appviewx

>> Case study

Federal agency reduces average time for certificate creation and renewals from four hours to <15 minutes with AppViewX

www.appviewx.com

An independent governmental agency assisting federal decision makers by providing statistical research on key geopolitical and socio-economic issues was facing system outages due to lack of public key infrastructure (PKI) visibility. Apart from this, manual certificate creation and requisition led to certificate duplication while consuming a lot of time.

IT Background

The customer made use of Linux and Windows virtual servers within their environments, and certificates were required for each server that was commissioned. The creation, deployment, and management of certificates was manually handled by the infrastructure team. Certificates had to be revoked or uninstalled when a server was decommissioned. Apart from the internal certificates required for the virtual servers, the customer also made use of TLS certificates for their external-facing web assets.

Problem Faced

- Lack of visibility into certificate infrastructure
- Unprecedented certificate expirations impacting business continuity
- Sluggish, undefined process for certificate creation on virtual machines
- Slow PKI lifecycle with high reliance on IT
- Lack of audit process and policy

Primary Business Challenges

Lack of PKI Visibility:

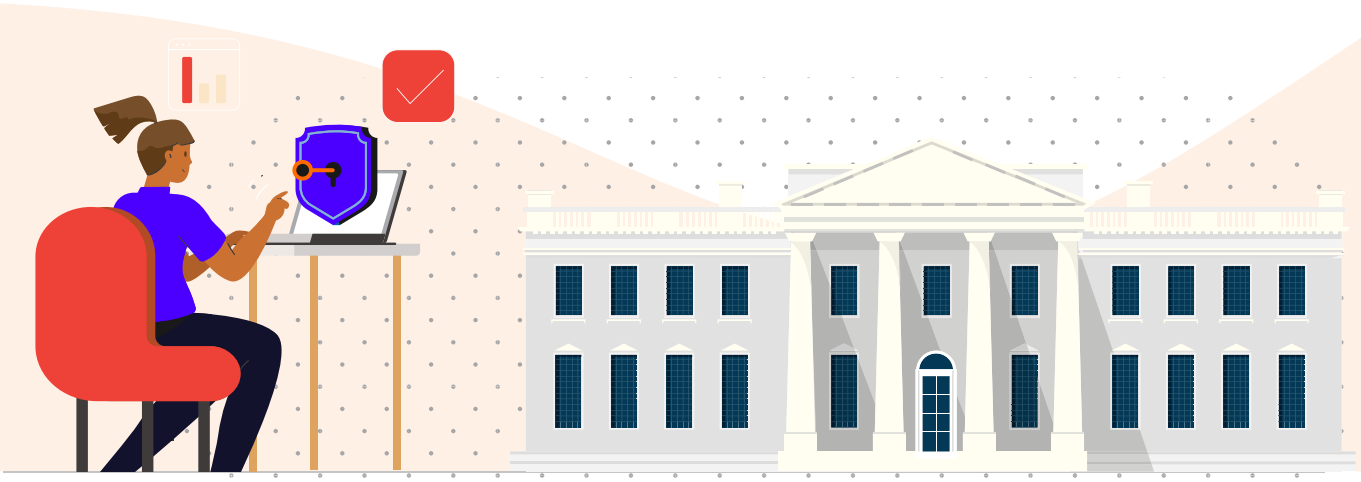
Certificates in the environment could not be effectively tracked due to a lack of visibility into PKI. The client made use of several endpoints and devices, and also virtual servers. Since there was inadequate information regarding validities and certificate locations, unprecedented certificate expirations would often occur, causing system downtime.

Disjointed Certificate Deployment Cycle:

Several Linux/Windows virtual servers were in operation. However, there was no coordination between the virtual servers and PKI, leading to certificates having to be manually created, requisitioned, and installed on the servers being commissioned using VMWare vRA/vRO – a process that consumed significant time to execute. This also led to certificate duplication on the servers.

Lack of Audit Control and Policy Enforcement:

Due to a lack of dedicated access control and audit processes, anyone could create and use a certificate, regardless of its adherence to organizational SSL policies.



Results Achieved

The AppViewX team worked with the customer to create a solution that both streamlined their certificate lifecycle, and integrated with VMWare to accelerate the certificate deployment process.

Certificate Discovery and Monitoring:

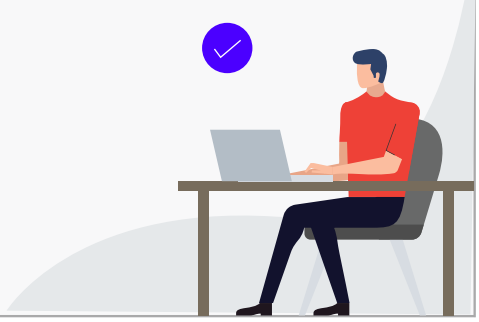
AppViewX's discovery engine was used to scan the client's environment to detect certificates on F5 devices, IIS servers, and Linux Servers. IP/Subnet scans were conducted across the production network to locate certificates and inventory them in AppViewX.

Expiry Reporting and Renewal:

AppViewX was used to set up and schedule periodic expiry reports to be sent to the teams/individuals owning certificate groups. The reports could be configured to be sent at set intervals, helping staff renew certificates well before their expiration dates – this resulted in a decrease of unexpected outages. Renewals were also expedited, making it possible to renew certificates across multiple CAs within the AppViewX platform. Thus, the average time for certificate creation and renewals was reduced from four hours to <15 minutes.

Key Benefits

- Discovery, monitoring, and inventory of **100%** of certificates
- Seamless creation and deployment of certificates for Linux server commissioning via integrations with VMWare and Thycotic Secret Server
- Improved SLAs for certificate creation **(4 hours to 15 minutes)** and deployment **(1 week to <24 hours)**



Accelerated Certificate Creation for Virtual Servers:

By integrating with VMWare vRA/vRO and Thycotic Secret Server, AppViewX automated the process of server provisioning and deployment of certificates on those servers. Whenever a new server is commissioned, AppViewX generates and signs a certificate, and automatically deploys it on the server – the server login credentials are securely obtained by means of the integration with Thycotic. This integration reduced the average certificate deployment time from a week to <24 hours.

Policy Enforcement:

AppViewX enabled administrators to define strict SSL policy for each team. As a result, non-compliant certificates would be flagged, and all incoming new certificates would be in compliance with the defined policy.

Self-servicing of PKI:

Self-service forms were made available to all users to remove their reliance on IT to create certificates. Role-based permissions were assigned to individuals for certificate creation and deployment capabilities as well.