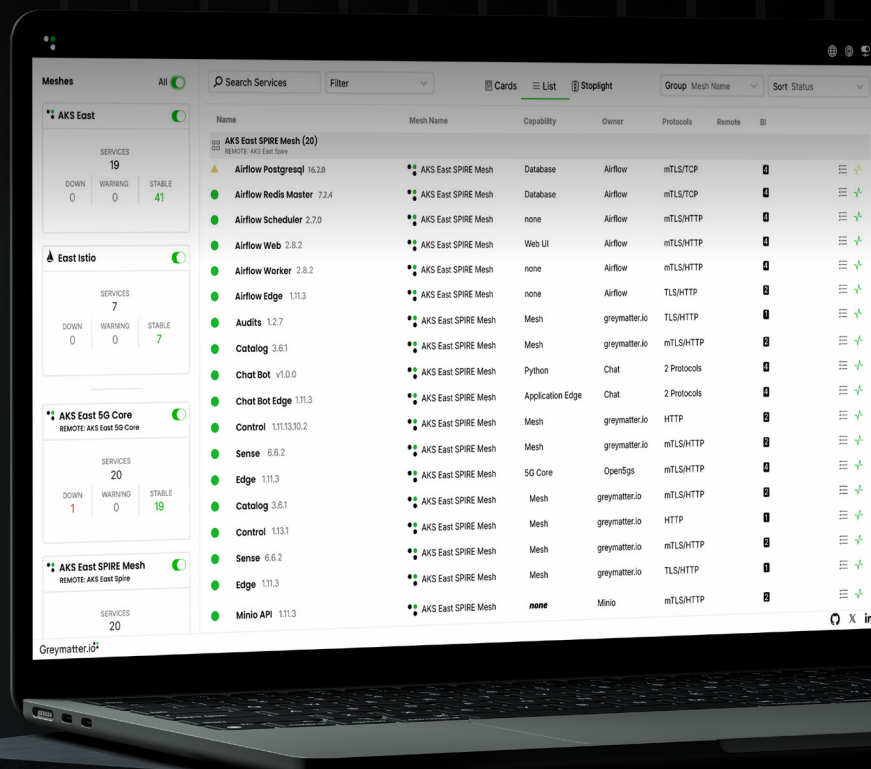




# Greymatter By The Numbers: 2025 Edition

How Greymatter Addresses Today's Biggest Tech Challenges





# How Greymatter Addresses Today's Biggest Tech Challenges

Since its inception, the Greymatter Zero Trust Networking (ZTN) platform has been built on a core principle: application-layer zero trust networking is too tightly coupled to the software and infrastructure layers it operates on. This coupling exacerbates challenges at scale, including complex multicloud deployments, security vulnerabilities, regulatory compliance, cloud waste, and zero trust adoption. These issues lead to lost opportunities, high modernization costs, and governance gaps—often reliant on scarce expertise.

In 2025, we conducted a meta-study of recent industry surveys and market reports to identify the most pressing pain points in application networking and cloud security. This updated report pairs those challenges with quantitative evidence of how Greymatter solves them, incorporating new metrics to reflect emerging threats like AI-driven attacks and container vulnerabilities. The numbers tell a compelling story of Greymatter's value.

## Real World Challenges, Greymatter Solutions

---

**03** Container Vulnerabilities  
Malicious User Attacks  
Injection Attacks & Misconfigurations

---

---

**04** Over-Privileged Identities  
Production API Vulnerabilities  
Cloud Misconfiguration

---

---

**05** AI-Driven Cyber Threats  
DevSecOps Integration  
Multicloud & Hybrid Complexity

---

---

**06** Regulatory Compliance  
API Security  
Visibility Across Tech Stacks

---

---

**07** Delayed Service Rollouts  
PII Exposure via APIs  
Internal API Vulnerabilities

---

---

**08** Cloud Vulnerabilities  
Skill Shortages  
Cloud Resource Waste

---

---

**09** Basic API Security Plans  
Zombie APIs and Legacy Components  
Shadow IT Detection

---

---

**10** Zero Trust Adoption  
Conclusion

---



# Container Vulnerabilities

## Challenge

61% of organizations report significant disruptions from container-related incidents.<sup>1</sup>

## Advantage

- 1 As a recent addition to the GigaOm Container Security Radar, Greymatter manages all ingress and egress traffic across containers and pods at L3, L4, and L7, shrinking enterprise blast radius and reducing exploitability.
- 2 Enforces specific ciphers, security protocols, and acts as a granular policy enforcement point for every workload—by default.

