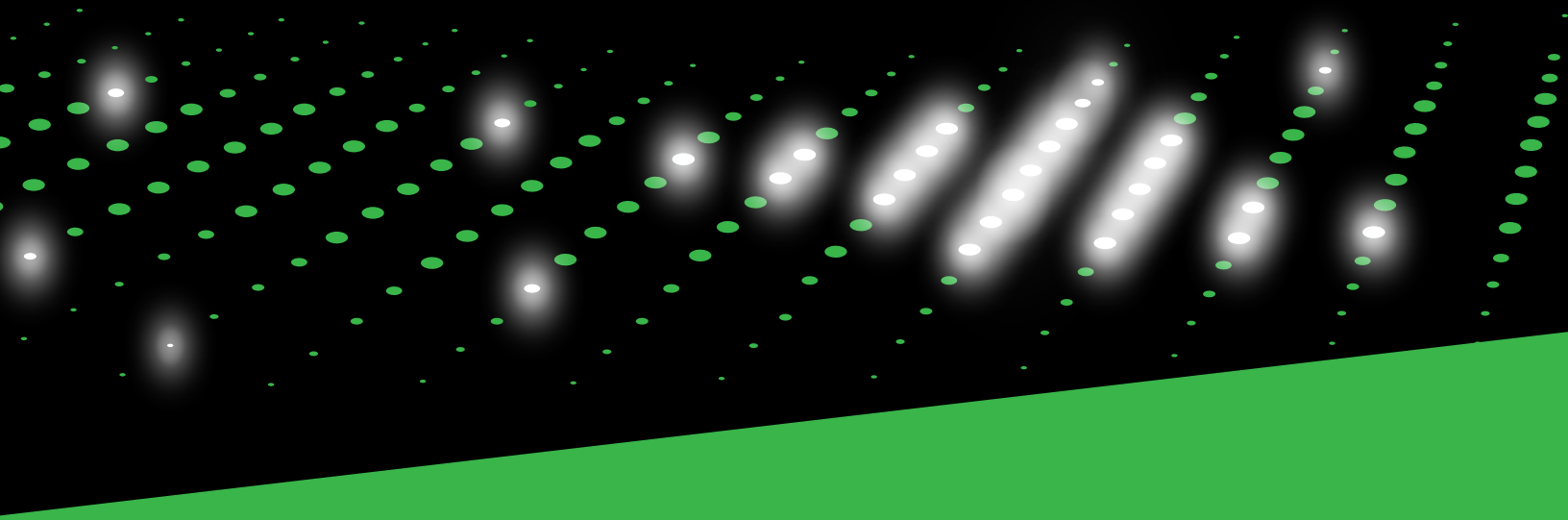
Greymatter.io

A Blueprint for the Future of Security

How Greymatter Supports Cybersecurity Mesh Architecture



Bettering the Connected World

www.greymatter.io

Table of Contents

Executive Summary

Over the past decade, cybersecurity investment has skyrocketed. Experts agree that service mesh technologies and zero-trust principles have become the core underlying tenants for modern enterprise security. Now, as the number of digital transformation initiatives and Infrastructure complexity continue to soar and cyberattacks continue to evolve, security requirements have grown exponentially.

> **90% of CISOs worldwide remain concerned about security control gaps and point to technology challenges including APIs and software supply chains make it difficult to protect data and enforce compliance, and also put them at increased personal risk of legal action." [1]**

Cybersecurity is the top investment priority for organizations in 2024. But where to invest for the greatest return is the question. To increase overall security effectiveness, research organization Gartner as introduced a new way to frame the next security evolution. They call is cybersecurity mesh architecture (CSMA). The goal of CSMA is to manage and provide trust to distributed digital assets and serve as an integrated cybersecurity defense system. The approach is to leverage components from different vendors and prioritize interoperability to break down silos and close security gaps so that organizations can strengthen security at scale. Gartner predicts that by 2024, organizations adopting CSMA will reduce the financial impact of individual security incidents by an average of 90 percent.[2]

Building on the Greymatter.io leadership in service mesh technologies and the company's **100 percent NIST-compliant zero-trust** controls for service connectivity out-of-the-box, Greymatter is a **fully cloud and environment agnostic platform** that addresses real-world challenges CISOs face today with capabilities that align to the four pillars of the emerging CSMA. From audit streams with live system and API telemetry, to identity-aware networking, centralized configuration management, and a first-class dashboard to track, measure, and control the entire service connectivity layer, Greymatter enables CSMA for full **zero trust across the entire ecosystem.**

Here are a few key takeaways from this white paper:

Security and Intelligence

77% of security, DevOps, and app development professionals say their existing tools are not effective enough to prevent API attacks. [3]

Greymatter agent-less sensors enable SIEM, SOAR, and other security tools with **real-time granular telemetry and user data** from throughout the stack. User level tracking ensures security teams know **who, what, where and when** anything is happening on the network.

Identity Fabric

99% of cloud environments have over-privileged IDs. [4]

Greymatter enables organizations to consolidate in-depth networking and security policy files into a central location with **less than 10 lines of code** to fast-track identity aware networking.

Centralized Policy, Posture, and Playbook Management

Over the past six years, cloud vulnerabilities grew 540%, with Azure and Dynamic 365 vulnerabilities growing 159% in 2022. [5]

With a simple implementation, users can catalog, visualize, and index all applications, APIs, and services running across multiple environments in **one view to measure security, operational health, and impact.**

Operational Dashboard

47% of organizations claim difficulty measuring and managing across differing tech stacks. [6]

Greymatter enables consolidation of intricate policy files into a centralized hub and allows users to **immediately apply fleet-wide security policies** to applications, APIs, and data services **in minutes, not days.**

Layer 1: Security Analytics and Intelligence

Currently, organizations use multiple tool sets for security analytics, correlation, and threat detection, including their SIEM, XDR solutions, SOAR platforms, and UEBA, as well as IDP/IPS, NTA, and vulnerability scanning tools. The effectiveness of these tools depends on the data they receive. However, configuring systems to pipe data into these tools and curating that data for ingestion and analysis requires significant work by development and engineering teams.

