appviewx

Case Study

Insuring Digital Trust

How PacificSource Transformed Certificate Management with AppViewX

About PacificSource

PacificSource is a not-for-profit health insurance provider dedicated to making healthcare more accessible and affordable. Serving individuals and organizations across the Pacific Northwest of the United States, their offerings include comprehensive medical and dental plans, self-funded benefit programs, and essential administrative services.

Pain Points

- Lack of visibility into the certificate environment
- Frequent outages caused by expired certificates
- No standardized processes for certificate issuance
- Significant time and effort spent on manual certificate management

The AppViewX Solution

- **Automated discovery and centralized inventory**
- **End-to-end certificate lifecycle automation**
- **A single, centralized platform for all certificate lifecycle actions**
- **PKI policy-driven governance for security and compliance**

Results

- **Complete centralized visibility across the certificate landscape**
- **100% reduction in certificate-related outages (from 3–4 per month to zero)**
- **Certificate deployment time cut from a full day to just 15 minutes**
- **97% reduction in time and effort spent on CLM tasks**
- **Full audit readiness and compliance reporting**

Challenges

As a health insurance provider, PacificSource handles large volumes of sensitive personal and financial data. Every digital interaction—from member portals to internal systems—relies on communication channels secured by digital certificates. In such a regulated and risk-sensitive industry, efficient and accurate certificate management isn't just operational hygiene; it's essential for trust, compliance, and business continuity.

But over time, PacificSource's certificate environment had grown sprawling and unmanageable. For years, application administrators were stuck in a fully manual cycle—handling renewals, provisioning, and tracking certificates without proper tools or formal processes. As the environment grew more complex, so did the risk.

Ad-hoc Certificate Management

Certificate issuance was entirely ad-hoc. With no standardized processes or even basic tools, administrators were left to their own devices. When a certificate request came in, administrators issued certificates from either the internal private CA or GoDaddy's public CA, with little documentation or oversight. When staff members transitioned out of the company, they often left behind certificates, lurking in systems, undocumented and forgotten. These orphaned certificates became ticking time bombs—ready to trigger security issues or outages at any moment.

Zero Visibility, Frequent Outages

Lack of visibility was a major issue. Without a centralized inventory, there was no reliable way to track certificates or monitor expiration dates. Administrators often resorted to jotting expiry reminders down in personal calendars, hoping they wouldn't miss a renewal. While GoDaddy-issued certificates came with alerts, those from the internal CA offered little to no warning. Unsurprisingly, certificates frequently expired unnoticed, leading to frustrating (and costly) outages.

Manual Work That Slowed Everything Down

Renewing and provisioning certificates was a major drain on productivity. When a certificate was used across multiple servers, administrators had to deploy it manually, logging into each server, copying and installing the certificate, binding it to every relevant application instance (sometimes up to three per server), and verifying it all worked correctly. This repetitive, time-consuming process pulled valuable time away from more strategic initiatives.

> As Aaron Zollinger, Sr. Network and Security Administrator from PacificSource shares
>
> **They had to go out to the CA server, generate the certificate there, download it, copy it to all. One of them was like 15 servers. So they would have to copy that certificate to all 15 servers and then install it there and then bind it to each instance that was on that server, which sometimes was up to about three different instances.**

The Shift Toward Smart, Centralized Certificate Lifecycle Management (CLM)

It became clear to PacificSource that manual, scattered certificate operations were no longer viable. To move from reactive firefighting to proactive management, they needed visibility, automation, and policy control at the core of their approach.

With that in mind, the team defined key criteria for their CLM solution:

- **Complete discovery and inventory** of all certificates across the environment
- **Expiry notifications** to prevent outages
- **Automation** to streamline renewals and deployments
- **Policy enforcement** to standardize encryption usage and certificate configurations

Choosing AppViewX AVX ONE CLM

After evaluating several certificate lifecycle management (CLM) solutions, PacificSource launched a proof-of-concept with AppViewX and quickly realized it was more than just a fit. The platform stood out for its depth, offering strong automation capabilities and advanced features that addressed both current needs and challenges they hadn't yet considered.

> As Aaron put it
>
> **It had all the features that we needed, plus some; it pretty much was the Ferrari of certificate management compared to the other ones.**

About AppViewX AVX ONE CLM

AppViewX AVX ONE CLM is an automated certificate lifecycle management solution designed to simplify PKI and certificate lifecycle management across complex hybrid multi-cloud environments. It provides centralized visibility, end-to-end automation, and policy-driven control of certificates to eliminate outages, mitigate machine identity risks, and enhance crypto-agility.

The Results

A Complete Turnaround in Certificate Management

Since deploying AVX ONE CLM in 2021, PacificSource has completely transformed its approach to certificate management. Today, over 1,500 public and private trust certificates are seamlessly managed through the platform by the IT team, spanning web administration, network and security, and application support.

What was once a fragmented, manual, and reactive process is now unified, automated, and resilient.

