

Rafay Service Mesh Manager

Centrally Manage all Application Traffic for your Kubernetes Infrastructure

TECHNOLOGY BENEFITS

Application Security

Provides fleet-wide inter-service connectivity including automated deployment, consistent delivery of application authentication, configuration, and mTLS encryption

Standardized Installation Profiles

Provides fleet-wide automated deployment and consistent delivery of applications

Microservices Observability

Enables real-time and historic replay into traffic flow connectivity visibility, latency, and errors

BUSINESS BENEFITS

Strengthen Application Security

Cluster-wide encryption between application services and CA authentication across the fleet

Faster Application Delivery

Simplified automation accelerates service delivery, policy updates, and full life-cycle cluster management

Reduce Service Outages

Consistent application policies and enforcement to reduce cluster misconfigurations, non-policy changes, application security and enforcement

With Service Mesh Manager, one of several services available on Rafay's Kubernetes Operations Platform, platform teams can automate Service Mesh management across clusters, clouds, and hybrid environments, enabling mutual TLS (mTLS) between services by default while allowing developers to simplify managing traffic routing policies for their applications. Service Mesh Dashboards, shown in Figure 1, provide real-time and historic replay views to accelerate troubleshooting, improve observability, and validate traffic management policies.

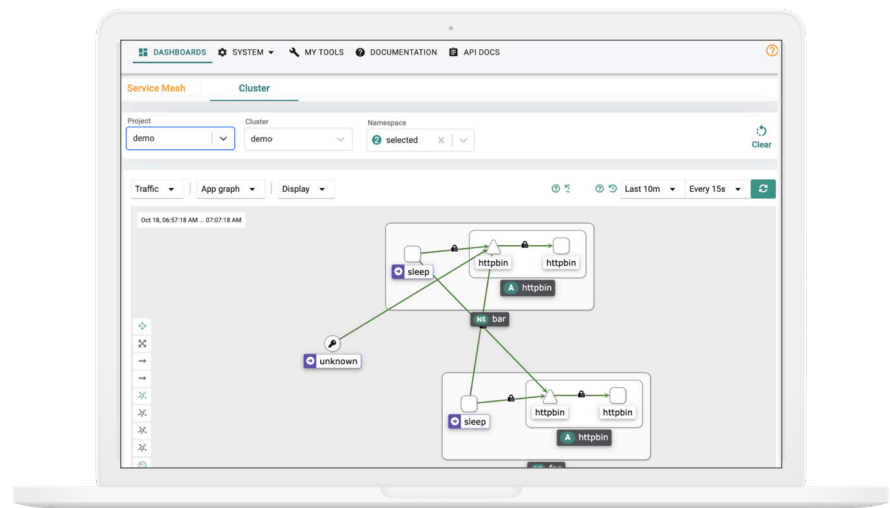


Figure 1 - Service Mesh Dashboard View

The Challenge

As the migration to microservices grows, organizations and operational teams run into challenges at scale in terms of application authentication and authorization, traffic routing, encryption, and security controls for inter-application services. This is why CISA recommends using application authentication, authorization, and encryption in their [Kubernetes Hardening Guide](#).

Enterprise requirements that solve these challenges include:

- **Secure application-level communication**, including fleet-wide secure authentication, authorization, and application traffic
- **Governance and standardization** for multi-cluster application policy, enforced configuration, and security compliance
- **Service Mesh Automation** and enforcement of application policy installation, configuration, and upgrades
- **Real-time and historical observability** into application traffic flows and reducing time to resolve issues

Key Capabilities of Service Mesh Manager

Service Mesh Manager, powered by Istio, is a service that allows defining how microservices and applications communicate and share data. This removes the burden and operational overhead of enabling application policy automation, standardization, and governance across your fleet of clusters and applications using disparate DIY tools.

The Service Mesh Manager provides:

- **Centralized Application Policy Enforcement:** Service Mesh policy management to secure (mTLS) and control cluster-wide inter-service communication, including application authentication, authorization, and encryption
- **Automated Deployment:** Consistent fleet-wide service mesh deployment and standards enforcement at scale with Istio targeted proxy injection to secure, connect and monitor applications
- **Built-in Dashboards:** Visibility into network traffic across clusters and namespaces and the ability to quickly debug applications with real-time visibility and historic replay into traffic flows, latency, and errors

Platform Teams enable Service Mesh Manager for fleet-wide Kubernetes clusters with a simple, centralized enable option via the Rafay Controller shown in Figure 2. Istio is automatically installed and configured on the target clusters, and configuration is applied via policies, rules, and Cluster Blueprints to ensure policy enforcement and service delivery.

