appviewx

APPVIEWX.COM

AppViewX Certificate Lifecycle Management (CLM) as a Service

Manage machine identities and mitigate risks with certificate lifecycle automation

Overview

The number of machines in the world is increasing and outnumbering the number of people who use them. The sheer number of machine identities that must be secured, including mobile, cloud, and IoT devices, makes keeping machine identities secure significantly a humongous effort.

The rapid evolution of cloud services comes with its set of challenges. This needs constant effectiveness check for machine trustworthiness, including cloud workloads, virtual machines, containers, and microservices, to ensure that identities are not compromised.

Connected devices use encrypted channels controlled by machine identitiies to transmit and store important data. It is critical to protect the identities of such connected devices as well.

Digital certificates help identify and control who can access and operate on company networks. With the increase in number of identities in a company, it becomes extremely challenging to manage and protect certificates at scale.

- **Challenge**
  Installation of a CLM software in enterprise environment requires provisioning or resources and coordination between various teams managing the software and the resources. This comes costly not just in terms of money but also in terms of time.

- **Solution**
  AppViewX makes its CERT+ available as service. It is a turnkey PKI solution that includes full featured CLM as well as workflow automation.

- **Benefits**
  AppViewX CERT+ SaaS solution allows enterprises to get benefits of all the certificate lifecycle functions and automation without having to wait for resources and time.

CLM Deployment Challenge

Resources and efforts required to install and operate the CLM

While every enterprise requires to manage their digital certificates effectively, installing and operating a certificate lifecycle management (CLM) system may be an overhead on the organization.

First step for having to install a software in the enterprise environment is provisioning of the resources like a virtual machine with adequate compute resources, networking resources operating resources etc.

AppViewX observed that enterprises take from a few weeks to a few months in allocating these resources. The time is taken because the resource planning must be done from long-term perspective because it is not just one-time investment and effort, the installation has to be maintained also for years to come

As different types of resources are involved, various teams and stakeholders are also involved in the single installation. After resource allocation, it requires immense amount of coordination between the teams to make the installation work. It takes approximately weeks of coordination between different teams. In case any team is working on some other higher priority project, installation of CLM gets delayed to months.

AppViewX CLMaaS Solution

Turn-key certificate lifecycle management solution available as a service

Available as a service, the cloud-based CLM (AppViewX CERT+) is fully managed and monitored by AppViewX. Customers can directly get an account on SaaS CERT+ and start using it. This eliminates the need of arranging the resources in enterprise environment.

Features and Benefits

The biggest benefit of using CLMaaS is to save resources, time and effort of installation and maintenance.

Another benefit is to start small and grow the subscription as your business grows. There is no need to invest upfront in large infrastructure. As the organization increase usage of certificates, capacity of CLM services can be increased.

Using CERT+ as a service takes away all the software upgrade and maintenance tasks. Users of SaaS always get the latest and greatest features on priority.

All the functionality of AppViewX CERT+ is available via its SaaS instance:

- Smart discovery of certificates as well as of the associated devices and applications
- Central inventory of all the certificates discovered via various methods
- Analytics of crypto standards used by PKI
- Certificate expiry alerts
- Automated well-in-time certificate renewals using native integration with all major CAs
- Automated provisioning of certificates on target devices and applications using native integrations with all major network devices and applications
- Flexible definition and enforcement of cryptographic policies
- End-to-end automation and enforcement of business policies and procedures
- Granular access control with single sign-on using the corporate user identity system
- Secure key generation and key management

Solution Components & Deployment Architecture

There are two major components of the solution:

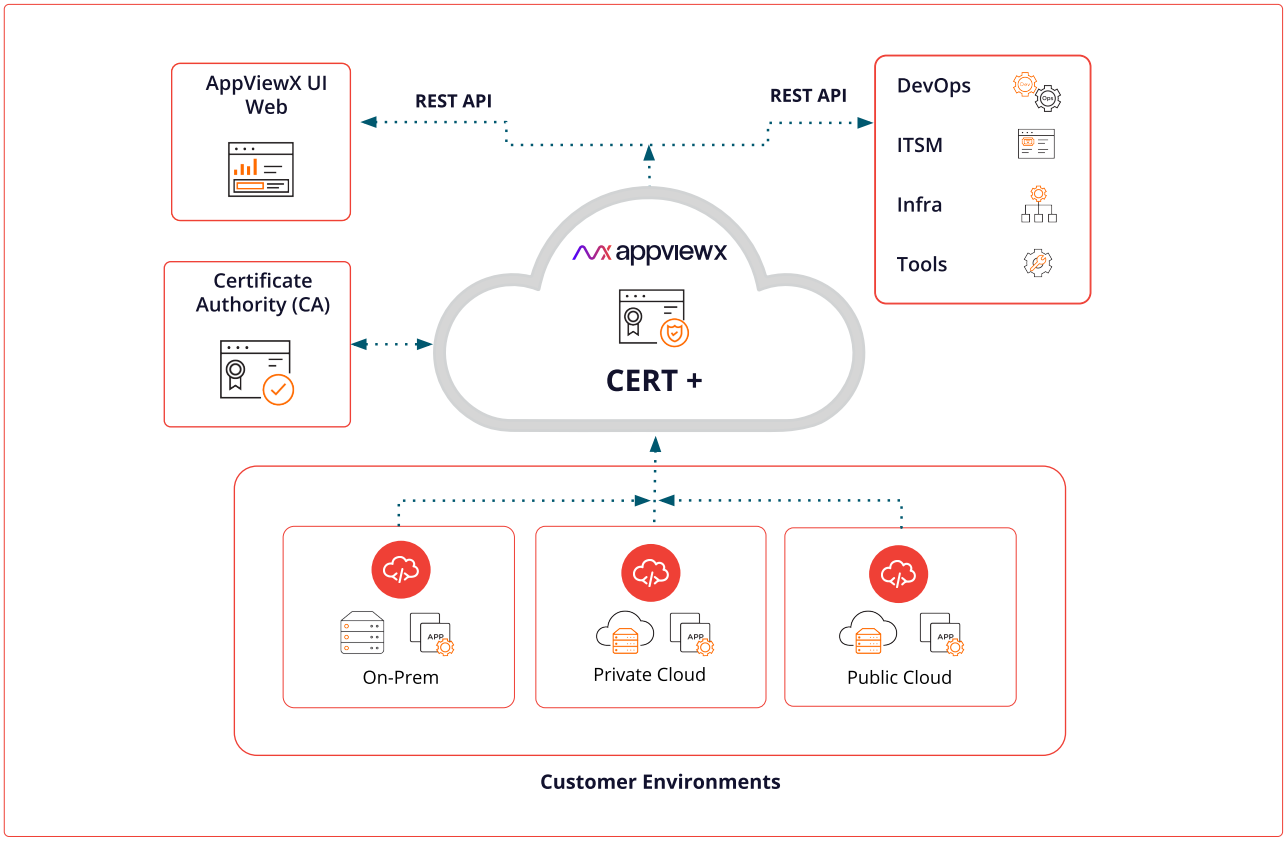
- AppViewX CERT+ Software
- AppViewX Cloud

AppViewX CERT+ Software

The CERT+ software is deployed in AppViewX cloud and is fully managed by AppViewX team. It is installed on top of a hardened operating system in a highly available configuration and hosted at a public cloud provider.

The AppViewX team runs regular security scans and audits for security vulnerabilities. CERT+ offers multiple layers of security that are reviewed to ensure security and compliance.
The SaaS CERT+ instances are hosted in an isolated environment with network layer access control lists (ACL)s and access is granted only to authorized personnel.

Data exchanges within the subsystems is also encrypted using strong ciphers and sensitive data like passwords; SSL private keys are stored in the cloud provider's key management system with strong encryption. External access is always through industry-standard transport layer security (TLS) communication.



AppViewX Cloud Connector

For connecting to the non-public corporate network segments without poking a hole into corporate firewall, AppViewX cloud connector is installed in the private network. Public network segments can directly be connected without the cloud connector.

All messages between CERT+ and the cloud connector flow via a secure, TLS-encrypted channel.
In case multiple private network segments are to be connected to SaaS CERT+, a cloud connector is to be placed in each network segment.

More Information

For more information about AppViewX CERT+, please visit www.appviewx.com

Security simplified with AppViewX

Trusted by one out of every five Fortune 100 companies, AppViewX CERT+ powered by enterprise-grade automation, helps with smart discovery, visibility into security standards and centralized management of certificates and keys across hybrid multi-cloud environments.

Scan QR code to learn more about how AppViewX can be your partner of choice in your cybersecurity journey

https://www.appviewx.com/