Greymatter.io

Zero Trust Networking Made Enterprise Ready

Common Use Cases in Securing Service Orchestration for Cloud, Hybrid, and Edge Networks

From A to ZTN: Covered from Cloud to Edge

Global enterprises are rapidly adopting Zero Trust Networking (ZTN) to stay ahead in securing their dynamic environments from Cloud to Edge. The Cloud Security Alliance reports that 80% of organizations have made ZTN a priority, recognizing it as critical for safeguarding against rapidly evolving threats. However, most are still struggling to fully integrate Zero Trust into their infrastructure and complex service orchestration layers, underscoring the urgency for faster, more decisive action to close security gaps. [1]

Greymatter.io's platform revolutionizes service orchestration by seamlessly integrating ZTN best practices. Our expertise in defense and intelligence sectors allows us to offer a solution that addresses the unique challenges faced by these organizations. Let's explore common use cases to illustrate how Greymatter.io tackles ZTN challenges.

ZTN Use Cases Covered

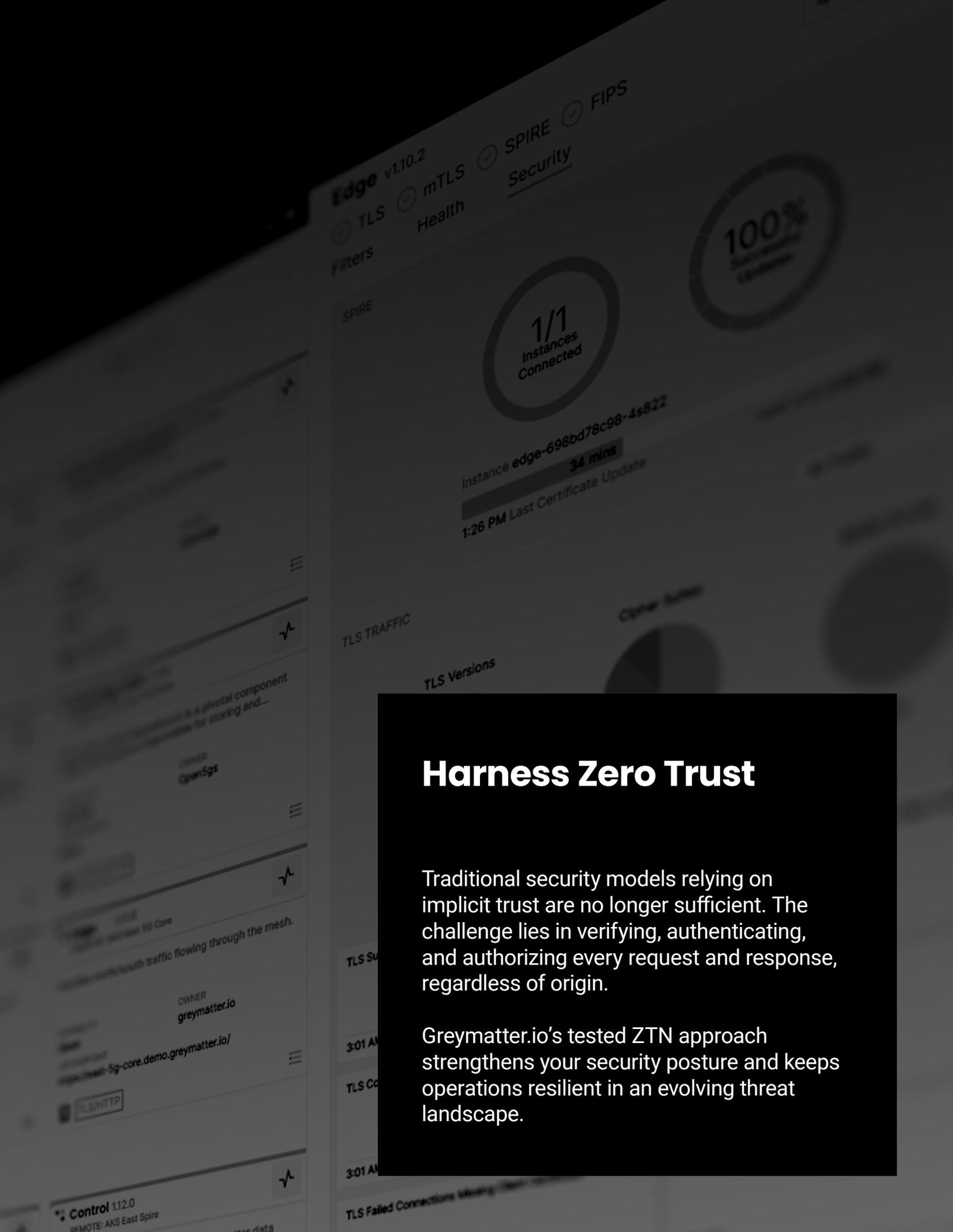**03** Harnessing Zero Trust

04 Transform Security Operations

05 Achieving Stringent Protocols

06 Surpassing Strict Standards

07 Automate Secure Connectivity

08 Orchestrating Security Playbooks

1 - https://cloudsecurityalliance.org/press-releases/2022/06/06/eighty-percent-of-it-and-security-professionals-list-zero-trust-as-a-priority-according-to-new-cloud-security-alliance-survey

Harness Zero Trust

Traditional security models relying on implicit trust are no longer sufficient. The challenge lies in verifying, authenticating, and authorizing every request and response, regardless of origin.

Greymatter.io's tested ZTN approach strengthens your security posture and keeps operations resilient in an evolving threat landscape.

Transform Security Operations

Challenge

Without a robust ZTN platform, operations risk exposure to security breaches, compromised data, and to operational disruptions. In contrast, organizations that implemented ZTN saw an 80% reduction in successful cyber attacks by minimizing their attack surface, according to a survey by Microsoft. [2]

Advantage

Greymatter automates continuous verification and policy enforcement, removing implicit trust across your network.

With Greymatter playbooks, your network becomes a fortified ecosystem, providing robust protection and future-proof security in complex hybrid and multicloud environments.
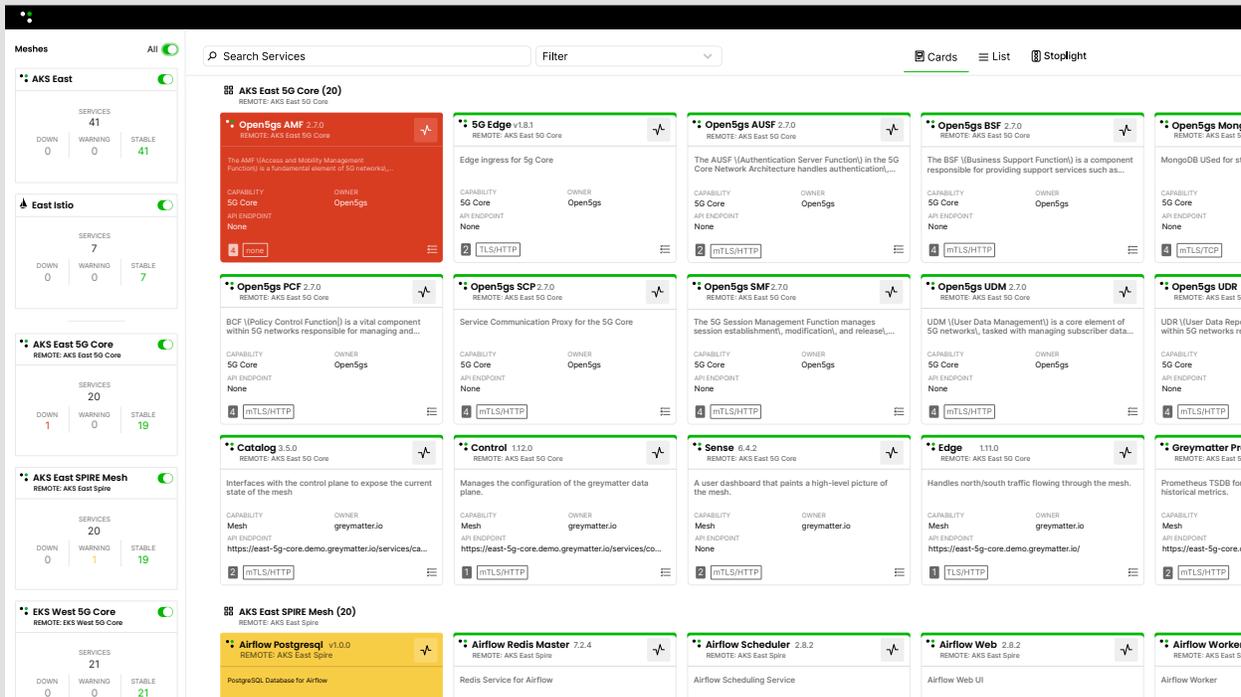
1 **Granular Insights:** The platform provides real-time visibility into service security usage, enabling precise traffic monitoring, essential for enforcing ZTN.

