Greymatter.io

Greymatter 101: Zero Trust Networking Platform

Mission Success Through Automation, Security, and Observability

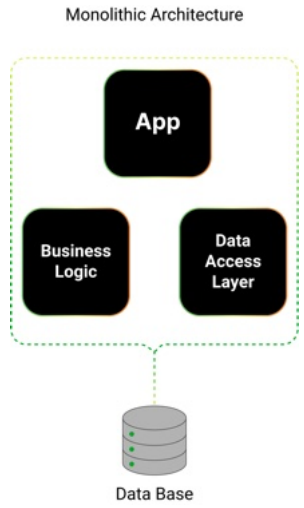


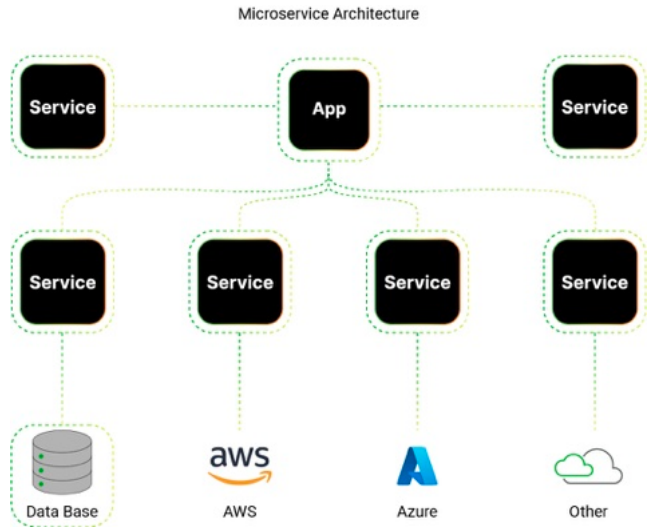
Greymatter.io | Trusted by Mission Critical Enterprises

©Greymatter.io

Understanding Containers & Microservices

- **Monolithic Applications: A Unified but Rigid Architecture**
  - A single, large machine where all components (UI, business logic, data access) are tightly connected. If one part fails, the whole system may stop.
    - **Simple but Inflexible** – Monolithic applications are easier to develop and deploy as a single unit but harder to scale and maintain due to tight coupling.
- **Containers: Standardizing Application Environments**
  - Containers are lightweight, self-contained software packages that include an application and all its dependencies, ensuring consistency across different environments. They:
    - **Consistent and Efficient** – Containers ensure reliable deployments across environments, enable rapid scaling, and reduce compatibility issues.
- **Microservices: Decoupling for Scalability and Resilience**
  - A team of smaller, independent machines (services), each handling a specific task (e.g., user service, payment service). If one fails, others keep running, enhancing flexibility and resilience.
    - **Scalable, Flexible, and Resilient** – Microservices enable independent scaling, faster updates, and improved fault isolation while allowing teams to use different technologies for optimal performance.
- **Key Points**
  - 93% of organizations currently use or plan to deploy containers in production, driving efficiency, scalability, and portability across cloud and on-prem environments.
  - 85% of large organizations (5,000+ employees) use microservices for agility and scalability.

