Greymatter.io

Elevate Your Security with NIST 800-207A Compliant Zero Trust for Cloud-Native Applications

1. Introduction

Experience heightened security with Greymatter, perfectly aligned with NIST's 800-207A Zero Trust Architecture Model for cloud-native applications. Greymatter simplifies the transition to a "trust no entity" approach, ensuring rigorous verification for all accessing resources. Move beyond the limitations of traditional perimeter security. Our platform ensures fortified applications, APIS, and microservices across diverse cloud settings, hybrid compute environments, and Kubernetes distributions; directly addressing CISO and CIO security mandates.

With full compliance to NIST 800-207A, Greymatter delivers tangible, state-of-the-art protection benefits to its users.

NIST SP 800-207A Section	Greymatter Score
2. The Enterprise Cloud-Native Platform and its Components	
With Greymatter, customers benefit from a robust, unified platform that not only simplifies service interactions through identity assignments and effortless discovery of all application connectivity across multiple environments but also elevates security. It ensures that every interaction, whether between users and services or among different services, undergoes stringent, policy-driven authentication and authorization checks. Plus, Greymatter's advanced application networking automation capabilities provide flexible networking options, enabling tailored routing strategies and enhanced system resilience. This comprehensive approach ensures seamless, secure, and resilient operations, optimizing both performance and protection.	100%
2.1 Enterprise Infrastructure Layer	
With Greymatter, customers enjoy enhanced security tailored to their organizational needs. Its adaptable control plane design ensures targeted defense, minimizing breach impact by halting potential lateral threats. Plus, through an intuitive CLI and APIs, organizations gain clear visibility and insights into their safeguarded services, ensuring peace of mind and a fortified environment.	100%
3. Designing a Policy Framework for ZTA for Cloud-Native Application Environments	
Benefit from a GitOps-driven policy approach that ensures only authorized individuals enact changes. Our policies are global, concise, clear, and user-friendly, defining precise connection permissions. With our embedded Policy Enforcement Point operating securely without the need for elevated privileges and distinct from application code, you're ensured robustness. Plus, Greymatter's smooth integration with Identity and Access Management (IAM) providers, support for x.509 certificates, and service-level authentication means unwavering, identity-focused security segmentation.	100%
3.1 Functional Components of Identity-Based Segmentation Policies for ZTA	
By default, all traffic is encrypted, ensuring trusted mutual TLS connections. Benefit from our innate ability to securely attest and bootstrap identity for software services. Our certificate automation and integration, provides short-lived, rotating certificates for top-tier security. Using SPIFFE Verifiable Identity Document (SVIDs), we ensure only authorized services connect with each other using strict access policies, enhancing your system's integrity. Plus, our advanced user authentication features issue JWT tokens for end-to-end secure connections. Paired with seamless integrations, Greymatter guarantees users access only what they're authorized for, optimizing both security and accessibility.	100%
3.2 Limitations of Identity-Based Segmentation Policies for Enterprise ZTA	
Benefit from a blended security approach with Greymatter, while network-tier policies are essential for compliance, solely depending on them can be challenging due to their maintenance demands. While identity-based segmentation offers potent policy formation, its standalone use has its hurdles. By integrating both strategies, we offer a more sustainable solution. Our method combines identity-level policies with streamlined network policies, enabling your organization to establish a powerful, flexible, and all-encompassing security framework that not only ticks enterprise governance boxes but also elevates your security and efficiency.	100%
3.3 Multi-Tier Policies for Enterprise ZTA	
With Greymatter, enhance your organization's security uniquely tailored to your needs. Harness the power of both Network-tier and Identity-tier policies, ensuring precise access restrictions. Our seamless integrations with tools and standards like OpenID Connect, built on top of the OAuth 2.0 authorization framework providers, Open Policy Agent and REGO, and SPIFFE guarantee robust future-proof access control. Benefit from our unparalleled flexibility in managing identities, empowering your organization to elevate security and governance, ensuring the utmost protection and controlled access to your resources.	100%
4. Implementing Multi-Tier Policies for ZTA for Cloud-Native Application Environments	