2 **Zero Trust Automation:** Greymatter empowers centralized control and decentralized policy enforcement across cloud and 5G IoT services, aligning with zero trust tenants for robust security.

3 **Fortified Security:** Greymatter strengthens your services with out of the box FIPS encryption and NIST controls, safeguarding against evolving cyber threats.

TE: AKS East 5G Core

SERVICES
20

WN | WARNING | STABLE
1 | 2 | 17

⚠ Chat Bot v1.0.0

● Control 1.12.0

● Minio Edge v1.8.1

● Spire Server 1.8.7

KS East SPIRE Mesh

EMOTE: AKS East Spire

◻◻ AKS East (41)
◻◻

SERVICES
13

DOWN | WARNING | STABLE
0 | 1 | 12

◼ Audits 1.2.6

◼ Bookinfo Reviews V2 v1.0.0

2.0

EKS

REM

1.0.0

Achieving Stringent Protocols

The Greymatter platform is designed to help customers meet the globally recognized security standards and compliance requirements, such as FIPS encryption, NIST zero trust, and enterprise security processing automation.

By automating compliance processes, enforcing robust security controls, and providing continuous monitoring, Greymatter ensures that your enterprise meets these critical standards with ease.
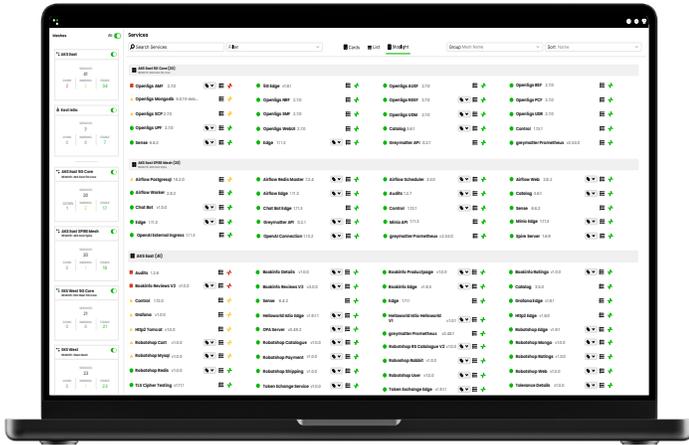
cat v1.0.0

p Cart v1.0.0

op Mysql v1.0.0

op Redis v1.0.0

REMOTE: West Mesh

Surpassing Strict Standards

Challenge
Adhering to ever-evolving, complex standards is a constant challenge but critical. Failure to secure services can lead to devastating breaches, operational paralysis, and irreparable damage to trust and reputation.

Advantage
Greymatter enforces FIPS encryption and NIST Zero Trust across all connected services, applications, and APIs, creating a more secure, stable environment. Automated security enforcement reduces breaches by 35%.[3]

This approach strengthens security, reduces risk, and ensures regulatory compliance.

1 **Proactive Defense:** Offers instant upscaling to FIPS-enabled security protocols and cipher suites, ensuring security is seamless across all deployed services.

2 **Real-Time FIPS/NIST Visibility:** Provides visual indicators of security status, enabling teams to monitor connections, certificate validation, and user-level audits in real time.

