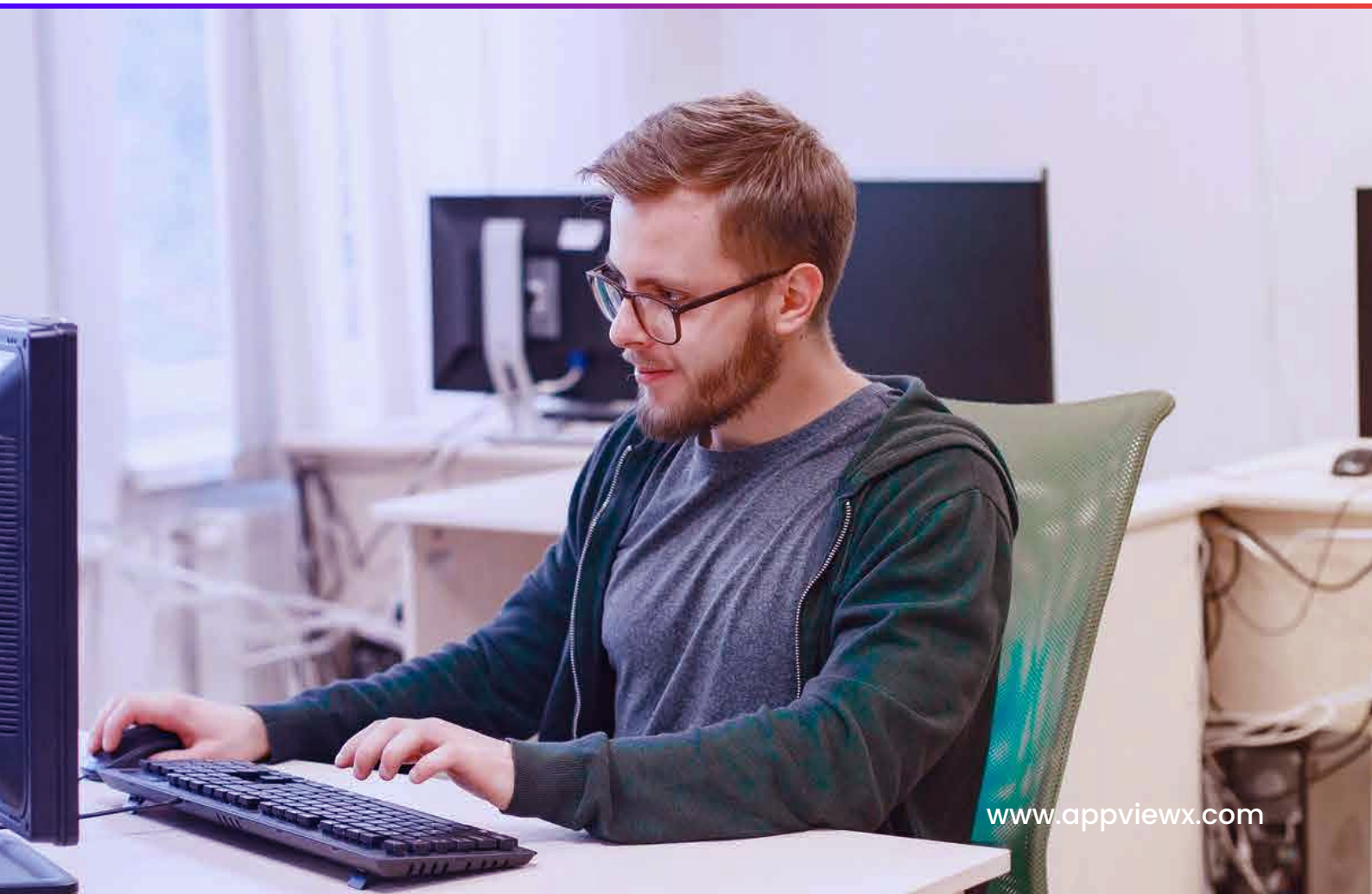
appviewx

Solution Brief

AppViewX CERT+

Comprehensive, Automated Certificate Lifecycle Management for the Modern Enterprise



www.appviewx.com

Overview

Initiatives like digital transformation, cloud adoption, DevOps, IoT, and remote work have driven a massive expansion of the enterprise IT ecosystem with more machines, devices, and applications than ever before. Protecting this growing, distributed IT ecosystem is a significant challenge, as traditional perimeter-based security controls are no longer effective.

