Greymatter.io•

Observability Overview

Gain Deep Visibility Across Decentralized Applications

As modern software architectures grow more complex, enterprises have more difficulty observing the health of decentralized applications. Too much information is generated across too many cloud-native applications, APIs, containers, services, and data sources for DevOps and platform engineering teams to make sense of these sprawling, opaque, distributed software application environments.

Unlike stand-alone service mesh solutions narrowly focused on service connectivity, Greymatter.io's service connectivity layer platform is purpose-built to capture telemetry from our underlying service mesh to surface heuristic insights, deliver operational intelligence and highlight the key points of light and insights that matter most to make informed business, operations, and infrastructure decisions. Continuously collect, aggregate, and analyze all application network traffic, data and usage patterns to gain real-time visibility across modern software applications.

Leverage AI and machine learning to automatically detect anomalies, conduct health checks, and surface heuristic insights to identify potential performance issues.

Run applications more efficiently across hybrid, multi-cloud and on-premise environments by understanding how users interact with data and services in real time.

View Distributed App Data in One Place

Greymatter.io aggregates metrics, events, logs and traces across hybrid, multi-cloud and on-premise environments into a single, centralized location to provide enterprises with real-time visibility into the health of decentralized software applications.

Our platform provides Network Operations Center (NOC) teams with real-time dashboards, scorecards and analytics to easily identify service status (stable, down, or warning), filter by business impact (critical, high, medium or low), view continuous health check alerts (pass, fail, or misconfigured), and more. These capabilities help DevOps engineers detect potential performance issues at scale across a chain of hundreds or thousands of microservices, without needing to access, correlate, and analyze data from multiple siloed cloud monitoring and observability tools.





"Enables network overwatch." 451 Research Report



Real-Time Dashboards, Scorecards and Analytics

EKS West	Search Services	Filter	✓ Elist Stop	Group Mesh Name	Sort Name
0 WARNING STABLE 20	III EKS West (2)				
	** DIAS Simulator 110	• AAC - A 2.0	•• AAC - B 2.0	• AAC Load Balancer 20	** AAC - DIAS Connector Latest
AKS East & REMOTE: East Mesh	SOAP service that mirrors the DIAS service	Access and Authentication Service	Access and Authentication Service	Access and Authentication Service	Connects AAC-A to DIAS
DOWN WARNING STABLE	CARABUSY OWNER None AAC AN ENDROMY https://www.dereo.greymether.loydias/	CARRELITY OWNER Authentication AAC An Experient None	CARABILITY OWNER Authentication AAC Ant Exponent None	CAMBLITY DANER Load Balancer AAC An Exception Intros/Veac.demo.greymatter.lo/	CAMABUTY OWNER None AAC AREADONNT None
		🛛 INTLS/HTTP	🛛 (mtl.s;http) 💿 👻 🖽	🛛 mtlshttp	TLS/HTTP
East Istio REMOTE East Mesh	◆ AAC Edgev1.9.11	* Redis-AAC Latest	•••Audits 12.5	Catalog 3.3.2	**Control 130.3
	Edge ingress for aac	No Description	A standalone dashboard visualizing data collected from greymatter audits.	Interfaces with the control plane to expose the current state of the mesh.	Manages the configuration of the greymatter data plane.
	EDGE AAC APESPOINT None	CARAGELITY OWNER Nome AAC ARE ENDPOINT Nome	CARABILITY OWNER Mesh greymatterio Are Disponent Jiservices/audits	CARRALITY OWNER Mesh groymatter.io ARI (DepOnit /services/catalog	CARADUTY CHART Mesh graymatter.io ARI Exponent /services/control-api
	ntlsmttp	atls/tcp	mtlshttp	TLS(HTTP E	TLSHTTP ==
	•••Edge 1:0.2	•••One2many Edge v1.8.1	• greymatter Prometheus v2.40.1 🔨	• Tolerance Details v1.0.0	• Tolerance Productpage v1.0.0
	Handles north/south traffic flowing through the mesh.	Edge ingress for one2many	Prometheus TSDB for collecting and querying historical metrics.	West Tolerance Details	West Tolerance Propductpage
	CANABURY OWNUR Mesh groymatter/o Antenceronit /	CANABUTY OWNER none One2many An ENDPOINT None	CARABILITY OWNER Mesh greymattecio Ant Expropert Jesnicosciposmetheus/graph	CAMBUTY OWNER None Tolerance AMERCIPONT Nane	CAMABUTY OWNER None Tolerance All Excents Thtps://westfailowscidemc.greymatter.je/productpage
				a milshitte	MTLS/HTTP
	◆ Tolerance Reviews v1.0.0 √L	• Tolerance Failover Brid v181 v	• Tolerance Edge v181		
	West Reviews Service	Failover ingress/egress point for tolerance	Edge ingress for tolerance		
	CANABUTY OWNER None Tolerance APRENDPOINT None	CAMABUTY OWNER None Tolerance API ENDPOINT None	CARABILITY OWNER None Tolerance AR INDRONT None		
	TLSHTTP	ntlshttp			
	💠 AKS East - East Mesh (39)				
	Bookinfo Reviews V2 v10.0	Audits 12.5 REMOTE: Fast Meth	Bookinfo Details v10.0	Bookinfo Productpage v1.0.0 BEMOTE: Fast Meth	** Bookinfo Ratings v10.0
	Bookinfo Reviews V2 - Black Stars	A standalone dashboard visualizing data collected	East Bookinfo Details	East Bookinfo Productpage	East Bookinfo Ratings