3 **Automated Control:** Enforces security policies with real-time updates, minimizing manual intervention.
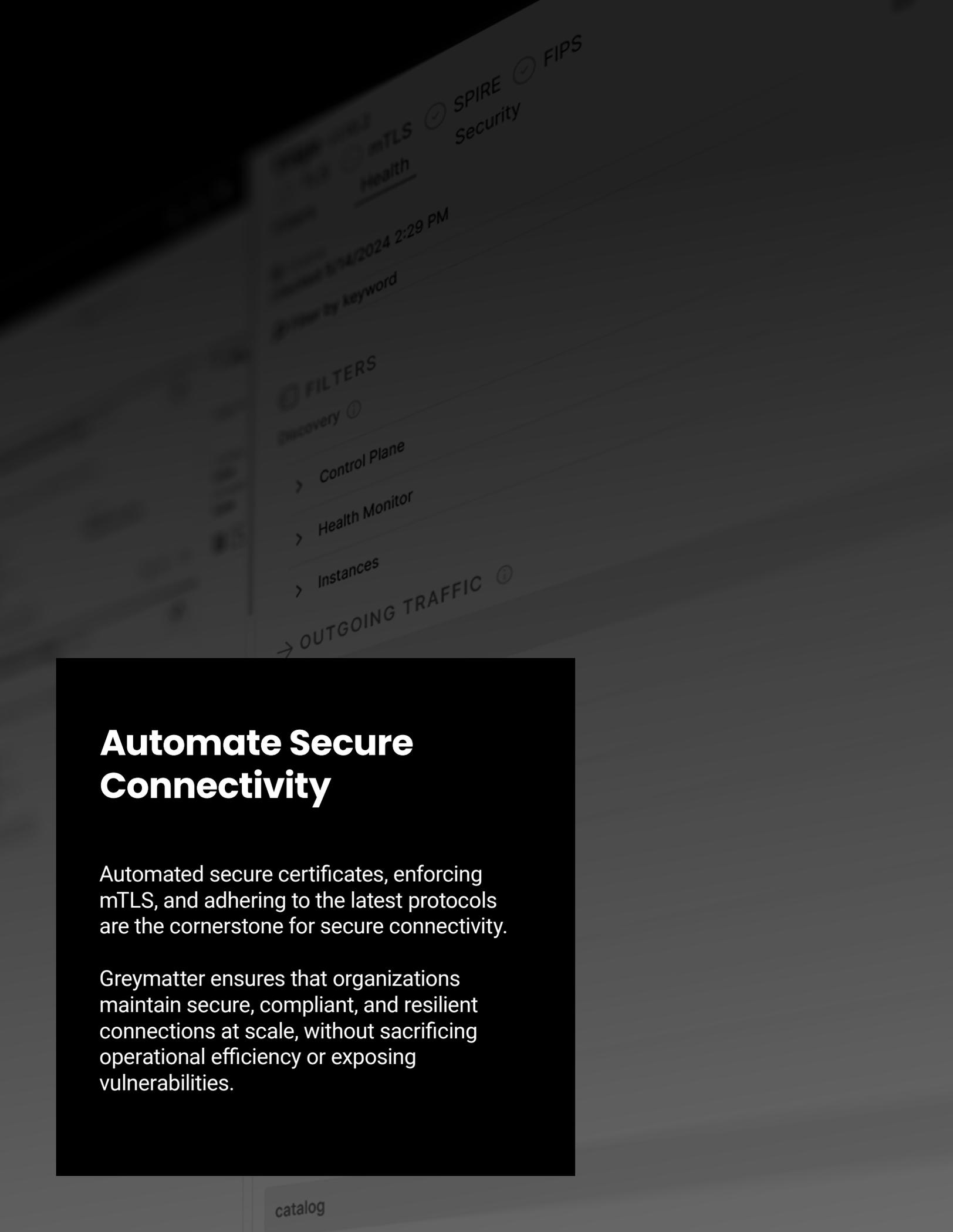
Automate Secure Connectivity

Automated secure certificates, enforcing mTLS, and adhering to the latest protocols are the cornerstone for secure connectivity.

