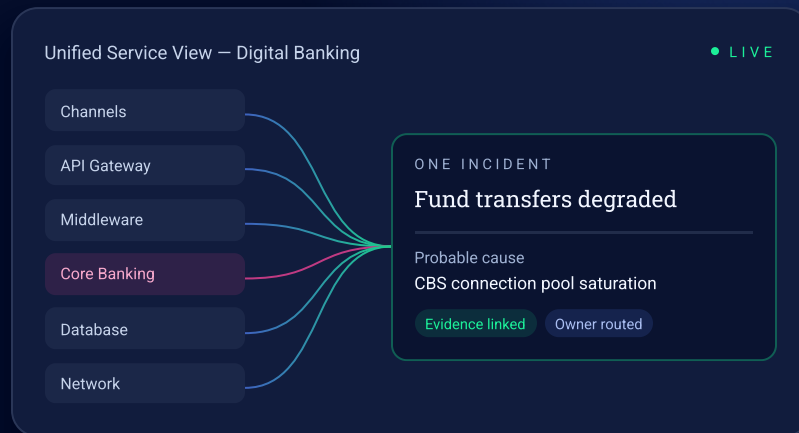


— AIOps FOR BANKING

From Monitoring to Understanding Faster

Unified observability and AI-assisted root cause analysis for modern banking operations.

● AIOps Solution by iStreet Network



What This Ebook Covers

The gap is not in data collection. It is in connection.

03	Executive summary	10	Transaction-centric observability
04	Why unified observability matters	11	AI-assisted root cause analysis
05	What a unified view should deliver	12	From technical to business-impact RCA
06	A practical architecture	13	From RCA to remediation
07	Building the telemetry foundation	14	Predictive operations
08	Real-time analytics	15	The Resilience Operations Centre
09	Cross-domain correlation	16	Conclusion and next steps

Banks do not lack monitoring data. They lack a connected understanding of it.

Digital banking runs on a deep chain of dependencies, each monitored by a different tool and a different team. When an incident occurs, the evidence is scattered, and the time taken to assemble it becomes the largest part of the outage.

A consolidated operational view with AI-assisted root cause analysis changes that, through four capabilities working together:

01

Real-time analytics

Detect abnormal behaviour as it emerges

02

Cross-domain correlation

Connect signals across every technology layer

03

Predictive insights

Identify service risk before customers are affected

04

Automated operations

Carry a diagnosis through to remediation

Operational resilience

Shorter incidents, fewer repeat failures, and continuity of digital services.

Why Unified Observability Matters for Modern Banking

WHY UNIFIED OBSERVABILITY MATTERS

- A single payment or login crosses channels, API gateways, middleware, core banking, databases, switches, and external networks.
- Application, infrastructure, network, and database teams each rely on their own tools, each raising its own alerts.
- During an incident, teams gather in a war room and compare screens to establish which signal matters.
- Root cause analysis depends on the experience of a few individuals, and the same incidents return.
- Customers expect continuous availability, and regulatory expectations on downtime and incident reporting continue to tighten.

CUSTOMER SERVICE

UPI payment — is it healthy?

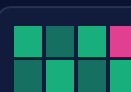
?



APM
App team



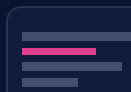
Infra
Infra team



NPM
Network team



DB
DBA team



Logs
Ops team

The gap is not in data collection. It is in connection.

What a Unified Operational View Should Really Deliver

A unified view should answer five questions within minutes:

What is happening?	Which services and transactions are behaving abnormally.
Where?	Which layer and component the behaviour originates from.
Why?	The probable root cause, with evidence.
Who is affected?	Customers, channels, and journeys.
What next?	The recommended or automated remediation.