© and [™] 2024 Greymatter.io , Inc. All rights reserved.

Service Summary

- 🖌 Uptime
- Average Response Time
- Error % Across All Requests
- CPU & Memory Utilization
- Chart of Requests Over Time

Historical Metrics

- Service-Level Latency
- Route-Level Usage
 Host Performance
- Host Performa
- Request Rate
- Error Rate
- Route-Level Performance
- Instances

Instance Metrics

- ✓ Route View
- 🖌 Heap (Runtime)
- Explorer Time-Series Metrics

Historical Metrics

- HTTP/3 Protocols
- Health Checks
- Outlier Detection
- Circuit Breakers
- Timeout Budget
- Load Balancers
- Request Response Size
- 🖌 And more ...





Aggregate decentralized software application metrics into a single-pane-of-glass dashboard, with memory and CPU utilization, percentile latencies, error rates, request rates, and more.

Why Greymatter.io?

Analyze Hundreds of App Metrics

Continuously collect, aggregate, and analyze more than 100+ default Envoy metrics and dozens of proprietary metrics across Layers 3, 4, and 7 (Network, Transport, and Application), reducing the need for manual log collection, analysis, and troubleshooting. Automaticaly capture every single network transaction flowing between all users, systems, and services down to the route level, providing a real-time audit trail of who is using what services, when, where and how to enforce compliance with FIPS, PCI, HIPAA, GDPR, and other industry regulations.

Surface AI Insights for IT Operations

Leverage AI and machine learning to analyze the vast amount of traffic, data and usage patterns generated across the service mesh to observe healthy network traffic, establish normal baseline thresholds, and automatically detect anomalies. Continuous health checks provide an early warning of traffic bottlenecks, service failures, or application downtime. Use built-in AlOps to surface heuristic insights to help DevOps teams conduct root cause analysis, pinpoint performance issues and take corrective action to reduce Mean Time to Recovery (MTTR).

Optimize Application Performance

Go beyond statistics, counters, and telemetry by correlating operational cues and recommending actionable insights to optimize performance. Developers discover which services are available, even in nonKubernetes, bare-metal VM, or legacy environments. Software architects use actual traffic, data, and usage to design more efficient applications, improve performance, reduce latency, and optimize utilization. DevOps engineers monitor traffic, scale workloads, identify bottlenecks, and troubleshoot issues to continuously meet or exceed service level objectives (SLOs).

