appviewx

AppViewX AVX ONE PKIaaS Solution Brief

Modern, Agile, and Secure Private PKI-as-a-Service (PKIaaS)

Current State of On-Premises Private PKI

Private PKI (Public Key Infrastructure) is the foundation for identity, security, and trust among applications, devices, workloads, machines, and services within internal IT environments. Despite its critical role and importance, managing private PKI remains a significant challenge for many organizations.

A majority of organizations manage private PKI on-premises because the perception is that they have greater control, security, and customization. However, with digital ecosystems expanding and new use cases emerging, the limitations of this traditional PKI approach are becoming increasingly apparent.

While deploying on-premises PKI solutions, such as a Microsoft CA (Microsoft Active Directory Certificate Services), was long regarded as the gold standard, organizations are now recognizing the hidden costs, operational complexities, and inherent shortcomings of running an in-house PKI. Security teams are often overwhelmed by the day-to-day demands of managing PKI, diverting focus from innovation and critical strategic initiatives.

As organizations grapple with these challenges, it's clear that the way forward requires rethinking how private PKI is deployed and managed.

Challenges of Managing On-Premises PKI

- **High Operational Costs:** Managing an on-premises private PKI comes with a hefty price tag. From investing in infrastructure to addressing scalability demands, routine maintenance, disaster recovery, and training specialized staff, the expenses add up quickly.

- **Scarcity of PKI Expertise:** PKI deployment and management requires specialized skills, and skilled PKI professionals are increasingly hard to find and retain. Inadequate expertise and employee churn can lead to mismanagement, which in turn, leads to certificate expirations, errors, and security vulnerabilities.

- **Ineffective Certificate Lifecycle Management (CLM) and Integrations:** Legacy PKI implementations often lack robust CLM capabilities. This forces security teams to rely on manual certificate management processes or invest in piecemeal tools—both inefficient and error-prone, especially as demands for scalability grow.

- **Outdated Hardware/Software:** The hardware used for storing private keys requires strict physical security and frequent updates to maintain compliance. Aging hardware and end-of-support software create operational risks and demand costly upgrades, contributing significantly to both capital (CAPEX) and operational (OPEX) expenses.

- **Scalability and Flexibility Issues:** On-premises PKI implementations are difficult to scale and often fail to integrate with modern environments like multi-cloud, DevOps, and IoT. They also fail to adapt to evolving cryptographic advancements like post-quantum cryptography (PQC). This stifles innovation while also creating security bottlenecks.

- **Security and Compliance Risks:** Managing PKI isn't just about scaling to meet growing certificate needs. Security and compliance are critical aspects of PKI management. Outdated PKI systems and procedures and lack of PKI expertise often lead to vulnerabilities, compliance issues, and failed audits.

AppViewX AVX ONE PKI-as-as-Service (PKIaaS)

AppViewX AVX ONE PKIaaS is a modern, agile, and secure Public Key Infrastructure (PKI) solution that seamlessly supports all private trust use cases. Whether ensuring compliance with data protection regulations, building ecosystem trust, or securing assets with strong authentication and encryption, AVX ONE PKIaaS delivers a comprehensive, turnkey PKI solution.

With AVX ONE PKIaaS, you can quickly set up compliant, secure private CA hierarchies tailored to your specific needs and begin issuing certificates in minutes. As a cloud-based service, there's no hardware to purchase or infrastructure to deploy. The management and security of the enterprise PKI is entirely handled by AppViewX.

AVX ONE PKIaaS is part of the AppViewX AVX ONE Platform, which combines modern PKIaaS with end-to-end certificate lifecycle management automation for all private and public certificates from a centralized console.

Features and Benefits

AVX ONE PKIaaS offers a comprehensive suite of powerful features that address the operational, security, and compliance challenges of managing private PKI.

