Secure Decentralized Software Applications Faster

As software modernization proliferates across large enterprises and government agencies, cloud applications have become one of the largest attack surfaces compromised by cybercriminals, leading to record numbers of security breaches, data exfiltration, and ransomware attacks.

Greymatter.io provides a service connectivity layer platform that helps organizations automatically address common software vulnerabilities, such as broken access control policies and security misconfigurations, as well as encryption, identification, and authorization failures. DevOps teams depend on our platform to meet CISO and CIO requirements along with industry regulations to harden distributed software applications that bridge legacy, on-premise IT infrastructure with hybrid/multi-cloud environments.

Ensure only the right users can access the right assets and resources across decentralized software applications with our built-in zero-trust architecture.

Enable mTLS authentication and end-to-end encryption of all internal service-to-service communication, external APIs and data flows across any environment

Demonstrate compliance with industry regulations automatically with comprehensive audit trails of every user, system, and transaction across the entire application.

Add Military-Grade Application Security

Founded outside Washington, D.C. in 2015, Greymatter.io is widely deployed worldwide throughout mission-critical defense and intelligence environments. Our platform is purpose-built with military-grade security that meets or exceeds any enterprise use case, allowing developers to focus on business logic, not security requirements.

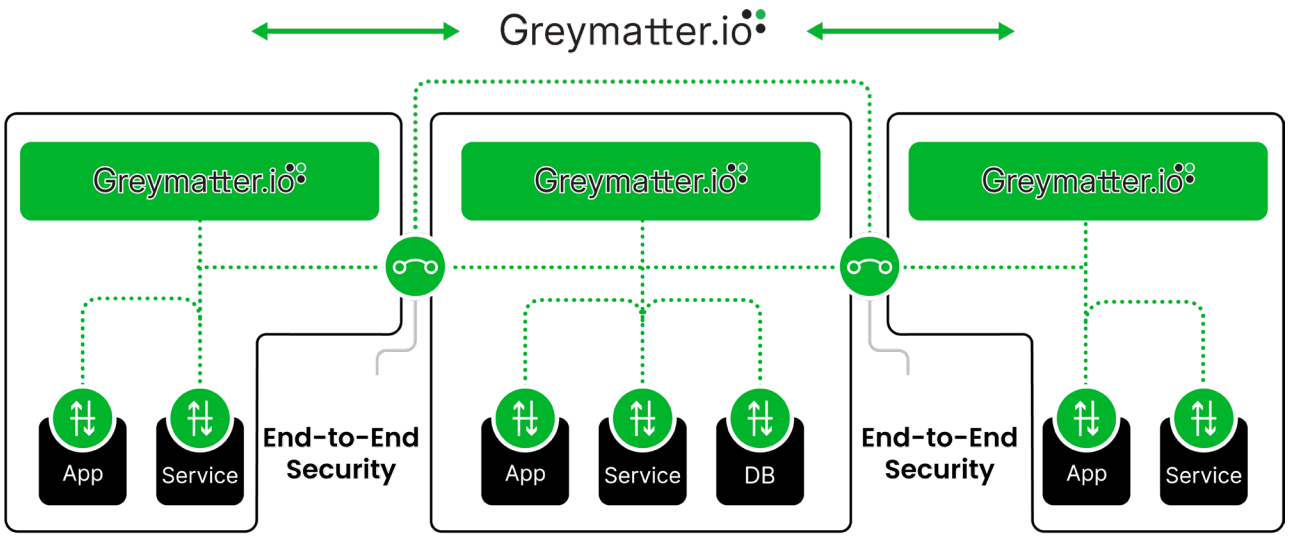
This service connectivity layer abstracts security away from developers into one central control plane that allows DevOps teams to enforce policy and configuration changes across a data plane of Envoy proxies connected to each individual microservice.
Our secure application development framework enables zerotrust security, user authentication, data encryption, certificate rotation, and policy compliance out of the box without writing a single line of code.

“Impact Level 6 (IL6+) Accredited”

“Commercial Cloud Enterprise (C2E)-Ready”

“Compliant with 92% of Zero-Trust Architecture criteria”
NIST 800-207

Authenticate and Authorize Across Environments



K8s
AWS, Azure, Google, etc.