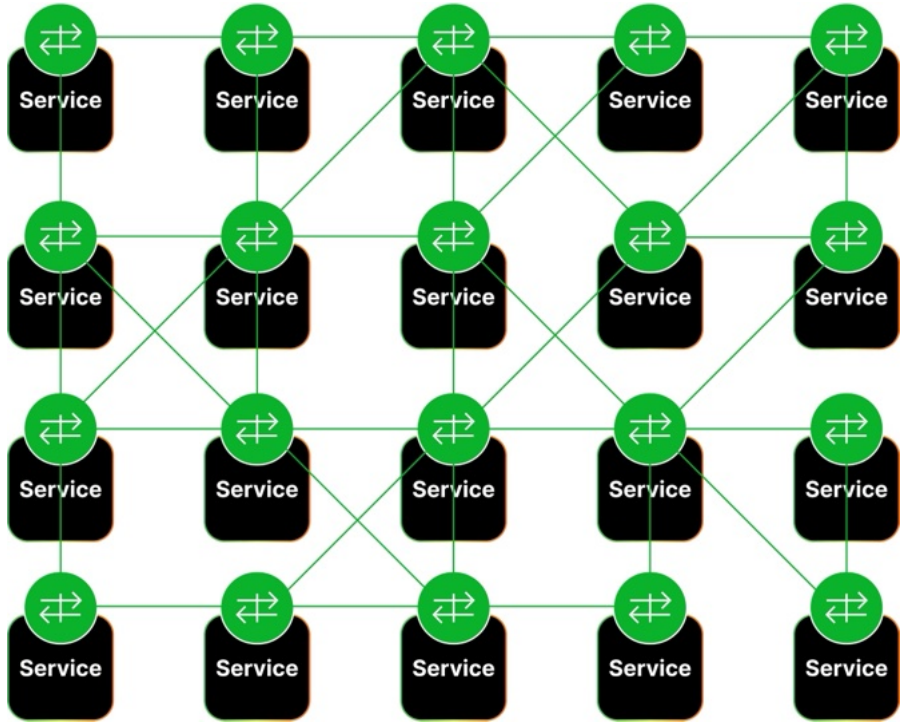




©Greymatter.io

The Role of a Service Mesh

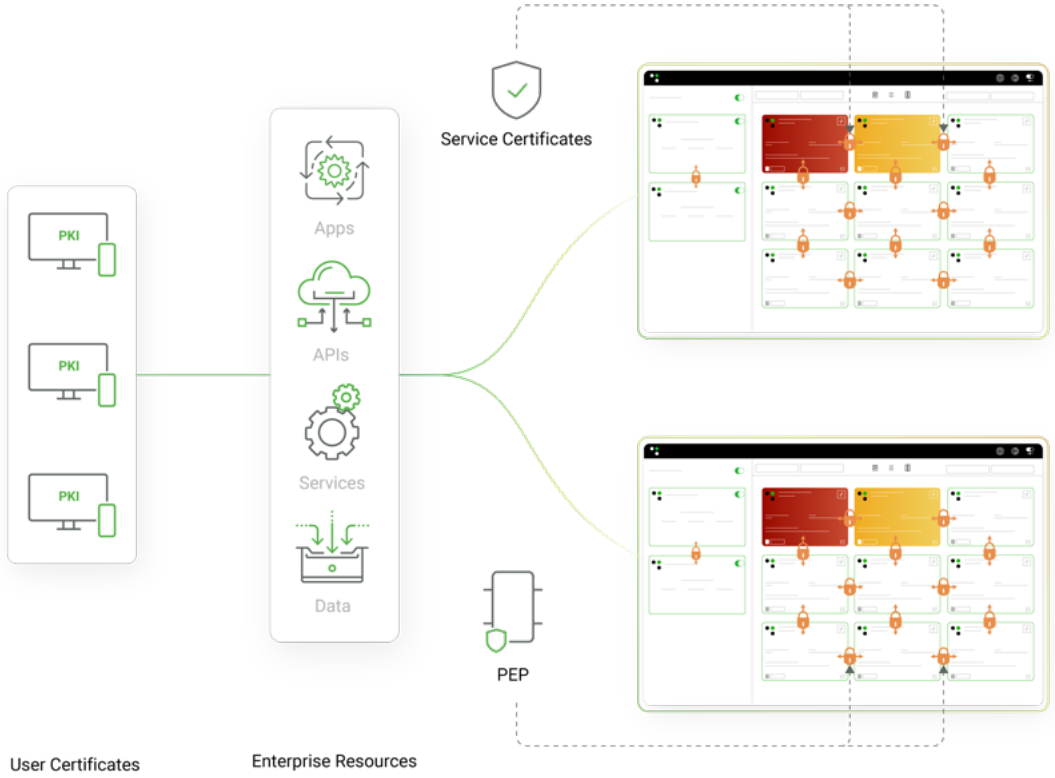
- **Definition:** A dedicated infrastructure layer that manages service-to-service communication in a microservices architecture, acting like a traffic controller.
- **Key Functions**
  - **Secure Communication:** Protects data between services with encryption.
  - **Reliability:** Ensures smooth operation despite failures.
  - **Observability:** Provides visibility into service performance.
- **How It Works**
  - Lightweight proxies (sidecars) are deployed alongside each microservice.
  - These proxies mediate all communication, enforcing security and collecting metrics.
- **Key Points**
  - **Service Mesh Adoption** – 85% of microservice adopters now use a service mesh for managing service-to-service communication, enhancing scalability and security.



©Greymatter.io

Addressing Microservices Challenges with a Service Mesh

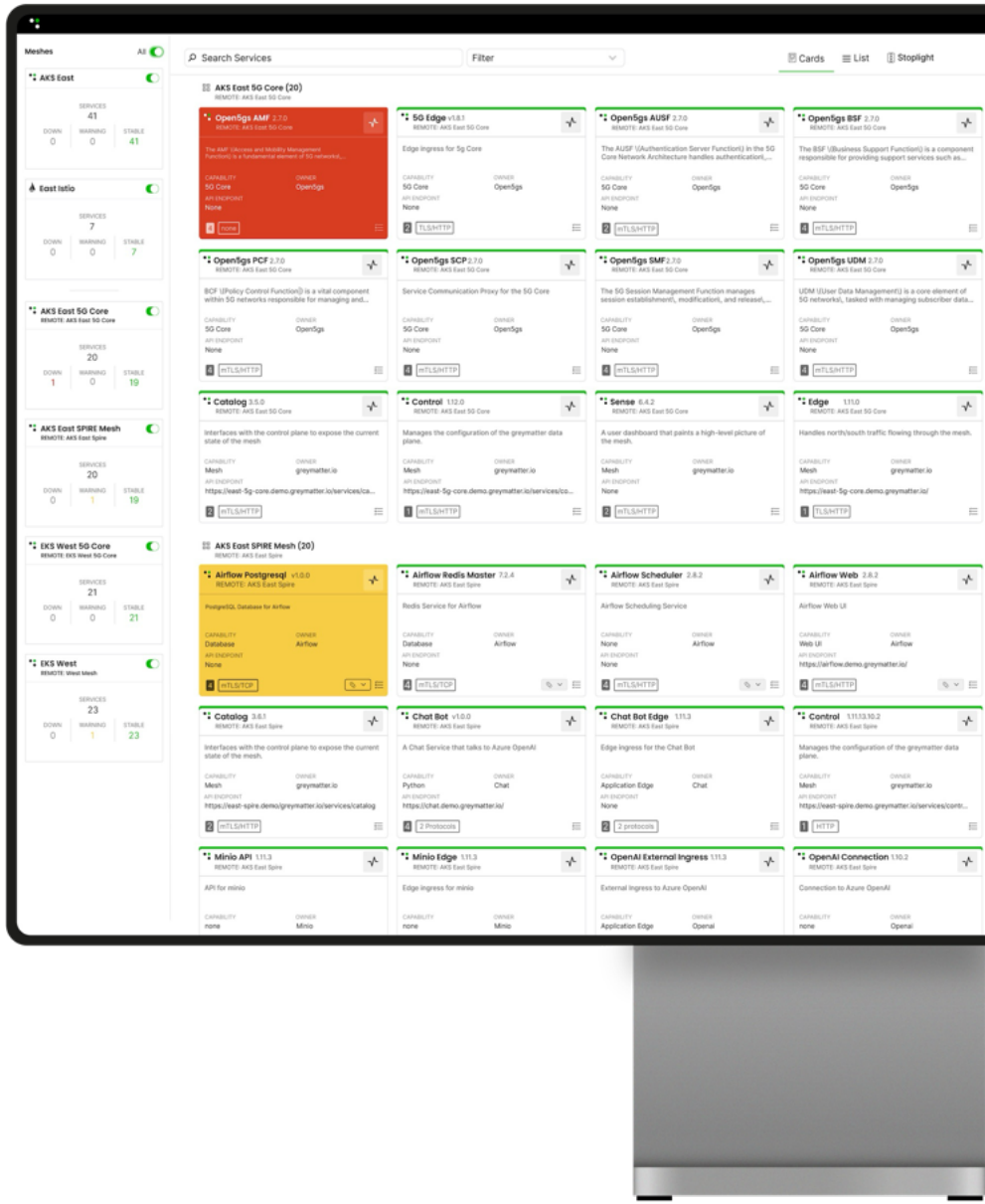
- **Challenges of Microservices**
  - **Communication Complexity:** Managing numerous service-to-service calls becomes a "spaghetti" mess.
  - **Security & Zero Trust:** Internal calls need authentication; perimeter security isn’t enough.
  - **Observability:** Hard to pinpoint issues without a holistic view of interactions.
  - **Operational Overhead:** Manual management of deployments and policies is overwhelming.
- **How a Service Mesh Solves These**
  - **Automates Communication:** Handles routing, load balancing, and retries.
  - **Enforces Security:** Implements zero-trust policies (e.g., encryption, authentication).
  - **Provides Visibility:** Collects metrics and traces for real-time monitoring.
  - **Reduces Complexity:** Centralizes networking tasks, freeing developers for business logic.



©Greymatter.io

Introducing Greymatter: A Zero-Trust Networking Platform

Evolving beyond a basic service mesh to enforce zero-trust principles, Greymatter is a comprehensive zero-trust networking platform that automates delivery, enhances service-to-service communication, and enforces security across applications, APIs, databases, AI tools, and more.



