appviewx

Fortune 500 Energy firm achieves 100% visibility into public key infrastructure (PKI) with 90% time savings via automated PKI and certificate lifecycle management (CLM)

A leading energy and utilities holding company that acts as an energy supplier in eight states across the USA. It operates multiple coal plants, wind farms, and nuclear power stations.

Background

Lack of defined PKI processes and visibility resulted in outages

Public certificate authority (CA)s were used to provide transport layer security (TLS) certificates for hundreds of external access points. The cyber-security identity and access management (IAM) team was responsible for certificate management, issuance support, and PKI processes. They would assist application support teams by responding to certificate task requests raised via tickets, as necessary. There were thousands of servers and employees that made use of PKI, but there was no well-defined process that dictated how certificates and keys were managed.

Problem Faced

- Manual PKI configuration errors
- Certificate outages caused due to lack of visibility
- Scattered ownership of certificates
- Cumbersome key regeneration/ re-keying
- Lack of defined PKI process
- Lack of PKI self-service resulting in increased reliance on IT

Primary Business Challenges

Lack of PKI Visibility

A lack of clear visibility into where every certificate was located resulted in frequent expiry-related outages, certificate duplication, cumbersome troubleshooting and complicated maintenance. Detecting the presence of all self-signed certificates and certificates with weak keys and deprecated algorithms was quite difficult to achieve manually, exposing the firm to vulnerabilities.

Manual, Decentralized Certificate Operations

Certificate tasks such as expiry monitoring and installations were done manually by the PKI team. There was a need for an automated system to inventory and group certificates, which would serve the purpose of providing visibility post-discovery. Most importantly, the customer desired a centralized system using which all aspects of PKI could be managed in a secure manner.

Insecure Endpoint Deployment

There were several different device types that certificates needed to be deployed to Windows servers, Red Hat servers, F5 LTMs, and so on. Key distribution was done in an un-encrypted fashion, and pushing the certificate to its respective endpoints required significant work due to its decentralized nature. The entire process of certificate deployment needed to be streamlined and made fully secure, as it was a critical component of the certificate lifecycle.

Results Achieved

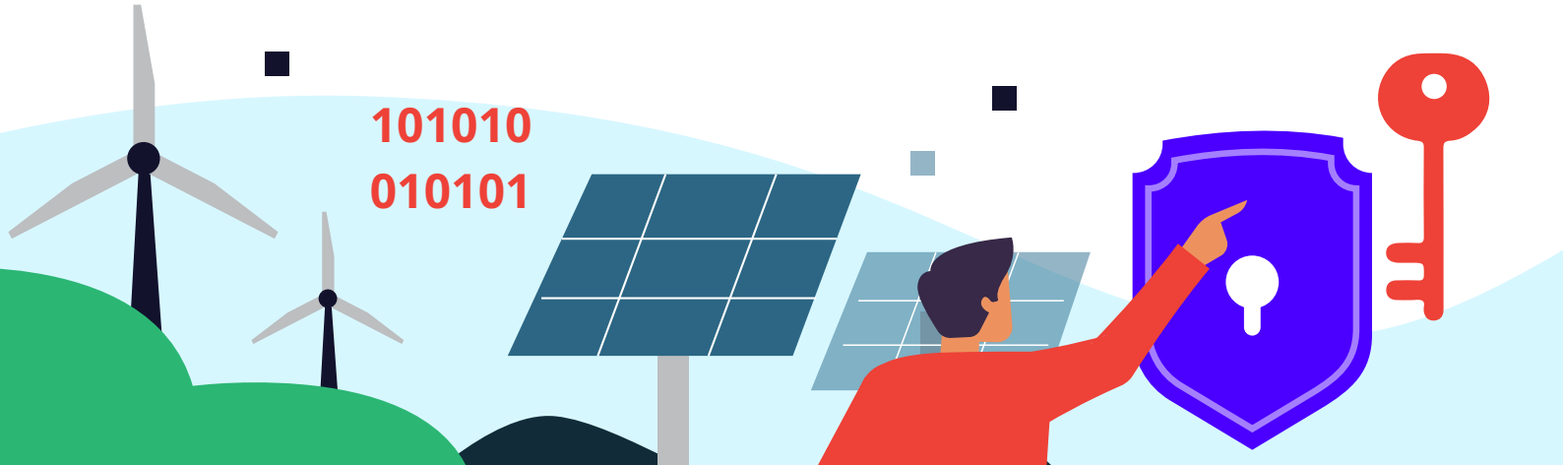
The AppViewX deployment worked seamlessly with our customer's IT infrastructure, and started delivering results right from the start.

Certificate Discovery and Inventory

AppViewX scanned and located certificates on a multitude of devices and servers, and across multiple CAs. The discovered certificates were automatically added to the inventory, and AppViewX allowed for grouping based on certain criteria. The discovery process could be carried out using a range of parameters – including scanning by subnet/IP, or by issuing CA, device, and so on. AppViewX also integrated with Rapid7 in order to query the asset group identified by the customer, in order to discover certificates.

Benefits

- 90% time saved on PKI operations
- 100% visibility into PKI
- Standardization of cryptographic policies
- Compliance reporting
- Significantly reduced risk of outage
- Self-servicing and automation capabilities



Alerts and Monitoring

AppViewX provided constant visibility into certificate health with reports that displayed validity statuses. Periodic alerts for imminent certificate expirations could be configured to be sent via email to the respective certificate/group owner, ensuring that a renewal was never missed. AppViewX also permitted the transfer of certificate ownership to solve the issue of alerts being sent to the wrong people (people who were no longer employed by the firm, for instance).

Self-Service of PKI

AppViewX made a self-service portal accessible to application maintenance teams that could be used to directly requisition certificates as necessary. This minimized their reliance on the PKI security team for trivial certificate tasks, and was a huge time-saver. Role-based control was also applied, ensuring that only authorized personnel would be able to make changes to PKI. Most importantly, AppViewX's low-code page builder was used to design self-service forms in such a way that different teams were exposed to only the information that was relevant to them.

Automation

Tasks such as certificate signing request (CSR) generation, email notifications, certificate signing, and CLM (more on that below) were completely abstracted and automated. AppViewX's automation engine tied together disparate tasks and was able to execute them in an orderly fashion based on activity triggers from users, minimizing significant manual effort.

End-to-end Certificate Lifecycle Management

The AppViewX platform integrates with most endpoints and commercial CAs available on the market. In this case, teams were able to discover, request, renew, revoke, deploy, and create certificates from right within the AppViewX console, without having to switch between various CA and device vendor portals. SSL policy could be defined and enforced across the organization as well.