tetrate

Tetrate Zero Trust Solutions for Federal Agencies

Modernize and strengthen your cybersecurity posture, reduce risk and better control access, assets and users while meeting Federal mandates for Zero Trust architecture

At a Glance

- A Zero Trust approach helps organizations modernize and strengthen their security environment in order to limit or prevent attacks.
- An Executive Order on improving the nation's cybersecurity instructed the government to move towards Zero Trust by 2024.
- The service mesh provides essential capabilities for effective Zero Trust.

Zero Trust Defined

- Zero Trust eliminates the idea of a trusted network edge and assumes that any user or service requesting access is a potential threat, regardless of whether they are inside your network or how many times they have connected before.

Why Zero Trust?

With the goal of modernizing cybersecurity defenses and protecting federal networks, Executive Order 14028 mandates cybersecurity improvements by the end of Fiscal Year (FY) 2024. A Zero Trust architecture (ZTA), as defined by the U.S. National Institute of Standards and Technology (NIST) in Special Publications 800-207 and 800-207A offers a strategic approach to cybersecurity that simplifies and unifies risk management under one important goal: eliminating implicit trust in every digital transaction. The Zero Trust model is built on three core concepts:

1. **Assume all network traffic is a threat, at all times.** Zero Trust takes the view that every user is hostile and that threats are omnipresent, both inside and outside the network. Therefore, any traffic that does not have explicit permission is automatically denied access. Every device, user and network flow is authenticated, authorized and validated when requesting access on an ongoing basis.
2. **Enforce least-privileged access.** Zero Trust security approaches grant least-privilege access, the minimum privileges and access to the necessary resources when they are needed without impacting the ability to complete a task. Least-privilege access helps restrict attackers from moving laterally to more critical resources if an account or device is compromised.
3. **Always monitor.** The Zero Trust model advocates for continuous monitoring and analyzes and manages activity on the network at all times. This enables real-time understanding of what entities are trying to access and helps identify potential threats, active incidents and any anomalies that should be investigated. In practice, Zero Trust entails continuous authentication, authorization and monitoring of activities across all networks.

Zero Trust Benefits

- Mitigate risk of security and data breaches
- Reduce attack surface
- Improve visibility and control
- Continuous compliance

The goal of Zero Trust is to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud or a combination of hybrid with resources anywhere as well as workers in any location.

NIST Standards

Tetrate works directly with NIST to develop Zero Trust architecture frameworks. Several of the publications and guidelines on ZTA, including (SP) 800-207 and 800-207A, were co-authored by Zack Butcher, a founding engineer at Tetrate. In NIST's SP 800-204 series of security standards for microservices applications, they establish a reference platform that incorporates Kubernetes for orchestration and resource management, with the Istio service mesh providing core security features. These functionalities include:

- Service identities and service discovery
- Traffic routing and resiliency functions such as retries, timeouts, blue-green deployments and circuit breaking
- Assurance of application integrity and confidentiality through service-to-service and user-to-resource authentication and authorization
- Integration with external policy-based authorization engines, such as Next Generation Access Control (NGAC), Attribute-Based Access Control (ABAC) and Open Policy Agent (OPA) automation. This integration is vital for establishing a robust and sustainable security program.

Why Tetrate?

- Tetrate aligns with the NIST 800-207 framework to accelerate Zero Trust adoption across government in accordance with EO 14028 and OMB M-22-09.
- Runs in any hybrid, multi-cloud environment.
- FedRamp Certified.
- First FIPS-compliant Istio distro.