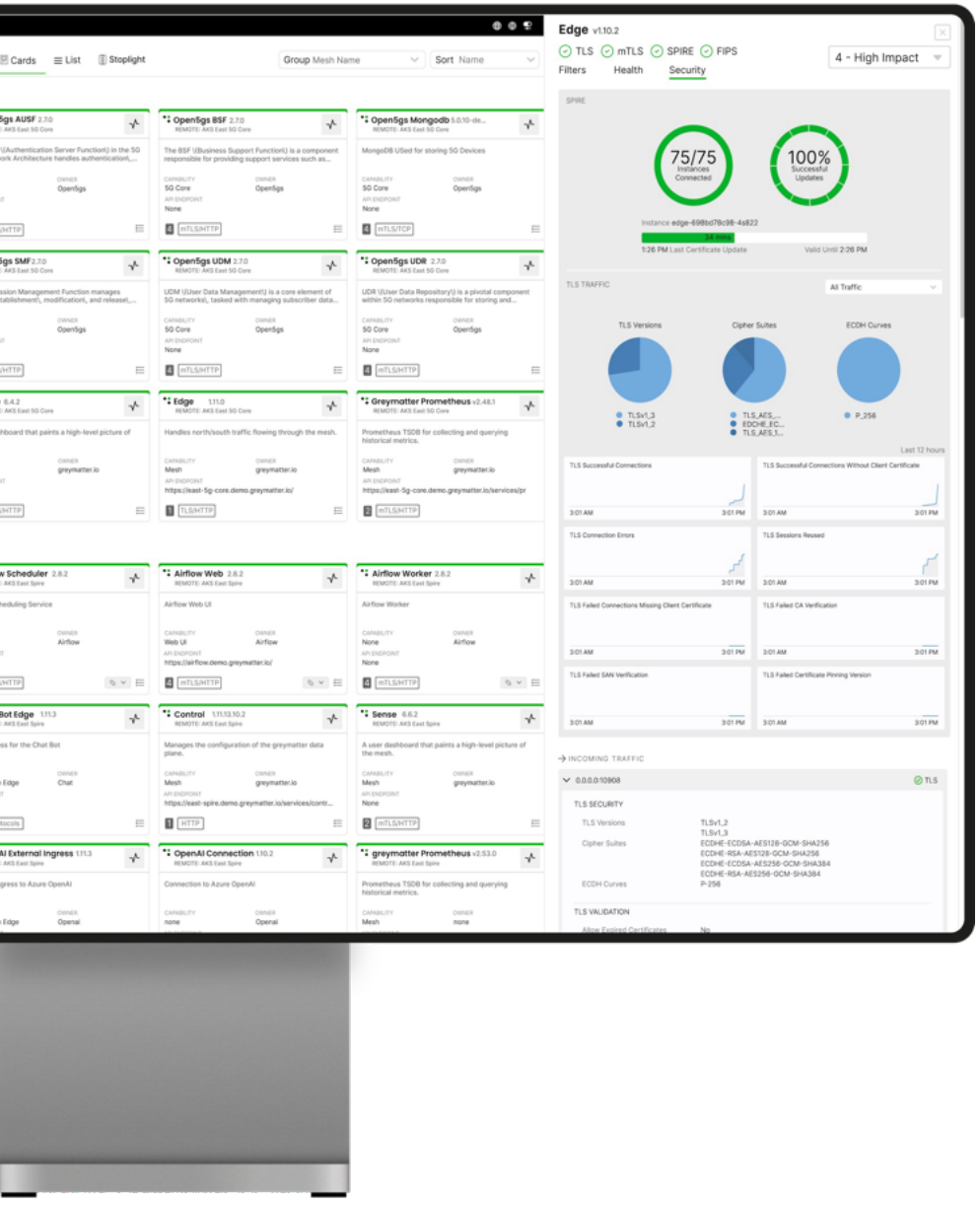
Why Greymatter?

Unlike traditional service meshes, Greymatter integrates advanced zero-trust security policies and governance.

Designed for highly regulated industries and government agencies, ensuring compliance and operational efficiency.

Provides an all-in-one management platform that eliminates the need for multiple networking and security tools.

