tetrate

White Paper

Service Bridge

Bridging Brownfield and Greenfield

by Shriram Rajagopalan

Istio

envoy

Executive Summary

Tetrate Service Bridge, powered by Istio and Envoy, is a self-service, multi-tenant platform to weave and manage the service mesh across VMs and Kubernetes clusters, on-prem and cloud. Developers, security engineers, and operations engineers across multiple teams can safely and securely manage their services without impacting others. A rich set of ecosystem integrations will simplify adoption in enterprise environments.

Background

Fortune 1000 organizations today are typically straddling two types of infrastructure: brownfield (typically on virtualization platforms like VMware vSphere, in addition to mainframes, database appliances, network security boxes, etc.), and "greenfield" (containerized applications on Kubernetes that are heavily automated for continuous integration and delivery). Businesses transitioning to microservices inevitably face three major hurdles: managing traffic flow, maintaining operational visibility, and enforcing consistent security policies across all services.

Service meshes solve these problems by weaving a uniform service management fabric across polyglot services using dynamically programmable layer-7 proxies that facilitates traffic management, consistent monitoring, authentication, and authorization. A service mesh such as Istio, setup in the right manner across brownfield and greenfield, is an ideal vehicle to accelerate brownfield transformation through safe and incremental migration of mission-critical legacy applications. But there are still several gaps when integrating open source service mesh solutions into traditional enterprises composed of heterogeneous infrastructure. Some of the key gaps include the ability to seamlessly integrate VM workloads, multi-tenancy and controlled access to configuration changes, and resilient multi-cluster deployment across multiple data centers.

What should an Enterprise Service Mesh Look Like?

Handle Infrastructure Heterogeneity

Compute and network infrastructures evolve constantly. Traditional VM-based workloads constitute a lion's share of enterprise deployments today. At the same time, enterprises have begun to adopt Kubernetes in house as well as on cloud. An enterprise service mesh solution should absorb this infrastructure heterogeneity seamlessly. A solution that simplifies onboarding and management of VM-based workloads will allow you to easily migrate and refactor applications from VMs to Kubernetes, or brownfield to greenfield.

In addition to absorbing heterogeneity, the mesh solution should also abstract away the compute and network layers for its end users. When configuring a service mesh for an application, developers and security engineers shouldn't have to think about whether the application is running on VMs or Kubernetes, on-prem or in the cloud, nor should they worry about network connectivity in this heterogeneous setup. Successful handling of heterogeneity will allow your teams to impose a uniform set of controls across all services, brownfield or greenfield alike.

Balance Cost & Resilience

Applications may be deployed on many clusters for redundancy, across on-prem and cloud, in one or more regions. Again, the consumers of these applications within the mesh should be oblivious to its location. At the same time, the underlying mesh infrastructure should allow you to take the most cost-effective route to the target. This is achieved by routing to the deployment in the same availability zone, if it is within the load threshold, before considering a (costlier) deployment in a different region. This capability should be fine-tunable so that you can make such a tradeoff at global and per-application level.

Multi-Tenancy & Compartmentalization

When your platform team weaves the service mesh across a heterogeneous infrastructure, they need to ensure that the fabric provides a sufficient level of isolation to each team on-boarded into the mesh. Accidental or willful tampering (insider exploit) of another team's configuration should be prevented. Istio's APIs are modular and composable. Consider an example of two teams accessing a shared service in the infrastructure. Istio's layer-7 routing rules enable you to perform transformations such as path rewrites before forwarding the traffic to the shared service. If two teams were to set up conflicting layer-7 routing rules for the same shared service, without proper isolation, traffic from both teams will be affected.

