VMware Tanzu Service Mesh built on VMware NSX

At a glance

Tanzu Service Mesh provides advanced, end-to-end connectivity and security for modern applications — across end-users, microservices, APIs, and data — enabling compliance with service level objectives (SLOs) as well as data protection and privacy regulations.

Key benefits

Multi-cloud, multi-runtime support
Tanzu Service Mesh gives teams choice and control over which technologies and locations are most appropriate for their applications in order to meet performance, reliability, security, and compliance objectives.

DevSecOps integration
By integrating data security into existing DevOps tools and CI/CD pipelines, developers now have self-service for their application and data security needs, and can implement Shift Left testing to increase feature velocity, improve software quality, reduce business risk, and more thoroughly enable security compliance for applications.

Transformation across datacenters, cloud, and applications

Trend 1: Datacenter transformation

Enterprise IT organizations are aggressively pursuing data center transformation strategies and accelerating their workload migration to the cloud. They are overhauling their infrastructure and transitioning to the public cloud to improve performance, efficiency, regulatory compliance, and cost models. This transformation includes, among other changes, expansion or a complete migration to the public cloud, adoption of Kubernetes and application/container platforms, CI/CD automation, and operational consistency across environments.

Challenge: Application teams lack seamless connectivity, security, and observability across different platforms and clouds. They are also looking for an application-centric approach that enables developers to efficiently connect and secure traffic between services, APIs, and data — without having to worry about the underlying networking and security infrastructure.

Trend 2: Shift-left testing/DevSecOps culture

With the adoption of a DevSecOps culture, security teams are working closely with operations and developers to bake security controls and security testing into the stages of the CI/CD pipeline.

The combination of DevSecOps culture and shift-left testing, in which testing is performed earlier in the software development process, has drastically improved software quality and security.

Challenge: However, outdated security practices designed for long software development cycles (SDLC) are pervasive in the enterprise — with security testing done on an adhoc basis or taking place late in the process, usually just before going to production — and can undermine a team's DevSecOps initiative.

Trend 3: Microservices architectures

Enterprises are implementing cloud-native application patterns as part of their application transformation initiatives. They are using distributed microservices architectures for their applications to foster innovation, reduce time-to-value, and support developer technology choice. Innovative enterprises are also using APIs to share data and services within and outside organizational boundaries.

End-to-end transaction visibility and policy control

Tanzu Service Mesh gives teams visibility and policy control based on what matters most to the business — that is, end-users, applications (services, APIs), and data (i.e., business fabric) — rather than just services. This deep, end-to-end transaction-level awareness helps to streamline compliance with application SLAs as well as data protection and privacy regulations.

Challenge: Adopting distributed application architectures means teams have many more decentralized services and APIs to monitor and secure. Additionally, transformation always coincides with periods of time in which old and new technologies exist simultaneously. Enterprises not only have a need to consistently connect and secure their microservices and APIs, but also their workloads deployed on virtual machines. It can be challenging to implement application connectivity and consistent security policy across such heterogeneous architectures.

What is Tanzu Service Mesh?

Tanzu Service Mesh (Tanzu Service Mesh) provides end-to-end connectivity, resiliency, security, and insights for modern applications running in single and multi-cloud environments. Tanzu Service Mesh is a leader in service mesh innovation, providing policy control and visibility across end-to-end communications from application end-users, to services and APIs, to data (e.g., PII and PCI data), and enabling compliance with service level objectives and data protection and privacy regulations. Tanzu Service Mesh streamlines and accelerates the deployment and management of application-level policies for application developers, security, and operations — and simplifies automation of CI/CD pipelines, DevSecOps, and related application workflows across multi-cloud environments.

