TECHNICAL BRIEF

Using Venafi Firefly to Scale Istio Service Mesh Across Multi-Cluster Environments

Common Security Challenges Impacting Istio

Istio service mesh is an open-source solution facilitating secure, easy-to-manage microservices communications. It provides tools for traffic management, observability, and security, including encryption of service-to-service communication.

A common security challenge in Istio environments is managing machine identities using Istio's default set-up which lacks the capabilities to ensure stringent workload authentication that Infosec teams will insist are critical. In many cases, enterprises have deployed Istio into production using the default: less secure, self-signed certificates. As the mesh environment scales across multiple clusters and clouds, these unmanaged certificates can create security risks tied to inconsistent policy enforcement, untrusted workload authentication and lack of visibility, leading to potential breaches and non-compliance issues.

Challenges of Self-Signed CAs

- Self-signed CAs increase the risk of attackers impersonating legitimate services.
- Using non compliant PKI undermines the trust mechanism for secure service-to-service communication leading to rogue CAs.
- Self-signed certificates do not undergo the rigorous lifecycle management found in enterprise-grade solutions like Firefly.

Firefly's Secures Workload Identities Within Istio

As a compliant, enterprise-grade issuer for workload identities, Venafi Firefly is ideal for Istio environments. Firefly overcomes the limitations of self-signed certificates, ensuring all mesh traffic adheres to enterprise security standards. This integration provides crucial policy controls for workloads, allowing Infosec teams to enforce consistent security policies right across the service mesh. It also extends to Virtual Machines (VMs) to secure workloads operating in non-containerized environments.

By ensuring robust policy control and visibility, Firefly enforces trusted communication for all service mesh traffic. Firefly streamlines workload authentication making it easier for organizations to implement scalable and secure mesh environments so all mesh identities are rooted using only enterprise approved PKI.

Firefly builds upon the widely-used SPIFFE workload identity framework by issuing unique SPIFFE IDs (SVIDs) to all workloads within the Istio service mesh. Istio's inherent use of SVIDs enables mutual TLS authentication and support precise access control policies between services. Firefly therefore ensures all SVIDs within the mesh can be verified using compliant PKI.

Firefly is the natural solution for compliant PKI and secure workload authentication in Istio, ensuring consistency and governance for mesh workloads operating across multiple Kubernetes clusters and clouds.

Security Benefits

Multi-cloud Istio trust domains. Firefly seamlessly authenticates multi-cloud mesh traffic so Infosec teams can establish Istio trust domains without relying on individual cloud provider CA solutions which can be highly complex and costly.

Compliant workload authentication. Firefly ensures that service-to-service communications within the Istio service mesh are secured using a trust root system for all workloads, including VMs, using a compliant CA solution for mutual TLS communication.

Leveraging SPIFFE workload identities. Firefly ensures SPIFFE workload identities (SVIDs) in Istio use approved PKI. This standardizes and strengthens the way services authenticate and communicate securely using SPIFFE.

Operational Benefits

Resilience to attacks and outages. Replaces untrusted self-signed certificates with policy-compliant certificates using a trusted identity issuer. This ensures secure, scalable operations for the mesh environments.

Kubernetes zero trust environments. As a workload identity issuer, Firefly ensures that service mesh traffic remains compliant with the enterprise's security policies. This directly aligns with Kubernetes zero trust security models that use workload identity to implement strict access and verification controls for workloads.

Simplified secrets management. Firefly bootstraps ephemeral trust anchors for issuing short-lived identities for mesh workloads. This reduces complexity with secrets management and improves threat prevention in high-scale Istio mesh environments.

Post-quantum readiness. Implements a trust system for workload authentication with operational readiness to dynamically support post-quantum (PQC) encryption standards.

Real World Attack Vector Targeting Self-Signed CAs in a Default Istio Set-Up

This attack vector scenario outlines the steps that would allow a state actor to exploit a company's software supply chain, specifically targeting self-signed CAs in Istio.

→ **Initial Compromise**: The attacker inserts malicious code into a widely used open-source supply chain tool which includes "phone-home" functionality to extract Kubernetes secrets.

→ **Malicious Tool Deployment and Access:** Supply chain automation deploys the compromised tool into its own namespace within the Kubernetes cluster but with access to all Kubernetes secrets.

→ **Secrets Extraction:** The tool exploits its access to scan and send the Istio self-signed CAs to an external attacker-controlled server. This action is facilitated through the phone-home functionality baked into the tool.

→ **Creating Impersonated Certificates:** The Istio CA is now compromised and the attacker can now generate fake SPIFFE workload identities (SVIDs) which impersonate legitimate Kubernetes workloads.