Cloud Provider
AWS, Azure, Google, etc.

On-Premise
VMWare, etc.

Greymatter.io

Cyber Mesh

Enables distinct security services to work together to create a dynamic security environment, through:

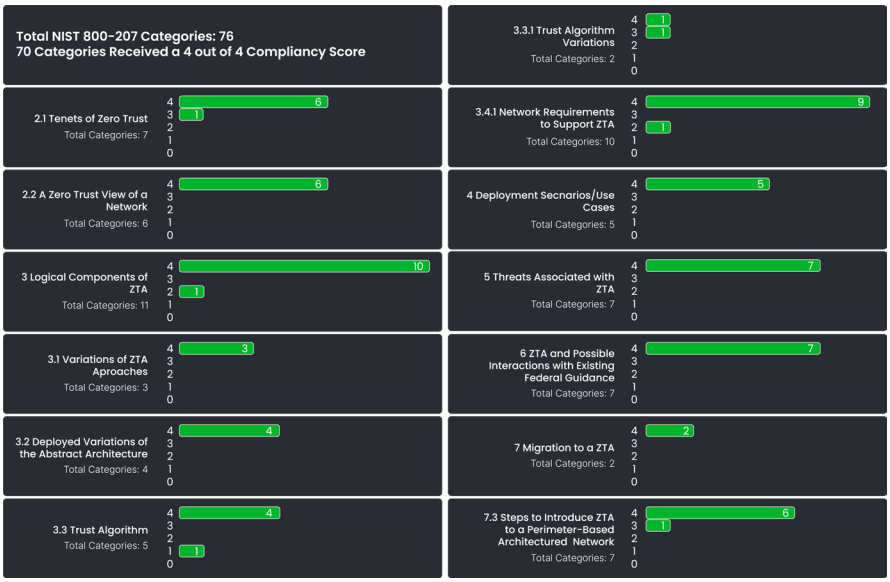
- Auditing
- Enforcement
- Policy Info & Decisions
- Token Management
- IAM Integration
- NPE Management
- Micro-segmentation
- Certificate Rotation

Security

- Zero-Trust Network Access
- Role-Based Access Control
- Attribute-Based Access Control
- Next-Gen Access Control
- User Authentication
- Identity Management
- End-to-End Data Encryption
- Traffic Splitting
- Circuit Breaking

Compliance

- FIPS
- PCI
- HIPAA
- GDPR
- And more ...



Authenticate and authorize users, services, and data to secure, manage and govern user-toservice and service-to-service communications across decentralized software applications.

Why Greymatter.io?

Enable Data Encryption Out of the Box

Enable complete Mutual Transport Layer Security (mTLS) authentication and end-to-end encryption of all service-to service communication, external APIs, and disparate datasources in transit across any environment. Organizations can also wrap Kubernetes environments with a service mesh to encrypt data and prevent security misconfigurations.

Secure, Manage & Govern All App Traffic

Assign individual identities to every user, service, or data source to provide organizations with granular role-based, attribute-based, and next generation access control to authenticate and authorize user-to-service and service to-service communications for every transaction. Implement micro segmentation policies across all North South and East/West traffic to reduce the blast radius of potential data breaches.

Audit and Enforce Policy Compliance

We help organizations in regulated industries enforce compliance with FIPS, PCI, HIPAA, GDPR, and other regulations by creating, managing and viewing policies for every transaction across the application network. This comprehensive audit trail provides granular, network layer detail to support GRC initiatives, verify compliance, and streamline audit processes. Our platform also captures, analyzes, and integrates more than 100+ metrics and analytics data with SIEM, SOAR, EDR, and other security systems.

Our Technology Partners

aws · Red Hat · Microsoft · Istio · CLOUD NATIVE COMPUTING FOUNDATION · envoy · Open Policy Agent · spiffe · SPIRE · CONFLUENT · KEYCLOAK

4201 Wilson Blvd, 3rd Floor, Arlington, VA 22203
www.greymatter.io | info@greymatter.io
(887) 356-3011