AGGREGATION



CONSOLIDATION

Mobile fund transfer

Incident · degraded

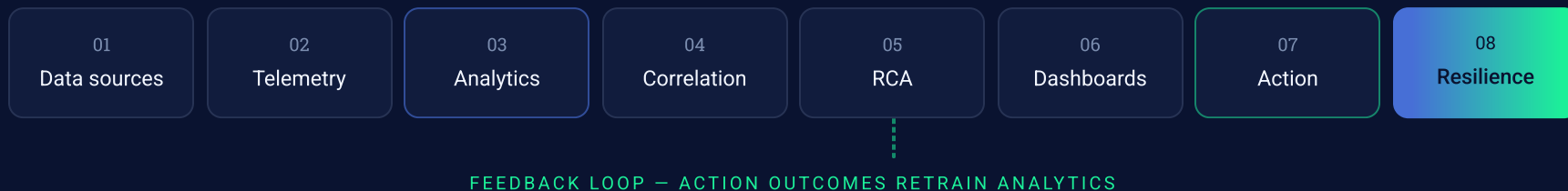
Cause: DB pool · Impact: mobile users

ONE SOURCE OF TRUTH, PRESENTED FOR EACH ROLE

NOC	Live incidents, correlated alerts, service health
App & infra teams	Anomalies, traces, probable cause evidence
Service owners	Health of their business service and its dependencies
CXOs	Availability, business impact, resilience trends

A Practical Architecture for AI-Assisted Banking Operations

One continuous flow from signal to resilience.



DESIGN PRINCIPLES FOR BANKING ENVIRONMENTS

Integrate, do not replace

Existing monitoring tools become data sources.

Vendor-neutral by design

Open standards prevent dependence on a single tool.

Deployment control

On-premises, private cloud, and hybrid options that respect data residency.

Explainable intelligence

Every AI conclusion is traceable to its evidence.

Root Cause Analysis Is Only as Complete as the Telemetry Beneath It

Metrics	How services perform over time
Events	What changed, and when
Logs	What the system recorded
Traces	How a request travelled across services
Packet data	What happened on the network
Topology	How components depend on one another
Business context	Which service and customer journey is involved

Mainframe / CBS

Packaged apps

Cloud-native

Network devices

Existing tools

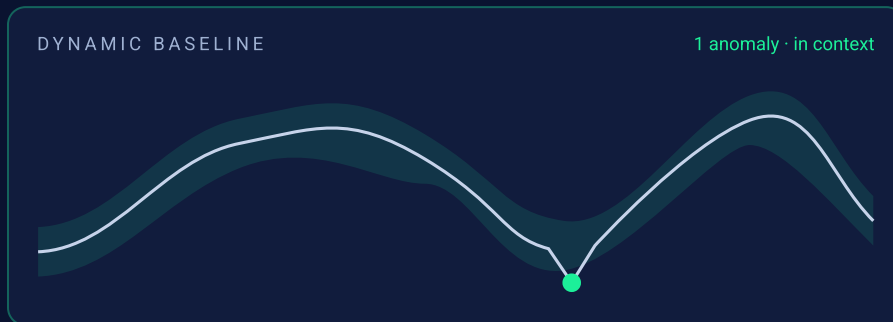
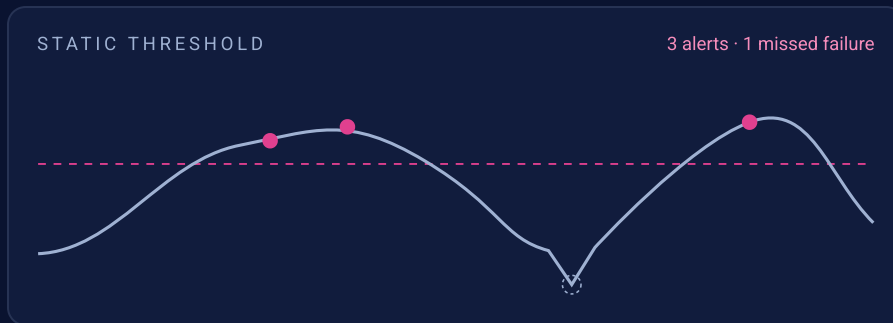
COLLECTOR
OpenTelemetryONE
Unified data layer

OpenTelemetry provides a common, open standard for collecting this data across legacy, packaged, and cloud-native systems — giving the bank portability of its own telemetry and freedom from vendor-specific agents.

