Greymatter.io

Mission-Ready Zero Trust for Cloud, Hybrid, and Edge Networks

How Greymatter Empowers Civilian, Defense, and IC Enterprises with Seamless Connectivity from Cloud to Edge

Greymatter.io Inc. is a small business Nontraditional Defense Contractor available through the Tradewinds Solutions Marketplace and via Carahsoft.

Contents

03 Why Is Zero Trust Service Connectivity Vital for Next-Gen Cloud and Edge?

04 Greymatter.io: Bettering the Connected World

05 Why Choose Greymatter.io?

06 Multicloud, Hybrid, and Edge Service Catalog

07 What Greymatter Brings to an Enterprise

08 Unified Cloud Services, MPN, and MEC

09 Segregated, Hybrid, and Isolated Solutions

10 Features, Advantages, & Benefits for Connected Enterprises

11 Resilient Network Architecture for Operations

12 Features, Advantages, & Benefits for Network Operations

13 Optimized App, AI, & Data Micro Gateways

14 Features, Advantages, & Benefits of Micro Gateways

15 Dynamic Policy Management for Command & Control

16 Features, Advantages, & Benefits for Command & Control

17 Zero Trust That You Can See

18 Features, Advantages, & Benefits for Zero Trust

19 Achieving Zero Trust Connectivity Objectives

20 A Trusted Partner for Civilian, DoD, and the IC Organizations

Why Is Zero Trust Service Connectivity Vital for Next-Gen Cloud and Edge?

In today's world, industries rely on secure, reliable networks. Use cases like **defense operations, Mission-Critical Communications, and Resilience Against Cyber Threats** all require Zero Trust Service Connectivity. This approach is the foundation of resilient, future-proof networks

Zero Trust Service Connectivity is a security architecture that eliminates implicit trust by verifying every network transaction, regardless of location. It provides continuous operations, encrypted communications, and granular control needed to protect against modern cyber threats.

Zero Trust is essential for securing cloud services, Mobile Private Networks (MPNs), and Multi-access Edge Computing (MEC) environments. These capabilities are critical for implementing Combined Joint All-Domain Command and Control (CJADC2), Commercial Cloud Enterprise (C2E), and the Cloud Smart Strategy.

Explore Greymatter.io's Zero Trust Service Connectivity Playbook and discover how to proactively secure and future-proof your network today.

Greymatter.io: Bettering the Connected World

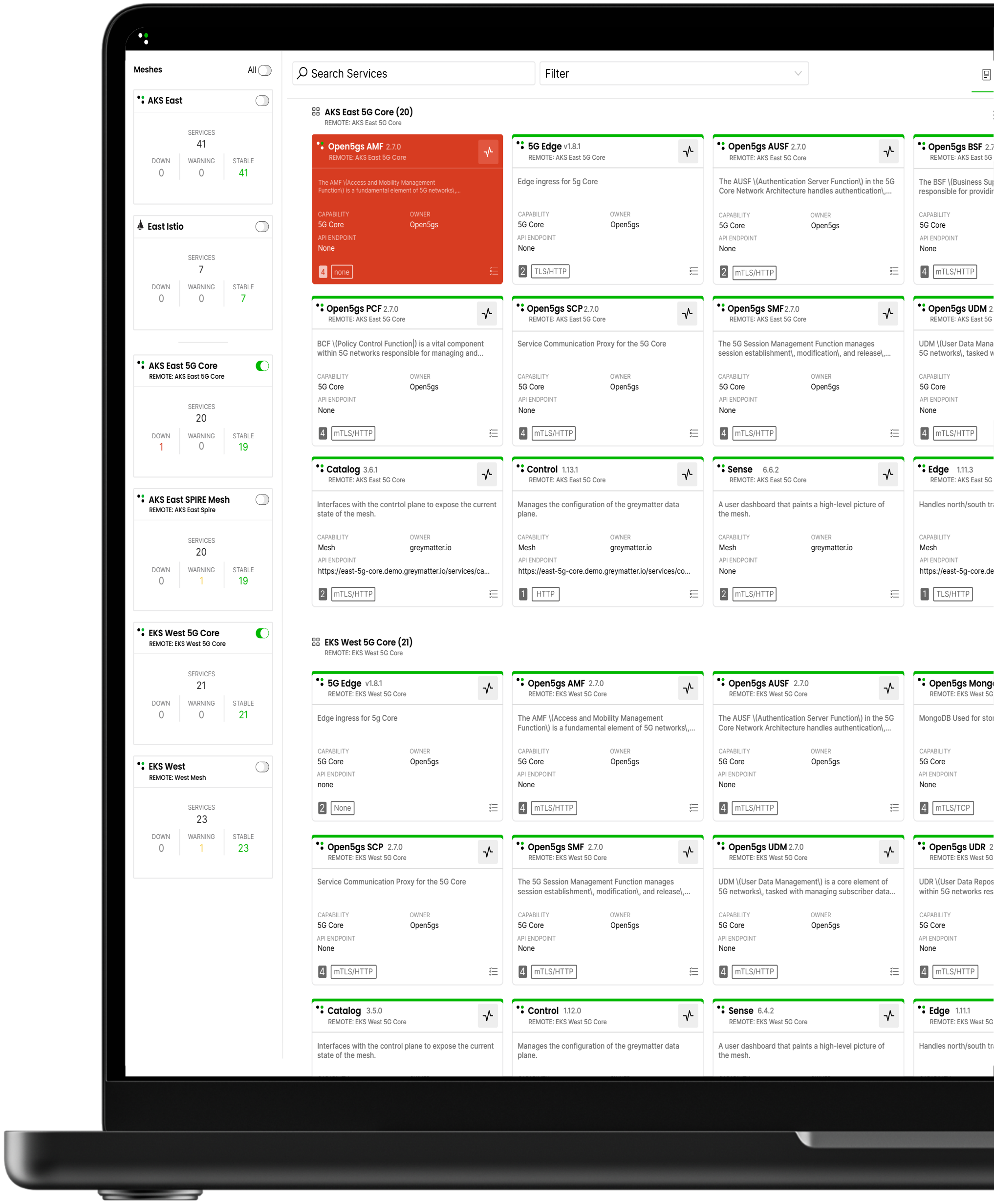
A Leader in Zero Trust Networking

Greymatter is an Enterprise-ready platform trusted by US Defense and Intelligence organizations to enhance zero trust strategies for securing data, APIs, and applications.

Greymatter.io has quickly established itself as a prominent player for use cases in zero trust service connectivity.

1. Certified and credited for automated policy controls, minimal overhead, and enforcement of NIST 207 and FIPS 140 standards.
2. Named a leader and outperformer for 3 years in a row in the GigaOm Radar Report for Service Mesh, excelling in features, emerging capabilities, and secure enterprise management.
3. Awarded the 2024 PAAS Security Solution of the Year from CyberSecurity Breakthrough.
4. Recognized twice in Gartner's Hype Cycle Reports for both Enterprise Networking and Zero Trust Networking.

These recognitions, along with our experience and acumen cement Greymatter's status as a driving force in business-critical zero trust service connectivity implementations.