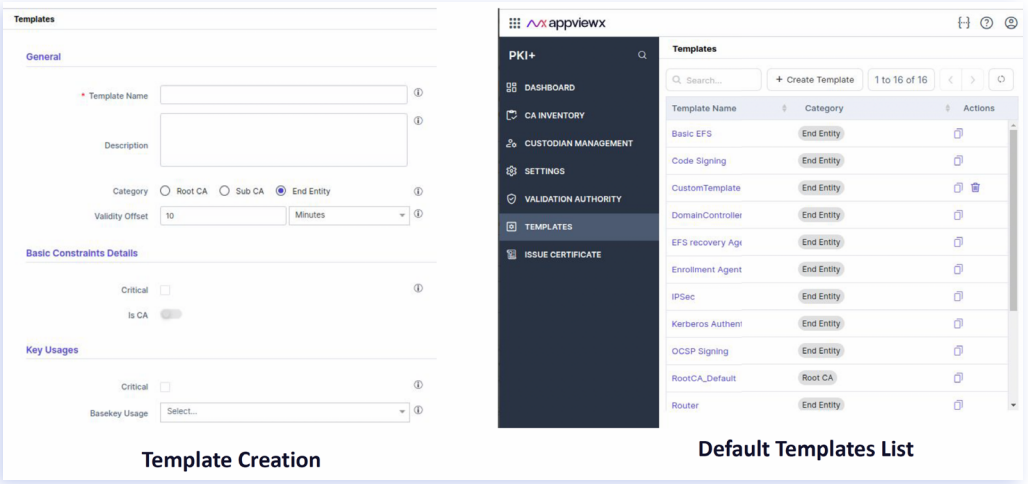
1. Modern and Agile PKI

AVX ONE PKIaaS offers an enterprise-grade private Certificate Authority (CA) that can be provisioned in minutes via a secure virtual key ceremony. CAs can be provisioned in your preferred regions while meeting stringent security and compliance standards. This simplifies and accelerates PKI deployment, enabling you to instantly issue and use private trust certificates.

AVX ONE PKIaaS also provides the flexibility to build a PKI infrastructure that meets the unique needs of your organization. Whether it’s creating tailored custom CAs or defining specific trust levels, our solution puts you in control. It also makes creating any level of CA within the PKI hierarchy easy, enabling you to establish robust multi-tiered trust chains that enhance security and ensure compliance across various domains and applications.

For those struggling with their on-premises PKI deployments, like Microsoft CA, AVX ONE PKIaaS makes migration to the cloud seamless. Leveraging certificate templates, native Windows Auto-enrollment support, group policies, and "lift and shift" capabilities, AVX ONE PKIaaS ensures a smooth transition with minimal disruption to your existing workflows.

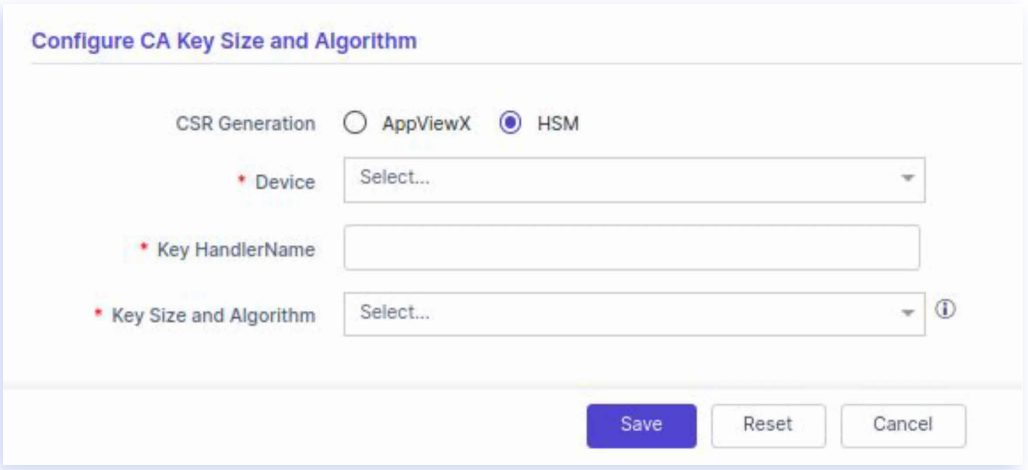
One of the standout features of AVX ONE PKIaaS is the simple template-based deployment for CAs and end-entity certificates. This approach helps standardize PKI processes, promote consistent security practices across the organization, and minimize the risk of misconfigurations. Template-based deployments also reduce the time and effort required to spin up custom private CAs and start issuing certificates, making it easier to scale PKI operations without sacrificing security or performance.