A Fixed Threshold Cannot Describe a System Whose Normal Changes by the Hour

- Banking workloads follow patterns: salary days, month-end, festive peaks, batch windows.
- Static thresholds raise alerts through every peak and stay silent during a quiet-hour failure.
- Dynamic baselines learn expected behaviour by time of day, day of week, and business cycle.
- Real-time analytics evaluate streaming data continuously against those baselines.
- Anomaly detection identifies deviations in context, across metrics, logs, and transactions together.

Fewer alerts, raised earlier, with higher confidence.



One Underlying Fault Can Raise Hundreds of Alerts. Operators Need One Incident.



Service topology

Maps how applications, services, databases, hosts, and network paths deliver each business service — discovered and refreshed automatically.

Cross-domain correlation

By time (they occurred together), topology (they share a dependency path), and pattern (they have occurred together before).

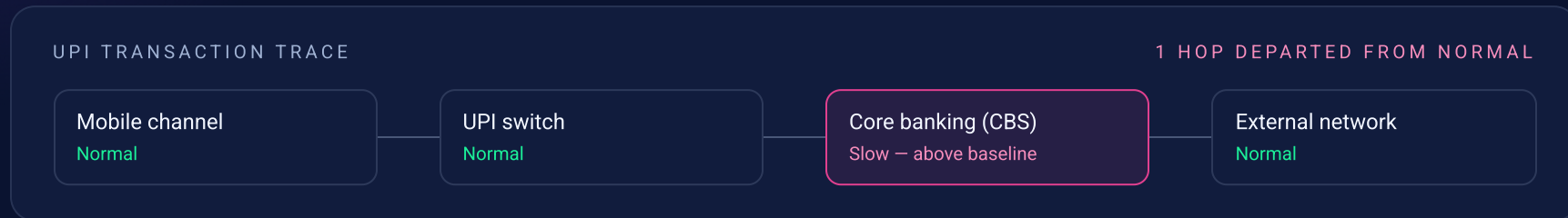
One incident, full context

Related alerts from application, network, infrastructure, and database layers consolidate into a single incident.

Less noise

Symptomatic and duplicate alerts are reduced, so attention goes to the originating condition.

Customers Do Not Experience Servers. They Experience **Transactions**.



Component health can be green while customers are unable to complete a payment.

Transaction-centric observability follows each journey end to end: success, failure, and response time at every hop.

Each hop links to its underlying components, so a rise in failures points directly to where behaviour departed from normal.

JOURNEYS TO OBSERVE

UPI & IMPS

NEFT & RTGS

Internet & mobile banking

Card authorisation

Core banking postings

Partner API calls

Root Cause Analysis Becomes a Matter of Evidence, Not Recollection

AI-assisted RCA combines anomalies, topology, correlated signals, change data, and historical patterns to produce a ranked list of probable root causes — each with supporting evidence and a confidence level.

- **Explainable.** Operators inspect, confirm, or reject each conclusion; the evidence trail supports post-incident reporting.
- **GenAI investigation.** Natural-language queries, incident summaries, recommended actions, and conversational dashboards — grounded in the bank's own operational data.

Anomalies

Topology

Correlated signals

Change data

Historical patterns

PROBABLE ROOT CAUSES — RANKED

1	DB connection pool saturation Config change 14:02 · 4 evidence links	
2	Middleware thread exhaustion 2 evidence links	
3	Network packet loss, DC-2 1 evidence link	

ASK OPERATIONS

Why are mobile fund transfers slow?

Most likely cause: connection pool saturation on a CBS database node after the 14:02 change. Recommended action: restore pool size.

The intent is not to remove expertise from RCA, but to make it available to every shift, every time.