> **Today, 77% of security, DevOps, and app development professionals say their existing tools are not effective enough to prevent API attacks.[7]**

So, SOC analysts spend time building queries to extract the data they need, iterating with engineers and developers on adjustments before finally arriving at a set of normalized, relevant, and actionable data.

The challenge compounds as organizations move to hybrid environments consisting of multiple cloud instances, multiple installations within a single cloud, and on-prem feature sets. Manual processes and increasing complexity make it costly to keep up and difficult to provide detailed real-time data on the disparate instances supporting the business operations leading to potential vulnerabilities.

Teams struggle to gain the security intelligence they need to understand what's happening across their environment and protect their operations. Organizations need a more efficient and effective way to strengthen their security posture and mitigate risk of breaches at scale. The CSMA security analytics and intelligence layer is designed to address this need, as it encourages an integrated, relationship-based approach for monitoring and analyzing network traffic to detect and prevent security threats.

> **More than 47% of security professionals detected unauthorized application usage (i.e., shadow IT), including torrent and crypto-mining as a major 2023 security challenge. [8]**

Greymatter Support for CSMA Layer 1

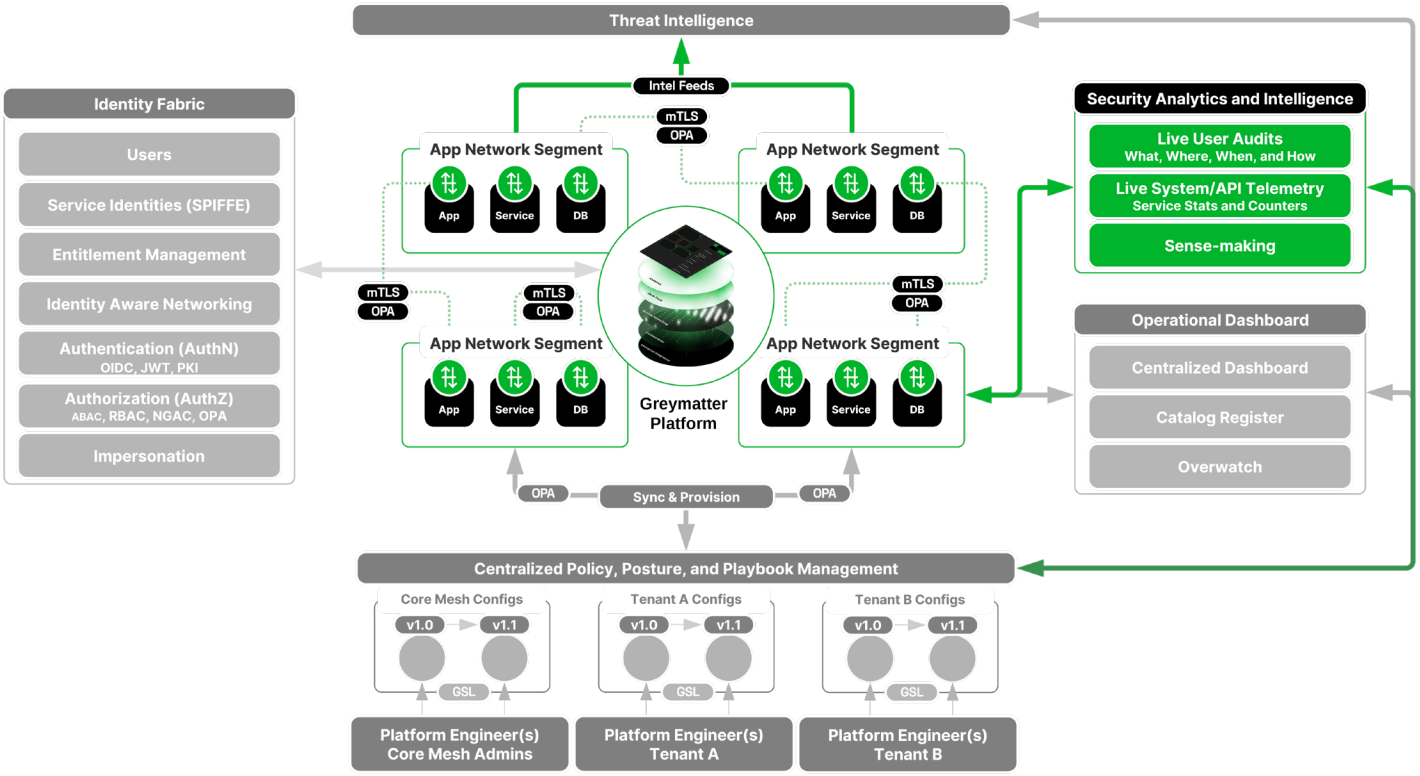


FIGURE 1: GREYMATTER SUPPORT OF CSMA LAYER 1

Greymatter plays a crucial role in enabling the **security analytics and intelligence layer** through scorecard heuristics and risk contextualization in combination with other security tools in the tech stack. Near real-time collection and delivery of contextualized threat data enables clients to address compliance, operational uptime, and security requirements more quickly and easily.

Specific capabilities to support CSMA Layer 1 include:

Greymatter agent-less sensors enable SIEM, SOAR, and other security tools with **real-time granular telemetry and user data** from throughout the stack. **Live user audits** ensure security teams know **who, what, where and when** anything is happening on the network to enable comprehensive and accurate security threat detection.

Thanks to a unique **live system/API telemetry approach**, the Greymatter platform enables teams to understand how people, systems, and processes are behaving compared to what they are authorized to do.