©Greymatter.io



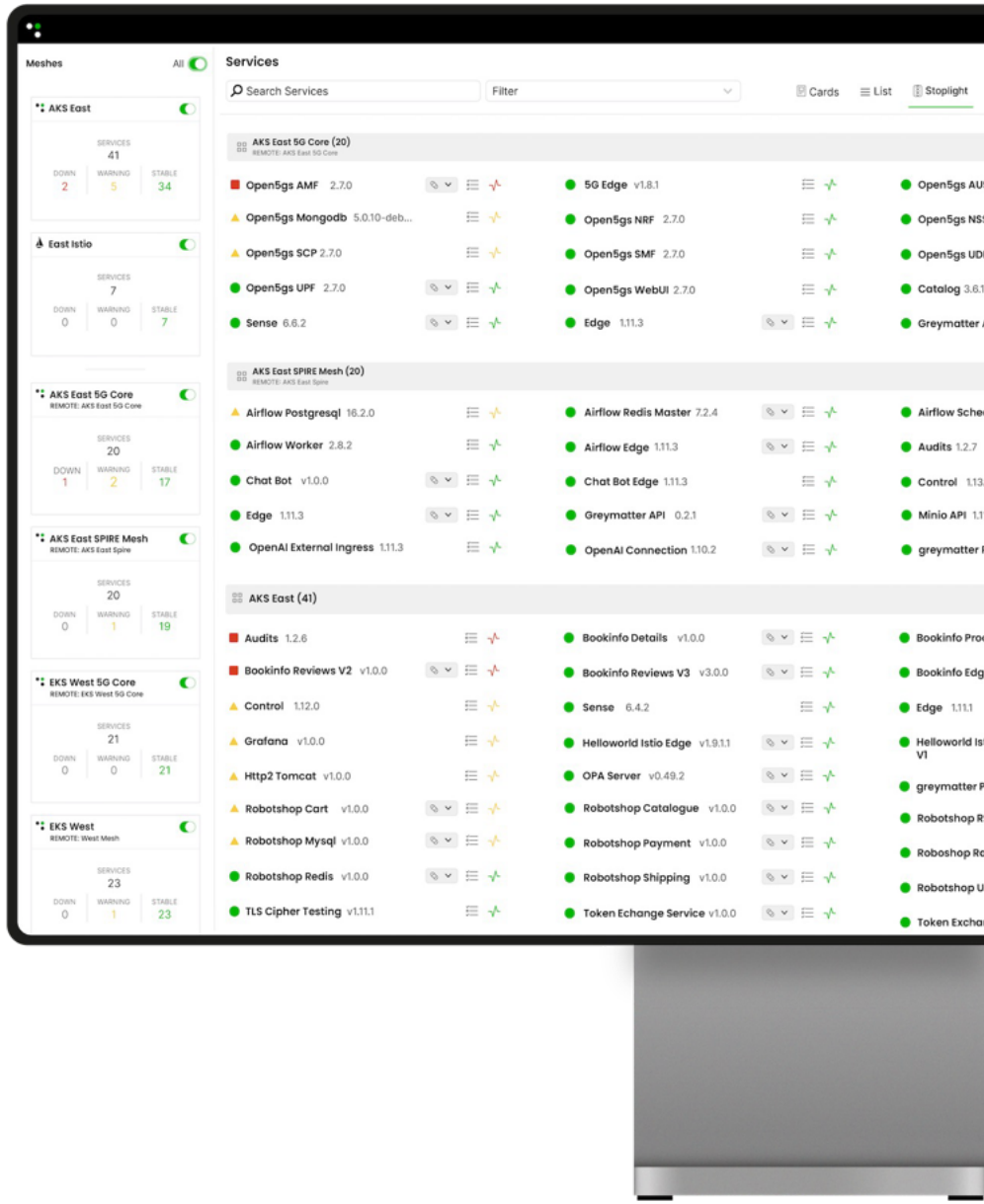
Exploring Greymatter's Core Features

- **Automated, Secure Service Connectivity**
  - Encrypts all traffic with mutual TLS.
  - Automates service discovery, routing, and authentication.
- **Built-in Policy Enforcement & Zero Trust Security**
  - Central policy engine with fine-grained access control.
  - Consistent security across cloud and on-premise environments.
- **Traffic Management**
  - Optimizes flow, supports canary deployments, and prevents overload with circuit breakers.
- **Governance & Configuration Management**
  - Declarative configuration and automated rollback.
  - Native GitOps support for streamlined management.
- **Application Networking Intelligence**
  - Auto-provisions metrics and audit infrastructure.
  - Offers multi-mesh visibility and dependency health checks.
- **Security & Compliance**
  - Meets NIST zero-trust and FIPS 140-2 standards.
  - Built-in forensic audit tracking.
- **Business & Operational Advantages**
  - Superior manageability and native observability.
  - Reduces total cost of ownership by minimizing tool dependency.

©Greymatter.io

Greymatter in Action: Use Cases & Integrations

- **Seamless Kubernetes vendor/container Integration**
- **Unified Zero-Trust Networking:** AWS, Azure, Google, on-premise, legacy systems
- **Government Use Case:** Trusted by U.S. DoD for mission-critical systems (Impact Levels 2-6, ATO certified)
- **Enterprise Use Case:** Simplifies multicloud/hybrid management, MPN, MEC security, and compliance
- **Key Benefits:**
  - Enhanced security with zero-trust
  - Reduced complexity & downtime
  - Cost savings via tool consolidation
  - Better compliance & visibility

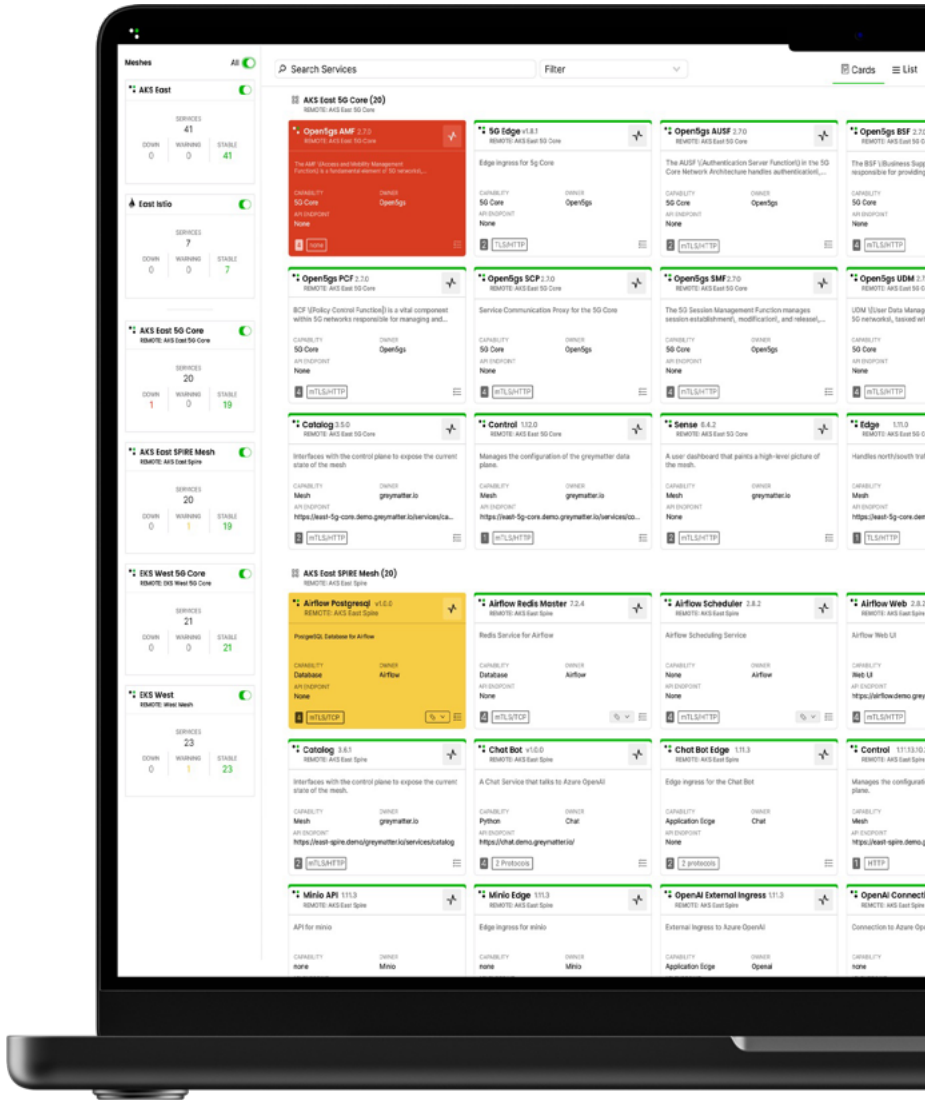


©Greymatter.io

Greymatter.io – A Leader in Zero Trust Networking

Greymatter is a proven ZTN platform trusted by defense and intelligence communities.

- Certified and accredited for DoD Impact Levels 2-6+ and enforcement of NIST ZTA and FIPS encryption standards.
- 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.
- Won the 2024 PAAS Security Solution of the Year from CyberSecurity Breakthrough.
- Recognized twice in Gartner's Hype Cycle Reports for both Enterprise Networking and Zero Trust Networking.



