appviewX

AppViewX CERT+ Next-Gen Machine Identity Management

Security with simplicity that accelerates your innovation and growth across hybrid-cloud/multi-cloud environment

AppViewX CERT+ is a turnkey solution for all enterprise public key infrastructure (PKI) needs. It not only simplifies setting up and operating a private CA environment with PKI as a Service (PKIaaS), but also provides very rich certificate lifecycle management (CLM) capabilities.

With AppViewX CERT+, enterprises can quickly setup their internal root certifying authority (CA) as well as issuing CAs without having to upfront invest in costly hardware or complicated processes or cumbersome PKI operations. Certificate lifecycle management (CLM) in CERT+ simplifies all certificate operations between CA and the applications where certificates are to be used.

CERT+ simplifies management of certificate and keys across various technologies like SSL/TLS, SSH, IoT, code signing etc. in varied hybrid cloud and multi-cloud deployment environments. CERT+ natively supports long list of devices and applications for certificate provisioning as well as all major public and private CAs for certificate enrollment. Support for protocols like enrollment over secure transport (EST), automatic certificate management environment (ACME) etc. especially comes handy for high speed certificate enrollment for IoT device manufacturing.

Key Benefits

AppViewX CERT+ simplifies PKI and certificate management operations to bring agility in teams so that teams can focus on business innovation and growth. CERT+ becomes the single and centralized console for managing all certificate across the organization. It also becomes the central place for automating all the business processes related to PKI so that manual errors can be avoided.

Cost savings from reduced operational overhead and less infrastructure

PKIaaS of CERT+ allows enterprises to easily setup a robust and secure CA hierarchy as well as other crypto policies without investing into costly PKI hardware or scarce security professionals – enterprises not even need to purchase CA software. AppViewX has ready templates for all configurations, documents and processes. Secure CAs are in cloud and all procedures including key ceremony can be performed virtually yet securely.

Easy audit and compliance

Complete logging of all certificate and configuration change events enables enterprises to go easy for internal as well as external audits for meeting the industry compliance. Periodic reports about cryptographic standards and their seamless enhancement also helps pass the audit with higher grade and allows to keep with up with industry compliance.

Prevention of application outages

CERT+ keeps inventory of all certificates, their expiry dates and the locations where the certificates are being used. It also has automated process for getting the certificate renewed from CA and provisioning it into the application well before expiry. Updating the certificate without human touch avoids delays and errors and eliminates outages.

Team agility and self-service

End-to-end automation of PKI and CLM processes eliminate manual delays and errors, reduce operational burden and makes the entire process agile. With granular access control provided by CERT+, central team can empower application teams for their own certificate operations. Even after enabling self-service for application teams, central team keeps the oversight and control so that everyone adheres to corporate policies.

Key Capabilities

All CERT+ features are targeted for simplifying PKI and CLM operations, reducing effort, avoiding manual errors and enhancing overall security posture of enterprises. CERT+ capabilities range from setting up CAs for issuing certificates to complete lifecycle management of certificate and keys for various applications (web servers, app servers, SSH etc.) in different operating environments (IT, OT & IoT).

Quick CA hierarchy setup

Setup of root CA as well as issuing CAs for different operations is done from the CERT+ user interface (UI) console. Key ceremony for root CA also happens virtually, yet securely. All CA policies as well as certificate policies configuration as related document publishing is also done via CERT+. It also runs the service for certificate revocation check.

Smart discovery

CERT+ discovers certificates from various devices and applications across hybrid-cloud or multi-cloud environment. Unauthenticated network scan as well as authenticated scan of devices, CA accounts and cloud accounts are used to discover as many certificates as possible. Appropriate knobs are available to balance discovery time and pressure on the network.

Central inventory and analytics

All certificates distributed into various devices and applications across hybrid-cloud or multi-cloud environments come under central inventory. This central inventory provides insights into certificate expiry timelines as well as crypto standards (e.g. cipher strength, key size, TLS protocol version etc.) being used for PKI. This insight not just helps avoid application outages by renewing on time, but also helps avoid data breaches by regular enhancement of crypto standards.

Cryptographic and business policies

CERT+ allows administrators to define and enforce various policies for teams to adhere to appropriate cryptographic policies for keys and certificates. These policies help enhance and keep the overall security posture of an organization. Another set of policy (e.g. what type certificate should be issued from which CA) helps teams adhere to the business processes laid out by the organization.

Seamless cryptographic standards enhancement

With CERT+, changing any aspect of crypto standard is very simple and seamless – it is done by creating a policy with higher standards and enforcing the policy for certificates. All of this seamlessly happens from single place i.e. CERT+ UI avoiding time consuming coordination between teams. CERT+ automates end-to-end - generating new certificate signing request (CSR), submitting CSR to CA, getting certificate from CA and provisioning the certificate in the application.

Granular access control

CERT+ employs a granular, multi-layer access control approach where access to each functionality in the certificate lifecycle (discovery, monitoring, renewal, issuance, provisioning) can be configured based on a person's role. Certificates can be tagged with additional metadata and can be grouped according to business need, application or team for easy management of access as well as policies. User management and access control becomes further simple after integrating with corporate user identify and access management system such as Microsoft Active Directory.

Secure key management

CERT+ generates keys either on the target machine or in the hardware security module (HSM). Automated certificate lifecycle processes further eliminate the need of human access to the key - this avoids key roaming and any potential key compromise.

