • Helped prioritize the top 11 vulnerabilities impacting the firm's core banking API integrations.
Validation	• Breach & Attack Simulation (BAS) and CART validated real-world exploit paths. • 38% of detected issues were proven exploitable within 2–5 steps of privilege escalation.
Mobilization	• Purple team worked alongside developers and DevSecOps to remediate gaps. • 89% of critical exposures closed within 30 days using remediation playbooks and patching pipelines.

Invinsense XDR+ Deception Deployment

- Custom deception environments mimicking UPI endpoints and fake banking APIs were deployed.
- Created multiple honeynets to lure threat actors away from production.

Results:

4x improvement in lateral movement detection accuracy	36% increase in early-stage threat visibility pre-exploitation)	0 false positives from deception-based alerts over 90 days

Key Result

- 63% faster detection-to-response cycle
- 72% reduction in attack surface exposures
- 87% improvement in compliance readiness across RBI, PCI DSS, and ISO 27001
- 4x increase in threat detection accuracy using deception technology

What Their CISO Said

"Invinsense didn't just help us respond to threats — it helped us see what we didn't know we were exposed to, then close the loop. From red teaming to patching to compliance, we now run a security program built for clarity, speed, and accountability."

Overall CTEM Outcome:

- 72% reduction in validated exposures across internet-facing applications
- 3x faster time-to-remediation for critical flaws
- 95% of validated attack paths neutralized within first 45 days

Invinsense GSOS for Compliance Automation

Mapped compliance needs across:

RBI Cybersecurity Framework (2023)	PCI DSS 4.0	ISO/IEC 27001:2022

GSOS streamlined evidence collection, task ownership, audit documentation, and GRC alignment.

Compliance Readiness Outcomes:

87% faster internal audit preparation	92% coverage of RBI & PCI DSS controls mapped automatically	100% visibility on control ownership, reducing audit friction

The Results

Metric	Improvement
Mean Time to Detect & Respond	↓ 63%
Alert Fatigue	↓ 41%
Exposure Reduction (CTEM)	↓ 72%
Threat Detection Accuracy (Deception)	↑ 4x
Time-to-Remediate Critical Flaws	↓ 3x
Internal Audit Preparation Time	↓ 87%

Why It Matters

For fintechs juggling innovation with regulation, exposure management is the next evolution of cybersecurity. With Invinsense, this firm achieved visibility, validation, and verified compliance — not just checkboxes, but confidence.

Infopercept | INVINSENSE

Imprint

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