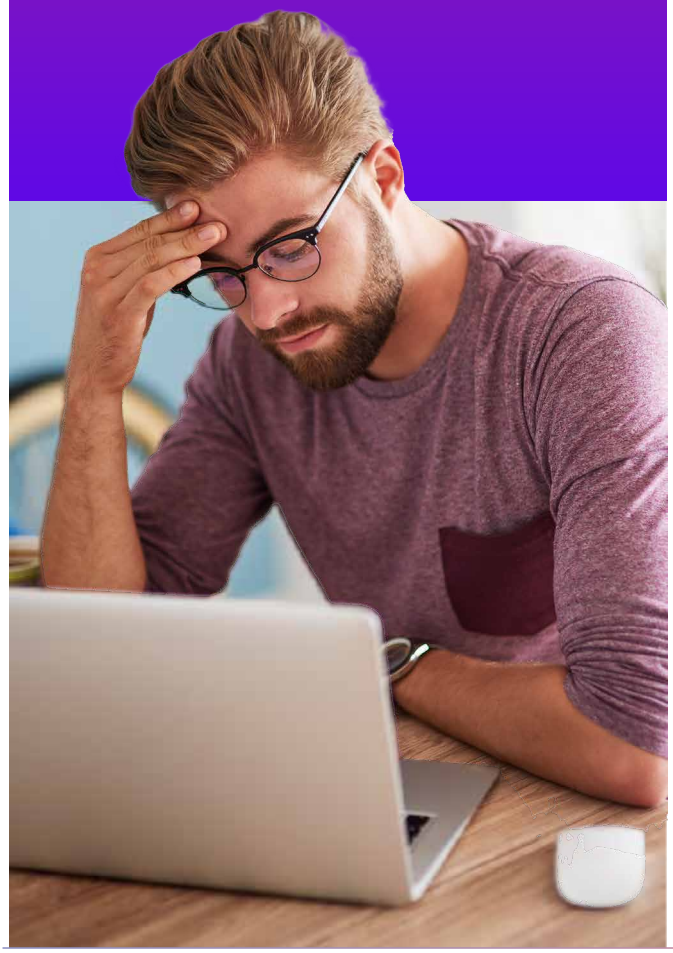
To keep pace with the evolving security requirements, more organizations are now turning to identity-first security. Public key infrastructure (PKI) and digital certificates are the foundation of identity-based security, providing strong authentication and encryption and enabling secure internet communications.

With the number of distributed machines, devices, and applications growing at a massive scale and the frequency of internet communication at an all-time high, PKI-based digital certificates and keys have become central to enterprise IT security today.

Given the critical role they play in cybersecurity, it is essential that organizations manage digital certificates efficiently and securely. However, most organizations continue to manage digital certificates using traditional and outdated manual processes, such as spreadsheets, homegrown tools, and Certificate Authority (CA)-provided point solutions. These manual processes are tedious, time-consuming, and highly error-prone. As a result, they give rise to serious operational and security concerns, causing outages, vulnerabilities, and non-compliance issues.

The problem is further compounded by the exponential increase in the number of digital certificates. As organizations today, on average, use thousands of certificates, the lack of a reliable system to manage certificates at scale has become a significant threat to enterprise cybersecurity.

Challenges with Manual Certificate Management



Poor visibility causing security blindspots

Visibility is non-negotiable for efficient certificate management in distributed hybrid and multi-cloud environments. Visibility into information such as—where a certificate is located on a network, when it expires, the CA that issued it, and the endpoint(s) it is provisioned to—is essential to proactively monitor certificates for expiry and vulnerabilities. However, when using spreadsheets and legacy monitoring tools, information is often inaccurately documented or there is lack of clear ownership, resulting in unmanaged certificates turning rogue and causing application outages and security breaches.

Manual processes causing loss of productivity

Manually managing certificate lifecycles is slow, error-prone, and inefficient. Manual certificate enrollment and provisioning stalls applications and devices from going online quickly, while manual renewal, revocation, and auditing can cause downtimes and outages. As networks expand across cloud environments and the volume of digital certificates increases, spreadsheet-based certificate lifecycle tracking systems can stretch over thousands of rows, making the whole effort tedious and resource-intensive. With shorter certificate lifespans, certificate renewals and installations are far more frequent, requiring significant manual effort. As manual effort increases, the possibility of delays, human error, misconfigurations, and vulnerabilities also increases proportionately.

