onum

Real-time control over your security telemetry data

Onum is a real-time data intelligence platform that gives security and IT teams complete control over how telemetry data is reduced, transformed, enriched, and routed in flight. With Onum, organizations gain operational agility, lower ingestion and storage costs, and accelerate threat response while avoiding brittle scripts or post-processing delays.

Onum / **Home**

+ Add filter   Range is **Last Week**   + Type   Data sink

Net Saved
65.19%
-501.88 GB

Listeners
149.5K EPS
-0.296%

Data Sink
87.92
+5.30%

Data source
Syslog

Show metrics   Show history

Events In (EPS)	AVG **5.517K** +0.041%	Bytes In (Bytes/sec)	AVG **11.58MB/s** +0.041%
Events Out (mb/sec)	AVG **2.864K** +0.041%	Bytes Out (Bytes/sec)	AVG **959.85KB/s** +0.041%

S3
40.94

584.49 GB

EL

Control your data in transit

- Process metrics, events, logs, and traces from any source to any destination, in real-time
- Reduce noise at the source by filtering unneeded telemetry data before it hits your analytics platforms
- Enrich with threat intel, asset data, geo-IP, and more
- Transform to fit schemas like OCSF with field and format changes
- Automatically route structured and enriched data to multiple systems in parallel

What you can do with Onum

Reduce

Drop unnecessary logs, fields in logs, sampling traffic, and deduplicating events at the edge.

Enrich

Add context in real-time with lookups, joins, and AI-driven insights to make raw data actionable.

Transform

Normalize formats, restructure payloads, and prepare data for downstream systems.

Optimize

Route enriched data to SIEMs, lakes, SOAR, and analytics tools to cut costs and boost efficiency.

Architecture

High-speed, in-memory pipeline

- Stateless, in-stream processing architecture with no intermediate storage
- Millisecond-level latency from ingest to output
- Native observability with stage-level telemetry

Deployment options

- Cloud-hosted (SaaS), on-premises, or hybrid deployment
- Deployable via containers, or Kubernetes
- Horizontally scalable per-core throughput

Integrations

- 50+ integrations with SIEM, SOAR, storage, observability, and data tools
- Agentless ingestion from syslog, HTTP, cloud APIs, Kafka, and more
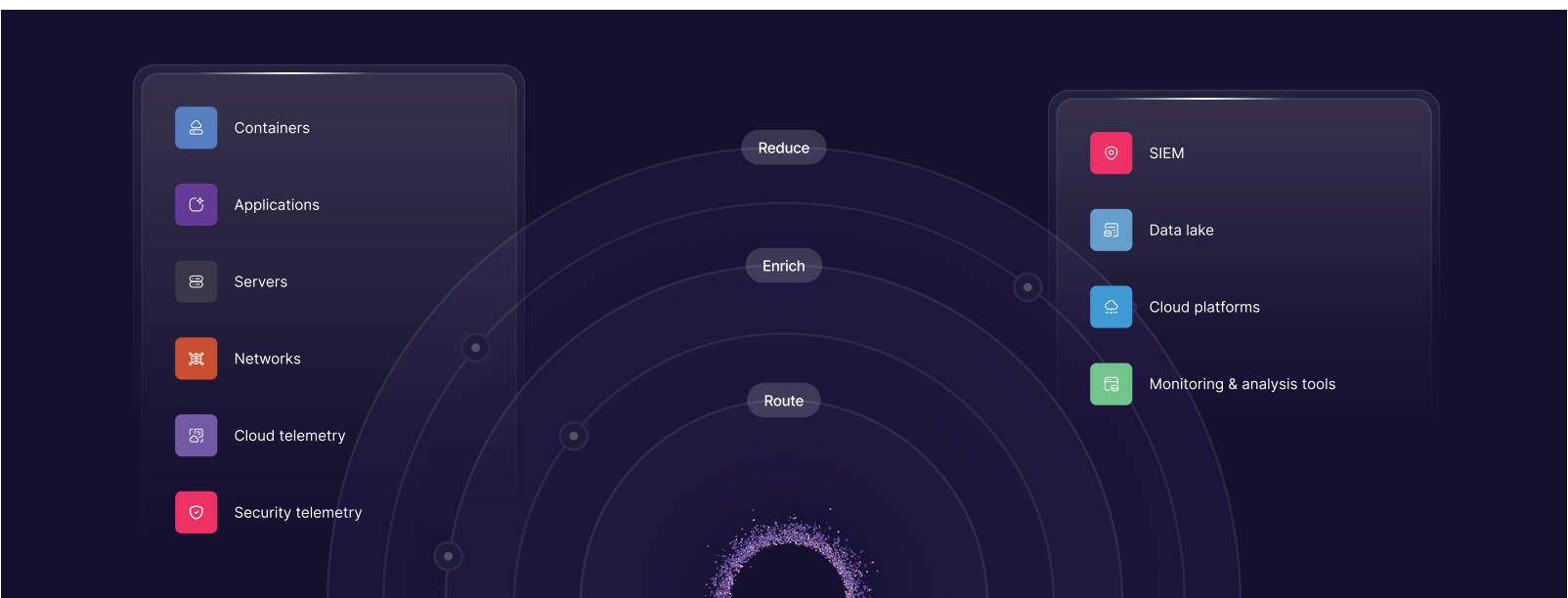- Protocol-aware output to Splunk, Sentinel, S3, GCS, BigQuery, Elastic, Datadog, and others

Plaform management

- Immutable audit logs and configuration change tracking
- AI assistant for pipeline building, tuning, and validation
- Visual pipeline editor with live preview and testing tools
- Configuration versioning and rollback support
- Marketplace of prebuilt processors, routes, and templates

Monitoring and visibility

- Built-in monitoring of source-to-destination pipelines
- Per-stage metrics for throughput, latency, and error rates
- Data flow visualization and live capture for inspection
- Alerting for flow interruptions and volume anomalies
- Forward logs and metrics to any observability platform

Containers	Reduce	SIEM
Applications	Enrich	Data lake
Servers		Cloud platforms
Networks	Route	Monitoring & analysis tools
Cloud telemetry		
Security telemetry		

Working with data

- Drag-and-drop UI for building, debugging, and modifying pipelines
- Data preview with live feedback at each pipeline stage
- Enrichment via lookups, joins, conditionals, tagging, and labeling
- Native support for JSON, CSV, key/value pairs, and custom formats
- Ingest via common protocols like Syslog and HTTP
- Visual or code-driven configuration (YAML optional, not required)
- Built-in masking, hashing, and transformation functions
- Parser libraries for common security log formats

Why Onum

- Process and act on data in milliseconds, not minutes
- Drop your SIEM and observability costs without losing fidelity
- Route only high-value data to high-cost tools
- Manage pipelines across all environments from a single control plane
- Reduce manual data prep and brittle log processing
- Leverage prebuilt integrations and templates from the Onum Marketplace
- Improve pipeline design, routing, and optimization with intelligent suggestions and actions

About Onum

Onum empowers enterprises to act on data in-stream, helping security and IT teams move at the speed of business. With real-time data processing, Onum reduces inefficiencies, optimizes pipelines, and minimizes the impact on analytical platforms—enabling actionable responses in milliseconds, not minutes.

Learn more at onum.com   Book a demo onum.com/book-a-demo