OCIENT FOR NETWORK INTELLIGENCE

Hyperscale Analytics for Internet Connection Records

Networks generate trillions of Internet Connection Records (ICR) every day. Extracting intelligence from this much metadata requires infrastructure purpose-built for hyperscale ingest, storage, and analytics. Ocient National Security Solutions for Network Intelligence turn massive ICR telemetry into actionable insight for cybersecurity, counterterrorism, and digital forensics.

Designated Awardable in the DoW CDAO Tradewinds Marketplace

List of Federal Contracts Available on Request

The National-Scale Data Challenge

Security organizations must analyze trillions of network records while retaining years of history. Traditional platforms cannot keep pace—especially as encryption grows and malicious activity hides within vast volumes of normal traffic—creating delays and intelligence blind spots.

Ocient Network Intelligence Solutions

Ocient delivers a unified analytics platform engineered for ultra-high volume metadata workloads including ICR. Key capabilities include:

- **Hyperscale Ingest**
  Trillion-record-per-minute potential
- **Multi-Year Retention**
  ~10:1 compression enables cost-efficient long-term storage
- **Interactive Analytics**
  Queries across trillons of current and historical records in seconds
- **Unified Architecture**
  Ingest, transform, store, and analyze on a single platform

Representative National ICR Workloads

United States

Processing ~8.7T ICR per day, national and commercial networks must correlate activity across dozens of ISPs to identify nation-state campaigns and large-scale cyber threats.

Malaysia

With ~337B daily ICR, Malaysian operators must identify SIM-box fraud networks and coordinated device activity across multiple mobile providers.

Singapore

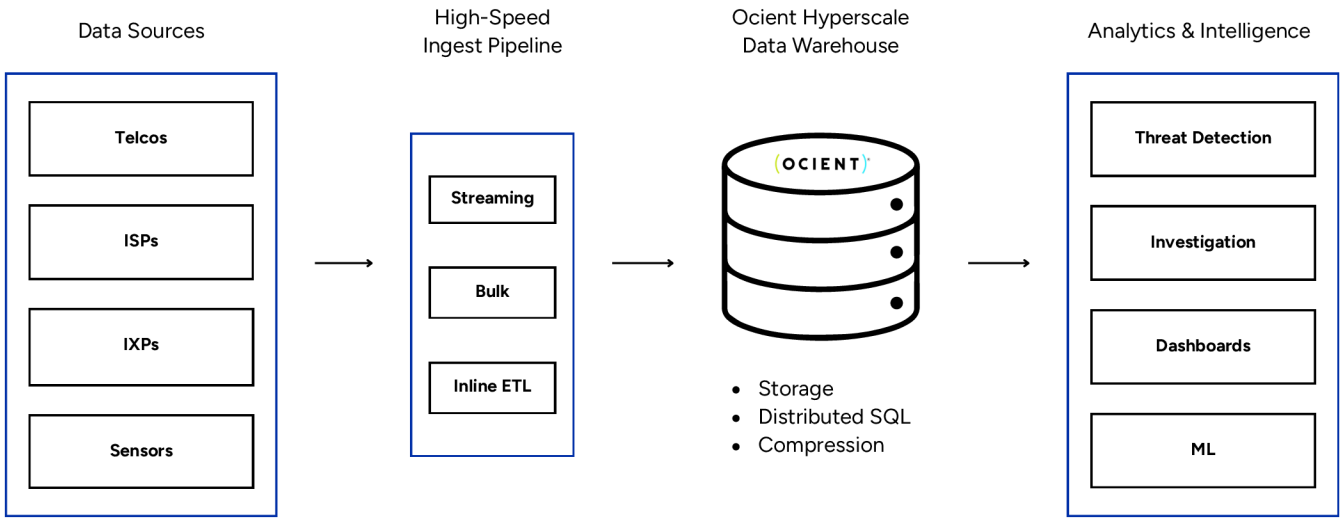
Processing ~63B ICR per day, Singapore's networks act as a global transit hub, requiring rapid detection of reconnaissance targeting financial and infrastructure systems.

India

At approximately 3.8T ICR daily, nationwide correlation of metadata is essential to detect cross-border cyber and terrorism activity.

(OCIENT)
NATIONAL SECURITY SOLUTIONS

OCIENT HYPERSCALE INTELLIGENCE ARCHITECTURE



Intelligence Outcomes

Rapid Threat Detection
Detect reconnaissance, C2 activity, and anomalies across trillions of network records.

Cross-Network Correlation
Integrate telemetry across telecom, ISP, cloud, and sensor networks.

Deep Forensic Investigation
Trace historical activity and infrastructure reuse across years of metadata.

Operational Efficiency
Replace fragmented pipelines with a unified analytics platform.

Deployment Options

Air-gapped national environments	Sovereign cloud deployments	On-premises infrastructure	Hybrid architectures with regional ingest nodes

Turning Network Metadata into National-Scale Intelligence

Turn trillions of network records into actionable intelligence. Ocient National Security Solutions for Network Intelligence enable security organizations to detect threats faster, investigate incidents more deeply, and maintain visibility across encrypted, distributed networks at national scale.

Learn More
ONSS@ocient.com