Greymatter ensures a separate, isolated layer of ingress/egress control for each application, API or service it manages with **no instrumentation required**. This deep visibility into service connectivity traffic and transactions based on enhanced data, which can be correlated with other information collected, further enriches network traffic analysis.

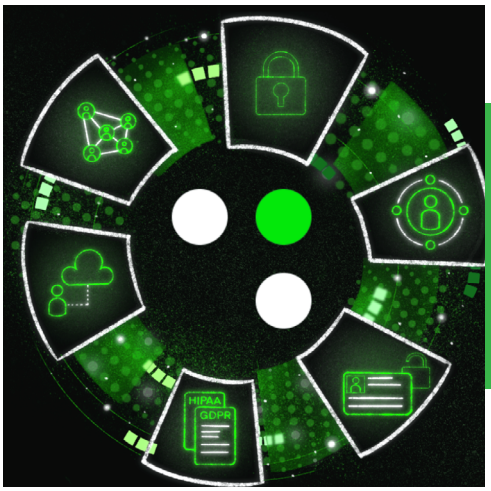
Sense-making models allow security teams to use this information to monitor and analyze application behavior, detect anomalies and potential threats, and understand network traffic patterns.

Other complementary capabilities include integration with threat intelligence systems, real-time updates on the latest service connectivity traffic and identity attribution, as well as network and user pattern of life analysis audits that allow security teams to identify and track potential threats based on user and network behavior over time.

> **Overall, Greymatter provides a comprehensive suite of capabilities that support the security analytics and intelligence layer across an enterprise.**

Benefits of the Greymatter Approach

Challenge	Greymatter Solution	Value
Organizations spend millions of dollars and hundreds of hours of developer and engineering time tooling for auditing.	Automation and analytics out-of-the-box that significantly reduce the resources required to write high-fidelity, custom audit code.	**Cost savings**
Organizations struggle to stay ahead of anomalous activity and potential threats and take proactive measures to protect their assets and avoid disruption of service.	Deep visibility into traffic and behaviors for analysis and action, including on-the-fly traffic rerouting to avoid disruption.	**Improved threat detection, response, and real-time analytics**
Government agencies and large enterprises with mission critical operations need to be able to collect user and telemetry data for attribution, forensic analysis, and analysis on important missions and customers.	Overlay telemetry data with automatic failover measures to maintain availability, and then seamlessly send data to security tool sets for analysis and resolution.	**Improved incident resolution**



Layer 2: Identity Fabric

Managing user and system identities and access in today's hybrid, multi-cloud environments is so complex that 99% of cloud environments have over privileged IDs.[9]

Organizations often have IAM solutions from multiple, external identity providers to manage different types of identities, applications, and access requirements. This results in siloed and fragmented identity management environments, which can lead to inefficiencies, security risks, and compliance issues.

Furthermore, applications often leverage different authentication and authorization mechanisms, leading to gaps in identity awareness. In fact, a quarter of security, DevOps, and app development professionals have no idea which of their APIs expose sensitive PII. [10] And internal APIs account for 8 percent of reported API attacks because they are typically left unprotected. [11] Auditing capabilities also differ depending on the code or application, making it difficult to maintain a complete picture of user identity across the network. And while OIDC is widely adopted, token exchange abilities are limited, forcing organizations to pass around large user claims to all network assets, regardless of need. Widespread propagation of identity and associated attributes allows threat actors to see what that user has access to, which opens the lens to an attack vector.

More than 75% of attacks are launched from seemingly legitimate, but malicious users with proper authentication.[12]

Arguably the most important layer of CSMA, the identity fabric layer is designed to address growing complexity and eliminate silos by encouraging a centralized approach to identity and access management, while still enabling the ability to segment identity based on network location, application, service, or network asset.

