American mortgage lending heavyweight eradicates network downtime caused by expired TLS certificates

Client Information

A veteran in the home loan and consumer refinance product space, this customer has been in the business since 1995. Catering to consumers and institutional partners in the United States, the organization generates an annual revenue of over $800 Million.

Industry

Mortgage Lending, Financial Services

Business challenges and effects

In the process of tightening their network-level security structure, the firm discovered the weak link in their PKI – the manual management of certificates via spreadsheets, which resulted in an onslaught of problems, including but not limited to:

Challenge #1:

The usage of spreadsheets to track TLS certificate expirations and renewals was an inefficient, manual method which led to frequent outages and downtime caused by the aforementioned expirations.

Consequence: Anomalous effects often follow system downtime – apart from internal inconveniences, outages of customer-facing systems are responsible for loss of business, customer trust, and more often than not, legal fines.

Challenge #2:

The establishment of a hybrid, diversified infrastructure with no real visibility into its workings.

Consequence: A lack of system transparency is synonymous with mismanagement – cluttered arrangements are layered upon each other, addling the system with unwanted complexity. For instance, tasks such as renewals of certificate chains become next to impossible, due to an inability to conveniently locate and document the associated keys.

Challenge #3:

The lack of a centralized system to manage certificates across multiple environments and endpoints.

Consequence: Considering the application used by an organization of this scale, it was bound to have thousands of certificates across environments. Manual management resulted in the credentials for each certificate being scattered across the various documentation methods, making certificate-related operations like renewals and revocations time-consuming, and in some cases, impossible, or at least error-prone.

The AppViewX solution

AppViewX CERT+ acted as a single point of control for the entire firm's network-related processes – from certificate lifecycle automation to vendor integrations for network devices. Here are the highlights:

- Our single-window capabilities for detection, renewal, and revocation helped centralize certificate lifecycle management, permitting documentation and grouping of certificates in a single, searchable repository.
- AppViewX's holistic view functionality provided complete visibility into the PKI associated with every environment or endpoint, permitting effortless, error-free management.
- Automated renewals, graphical reporting, and reminders eliminated certificate expirations, which, in turn, resulted in outages and application downtimes being nearly nullified.
- The firm leveraged out-of-the-box vendor integration capabilities to automate network tasks across CAs (Entrust, GoDaddy etc.) and endpoints (Windows Server, F5, Citrix Netscalers, AWS etc.)

Granular role-based access allowed central PKI teams to delegate and self-service tasks such as certificate creation, revocation, and deletion.

About AppViewX

AppViewX is revolutionizing the way DevSecOps and NetOps teams deliver services to enterprise IT. The AppViewX platform is a modular, low-code software application that enables the automation and orchestration of enterprise network infrastructure and certificate management using an intuitive, context-aware visual workflow. It is built to rapidly enable users to implement crypto-agility, enforce compliance, eliminate errors, and reduce cost. AppViewX is headquartered in New York City with additional offices in the US, UK, and India. To know more, visit **www.appviewx.com** or **info@appviewx.com**