Platform-agnostic installation

AppViewX CERT+ is a Kubernetes based application, hence it can be easily installed on a Linux (any CentOS or RHEL) machine or a managed Kubernetes environment like Rancher, Openshift, EKS, AKS, GKE etc. AppViewX comes prepackaged with all the necessary prerequisites, including Docker, Kubernetes, Secrete Management System, and a database.

Alerting, reporting and logging

CERT+ comes with built-in alerts for various events like upcoming certificate expiry. These alerts can be delivered via emails for manual actions or via simple network management protocol (SNMP) traps for automation. CERT+ also comes with many pre-configured dashboard reports. Custom alerts and reports can be added as per the need of organization. Individual users can also customize their dashboard as per their needs. All important activities related to certificate lifecycle or configuration changes are logged. These logs can be transported into enterprise log storage systems for long-term storage as per enterprise policies.

End-to-end automation

CERT+ automates entire business process right from issuance/renewal of certificates to provisioning/binding of certificates to the application that is using the certificate. This automation not just saves time and effort but also avoids manual errors as well as potential compromises.

Discover and provision certificates and keys for multiple scenarios

CERT+ can be used for various scenarios in different enterprises. Single instance of CERT+ can be used in an enterprise for multiple scenarios as well.

Private CA for internal certificates

In case, certificates are needed in high volumes and only for internal trust domains, CERT+ PKIaaS can be used to setup hierarchy of private CAs and issue internal certificate as needed. The certificates may be issued for SSL/TLS applications, SSH applications, code signing or for IoT devices.

Management of SSL/TLS certificates for IT devices/applications

In this scenario, CERT+ discovers the TLS certificates from various network devices, applications, CAs and cloud accounts. It also takes care of all lifecycle activities in automated fashion. Certificates are provisioned to network devices and applications typically via the native integration with the them. Activities like certificate enrollment can be done either by in integrated third party CA or certificate can be issued by the private CA setup by CERT+.

Central management of SSH keys

In this case, CERT+ is used for generating and managing SSH keys centrally. Periodically or when an user moves out or moves to different authorization group, SSH keys of the machines are generated again and distributed to all machines as well as users of those machines.

Why AppviewX?

- **Expertise**
  Product built by security professionals. Best practices derived from diverse set of customers across industries and an unmatched support team.
- **Pay-as-you-go**
  No upfront investment for hardware or software. Tiered subscription pricing to start small and expand as usage increases.
- **Vast Integrations**
  Native integration with verity of network devices, applications, CAs and HSMs.
- **End-to-end Automation**
  Automation for the entire lifecycle, from certificate issuance to provisioning.
- **Discovery, Visibility and Response**
  Shift to proactive mode by speeding up discovery with holistic visibility, threat hunting and response to eliminate outages.
- **Easy APIs**
  Developer-friendly APIs making it easy to integrate with your DevOps toolchain and IT service management (ITSM).
- **Security with Simplicity**
  Security solution that is automated, compliant, easy to deploy and manage, and integrates into your existing security strategy. Above all, it simplifies the business operations rather than making them complicated.

High speed certificate enrollment for IoT devices

In case of short lived IoT device manufacturing, high volume of certificates is needed at very high rate. Device manufacture request these certificates from CERT+ using auto enrollment protocols like ACME, EST, simple certificate enrollment protocol (SCEP) etc. CERT+ fulfils the requirement based on pre-set policy either enrolling the certificates from an integrated third party CA or issuing certificates from a private CA setup via CERT+ itself.

Certificate management for operational technology (OT) devices

Management stations of OT devices connect to CERT+ for obtaining certificates for the devices. Other lifecycle actions like renewal and provisioning of certificate on devices also happen via the management station.

Consumption Models

CERT+ can either be consumed as a service or deployed in the enterprise network. Features, capabilities and benefits of CERT+ remain the same irrespective of how it is being consumed.

SaaS – operated by AppViewX

Available as a service, the cloud-based CERT+ is fully managed and monitored by AppViewX. Customers can directly get an account on SaaS CERT+ and start using it. 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. All messages between CERT+ and the cloud connector flow via a secure, TLS-encrypted channel. CERT+ is installed on top of a hardened operating system, installed 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.

On-Prem – operated by customer

CERT+ software may also be deployed within a customer's environment in hypervisor based virtual machines (VM)s or private clouds at data centers or public clouds like AWS, GCP and Microsoft Azure etc. CERT+ can be installed on any virtual machine instance running CentOS or Red Hat Enterprise Linux (RHEL) operating system. As CERT+ is a Kubernetes based application, it can also be installed in a managed Kubernetes environment like EKS, AKS, GKE, RedHat Openshift, Rancher etc.

Platforms

aws

Microsoft Azure

Google Cloud

Extensible open-source

Red Hat Enterprise Linux

Licensing

CERT+ subscription is based on the number of licenses being managed or being issued. The subscription period is annual. Choices for various packages (based on types of certificates) and tiers (based on number of certificates) are available and customers need to subscribe only for the package and tier that suit their needs. In case of expansion, customers can seamlessly move to higher tier at any given point in the middle of the term.

Security simplified with AppViewX

Trusted by one out of every five Fortune 100 companies, AppViewX CLMaaS and PKIaaS help with smart discovery, visibility into security standards and centralized management of certificates and keys powered by enterprise grade automation.

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

https://www.appviewx.com/