Complete Visibility

With AVX ONE CLM automatically discovering certificates across the infrastructure and consolidating them in a centralized inventory, PacificSource now has full visibility into its certificate environment. No more digging through systems or relying on calendar reminders, the entire certificate landscape is accessible in a single, unified dashboard.

This visibility empowers the IT team to:

Instantly identify expiring, weak, or misconfigured certificates

Monitor vulnerabilities and compliance across the environment

Proactively reduce downtime and mitigate risk

Centralized Management, Zero Downtime

One of the biggest game-changers for PacificSource has been the ability to centrally manage and deploy certificates across multiple servers using AVX ONE CLM. Tasks that once took hours of manual, repetitive effort can now be completed in just a few clicks, saving time, reducing human error, and improving overall efficiency.

Most importantly, this shift has had a direct impact on uptime: certificate-related outages have dropped from three or four per month to zero.

With centralized visibility and deployment, PacificSource no longer worries about certificates slipping through the cracks.

> As Aaron shared **We've been able to update certificates that are not up to our standards quite easily, as a matter of fact, and it has saved us from downtime due to expired certificates. I think our downtimes went down from three or four a month down to zero.**

End-to-End Lifecycle Automation

With AVX ONE CLM, PacificSource has fully automated the certificate lifecycle, from renewal and reissuance to provisioning. Even the final step of binding certificates to the right application instances happens automatically. What once required logging into each server manually now takes just a few clicks.

> **We have several groups that utilize one certificate for multiple servers, and they were in awe when I showed them that you could create a certificate and then push it out to all the devices all at once in one pane.** Aaron added.

This automation has significantly boosted daily efficiency. Beyond easing current workloads, it's also helping PacificSource prepare for what's next.

With the industry shifting to 47-day TLS certificate lifespans, more frequent renewals and tighter timelines are inevitable. PacificSource feels ready. AVX ONE CLM automates renewal and reissuance workflows, making short-lived certificate management effortless at scale. "We'll be able to just change the expiration date and automate the rest internally," said Aaron.

Hours Saved, Teams Empowered

With AVX ONE CLM, PacificSource now manages the entire certificate lifecycle from one centralized platform. The shift from manual, repetitive work to streamlined automation is saving valuable time for the IT team. Tasks that once consumed hours can now be completed in minutes, even at scale.

> Aaron shared a striking example: **Last year, we had a group that needed 35 certificates generated and pushed out to dozens of servers, each with multiple DNS entries. Before AppViewX, it took them an entire day to generate certificates and push them out. And then with AppViewX, the same task for the next set of certificates took them just 15 minutes.**

That's not just time saved, it's hours returned to teams that can now focus on innovation instead of infrastructure.

One feature the IT team values most is the platform's ability to automatically push and bind certificates to the right servers and application instances, without any manual effort.

"Even just creating and pushing a certificate saves our application admins a huge amount of time, an hour or two easily, especially when they're deploying to multiple servers", Aaron added.

Audit Readiness and Compliance, Built In

With AVX ONE CLM, PacificSource has introduced structure and standardization to certificate operations, making compliance easier to achieve and maintain.

Using policy-driven controls, the team has defined clear rules for issuing CAs, organized certificates into groups, and implemented role-based access controls (RBAC) to ensure only authorized users can perform specific certificate operations. This has reduced the risk of human error while making the entire process more secure and predictable.

With the reporting dashboard that AVX ONE CLM offers, PacificSource now has real-time insights into certificate status and compliance across the enterprise. Audit readiness is no longer a scramble; it's a built-in capability.

Where They Are Now: Resilient, Efficient, and Ready for the Future

PacificSource's journey with AppViewX shows what's possible when visibility, automation, and policy-driven governance converge in a single platform.

With zero outages, a radically more efficient CLM framework, and full compliance oversight, the team has shifted from firefighting to future-proofing. They've reclaimed hours, eliminated risk, and now manage more than 1500 certificates with ease and confidence.

By investing in a scalable solution like AVX ONE CLM today, PacificSource has done more than solve immediate challenges; they've set themselves up to continue reaping dividends well into the future. As certificate lifespans shorten, volumes rise, and the threat of quantum computing looms, PacificSource has already made the smart move to ensure that future teams inherit a stronger, more trusted foundation to build on.

In the highly regulated world of healthcare and insurance, where security and business continuity are non-negotiable, PacificSource isn't just managing certificates; it is managing digital trust without compromise.

AppViewX Inc.,

AppViewX provides digital identity protection solutions that simplify PKI and certificate lifecycle management for modern enterprises. The AVX ONE CLM solution is the most advanced SaaS certificate lifecycle management (CLM) platform for enterprise PKI, IAM, security, DevOps, cloud, platform and application teams. With visibility, automation and control of certificates and keys, AVX ONE enables crypto-agility to rapidly respond to cryptographic changes, mitigate threats, prevent outages, achieve Zero Trust, and prepare for Post-Quantum Cryptography.

appviewx

City Hall, 222 Broadway
New York, NY 10038

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+44 (0) 203-514-2226