Leading life sciences company improves security posture by automating certificate enrollment.

About Customer

A leading U.S.-based life sciences company that specializes in providing instrumentation, equipment, software, services, and consumables to the healthcare, pharmaceutical, and biotechnology sectors.

IT Background

This customer is a firm that has multiple internal public key infrastructures (PKIs) for issuing certificates. The organization also has both on- and off-network client computers that required regular system updates and patches. This is a critical infrastructure security, especially for supporting increased remote work scenarios used during the COVID-19 pandemic.

Microsoft System Center Configuration Manager (SCCM) performs the patch and software deployments. SCCM requires machine certificates to authenticate and establish connectivity with the hosts.

Machine-identity certificates used for application security purposes are issued to client computers, services, and servers. This PKI system required extensive management, particularly the acquisition, enrollment, and management of certificates.

Primary Business Challenges

The IT team sought an abstraction tool that could achieve the following objectives:

Uniform Certificate Auto-Enrollment: While computers connected to Active Directory can leverage the Group Policy-based Windows Auto-Enrollment feature, those without regular connectivity to Active Directory cannot; hence, there was no way to enroll certificates on these devices. SCCM could not function because it requires certificates to authenticate.

Industry

Biotechnology & Pharmaceuticals

Challenges

- Lack of uniform certificate enrollment for computers having varying degrees of connectivity to Active Directory
- Lack of visibility into certificate infrastructure
- Automation of the certificate lifecycle, associated Security Operations processes, and controlled access

Results Achieved

- Deployed an Enrollment over Secure Transport (EST) protocol-based agent to auto-enroll certificates on all computers
- Improved certificate discovery, inventory, and reporting functionality to enhance visibility and control
- Implemented auto-renewal and full lifecycle management of certificates
- Supported business continuity and minimized security risk

Furthermore, certificates had to be renewed, enrolled, and installed on their respective clients periodically, and new computers were continually onboarded onto the network. This necessitated use of a tool that could standardize enrollment and connect to computers primarily running off-network.

Inventory and Reporting: Frequent acquisitions, ad-hoc deployments, and use of multiple certificate authorities and vendors posed a challenge for obtaining a comprehensive overview of certificates and their respective endpoints. This leading life sciences company identified the need for a centralized inventory for certificates deployed across the network. The company also wanted a transparent view of the certificate infrastructure.

Delivering a solution with AppViewX

After careful analysis, the AppViewX team crafted a solution for each of the aformentioned challenges. By helping implement an EST-based enrollment agent and a full-cycle certificate management suite, the solution met all objectives and delivered rapid results, which are detailed below.

Standardized Auto-Enrollment: An agent leveraging the EST protocol for certificate enrollment was deployed. It enabled AppViewX to act as an EST server, thus automating the enrollment and provisioning process. This also established a standard means of enrolling certificates across all machines, where AppViewX acted as a single, uniform interface for auto-enrollment. This enabled smooth patch and software management on SCCM client computers. Furthermore, new certificates were configured automatically on the end devices without human intervention. This particular use case was a distributed, multi-node deployment across multiple Amazon Web Services data centers across the U.S. and Europe.

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. AppViewX's audit trail feature also helped in this regard.

Full-cycle visibility, management, and automation: AppViewX's environment scanning and inventory consolidation tool helped IT Operations build comprehensive inventories of certificates on file, complete with endpoint maps, statuses, and cryptographic details. AppViewX's workflow automation capabilities enabled automation of certificate request/renewal processes while its reporting capabilities provided clear visibility into critical details such as validity. This increased visibility and control help prevent outages and contributed toward upholding organization-wide business continuity.