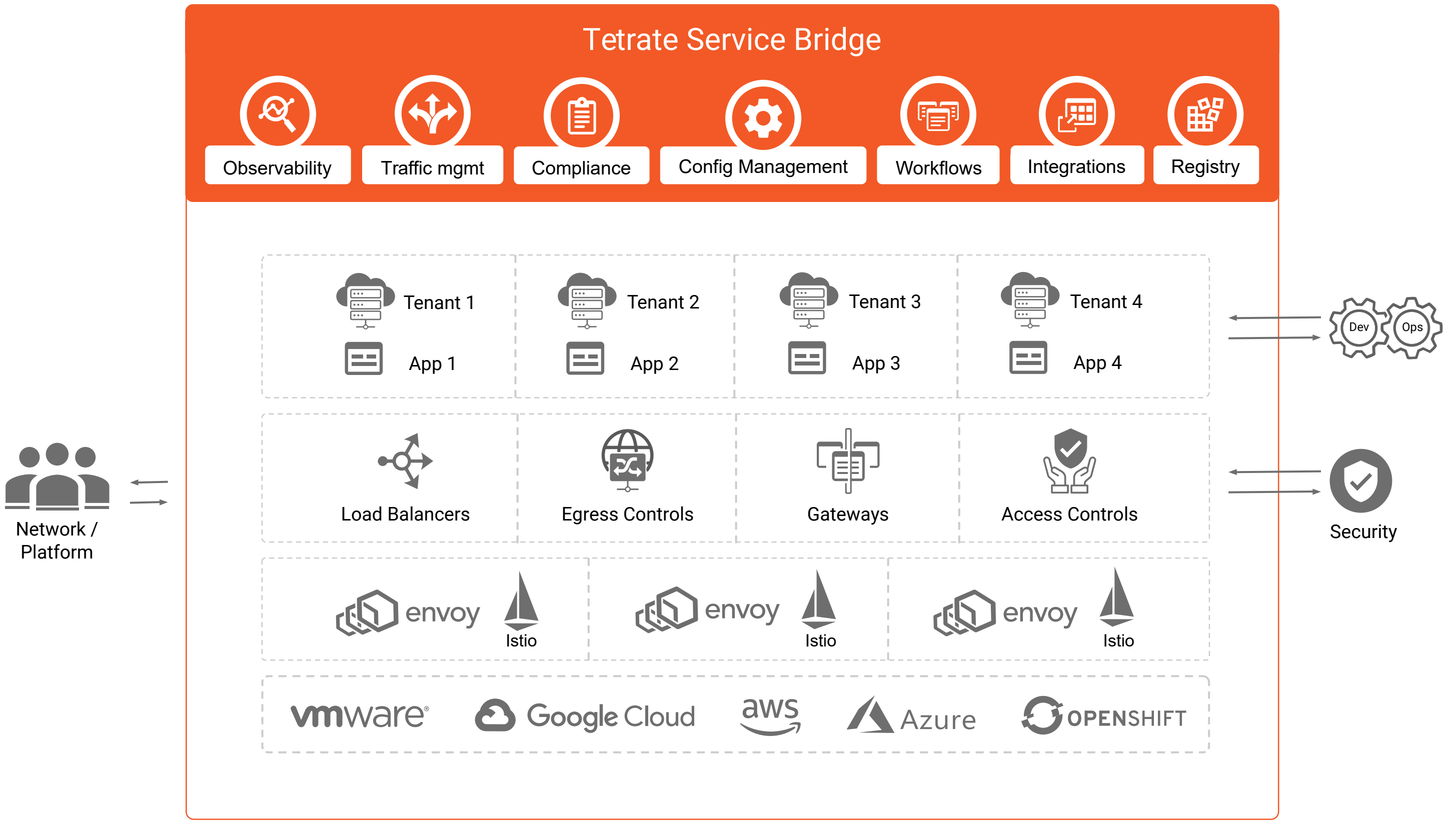
The service mesh solution should allow your engineers to easily and safely manipulate only services they own, and only features pertinent to their role. A developer may wish to do a few URL transformations and enhance application resilience through timeouts, retries, circuit breakers, etc. The security engineer, on the other hand, would want to ensure that all data in transit is encrypted, properly segmented, authenticated and authorized. The platform owner operating the service mesh may care about how a network path is taken by requests across different compute types (e.g., Kubernetes and VMs). The solution should isolate different roles and teams such that users are capable of impacting only resources they own, and only the configurations related to their role. Open source service meshes aren't built for this kind of compartmentalization. They are, by design, an infrastructure-level platform offering a set of modular APIs that need to be combined together to achieve a desired outcome.