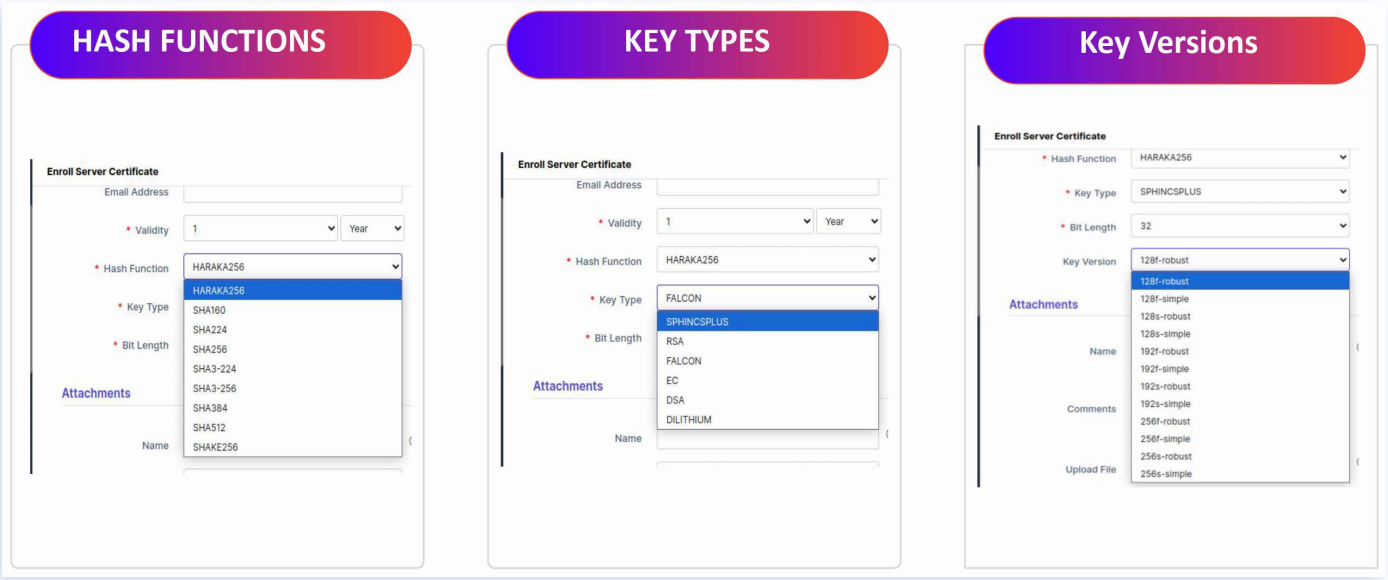
Template Creation

Default Templates List

On the other hand, AVX ONE PKIaaS allows you to design private CAs and certificates tailored to your specific security needs. Certificate policies and fields, such as extensions, keys, key lengths, validity periods, and templates, can be customized to cater to modern certificate use cases (i.e. to include custom IoT certificate attributes and device-based policies).



AVX ONE PKIaaS supports a wide range of cryptographic algorithms and standards, ensuring resilience against both current and emerging security threats. A key advantage is its ability to support the new NIST-standardized PQC encryption algorithms, such as CRYSTALS-Dilithium and SPHINCS+ (including Falcon, which is yet to be announced). You can issue PQC-enabled certificates for internal PKI uses and take a proactive approach to future-proofing cryptographic systems against quantum threats.