4.1 Reference Application Infrastructure Scenario	
Implement unmatched flexibility and security regardless of where your services and applications are hosted, be it on cloud platforms or on-premises hardware. Experience seamless connectivity coupled with guaranteed encryption for every connection. Our user-friendly configuration language simplifies managing both inbound and outbound connections. Benefit from the ease and speed of integrating Greymatter into your system, ensuring optimal performance and protection.	100%
4.2 Role of the Service Mesh in Policy Deployment, Enforcement, and Updates	
With the Greymatter Data Plane, experience seamless, centralized, and fortified service communication tailored to your policies. Not only does it act as your sole gateway ensuring utmost scrutiny for every connection, but it also equips you with top-notch mTLS encryption, providing valuable metrics and crucial audit insights. Stay updated and fortified, as Greymatter ensures your services utilize the latest TLS versions and ciphers, guaranteeing secure handshakes across all applications and API layers. Streamline, protect, and always be a step ahead with Greymatter.	100%
4.3 Policy Deployment for Reference Application Infrastructure	
With Greymatter, empower your organization with precision-driven application-level policy enforcement, tailored for both service-to-service and user-to-service interactions. Experience unparalleled control, restricting connections using detailed network-tier and Identity-tier policies on any application, API, or service be it a web application or a data serving API. Tailor, enforce, and elevate your organization's security and connectivity standards effortlessly with Greymatter.	100%
4.4 Another Application Infrastructure Scenario	
Harness the power of Greymatter as your edge gateway, seamlessly integrating the DMZ pattern for top-tier application deployment. Benefit from inherent encryption and mTLS, ensuring your edge ingress isn't just connected, but authentically authorized. Dive deeper with configurations that refine service connections, granting permissions exclusively to policy-specified services. This precision control optimizes access within your microservice architecture, elevating security and streamlining operations. With Greymatter, you get precision, protection, and peace of mind.	100%
4.5 Functional Roles of Application Infrastructure Elements in Enforcing Policies	
Experience streamlined operations with Greymatter's Data Plane, strategically positioned to manage all your application traffic, guiding it seamlessly within your environment. Acting as both an ingress and egress gateway, it simplifies configurations, enhancing operational ease. Plus, with Greymatter's edge functioning akin to a top-tier edge gateway, you're assured of consistent functionality and robust security for North/South or regional cross-cluster secure and controlled connectivity. Trust Greymatter for a seamless, secure, and simplified traffic management experience.	100%
4.6 Comparison of Identity-Tier and Network-Tier Policies	
4.6.1 Approaches for Deployment and the Limitations of Network-Tier Policies	
Leverage the power of Greymatter for precision in your service connectivity. With application network interface-driven policies, Greymatter ensures only the right applications, APIs, and services connect with each other. Its user-friendly configuration files offer clarity and ease, granting users a transparent view into the environment's connectivity framework. With Greymatter, enjoy both control and clarity, enhancing your operational efficiency.	100%
4.6.2 Prerequisites for the Deployment of Identity-Tier Policies	
Benefit from Greymatter's advanced security and connectivity capabilities: Harnessing the SPIFFE protocol, each service in your environment is uniquely identified, reinforcing security in every interaction. Plus, Greymatter's tailored control plane promotes seamless service discovery, ensuring reliable connections between services. Trust Greymatter for a secure, smooth, and smart operational experience.	100%
4.6.3 Advantages of Identity-Tier Policies	
Experience seamless policy deployment with Greymatter. Leveraging GitOps procedures, Greymatter ensures policies and configurations are clear and easily understandable, thanks to its concise configuration file. Enjoy enhanced readability and simplicity, streamlining your operations with Greymatter's user-friendly approach.	100%
5. Support for Multi-tier Policies Through a Monitoring Framework	
Benefit from unparalleled transparency with Greymatter. It provides clear insights into network components, authentication, and access control. Not only does it facilitate behavior and metric configurations, but it also ensures accountability with audit-ready logs seamlessly integrated into your enterprise log collection service. Trust Greymatter for clarity, compliance, and comprehensive network management.	100%