Approval Workflows

Shared resources such as a common ingress gateway may be owned by the platform team. However, different teams should still be able to propose changes to these shared resources (e.g., exposing their applications). Workflow systems enable various stakeholders to review change requests, approve or request further changes. The desired changes can be staged, such that they could be applied during a specific change window.

Tetrate Service Bridge

Tetrate Service Bridge (TSB) provides a uniform service fabric across VMs and Kubernetes, multiple clusters and hybrid cloud environments with a single pane of glass to operate the mesh. Built by founders of the Istio service mesh, the product uses OSS Istio as its core service mesh and provides a suite of enterprise-friendly features that accelerate your modernization journey.



Different Teams, Different Infrastructures, Different Processes.

Tetrate Service Bridge: One Operator Experience for All

Mesh Lifecycle Management

A distribution of TSB includes a vetted version of Istio & Envoy with all the latest security fixes and enhancements. TSB takes over the lifecycle management of Istio and Envoy across any number of clusters on-prem and in cloud, including easy installation and automatic upgrades of the control plane as well as the sidecars and gateways of the data plane. Because TSB decouples control and data plane lifecycles, platform teams can manage control plane upgrades centrally while application teams upgrade the data plane alongside their normal application lifecycle. Platform teams deploying TSB can continuously monitor the health of the service mesh across clusters via a single pane of glass.

Seamless Integration of all Compute Types

TSB treats VMs as first-class citizens, just like pods on Kubernetes clusters. By integrating with VMware vSphere®, VMs in on-premise environments can be effortlessly onboarded into the service mesh. Services on Kubernetes can securely communicate with services on VMs, and vice versa using the ambient mutual TLS authentication in Istio. Once integrated into the mesh, the team owning the service on VM can gradually migrate into Kubernetes without disruption to any of the service's consumers.

TSB is agnostic to the compute locality. The mesh established by TSB can span across clusters on-prem and cloud irrespective of the network, enabling the organization to bring all the services under a single fabric.

Multicluster with a Focus on Your APIs

TSB's multicluster model is designed around the application developer and not around the network admin. An application, in TSB parlance, is a composition of one or more services, fronted by a logical API gateway that routes API calls to appropriate backend services. While other services in the mesh consume these APIs exposed at the gateway, the backend is free to evolve from monolith to microservices, without breaking compatibility. The DNS hostname of the application resolves to the logical API gateway, irrespective of the location, or infrastructure type (VM or Kubernetes). This model allows developers to consume APIs without worrying about its locality or internal implementation, as well as expose APIs without being encumbered by an existing application architecture.

TSB takes care of resolving the DNS query within the client service, intelligently figuring out routing and mutual TLS authentication, as well as imposing cross-organizational access controls as configured.

Smart Geo-Routing

Applications can be deployed on multiple clusters in one or more regions, for redundancy purposes. Choice of a replica is determined by the caller locality, health of the application, and policy issues (e.g., GDPR). Within the mesh, TSB configures the mesh to intelligently choose the closest locality to the caller, to reduce cross-region data transfer costs, and fail over to the next closest locality upon detecting failure. To facilitate intelligent load balancing for internet traffic, TSB exposes application health metrics to your organization's DNS load balancer (i.e. GSLB) so that it can decide the appropriate location to route traffic to. You can configure global failover policies in addition to letting application teams configure failover individually. A combination of these two techniques will ensure the best balance between reducing operational costs and maximizing the overall availability of the application.