©Greymatter.io

Backup Slides

©Greymatter.io

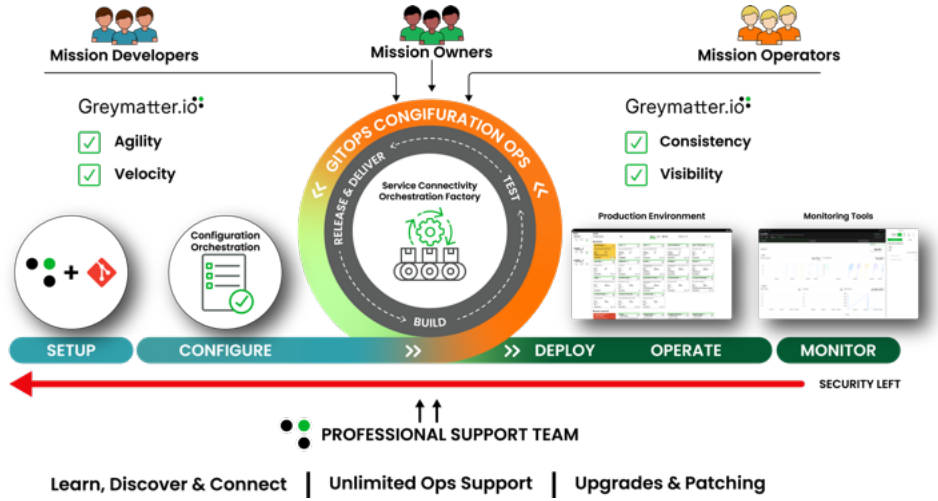
Engineering to Operations – Bridging the Gap

A Real-World Scenario

Technology team transitions new capabilities for customers from dev to ops. Greymatter's playbooks and Canary deployments can streamline the rollout, ensuring uninterrupted support for integration.

Current Challenges

- Response teams struggle to validate updates that are critical for security management, secure protocols, and compliance - delaying capabilities.
- Without user-to-workload transition insights, issues linger undetected, stalling capabilities.
- Manual handoffs without rolling upgrade strategies slow critical mission application readiness



The Greymatter Advantage

Feature	Advantage	Benefit
Greymatter GitOps Playbooks	Automates dev-to-ops transitions	Speeds deployment to production, ensuring security and resiliency
Real-Time Validation via Greymatter Catalog	Confirms system stability	Ensures mission-ready applications, APIs, and services
Canary and Rolling Deployments/Upgrades	Rolls out updates safely, with full support for rollback	Minimizes disruption to analysts

©Greymatter.io

Mission Service Connectivity – Everywhere That Matters

A Real-World Scenario

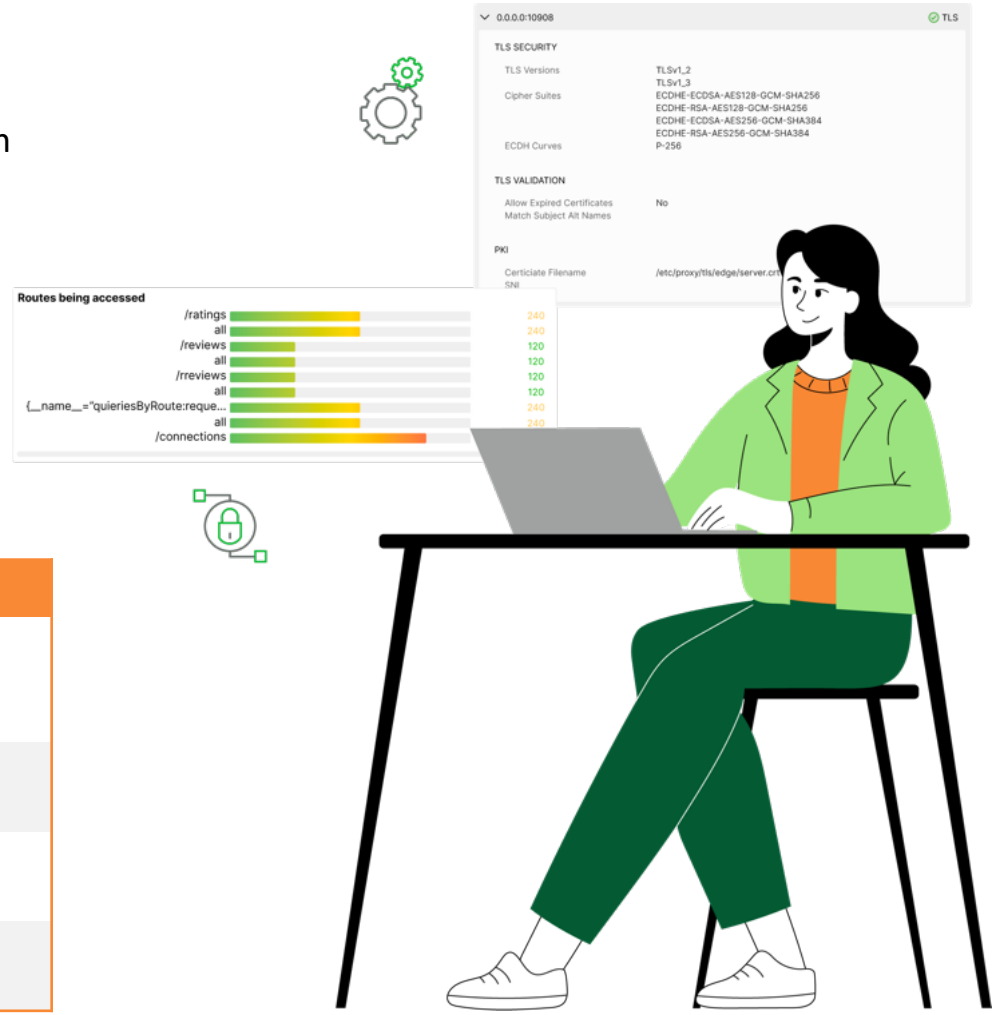
Technology team deploys capability to customers into 5G environments. Greymatter's ZTN management platform ensures security, visibility, and orchestration of applications accessing services from cloud to edge, maintaining connectivity.

Current Challenges

- Manual and disjointed configs delay delivery, impacting business operations and customers.
- Constraints demand automated, scalable, low-overhead solutions.