# Malicious User Attacks

## Challenge

47% of organizations cite advances in AI-driven attacks, like phishing, as a primary concern.<sup>2</sup>

## Advantage

- 1 Greymatter's forensic tracking requires zero configurations, detecting malicious behavior from seemingly legitimate users.
- 2 Centralized policy management via Git ensures version-controlled responses to new threats.

# Injection Attacks and Misconfigurations

## Challenge

45% of breaches are cloud-based, with microconfigurations and injection attacks as leading causes.<sup>3</sup>

## Advantage

- 1 Greymatter's enforcement layer applies always-on identity protections, impersonation safeguards, WAF, and deep packet inspection—without manual configuration.
- 2 Automated checks reduce OWASP Top 10 vulnerabilities by over 90%.

1, 2, - Check Point Cloud Security Challenges, 2025

3 - Expert Insights Cloud Security Statistics, 2025



# Over-Privileged Identities

## Challenge

82% of data breaches involve human error, including over-permissioned identities.<sup>4</sup>

## Advantage

- 1 Zero-config forensic user tracking reduces privilege escalation risks.
- 2 Integrates with IAM systems in fewer than 10 lines of code, enforcing least-privilege access.

# Production API Vulnerabilities

## Challenge

80% of companies experienced at least one cloud security incident in the past year, often tied to APIs.<sup>5</sup>

## Advantage

- 1 Greymatter provisions cryptographic mTLS identities and verifiable trust boundaries with a single declarative command.
- 2 Secure token impersonation and IAM integrations protect APIs across multicloud environments.

# Cloud Misconfigurations

## Challenge

88% of government agencies cite cloud misconfigurations as a top security concern in 2025.<sup>6</sup>

## Advantage

- 1 Greymatter consolidates network and security policies in a GitOps repository with fewer than 10 lines of code.
- 2 Automated playbooks reduce boilerplate by 800%+, with dry-run validation ensuring deployment confidence.

4, 5 - Expert Insights Cloud Security Statistics, 2025

6 - Spacelift Cloud Security Statistics, 2024



# AI-Driven Cyber Threats

## Challenge

47% of organizations prioritize threat detection and response due to AI-enhanced attacks.<sup>7</sup>

## Advantage

- 1 Greymatter's AI-aware gateway secures AI tools, LLM APIs, and agents. All telemetry is auto-routed to SIEM/SOAR tools for real-time anomaly detection.
- 2 Fine-grained policy enforcement enables immediate containment.

# DevSecOps Integration

## Challenge

41% of organizations face complexity from cloud-native approaches impacting DevSecOps.<sup>8</sup>

## Advantage

- 1 Greymatter's DevSecOps playbooks cut integration time by over 70%.
- 2 Automated IaC scanning ensures secure deployment in both CI/CD pipelines and live environments

# Multicloud and Hybrid Complexity

## Challenge

54% of organizations struggle to maintain consistent security and compliance across hybrid or multicloud environments.<sup>9</sup>

## Advantage

- 1 Greymatter reduces zero trust configuration drift by a factor of 4x, ensuring consistency across clouds.
- 2 Integrates with 100+ security and API defaults to simplify hybrid/on-prem management.

7 , 9- Cybersecurity Insiders Survey, 2024

8 - Spacelift Cloud Security Statistics, 2024



# Regulatory Compliance

## Challenge

70% of enterprises express concerns over adhering to evolving compliance standards in cloud environments.<sup>10</sup>

## Advantage

- 1 Greymatter's centralized policy layer manages application networking as code—version-controlled, attributable, and Git-native.
- 2 Fleet-wide policy enforcement aligns with NIST ZTA, FIPS, GDPR, SOC 2, PCI DSS, and more.

# API Security

## Challenge

91% of organizations are concerned about their security systems' ability to manage zero-day API attacks.<sup>11</sup>

## Advantage

- 1 Greymatter agentless sensors stream real-time telemetry to SIEM/SOAR tools.
- 2 Delivers 100% NIST-compliant Zero Trust API security with FIPS encryption and OPA enforcement.

# Visibility Across Tech Stacks

## Challenge

56% of organizations struggle to safeguard data across multicloud environments due to inconsistent tools.<sup>12</sup>

## Advantage

- 1 Greymatter's unified console provides real-time visibility into services, APIs, and infrastructure across all environments.
- 2 Apply fleet-wide policies in minutes—with actionable telemetry and health insights.

