CUSTOMER STORY

Fortanix | BeeKeeperAI®

BeeKeeperAI Accelerates Healthcare AI and Enables Secure Healthcare Data Collaboration with **Fortanix Confidential Computing**

Customer Profile

Created at the University of California, San Francisco (UCSF), Center for Digital Health Innovation (CDHI), BeeKeeperAI accelerates the development and deployment of artificial intelligence (AI) algorithms in healthcare. The BeeKeeperAI platform allows healthcare data stewards to keep their sensitive data in their secure cloud environment while safely providing access to the data for 3rd party development and deployment of AI solutions to improve outcomes and reduce the cost of healthcare.

Accelerating Deployment of Healthcare AI by 1000x

BeeKeeperAI® cdhi Center for Digital Health Innovation at UCSF

Role of AI in Healthcare

Experts have estimated that Machine learning (ML) and algorithms have the potential to improve outcomes by 30-40% while cutting treatment costs by as much as 50%[1] . As a result, healthcare AI is predicted to become a $45 billion industry over the next five years.

PROBLEM:

The Problem of Timely and Secure Access to Highly Diverse, Real-World Data

The primary challenge with clinical quality ML algorithms is the need to access to high quality, diverse datasets that are representative of global patient populations. The standard of clinical generalizability applied by most regulatory agencies requires that algorithms must produce similarly accurate results regardless of the type of data acquisition equipment, the demographics of the patient population, clinical setting, or other social determinants. To meet the standard, an algorithm developer must have access to data representative of that which the model will face when it is deployed into diverse clinical environments.

As stewards of protected health information, healthcare organizations have a legal and ethical obligation to prevent inappropriate data access resulting in privacy breaches. This obligation and the risk of financial and reputational consequences of a privacy breach has created an environment where data stewards are extremely hesitant to share or allow access to their sensitive patient data. Escalating cyber-attacks on healthcare data have further increased pressure on data stewards to limit third-party data access. This enhanced security results in protracted contracting and internal approval processes that typically takes 9 to 18 months per data steward organization in order to gain access to the data required for an AI or ML model. Costs for sufficient data access to develop a clinical quality, generalizable algorithm can be up to $3 to $5 million per algorithm. With most models requiring access to data within multiple institutions, the time and cost to secure access has become a major barrier to the development of AI/ML.

- Several solutions have been developed to overcome the data access challenge including data de-identification and synthetic data. While these methods are appropriate for certain applications, the process of de-identifying and creating fake (i.e., synthetic) data introduces artificial noise into the data that are not found in the real-world. Developing AI/ML algorithms on these data, runs the risk of unreliable or unpredictable performance, reducing their clinical utility

- For data stewards with a mission to advance scientific discovery, clinical care, and innovation, this added data security can make it difficult to collaborate with other researchers and algorithm developers to create the next medical breakthrough.

1 Frost & Sullivan

In summary, the challenges in realizing the promise of healthcare AI include:

• Generalizability requires access to large, high quality, highly diverse real-world data
• Gaining access to diverse data is time consuming and costly
• With increasing incidents of cyberattacks and ransomware, secure management of data is a major challenge and a key risk for data stewards

> *The biggest barrier to the development and deployment of generalizable, high quality healthcare AI is the challenge of accessing sufficient real-world data for algorithm development. The challenge for data stewards is they want to advance their mission of scientific innovation, improved quality, and lower costs but need to do so without creating significant risks to patient privacy or data misappropriation*

Dr. Michael Blum
Co-founder and CEO BeeKeeperAI, Inc.

-Dr. Michael Blum

Changing the Healthcare Data Access Paradigm

BeeKeeperAI's leadership team has years of experience in overcoming the challenges in gaining access to sufficient data to ensure algorithms are free of bias and capable of consistent performance.

After years of utilizing the traditional approach, the team decided to find a safer and more efficient method for accessing data to help accelerate their healthcare AI development. They began to challenge the paradigm of "sharing data" to eliminate the risks associated with loss of control of the data. They asked how the data could remain in the control of the data steward (within their HIPAA compliant cloud environment), and they envisioned a model where an algorithm could be sent, via a secure cloud, to the data where it would compute against the data. By keeping the data and the algorithm encrypted there would be no risk of data exposure or privacy breach.

In 2018, BeeKeeperAI's leaders saw the application of confidential computing and privacy preserving analytics in the financial services and government security sectors. They realized that if these technologies could be applied to healthcare data, it could be possible to provide an even more secure method for accessing data and developing ML algorithms. The founders set out to create a minimum viable demonstration of integrating healthcare workflows and tools with the enhanced security features. In June 2020 a minimum viable product successfully demonstrated the promise of leveraging confidential computing in healthcare.

BeeKeeperAI allows the data steward to curate a specialized data set required for an algorithm, encrypt, and place the data into a BeeKeeperAI node running in the data steward's HIPAA-compliant cloud environment, where a model is brought to it and runs against the data. The data remains under the data steward's control, even when they're participating in an AI/ML development or deployment.