A Root Cause Is Not Fully Understood Until Its Business Impact Is Known

Technical RCA answers what failed. Business-impact RCA answers what it meant.

SERVICES

Which were degraded or unavailable

TRANSACTIONS

Which, how many, and for how long

CUSTOMERS & CHANNELS

Mobile, internet banking, ATM, partner APIs

JOURNEYS

Payments, onboarding, lending, servicing

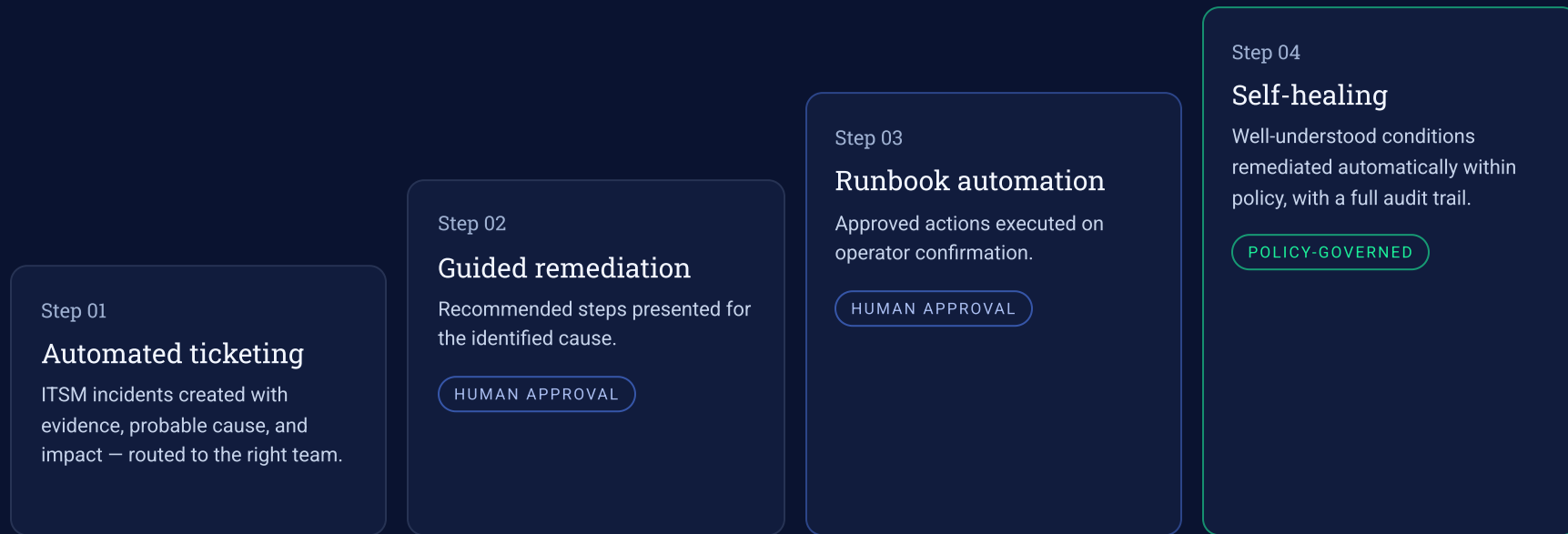
TECHNICAL STATEMENT

Connection pool saturation on a database node

BUSINESS-IMPACT STATEMENT

Fund transfers through mobile banking degraded for **few minutes**; transactions delayed

Diagnosis Has Value Only When It Leads to Action



Automation is extended as confidence is established, and human approval remains for actions with material risk.

