KEYFACTOR

CASE STUDY

Global Investment Firm Reduces PKI Management & Accelerates DevSecOps with Keyfactor

COMPANY OVERVIEW

This global investment firm has close to 100 years in experience applying discipline and long-term perspective to managing client portfolios. With global offices in North America, Europe, Asia, and Australia, this firm provides diverse investment strategies and wealth management solutions.

CHALLENGES

Over the past several years, this global investment management firm has made a concentrated effort to innovate and bring new products and services to market in a cost-efficient way that adds value to clients.

The organization's security team has played an important role in this innovation, partnering closely with the product development team to launch new, cloud-centric products in a secure way. Overall, the organization has started to embrace a DevOps approach in these processes, which requires the security team to shift left to help speed development securely.

However, the organization's security team is a lean one. According to the VP of Information Security, the team is responsible for all security operations, planning, consulting and risk management as well as some compliance and governance efforts. This means that in order to fully shift left, the team needs the proper bandwidth to focus on partnering with developers rather than day-to-day maintenance.

"We're a lean team that supports a lot of operations, so we typically look for tools that will be easy to manage or will even 'manage themselves' so that we can focus on providing value back to the organization," he explains.

Most recently, the team found an opportunity to embrace this ethos with the organization's PKI program. They had used an on-premise PKI environment to issue certificates for internal devices and systems for ten years. While the system still worked, it required significant attention from the security team.

"We had to focus on a lot of operational efforts for the PKI program. Generating CRLs, rotating keys and identifying when certificates were going to expire were all maintenance-heavy activities. We also had to worry about backing up the HSM, keeping it secure and maintaining high reliability. Even integrating the system with most of our other tools was challenging."

On top of those day-to-day operational challenges, disparate teams were responsible for managing certificates, which made it confusing for users to know who to contact when they had a request or needed help.

Industry

Investment Management

Company Size

Global 2000

Employees

1,300+

Keyfactor Products:

Keyfactor Command

Certificates Managing:

7,500-10,000

> "We're a lean team that supports a lot of operations, so we typically look for tools that will be easy to manage or will even 'manage themselves' so that we can focus on providing value back to the organization"

SOLUTION

As the organization's security team continued to take a more active role in the development process, the VP of Information Security knew they would need to find a better approach to PKI that required less day-to-day maintenance.

"First, we needed a solution that would relieve an operational burden for us by paring down the number of tools we had to manage and by integrating well with the tools we already adopted. Second, we wanted to partner with a service provider who could offer additional value by helping us use the platform in ways we simply aren't able to on our own," he says.

This search led the organization to Keyfactor. The team looked at several other cloud providers for hosted PKI, but ultimately chose Keyfactor to gain access to the PKI-as-a-Service model and because of the team's overall expertise.

Now, they rely on Keyfactor for two primary use cases. First is adding traditional TLS certificates to internal web servers and devices. Second is integrating into the company's MDM and hardware inventory system to fully automate the process of issuing and revoking certificates for endpoints as they go on and offline. This approach has allowed the security team to become the single point of contact for all things PKI to centralize management and reduce confusion within the organization about who to engage for requests.

While these use cases sound simple, there's a lot that goes on behind the scenes to make them that way. Keyfactor's inventory and reporting capabilities allow the security team to quickly and easily pull a single report that shows information like how many certificates are in use and when they're expiring. Even better is the ability to automatically alert team owners when their certificates are about to expire, which relieves the security team from having to manage these expirations manually. This type of reporting also simplifies the process of charge backs to allocate internal spend by showing a single view of how many certificates each business unit within the company uses.

Equally as important is the seamless integration between Keyfactor and other systems, including the organization's ticketing system, MDM and Active Directory. In fact, Keyfactor integrates so well with Active Directory that the security team says they often forget it's even there.

Beyond the platform itself, the organization has also found a trusted strategic partner in Keyfactor. The VP of Information Security shares: "We want to focus on what we know works and have someone else who is an expert manage it. We want to partner with someone who's going to make us stronger. The platform is one piece of that, but the other is the ability to say we have a problem and ask Keyfactor for advice on solving it based on their expertise and knowledge of what other organizations are doing."

RESULTS

The investment firm has realized several benefits since moving to Keyfactor's PKI-as-a-Service. Most notably, they have:

REMOVED PKI COMPLEXITY, SAVED TIME

The organization's **security team has saved 20% of their time** since moving to PKI-as-a-Service with Keyfactor. This is time they can now devote to adding more value back into the business, rather than spending it on operational care and feeding.

"Keyfactor has resolved an operational headache for us by relieving the day-to-day management of PKI. They're also a trusted operational resource that we can go to for help figuring out solutions as new challenges arise. Together, this allows our team to get involved in more advanced business conversations around further increasing speed and agility, and we know that Keyfactor can help in those areas too," the VP of Information Security explains.

> "Keyfactor has resolved an operational headache for us by relieving the day-to-day management of PKI."

IMPROVED DEVSECOPS EFFICIENCY AND DEV COLLABORATION

By saving the time spent formerly managing their own PKI, the security team can get more involved in product development conversations from the very beginning. This includes talking about security and privacy requirements based on factors like who will access the system and the types of data that will be stored in the system so that they can be addressed in the product design from the very beginning.

He adds: “We’re working to gain the trust of our development teams. Previously what prevented them from working with us more was the fear of something being blocked, so we want to make sure those cases are few and far between. We want them to engage us without any fears, and being a part of their conversations from day one has helped strengthen the relationship between our teams and establish a pattern for how to evaluate security needs without slowing anything down.”

For example, the two teams previously took a blanket approach of “encrypt everything.” But now instead of simply handing out certificates, the security team can be more consultative and look at each piece of software to determine whether it really needs encryption based on its purpose and provide unique security solutions accordingly.

“We’re really able to take the time we previously spent on operational support and use it to shift left and have conversations with developers early on in the product development lifecycle. We want to make that process as frictionless as possible. We want to make them comfortable coming to us by offering easy and flexible solutions that are also secure. Traditionally that wasn’t easy to do, but we’re making progress and we’re leaning on Keyfactor as a partner to help us achieve that goal.”

This type of relationship will only grow in importance as development processes continue to speed up and the volume and velocity of certificates required increase as a result. In fact, the organization is eying a future state in which the development team will spin up pieces of infrastructure that will only last for a few hours or a day and will require a certificate to be issued and revoked accordingly.

Based on these growing needs, the organization plans to continue to expand the relationship with Keyfactor. Some of the most immediate projects include introducing a self-service process for developers to request certificates and integrating with the company’s external CA to manage all certificates from a single place.