The Greymatter Solution

Feature	Advantage	Benefit
Playbook-Driven Policy Automation	Enforces dynamic, rule-based access controls to fleet-wide resources	Adapts security to evolving threats in real-time
Continuous Session Monitoring	Tracks user activity across all systems	Detects and stops lateral movement instantly
Automated SIEM/SOAR Integration	Feeds real-time forensic data into security tools	Speeds up detection and response
Least-Privilege Access Control	Restricts access based on contextual policies	Minimizes insider threat exposure



©Greymatter.io

Service Certificate Managment – Compliance and Readiness

A Real-World Scenario

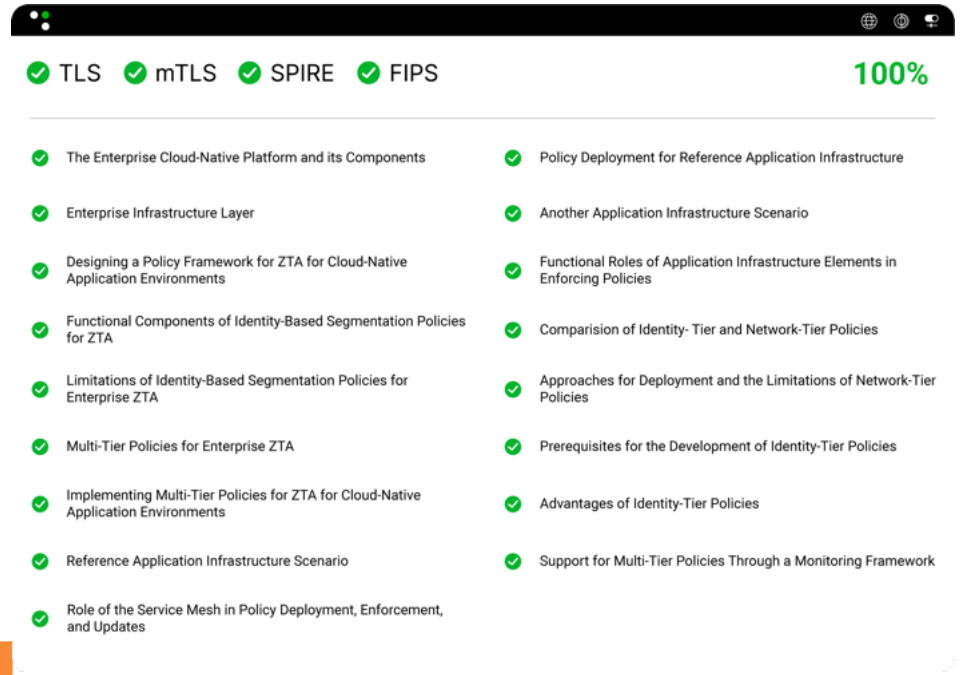
Technology team networks, critical for deterrence against adversary cyber operations, are compromised due to certificate mismanagement. Greymatter's certificate automation and attestation secures every service connection, ensuring compliance with NIST and FIPS standards—vital to the technology operations.

Current Challenges

- Manual certificate management delays updates, leaving systems vulnerable to evolving cyber threats.
- Non-compliance with security standards (e.g., TLS protocols, outdated certificate ciphers) jeopardizes operations and the Zero Trust needs.

The Greymatter Advantage

Feature	Advantage	Benefit
Automated Service Certificates with SPIRE	Automates dev-to-ops transitions	Speeds deployment to production, ensuring security and resiliency
End to end mTLS Encryption both East/West and North/South	Confirms system stability	Ensures mission-ready applications, APIs, and services
NIST/FIPS Compliance	Meets strict government security standards	Ensures regulatory adherence and data integrity



©Greymatter.io

Traffic Management – Resilience Under Pressure

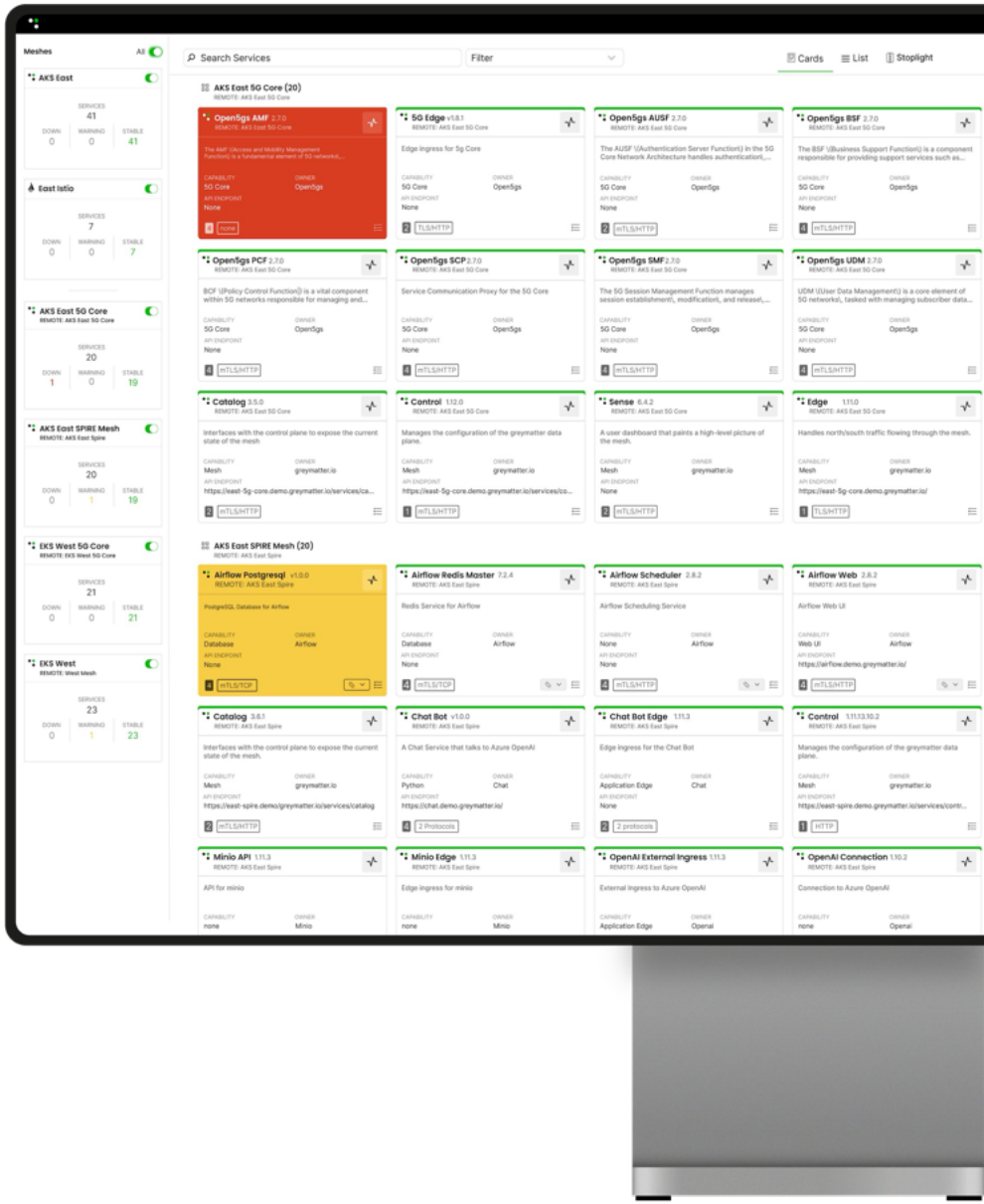
A Real-World Scenario

Customers rely on applications and services to connect and stay online during heavy use periods. Greymatter's traffic management ensures seamless data flows across multi-cloud systems, maintaining operations tempo.

