Case Study

Fortune 500 Insurance Company Chooses Keyfactor to Achieve Automation

Shifting from manual certificate management to certificate lifecycle automation allows company to achieve crypto-agility and secure digital initiatives.

Company Overview

As one of the world's largest commercial property insurers, this Fortune 500 mutual insurance company has been in business for nearly 200 years. With clients in more than 100+ countries, they deliver solutions to help business mitigate risks and prevent losses. As a global financial services provider, cybersecurity is a top priority to ensure they can protect themselves as much as their clients when it comes to trust and identity.

Challenges

This Fortune 500 insurer is no stranger to innovation, having evolved several times during its 200-year history. Most recently, this meant leading a sizeable Agile transformation to reimagine the firm's digital client experience — which also created a vital security imperative for their infrastructure and operations team.

"Our digital teams can have the most wonderful vision, but we need to execute on it in a secure way, because if the end result isn't secure, then none of the innovation matters," explains Anthony, a member of the infrastructure security team.

Industry

Insurance

Employees

5,000+

Keyfactor Products

Keyfactor Command

"Our digital teams can have the most wonderful vision, but we need to execute on it in a secure way, because if the end result isn't secure, then none of the innovation matters."

This thinking led his team to realize their legacy certificate management solution just couldn't keep up with their cloud-first and agile initiatives. A homegrown portal for users to request certificates would need a complete upgrade to meet their transformation needs, and three key challenges stood in the way of success:

> "We're all about security through enablement, so we started looking for the sweet spot that would deliver functional benefits to our users by making things easier for them while also increasing security."

1. Lack of visibility:

The monitoring process was manual and offered limited visibility, which created a high risk of outages for internal and external systems due to expired certificates.

2. Manual process:

The provisioning process used a homegrown system with security issues and time-consuming, manual workflows for the security team.

3. Limited integration:

Existing tools did could not programmatically deploy certificates within their CI/CD pipeline, making integration work with new or existing applications in the development process near impossible.

To resolve these challenges and ensure the firm's security could support the vision for a new digital client experience, Anthony and his team began looking for a certificate lifecycle automation solution. He highlighted that a key priority was to balance ease of use with security.

"We're all about security through enablement, so we started looking for the sweet spot that would deliver functional benefits to our users by making things easier for them while also increasing security," he explains.

Solution

The company's team reached out to Gartner with a specific list of requirements to help jumpstart their search for a solution. Gartner used that list to recommend three potential vendors, and the company decided to do a proof of concept with two of those vendors.

According to Anthony, they quickly realized some "illusions" in what one of the vendors offered. He mentioned, "when we did the proof of concept, they failed left, right, and center on key capabilities and that gave us tremendous pause. The product really wasn't well-operationalized, and made even basic tasks like changing SSL certificates complex and time-consuming."

This experience stood in stark contrast to the Keyfactor proof of concept. Anthony says, "the Keyfactor team was outstanding every step of the way. They asked about our environment and then built something very similar to it within their product, and they got the whole proof of concept built out quickly," Anthony shares.

Importantly, not only did Keyfactor's product provide everything their team was looking for and then some, but they had the right team and expertise to back it up. Anthony adds: "I had a use case in my mind that had to be satisfied in a certain way, but the Keyfactor team asked if I would be open to solve it differently. I'm not an easily persuaded person, but they got me on board, and it really was a better way to do it. That spoke to Keyfactor's overall experience and approach to solving problems based on the desired end state, not just the means."

"Keyfactor is a very complete solution, and I know we're getting everything we wanted and then some. I always get nervous that salespeople make everything sound wonderful, and then you get to the implementation, and the product or the team isn't what you expected, but that's not the case with Keyfactor," Anthony shares. "Plus, if there's anything that hasn't gone the way we've intended, the Keyfactor team has responded instantly to fix it."

"I see Keyfactor as very forward-thinking and I want them involved in our digital security initiatives. Digital certificates are only going to increase for us, and I want to make sure we're using Keyfactor to automate as much as possible."

The Results

The Fortune 500 mutual insurance provider decided to move forward with Keyfactor based on their proof of concept, and Anthony says they could not be more pleased with the outcomes.

“Keyfactor is a very complete solution, and I know we’re getting everything we wanted and then some. I always get nervous that salespeople make everything sound wonderful, and then you get to the implementation, and the product or the team isn’t what you expected, but that’s not the case with Keyfactor,” Anthony shares. “Plus, if there’s anything that hasn’t gone the way we’ve intended, the Keyfactor team has responded instantly to fix it.”

To start, the team is working with Keyfactor to enable discovery, monitoring, and lifecycle automation for internal certificates through Active Directory Certificate Services (ADCS) and external certificates through DigiCert. They also plant to integrate with Azure Key Vault as part of their cloud-first transformation.

The results so far have exceeded the team’s expectations. Anthony notes that not only does his team have the necessary monitoring tools and visibility to prevent outages that they lacked before, but Keyfactor also makes processes far more efficient. What took three days in some other solutions takes a matter of five minutes with Keyfactor. As a result, Keyfactor has succeeded in making security a benefit for the firm and its employees, not an obstacle.

Based on this initial success, the company plans to continue expanding its relationship with Keyfactor. First, Anthony notes that there’s an appetite for shifting to Keyfactor’s Cloud PKI as-a-Service model to help future-proof their strategy and offload unnecessary complexity. Second, he shares that his team plans to bring Keyfactor into decisions as a trusted partner.

“I see Keyfactor as very forward-thinking and I want them involved in our digital security initiatives. Digital certificates are only going to increase for us, and I want to make sure we’re using Keyfactor to automate as much as possible.”

About Keyfactor

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human.

Contact Us

- www.keyfactor.com
- +1.216.785.2946