KEYFACTOR

CASE STUDY

Multinational Oil and Energy Company Adds Cloud PKI to Their Zero Trust Strategy

Moving PKI to the Cloud Allows Company to Drastically Reduce Overall On-Premise Costs and Automate Certificate Lifecycles

Company Overview

This Texas-based oil and energy company refines and markets petroleum products to power various uses, including home-based heat, cooking and electricity, manufacturing processes, and everyday electronics.

Challenges

As a large organization that serves various industries, this oil and energy company takes security very seriously. Most of this responsibility sits with the company's identity and access management team, covering everything from identity management and remote access to encrypted data storage and data management. One of their critical responsibilities is maintaining the company's public key infrastructure (PKI) program.

The company historically ran this program on-premise, which involved managing the root certificate and issuing servers on-premise, and maintaining an internally-hosted website where users could request certificates. This approach worked for many years; however, new company initiatives from the organization's CISO led the team to look for a new PKI solution that would better match the direction in which their organization was moving.

Specifically, their CISO introduced an initiative to start moving operations to the cloud wherever possible. According to the Director of Identity and Access Management, this cloud-first mindset contained three core business objectives:

- adhering to a zero trust principle (and its corollary of least privilege)
- embedding cost containment into all technology decisions
- automating wherever possible

"A lot of the capabilities our team provided in the past were very manual, PKI included. As we looked to move forward, we knew it would be important to find a more automated solution that could also align with our new cloud-first and zero trust objectives."

The Solution

These imperatives for a new PKI program led the company to Keyfactor, which offers Keyfactor Command in a PKI-as-a-Service model that enabled the organization to fully bring its program into the cloud. Importantly, Keyfactor Command also supported a highly automated, zero trust environment in a cost-effective way.

"We found Keyfactor provided an advantage not only from an overall management and cost standpoint but also by aligning with our broader strategy of going cloud-first. To the point where we can use SaaS to accomplish overall IT capabilities that we need, we're driving toward the cloud, and Keyfactor provided how to do that."

Working with Keyfactor, the company moved all of its 34,000 certificates, primarily cover

Industry

Oil & Energy

Employees

10,000+

Keyfactor Products:

Keyfactor Command

Certificates Managing:

34,000+

> **"A lot of the capabilities our team provided in the past were very manual, PKI included. As we looked to move forward, we knew it would be important to find a more automated solution that could also align with our new cloud-first and zero trust objectives."**

web servers, computers, and applications, to the cloud. They also gave internal users access to request new certificates within Keyfactor through single sign-on with Okta to make the end-user process as easy as possible.

The company took several steps to expand on the PKI program compared to what they had in place previously.

- First, they brought all of their external certificates under management through Keyfactor to simplify that process for their web infrastructure team, who previously handled those certificates.
- Second, they introduced automated alerts to notify certificate owners (as well as each person's broader team for accountability purposes) about upcoming certificate expirations. They set these alerts to go out via email on a cadence of two months, one month, two weeks, one week, and one day ahead of the expiration until the certificate gets renewed.

Before setting up the expiration alerts, the team led an extensive effort to clean up all of the data and contacts for every certificate they issued to ensure the alerts reach the organization's right people. This advanced effort, combined with the introduction of the alerts, made an enormous difference in curbing the number of certificate-related outages the organization experienced.

"Previously, we had several outages because teams didn't realize their certificates were expiring, and that could cause systems to go down for up to three days, which had both a financial and reputational impact. The combination of the cleanup effort and introducing the alerts helped reduce the outages significantly, and we started to get recognition around that from leadership about six months in."

Along the way, they have also found significant value in Keyfactor's overall level of service and PKI expertise. "Our team is not made up of PKI experts by any means, but we can pose any kind of question to Keyfactor, and they are great about responding with solutions. They recently ran a health check on our environment, and that helped us identify several new ways to use the platform and improve our program, which was extremely helpful."

"Previously, we had several outages because teams didn't realize their certificates were expiring, and that could cause systems to go down for up to three days, which had both a financial and reputational impact. The combination of the cleanup effort and introducing the alerts helped reduce the outages significantly, and we started to get recognition around that from leadership about six months in."

The Results

Overall, Keyfactor has gone a long way toward helping the identity and access management team achieve their goals around enabling a zero trust environment, remaining cost-effective, and automating wherever possible.

In terms of introducing a zero trust environment, the team shares that they have complete confidence in the security measures enabled by Keyfactor. And on the cost front, they note that the total cost of ownership goes beyond the infrastructure itself. "Our on-premise solution required ongoing management within our data center, so moving the program to the cloud with Keyfactor helped reduce our internal footprint and give our team more flexibility. All of that moves us forward from a strategic standpoint in meeting our broader organizational

"Our team is not made up of PKI experts by any means, but we can pose any kind of question to Keyfactor, and they are great about responding with solutions. They recently ran a health check on our environment, and that helped us identify several new ways to use the platform and improve our program, which was extremely helpful."

goals and providing more variable services to our internal customers. We also see how a lot of the capabilities Keyfactor offers can help us support moving other systems to the cloud in a highly secure way."

Meanwhile, the self-service nature of the request process and ability to automate certificate expiration alerts have also proven huge wins for the team. The team says this level of automation has been a big differentiator from the manual processes they had previously. "Keyfactor maintains itself for the most part. The request process is straightforward for our users, and the other big thing for us was getting team notifications about expirations up and running. Since then, the only thing we do on our side is answer a question here and there since the system doesn't require a whole lot of intervention on our part to keep things working."

The team notes this effort is only the beginning, as they plan to automate the process even further. Right now, the alerts about upcoming expirations are automated, but users still have to go into the system manually to renew their certificate. Going forward, the team plans to automate the full renewal process with Keyfactor to reduce the chance of outages further.

This type of automation is just one of many ways they plan to expand their use of Keyfactor. Another top priority is integrating Keyfactor with ServiceNow to continue improving automation and to allow users to request and renew certificates in a more self-service way through the ServiceNow console.

Beyond that, the team plans to continue leaning on Keyfactor's expertise for even more ways to improve their environment in pursuit of their top-line goals. "Keyfactor is easy to use and has very low transactional costs in terms of what we need to do to keep it running. That, along with with the strong customer support they offer when we do need help, is why we foresee a long partnership with the Keyfactor team."

> "Keyfactor is easy to use and has very low transactional costs in terms of what we need to do to keep it running. That, along with with the strong customer support they offer when we do need help, is why we foresee a long partnership with the Keyfactor team."