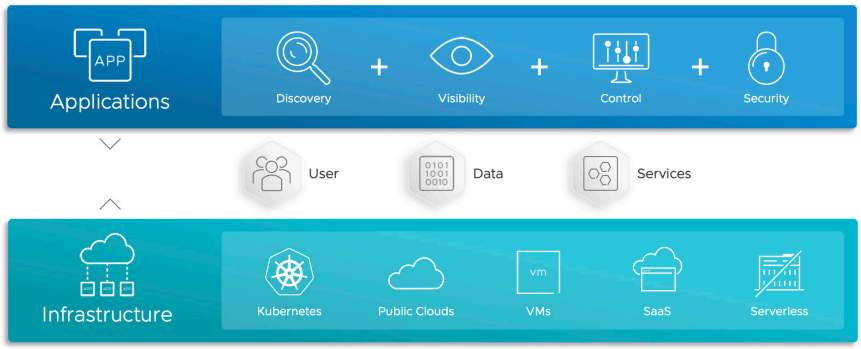

Figure 1: Tanzu Service Mesh application connectivity services.

Key capabilities

Seamless application connectivity and security for multi-cloud and multi-runtime service bridging

Tanzu Service Mesh provides boundless extensibility for distributed application architectures and helps to accelerate the journey to microservices. Tanzu Service Mesh provides a global management plane to streamline application management and operations across single and multiple clusters, clouds, and data centers. Unlike vendors that offer service mesh for their stack/services only, Tanzu Service Mesh provides service mesh capabilities across Tanzu and other third-party Kubernetes providers. Tanzu Service Mesh is used by enterprises with VMware Tanzu (TKG) and Tanzu Application Platform (TAP), and/or with third-party application platforms and cloud services such as RedHat OpenShift, Amazon AWS (EKS), Google Anthos (GKE), and Microsoft Azure (AKS).

Codify data security policies and security testing into the CI/CD pipeline to enable DevSecOps and shift left

Tanzu Service Mesh helps DevOps build, test, deploy, and run applications with data security in mind. Tanzu Service Mesh enables teams to make security and compliance available as a service to developers and to deliver secure applications to market with greater speed. Teams can build data security policies and security testing into their existing DevOps tools and CI/CD pipelines. Declaring policies as code helps teams to shift data security to the left — into the Continuous Integration (CI) and Continuous Delivery (CD) phases — which allows them to automatically and continuously identify and fix misconfigurations, and detect vulnerabilities and security bugs before their applications run in production.

End-to-end transaction visibility and policy control — across application end-users, services, APIs, and data

Tanzu Service Mesh provides visibility and policy control for end-to-end application communications — across an entire business fabric consisting of end-users, applications, and data. Tanzu Service Mesh is able to track complete transactions — from the point an application end-user makes a request and continuing as that request flows through the service mesh — including services, APIs, and data (databases and data elements). Rather than defining control on a hop-by-hop basis (e.g., Service A can talk to Service B) or on a per pod basis (e.g., Horizontal Pod Autoscaler), Tanzu Service Mesh enables application teams to implement context-aware policies to ensure performant and secure transactions. In addition to rich transaction-level metrics and visualizations, Tanzu Service Mesh offers application and data-level security policies — for example, attribute-based access control (ABAC) policies, end-to-end encryption policies, API segmentation, threat protection policies, and SLO-based policies combined with graph-aware autoscaling policies.

	Tanzu Service Mesh Advanced Edition	Tanzu Service Mesh Enterprise Edition
Value	• Multi-cloud service mesh with advanced application connectivity, continuity, resiliency, and security.	• Multi-cloud service mesh with advanced application connectivity, continuity, resilience and security. • Contextual, high-fidelity observability and security policies for APIs and API traffic with developer-friendly tooling.
Persona	Tanzu Service Mesh Advanced is designed for Platform Owners, Cloud Ops, DevOps teams.	Tanzu Service Mesh Enterprise is designed for Application Owners, Developers, Security Architects, SecOps teams.

vmware®

Copyright © 2021 VMware, Inc. All rights reserved. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001
VMware and the VMware logo are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware products are covered by one or more patents listed at vmware.com/go/patents.