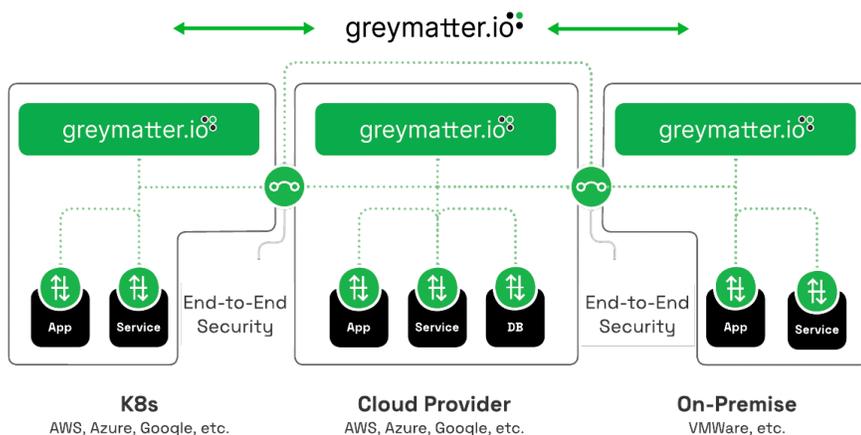


## Secure Decentralized Software Applications Faster

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 an enterprise application networking 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.

## 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 mesh infrastructure 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 zero-trust security, user authentication, data encryption, certificate rotation, and policy compliance out of the box without writing a single line of code.



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



### Implement Zero-Trust

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



### Encrypt All App Data

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



### Enforce Compliance

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

“Impact Level 6 (IL6+) Accredited”

“Commercial Cloud Enterprise (C2E)-Ready”

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

## Enable Data Encryption Out of the Box

Because modern software applications are distributed across multiple cloud, container, and on-premise environments, developers must protect application data from being exposed to attackers across every endpoint. Our platform enables complete Mutual Transport Layer Security (mTLS) authentication and end-to-end encryption of all service-to-service communication, external APIs, and disparate data sources 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

Greymatter.io provides software architects with the ability to secure, manage, and govern traffic patterns across all running services in any environment. Our platform assigns 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

Greymatter.io helps organizations in regulated industries, such as banking, finance, insurance, healthcare, telecom, and oil and gas 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.

## 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 ...



The greymatter.io platform is compliant with 92% of the NIST Special Publication 800-207 criteria for Zero-Trust Architecture to ensure the security of decentralized software applications.

## Technology Partners:

