anjuna

CASE STUDY

Scalability and Security in the Cloud: Israel Ministry of Defense

Background

Israel's Ministry of Defense (IMOD) is responsible for protecting and securing Israel and its civilians. It provides solutions to tackle Israel's security challenges by strengthening the Israel Defense Forces (IDF), promoting the research and development of advanced technology, encouraging Israel's defense exports, supporting local industries, and promoting social involvement.

Like many other security-conscious organizations, IMOD has been wary of moving data and apps to the public cloud because of security concerns. Yet, the IT team felt the organization was missing out on the scalability and software stack available on the cloud. Without access to the cloud-based scalability and software stack, IMOD could not be as effective as it would like, which in the defense arena, could result in loss of life. IMOD therefore wanted to find a way to securely move many key workloads to cloud-based computing.

Israel Ministry of Defense

Challenges:

Take advantage of cloud scalability and software stack without sacrificing security.

Key Result:

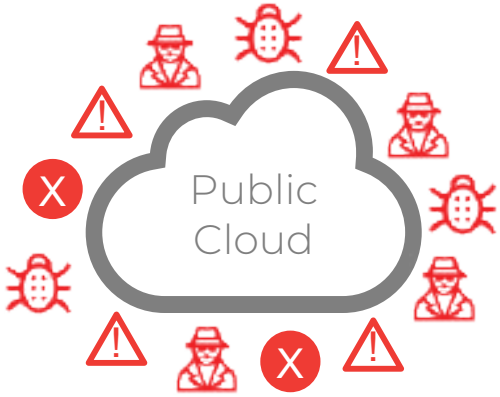
Anjuna® Confidential Computing software allows IMOD to move secure applications to the cloud without recoding or refactoring applications.

Challenges

The IMOD infrastructure group looked at a number of potential security options. Any solution the team evaluated needed to provide the highest level of security possible. However, the review team had additional considerations: The solution had to be available now, run across multiple cloud platforms, and make both moving applications and administration simple.

The group's concerns about cloud security fell into three main areas:

- Insider threats and third parties—This includes not only those insiders with malicious intent, but inadvertent mistakes made by users, developers, and administrators at cloud service providers that could expose data and code.
- Regular hackers—Standard hackers that target a range of organizations.
- Nation states—In addition to the bad actors that attempt to break into systems anywhere in the world, many hackers and nation states target Israel specifically. Some of these groups have near unlimited time and resources to devote to intrusions.



Solution

The cloud infrastructure group decided to use compute-intensive AI workloads as the initial application within a confidential cloud computing environment. Data in use was a key parameter on which they wanted to focus.

Homomorphic encryption looked like a potentially interesting option, but it soon became apparent this was not a practical choice. Not only would this technology not be available in the time frame needed by the IMOD, but homomorphic encryption wouldn't be able to handle all of the use cases needed, and would require enormous compute resources. IMOD could not afford to wait to see whether or not this technology would eventually be proven enterprise-ready.

The group made the decision to go with Anjuna Confidential Computing software for several reasons. First, they wanted a security perimeter that would move with the data—regardless of where that data resides. IMOD understood that the hardware root of trust offered by cloud providers and leveraged by Anjuna would protect their data. In addition, they wanted a flexible technological solution, and Anjuna was the only solution that could protect any application in any cloud—and in the datacenter as well. Because not all applications will migrate to the cloud, IMOD wanted a solution that would also work well in a hybrid cloud environment.

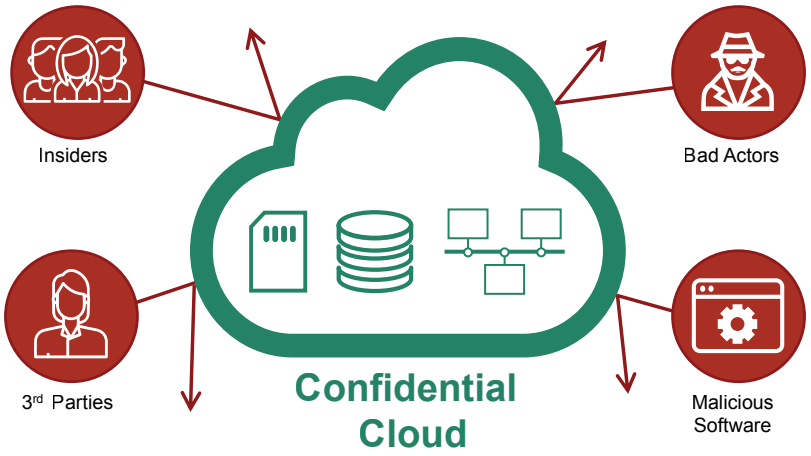
The IMOD team needed to protect extremely large data loads. Because of this, scaling while maintaining performance would be crucial, which is why Kubernetes support was also a factor in the decision. With Anjuna Confidential Computing software, there are no compute and storage limitations, which makes the immense global scale of the cloud available to IMOD for its operations.

The result is a security architecture that protects data by default and compartmentalizes data to those with a need to know. This means employees of cloud providers, system administrators, and third parties no longer have access to sensitive data and are therefore no longer targets for attacks.

Results

IMOD assigned a red team to conduct a thorough evaluation of the proposed solution. As a result of their due diligence, they understood that Anjuna Confidential Computing software could provide the level of security needed to meet the ministry's need.

IMOD can now move secure applications to the cloud more rapidly than with any other alternative. IMOD's cloud infrastructure group leader noted that, "By implementing Confidential Computing, we can make workloads secure without having to recode or refactor applications. We expect this will allow us to move many sensitive apps to the cloud without compromising the high level of security necessary for our operations."



The Bottom Line

The IMOD has a reputation for being one of the most security-conscious groups on the planet, with one of the most highly respected security research teams. Anjuna Confidential Computing software meets their criteria for moving sensitive applications and data to the cloud: It can therefore meet the needs of enterprise IT and security teams as well.

About Anjuna

Anjuna Security makes the public cloud secure for business. Software from Anjuna Security effortlessly enables enterprises to safely run even their most sensitive workloads in the public cloud. Unlike complex perimeter security solutions easily breached by insiders and malicious code, Anjuna leverages the strongest hardware-based secure computing technologies available to make the public cloud the safest computing resource available anywhere. Anjuna is based in Palo Alto, California.

anjuna.io | info@anjuna.io | 650-501-0240