Greymatter ensures that organizations maintain secure, compliant, and resilient connections at scale, without sacrificing operational efficiency or exposing vulnerabilities.

Orchestrating Security Playbooks

Challenge

Organizations must automate certificate management, secure service communications, and enforce dynamic policies to prevent downtime, breaches, and compliance failures. In fact, the absence of automation in policy enforcement can increase operational costs by as much as 20%. This is due to the manual oversight and response efforts required, according to a report by IDC. [4]

Advantage

Greymatter integrates certificate management, mTLS encryption, and dynamic policy enforcement into one cohesive solution. We provide enterprises with unmatched automation and adaptive security, ensuring operational integrity and confident leadership in any environment.
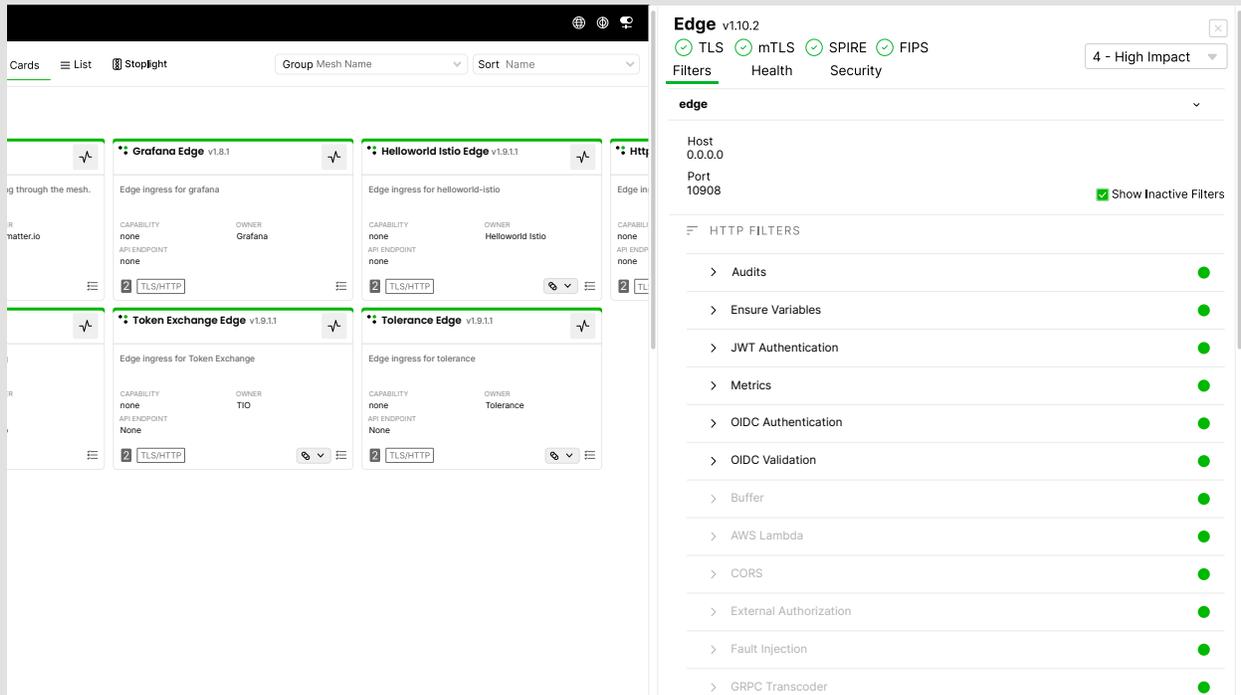
1 **Automate Certificate Management:** Remove vulnerabilities with automated service certificate lifecycle management, preventing downtime and breaches.

2 **Multi-Layered Security:** Ensure the latest TLS, mTLS protocols and SPIFFE standards are enforced across traffic, ensuring secure communication between services.

3 **Scalable Management:** Manage service certificates and security policies at scale, ensuring consistent security even as workloads shift across environments.

Greymatter.io

Let Us Better the Connected World. Together.