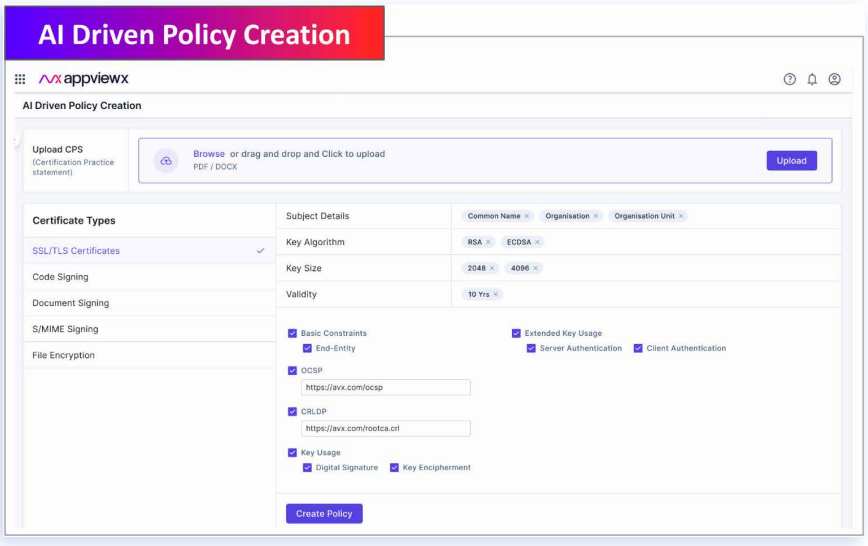


2. Robust and Secure CA Environment

AVX ONE PKIaaS offers a highly secure virtual key ceremony for remote Root CA creation. This process is safeguarded with hosted FIPS 140-2 Level 3 compliant Hardware Security Modules (HSMs), ensuring cryptographic keys are generated, stored, and managed in a tamper-proof environment. This prevents key roaming and any potential key compromises. For organizations that require the highest level of security, AVX ONE PKIaaS supports the implementation of air-gapped or offline root CAs. Isolating root CA from the Internet or network provides additional protection for critical certificates, significantly reducing the risk of compromise.

Revocation services, such as Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP), play a crucial role in certificate lifecycle management, ensuring that compromised or untrustworthy certificates can be promptly invalidated before their expiration. AVX ONE PKIaaS enhances this process with real-time OCSP validation and automated updates to Certificate Revocation Lists (CRLs), ensuring continuous trust and security across your digital ecosystem.

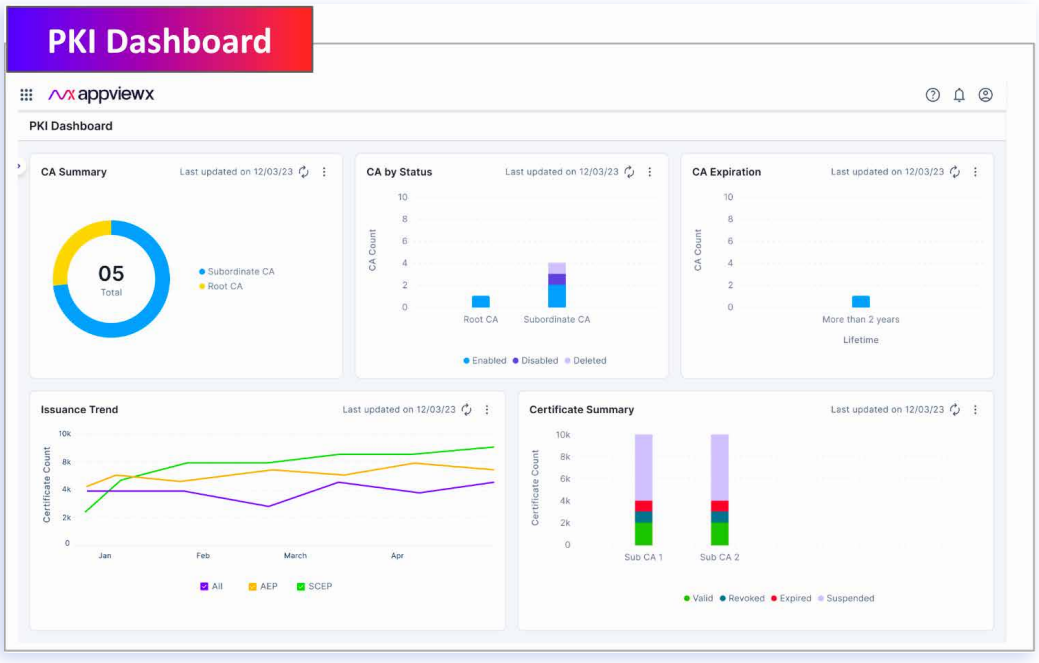
To maintain the highest levels of security and compliance, AVX ONE PKIaaS enforces strict access and security policies, including multi-factor authentication for accessing root CAs and role-based access control (RBAC) for creating and managing CAs. The solution also supports the M of N concept, ensuring that sensitive CA key operations can only be performed with the approval of multiple authorized participants, adding a layer of governance and control.