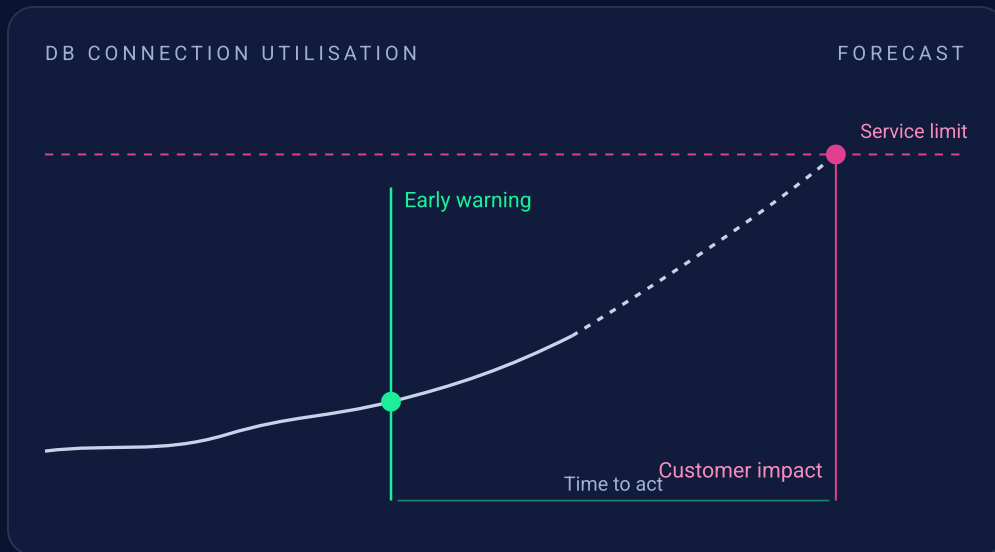
The Most Valuable Incident Is the One That Does Not Occur

Early-warning signals. Gradual deviations identified before they breach service levels.

Capacity forecasting. Demand projected against salary days, festive peaks, and month-end.

Anomaly trends. Recurring low-level anomalies recognised as indicators of an underlying condition.

Service risk scoring. A forward-looking view of each critical service, not only its current status.



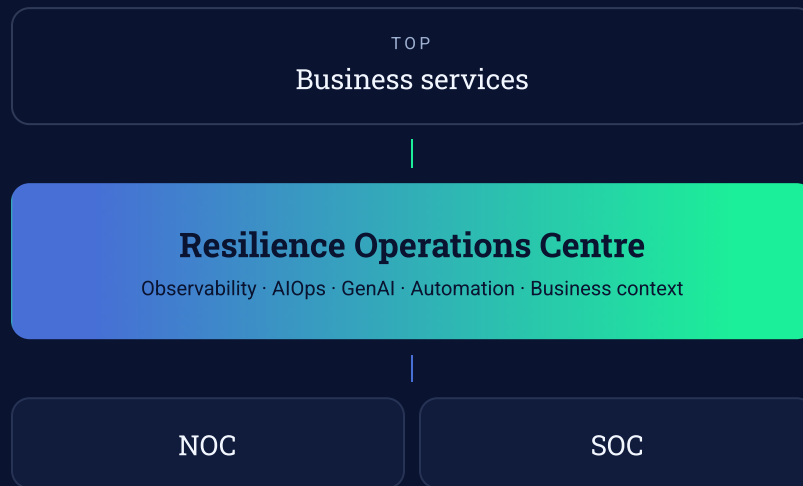
Predictive insights move operations from responding to incidents towards preventing them.

The Measure of Success Is Not More Data. It Is Continuity of Service.

OUTCOMES TO MEASURE



The Resilience Operations Centre (ROC) is an AI-powered convergence layer above the NOC and SOC — bringing observability, AIOps, GenAI, automation, and business context into one framework.



The question changes from "is each system running" to "is the bank's service resilient".

— CONCLUSION AND NEXT STEPS

From Monitoring More to **Understanding Faster**

The next advance in banking operations comes from understanding technology as one connected service: analysing in real time, correlating across domains, identifying root cause with evidence, anticipating failure, and acting with confidence.

AIOps Solution by iStreet Network delivers this in a single consolidated view with AI-assisted root cause analysis.

[Book a Resilience Assessment →](#)