A Leader in Zero Trust Networking

Greymatter is an enterprise-ready platform trusted by U.S. 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 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 mission-critical zero trust service connectivity implementations.
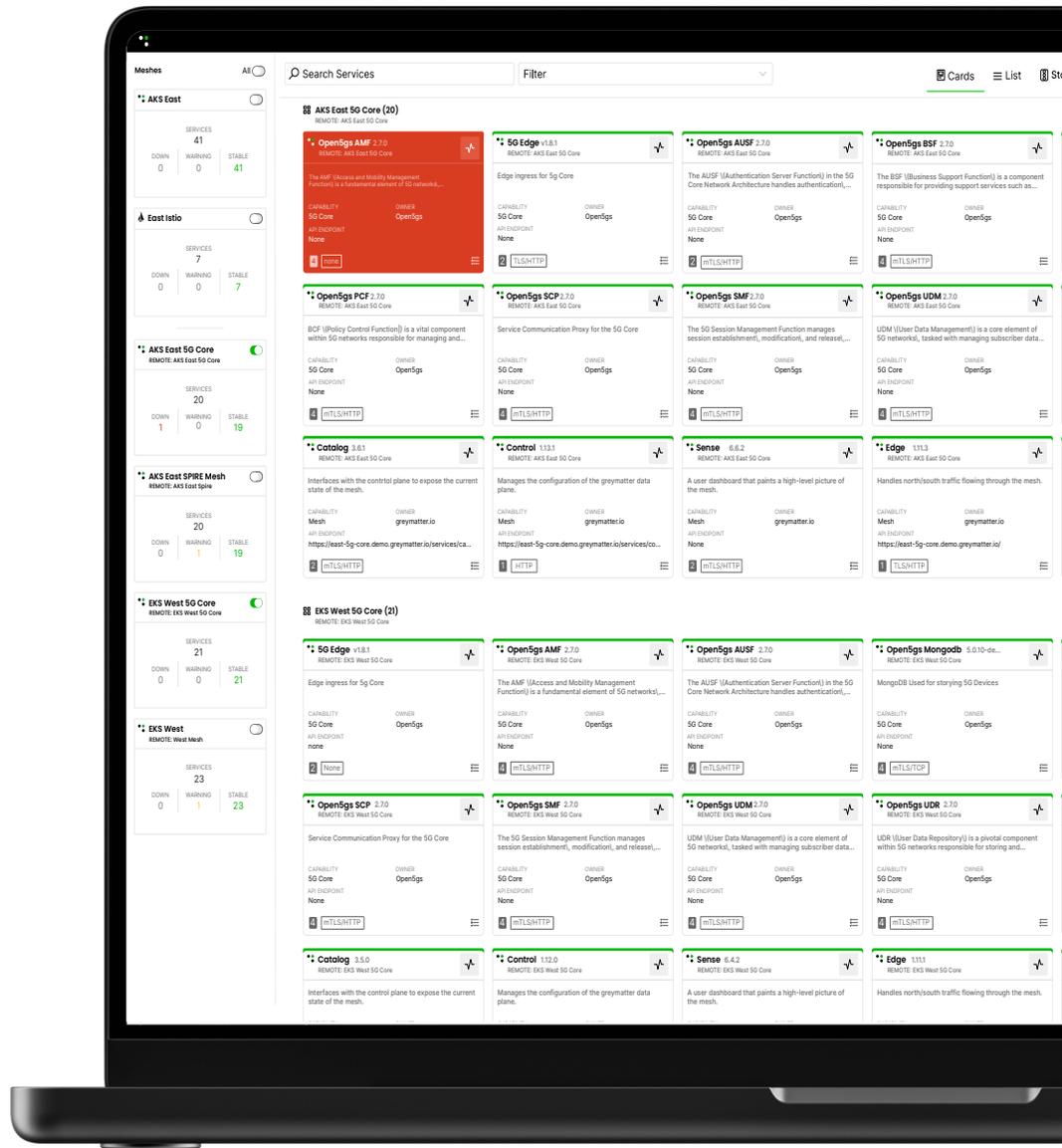
Greymatter.io

Ready to take the next step?

Let's connect you with a Greymatter service connectivity expert.