Certificate Policies (CPs) and Certificate Practice Statements (CPSs) are integral to the security and trustworthiness of PKI. The CP provides the framework for how certificates should be used, while the CPS provides the operational processes for implementing and enforcing those policies. Together, they help ensure that certificates are issued and managed securely, fostering trust for authentication, encryption, and data integrity. AVX ONE PKIaaS simplifies these crucial aspects with template-based Certificate Policies (CP) and Certificate Practice Statements (CPS), ensuring adherence to industry standards and regulatory requirements.

3. Simplified PKI Management - Fully Integrated with AVX ONE CLM

AVX ONE PKIaaS integrates seamlessly with AVX ONE CLM to automate certificate lifecycle management. From issuance and renewal to revocation and provisioning, all certificate processes can be automated end to end, regardless of the issuing public or private CA. Certificates can be automatically requested and provisioned via auto-enrollment protocols, workflows, or AppViewX APIs.



AVX ONE CLM offers a single-pane-of-glass view for complete certificate discovery, lifecycle automation, and policy-driven control. Its CA-agnostic architecture allows you to manage both public and private trust certificates from a central console. Centralized visibility and management help streamline certificate processes across diverse environments, stay on top of certificate expirations and vulnerabilities, prevent outages and security breaches, and ensure continuous compliance.

4. Highly Available and Scalable Infrastructure

Scalability and performance are critical for effective PKI management. With high availability across various geographies with multi-node clusters, AVX ONE PKIaaS allows you to auto-scale your PKI on demand without compromising performance. The architecture is designed to scale horizontally, allowing you to add capacity as needed to efficiently handle large volumes of certificate requests. For IoT ecosystems, AVX ONE PKIaaS can provision certificates at speed and on a massive scale. With built-in load balancing and high availability configurations, AVX ONE PKIaaS ensures reliable PKI operations, even under heavy loads.

