Law Firm 'Shifts Security Left' with PKI as-a-Service

COMPANY OVERVIEW

With nearly 1,000 attorneys across the United States, this firm offers a broad range of legal services that span everything from business and digital assets to employment and tax.

CHALLENGES

As a large law firm, this organization has a variety of strict security requirements to protect its clients' data. The firm centralizes this security with a small team focused on engineering services that support network, cloud, and client engineering. One of their key goals along the way is to provide this support with zero disruptions to end-users.

The engineering services team had built a homegrown public key infrastructure (PKI) program many years ago to stand up certificates on web servers. However, their PKI needs evolved in the years since then to cover efforts like providing secure access to remote systems and this growth began to stretch the limits of the homegrown solution. At the same time, the system on which they built this solution, Windows Server 2003, was nearing its end of life, which left the team with a decision to rebuild their program or introduce a new platform. Ultimately, they chose to go with a new platform to gain access to more advanced capabilities that would help continue expanding and maturing the PKI program.

"We stepped back, looked at what we had, and thought about what we wanted in a better end state. At the time, people could submit requests for certificates and

wait days because information got lost or wasn't entered properly and because all approvals had to go through one person. We also had multiple templates, which created confusion. We decided we wanted to bring more structured workflows to the program to streamline processes and help us continue to offer the most secure solutions," the Senior Manager of Engineering Services explains.

Additionally, they identified finding a managed solution as an important part of this search in order to reduce the disruption for end-users and help outsource work from their small team.

SOLUTION

The law firm evaluated several PKI platforms and found that Keyfactor offered the best solution for their needs based on capabilities, managed services and overall value.

"We looked at multiple managed PKI solutions, and Keyfactor's PKI-as-a-Service was the only one that met our needs. It's also lived up to that promise. Keyfactor has been a true partner for us, helping build an

Industry
Law Practice

Employees
1,000+

Keyfactor Products:
Keyfactor Command

Certificates Managing:
10,000+

> The solid PKI foundation we've built with Keyfactor has been the key to leveraging these advanced systems, especially as we adopt more cloud solutions."

environment where we can easily do everything we need to, from rolling out new certificate templates to notifying application owners about upcoming expirations," the Senior Manager of Engineering Services shares.

Specifically, Keyfactor has given the firm a more secure solution with better workflows to meet key goals like:

- Guaranteeing certificates are approved, renewed, and updated on schedule, and that the team gets notified when

those activities happen—which is no easy feat since the firm's policy dictates a one-year lifespan for all certificates.

- Streamlining certificate requests and management processes by offering a self-service model for certificate requests, delegating certificate approvals to multiple managers (vs. having only one approver), and automating expiration alerts to certificate owners.

- Using certificates to provide secure, remote access to the firm's VPN to power wireless authentication for nearly 1,000 attorneys across 17 offices.

RESULTS

Overall, using Keyfactor has helped the law firm improve visibility, efficiency, and the overall organization of its PKI program, leading to a more secure environment that can support increasingly advanced use cases. Some of the most notable advancements the firm has made since working with Keyfactor include:

❝ We looked at multiple managed PKI solutions, and Keyfactor's PKI-as-a-Service was the only one that met our needs."

SHIFT LEFT OF SECURITY PRACTICES TO SPEED DEVOPS PROCESSES

First, the firm has been able to shift security practices left within development to deliver new solutions faster. The best example of this was the organization's ability to quickly roll out a new, health-focused application to help its employees safely and easily return to work during the Covid-19 pandemic.

The firm needed a way for employees returning to the office to easily complete a health checklist and then route that information to HR, and they wanted to make this process as simple as possible. Ideally, this meant avoiding log-ins or form submissions.

They decided to build this solution in house, and the engineering services team was able to offer a hassle-free way for users to submit their information by incorporating certificates for secure authentication and data transmission. Additionally, using Keyfactor to issue these certificates allowed the team to introduce this capability efficiently within the development process to get the application into the hands of users quickly.

Overall, this is one example of many that demonstrate the value of shifting security left within the development process. The firm has moved a lot of development work to the cloud with Microsoft Azure and developers now spin development environments up and down frequently, so having an agile PKI program that can support that speed has been a huge win for the organization overall.

STRONGER, MORE MATURE SECURITY WITH A PASSWORD-LESS ENVIRONMENT

Next, the firm has reached the point where they aim to use certificates wherever possible to strengthen and mature their security by moving away from passwords.

"We push out certificates to every endpoint, whether it's a laptop, desktop, mobile phone, internal web server, client-server, or anything else. Our policy is, if you can use our PKI, you use it," the Senior Manager of Engineering Services says.

"We're always looking for ways to continue strengthening security and simplify things for our users, like trying to get away from passwords wherever we can. There's a lot going on right now with the transition to a more mobile workforce, so pushing password-less, certificate-based authentication makes it a lot easier for end-users."

MORE SEAMLESS PKI WORKFLOWS

Finally, the firm has been able to streamline and standardize a variety of PKI workflows since using Keyfactor. This covers everything from how certificates get requested and approved to how the firm handles upcoming expirations for those certificates. In doing so, Keyfactor has helped the firm increase visibility into their PKI program and avoid outages due to a lack of visibility into upcoming certificate expirations.

Altogether, having these seamless PKI workflows has not only made the day-to-day management activities the organization was already doing easier, but it's also enabled them to introduce more advanced measures, like moving to certificate-based authentication for machines and improving wireless VPN access.

Going forward, the firm plans to further expand on these results by continuing to introduce more advanced uses of PKI. Top priorities include strengthening Powershell scripts for deploying updates to endpoints and more effectively managing and securing a newly remote workforce.

The Senior Manager of Engineering Services concludes: "The solid PKI foundation we've built with Keyfactor has been the key to leveraging these advanced systems, especially as we adopt more cloud solutions. Having a structured PKI program with good workflows has unlocked a lot of opportunities for us and it will help us continue to strengthen and mature our program as we embark down new roads."