> *We accomplished some great advances in care through our AI development at UCSF's CDHI. But even in the context of a leading academic medical center, we experienced the difficulties of accessing high quality diverse data sources to develop and validate our clinical AI. That led directly to the development of BeeKeeperAI. It became our mission to enhance the security of real-world patient data while providing faster, easier, less expensive access to that data for AI development and deployment."*
>
> **Dr. Michael Blum**

Why BeeKeeperAI Chose Fortanix

BeeKeeperAI required Confidential Computing

Traditional security models have been widely used to mitigate risks involved in data lakes, data storage, and transmission but have fallen short of securing the data while it is being processed. Over the years, data security has evolved and is now focused on a more holistic approach that can help mitigate risks across the data lifecycle. Confidential Computing offers a comprehensive approach to securing data across its lifecycle as it protects data and applications when in use, ensuring data and code integrity and, auditable, data confidentiality. Confidential Computing allows organizations to process data inside trusted execution environments (TEEs) using compute resources that are now available within the cloud.

To enable secure access to real-world healthcare data for AI developers, BeeKeeperAI turned to Confidential Computing technology and Fortanix as the pioneer and global leader for this capability within its platform. Partnering with Microsoft, Intel, and Fortanix BeeKeeperAI is leveraging cutting edge security technology and environments for its healthcare AI collaboration platform allowing healthcare organizations to host privacy preserving analytics within a trusted environment, while keeping data secure. Healthcare data can now be utilized to develop and deploy algorithms or analytics without the risk of compromise or unauthorized access.

Progress in AI approval by regulators and its subsequent adoption has been slow primarily because of the difficulty in acquiring access to sufficient real-world data to meet the generalizability standard. Even though hundreds if not thousands of healthcare AI algorithms are forecasted fewer than 50 that have made it through the FDA approval process. BeeKeeperAI, secured by Fortanix' Confidential Computing technology, is helping to accelerate AI adoption within the global healthcare industry.

Fortanix Confidential Computing Technology

Fortanix offers the most complete solution for Confidential Computing – providing customers with the fastest and easiest path to protect their applications and data while in use. Fortanix makes it possible to enroll computing resources, in the cloud or on-premises, and deploy existing applications within a secure TEE in minutes. This capability is unique and enables widespread adoption of Confidential Computing with no development or integration costs. And this was the promise that the BeeKeeperAI leadership identified in their initial discussions.

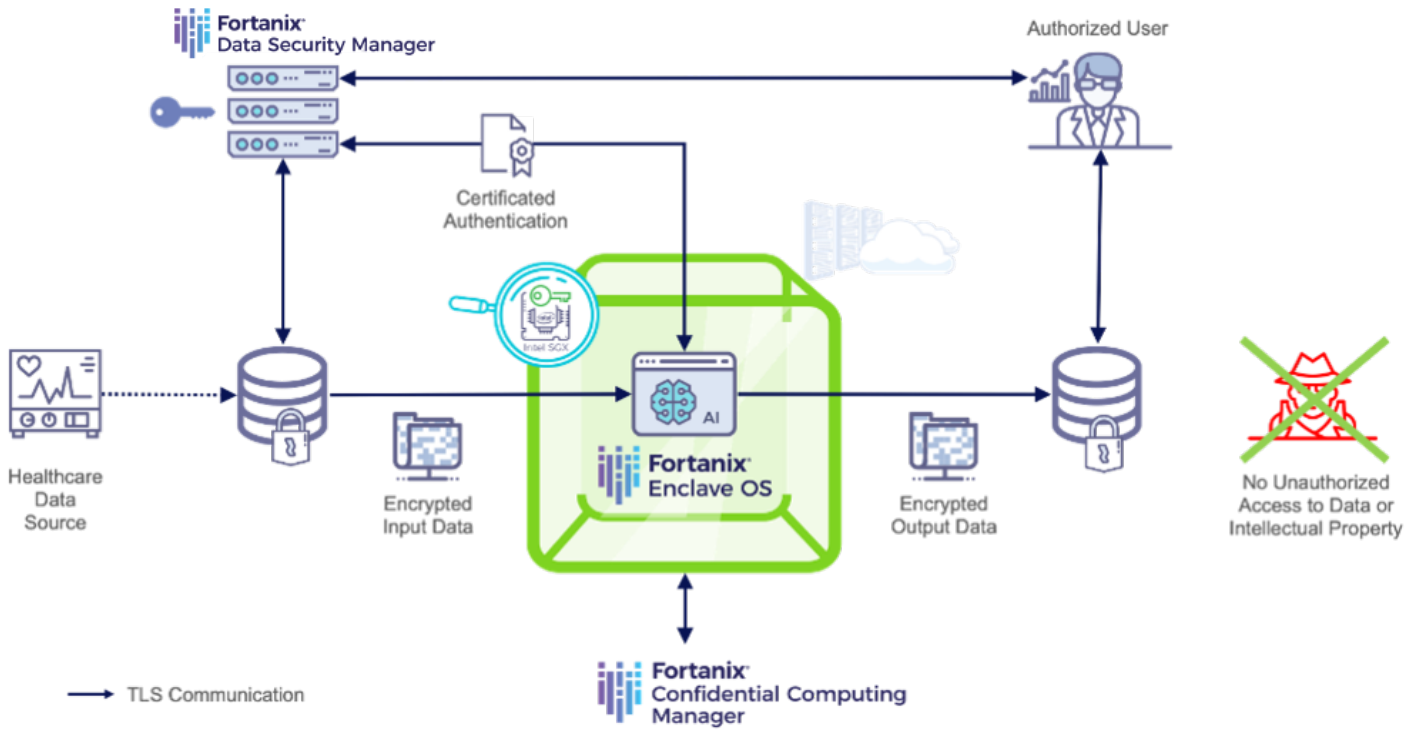
The Confidential Computing technology developed by Fortanix, combined with the data at rest protection offered by Fortanix Data Security Manager, provides healthcare organizations with the ability to protect both electronic private healthcare information (e-PHI) data and the intellectual property contained in AI algorithms, even on untrusted infrastructure. Data stewards can verify the integrity of the consuming AI application using the attestation properties of Intel SGX before sending this data via a TLS pathway to the secure TEE, or "enclave" - with TLS communications terminating inside of the enclave boundary to prevent any exposure of the data outside of this environment.

