KEYFACTOR

CASE STUDY

Global Medical Device Company Introduces Cloud-Hosted & Managed PKI as-a-Service with Keyfactor

Company Overview

This Keyfactor customer is a global leader in medical devices. Driven by a passion for helping patients, the company partners with clinicians to develop innovative technologies that save and enhance lives.

CHALLENGES

This customer has relied on PKI to manage security for quite a while, moving through various iterations of a PKI program throughout the years. For example, around 2013, the security team moved from a legacy setup of several different root Certificate Authorities (CAs) hosted on domain controllers to a two-tier PKI model designed to handle web server certificates and client certificates.

While this shift brought several improvements to the PKI program, it still left many challenges. According to the Senior Information Security Architect, the team didn't have any formal system for managing or reporting on upcoming certificate expirations. This gap led to several critical service interruptions due to expired certificates.

The height of these service interruptions coincided with the support for the on-premise Hardware Security Module (HSM) hosting the customer's Root CA keys. By recognizing the need for a better approach, the team began evaluating their options for more advanced certificate life-cycle management solutions.

SOLUTION

Around 2016, the search for a better certificate lifecycle management solution led this company to Keyfactor. At the time, the organization chose to go with a hybrid model, including hosting their own issuing CAs on-premise. The customer evaluated build vs buy and on-premise vs cloud. They ultimately decided to buy Keyfactor's certificate lifecycle automation capabilities to reduce operating expenditure, and deploy a hybrid approach since the organization was still very much on premise at that point.

In terms of evaluation criteria, the customer notes that the most critical capabilities were reporting and instant alerts that would provide centralized visibility into upcoming expirations. Beyond that, the team also wanted an admin portal to introduce a workflow for web app owners to request certificates.

For the next several years, the customer ran a steady state with their PKI and kept up with all software upgrades. However, they did not take advantage of any new

INDUSTRY

Medical Devices

EMPOYEES

13,000+

KEYFACTOR PRODUCTS

Keyfactor Command

CERTIFICATES MANAGING

40,000+

> "Everyone else we evaluated either had gaps in service offerings compared to what we were used to with Keyfactor or were priced significantly higher."

Keyfactor features or introduced sophisticated, automated workflows around certificate requests, certificate issuance, and reporting.

This changed in 2020 when the customer decided to move from the hybrid environment to a fully hosted PKI as-a-Service model with Keyfactor Command. “We re-evaluated our priorities and looked at the cost of operating on-premise vs. going to a cloud-hosted model. The total cost of ownership analysis was compelling. We found that moving to the PKIaaS model would drastically reduce time spent for our team and help ensure the right level of attention gets paid to certain efforts so that they don’t fall on the back burner -- both of which will be a huge win,” said the Senior Information Security Architect.

He continues that while the team had been happy with their relationship with Keyfactor before, they decided to do their due diligence rather than automatically choosing Keyfactor Command for PKIaaS. “Keyfactor had been a trusted partner for so many years, but we wanted to set that relationship aside to help bolster our business case for the new solution. So we did a bake-off between Keyfactor and other vendors. Everyone else we evaluated either had gaps in service offerings compared to what we were used to with Keyfactor or were priced significantly higher. Ultimately, that helped us reaffirm that Keyfactor is a great fit for us in terms of service offerings and cost for value.

RESULTS

This customer has realized numerous benefits since first introducing Keyfactor on-premise, and they’ve started to reap even more since maturing their program with the Keyfactor cloud-hosted, PKIaaS model.

Specifically, this customer has used Keyfactor to introduce sophisticated governance around certificate lifecycle management. This governance includes offering role-based access to CAs rather than granting access on an individual basis and creating centralized reports and automated alerts to help prevent unnecessary service outages due to certificate expirations.

For example, the customer has set up automated alerts that notify the certificate owners and the IT team about expirations coming up in 60 days, 30 days, and two weeks. The security team now has access to reports that offer a consolidated view of certificates across the organization, including how many certificates are active, when certificates are expiring, where certificates live, and how many certificates have were revoked.

> “Keyfactor does what it says it will do. We’ve been able to customize it to the extent that we’ve needed, and we’ve always had a comfortable working relationship with the account team.”

The customer has also used Keyfactor Command to roll out self-service enrollment for new certificates, which has reduced the amount of time the security team spends on issuing new certificates from 2-3 hours a week to 1-2 hours a month.

This 90%+ time savings includes the issuing process and follow-up requests for help implementing the certificate.

Based on this initial success, the customer plans to expand its use of the Keyfactor platform going forward. Next, they want to integrate Keyfactor with DigiCert (which they use for public CA purchases and public web properties) and ServiceNow.

First, integrating DigiCert will enable the team to manage all of their certificates through Keyfactor, including those purchased from public CAs, and expand the types of certificates available for web app owners through Keyfactor’s self-service enrollment process.

Second, integrating ServiceNow will help further automate the self-service certificate request process by getting the customer to the point where there is the minimal-to-no workload for the security or identity and access management teams to help fulfill the certificate signing requests.

Throughout their partnership, the customer notes that Keyfactor has always been very “low maintenance” for their environment. They concluded the case study by saying: “Keyfactor does what it says it will do. We’ve been able to customize it to the extent that we’ve needed, and we’ve always had a comfortable working relationship with the account team. All of that can’t be said for a lot of other technologies we use.”