Meshes All

AKS East
SERVICES 41
DOWN 0 | WARNING 0 | STABLE 41

East Istio
SERVICES 7
DOWN 0 | WARNING 0 | STABLE 7

AKS East 5G Core
REMOTE: AKS East 5G Core
SERVICES 20
DOWN 1 | WARNING 0 | STABLE 19

AKS East SPIRE Mesh
REMOTE: AKS East Spire
SERVICES 20
DOWN 0 | WARNING 1 | STABLE 19

EKS West 5G Core
REMOTE: EKS West 5G Core
SERVICES 21
DOWN 0 | WARNING 0 | STABLE 21

EKS West
REMOTE: West Mesh
SERVICES 23
DOWN 0 | WARNING 1 | STABLE 23

Search Services

Filter

AKS East 5G Core (20)
REMOTE: AKS East 5G Core

Open5gs AMF 2.7.0
REMOTE: AKS East 5G Core
The AMF \(Access and Mobility Management Function\) is a fundamental element of 5G networks\,...
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 none

5G Edge v1.8.1
REMOTE: AKS East 5G Core
Edge ingress for 5g Core
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
2 TLS/HTTP

Open5gs AUSF 2.7.0
REMOTE: AKS East 5G Core
The AUSF \(Authentication Server Function\) in the 5G Core Network Architecture handles authentication\,...
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
2 mTLS/HTTP

Open5gs BSF 2.7
REMOTE: AKS East 5G
The BSF \(Business Su
responsible for providi
CAPABILITY 5G Core
API ENDPOINT None
4 mTLS/HTTP

Open5gs PCF 2.7.0
REMOTE: AKS East 5G Core
BCF \(Policy Control Function|) is a vital component within 5G networks responsible for managing and...
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs SCP 2.7.0
REMOTE: AKS East 5G Core
Service Communication Proxy for the 5G Core
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs SMF 2.7.0
REMOTE: AKS East 5G Core
The 5G Session Management Function manages session establishment\, modification\, and release\,...
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs UDM 2
REMOTE: AKS East 5G
UDM \(User Data Mana
5G networks\, tasked w
CAPABILITY 5G Core
API ENDPOINT None
4 mTLS/HTTP

Catalog 3.6.1
REMOTE: AKS East 5G Core
Interfaces with the contrtol plane to expose the current state of the mesh.
CAPABILITY Mesh | OWNER greymatter.io
API ENDPOINT https://east-5g-core.demo.greymatter.io/services/ca...
2 mTLS/HTTP

Control 1.13.1
REMOTE: AKS East 5G Core
Manages the configuration of the greymatter data plane.
CAPABILITY Mesh | OWNER greymatter.io
API ENDPOINT https://east-5g-core.demo.greymatter.io/services/co...
1 HTTP

Sense 6.6.2
REMOTE: AKS East 5G Core
A user dashboard that paints a high-level picture of the mesh.
CAPABILITY Mesh | OWNER greymatter.io
API ENDPOINT None
2 mTLS/HTTP

Edge 1.11.3
REMOTE: AKS East 5G
Handles north/south tr
CAPABILITY Mesh
API ENDPOINT https://east-5g-core.de
1 TLS/HTTP

EKS West 5G Core (21)
REMOTE: EKS West 5G Core

5G Edge v1.8.1
REMOTE: EKS West 5G Core
Edge ingress for 5g Core
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT none
2 None

Open5gs AMF 2.7.0
REMOTE: EKS West 5G Core
The AMF \(Access and Mobility Management Function\) is a fundamental element of 5G networks\,...
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs AUSF 2.7.0
REMOTE: EKS West 5G Core
The AUSF \(Authentication Server Function\) in the 5G Core Network Architecture handles authentication\,...
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs Mong
REMOTE: EKS West 5G
MongoDB Used for sto
CAPABILITY 5G Core
API ENDPOINT None
4 mTLS/TCP

Open5gs SCP 2.7.0
REMOTE: EKS West 5G Core
Service Communication Proxy for the 5G Core
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs SMF 2.7.0
REMOTE: EKS West 5G Core
The 5G Session Management Function manages session establishment\, modification\, and release\,...
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs UDM 2.7.0
REMOTE: EKS West 5G Core
UDM \(User Data Management\) is a core element of 5G networks\, tasked with managing subscriber data...
CAPABILITY 5G Core | OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs UDR 2
REMOTE: EKS West 5G
UDR \(User Data Repos
within 5G networks res
CAPABILITY 5G Core
API ENDPOINT None
4 mTLS/HTTP

Catalog 3.5.0
REMOTE: EKS West 5G Core
Interfaces with the control plane to expose the current state of the mesh.

Control 1.12.0
REMOTE: EKS West 5G Core
Manages the configuration of the greymatter data plane.

Sense 6.4.2
REMOTE: EKS West 5G Core
A user dashboard that paints a high-level picture of the mesh.

Edge 1.11.1
REMOTE: EKS West 5G
Handles north/south tr

GIGAOM RADAR REPORT LEADER 2024 SERVICE MESH

CYBERSECURITY BREAKTHROUGH AWARD 2024

Gartner®

Why Choose Greymatter.io?

Greymatter is the ideal partner to enhance Civilian, Defense, and IC Enterprise's zero trust initiatives for data, APIs, and applications due to its advanced capabilities in zero trust networking and distributed control architecture. Greymatter has been trusted and certified across Defense and IC environments ranging from IL2 to IL6+. Our platform minimizes overhead on tactical connections, provides unparalleled security and observability, and automates policy controls across all network layers.

Customer Use Cases:

- ✓ Zero Trust Connectivity
- ✓ Automation & Orchestration
- ✓ NIST 207 & FIPS 140 Compliance
- ✓ Traffic Management & Control
- ✓ Automated SOC: playbooks, cloud security, & incident response

Stakeholders:

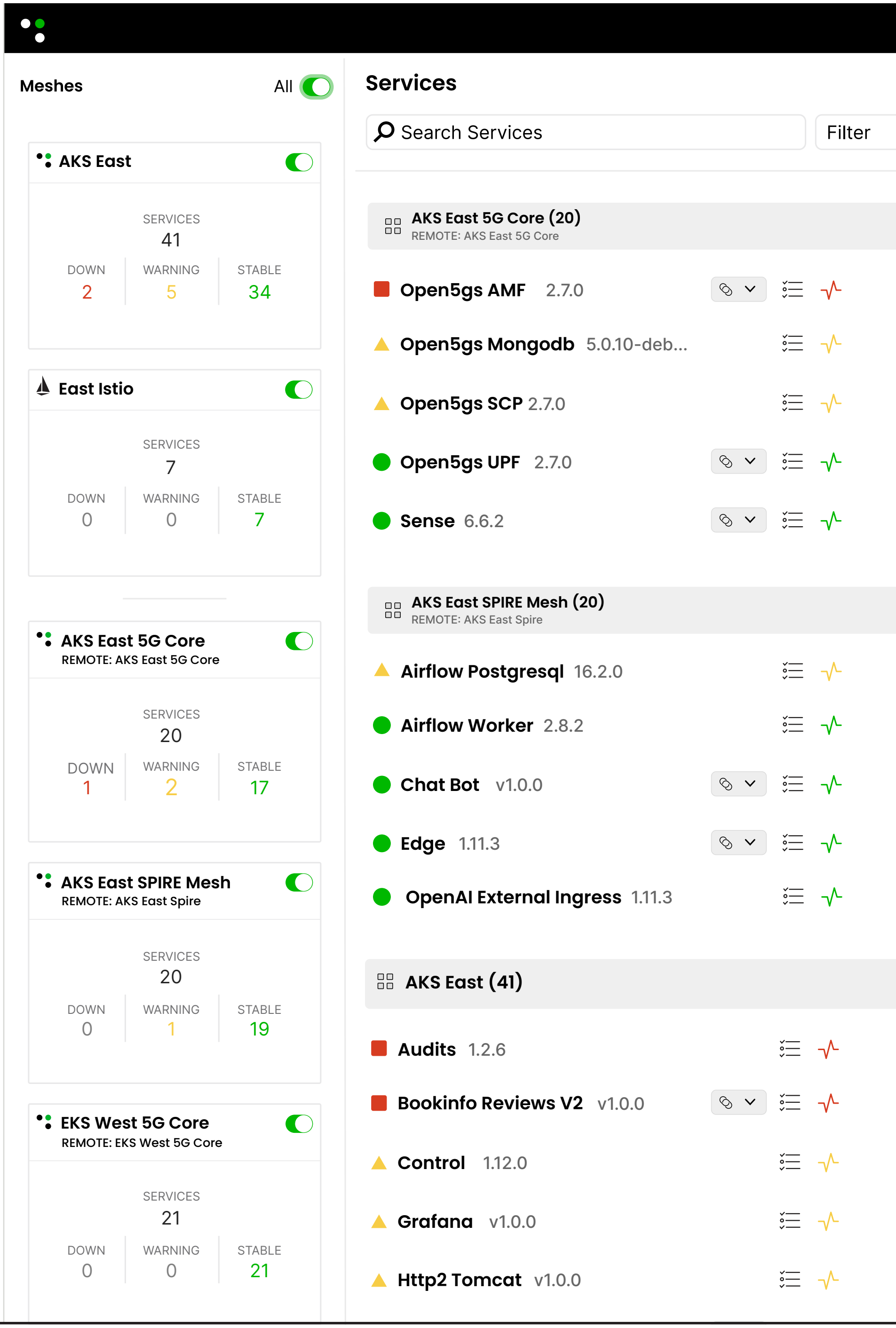
- ✓ Mission Team
- ✓ CIO
- ✓ CISO
- ✓ Platform Engineering
- ✓ Network Modernization

Multicloud, Hybrid, and Edge Service Catalog

Greymatter's flexible platform integrates with multicloud, hybrid cloud, and 5G MPN/MEC platforms. It controls secure, efficient communication across cloud, tactical, and edge environments. The platform catalogs connected services, providing real-time telemetry, health information, and a visual overview of every component. This ensures observability and control, critical for critical business, defense, and IOT operations that need scalable, secure performance across diverse environments.

Key Points:

1. A unified Cloud/MPN/MEC architecture can **reduce latency by up to 70%** for defense operations. (Source: GSMA)
2. Defense operations rely on cloud services, MPNs, and MEC for secure communications. **ZTN blocks unauthorized access** to sensitive networks, even if the perimeter is breached.
3. Sensitive communications across multiple clouds are secured with Zero Trust, which **continuously verifies policies and encrypts traffic.**



Meshes All

AKS East

DOWN	WARNING	STABLE
SERVICES 41		
2	5	34

East Istio

DOWN	WARNING	STABLE
SERVICES 7		
0	0	7

AKS East 5G Core
REMOTE: AKS East 5G Core

DOWN	WARNING	STABLE
SERVICES 20		
1	2	17

AKS East SPIRE Mesh
REMOTE: AKS East Spire

DOWN	WARNING	STABLE
SERVICES 20		
0	1	19

EKS West 5G Core
REMOTE: EKS West 5G Core

DOWN	WARNING	STABLE
SERVICES 21		
0	0	21

Services

Search Services | Filter

AKS East 5G Core (20)
REMOTE: AKS East 5G Core

🟥	Open5gs AMF	2.7.0
▲	Open5gs Mongodb	5.0.10-deb...
▲	Open5gs SCP	2.7.0
●	Open5gs UPF	2.7.0
●	Sense	6.6.2

AKS East SPIRE Mesh (20)
REMOTE: AKS East Spire

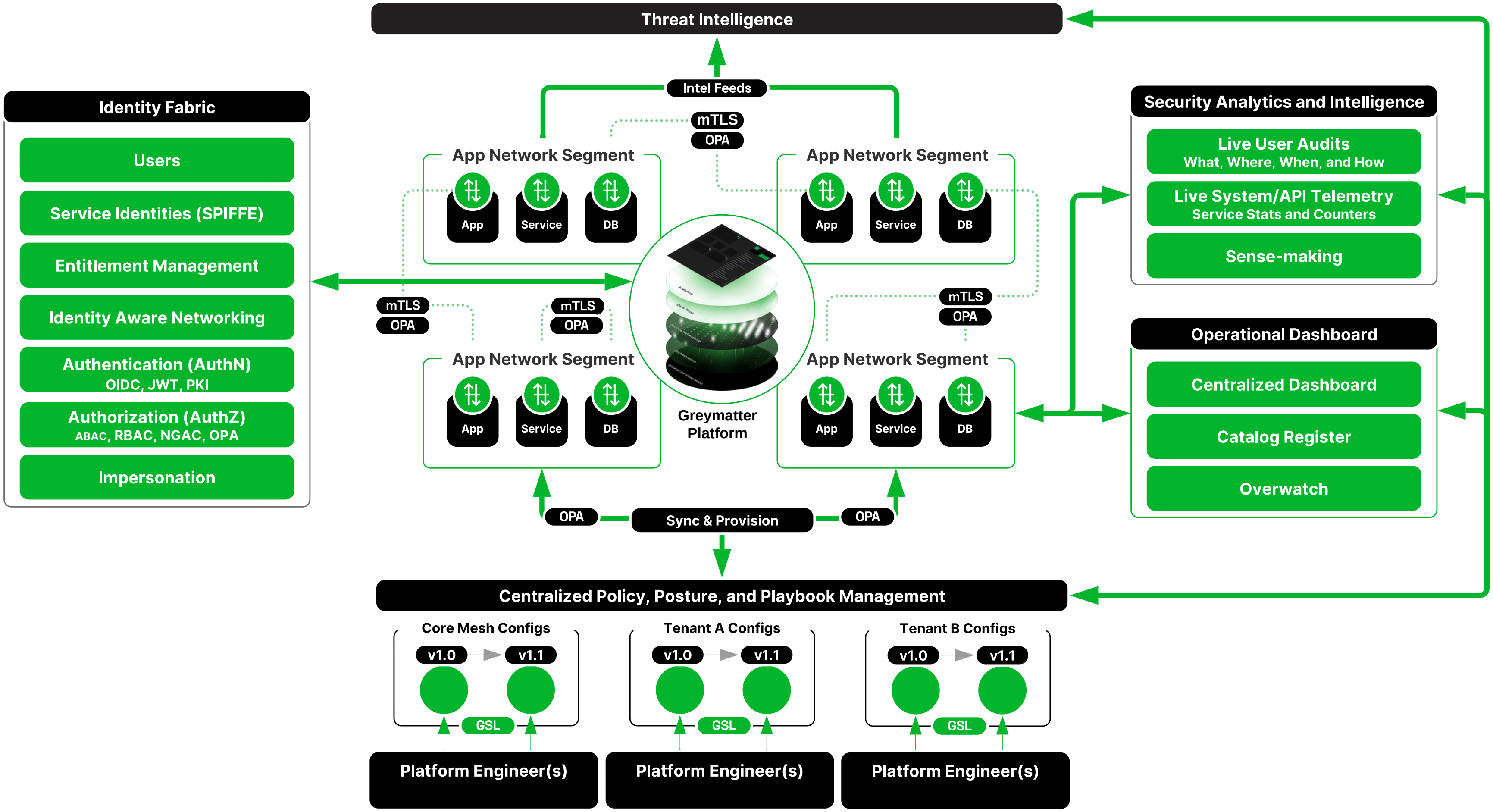
▲	Airflow Postgresql	16.2.0
●	Airflow Worker	2.8.2
●	Chat Bot	v1.0.0
●	Edge	1.11.3
●	OpenAI External Ingress	1.11.3