<sup>10, 12</sup> - Adivi Cloud Security Statistics, 2024

<sup>11</sup> - Spacelift Cloud Security Statistics, 2024



# Delayed Service Rollouts

## Challenge

70% of financial services firms report deployment delays due to cloud API security concerns.<sup>13</sup>

## Advantage

- 1 Greymatter accelerates secure delivery cycles, reducing deployment times from months to hours.
- 2 Prebuilt playbooks simplify compliance-ready rollouts.

# PII Exposure via APIs

## Challenge

75% of organizations report that 40% of cloud-stored data, including PII, is sensitive.<sup>14</sup>

## Advantage

- 1 Greymatter's tracking and cataloging identifies exposed APIs, applications, and access events tied to PII.

# Internal API Vulnerabilities

## Challenge

44% of corporate data exfiltration attempts originate from personal cloud apps, including internal APIs.<sup>15</sup>

## Advantage

- 1 Greymatter secures internal APIs using mTLS and impersonation with a simple declarative command.
- 2 Centralized enforcement in under 10 lines of code.

<sup>13, 15</sup> - Spacelift Cloud Security Statistics, 2024

<sup>14</sup> - Thales Cloud Security Report, 2024



# Cloud Vulnerabilities

## Challenge

76% of enterprises use at least two cloud providers, increasing vulnerability complexity.<sup>16</sup>

## Advantage

- 1 Greymatter's 100+ automation defaults simplify adoption and reduce human error.
- 2 New application onboarding takes hours—not weeks.

# Skill Shortages

## Challenge

71% of organizations report a lack of skilled cybersecurity professionals for cloud security.<sup>17</sup>

## Advantage

- 1 Greymatter's 100+ automation defaults simplify adoption and reduce human error.
- 2 New application onboarding takes hours—not weeks.

# Cloud Resource Waste

## Challenge

94% of organizations report negative impacts from avoidable cloud resource waste.<sup>18</sup>

## Advantage

- 1 Greymatter's real-time service and dependency maps cut waste by up to 50%.
- 2 Automatically right-sizes provisioning based on observed workload health.

<sup>16, 17</sup> - Spacelift Cloud Security Statistics, 2024

<sup>18</sup> - Forrester Study by HashiCorp, 2023





## Basic API Security Plans

### Challenge

62% of organizations have basic or no API security plans in place.<sup>19</sup>

### Advantage

- 1 Greymatter delivers turnkey, NIST-compliant API protections—instantly.
- 2 Tracks and secures all APIs with zero setup required.

## Zombie APIs and Legacy Components

### Challenge

35% of IT leaders identify outdated APIs and components as significant threat surfaces.<sup>20</sup>

### Advantage

- 1 Greymatter automatically catalogs and tracks all APIs, including dormant or legacy ones.
- 2 Security patches can be applied fleet-wide in minutes.

## Shadow IT Detection

### Challenge

47.2% cite detecting unauthorized application usage (e.g., shadow IT) as a major challenge.<sup>21</sup>

### Advantage

- 1 Greymatter's granular visibility identifies shadow IT with no instrumentation.
- 2 Ingress/egress policy enforcement isolates unknown applications.

<sup>19</sup> - Salt Labs State of API Security, 2023

<sup>20</sup> - Google Cloud API Security Report, 2022

<sup>21</sup> - CyberEdge ISC2 Survey, 2022



# Zero Trust Adoption

## Challenge

20% cite skill shortages as a top zero trust adoption challenge.<sup>22</sup>

## Advantage

- 1 Greymatter's out-of-the-box, 100% NIST-compliant zero trust controls reduce friction.
- 2 Simplified mTLS and IAM setups accelerate rollout.

# Conclusion

The Greymatter Zero Trust Networking platform directly addresses 2025's most urgent enterprise security and modernization challenges—from AI threats and API risk to hybrid cloud sprawl and compliance delays. By centralizing policies, automating enforcement, and providing real-time visibility across all environments, Greymatter empowers organizations to govern their infrastructure securely and at scale. Proven in defense and intelligence environments, Greymatter enables operational confidence—at speed.



Ready to take the next step?

Let's connect you with a Greymatter zero trust networking expert.

[@greymatter.io](https://greymatter.io)

4201 Wilson Blvd Floor 3  
Arlington, VA 22203



©2025 Greymatter.io