iOPEX

FinTech

North America

Global FinTech Leader Optimizes Observability License Costs by 30% with Autonomous SOC

For a global FinTech leader running one of the most complex SOC environments in financial services, iOPEX unlocked an Autonomous SOC that turned weeks of data onboarding into minutes, enabling the infrastructure performance to manage itself.

Highlights

- Exponential growth in machine data ingestion across legacy, streaming, and multi-cloud environments was overwhelming platform capacity, inflating license costs, and degrading SOC performance.
- iOPEX delivered a three-phase Autonomous SOC combining DevRPA-driven onboarding, AI/ML-powered smart filtering, and continuous autonomous governance.
- The transformation lowered license utilization by 30%, reduced onboarding from weeks to minutes, and delivered zero-lag system performance across the SOC environment.

Business Challenge

The client operated one of the most complex enterprise observability environments in financial technology. Daily machine data ingestion was growing exponentially across cloud-native applications, real-time streaming infrastructure, and legacy systems of record. Traditional monitoring approaches were buckling under that scale — driving up cost, slowing the SOC, and consuming the engineering capacity needed for proactive security work.

Escalating License Costs Outpacing Visibility Gains

The observability platform's licensing model was tied to daily ingest volume, but a significant share of that ingest added little to threat investigation or compliance posture. Costs climbed without a matching improvement in security insight.

Search Latency Slowing Threat Response Heavy

Indexing loads were stretching query response times across the SOC. Slow searches delayed investigations, lengthened mean time to detect and respond, and reduced analyst effectiveness in exactly the moments speed mattered most.

Skilled Engineers Stuck in Repetitive Work

Engineering capacity was absorbed in manually deploying forwarders, validating sourcetype mappings, troubleshooting ingestion bottlenecks, and monitoring platform health. Strategic detection engineering and proactive threat hunting were chronically deprioritized as a result.

Fragmented Visibility Across Environments

Without a unified data framework spanning proprietary systems, Kafka topics, Kubernetes workloads, and cloud-native infrastructure, normalization gaps fragmented cross-environment search. Correlation across data sources was inconsistent, and operational intelligence lagged the events it was meant to surface.

iOPEX Solution – FieldPilot

iOPEX designed a three-phase Autonomous SOC framework — intelligent onboarding, AI/ML-driven optimization, and proactive governance — that converted a high-friction observability environment into a self-regulating one.

Phase 1 — Intelligent Data Onboarding

Outcome: Onboarding compressed from weeks to minutes, with engineering effort virtually eliminated.

iOPEX established a unified enterprise data fabric to standardize ingestion across distributed environments. DevRPA workflows automated Universal Forwarder deployment, configuration, and validation across endpoints — collapsing work that had previously required hands-on engineering for every new source. Real-time pipelines onboarded Kafka topics and Kubernetes log streams directly into the platform, and a Common Information Model (CIM) framework normalized incoming events so they were immediately searchable and correlatable across environments.

Key Capabilities Delivered

- Automated forwarder deployment, configuration, and health validation across distributed infrastructure
- Real-time onboarding pipelines for Kafka and Kubernetes
- CIM-based normalization for unified search, correlation, and detection content
- Engineering hours redirected from onboarding plumbing to detection and threat work

Phase 2 — AI/ML-Driven Intelligent Optimization

Outcome: 30% reduction in license utilization with no compromise to security visibility or compliance coverage.

To attack escalating license costs at the root, iOPEX deployed AI/ML-powered Smart Filtering at the Heavy Forwarder layer — the point in the pipeline where filtering reduces both license consumption and downstream indexing load. Machine learning models continuously analyzed ingestion patterns to classify events by operational and security value: repetitive debug output, low-cardinality heartbeats, and non-critical verbose telemetry were routed away from indexing, while security-relevant, audit-relevant, and operationally meaningful events flowed through untouched. Filtering rules adapted dynamically as event patterns and source behavior shifted.

Key Capabilities Delivered

- AI/ML classification of events by operational and security value
- Dynamic, adaptive filtering rules at the Heavy Forwarder layer
- Indexing capacity preserved for high-signal, high-value data
- Cost-performance balance restored without visibility tradeoffs

Phase 3 — Autonomous Governance and Performance Rebalancing

Outcome: Zero-lag SOC performance, with platform health managed without human intervention.

A Continuous Health Monitoring framework tracked indexer load, queue depth, ingestion throughput, search concurrency, and cluster health in real time. When indexing spikes, search contention, or workload imbalances were detected, DevRPA-driven remediation workflows automatically rebalanced data distribution.

Key Capabilities Delivered

- Real-time telemetry on indexer load, queue depth, and search performance
- Automated remediation workflows for cluster rebalancing
- Autonomous reallocation of indexing traffic during peak demand
- Continuous, zero-lag operational performance management

The Impact

Outcomes spanned operational, financial, and infrastructure dimensions.

30% Lower License Utilization

- AI/ML filtering removed repetitive low-signal logs before they reached indexing
- Observability efficiency improved with no compromise to threat visibility, compliance, or audit
- License costs decoupled from raw data volume growth

100% Unified Platform Visibility

- Coverage extended across legacy systems, Kafka streams, Kubernetes, and multi-cloud
- Unified operational intelligence across AWS, Azure, Kubernetes, Kafka, and mainframe
- Cross-platform searchability, correlation, and consistency restored across the SOC

Autonomous, Zero-Lag SOC Performance

- Reactive troubleshooting replaced with continuous autonomous governance
- Indexing latency, queue depth, and infrastructure performance monitored in real time
- Automated rebalancing kept search performance stable through peak load and event spikes

Onboarding Compressed from Weeks to Minutes

- RPA-driven automation collapsed onboarding across distributed infrastructure
- Kafka and Kubernetes streams ingested and normalized in real time
- Manual onboarding dependencies eliminated across the environment

About iOPEX

iOPEX Technologies is a new-generation agentic AI and automation-led enterprise transformation partner headquartered in San Jose, California. At the intersection of enterprise operations, agentic AI, and intelligent automation, we deliver Intelligence as a Service. Over 70 global brands trust iOPEX as a strategic partner to turn AI into results that scale. We help clients accelerate enterprise transformation without endless consulting cycles by embedding intelligence directly into workflows. Contact us at www.iopex.com.