AKS East (41)

🟥	Audits	1.2.6
🟥	Bookinfo Reviews V2	v1.0.0
▲	Control	1.12.0
▲	Grafana	v1.0.0
▲	Http2 Tomcat	v1.0.0

What Greymatter Brings to an Enterprise

Initiatives such as CJADC2, C2E, and the Cloud Smart Strategy are designed for U.S. Federal Government Agencies to tackle the significant challenges faced by operations from Cloud to Denied, Disrupted, Intermittent, and Limited (DDIL) environments. With the increasing complexity of connected networks, the U.S. Civilian, Defense and Intelligence Community (IC) Enterprises require a resilient, agile, and secure zero trust connectivity architecture that can thrive even in the most restricted and difficult operational environments.



Threat Intelligence

Intel Feeds

Identity Fabric

- Users
- Service Identities (SPIFFE)
- Entitlement Management
- Identity Aware Networking
- Authentication (AuthN) OIDC, JWT, PKI
- Authorization (AuthZ) ABAC, RBAC, NGAC, OPA
- Impersonation

App Network Segment: App, Service, DB

mTLS OPA

Greymatter Platform

Security Analytics and Intelligence

- Live User Audits — What, Where, When, and How
- Live System/API Telemetry — Service Stats and Counters
- Sense-making

Operational Dashboard

- Centralized Dashboard
- Catalog Register
- Overwatch

OPA — Sync & Provision — OPA

Centralized Policy, Posture, and Playbook Management

Core Mesh Configs: v1.0 → v1.1, GSL

Tenant A Configs: v1.0 → v1.1, GSL

Tenant B Configs: v1.0 → v1.1, GSL

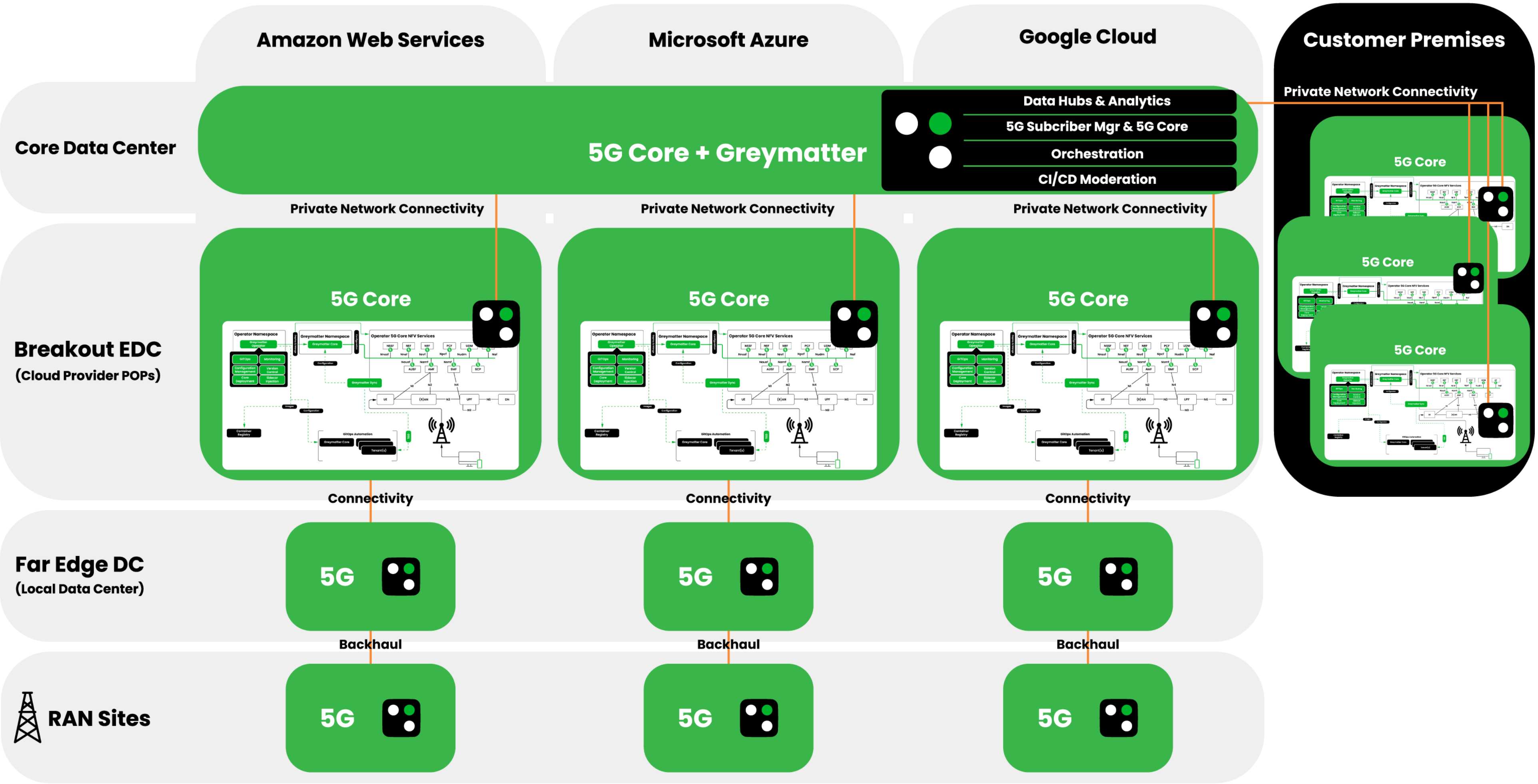
Platform Engineer(s)

Platform Engineer(s)

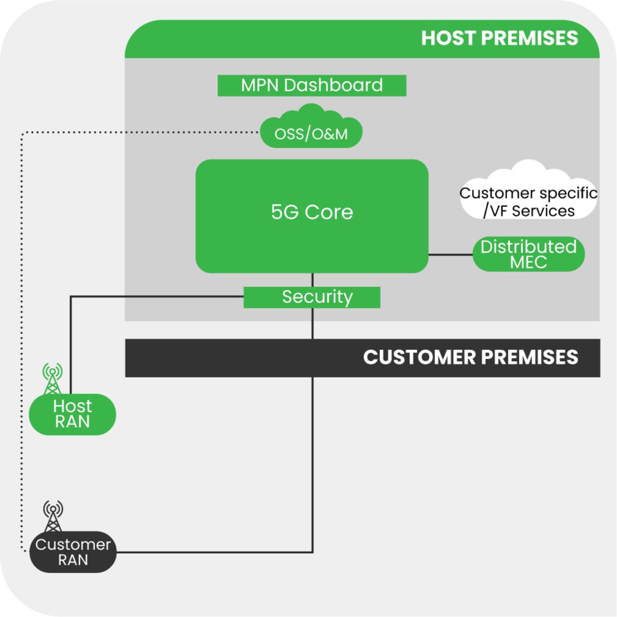
Platform Engineer(s)