Current Challenges

- Heavy data loads strain multi-cloud networks and applications, risking delays in customer support and troubleshooting.
- Manual traffic routing without an ability to coordinate workload level assets slows critical updates, especially under budget constraints.
- Disparate systems hinder rapid dissemination.

Feature	Advantage	Benefit
Automated Load Balancing	Optimizes application, APIs, and Data traffic across clouds	Ensures timely delivery via prioritized workloads
Global Traffic Management	Routes data efficiently via Envoy	Boosts mission resilience
Management Playbooks	Simplifies configs 50% vs. legacy and enforces NIST/FIPS security and monitoring	Reduces overhead for CIO technical teams and security teams



©Greymatter.io

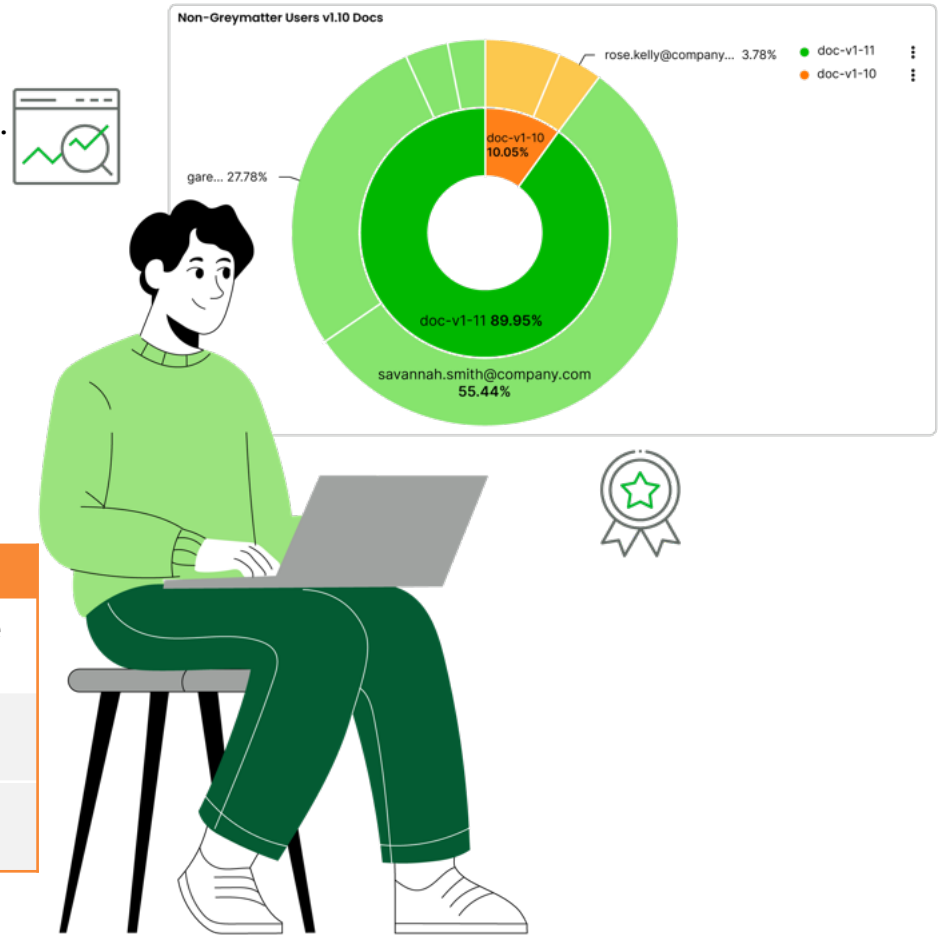
Observability – Visibility for Decision-Making

A Real-World Scenario

Delivery team initiatives integrate disparate capabilities for customer provided activities. Greymatter's observability provides real-time usage insights across systems, ensuring effective decision-making enabling appropriate budgeting activity.

Current Challenges

- Customer need instant visibility into activity flows to support operational tempo.
- Siloed tools obscure system performance, slowing mission analysis.
- Resource constraints limit manual monitoring, risking missed insights.



The Greymatter Advantage

Feature	Advantage	Benefit
Comprehensive Audit Trails	Tracks every access, download, and transfer	Provides clear forensic evidence for investigations
Enterprise Security Integration	Integrates directly with SIEM/SOAR systems	Speeds up threat detection and response
Real-Time Telemetry	Tracks application, API, and service usage end-to-end	Optimizes mission support efficiency

©Greymatter.io

Proactive Operations – Seeing the Threat Before It Happens

A Real-World Scenario

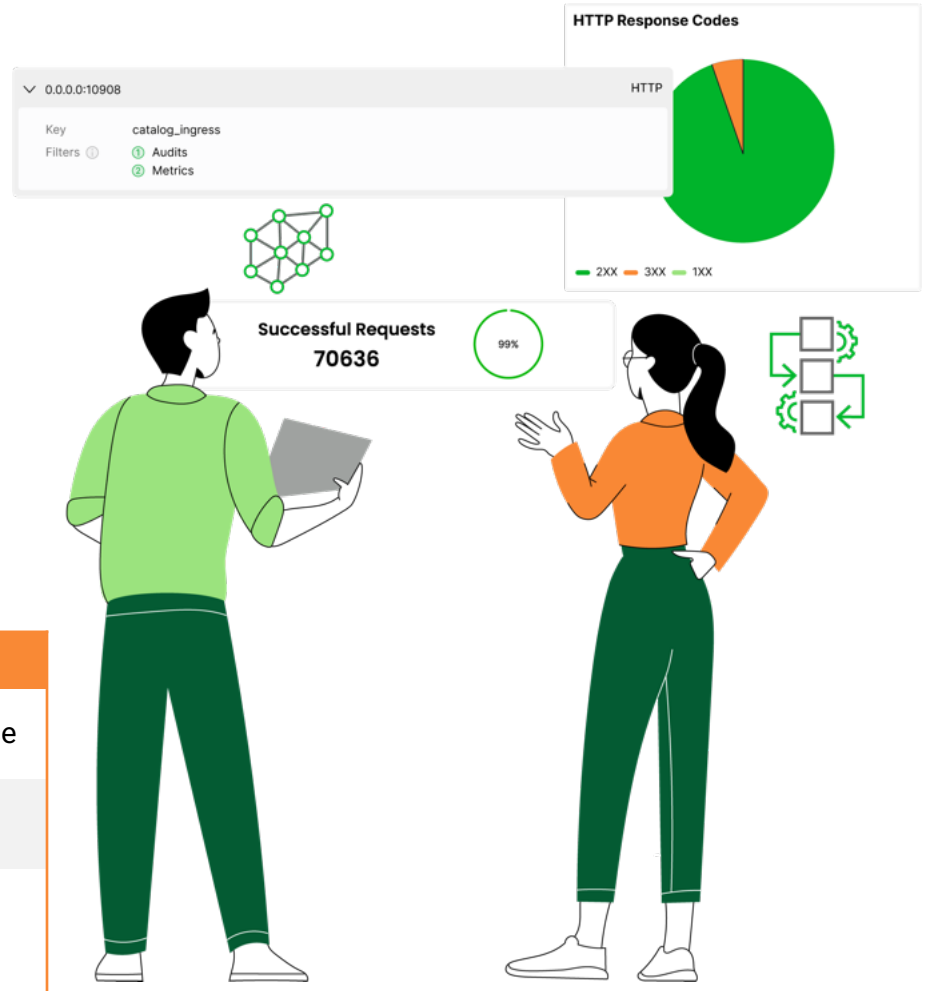
An internal employee with authorized access slowly exfiltrates sensitive data, blending in with routine activity. Security teams rely on SIEM/SOAR tools to detect anomalies, but without unified enforcement, they struggle to respond quickly.