→ **Overcoming Networking Policies:** The attacker mimics legitimate workloads and bypasses the networking policies to communicate undetected within the trust framework of the cluster.

→ **Query and Data Access:** The attacker queries other services within the Kubernetes cluster, such as accessing sensitive data and is able to perform unauthorized actions.

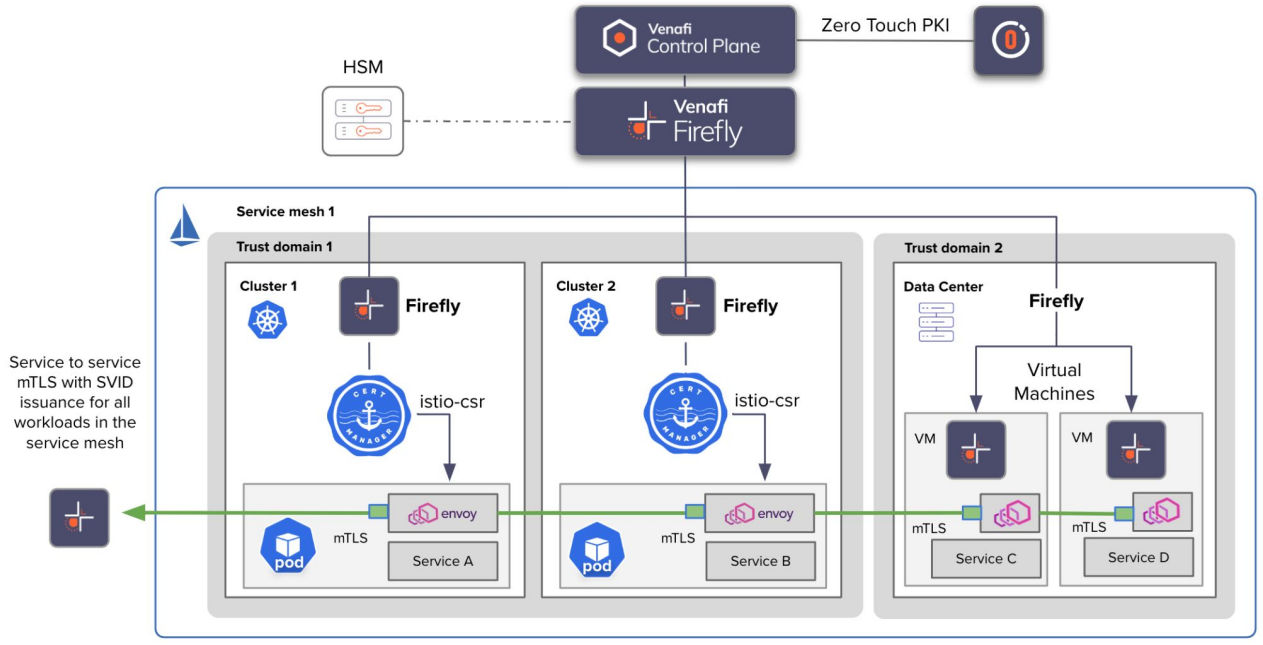
How to Prevent This Type of Attack
Replacing Istio's default CAs using Firefly mitigates this threat by ensuring strict certificate security controls that validate and monitor the authenticity of certificates and workload identities.

Securing Istio Trust Domains Using Service to Service Mutual TLS with cert-manager and Firefly

In the diagram there are multiple clusters in the mesh where services in pods and Virtual Machines (VMs) in data centers must communicate directly with each other using mutual TLS. Default Istio CAs using self-signed certificates have been replaced using Firefly as a lightweight private CA solution to provide consistent authentication and ensure all workload activity is compliant and trusted using approved PKI via the Venafi Control Plane. Instances of Firefly can be easily deployed by platform teams to integrate with cert-manager and provides a developer-friendly trust root system with governance to ensure that all workload authentication is consistent and compliant.

Firefly integrates directly with cert-manager, the highly popular open source that automates certificate management in Kubernetes clusters. Firefly leverages cert-manager's Istio components to mint SPIFFE IDs (SVIDs) ensuring that all mesh traffic adheres to Infosec policy for compliant PKI. This improves security and operational reliability, reduces complexity and improves threat management for Istio mesh environments that are scaling.

Furthermore Infosec teams can significantly reduce complexity and cost by using Firefly to consolidate all mesh authentication and identity issuance onto a single Venafi solution. This includes reduced complexity for secrets management. Firefly's lightweight design is effective for using ephemeral identities to replace storing secrets inside clusters and also supports hardened storage environments using Hardware Security Modules (HSMs) if required.



To improve threat prevention, remove complexity and reduce cost with operating Istio across multiple clusters and clouds, you can get started with Firefly by reaching out to Venafi here.