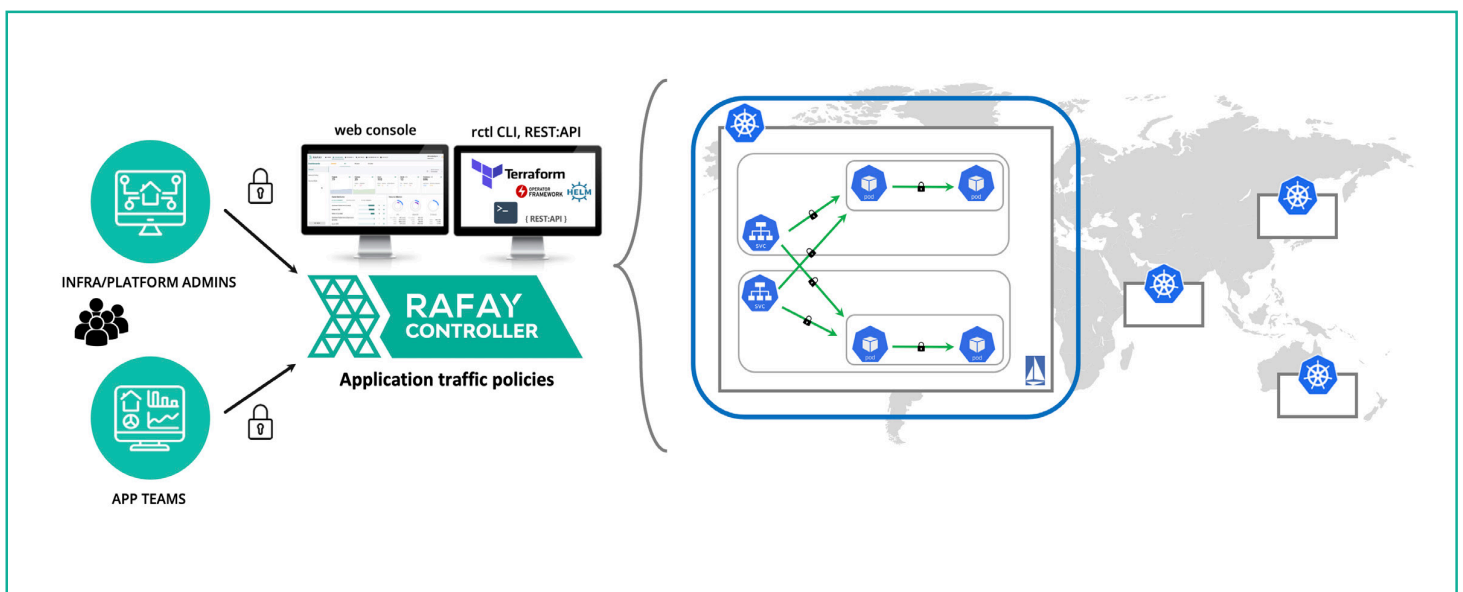




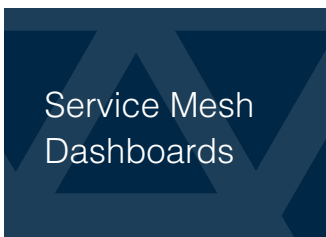
Figure 2 - Rafay Service Mesh Manager

Service Mesh Installation Profile provides a set of parameters, including the Istio Managed Add-On, Certification Type, Sidecar Injection, Enable Ingress, and Resource Quotas. In addition, the installation profile supports two certificate types, “self-signed,” where the Istio control plane is the Certificate Authority (CA), or a more enhanced signing authority using Cert Manager Add-Ons. Service Mesh Rules help define traffic flows and configure security controls cluster-wide or namespace-wide.

Service Mesh Dashboard provides visibility into your applications and traffic flows running in a service mesh on a given cluster. Administrators can check the visualization to see how the traffic flows are initiated and where & when the communication is failing. In addition, you can go back and replay traffic patterns over a period (7 days' worth of historical traffic flows are captured). Finally, you can filter traffic for a certain period of time, for example, the last 1 minute or the last day. This is extremely useful when debugging applications and seeing at what point things started or stopped working from an application point of view and why. More details can be found in [Rafay's online documentation](#).

Summary

Rafay Service Mesh Manager provides strengthened application security, accelerates service delivery, and increases visibility for reducing service outages. Key highlights are:

 Service Mesh Policy	Centralized Networking and Security for secure (mTLS) and control communication between services fleet-wide. These include consistent service-to-service security so developers can simply call microservices without having to program security into each application or manage keys and certificates, to strengthen application security.
 Installation Profile	Provide policy management for standardizing policies and rules for secure connectivity and fleet-wide traffic management. Increase the reliability and reduce the operational cost of service mesh deployments by applying service mesh upgrades without interruptions across pods, proxies, and clusters accelerating application service delivery.
 Service Mesh Dashboards	Provides real-time and historic replay to accelerate troubleshooting, improve visibility, and validate traffic management policies are being applied as envisioned, including mTLS encryption and connectivity policies.

The information contained herein is subject to change without notice. The only warranties for Rafay Systems products and services are outlined in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Rafay Systems shall not be liable for technical or editorial errors or omissions contained herein.