Lack of crypto-agility creating security risks

Encryption standards determine the security of the infrastructure. A certificate using a weak or deprecated algorithm such as SHA-1 is a tempting invitation for hackers. This is why organizations must continuously analyze certificate crypto standards and update outdated algorithms or protocols quickly to avoid security and non-compliance issues. However, in a manual certificate management setup, organizations have little insight into weak certificates and struggle with agility when it comes to reconfiguring cryptographic algorithms. Manually upgrading crypto standards is a complex task especially at scale, involving several months of planning, coordination, and extensive resource effort, leaving certificates open for attacks.

Weak policy enforcement causing security and non-compliance issues

Enforcing uniform policies is key to preventing certificate weaknesses and regulating access and permissions. Lack of well-defined certificate policies and templates often leads to problems, such as significant variations in the crypto standards used in certificates, use of vulnerable self-signed certificates, and procuring certificates from unapproved CAs—all of which create security risks and non-compliance issues. Certificate ownership is another critical aspect that helps enforce accountability for certificate actions and prevent unauthorized access. Lack of clear ownership and approval workflows can lead to undocumented certificates expiring, unauthorized or rogue certificate issuance, and further security risks.

Certificate mismanagement and misconfigurations causing security vulnerabilities

Typically, there are many stakeholders involved in the development, deployment, and management of a single application. Likewise, there are multiple groups handling the certificates used to secure applications. When certificates are requested and provisioned manually, given the amount of people and effort involved, the margin for delays, errors and misconfigurations is significantly higher. Organizations need a method to streamline and automate certificate lifecycle management, especially the complex task of installation to avoid misconfigurations that can lead to outages and security breaches. Also, while it is obvious that private keys are the most valuable element of data encryption, many organizations still struggle with managing and protecting them. Failing to use proper storage like HSMs or mistakenly sharing or losing private keys poses a serious threat to an organization's security posture.

Simplify and Streamline Certificate Management with AppViewX CERT+

Discover, monitor, enroll, renew, revoke, and provision certificates – all from a single, secure cloud-based solution.

AppViewX CERT+ is a comprehensive, automated certificate lifecycle management (CLM) solution that simplifies PKI and certificate management. It combines the best of automation, security, and insights to simplify all certificate operations between public and private Certificate Authorities (CAs) and the applications where certificates are deployed.

CERT+ features are purpose-built to meet the certificate management needs of growing enterprise use cases, such as hybrid/multi-cloud, DevOps, IoT, and SSH. By simplifying PKI and certificate operations end-to-end, CERT+ promotes agility, minimizes security risks, and enables teams to focus on business innovation and growth.

CERT+ Key Features

- Smart Discovery
- Certificate Inventory with Holistic Visibility
- End-To-End Certificate Lifecycle Automation
- Robust Policy and Compliance Engine
- Cryptographic Standards Enhancements
- Secure Key Management
- Alerting, Reporting, and Logging
- Extensive Native Integrations

Features and Benefits of AppViewX CERT+

Smart Discovery

Being aware of the entire certificate inventory is key to preventing security vulnerabilities. CERT+ helps discover all the certificates installed across various devices and applications in your enterprise environment through an automated discovery process. You can run authenticated, or unauthenticated network scans based on your need. CERT+ also allows you to optimize the scanning process to balance discovery time and alleviate pressure on the network. Automated discovery helps eliminate rogue, unknown, and unmanaged certificates that hackers frequently target.

Certificate Inventory with Holistic Visibility

To help organizations gain complete visibility of the certificate ecosystem, CERT+ consolidates all discovered certificates in a central inventory with full details of every certificate discovered— the chain of trust, certificate location, owner, expiry date, associated application, and more. It also allows you to group certificates based on CA or device location to ease the process of renewals and revocations. Having single-pane-of-glass visibility of certificates helps monitor expiry status, get notifications, and renew expiring certificates on time to prevent application outages. It also helps proactively identify and remediate certificate issues to mitigate security risks.

End-To-End Certificate Lifecycle Automation

One of the biggest advantages of CERT+ is the end-to-end automation it provides. With easy-to-use APIs and pre-built integrations, including Active Directory auto-enrollment, CERT+ automates the entire certificate lifecycle, from certificate issuance to provisioning. Automated workflows reduce administrative burden, eliminate manual errors, and allow teams to do more in less time, increasing team productivity. CERT+ provides teams with the ability to generate, request, and issue certificates from any Certificate Authority via self-service UI or API. Automated workflows, including approval workflows or auto-renewal can also be configured, allowing certificates to be automatically provisioned and installed on endpoints. Certificate self-service and automated workflows significantly simplify certificate operations for large volumes of certificates, saving both time and money.