Greymatter Support for CSMA Layer 2

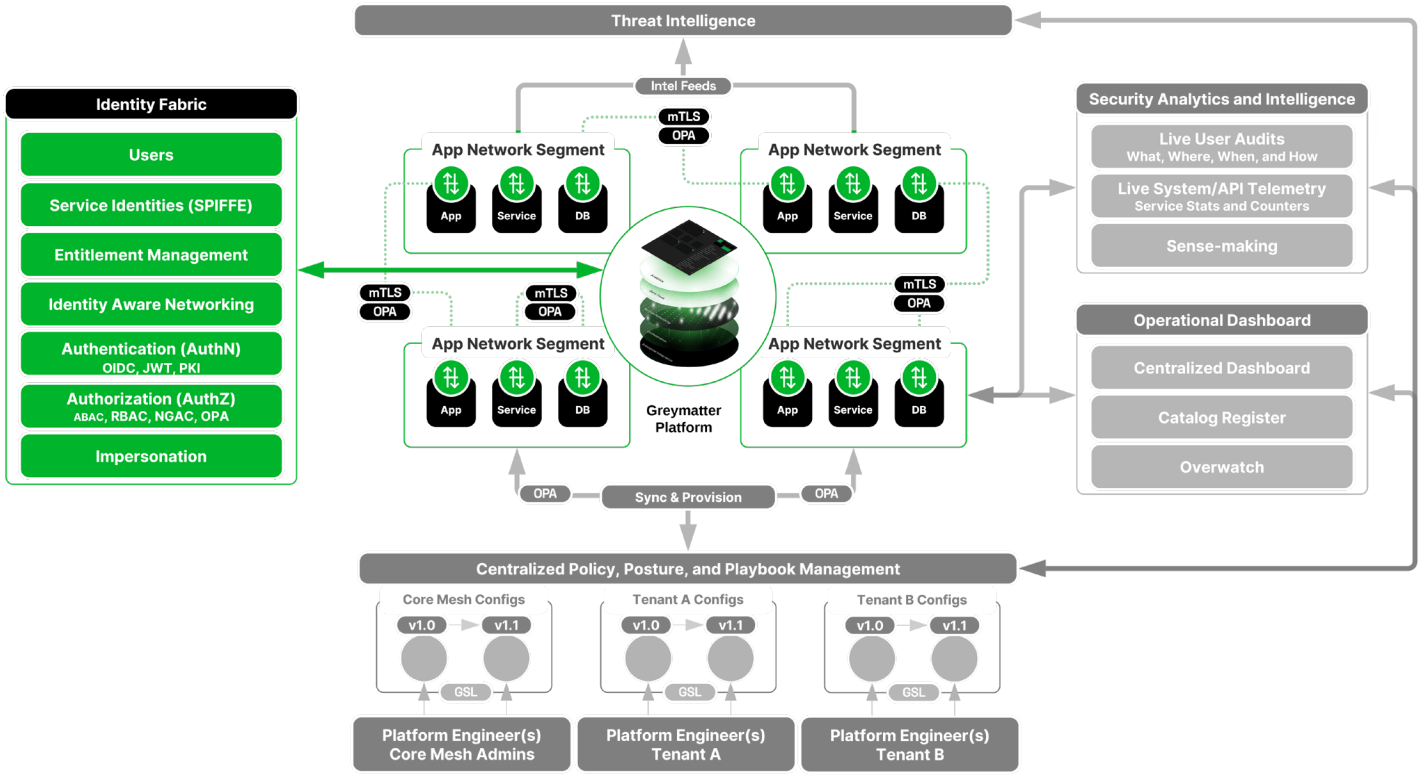


FIGURE 2: GREYMATTER SUPPORT OF CSMA LAYER 2

Greymatter plays a unifying role in the **identity fabric layer.** The platform's approach to zero trust bridges person identities to non-person identities, providing an innovative and battle tested way for users to easily and securely connect to applications, APIs, services, and data sources running in different environments – from hybrid and multi-cloud, to on-premise. A range of capabilities enable organizations to manage identities and access controls centrally while decentralizing and simplifying enforcement. With a comprehensive and consistent view of identities, access controls, and policies across the environment, clients can improve security, simplify compliance, and streamline identity and access management (IAM) operations.

Specific capabilities to support CSMA Layer 2 include:

To validate **user identity,** organizations use various **authentication** mechanisms, whether PKI, MFA, OIDC, JWT tokens, or something else. Greymatter enables organizations to consolidate in-depth networking and security policy files into a central location with **less than ten lines of code.** With built-in support for OIDC, Greymatter brings together different authentication methods and tools to simplify authentication so that it flows seamlessly through the network based on the user and the service, application, or data they need to access.

Within Greymatter, each service also receives its own identity. Greymatter's SPIFFE/SPIRE integration enables automated and secure issuance and revocation of identity certificates for services. Control over **service identities** helps to prevent unauthorized access to sensitive data and transactions within the microservices environment.

Leveraging an organization's need to ensure **least-privilege access policy models,** policy layer, Greymatter taps into the role-based access control (RBAC), attribute-based access control (ABAC), and next-generation access control (NGAC) based approaches that the security teams develop using Open Policy Agent (OPA) Rego. This helps offload the work for development teams. Every service that is tied into the Greymatter service connectivity layer can benefit from the organization's centralized policy engine and fine-grained access controls.

The platform further strengthens security by rotating service identities on an hourly or configurable basis. In the event of a service compromise, **entitlement management** reduces the blast radius and mitigates risk as threat actors must regain access to the service and organizations have a greater opportunity to detect a compromise.

The ability to understand both user and system identities and claims and propagate that information across hybrid and multi-cloud environments in a seamless and automated fashion enables Greymatter unifies identities across external identity providers such as Keycloak, Okta, Google, and Microsoft and provides only the necessary identity attributes and access controls specific to each application, service, or network asset, based on the employee's role and location.

With Greymatter, it is simple for organizations to leverage Open Policy Agent (OPA) to write and configure RBAC and ABAC **authorization** policies for each service at a granular level via a centralized repeatable process and apply **immediatefleet-wide security policies in minutes, not days.** Integration with Greymatter ensures that only authorized users have access to specific resources, for example applications, APIs, and sensitive data. Access can be automatically blocked based on contextual data such as request payloads, device posture, location, and more.

With **two lines of configuration**, Greymatter supports mTLS **impersonation** for additional security, whereby authorization to access a service is dependent on their having already accessed another service. Access controls are defined so that if a user tries to access that service directly then access is denied. Linking the user and service together provides additional fine-grained controls and is easy to configure as part of Greymatter's role-based access control configurations.

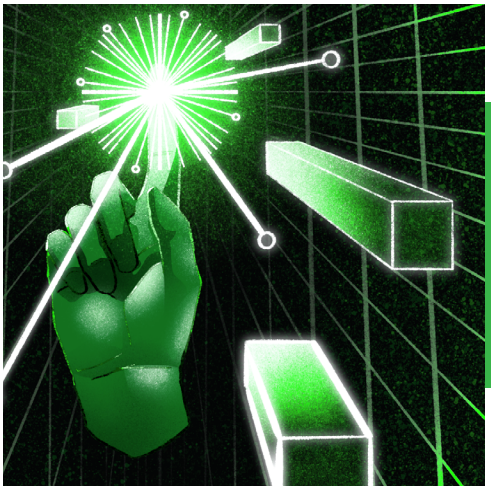
With zero configurations required, organizations can add **immediate forensic user tracking audits** to any application, API, or service running on the network or in a cloud environment to accelerate analysis and action.

Additional capabilities include scalability and high availability features, logging of all authentication and authorization activity, comprehensive reporting, and integration with security tool sets.

Overall, Greymatter offers a comprehensive and battle-tested suite of capabilities that support the identity fabric layer today, and as organizations scale and expand their IT environments.