Unified Cloud Services, MPN, and MEC

Greymatter offers a unified platform that supports deployments across edge, private data centers, and public clouds **without vendor-specific adjustments or configurations**. The combined platform efficiently orchestrates low-latency 5G NFV functions at the edge while managing cloud services centrally. This enables cloud-based processing and real-time execution at the edge, all with **consistent security, lifecycle management, and orchestration across environments.**



Segregated, Hybrid, and Isolated Solutions



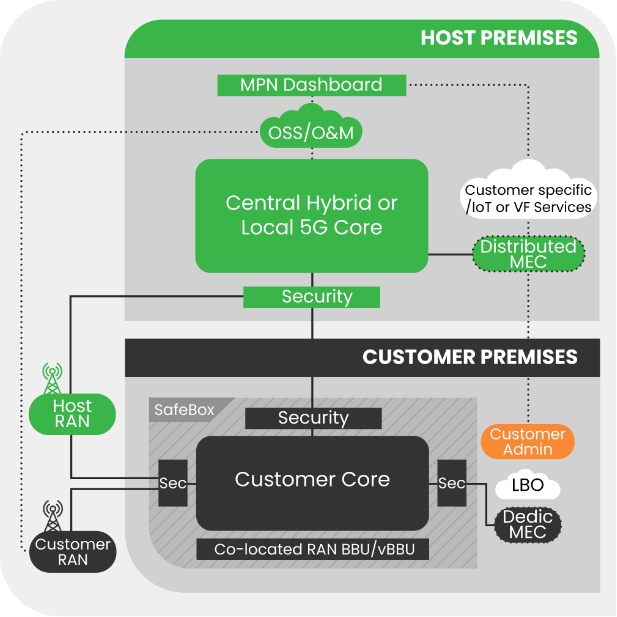
Segregated MPN

Workload isolation using dynamic access policies and service identity attestation.

Encrypted east/west communication between services.

Segmented customer-driven security policy automation.

Metrics and audits collection from services for centralized monitoring and customer reporting continuity of operation.

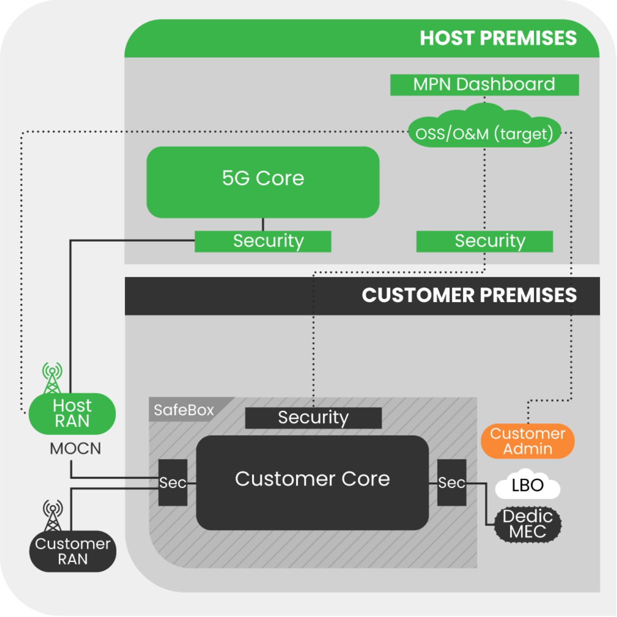


Local/Central Hybrid MPN

Workload and control plane isolation reducing customer attack surface in hybrid MPN.

Certificate automation simplifies certificate handling, ensuring seamless mTLS encryption.

Dynamic routing, load balancing, flow control, and failover from customer premises to host agency or alternative COOP site updates across customer resources.



Isolated (Dedicated) MPN

(with Public and/or Spectrum)

Unified visibility and monitoring for easy management and troubleshooting.

Secure, interoperable communication between MPN and diverse customer region deployments.

Microsegmentation and traffic isolation across any cloud platform or customer site.

Dynamic security policy adjustments to match specific cloud or operating region needs.

Features, Advantages, & Benefits for Connected Enterprises

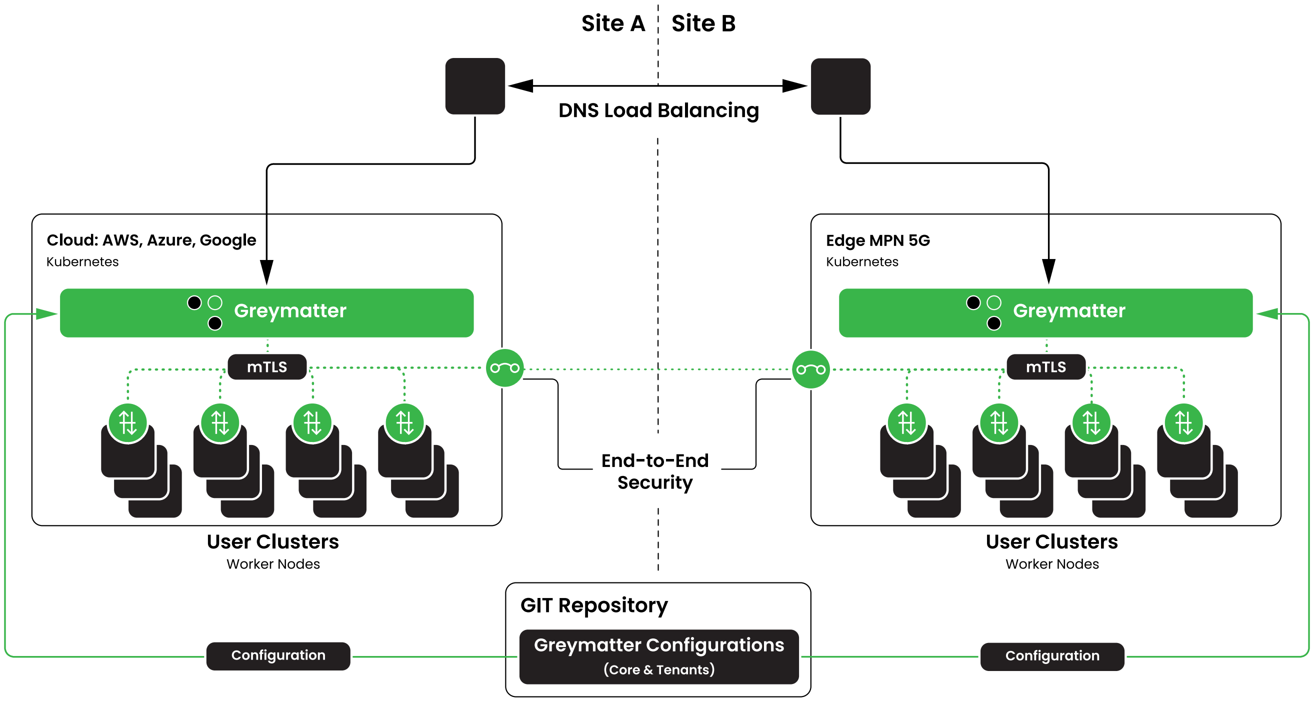
Feature	Advantage	Benefit
Agnostic Integration and Management	Supports seamless integration across multicloud and hybrid environments	Ensures compatibility and flexibility with diverse cloud providers and on-premises systems
Multi-Mesh Connections and Federation	Enables secure, efficient communication across various network environments	Enhances strategic observability and control, improving operational efficiency in tactical deployments
Service Cataloging with Real-Time Telemetry and Auditing	Manages connected services with real-time health monitoring and visual oversight	Provides comprehensive, end-to-end visibility, ensuring seamless operations and minimizing vulnerabilities

Resilient Network Architecture for Operations

Greymatter's architecture is built for resilience. At the heart of this are distributed control planes that ensure continuous operations even when parts of the network are compromised. Each Greymatter data plane autonomously manages policy control and data processing at the edge, reducing reliance on central systems and enabling faster decision-making. This localized service management ensures that critical services are secure and always available, no matter the environment.

