One Sovereign AI Framework for Secure, Intelligent, and Resilient Financial Operations

Correlating every signal across operations, security, and AI so financial services stay always-on and under sovereign control.

Sovereign AI Infrastructure | Observability | Application Performance Monitoring | AIOps | SIEM++ | AI Governance

EXECUTIVE OVERVIEW

Secure, Intelligent, Resilient Operations

Every transaction depends on applications, APIs, infrastructure, identities, third parties, and increasingly AI models and agents working together. When those layers are monitored, secured, and governed in separate tools, alerts sit in silos and teams respond without shared context.

Why Sovereign AI Matters

Institutions want AI that runs on infrastructure they control, keeps data within defined jurisdictions, and records every model and agent action for audit. Sovereign AI makes this control part of the architecture, rather than a compliance layer added after deployment.

iStreet's Unified Approach

Sovereign AI infrastructure, monitoring, APM, AIOps, SIEM++, and AI governance come together as one connected BFSI framework. Operations, security, and risk teams work from the same data, context, and service view — within a data-resident, institution-controlled environment.

THE CHANGING BFSI TECHNOLOGY LANDSCAPE

Digital transaction growth

Real-time payments, mobile banking, and digital lending have made transaction availability a direct measure of customer trust. Every second of degradation is visible to customers.

Hybrid and multicloud complexity

Core systems on-premises, digital channels in private and public clouds, and partner services over APIs create dependencies no single team can trace manually.

Expanding cyber-risk landscape

Identities, endpoints, applications, APIs, and third-party connections each widen the area that security teams must observe, correlate, and defend.

Growing AI governance requirements

As AI enters credit, fraud, service, and operations workflows, institutions need visibility into how models and agents behave and who remains accountable. Data localization makes sovereign AI a design requirement.

UNIFIED BFSI SOLUTION FRAMEWORK

Sanjeevani of AI™

Sanjeevani of AI™ is iStreet's sovereign infrastructure and intelligence framework that keeps enterprise AI compliant, observable, and always-on. It is the connected framework within which every BFSI capability operates.

Integrated architecture across operations, security, and governance

Monitoring, APM, AIOps, and SIEM++ share one telemetry foundation, with AI governance applied to that intelligence layer. A performance anomaly, a security event, and a policy exception can be viewed as parts of the same incident.

Sovereign control across data, infrastructure, and AI

Models, analytics, and agents run within the institution's chosen environment. Institutions retain control over where data is stored, how intelligence is applied, and how AI decisions are recorded and reviewed.

SOLUTIONS

01

End-to-End Monitoring and Observability

A continuous, service-level view of the technology that supports every financial transaction.

Infrastructure, network, application, and database monitoring — health and capacity visibility across servers, storage, network devices, virtualized and containerized workloads, and databases.

Business transaction monitoring — tracking of payments, transfers, policy issuance, and loan journeys from initiation to completion.

Unified telemetry and service visibility — metrics, events, logs, and traces brought into one model and mapped to the business services they support.

Real-time operational dashboards — role-specific views for command centres, application owners, and leadership.

02

Application Performance Monitoring

Visibility into how applications and APIs perform for every customer and partner.

Application and API performance visibility — response times, error rates, and throughput across digital channels and integration layers.

Service dependency mapping — automatically discovered relationships between applications, APIs, and infrastructure.

Transaction tracing — end-to-end tracing across microservices, middleware, and core systems.

User-experience monitoring — insight into the digital experience delivered across web and mobile channels.

03

AIOps for Operational Resilience

Intelligence that helps operations teams move from reacting to events to anticipating them, with AI models running on sovereign infrastructure.

Behavioural baselining and anomaly detection — learned patterns of normal behaviour that account for business cycles such as month-end, salary days, and festive peaks.

Root-cause analysis — probable cause identified across application, infrastructure, and change data.

Event correlation and alert-noise reduction — related alerts grouped into a single, actionable incident.

Predictive incident detection — early indicators of degradation raised before customers are affected.

04

SIEM++ for AI-Native Security Operations

Security operations designed for the scale and speed of digital finance, with telemetry and AI-driven analytics retained within sovereign, data-resident infrastructure.

Unified security telemetry — security data from across the institution collected and normalized in one platform.

Identity, endpoint, application, and network correlation — connected context that reveals multi-stage threats.

Threat and behavioural analytics — detection of anomalous activity by users, entities, and systems.

