KEYFACTOR

CASE STUDY

Leader in Healthcare Information Technology Replaces Venafi to Scale PKI

COMPANY OVERVIEW

This company is the leading US supplier of healthcare information technology solutions that optimize clinical and financial outcomes. Around the world, health organizations ranging from single-doctor practices to entire countries turn to this company for powerful yet intuitive solutions. This company offers clients a dedicated focus on healthcare, an end-to-end solution and service portfolio and proven market leadership.

CHALLENGES

This large, global organization supports a variety of complex and highly regulated needs. As a result, security is of utmost importance for the organization. One of the many ways that this company maintains security for its global corporate users, as well as federal government clients like the Department of Defense and Veteran Affairs, is through a best-in-class PKI program.

That's where Robert, Senior Security Systems Engineer, and his team come into play. According to Robert, they are responsible for handling end-to-end PKI for the entire organization, including standing up internal Certificate Authorities (CAs), owning Certificate Revocation Lists (CRLs), issuing certificates and managing those certificates throughout their entire lifecycle, as well as supporting certain transformational projects, such as a recent transition to the cloud with Amazon Web Services.
It's a big job, to say the least, and the complex nature of the organizational structure, along with the unique needs of its federal clients, don't make it any easier. As a result, when Robert and his team began to experience challenges with their legacy PKI solution, they knew something would need to change.

"We had Venafi, and it was fine for what it did, but there were several drawbacks," Robert explains. "First, it didn't offer any sort of self service for our internal users, so they had to come to us with requests for everything they needed. Second, with Venafi it wasn't possible to manage or report on certificates we didn't issue through Venafi itself, but that was becoming a big need for our federal clients. Third, it just wasn't intuitive. In Venafi, if you don't know what you're doing, it's very difficult to get what you want."

These challenges made it difficult to scale the PKI program and ultimately forced the his team to look for another solution.

SOLUTION

The search for a new PKI solution led Robert's team to Keyfactor. Robert says that one of the biggest selling points for his company's leadership was the cost, as there was a huge difference in price between Venafi and Keyfactor, with the latter coming in far less expensive despite offering more of the advanced features the organization needed.

Industry

Healthcare Information Technology & Services

Employees

10,000+

Keyfactor Products:

Keyfactor Command

Integrated CAs:

50+

> "Comparing Keyfactor to Venafi, Keyfactor is more willing to work with us on getting the product to fit our needs"

Beyond price, he notes many important selling points for his team when it came to managing the PKI program through Keyfactor versus Venafi. For instance, Keyfactor allows for a self-service program in which users can get their own certificates and receive automated notifications when they are about to expire. Robert also found value in Keyfactor's graphical user interface, which he says offers a guided experience that makes it easy for his team to get what they need.

Another important feature for the team was the ability to manage certificates regardless of where they originated from. Specifically, Robert explains there are some certificates that his team doesn't issue but are still liable for, so they needed a solution that could identify and report on certificates it didn't create.

Keyfactor does just that, making it easy for Robert's team to manage and report on any certificates within the organization — no matter where they were issued from — including handling activities like notifications about upcoming expirations.

Equally as important, making the switch to Keyfactor proved relatively easy. "Switching a critical system like PKI is painful in general, especially given all of our security requirements, but it was something we needed to do. Fortunately, Keyfactor made it so the migration was not too difficult. We were able to create a script that pulled all of our certificates and private keys from Venafi and imported them directly into Keyfactor's certificate lifecyle automation solution, so it was just a matter of tweaking the connection points as needed and then running it," Robert shares.

He continues that the easy migration was only the beginning of a positive partnership with the Keyfactor team. "Comparing Keyfactor to Venafi, Keyfactor is more willing to work with us on getting the product to fit our needs, whereas Venafi would just tell us that's the way they do it and to deal with it. Plus, the Keyfactor team is very responsive. If I put in a support ticket, Keyfactor responds within less than 24 hours and they stick it out until it's fixed. I've never had a problem with Keyfactor that wasn't fixed within a short period of time, and I can't say that about anyone else."

RESULTS

Since moving to Keyfactor, this company has resolved the challenges limiting its PKI program and realized several benefits along the way. Specifically, this company has been able to improve its PKI reporting to reduce outages, save time due to self-service certificate requests and scale the program better to accommodate the organization's unique and growing needs.

> "Before, we'd have outages at least twice a month. Now, we've reduced that down to almost nothing."

IMPROVED REPORTING TO REDUCE OUTAGES

Previously, the team had minimal reporting from Venafi. Robert shares that his team had to proactively go into the system to check information like upcoming expirations, and if they didn't catch something and an outage occurred, they were accountable. Keyfactor has changed that entirely.

Now, the team can automatically email people about upcoming certificate expirations so that they can renew the certificates before an outage occurs. The team sets these notifications to go out multiple times for two months leading up to the expiration date to ensure users have ample time to renew. They also go over a full report of upcoming expirations in weekly meetings with business users.

"Before, we'd have outages at least twice a month. Now, we've reduced that down to almost nothing," Robert says.

SAVED TIME WITH SELF SERVICE FUNCTIONALITY

Introducing self-service functionality for certificate requests and certificate renewals has also saved an enormous amount of time for Robert's team.

To start, Robert says that the ability for users to get their own certificates has reduced the turnaround time from **several days to a matter of minutes** and cut down on errors and misspellings for the information required for certificates. He says an important part of making this type of self-service possible is the ability to set guardrails within Keyfactor so that end users who go in to request certificates can only see the templates that are relevant to their group.

Next, the team has also used the Keyfactor API to allow for auto-renewal of certificates. Currently, the team is working on configuring Keyfactor so that it can find an expiring certificate, create a new one and then install it on the proper device automatically.

Altogether, Robert reports that these types of self-service functionality along with the simplified reporting within Keyfactor have **saved his team several hours a week.**

Best of all, Robert says these types of improvements are only the beginning of what his company has planned for its relationship with Keyfactor. Going forward, the his team plans to expand their use of Keyfactor to include additional features like Keyfactor Orchestrator to better manage auto-enrolling of certificates and CRL checking to eliminate outages caused by expiring CRLs. And as his company completes its transition to the cloud with AWS, the team will evaluate how they can better take advantage of Keyfactor's cloud solutions for PKI-as-a-Service.

BETTER SCALABILITY FOR A LARGE AND COMPLEX PROGRAM

Finally, Robert points to the importance of Keyfactor's broad use cases and intuitive interface to helping scale his company's PKI program.

Robert's company manages more than 50 CAs, including a mix of internal and external ones, and Venafi simply could not scale to support this type of program. Robert says that's no longer an issue with Keyfactor, especially because it's easy to manage certificates issued by multiple external CAs within Keyfactor.

In particular, Robert points to the flexibility to customize reports as an important feature for helping scale their PKI program. "With Keyfactor, we can create a collection and say only collect data from the certificates that fall under these templates. This allows us to filter out noise from templates we have that are auto-enrolled or not important to us for various reasons, that way we can easily get to the data we need to do our jobs effectively."

He says Keyfactor not only makes it easy to report on every certificate within their company's environment no matter where they originated, but it also makes it significantly easier to find them. Previously, his team would have to spend several minutes searching through "certificate trees" in Venafi to find a certificate, but with Keyfactor they can simply type information into a search bar and find the information they need in seconds.