Case Study: Securing a Shariah-Compliant Finance Provider's Digital Ecosystem with Invinsense

About the Customer

The customer is a Shariah-compliant financial services provider that offers financing solutions aligned with Islamic banking principles. Focused on empowering individuals and SMEs, the organization leverages digital platforms to deliver streamlined financing services in compliance with ethical and religious values. Their operations span across loan origination portals, credit evaluation engines, customer service systems, and cloud-based financial management applications.

The Challenge

Operating in a tightly regulated financial environment, the customer faced the dual challenge of aligning with Islamic finance regulations while ensuring compliance with regional cybersecurity mandates such as the SAMA Cybersecurity Framework. Their increasing dependence on digital workflows made them susceptible to cyber threats that could disrupt trust and compliance.

Key challenges included:

Securing digital lending portals and customer onboarding systems from fraud and credential abuse.	Ensuring data integrity and confidentiality across cloud-hosted financial apps.	Protecting API endpoints from automated and targeted attacks.
Achieving visibility across hybrid infrastructure spanning on-premise and cloud.	Demonstrating ongoing compliance with Shariah and SAMA cybersecurity controls.	Responding to incidents quickly without a fully mature internal SOC.

Deception Outcomes with Invinsense XDR+

- Deployed decoys in cloud environments and admin interfaces.
- Detected 6 unauthorized access attempts through credential harvesting traps.
- Cut down potential dwell time of attackers by 78% through early alerting.

Compliance Enablement with Invinsense GSOS

- Mapped SAMA cybersecurity framework controls to technical assets.
- Automated evidence collection reduced internal compliance effort by 42%.
- Enabled centralized reporting for Shariah-compliant IT governance.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Identified 290+ potential exposure points, primarily in APIs and cloud-hosted loan origination tools.
Discovery	Mapped backend systems and found 22 instances of over-permissioned accounts.
Prioritization	Flagged 30 critical exposures with potential for financial fraud or system downtime.
Validation	Simulated adversarial attacks leading to the discovery of 5 high-risk misconfigurations.
Mobilization	Achieved closure of 85% of critical issues within 10 days through automated and manual patching.

Executive Quote

"Invinsense has helped us not only meet cybersecurity mandates but also build digital trust in line with our ethical finance values. Their continuous exposure management and deception technologies are game-changers."

– Head of IT & Compliance, Shariah-Compliant Finance Institution

Solutions Used

- Invinsense XDR for unified monitoring of threats across endpoints, identity infrastructure, and cloud applications.
- Invinsense XDR+ for deploying deception layers within the lending environment to catch unauthorized movements early.
- Invinsense OXDR for proactive exposure management across APIs, cloud services, and internet-facing apps.
- Invinsense GSOS to track cybersecurity governance, risk, and compliance requirements including alignment with the SAMA Cybersecurity Framework.
- Collaboration with Infopercept's security experts for continuous monitoring and manual patching of high-risk exposures.

Key Results

- 61% reduction in overall digital attack surface across loan and finance platforms.
- 4.2x improvement in detection and response time.
- Zero critical misconfigurations reported in the last two compliance audits.
- Compliance readiness with SAMA achieved within 90 days.
- 85% automation in remediation across cloud and API layers.
- Early-stage threats detected through deception, stopping 6 real-world intrusion attempts

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.

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