greymatter.io

NIST 800-207 Compliance

greymatter.io's
Enterprise Microservices Platform

Introduction

Under a new Executive Order issued on January 26, 2022, federal government agencies are required to move toward the adoption of Zero Trust Architecture (ZTA) by the year 2024, in accordance with NIST Special Publication 800-207. Zero Trust Architecture is based on the principle that nothing can be trusted, a philosophy in which no device, user or application attempting to interact with your architecture can be considered secure by default. The objective behind ZTA is to reduce the risk of security breaches and ransomware attacks that have increased as a result of more federal employees working from outside the office and more federal IT applications, data and resources migrating from centralized, on-premise locations to distributed cloud environments.

Founded outside Washington, D.C. in 2015, greymatter.io's enterprise microservices platform is widely-deployed around the globe throughout mission-critical defense and intelligence environments in compliance with the zero trust requirements needed across federal government agencies. Although our platform is not a cybersecurity solution, it provides federal IT developers and DevOps teams with a secure application development framework that meets CISO and CIO needs to harden distributed software applications by enabling zero-trust security, user authentication, data encryption, certificate rotation, and policy compliance out of the box without writing a single line of code. This whitepaper provides a high-level overview of our platform's compliance with 70 of the 76 criteria set forth in NIST Special Publication 800-207, Zero Trust Architecture, and at least partially compliant with the six remaining criteria, a testament to our security-centric design and implementation.

ABOUT NIST 800-207

The National Institute of Standards and Technology (NIST) released Special Publication 800-207, Zero Trust Architecture in August 2020. The document outlines the core logical components and evolving paradigms of zero trust architecture, serving as a guidepost for the adoption of zero trust security throughout federal government agencies.

Our Methodology

Our technologists conducted an in-depth mapping exercise to compare our enterprise microservices platform's ZTA capabilities against the full list of NIST 800-207 ZTA specifications. The following report details our methodology, findings, and analysis of how our enterprise microservices platform aligns with NIST ZTA standards.

We reviewed each section of NIST 800-207, extracting key tenets and critical components for review and comparison against current Greymatter.io ZTA functions and capabilities. We employed Harvey Ball chart analytics and scoring techniques to grade levels of compliance. We then charted the platform's capabilities against each criterion, weighing our level of compliance based on the current capabilities of our enterprise microservice platform.

- **Harvey Balls** are round ideograms used for the rapid visual communication of qualitative information. They are commonly used in comparison tables to indicate the degree to which a particular item meets a particular criterion.

For the purposes of this exercise, we scored on a range of 0-4 as follows:

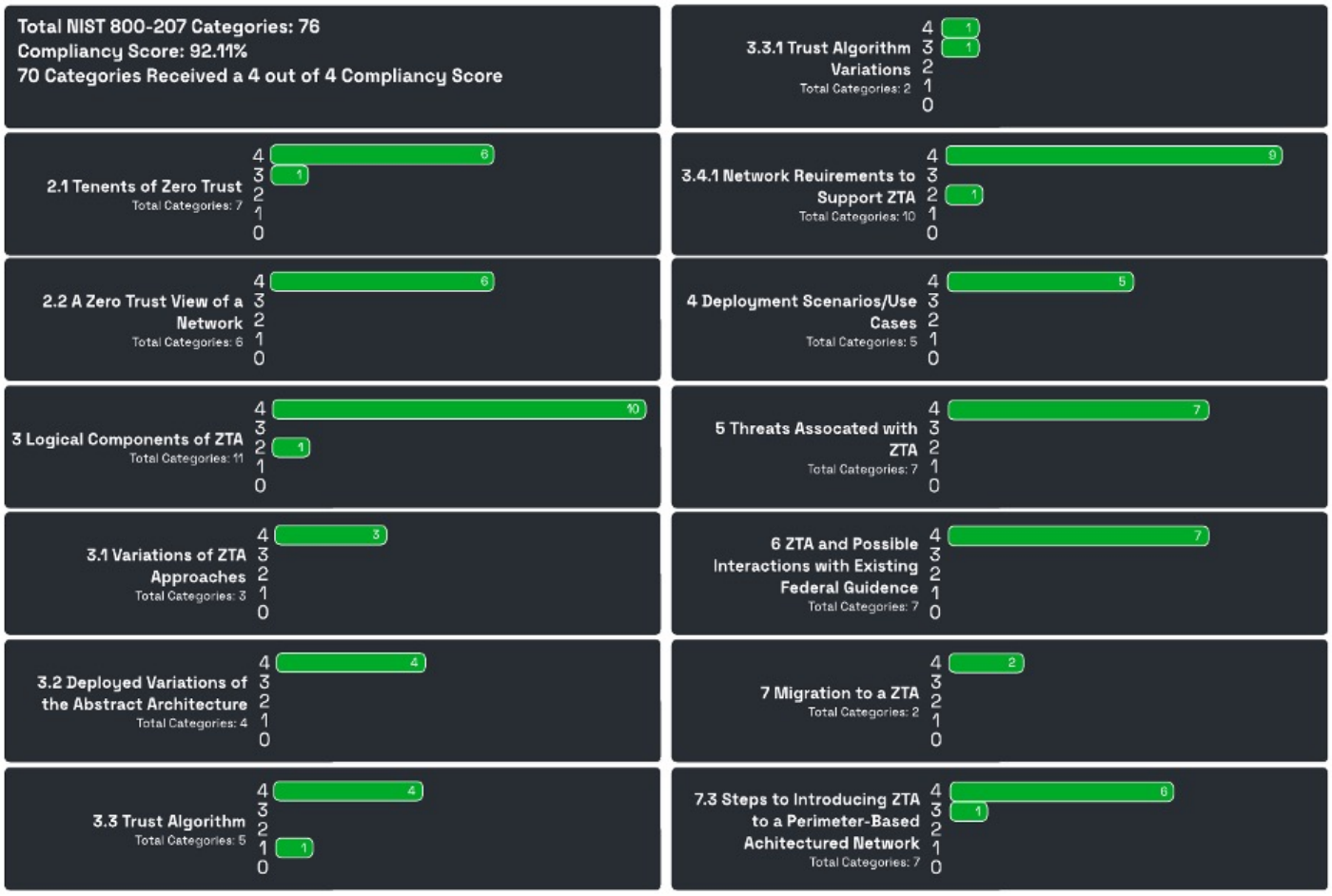
- 0: Does not meet the criteria.
- 1: Partially meets criteria, but unmet aspects are either out of scope or not currently on the roadmap.
- 2: Generally meets the criteria, but gaps exist that are not on the current roadmap.
- 3: Meets majority of criteria, and gaps can be addressed through partnerships or roadmap inclusion.
- 4: Meets all criteria.

Our review surfaced 76 distinct NIST 800-207 specification criteria, ranging from the demonstration of expected best practices to the presence of specific technical capabilities. Each was categorized based on the section of the NIST report from which they were extracted:

- 2.1: Tenets of Zero Trust
- 2.2: A Zero Trust View of a Network
- 3: Logical Components of Zero Trust Architecture
- 3.1: Variations of Zero Trust Architecture Approaches
- 3.2: Deployed Variations of the Abstract Architecture
- 3.3: Trust Algorithm
- 3.3.1: Trust Algorithm Variations
- 3.4.1: Network Requirements to Support ZTA
- 4: Deployment Scenarios/Use Cases
- 5: Threats Associated with Zero Trust Architecture
- 6: Zero Trust Architecture and Possible Interactions with Existing Federal Guidance
- 7: Migrating to a Zero Trust Architecture
- 7.3 Steps to Introduce ZTA to a Perimeter-Based Architectured Network

Our Findings

The following chart identifies each NIST 800-207 category, highlighting the total number of criteria with which we are either 1) fully compliant, 2) demonstrate one identified gap, or 3) demonstrate multiple identified gaps.



Our enterprise microservices platform is fully compliant with 92.11% (70 of the 76) of NIST 800-207 criteria. We are mostly compliant with 3.95% (3 of the 76). We are generally compliant but demonstrate gaps that do not exist on our roadmap with another 2.63% (2 of 76) and are partially compliant with gaps that do not currently exist on our roadmap with 1.32% (1 of 76). There are no categories or criteria with which our platform is not at least partially NIST 800-207 compliant.