Risk-based vulnerability management — vulnerabilities prioritized by exploitability, asset criticality, and business impact.

05

AI Governance and Guardrails

Structured oversight for AI models and agents across their full lifecycle — the governance layer of iStreet's sovereign AI framework.

Sovereign AI boundaries — models, agents, and their data kept within approved infrastructure and jurisdictions.

Explainability and decision traceability — recorded reasoning and evidence for AI-assisted decisions.

Data, model, and agent governance — policies applied to training data, model behaviour, and agent actions.

Access, action, and execution guardrails — defined limits on what AI systems can access and execute.

06

Connected Operations Across IT, Security, and AI

The value of the framework lies in how its capabilities work together.

Unified operational context — one shared view of services, assets, identities, and AI systems.

Shared risk and service intelligence — operations and security teams prioritize by the same measure of business impact.

Cross-domain incident correlation — a performance drop, a suspicious login, and an AI policy exception recognized as one event where related.

Coordinated response workflows — IT, security, and governance teams act on one incident record, with clear ownership.

PRIORITY BFSI USE CASES

USE CASE	HOW ISTREET HELPS
Digital banking and payment-service availability	Monitors payment rails, channels, and APIs end to end, with early warning of degradation.
Core banking application performance	Traces transactions through core systems and identifies bottlenecks before batch and peak windows.
Fraud and transaction-risk monitoring	Correlates transaction behaviour with identity and security signals for faster risk decisions.
Third-party and API risk visibility	Tracks partner and API performance, availability, and security exposure.
Governed deployment of AI agents	Applies guardrails, oversight, and traceability to agents operating in financial workflows, on sovereign AI infrastructure.

REFERENCE ARCHITECTURE

Dashboards, workflows, and automation
Role-based dashboards, incident workflows, and governed automation.

Monitoring, security, and governance controls
Observability, SIEM++, risk-based vulnerability management, and AI guardrails on the same intelligence.

Intelligence and correlation layer
AI-driven baselining, correlation, analytics, and root-cause intelligence.

Data and telemetry ingestion
Metrics, logs, traces, events, security data, and AI activity from across the estate.

Sovereign AI infrastructure foundation
Data-resident compute, storage, and AI runtime in the institution's chosen environment.

INTEGRATION WITH EXISTING ENTERPRISE TOOLS

DEPLOYMENT AND SOVEREIGNTY

Sovereign AI runtime — models and agents run on infrastructure the institution controls, with no dependency on external AI processing.

On-premises, private cloud, and hybrid deployment — deployment models chosen to match regulatory and operational requirements.

Role-based access and auditability — granular permissions and complete audit trails for every user and system action.

Scalability and integration model — an architecture that grows with transaction volumes and connects with the existing landscape.

WHY ISTREET NETWORK

India-rooted and AI-native
Conceived in Bharat, with deep understanding of the Indian regulatory and financial landscape.

Unified operations, security, and governance
One connected framework in place of disconnected tools.

Enterprise-grade architecture
Built to take AI and operations from pilot to production at institutional scale.

Sovereign AI, control at every layer
Data-resident by architecture, with control retained across data, infrastructure, and AI.

BUSINESS AND OPERATIONAL OUTCOMES

Improved service availability
Customers experience consistent access to digital financial services.

Faster detection and resolution
Teams identify and resolve issues with shared context.

Reduced alert fatigue
Correlated incidents replace fragmented alert streams.

Stronger cyber resilience
Threats are detected and addressed with connected intelligence.

Governed, explainable AI adoption
AI moves into production with traceability and oversight.

Sovereign control over data and AI
Data, models, and decisions remain within the institution's jurisdiction.

Continuous operational control
Leadership retains ongoing visibility across operations, security, and AI.

One framework, one context
Operations, security, and risk work from a single service view.

Shape the Next Phase of Your Operations with iStreet

iStreet Network Limited (BSE: 524622) is a Sovereign AI-native platform ecosystem. Its Sanjeevani of AI™ gives financial institutions one complete, sovereign framework for operations, security, and AI governance. It covers every layer from data and infrastructure to intelligence and oversight, under the institution's own control.

Schedule a BFSI solution briefing

STREET
Sanjeevani of AI™

contact@istreetnetwork.com · istreetnetwork.com
4-A Wing, D J House, Old Nagardas Road, Andheri East, Mumbai 400069