Key Points:

1. **Edge processing** reduces latency and enhances reliability during tactical missions.
2. **Decentralized control plane** ensures continuous operations even in compromised network conditions.
3. **Active service discovery** ensures efficient traffic management, optimizing bandwidth and performance in DDIL environments.



Features, Advantages, & Benefits for Network Operations

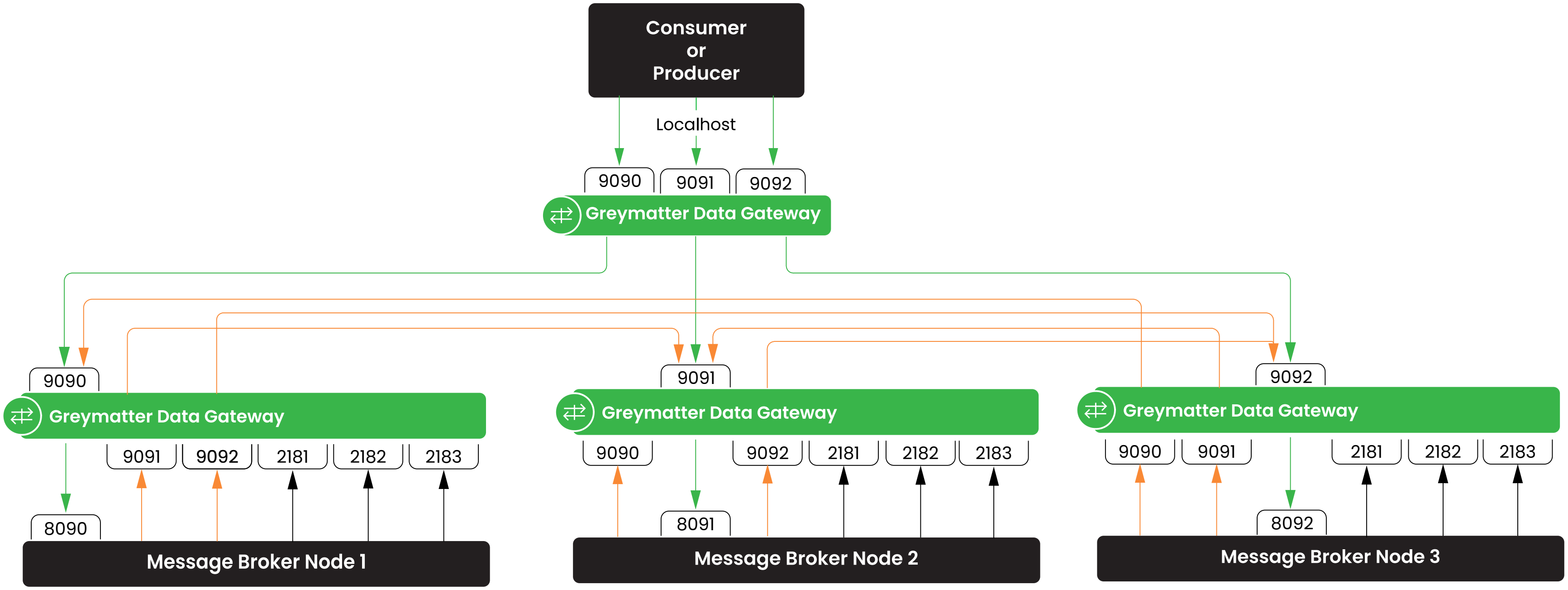
Feature	Advantage	Benefit
Decentralized Control and AI, Data, API, and Service Microgateways	Enables direct routing and processing at the edge	Eliminates reliance on central hubs, reducing latency and improving reliability
Localized Service Discovery and Routing	Automatically routes data based on local network conditions	Ensures continuous operation even when central connections are compromised
Multi-Protocol Support, including 5G streaming and RAN connectivity	Supports diverse protocols for edge and cloud communication	Increases flexibility and ensures compatibility with various tactical environments, avoiding single points of failure

Optimized App, AI, & Data Micro Gateways

In tactical operations, uninterrupted data flow is critical. Greymatter's platform utilizes application, AI, and data micro-gateways to manage diverse tech stacks, including JavaScript applications, AI modules, APIs, and message brokers like Kafka and RabbitMQ. This ensures seamless communication, even in highly constrained environments. By eliminating traditional single points of failure, Greymatter dynamically adjusts routing and network load on your data systems to ensure mission-critical data always reaches its destination.

Key Points:

1. **Uninterrupted data flow** is essential in tactical operations.
2. **Greymatter micro-gateways** manage diverse tech stacks, including JavaScript apps, AI, and APIs.
3. **Dynamic flow control** minimizes network congestion and ensure reliable, secure data delivery across segments.



Features, Advantages, & Benefits of Micro Gateways

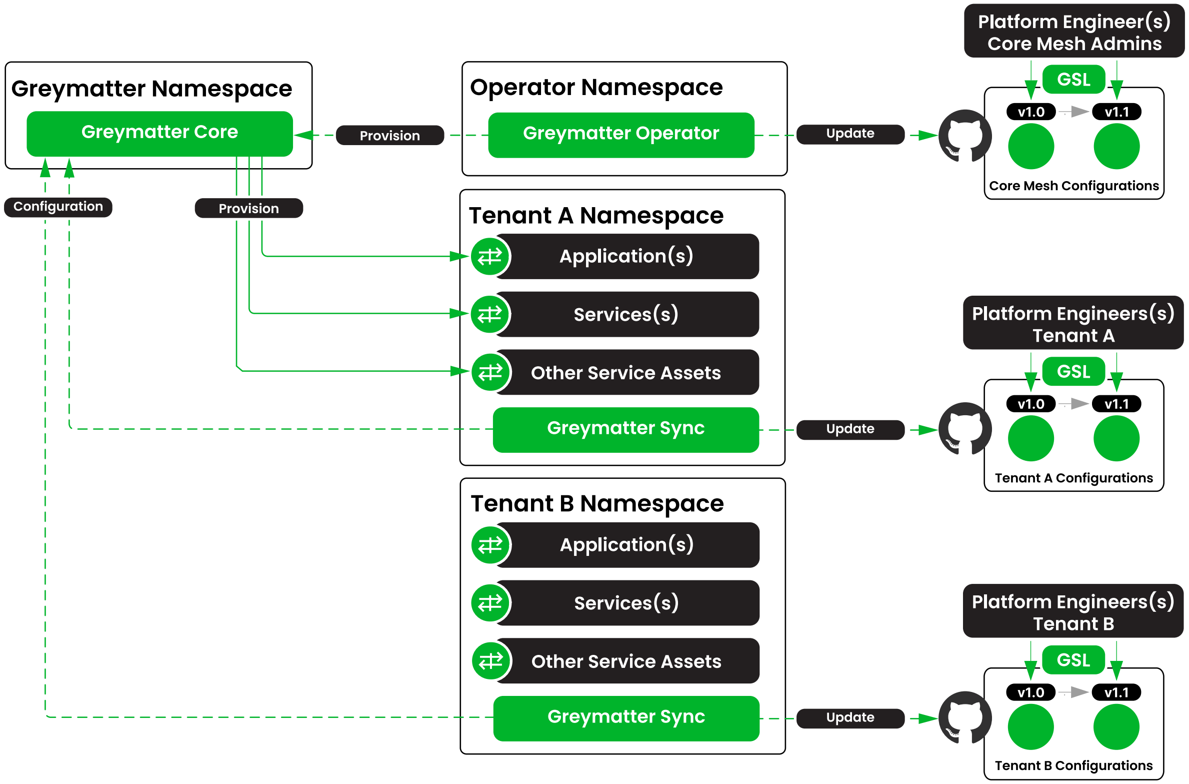
Feature	Advantage	Benefit
Agnostic Micro Gateways to manage applications, APIs, AI modules, and data services	Supports multiple technologies and clouds like JavaScript, Open AI and AI modules, Object Storage, Kafka, and RabbitMQ.	Eliminates single points of failure and vendor specific implementations, ensuring efficient data sharing from Cloud to DDIL Edge environments
Dynamic Prioritization and Flow Control	Optimizes network traffic with active and passive failover within clusters, across clouds, and across geographic regions	Minimizes network congestion and ensures reliable data delivery across segments
Decentralized Control and Data Planes	Direct, optimized connections at the edge	Eliminates central bottlenecks, enhancing speed, security, and reliability for tactical operations