Compliance Gap Analysis

The following chart provided details regarding the 6 criteria in which our enterprise microservices platform did not meet full NIST 800-207 ZTA requirements. This chart aligns the primary NIST category with the specific criteria, our score, and the areas in which we comply, accompanied with context explaining why we do not fall within full compliance. In most cases, the platform's lack of compliance stems from opinionated design or the criteria falling out of scope with our platforms' intended use cases.

Category	Criteria	Score	Areas of Compliance	Greymatter.io Context
2.1 Tenets of Zero Trust, Item 5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	3	Our platform will log all information to the enterprise monitoring system for review by enterprise personnel. Our platform will regularly patch for security related vulnerabilities and findings within our suite of software.	Our platform applies security patches to the product but more automation is required to automatically deploy patches to customer environments.
3 Logical Components of Zero Trust Architecture	Continuous diagnostics and mitigation (CDM) system	2	Our platform gathers information about actions being taken by entities attempting to access a service that has been configured to use the service mesh. The platform can enforce policies around identified services that need to be protected from known security vulnerabilities. It can continuously monitor and diagnose issues within the service mesh.	Our platform is not designed to identify and highlight vulnerabilities within an environment and assert backwards compatibility of what sidecars are currently connecting to the mesh.

3.3 Trust Algorithm	Threat intelligence	1	Our platform collects information about connections to assets in the environment and can be used to feed information to a threat intelligence feed. It can be leveraged to mitigate known attack vectors and provide additional security around potential endpoint exploitation.	Our platform does not currently incorporate attack signatures into the PE to look for known threats and vulnerabilities or provide further intelligence around misconfigured systems.
3.3.1 Trust Algorithm Variations	Singular versus contextual	3	Our platform uses a singular TA to evaluate an entity's permissions to service and make determinations based on the roles and responsibilities of the entity.	NIST recommends contextual TA. Since our platform uses a Singular TA, it does make decisions based on the recent activities of a subject. If a threat actor is actively looking at several things that they should not be, the PE will not shut down that potential actor. However, our platform will log all attempts and feed the information for a SOC or NOC analyst to identify this threat and can respond appropriately to the situation.

3.4.1 Network Requirements to Support ZTA	The enterprise can observe all network traffic.	3	Our platform records connections between entities, which could be users to services or services to services.	Our platform does not record packet captures and does not dynamically update the PE as it evaluates requests. If the platform adjusts to a contextual model, then dynamic policy updates would be possible.
7.3.2 Migrating to a Zero Trust Architecture	Identify Assets Owned by the Enterprise	3	Our platform implementation is cloud, hardware, and vendor agnostic. When implemented in an environment, Greymatter.io can discover assets in many types of cloud and container technologies, reporting metrics, logging, and communication channels.	Our platform is not designed to identify and highlight vulnerabilities within an environment and assert backwards compatibility of what sidecars are currently connecting to the mesh.

For two criteria (2.1, 7.3.2), we believe we can meet full compliance with the inclusion of external partner capabilities. NIST criteria 3.3.1 cites a preference for contextual over singular trust algorithms (TA). Our platform employs singular TA out of preference for limiting resource consumption. We also believe the difference in capabilities between singular and contextual TA is offset by our anomaly detection AI. Other items are out of scope with our platform, such as 3, Continuous diagnostics and mitigation (CDM) system, which calls for monitoring the OS for patch levels. Criteria 3.4.1 may warrant additional consideration for our roadmap but is not currently listed as such. The remaining criteria (3.3, threat intelligence) is not fully met because our platform is not currently incorporating attack signatures into the policy engine.

Conclusion

ZTA is critical to ensuring that only the right users can access the right assets and resources across federal IT systems. As proven by this study, our enterprise microservices platform is fully compliant with 70 of all 76 NIST 800-207 ZTA standards, and at least partially compliant with the remaining 6, with areas in which we fall short often due to the scope of platform and opinions on technical requirements.

We stand ready to provide the critical ZTA necessary to support federal government agencies in achieving NIST 800-207 compliance for any cloud migration or software modernization effort that requires bridging legacy, on-premise environments with modern, cloud-native applications.

greymatter.io builds our enterprise microservices platform for enterprise microservice, container, and hybrid cloud operations.

greymatter.io
106 N. Lee Street, Floor 2
Alexandria, VA 22314

1 (877) 356-3011
greymatter.io