

Case Study

Containerizing Security: How Keyfactor Leverages Docker and Open Source Ethos for Scalable Digital Protection

About company: Cybersecurity

Company size: Serves over 1,500 customers in 70 countries, including major U.S. commercial banks and telecom companies

Industry leader: Recognized with multiple industry awards for contributions to cybersecurity, workplace culture, and technological innovation

Highlights



MLOps team scales AI/ML efficiency with Docker and Kubernetes



A unified platform makes collaboration among Ingka Group's AI/ML teams more consistent and efficient



Noticeable advancements in development speed, scalability, and security

Introduction

Global reach and essential products

Keyfactor is a leading cybersecurity company with a global footprint that provides robust digital identity and signing solutions. With a diverse customer base ranging from small start-ups to government agencies and multinational corporations, Keyfactor's products are essential for organizations who want to secure digital transactions and communications for a robust open source community of users. The innovative security company provides solutions to over 1,000 customers across 70 countries, including four of the top ten U.S. Commercial banks and three of the top U.S. telecom companies.

Since the early 2000s, Keyfactor has been committed to open source principles integral to its identity and mission. Embracing the collaborative ethos of openness and transparency, teams recognized the transformative potential of community-driven collaboration and innovation, particularly in cybersecurity software.

"Docker Hub provides visibility and facilitates discovery, particularly for our solution. Generally, developers often turn to Docker Hub to search for software, which is also advantageous for us."

Malin Ridelius
Keyfactor's Vice President
of Community



For developers and engineers that need Public Key Infrastructure (PKI), certificates and digital signing, self-signed certificates and tools like OpenSSL might suffice for basic needs. Keyfactor offers essential products like EJBCA PKI and SignServer as open-source community editions, which are easy to start with for testing and piloting. Additionally, Keyfactor provides a seamless transition to production with its Enterprise editions, which includes SLA and secure scaling capabilities necessary for a compliant production environment.

EJBCA is a versatile and comprehensive enterprise PKI and certificate management solution that underpins digital security across various sectors. SignServer was initially developed to support electronic or biometric passports and has since broadened its utility to encompass code and container signing, document/PDF signing, and timestamping. Since their respective developments in 2001 and 2007, both products have significantly evolved.

As a community and open-source user, deploying these technologies from source required a steep learning curve for installation before they could use these high-value security solutions. Keyfactor looked to Docker to help them with a more straightforward packaging format and, as a side benefit, saw Docker Hub as a way to improve the reach of their products.

Challenges with traditional open-source and community deployment methods

Keyfactor's challenges stemmed from the fact that their existing community users heavily relied on Keyfactor's community editions delivered as source code. Security experts or engineers who were very technically adept at building new products and securing systems were not as savvy when it came to compiling these solutions from scratch. While effective for some, this approach proved complex and inaccessible to many users, particularly as the demand for their PKI and Signing technologies increased and their user base diversified.

The dilemma centered on making open source security software accessible to a broader audience in an easily consumable format. Their user base required that it should be easy to get started and try the software out. Keyfactor needed to devise a more straightforward means of software consumption and a platform to reach a larger audience of security experts and engineers.

“Integrating Docker into our deployment strategy was a turning point for Keyfactor. It simplified our processes and significantly reduced the time from development to deployment, making our cybersecurity tools more accessible to developers and organizations worldwide.”

Sven Rajala
Keyfactor's International PKI
man of Mystery

“Our relationship with Docker thus far has been instrumental. Docker containers and Docker Hub stand out as the go-to platforms for building and accessing containers, catering to developers worldwide. Docker has consistently upheld high standards of security assurance concerning containers, a quality that aligns perfectly with our own priorities. Looking ahead, we aspire to deepen our collaboration with Docker, particularly in container signing. By pooling our expertise, we would like to work on standardized approaches to address signing concerns using our open-source tool. This topic is a heightened focus within organizations today.”

Malin Ridelius
Keyfactor's Vice President of Community



The shift to Docker for simpler deployment

Packaging their EJBCA and SignServer software into Docker containers made the community editions even more accessible to a new audience. This approach dramatically lowered the barrier to entry, facilitating easier adoption for users. They made EJBCA and SignServer available through the Docker Hub container registry, designed for developers and open source contributors to discover, utilize, and distribute container images. EJBCA and SignServer Enterprise editions offer various deployment options to meet typical enterprise needs, including software and hardware appliances, SaaS, and PKI as a Service.