A Service Mesh Provides Essential Capabilities for Effective Zero Trust

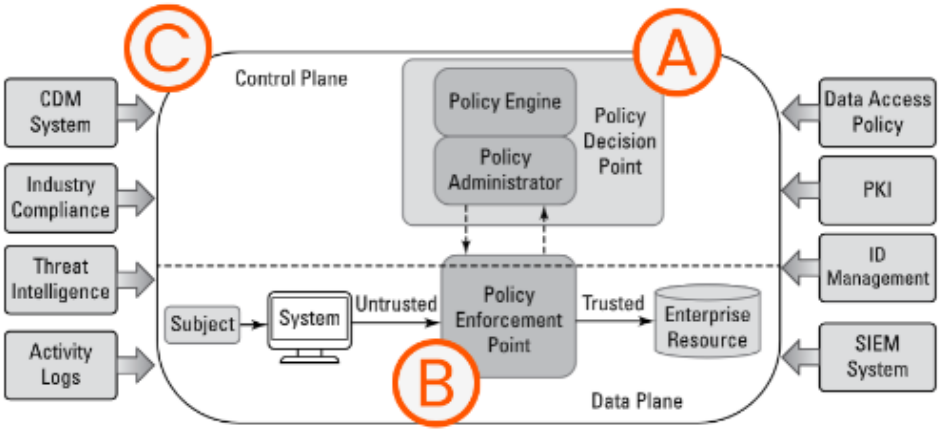

FIGURE 1-1: Logical components of a zero trust architecture.
(Source: NIST SP 800-207, *Zero Trust Architecture*)

A- Istio Control Plane: Policy decision point (PDP).
B- Envoy Data Plane: Policy enforcement point (PEP).
C- Service Mesh: Modern cloud-native security kernel.

"The control plane of the service mesh acts as the **policy administration point**, while the underlying policy tools become the **policy decision point**. In addition, the control plane also enables those policies to be distributed to the various proxies described in the previous section. Once distributed, these proxies intercept all traffic in and out of the applications, where it acts as a **universal policy enforcement point**. This allows the service mesh - which centrally manages a fleet of the applications' proxies - to become the modern cloud-native security kernel" NIST SP-800-207A § 4.2

Tetrate aligns with the NIST 800-207 framework, adopted by government and enterprise organizations to enable security in today's multi-cloud environment. Tetrate's Application Networking and Security Platform provides a dedicated infrastructure layer that manages service-to-service communication, typically through a sidecar proxy deployed alongside each service.

This enables agencies to implement several essential security capabilities to support ZTA:

1. **Authentication and Authorization:** The service mesh enforces robust authentication and authorization mechanisms for all service-to-service communications. This ensures that only authenticated and authorized services can communicate with each other, mitigating risk of unauthorized access.

2. **Microsegmentation and identity-based segmentation:** The service mesh provides advanced microsegmentation and application-level, identity-based segmentation capabilities, allowing agencies to configure granular access control for different segments based on both networks and workload identities. In a Kubernetes setup, Tetrate-managed workspaces span across multiple clusters to provide amenable access control across microsegments.

3. **Secure Service-to-Service Communication:** The service mesh facilitates secure communication by encrypting traffic between services. It can enforce the use of mutual Transport Layer Security (mTLS) to authenticate both ends of the communication and establish encrypted channels, reducing the risk of eavesdropping and tampering.

4. **Traffic Monitoring and Visibility:** A service mesh provides observability for communication between services, allowing organizations to monitor and analyze communication patterns. This enables the detection of anomalous behavior and potential security threats, enhancing overall network security.

5. **Centralized Policy Enforcement:** With a service mesh, organizations can centrally define and globally enforce fine-grained policies for service-to-service communication. This includes policies related to traffic routing, access control and data protection. By consistently applying these policies, organizations can maintain strict control over communication flows and reduce the attack surface.

Benefits

Cyber threats and vectors are constantly evolving. The ability to not trust any connection without proper verification is essential given the amount of cloud, endpoint and data sprawl in today's multi-cloud IT environments. Plus, the increase in visibility will make life much easier for IT and security from the administrator level all the way up to the CISO.

Application Team	Reduce microservices complexity and improve reliability for application releases.
Platform Team	Deliver a more robust and secure platform infrastructure with a reduced attack surface, improved visibility and control, continuous compliance with and the ability to adapt to evolving threats.
CISO	Build a NIST 800-207-compliant Zero Trust architecture. Mitigate risk. Scale business and cloud innovation, securely.

How Tetrate Supports Zero Trust Adoption

1. Tetrate's Application Networking and Security platform helps streamline and action many of NIST's SP 800-207A recommendations by extending visibility, analytics and response capabilities across endpoint, identity, cloud and network surfaces.
2. Behind our software is a team of experts supporting you at each step of your Zero Trust journey.
3. Additionally, Tetrate's team includes people involved with the Istio and Envoy projects since inception. They regularly contribute to open source projects within the ecosystem and are part of technical oversight and steering committees.

Additional Resources

Discover how a Zero Trust architecture can improve your security posture and fortify your defenses against modern cyber threats.

Visit **tetrate.io/zero-trust**

Get Started

Take your first step towards Zero Trust. Contact the Tetrate federal team, visit tetrate.io/government or subscribe to our blog.