Multi-Tenancy Based on Organizational Hierarchy

Each team gets access to a set of services in the mesh that they can then configure accordingly. Hundreds of teams can comfortably co-exist on the same service mesh established by TSB, irrespective of whether the underlying infrastructure is shared or not. Platform teams can rest assured that no two teams can step on each other's toes by misconfiguring the other's resources. With the help of hierarchical teams in TSB, a platform team in a large organization can create a self-serve model wherein a single team from a business unit can be onboarded first and allowed to onboard other teams in the unit on their own.

Role-Centric UX

One or more teams are involved in successfully running an application in production in the enterprise. Each team is typically responsible for a specific facet of the application such as business logic, monitoring, security, etc. In more modern enterprises, a single team is usually responsible for all aspects of the application. Whether it is a single team or multiple teams, the set of different roles involved remains the same.

TSB provides sufficient compartmentalization and isolation across roles to ensure that they don't step on each other's toes. For example, through TSB, a security engineering team can group a set of related services and impose a consistent set of Istio authentication and authorization policies on them. They won't need to worry about the developer-specific settings or the cluster and the namespaces where the services will be deployed, or whether they are running on a VM or Kubernetes pod. Such focused experiences allow multiple types of users managing an application to co-operate effectively.

Use cases for Tetrate Service Bridge

Manage workloads running on bare-metal, VM, k8s and cloud

Manage workloads running on bare-metal, VM, k8s and cloud
Tetrate Service Bridge provides a multi-cluster control plane extending to VMs, bare metal and multiple Kubernetes clusters.

Achieve safety and efficiency with multi-tenant mesh
Different business units and different teams can manage their application and service configurations safely on shared infrastructure with workflows and multi tenancy.

Manage SLOs for services and maintain business continuity
Manage ingress and egress of traffic for all services and seamless disaster recovery between services and application instances across clusters, data centers and clouds, maintaining high availability while modernizing. Achieve cost-optimized load balancing out of the box.

Obtain complete inventory of services and interactions
View runtime topology of all your services across clusters, data centers and clouds along with health of all service-service communication and customizable alerts on service operations and configuration changes.

Simplify compliance programs like PCI, FISMA
Risk-based scoring of services and access paths enables protection of your sensitive data and services and simplifies compliance.

