AVX ONE | CLM for Kubernetes

AppViewX AVX ONE CLM for Kubernetes Datasheet

Simplify Kubernetes Certificate Lifecycle Management with AVX ONE

Challenge

Containerization and the popular container-orchestration platform, Kubernetes, have become an integral part of modern application development and delivery. While Kubernetes automates the operational tasks of container management, its sprawling infrastructure layers, that range from cloud and clusters to containers and code, must be secured and protected.

Whether standing up a cluster or securing the critical interactions with and within a cluster, PKI and TLS certificates are foundational to Kubernetes security. TLS certificates act as machine identities for Kubernetes components and provide strong authentication, encryption, and data integrity across containerized workloads. Managing these short-lived certificates at scale and speed and across complex cloud-native environments introduces significant challenges.

Challenge

- 100s to 1,000s of Kubernetes clusters (self-managed and cloud provider-managed) require 1,000s of certificates for securing:
  - *Ingress Traffic TLS (North-South)*
  - *Service Mesh, Pod-to-Pod mTLS (East-West)*
  - *K8s Infrastructure mTLS*
- DevOps needs speed, agility, and scalability
- SecOps needs visibility, consistency, and control

Problem

- DevOps workarounds and security blind spots
- Certificate sprawl with untrusted and non-compliant certificates
- Misconfigurations, security risks, and application outages

The AppViewX AVX ONE Solution

Simplify and Modernize Certificate Lifecycle Management in Kubernetes Environments with AVX ONE

AVX ONE CLM for Kubernetes is a comprehensive certificate lifecycle management solution for Kubernetes environments. It provides a central platform to discover, manage, automate, control and govern certificates across containerized workloads and Kubernetes infrastructure. Through holistic visibility, end-to-end automation, and policy control, AVX ONE CLM for Kubernetes secures containerized workloads at scale while keeping speed and agility intact.

AVX ONE CLM for Kubernetes features are purpose-built to address both the operational and security challenges of certificate management in complex Kubernetes environments to effectively mitigate application outages, service disruptions, and security and compliance risks.

Why AVX ONE CLM for Kubernetes

- **Prevent Security Blind Spots**
- **Eliminate Outages**
- **Improve Team Productivity**
- **Ensure Compliance**
- **Achieve Speed, Agility, Resiliency**

AVX ONE CLM for Kubernetes Features

Smart Discovery

- Discovery of all SSL/TLS certificates (self-signed and/or from any CA) across Kubernetes clusters (self-managed and/or cloud provider-managed Kubernetes)
- Granular Kubernetes data detected and documented including the cluster, namespace, secrets, etc.

Certificate Inventory and Insights

- A comprehensive inventory of discovered certificates that are automatically segmented into groups and mapped to enterprise-wide Kubernetes teams
- Intuitive dashboards with at-a-glance visibility into certificate expiration, cluster specific usage, compliance etc.
- Customized alerts and custom-built reports with critical insight into certificate metadata such as namespace and secrets, chain of trust, location, expiration dates, and crypto standards, etc.

End-to-End Certificate Lifecycle Automation

- End-to-end certificate lifecycle automation from enrollment to auto-renewal for TLS/ mTLS certificates across Kubernetes
- Secure and automated certificate provisioning across kubernetes environments, including into ephemeral pod volumes
- Fully customizable automation workflows that can trigger any number of approvals, notifications, and change controls
- REST APIs and Auto-enrollment protocol support for CA-agnostic operations and full crypto-agility with simple CA-switch feature

Extensive Native Integrations

- One centralized platform integrated with public/private CAs, Kubernetes platforms, DevOps tools, ITSM & SIEM
- Support for all major Kubernetes platforms such as hybrid/on-prem (Openshift, Tanzu, Rancher) and cloud provider solutions (EKS, AKS, GKE)
- Seamless integrations with DevOps and CI/CD tools (Ansible, Terraform, Jenkins), secrets managers (HashiCorp Vault) and service mesh (Istio, Linkerd)
- Auto-enrollment protocol support for Kubernetes certificates – EST

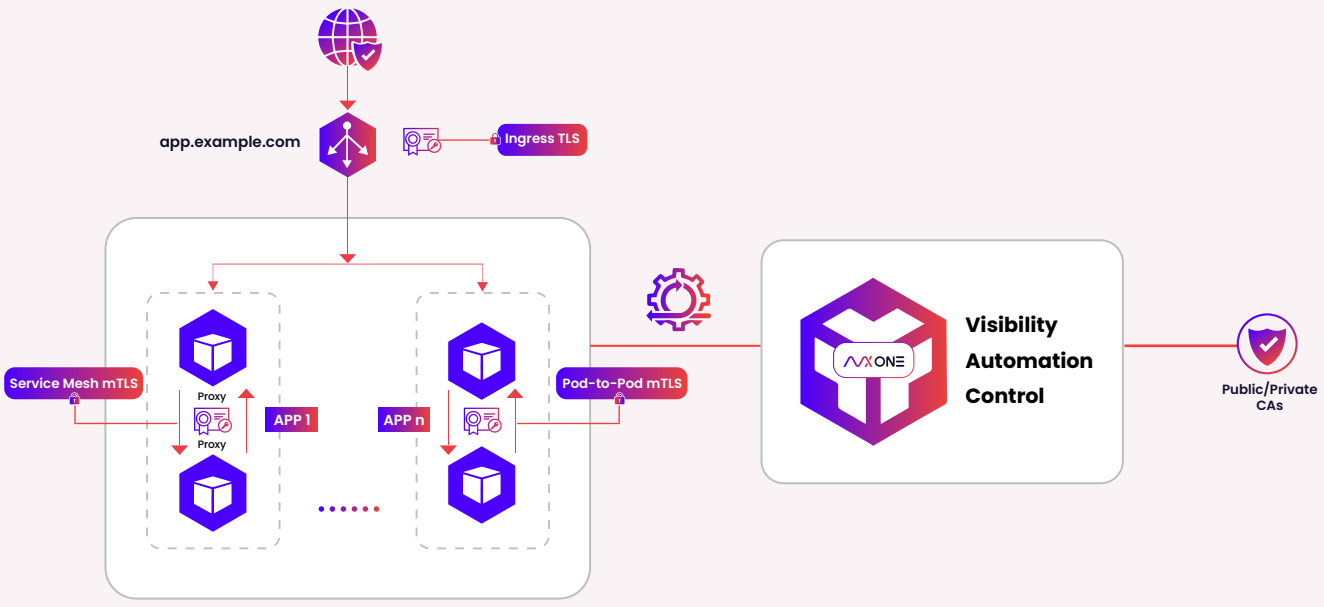
Self-Service

- Cross-functional team alignment between DevOps, CloudOps, application, and platform teams to provision certificates faster and without dependencies
- Streamlined self-service orchestration for requesting and managing certificates that are validated by SecOps policy enforcement

Robust Policy and Compliance Engine

- Consistent enforcement of PKI policies to ensure the use of compliant and approved CAs, crypto-standards, validity periods, and trust levels across all clusters
- Role-based access control for separation of visibility and duties across multiple Kubernetes teams
- Audit logs and reports of certificate usage for easier audits and regulatory compliance

AVX ONE CLM for Kubernetes Solution



AppViewX Inc.,

City Hall, 222 Broadway
New York, NY 10038

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+44 (0) 203-514-2226