Current Challenges

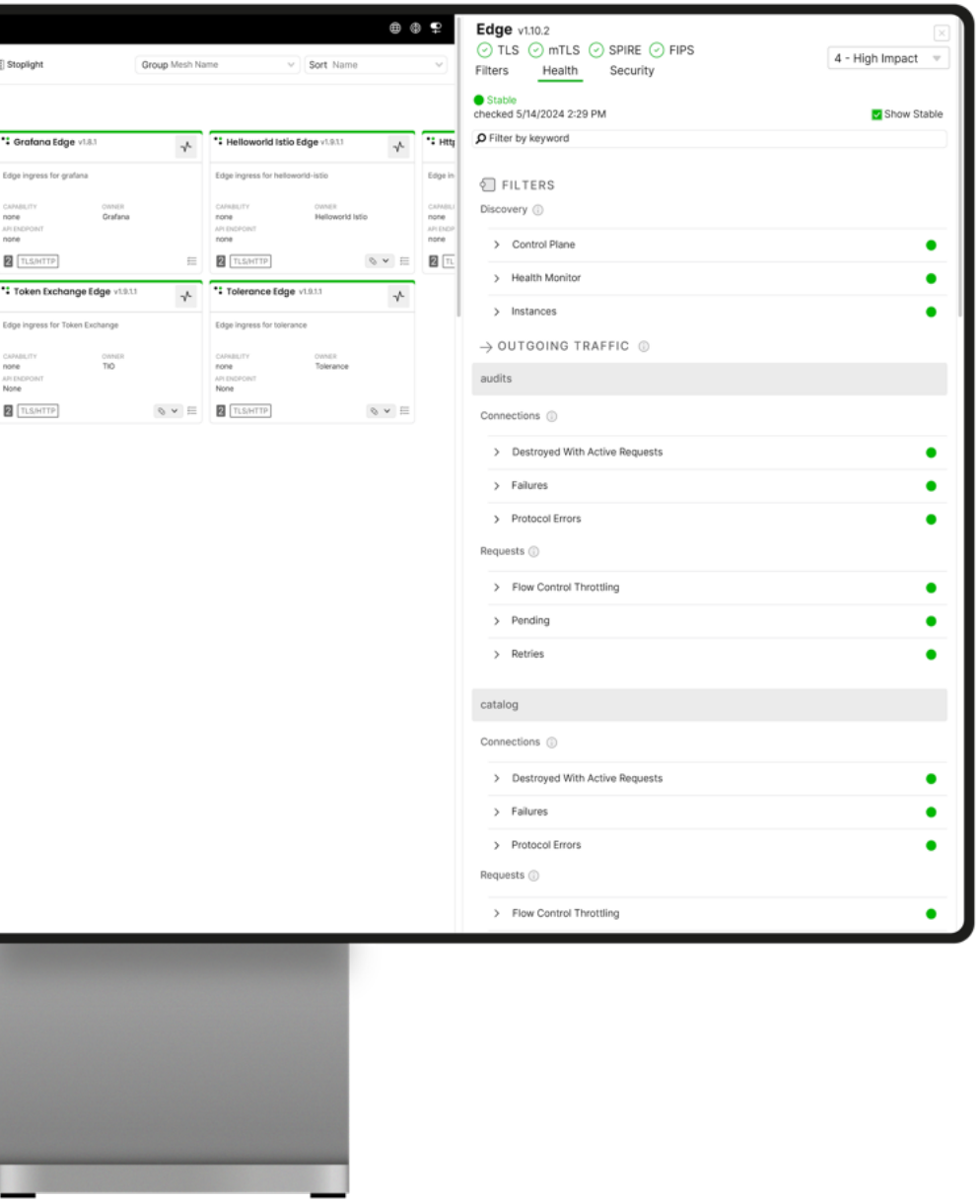
- Disparate systems and manual controls hinder rapid adjustments, stalling business operations support under budget strain.
- Without user-to-workload traffic mappings, response teams face slowdowns, obscuring critical updates until too late.

The Greymatter Advantage

Feature	Advantage	Benefit
Fleet-Wide Playbook Enforcement	Instantly applies security policies across all resources	Enables real-time threat response
Distributed Workload PEP/PDP Policy Control	Deploys updates to every Greymatter-protected service	Reduces manual effort and response time
Seamless Analytics Integration	Feeds enriched audits and telemetry into existing AI and Reporting tools	Enhances threat detection and automated workflows
Zero Trust Data Plane Enforcement	Verifies and restricts access at the workload level	Prevents unauthorized activity before it spreads



©Greymatter.io



The Greymatter Advantage – Value in Context

Greymatter aligns with 2025 Enterprise priorities and long-term realities.

- **Business Readiness:** Secures applications, APIs, AI modules, and data services across clouds and deployments through repeatable Playbook management.
- **Cost Efficiency:** Increases speed of delivery, while cutting operational overhead through automation.
- **Lasting Security:** Locks down every service, manages ephemeral certificate and enforces protocol encryption best practices.

Enterprise-Ready ZTN: Automate, Secure, Observe

Greymatter drives Enterprise success with fast automation, top security, and full visibility. It streamlines ops, protects critical systems, and keeps you in control—no weak spots, just readiness.

©Greymatter.io

Thank you



Chris Holmes

CEO

Greymatter.io

chris.holmes@greymatter.io



Jonathan Holmes

CTO

Greymatter.io

jon.holmes@greymatter.io



Honey Elias

SVP | Operations

Greymatter.io

honey.elias@greymatter.io

©Greymatter.io