Benefits of the Greymatter Approach

Challenge	Greymatter Solution	Value
Implementing and managing secure service-to-service communication for every transaction is incredibly complex and time-consuming.	Eliminate silos and gain real-time capabilities and granular visibility into who's doing what, where, when, and how for analysis and action.	**Improve threat detection, response, and real-time analysis**
A combination of different authentication methods and audit capabilities make it difficult to maintain a complete picture of user identity and access.	Detailed logs of all interactions between users, services, applications, data, and assets, and exporting of data to security tool sets for analysis and resolution.	**Improved incident resolution**
Highly regulated industries such as healthcare and finance are challenged to strike a balance between access and compliance policies.	Fine-grained controls to maintain strict compliance with regulations such as NIST 800-207 and 800-207A publications, GDPR, HIPAA, and PCI, as well as capabilities that increase transparency and auditability.	**Increased regulatory compliance and reduce risk of exposure**
Teams must move between multiple, different IAM solutions to support multi-cloud and on-prem environments. And IAM products that support OIDC integration require significant coding and developer time.	Reduce the number of IAM solutions in place as well as development time to streamline operations and impact of a breach.	**Cost savings**



Layer 3: Centralized Policy, Posture, and Playbook Management

With the growing adoption of cloud-native technologies and multi-cloud environments, managing policies, posture, and playbooks in a decentralized way is creating management complexity and security gaps, while exposing the enterprise to unnecessary risks.
So, SOC analysts spend time building queries to extract the data they need, iterating with engineers and developers on adjustments before finally arriving at a set of normalized, relevant, and actionable data.

> **Over the past six years, cloud vulnerabilities grew 540%, with Azure and Dynamic 365 vulnerabilities growing 159% in 2022.** [13]

Policies specific to applications, APIs, and data services are created and enforced in a decentralized manner. Furthermore, implementing separation of concerns, least privilege access models, and impersonation certificate rotations are very difficult, so these policies tend to be lowest common denominator control gates. Inconsistencies across different applications and infrastructure components makes zero trust architecture unattainable. This opens the door to threat actors and hinders compliance with best practices, regulations, and industry standards.

> **In fact, 76% of cloud accounts for sale on the dark web are for remote desktop portal (RDP) access*. And injection attacks and security misconfigurations are the top most common attack attempts mapped against the top 10 (OWASP) vulnerabilities.** [14]

Additionally, manual policy management can be time-consuming and error-prone, as policies must be manually reviewed and updated. Keeping up with the rapidly evolving threat landscape is difficult at best. And the lack of unified visibility and control over security policies can lead to confusion, leaves unintentional holes in the enterprise's networking, and makes it difficult to identify and mitigate security risks. It comes as no surprise that prevention of cloud misconfiguration and regulatory compliance were major security priorities in 2022.[15]

The CSMA centralized policy, posture, and playbook management layer addresses the challenges of building and managing policies and posture settings while maintaining ongoing verification of security and compliance requirements.