Dynamic Policy Management for Command & Control

Greymatter allows operators to adjust and orchestrate network configurations in real-time through its powerful policy engine. Fleet-wide playbooks can be deployed and applied in real-time to manage multiple system changes dynamically, ensuring that the network adapts to evolving mission requirements. Using built-in service discovery, Greymatter routes traffic efficiently based on real-time conditions, optimizing bandwidth and performance for critical mission operations.

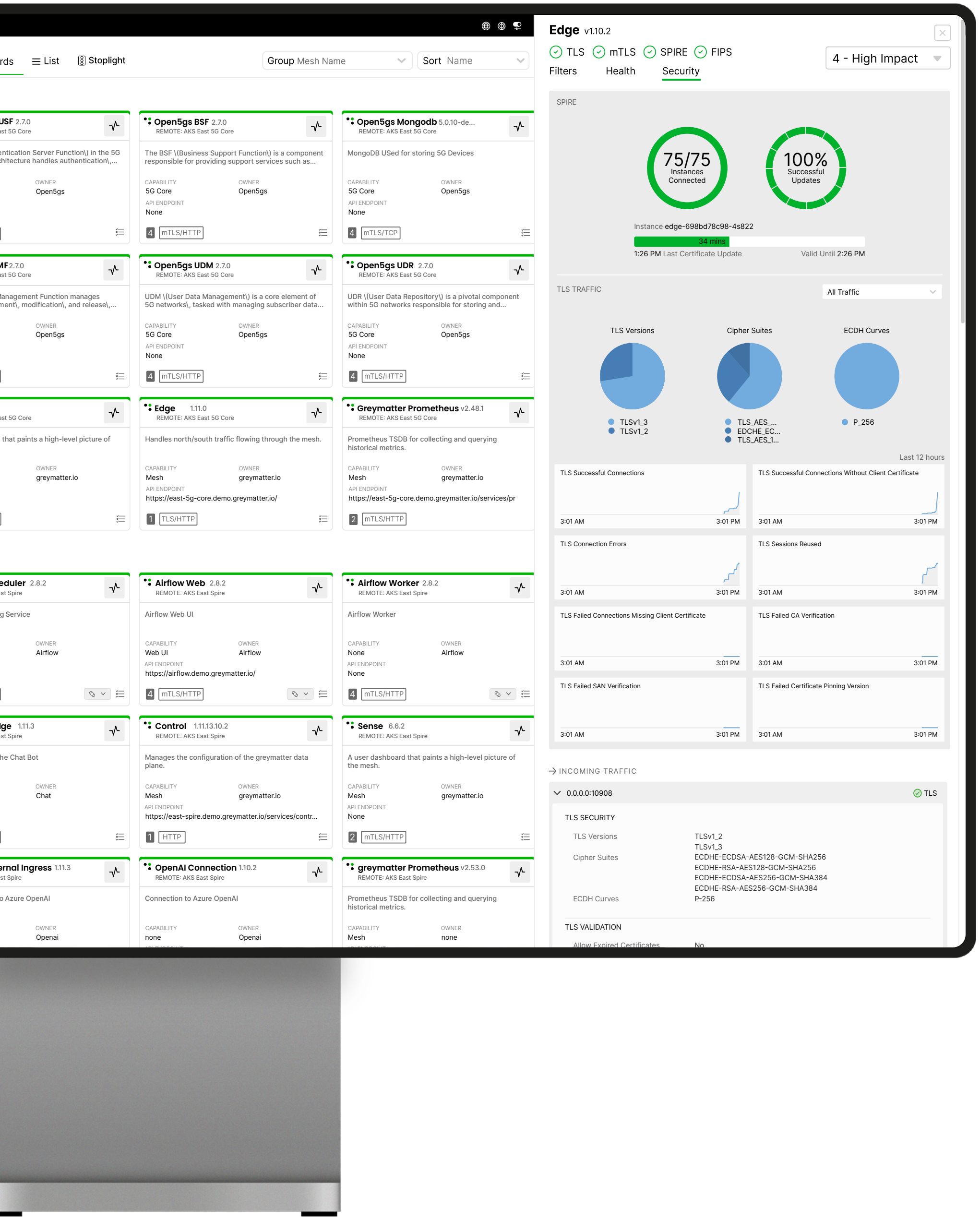
Key Points:

1. **Real-time network orchestration** is enabled through Greymatter's powerful policy engine.
2. **Fleet-wide playbooks** allow dynamic system changes, adapting to evolving mission requirements.
3. **Scalable deployment automation** reduces latency and improves decision-making speed, enhancing operational efficiency.



Features, Advantages, & Benefits for Command & Control

Feature	Advantage	Benefit
Flexible Policy Engine for Mission-Critical Playbooks managed by Git	Enables real-time orchestration of configuration changes	Allows dynamic system reprioritization to meet evolving mission needs across all environments
Fleet-Wide Playbook Management with Dynamic Service Discovery	Adapts to changing network conditions and cybersecurity activities	Ensures efficient data routing, reduces unnecessary traffic, and conserves bandwidth during tactical operations
Scalable Edge and Cloud Deployment	Supports seamless deployment of services closer to data sources	Reduces latency and improves decision-making speed, enhancing operational efficiency



USF 2.7.0
ast 5G Core
entication Server Function\) in the 5G chitecture handles authentication\,...
OWNER Open5gs

Open5gs BSF 2.7.0
REMOTE: AKS East 5G Core
The BSF \(Business Support Function\) is a component responsible for providing support services such as...
CAPABILITY 5G Core
OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs Mongodb 5.0.10-de...
REMOTE: AKS East 5G Core
MongoDB USed for storing 5G Devices
CAPABILITY 5G Core
OWNER Open5gs
API ENDPOINT None
4 mTLS/TCP

