appviewX

>> Case study

Slovakian Commercial Bank eliminates outages and saves cost on compliance with certificate lifecycle automation.

A Slovakian commercial banking giant that tends to the banking needs of over two 2 million clients faced recurring business outages due to unexpected certificate expirations. This resulted from a lack of expiry notification mechanisms.

IT Background

The customer had an extensive public key infrastructure (PKI) environment, subject to predefined policies and mandated management practices. Some of the certificates in their network were managed manually, while a fraction of the certificates was handled by a proprietary in-house solution.

The manual management method meant that there was no standard and automated way of notification mechanism for expirations and renewals. The complete process required significant human intervention per renewal.

Problem Faced

- Lack of visibility into the certificate infrastructure
- Proprietary certificate tools were operated manually
- Lack of agility
- Additional costs incurred from certificate compliance errors.
- Recurring business outages due to unexpected certificate expirations, and a lack of expiry notification mechanisms.

Primary Business Challenges

The client's IT department clearly identified their pain-points:

Low Certificate Visibility:

Certificates were being cycled through the environment – however, a lack of an inventory visibility meant there was no definite documentation of every certificate that resided on their network. A lack of visibility into certificate location also meant that administrators would have to look for certificates before they could perform operations on them. This presented a two-pronged challenge – it made certificate operations more time consuming, and also magnified the risk factor of possessing rogue, invalid, or expired certificates that were still associated with the network, thus acting as a potential vulnerability.

Lack of grouping and monitoring mechanisms:

With multiple departments leveraging a centralized PKI, end-users felt the need for certificate grouping based on business unit or ActiveDirectory groups in order to streamline operations. The need for a monitoring system that could work in tandem with grouping mechanisms in order to report on certificate statuses would make the work of PKI owners significantly easier.

Outages due to Manual Management:

Certificate lifecycles were managed using manual methods and proprietary systems – both of which often contributed to unexpected expirations and business outages. The lack of an alerting system prior to each expiry limited administrators' capabilities to renew certificates well before they expired.

Policy-related costs:

Without a robust PKI policy framework, policy enforcement mechanisms were not easy to implement, leading to significant error margins and increased costs in the form of outage remediation, business interruption due to downtime, and compliance fines.

Results Achieved

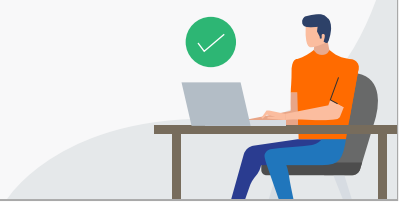
The AppViewX team worked with the client to implement a solution that not only solved issues with the existing setup, but also provided added value that would ease operations in the long-term (role-based access, and management workflows).

Full Visibility into Infrastructure:

AppViewX's discovery system scanned the entire network for the client's certificates and documented them in an inventory, providing teams with full visibility into their certificate infrastructures. This way, the team had knowledge on the exact location of every certificate, so they didn't have to go looking for it prior to an operation on the certificate. They could also keep track of certificates that were cycled out of use, or were vulnerable, in order to remediate them instantly. The monitoring and reporting system came in handy too.

Benefits

- Elimination of outages due to automated renewals and expiry alerting
- 100% certificate compliance achieved
- Cost savings resulting from compliance enforcement for certificate processes
- Automation of certificate processes



Minimized Outages:

AppViewX's inbuilt expiry notification and alerting system notified teams about impending expirations well in advance, thereby preventing the possibility of unexpected expirations catching them off guard. That way, network outages and downtime owing to certificate expirations were eliminated. An integration with JIRA was also built into the AppViewX suite, enabling certificate processes to work in tandem with their existing project management lifecycle. AppViewX's monitoring and reporting features also empowered teams with the visibility and cognizance about the lifecycles of certificates, so they could better plan the management and maintenance of their PKIs.

Compliance and Policy Enforcement:

PKI teams used AppViewX to define and enforce policy that was in line with their organizational compliance rules. These rules, catering to issues such as certificate lifespan ceilings, were adhered to by default, resulting in 100% certificate compliance. This, in turn, delivered consistency in certificate management practices and eliminated the costs associated with non-compliance, resulting in significant savings on operational costs. Administrators from various teams, including F5 admins, Apache/Tomcat admins, and weblogic teams were able to use this feature to their advantages.

Controlled Access to PKI:

To preserve PKI confidentiality and integrity, a role-based access control system was enforced across the network. It restricted access to infrastructure components, and, when necessary, provisioned them on an ad hoc basis. This system worked in tandem with the client's ActiveDirectory, and was immensely useful to the teams mentioned above.

Certificate Lifecycle Management and Automation:

Using AppViewX, the client's PKI teams were able to minimize their dependence on manual scripts for certificate management. They could now renew or provision certificates with a single click, regardless of the CA leveraged or the endpoint in question. AppViewX's lifecycle management workflows enabled automation of processes such as certificate requests and installations, saving the client valuable time and eliminating manual error.