Fortune 500 Biotechnology Company Improves Security Posture for Remote Workforce using VPN Certificates and PKIaaS

About Customer

A US-based firm that specializes in providing instrumentation, equipment, software, services, and consumables to the healthcare, pharmaceutical, and biotechnology sector.

IT Background

The customer has multiple internal PKI that is used to issue certificates. External users and consultants could not access the network without a client VPN certificate – they would have to physically visit a company location to enroll and set up those VPN certificates.

There is a need for the device to possess an initial trust in order to enroll it and enable VPN. Furthermore, Network ID certificates are issued to machines, services, and servers and are used for application security purposes. As with all PKI systems, this one required extensive management, particularly, the acquisition, enrollment, and management of certificates.

Primary Business Challenges

The IT team were on the lookout for an abstraction tool which would enable them to achieve the following objectives:

Remote Access of Corporate Systems: The existing PKI was an in-house system, which meant external access of resources secured with this PKI was impossible without a VPN. This presented a chicken-or-egg problem – without a VPN, the network could not be accessed, and without access to the network, VPN certificates could not be securely deployed. The customer required an automated and scalable PKI system which enabled them to solve this problem.

Certificate Auto-Enrolment: The existence of a multitude of endpoints meant there were as many, or even more, certificates to periodically renew, enroll, and install on their respective endpoints.

Industry

Biotechnology & Pharmaceuticals

Challenges

- Use of internal PKI to issue VPN certificates that prevent unauthorized access – this prevented users from using VPN temporarily from a RMA device (mobile or otherwise) unless they could visit an office location to get it configured.
- Lack of a secure initial trust in auto-enrolment and endpoint provisioning options for TLS certificates.
- Lack of visibility into certificate infrastructure.
- Automation of certificate lifecycle, associated SecOps processes, and controlled access.

What's more, new machines were continually on-boarded onto the network – these required certificates to be installed on them as well. Manual handling of these operations meant it was rife with inefficiencies, and presented ample room for error.

Inventory and Reporting: Between frequent acquisitions, multiple CAs and vendors, and ad-hoc deployment, there was no reliable way to obtain a comprehensive overview of certificates and their respective endpoints. The customer's IT team identified the necessity of a centralized inventory for certificates deployed across the network. Further, a thorough reporting system on certificate issues and statuses was required, too.

Delivering a solution with AppViewX

Our customer opted for our PKIaaS (PKI-as-a-service) offering in order to address their pain points. By helping implement a rolling CA migration system, and a full-cycle certificate management suite, AppViewX's PKIaaS solution ticked all the right boxes and delivered rapid results, which are detailed below.

The customer's organization consumed the entire PKI and PKI management system as a service, allowing them to rapidly scale to thousands of certificates and over 100,000 users across the globe with minimum setup and maintenance costs involved – all this during the travel restrictions and remote work setups due to the COVID-19 pandemic.

Seamless CA Migration: The AppViewX platform incorporated a CA-switching system wherein all Microsoft CA-issued certificates were migrated and rapidly configured onto their endpoints with minimal downtime. What's more, the system also implemented a workflow which replaced all expiring server certificates with the auto enrollment process. By consolidating multiple CAs into a single PKI platform, the client achieved improved security and control over their PKI security.

Remote Access via VPN Certificates: The bulk migration of all existing certificates from Microsoft CA to an enterprise CA of the client's choice made it possible for certificate-based authentication in order to obtain gateway access.

Results Achieved

- Automated deployment with inherited trust and enrollment of client certificates at scale
- Enablement of external access to company resources via VPN certificates
- Auto-enrollment using EST for VPN certificates across all device types
- Auto-renewal and full-cycle management of certificates
- Business continuity and minimized risk associated with remote work
- Rapid scaling and minimization of time-to-value with a PKIaaS implementation

EST-based auto-enrollment system: A standards-based EST auto-enrollment option was implemented that enabled AppViewX to act as an EST server, thus automating the enrollment and provisioning process on machines like desktops and laptops. This way, any new certificates that entered the system were automatically configured on the end devices without requiring any human intervention.

Full-cycle visibility, management, and automation: AppViewX's environment scanning and inventory consolidation tool helped IT Ops build comprehensive inventories of certificates on file, complete with endpoint maps, statuses, and cryptographic details. AppViewX's workflow automation capabilities enabled automation of certificate requesting/renewal processes as well, while built-in reporting capabilities provided ample visibility into critical details like validity

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**