Robust Policy Enforcement and Compliance Engine

Standardizing certificate processes is key to regulating access to certificates and keys and eliminating security and compliance issues. CERT+ allows PKI administrators to define and enforce various business-specific policies across the enterprise to control certificate issuance, crypto-standards, validity, trust levels, and access privileges, eliminating the existence of rogue, unknown, and non-compliant certificates. Clear policies help teams adhere to recommended certificate management practices, which, in turn, ensures compliance.

Along with policies, CERT+ also allows implementing role-based access control for certificate actions to provide conditional access and enable secure certificate provisioning. Certificates can be tagged with additional metadata and grouped based on business needs, applications, or teams for easy access and policy management.

Cryptographic Standards Enhancements

To help organizations stay ahead of crypto-related security risks, CERT+ provides insight into crypto standards used in certificates (cipher strength, key size, TLS protocol version, etc.). This helps detect certificates that use weak or outdated crypto standards and update them to avoid security compromises. CERT+ also simplifies the process of upgrading weak crypto standards by allowing PKI teams to automatically upgrade crypto standards without any manual intervention. All you have to do is to configure policies with strong crypto standards and renew the certificates using CERT+. The loop gets closed with the automatic push of certificates to the end devices or applications.

Secure Key Management

AppViewX CERT+ enforces secure key management by generating them either on the target machine, key management system (KMS), or in the hardware security module (HSM). Automated workflows pushing certificates and keys to associated devices further minimize human access to keys, preventing unauthorized key roaming and any potential key compromise.

Alerting, Reporting, and Logging

CERT+ comes with built-in alerts for various events like upcoming certificate expiry. These alerts are delivered via emails for manual actions or via simple network management protocol (SNMP) traps for automation and integration with ITSM and SIEM solutions. Custom alerts and reports can be added as per the need of your organization. CERT+ also provides many pre-configured dashboard reports. Individual users can customize their dashboards as per their needs.

All certificate-related activities and configuration changes are logged to make both internal and external audits easier. These logs can be transported into enterprise log storage systems for long-term storage as per enterprise policies. CERT+ also creates audit trails for each user and certificate or key-related activity, and generates periodic reports on the certificate and key compliance to keep up with industry standards.

Extensive Native Integrations

CERT+ provides seamless API-based integration with multiple Certificate Authorities, cloud services, DevOps toolchains, ITSM, SIEM, and MDMs. It also offers auto-enrollment protocol support—EST, SCEP, NDES, CEP/CES, CMP, ACME—to simplify certificate enrollment for DevOps and IoT. Additionally, CERT+ fully integrates with AppViewX PKI+, a turnkey, modern and compliant PKI-as-a-Service for all private trust certificate use cases.

Flexible Consumption Models

AppViewX CERT+ can either be consumed as a service or deployed in the enterprise network. Irrespective of how the solution is consumed, the features and benefits remain the same and are available from one centralized console.

SaaS – Operated by AppViewX

Available as a service, AppViewX CERT+ is fully managed and updated by AppViewX. Customers can directly set up an account and start using it. For connecting to the non-public corporate network segments without poking a hole into the corporate firewall, AppViewX provides a Cloud Connector that needs to be installed in the private network.

On-Prem and Hosted Deployment

The CLM automation capabilities of AppViewX CERT+ can also be deployed within a customer's environment in hypervisor-based VMs, private clouds, or public clouds using AWS, GCP, Microsoft Azure, and others. AppViewX CERT+ can be installed on any virtual machine instance running CentOS or RHEL operating system. As AppViewX CERT+ is a Kubernetes-based application, it can also be installed in a managed Kubernetes environment like EKS, AKS, GKE, RedHat Openshift, Rancher, and others.

Security simplified with AppViewX

AppViewX is trusted by the world's leading global organizations to ensure application availability, security and compliance with centralized visibility and control of public key infrastructure (PKI) and application delivery services across complex hybrid multi-cloud environments. The AppViewX Platform enables self-service automation and orchestration for NetOps, DevOps, SecOps and application teams to quickly and easily translate business requirements into automation workflows that improve agility, harden security, enforce compliance, eliminate errors, and reduce cost.

Make visibility the cornerstone of your protection mechanism.

https://www.appviewx.com/live-demo/

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