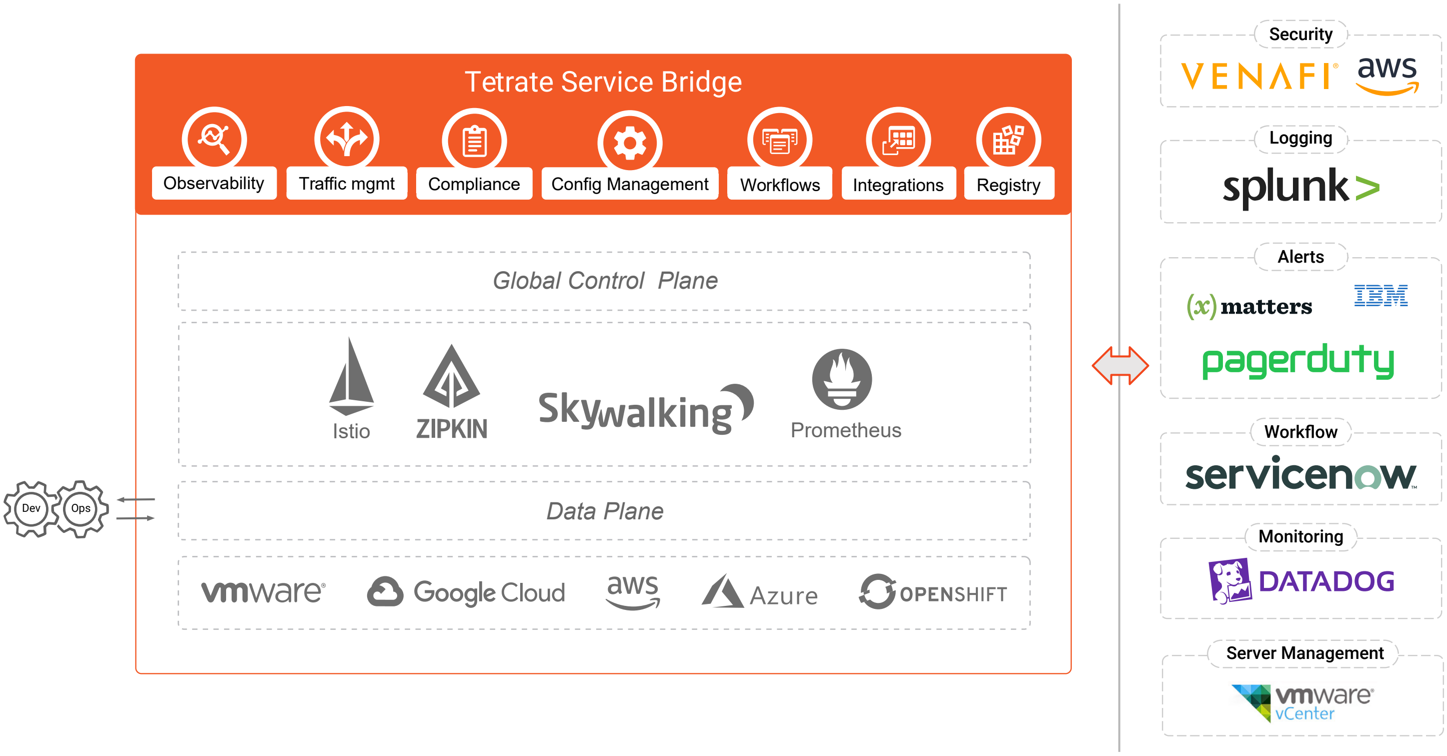
Keep your service mesh updated with latest version and security fixes
Get seamless security patches and upgrades for all Envoy, Istio, and Tetrate Service Bridge components as well as platform troubleshooting and support for the entire stack.

Workflows to Streamline Change Management

Workflows in TSB respect existing change management practices in organizations. Production changes to the service mesh configuration can be configured to trigger a ServiceNow® workflow that can be approved by all the stakeholders before being pushed to the Istio control plane. In addition, teams can also propose configuration changes to shared resources owned by the platform team, such as cluster level gateways. These changes are queued for review and approval by the resource owner before being pushed to Istio.

Ecosystem Integration

TSB ships with a rich set of integrations to ease the adoption of the platform in your enterprise infrastructure. On the compute side, TSB integrates with VMware vSphere® to simplify onboarding of VMs in the enterprise. Integration with Venafi® Trust Protection Platform allows the information security team to continue to use and monitor Venafi as a common store for all certificates in the enterprise. TSB can kick off workflows for change requests into ServiceNow®, allowing the existing change management team to review critical changes before approving them for production.



TSB Integration

Plus all the Features of Istio

The Istio service mesh, at the core of TSB, provides flexible routing controls, request tracing through Zipkin, mTLS & JWT authentication, authorization controls, ingress and egress gateways. And you get a uniform set of metrics that can be piped to a Prometheus service or to your inhouse Elasticsearch using ApacheSkyWalking.

Get started quickly with Tetrate

Enterprise ready service mesh for any workload on any environment

Contact Us   Schedule a Demo

About Tetrate

Tetrate enables a safe and fast modernization journey for enterprises. Built atop Envoy and Istio, its flagship product, Tetrate Service Bridge, spans traditional and modern workloads so customers can get consistent baked-in observability, runtime security, and traffic management—for all their workloads, on any environment. In addition to the technology, Tetrate brings a world-class team that leads the open Envoy and Istio projects, providing best practices and playbooks that enterprises can use to modernize their people and processes.

Location: Tetrate, 691 S Milpitas Blvd, Suite 217, Milpitas, CA 95035, USA

www.tetrate.io | info@tetrate.io