5. Extensive Native Integrations

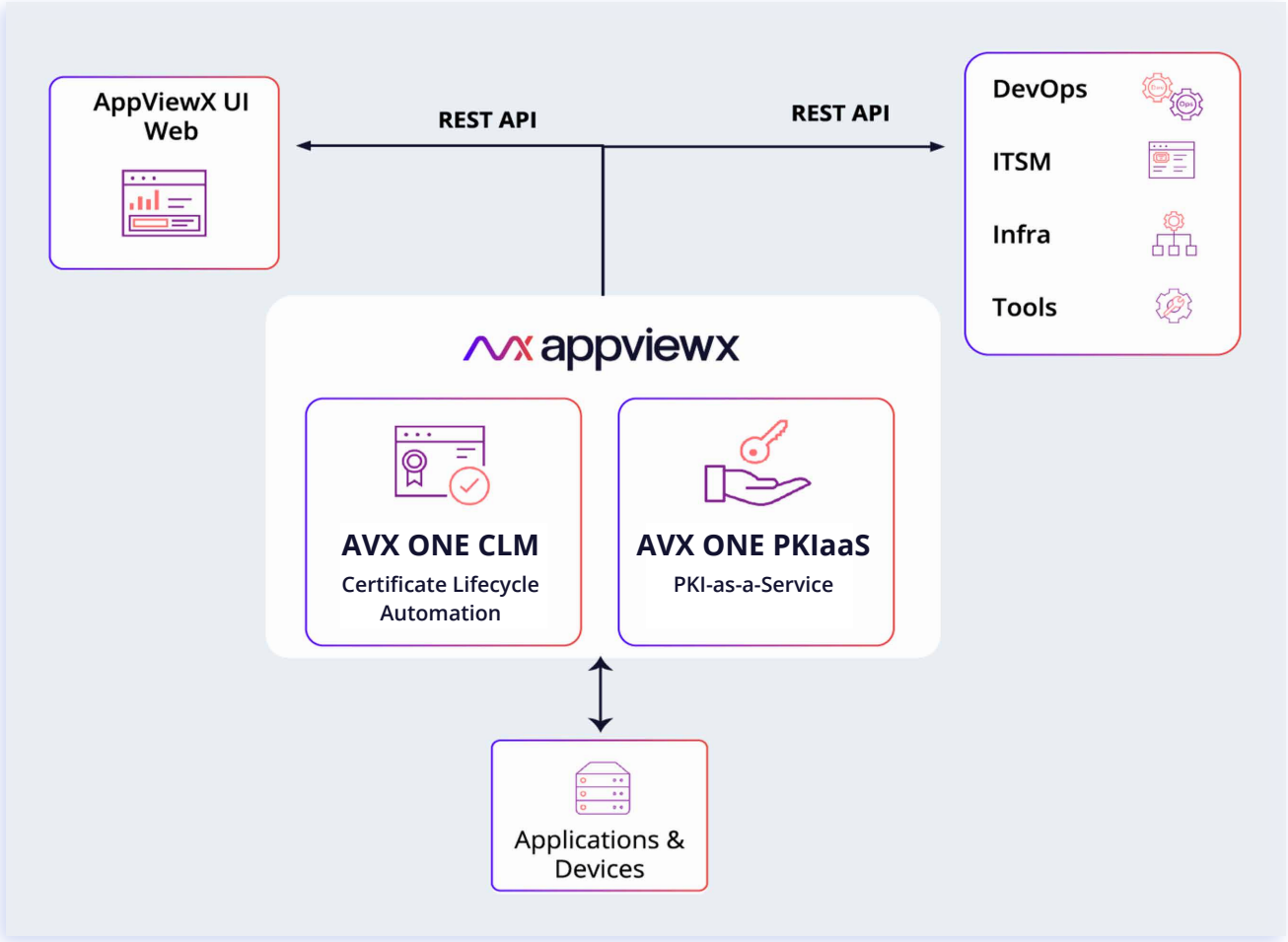
AVX ONE PKIaaS offers a host of flexible integrations to meet diverse infrastructure needs. The solution integrates seamlessly with leading HSMs (Fortanix, Utimaco, Entrust, Thales, and others) and cloud solutions (AWS CloudHSM, Azure Key Vault). It also includes support for bring-your-own-HSM so you can utilize your existing HSM investments as well as bring-your-own-keys (BYOK), allowing you to retain full control over your encryption keys. Through robust API-based integrations, AVX ONE PKIaaS works seamlessly with multiple CAs (public and private), Windows Auto-enrollment, cloud services, DevOps toolchains, ITSM, SIEM, and MDMs for effective certificate lifecycle management across hybrid multi-cloud infrastructure. Additionally, support for all major auto-enrollment protocols, such as EST, SCEP, NDES, CEP/CES, CMP, and ACME, simplifies and automates certificate provisioning and management at scale.

6. Reduced Operating and Overhead Costs

AVX ONE PKIaaS offers an enterprise-grade PKI solution that is ready to use without the need for hefty upfront investments in hardware and software, hiring PKI experts, or ongoing maintenance. Instead, you can opt for a simple, predictable subscription model where AppViewX takes care of all updates, maintenance, security, and scalability, resulting in considerable cost savings.

Flexible Consumption Models

AppViewX AVX ONE PKIaaS is delivered as a cloud-based service, and the powerful certificate lifecycle management (CLM) capabilities of AppViewX AVX ONE CLM can either be consumed as a service or deployed in the enterprise network. Irrespective of how the solutions are consumed, the features and benefits remain the same and are available from one centralized console.



SaaS – Operated by AppViewX

Available as a service, AVX ONE PKIaaS and AVX ONE CLM are fully managed and updated by AppViewX. Customers can directly set up AVX ONE PKIaaS and AVX ONE CLM accounts and start using the products.

Optional AppViewX AVX ONE CLM Deployment Models

To complement AVX ONE PKIaaS, the CLM automation capabilities of AVX ONE CLM may also be deployed within a customer's environment in hypervisor-based VMs, private clouds, or public clouds using AWS, GCP, Microsoft Azure, 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
+1 (212) 951 1146