Since the input data is encrypted at rest, it is necessary for the AI application to decrypt the data prior to processing. Fortanix Confidential Computing Manager automates enclave attestation and provides the application with a certificate that can subsequently be used to authenticate to the Fortanix Data Security Manager. Once authentication is completed, the data encryption key can be used by the AI application to decrypt the sensitive healthcare data for use by the model characterizing the workload. Throughout the runtime of the algorithm, data is always encrypted in memory and only ever processed unencrypted within the enclave. Hence, any attempt to implement a memory scraping attack results in retrieval of encrypted data that retains the protection of the healthcare data required by legal frameworks such as HIPAA and GDPR.

We were introduced to Fortanix by Intel as we were exploring their new processor technologies and the Intel Software Guard Extensions technology. Fortanix had worked very closely with Intel, and they did some matchmaking and said you guys need to get together to drive this concept. Fortanix has been an exceptional partner, leveraging their deep technology roots and a dedicated, focused approach to security. They've developed an understanding of our needs and use cases in healthcare and helped us develop the security technology that supports zero-trust computing within health care

Dr. Michael Blum

An attempt to access the enclave to retrieve data during processing is prevented by the isolation provided by the TEE. Implementing encryption of the results of the AI algorithm, within the boundary of the enclave, before the secure transfer of the output data to disk or to a downstream application, ensures complete end-to-end protection of the healthcare data being processed and the intellectual property within the application code deployed to the enclave. A model workflow employing Fortanix products to provide security for healthcare AI with Confidential Computing is represented in Figure below:



Protection of healthcare AI workflows using Fortanix Confidential Computing technology.

The Impact

BeeKeeperAI is utilizing Fortanix Confidential Computing as its security infrastructure of its collaboration platform which is enabling:

Enhanced protection of and access to real-world datasets for non-biased, generalizable healthcare AI

With Fortanix Confidential Computing technology, healthcare organizations can allay any fears associated with data security or privacy, allowing access to real-world data required to meet the generalizability standard. This helps improve existing models, train new models, deploy novel AI into the clinical setting, and accelerates the development timeline for healthcare AI.

Protection of the intellectual property of algorithm models

With Fortanix, it's become possible to secure intellectual property by publishing the algorithm in a secure enclave that prevents access to code by unauthorized parties of the infrastructure provider.

Reduced the time and cost of AI development and deployment

The technology has steeply reduced the time and cost required to access datasets, thereby allowing organizations to build and deploy AI models faster with higher quality data.

Fortanix brought technology that is incredibly secure, powerful, and functional, and they've adapted when we've asked for new pieces and new API's or to let me start over again. From a technology perspective, Fortanix has been a great partner. They deliver when they say that they're going to deliver. We've been able to rapidly develop new pieces of our technology on the platform. And when we point out specific needs because of the healthcare environment, they're quickly able to adapt to meet the needs of the product.

Dr. Michael Blum

Chief Digital Transformation Officer, UCSF

Fortanix®

About Fortanix

Fortanix® is a data-first multicloud security company solving the challenges of cloud security and privacy. Data is the most precious digital asset of businesses, but this data is spread across clouds, SaaS, applications, storage systems, and data centers. Security teams struggle to track, much less secure it. Fortanix empowers customers to secure all this data with a centralized solution. Its pioneering Confidential Computing technology means data remains protected at-rest, in-motion, and in-use, keeping it secure from even the most sophisticated attacks. For more information, see **www.fortanix.com**

REQUEST A DEMO