Greymatter Support for CSMA Layer 3

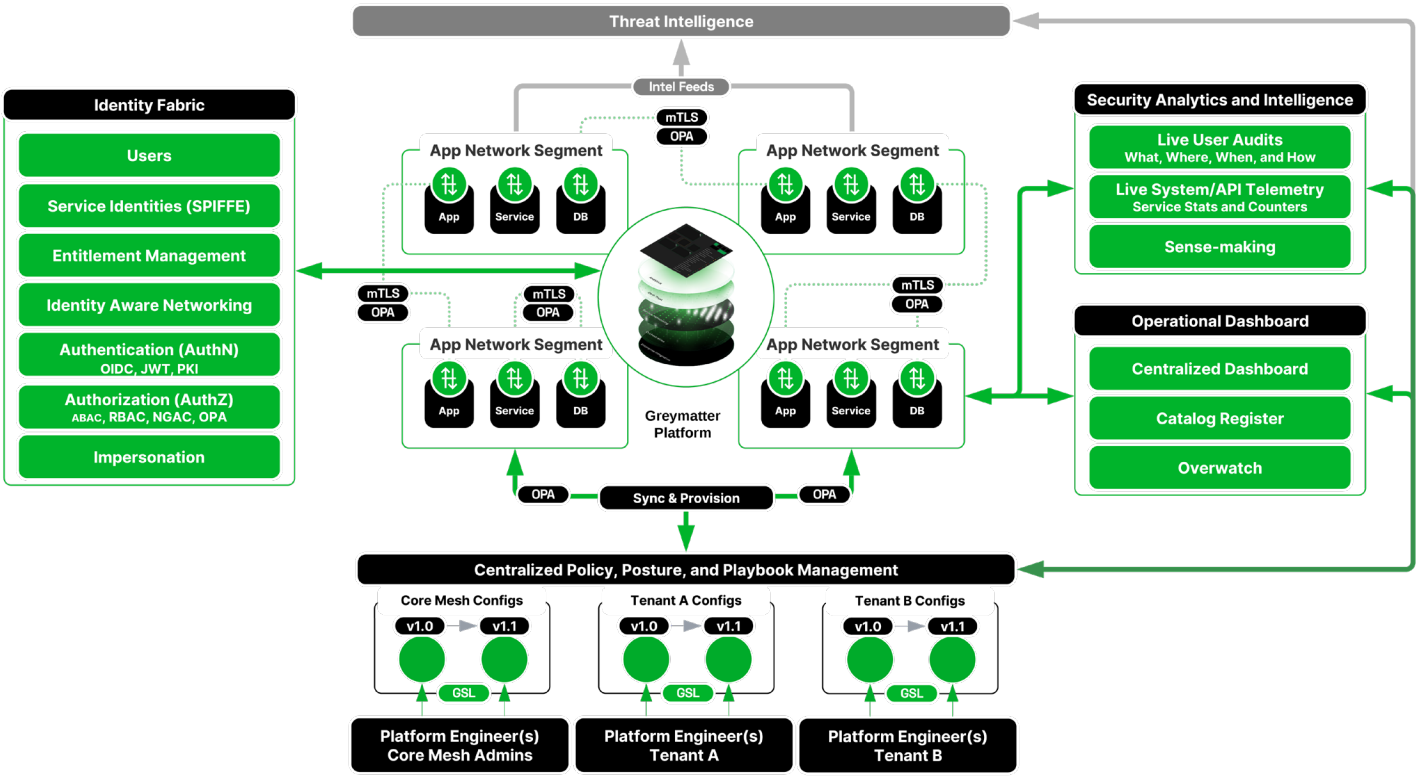


FIGURE 3: GREYMATTER SUPPORT OF CSMA LAYER 3

Greymatter plays a critical role in the **centralized policy, posture, and playbook management layer** by empowering organizations to author enterprise playbooks that are applied at runtime. By introducing Greymatter Specification Language (GSL) and combining it with GitOps, automation, rich graphical auditing, and fine-grained controls, Greymatter helps track each app, API and service across tech stacks. This simplifies the management of security policies across the infrastructure, improves compliance, and enables a collaborative and proactive approach to cybersecurity.

Specific capabilities to support CSMA Layer 3 include:

Greymatter uses built-in **GitOps sync services** for **centralized policy management,** managing application **networking as code** and leveraging attribution and version control across multi-cloud and hybrid environments. Fleet-wide policy is a centralized and separate layer of concern managed only by those that need to apply it. Policies can be defined in GSL code and Greymatter employs standardization and automation to ensure all environments remain in sync and consistent with the desired state. Acting as the source of truth for all application networking configurations and security policies, Greymatter's GitOps implementation ensures changes are auditable and version-controlled, and code review processes are enforced to approve changes before merging.

Centralized posture management is enabled by providing operational support and real-time auditing of configuration changes and application usage. **With less than 40 lines of code**, users can catalog, visualize, and index all applications, APIs, and services running across multiple environments in **one view to measure security, operational health, and impact**. Organizations can quickly detect and respond to security incidents while maintaining compliance with regulations and industry standards.

Greymatter's **GSL** is a declarative domain specific language built on top of CUE. Greymatter.io designed GSL primarily to ease the burden associated with configuring application networking rules within a modern mesh-like topology. These centralized **playbook management capabilities** are enabled by providing natural object relationships and drop-in customization. Revolutionary playbooks and automation **reduce boilerplate configuration by over 1000 percent.** For the first time, users from across the experience spectrum are empowered to make sophisticated application networking configuration changes rapidly and with confidence. With Greymatter's dry-run command, users can validate configuration and receive **immediate feedback** before deployment to production. Enterprises have greater flexibility to enforce separation of concerns while increasing collaboration between teams and promoting greater agility and flexibility.

Additional capabilities include disaster recovery through version-controlled backup of application networking configurations, and integration with security tool sets such as SIEMs and SOARs. These integrations enable **playbook management** support – streaming deep insights to these solutions to help improve incident response procedures.

Benefits of the Greymatter Approach

Challenge	Greymatter Solution	Value
Lack of standardization and repeatability when deploying a microservices-based architecture leads to misconfigurations and human errors which opens the door to risk.	Consolidating network and security policies in a single location enables consistent and repeatable deployments across multi-cloud environments, consistent implementation of security controls, and accelerates troubleshooting to mitigate risk and swiftly respond to incidents.	**Centralized management and improved incident response**
As the number of interdependent applications, APIs, and microservices increases, automation and standardization hold the key to effective policy enforcement at runtime.	Posture management capabilities streamline runtime policy control and enforcement across an organization to protect workloads and services from overload or attack and more easily manage a secure application networking posture.	**Increased regulatory compliance**
Tightly coupling application networking configurations with application code or deployment technologies hinders the ability to make changes quickly and efficiently and can compromise security.	Playbooks management capabilities enable teams to manage application networking configuration as code, decouple networking security and traffic control from apps, APIs, and data services, and leverage attribution and version control.	**Increased collaboration**

Layer 4: Operational Dashboard

In today's multi-cloud and hybrid environments many organizations have different security teams responsible for network, cloud, and endpoint security.

Each team tends to use its own set of tools which operate independently and do not communicate with each other. And each tool has its own visualization, alerting, and reporting capabilities. As a result, 47 percent of organizations claim difficulty measuring and managing across differing tech stacks. [16]

A lack of holistic visibility into the overall security posture and health across the enterprise makes it difficult to detect inconsistent controls and policies, and misconfigurations that weaken security posture.

Fragmentation also creates inefficiencies in incident detection, response, and mitigation, as security teams need to manually gather and analyze data from multiple sources to identify patterns, anomalies, and potential security threats.

More than a third (35%) of IT security leaders identify out-dated zombie APIs, data, and components as significant threat surfaces. [17]

Through integration and interoperability, the CSMA operational dashboard layer aims to facilitate the creation of comprehensive sets of views that break down silos and empower different security teams to proactively protect their environments and detect upcoming trends or threats before any damage occurs. Serving as a jump point into the security ecosystem, the dashboard layer enables swift and effective response to security events.