MF 2.7.0
ast 5G Core
lanagement Function manages ment\, modification\, and release\,...
OWNER Open5gs

Open5gs UDM 2.7.0
REMOTE: AKS East 5G Core
UDM \(User Data Management\) is a core element of 5G networks\, tasked with managing subscriber data...
CAPABILITY 5G Core
OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

Open5gs UDR 2.7.0
REMOTE: AKS East 5G Core
UDR \(User Data Repository\) is a pivotal component within 5G networks responsible for storing and...
CAPABILITY 5G Core
OWNER Open5gs
API ENDPOINT None
4 mTLS/HTTP

ast 5G Core
that paints a high-level picture of
OWNER greymatter.io

Edge 1.11.0
REMOTE: AKS East 5G Core
Handles north/south traffic flowing through the mesh.
CAPABILITY Mesh
OWNER greymatter.io
API ENDPOINT https://east-5g-core.demo.greymatter.io/
1 TLS/HTTP

Greymatter Prometheus v2.48.1
REMOTE: AKS East 5G Core
Prometheus TSDB for collecting and querying historical metrics.
CAPABILITY Mesh
OWNER greymatter.io
API ENDPOINT https://east-5g-core.demo.greymatter.io/services/pr
2 mTLS/HTTP

eduler 2.8.2
ast Spire
g Service
OWNER Airflow

Airflow Web 2.8.2
REMOTE: AKS East Spire
Airflow Web UI
CAPABILITY Web UI
OWNER Airflow
API ENDPOINT https://airflow.demo.greymatter.io/
4 mTLS/HTTP

Airflow Worker 2.8.2
REMOTE: AKS East Spire
Airflow Worker
CAPABILITY None
OWNER Airflow
API ENDPOINT None
4 mTLS/HTTP

ge 1.11.3
ast Spire
he Chat Bot
OWNER Chat

Control 1.11.13.10.2
REMOTE: AKS East Spire
Manages the configuration of the greymatter data plane.
CAPABILITY Mesh
OWNER greymatter.io
API ENDPOINT https://east-spire.demo.greymatter.io/services/contr...
1 HTTP

Sense 6.6.2
REMOTE: AKS East Spire
A user dashboard that paints a high-level picture of the mesh.
CAPABILITY Mesh
OWNER greymatter.io
API ENDPOINT None
2 mTLS/HTTP

ernal Ingress 1.11.3
ast Spire
o Azure OpenAI
OWNER Openai

OpenAI Connection 1.10.2
REMOTE: AKS East Spire
Connection to Azure OpenAI
CAPABILITY none
OWNER Openai

greymatter Prometheus v2.53.0
REMOTE: AKS East Spire
Prometheus TSDB for collecting and querying historical metrics.
CAPABILITY Mesh
OWNER none

Edge v1.10.2
✓ TLS ✓ mTLS ✓ SPIRE ✓ FIPS
Filters Health Security
4 - High Impact

SPIRE
75/75 Instances Connected
100% Successful Updates
Instance edge-698bd78c98-4s822
34 mins
1:26 PM Last Certificate Update
Valid Until 2:26 PM

TLS TRAFFIC
All Traffic

→ INCOMING TRAFFIC
0.0.0.0:10908 ✓ TLS

TLS SECURITY

TLS Versions	TLSv1_2 TLSv1_3
Cipher Suites	ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384
ECDH Curves	P-256

TLS VALIDATION

Allow Expired Certificates	No

Zero Trust That You Can See

With security at the forefront, Greymatter's zero trust model ensures that communications, both internal (east-west) and external, are encrypted and verified. Automated certificate management and mTLS cryptographic handshakes secure every transaction, using compliant NIST and FIPS standards to guarantee robust protection for data services, APIs, AI modules, and user-facing applications. This is critical for operations where security breaches are not an option.

Key Points:

1. **Real-time zero trust visibility** enables admins to quickly detect, verify, and address threats, reducing the risk of undetected breaches.
2. **Automated certificate management** and cryptographic handshakes reduce human error and eliminate manual intervention.
3. **Granular resource level policy enforcement** is crucial for managing security risks in Cloud/MPN/MEC environments.

Features, Advantages, & Benefits for Zero Trust

Feature	Advantage	Benefit
Zero Trust Security Model used on DoD IL2 – IL6+ environments	Secures all communications with end-to-end encryption	Protects against unauthorized access and cyber threats
Automated Certificate Management	Automates the issuance and renewal of encryption certificates	Ensures continuous, secure communication without manual intervention
Advanced Telemetry and Analytics	Provides real-time insights into network performance and security	Enables proactive threat mitigation and optimized data routing

Achieving Zero Trust Connectivity Objectives

Let's review how Greymatter directly supports Zero Trust Service Connectivity objectives with its resilient architecture, optimized data routing, and military-grade security.

Enterprise Objective	How Greymatter Meets the Objective	Benefit to DoD and IC Missions
Resilient Network Operations from Cloud to DDIL Environments	Decentralized control plane ensures continuous operation and edge processing.	Enables uninterrupted mission-critical operations in disconnected environments.
Efficient Zero-Trust Networking Overhead Management	Fleet-wide playbook management and dynamic service discovery optimize routing and minimize traffic.	Maximizes bandwidth efficiency, supporting fast decision-making in constrained conditions.
Workload Optimization & Flooding Prevention	Safeguards against message flooding, request storms, and single points of failure.	Prevents network congestion, ensuring reliable data flow in mission scenarios.
Access Command and Control	Integrated NGAC for controlled data service, APIs, and application access across classifications.	Enhances security by preventing unauthorized access to classified information.
Dynamic Traffic Routing and Prioritization	Network-aware routing with dynamic prioritization based on mission needs.	Ensures timely delivery of critical data in bandwidth-constrained environments.
Real-Time Policy Engine via Mission Playbooks	Policy engine supports using mission playbooks for real-time system adjustments.	Enhances agility to adapt to changing mission needs quickly.
Secure Data Sharing Across Classification Levels	Automated, explicit Zero Trust connectivity with end-to-end encryption.	Enables seamless, secure collaboration across DoD and IC networks.
Monitoring and Reporting	Advanced telemetry that can enabled geo-fencing capabilities for data sovereignty compliance.	Provides visibility and compliance for data service network and security operations.
Integration with Government Authentication Systems	Supports multiple DoD authentication methods for secure access to a single service to include PKI and Auth tokens.	Strengthens operational security by aligning with government standards.
Multicloud and MPN Support	Seamless integration with multicloud, hybrid, and 5G enabled MPNs.	Ensures flexible, scalable deployment in any network environment, including tactical and battlefield contexts.

A Trusted Partner for Civilian, DoD, and the IC Organizations

Greymatter is uniquely positioned to meet Civilian, DoD, and the IC Enterprise requirements for secure, resilient, and efficient zero trust networking operations from Cloud to DDIL environments. By providing a robust, zero trust, and distributed connectivity platform, Greymatter empowers Enterprise's to meet their mission-critical objectives with confidence, without the need to build "yet another data system". Its compatibility with existing architectures makes it a seamless addition to any deployment.

Learn more at https://greymatter.io or visit us on the Tradewinds Marketplace.

Greymatter.io

CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICE
AWARDABLE
TRADEWINDS SOLUTIONS MARKETPLACE

carahsoft®

Chris Holmes
CEO
703-772-0862
chris.holmes@greymatter.io

Honey Elias
COO
honey.elias@greymatter.io