Docker Hub's functionality significantly enhanced the visibility of EJBCA PKI and SignServer, making it easier for their audience to find and engage with the software. Docker Hub also exemplified quality assurance by scanning containers for vulnerabilities, aligning seamlessly with the Keyfactor sustainability theme.

The Solution

Optimizing community deployment with containerization technology

Keyfactor's core principles are grounded in the open source philosophy. By leveraging Docker, they simplified the distribution and deployment of their open source cybersecurity tools, making essential security practices accessible to a broader audience as they embark on their PKI and signing journey.

Recognizing the complexities and challenges associated with deploying open source software from code, Keyfactor saw only one practical solution: leveraging Docker containerization technology.

Docker containers are lightweight and self-contained, which means they can be easily deployed on any infrastructure that supports Docker. This reduced the time and effort required to deploy and get started with testing or prototyping the PKI and signing solutions allowing the engineers to focus on other tasks, like building new products or applications.

"The beauty of Docker is in its simplicity and unique way of packaging applications. For Keyfactor, we could offer our EJBCA and SignServer solutions so that anyone, regardless of their technical background, could easily deploy and manage their own PKI infrastructure."

Sven Rajala
Keyfactor's international
PKI man of Mystery

"The advent of containerization with Docker Hub has simplified the deployment process. In the past, people faced significant challenges in deploying our applications effectively. However, we witnessed a remarkable shift with Docker Desktop and Docker Hub. Instead of customers bombarding us with inquiries about building the source code, we encouraged them to try the application with a simple "Docker pull" and "Docker run" command. This quick and straightforward approach reduced the need for extensive technical assistance."

Tomas Gustavsson
Chief PKI Officer at Keyfactor



Key Benefits

Following the integration of Docker into Keyfactor's deployment processes for EJBCA and SignServer, several vital benefits were realized that directly contributed to the company's wish to grow the community and make PKI and Signing software available to all:

- **Streamlined deployment process:** Docker's containerization simplified the initial setup and ongoing management of Keyfactor's cybersecurity tools, significantly reducing the time and complexity of deploying new instances of EJBCA and SignServer.
- **Consistent and reliable environments:** Keyfactor used Docker containers to ensure its applications ran consistently across different computing environments. This consistency reduced the "it works on my machine" problem, leading to fewer deployment-related issues and a more reliable service for end-users.
- **Simplified management and maintenance:** Docker containers encapsulate an application and its dependencies into a single, portable unit, simplifying software updates and maintenance. This encapsulation meant Keyfactor could update or patch their applications with minimal downtime and client disruption.
- **Open source advantages:** Keyfactor's commitment to open source solutions, such as EJBCA and SignServer, combined with Docker's large community of users, helped distribute and raise awareness of Keyfactor's products.

Keyfactor has witnessed a steady increase in downloads, and they anticipate further growth, given the endless demand for robust cyber security tools. Continuously striving to enhance its software, the company actively engages with the Docker community to simplify deployment processes.

Keyfactor believes engineers and developers must prioritize security from the outset to mitigate future risks and costs. The company emphasizes the importance of scalability planning during prototyping and testing, ensuring a secure and adaptable solution to evolving needs.

Results

Stronger digital defenses through innovative integration

Keyfactor aspires to impact the world positively through their technology. It's crucial for them to develop the best software and explore innovative avenues for reaching users wherever they frequent. Keyfactor's adoption of Docker to deploy EJBCA and SignServer Community editions illustrates a successful strategic move in cybersecurity. Upon moving to Docker, Keyfactor saw many improvements in their user adoption, fewer technical hassles, and a broader scope for innovation, allowing them to reach a more diverse range of use cases and users.

Docker allowed Keyfactor to offer more reliable and efficient security solutions by addressing deployment complexity challenges. Keyfactor witnessed how embracing innovative technologies like Docker can significantly impact the cybersecurity industry's operational efficiency and market responsiveness. As Keyfactor continues to evolve, its foundational commitment to open source solutions and the strategic use of Docker technology will remain integral to its mission of providing accessible, secure digital environments.