Greymatter Support to CSMA Layer 4

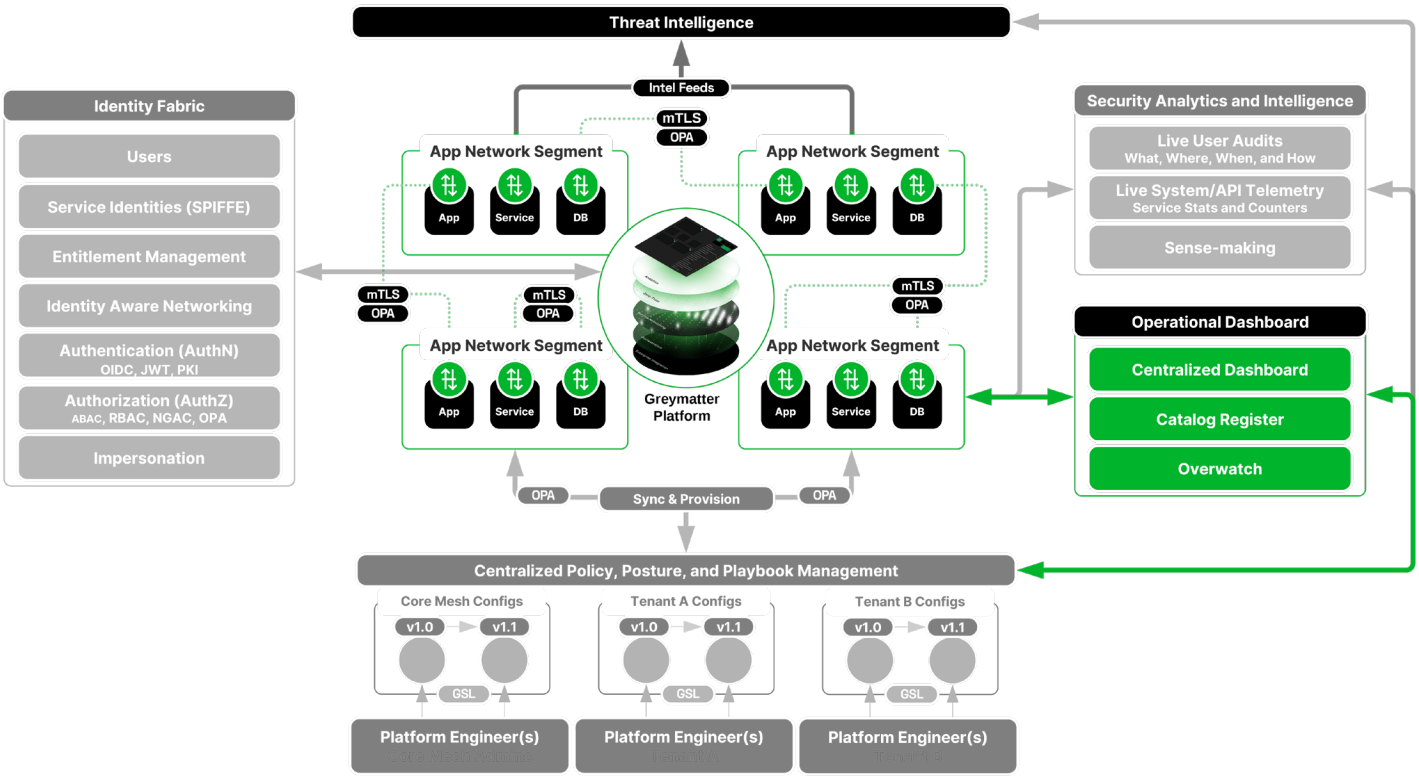


FIGURE 4: GREYMATTER SUPPORT OF CSMA LAYER 4

Greymatter's unified and intuitive platform unlocks the full potential of the **operational dashboard layer,** delivering a single-pane-of-glass view and powerful audit capabilities for visibility and understanding of who is doing what, when, where, and how, across multi-cloud and hybrid environments. Teams can more easily collaborate, manage, and maintain a cohesive security posture and coordinate actions.

Specific capabilities to support CSMA Layer 4 include:

Greymatter enables consolidation of intricate policy files into a centralized hub and then, with under ten lines of code, reference that applies **immediate policy for effortless fleet-wide security policies** updates across to applications, APIs, and data services **in minutes, not days** - regardless of cloud or hybrid infrastructure. Through a **centralized dashboard**, users gain a holistic view of the entire service connectivity layer infrastructure. **One pane of glass** provides This includes unparalleled visibility and control across hybrid, multi-cloud, and hybrid on-premise environments, providing critical insights into every activity occurring across the tech stack. and is inclusive of applications, services, databases, data stream services, and more.

The single-pane-of-glass view enables organizations to quickly assess the health, status, and performance of their network assets, inclusive of applications, services, databases, data stream services, and more. Gaining valuable insights into their operational environment, organizations can make informed decisions, troubleshoot issues more efficiently, and optimize resource allocation for improved operational efficiency.

Network or cloud environments can stay one step ahead with Greymatter's unrivaled capability to effortlessly integrate **immediate forensic user tracking audits** with **zero configurations needed.** The platform streamlines API management with **Catalog Register.** This enables developers and administrators to easily discover, organize, and document their APIs and services and programmatically integrate with other systems and tools. The robust catalog encompasses all operationally running network assets for visualization in one dashboard, empowering teams to efficiently manage and leverage their resources, ultimately enhancing security and compliance across applications, APIs, and services with ease.

Greymatter **immediately tracks and catalogs all applications, APIs, and services,** including health and traffic flow capture for everything connected to the mesh. Greymatter's powerful **overwatch** capability offers real-time insights into the activities taking place within the network, including within multi-tenant spaces for separation of concern. Integration with the centralized dashboard provides a unified view and comprehensive understanding of who is involved, what actions are being performed, where they are occurring, when they are happening, and how they are being executed. Customers gain the power to seamlessly view multiple application mesh networks in a unified interface, featuring health status, dependency lists, and comprehensive search capabilities across clouds. Insights include:

- Real-time health heuristics for proactive monitoring and detection of potential performance issues or anomalies to get ahead of potential service disruptions or degradation.
- Application insights, audits, and scorecards to assess the operational performance of applications or services by route or user. These assist in informed process optimization decision making and help strengthen security within the network.
- Business intelligence and scoring for insights into the business implications of distributed services and data. These are crucial to evaluating cost increases versus reductions, optimize resource consumption, and even make informed decisions about allocating development and engineering time.

