KEYFACTOR

CASE STUDY

Global Healthcare Leader Matures PKI for IoT With Keyfactor

COMPANY OVERVIEW

A global healthcare leader, this company manufactures healthcare technologies and products that cover everything from diagnostics and medical devices to branded generic medicines.

CHALLENGES

As a global healthcare leader, security is of utmost importance for the entire organization. This importance has only grown over the past few years. The organization has started to manufacture more advanced medical devices, including connected Internet of Things (IoT) devices that require identification and verification to secure data sharing and software updates.

According to the organization's Senior Manager of Product, Technology, Infrastructure, and Security, they had long used public key infrastructure (PKI) as the backbone of security. While the company was leveraging many best practices of PKI, they did so in a very manual way. He said the organization used a traditional PKI system and deployment model that didn't offer any reporting capabilities and required significant scripting to operationalize the environment.

"The biggest downsides of this approach were a lack of visibility and an inability to scale. On the visibility front, we didn't really know what was being done where or how and why it was being done. But when you're starting to build IoT devices and then selling them to external customers, visibility into what has access to each device is critical. The ability to track, report and manage those devices also becomes extremely important because you no longer have physical access to control them. Some potential solutions emerged over the years to alleviate these visibility problems, but most of them were geared toward corporate laptops and phones, not IoT devices."

The desire to get ahead of these challenges and proactively prepare for even more connected devices led the organization to look for a new solution to manage its PKI program, and to be adequately prepared as the volume of connected devices continued to grow.

SOLUTION

While searching for a new PKI solution, the organization knew they would need a platform that could handle the unique requirements of securing such a large IoT ecosystem. This search led the organization to Keyfactor.

The team evaluated several solutions but ultimately chose to work with Keyfactor based on the platform capabilities and the team's subject matter expertise around PKI for IoT, particularly in the medical device space.

Industry

Healthcare & Medical Device

Employees

100,000+

Keyfactor Products:

Keyfactor Control

Certificates Managing:

200,000+

> "We recently had to do a bulk revocation for an end-of-life product line that covered hundreds of thousands of certificates. Previously, it would've taken an admin a year to do it manually, but with Keyfactor, we revoked everything within 10 minutes."

"We needed someone with granular expertise around PKI, and it's difficult and expensive to bring that type of resource in-house, so the ability to leverage a team like Keyfactor to jumpstart that initiative is huge. Beyond the fact that Keyfactor offered management, reporting, and native integration capabilities that other platforms did not, their expertise and ability to act as a true partner for our team was a major reason we chose to work with them."

This decision paid off: Introducing Keyfactor has led to faster and easier product launches since developers can now programmatically call the PKI system to take certain actions rather than having to write scripts manually.

Additionally, the team uses Keyfactor to issue certificates and keys to build relationships between different components in medical device ecosystems, establish identities for those devices, and build key derivations that allow for data encryption and decryption. Specifically, this leads to a workflow that covers:

- Encrypting data from a trusted endpoint like a pacemaker
- Sending that encrypted data to an untrusted device like a patient's personal phone
- Authenticating that phone to the cloud server using certificates, and enabling transfer of encrypted data
- Allowing the server to decrypt the data

Ultimately, this is one example of how the organization uses certificates to communicate and share data with IoT devices. Importantly, Keyfactor also enables the team to tie metadata to IoT device certificates to enable actions such as secure enrollments, which help verify device origin and authenticity.

The organization also uses Keyfactor for secure device provisioning in manufacturing. They install cryptographic identities using trusted ATE stations, making certificate requests on behalf of pacemakers and other medical devices. This approach allows the team to tie roles to certificates so that devices can only accept certain types of communications, for example to only accept an over the air (OTA) update from a trusted provider.

RESULTS

The organization has realized several benefits since introducing Keyfactor into their day to day IoT device security operations. Most notably, they have:

> "Keyfactor solves IoT operational issues that simply don't come standard with other PKI solutions."

INCREASED VISIBILITY

First, the organization has increased visibility into their overall IoT device security platform. Keyfactor's user-friendly interface makes it easy to build reports that provide insight into which keys and certificates get created, where they exist, when they get created, what access they provide and when they're set to expire.

This increased visibility has helped operationalize the PKI environment, for example, by making it easy to identify upcoming expirations and respond accordingly to keep IoT device security up to date. Prior to this, the organization housed all this information manually in spreadsheets, which led to a time consuming and error-prone process that simply wouldn't scale. Now, Keyfactor puts all this information at users' fingertips in an easy-to-view, error-free format and automates processes like certificate renewal.

"Keyfactor solves IoT operational issues that simply don't come standard with other PKI solutions. Now, when I go into the Keyfactor portal to see what's going to expire soon, I know I'm not going to get false information because of human error that could lead to an outage."

AUTOMATED CRITICAL ACTIVITIES

Second, Keyfactor has enabled the organization to automate many PKI activities, leading to **significant time savings**.

This automation has proven extremely valuable when it comes to revocations. For example, if the company had a 5% failure rate for a device, previously, the security team would have to find those devices and manually revoke each certificate. But with Keyfactor, they can simply feed the list of serial numbers for those devices to the API and automate the revocation process.

"We recently had to do a bulk revocation for an end-of-life product line that covered hundreds of thousands of certificates. Previously, it would've taken an admin a year to do it manually, but **with Keyfactor, we revoked everything within 10 minutes**."

INTEGRATED PKI INTO DEVOPS PROCESSES

Third, Keyfactor has allowed the organization to integrate PKI into DevOps processes seamlessly. Prior to implementing Keyfactor's automation platform, users had to write complex scripts to talk to the native crypto-libraries. Keyfactor's programmatic interface eliminates that need, which has **saved the organization significant time and money**.

"Keyfactor adds a nice front layer that you can run programmatically, so anyone can handle it. That's a big difference from our traditional systems, which had crypto-library integrations and required a particular skill set."

Throughout it all, the organization has valued Keyfactor's strong expertise and overall responsiveness to answer questions and put in place the right processes to establish a robust PKI program for their IoT devices.

Going forward, they plan to expand their use of Keyfactor as the organization prioritizes DevOps and cloud and data localization. "We handle patient health data, so we work in a highly regulated industry, and that has made more local connectivity for data a top priority for us. Right now, we're looking at how we can scale Keyfactor for our programs around the world and do so in a more automated and centralized way to continue maturing our program."