Additional capabilities include integration with the other layers of the CSMA framework to ensure smooth information flow and coordination between different security functions. This also includes integration with existing cybersecurity infrastructure, such as SIEMs and SOARs, feeding deep insights that can be leveraged to improve threat detection and response and increase ROI of complementary tool sets.

Benefits of the Greymatter Approach

Challenge	Greymatter Solution	Value
Threat intelligence monitoring and early detection of threats are incredibly difficult to address given limited insights into distributed applications, services, and APIs across many, different infrastructures.	Data streams, audits, and insights enable deeper understanding of the who, what, when, where, and how of activity within the application ecosystem across the entire environment, and fuel faster, comprehensive actions to improve security posture and risk mitigation.	**Improved threat detection, response, and real-time analysis**
Enterprises engaged in mission- critical activities need real-time monitoring of user activities and interactions in a single view and the ability to feed that data into existing security and risk mitigation tools.	Unified views and powerful auditing capabilities of applications, services, and APIs, empower teams to conduct analysis from the tactical to the strategic level, make more informed decisions, and improve security and business operations.	**Centralized management**
As software is deployed and enters operational use, the ability to monitor and manage security in production environments becomes more crucial but less visible and hard to track.	Breaking down silos between teams and tools with access to shared data and visualizations that facilitate communication and coordinated response.	**Increased collaboration**

Greymatter ROI

Greymatter's security features help enterprise IT achieve optimal cybersecurity mesh architecture ROI.

> **Consider this: security incidents are often a major driver of system downtime, with cost estimates ranging from 1 to 5 Million per hour."** [18]

However, other hidden impacts such as legal ramifications, lost productivity, remediation time, and lost business can drive downtime costs for large businesses up to $300,000 per minute. That is $18 million in direct losses for every hour of downtime!

Greymatter's powerful OOTB combination of zero-trust and cybersecurity mesh architecture-enablement cuts down on security incident-induced downtime. Once in place, Greymatter's layered defense in depth delivers continuous value, providing granular access control, real-time health monitoring to help keep the enterprise ahead of potential incidents, and service and network segmentation to minimize the blast radius of incidents when they do arise.

Greymatter also helps ensure the enterprise gets the most out of their SIEM, SOAR, and other cybersecurity investments, serving as a real-time telemetry feeder source enhancing their speed and accuracy for faster diagnosis and remediation.

Finally, Greymatter drives down lost opportunity cost. Not only does the platform stop time and resource-intensive security incidents before they occur, it also automates several tedious tasks such as certificate rotation and policy and configuration management. This frees developers to focus on app and service development, instead of tedious security plumbing.

Greymatter.io

Are you ready to take the next step on your Enterprise IT journey toward Zero Trust and Cybersecurity Mesh Architecture-based security?

Greymatter's service connectivity layer helps platform engineers meet CISO/CIO security requirements by automatically hardening microservices-based software applications across fragmented application networks and clouds.

Reach out to set up your free security assessment today.

Sources

[1] Salt Labs State of API Security Q1 2023 Survey of over 400 industry-wide security, DevOps, and app development professionals

[2] Top Strategic Technology Trends for 2022: Cybersecurity Mesh; https://www.gartner.com/en/doc/756665-cybersecurity-mesh

[3] Salt Labs State of API Security Q1 2023 Survey of over 400 industry-wide security, DevOps, and app development professionals

[4] 2022 IBM Security X-Force Cloud Threat Landscape Report

[5] Source: Gartner Survey results posted at 2023 Security and Risk Management Summit

[6] CyberEdge: ISC2, November 2022; 1,200 respondents to Survey

[7] Salt Labs State of API Security Q1 2023 Survey of over 400 industry-wide security, DevOps, and app development professionals.

[8] CyberEdge: ISC2, November 2022; 1,200 respondents to Survey

[9] 2022 IBM Security X-Force Cloud Threat Landscape Report

[10] Salt Labs State of API Security Q1 2023 Survey of over 400 industry-wide security, DevOps, and app development professionals

[11] Salt Labs State of API Security Q1 2023 Survey of over 400 industry-wide security, DevOps, and app development professionals

[12] Salt Labs State of API Security Q1 2023 Survey of over 400 industry-wide security, DevOps, and app development professionals

[13] Gartner Survey results posted at 2023 Security and Risk Management Summit

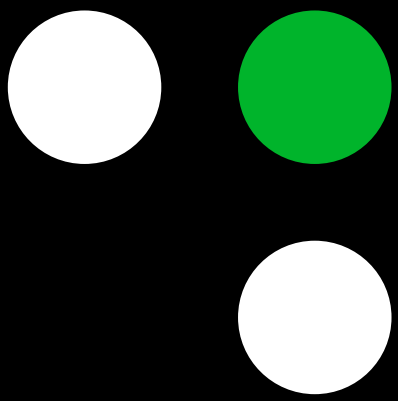
[14] Salt Labs State of API Security Q1 2023 Survey of over 400 industry-wide security, DevOps, and app development professionals

[15] Worldwide Cybersecurity Insiders Survey, March 2022, Fortinet

[16] CyberEdge: ISC2, November 2022; 1,200 respondents to Survey

[17] API Security: Latest Insights & Key Trends Google Cloud 2022 Research Report

[18] Average Cost of Downtime Per Industry; Solarwinds Pingdom; https://www.pingdom.com/outages/average-cost-of-downtime-per-industry



Greymatter.io
www.greymatter.io
info@greymatter.io

LinkedIn
Twitter
Vimeo

4201 Wilson Blvd Floor 3
Arlington, VA 22203