The Next Frontier in Security: Confidential Computing

By Rohit Badlaney, VP of IBM Z Hybrid Cloud & Hillery Hunter, VP & CTO, IBM Cloud

IBM has a long history of providing the highest available levels of security for our clients, as well as a strong heritage of investing in the future of computing to make security features like homomorphic encryption or emerging platforms like quantum computing a reality for clients today.

As we look ahead to the next era of computing, there are lots of predictions and assumptions on what the next great innovation will be – but one thing is indisputable: data and securing that data is and will remain an incredibly important asset to companies and consumers. As our reliance on data grows in the era of hybrid cloud, the need for data privacy becomes even more critical for everyone – and for businesses, an imperative. As part of this, we need to actively invest and innovate in areas that we believe will better prepare us for the future, and better help our clients to protect their highly sensitive data.

For IBM, one key area we're focused on is Confidential Computing – a concept that has moved quickly from research projects into fully deployed offerings across the industry. In order to deliver Confidential Computing, we believe a technology provider must provide protection across the entirety of the compute lifecycle – which includes everything from the build process and key management to the security of data services. Failure to fully protect any of these layers can leave a client's business process exposed.

IBM has been investing in Confidential Computing technologies for over a decade and is on its fourth generation of the technology, delivering on end-to-end Confidential Computing for its clients' cloud computing for more than two years. From IBM's point of view, data protection is only as strong as the weakest link in end-to-end defense – meaning that data protection should be holistic. Companies of all sizes require a dynamic and evolving approach to security focused on the long-term protection of data. Solutions that might rely on operational assurance alone simply do not meet our standards.

IBM first announced our generally-available Confidential cloud computing capabilities in 2018 with the release of IBM Cloud Hyper Protect Services and IBM Cloud Data Shield. The family of IBM Hyper Protect Cloud Services is built with secured enclave technology that integrates hardware and software and leverages the industry's first and only FIPS 140-2 Level 4 certified cloud hardware security module (HSM) to provide end-to-end protection for clients' entire business processes. IBM Cloud Data Shield provides technology that helps developers to seamlessly protect containerized cloud native applications, without needing any code change.

Over the past year, along with several feature enhancements, the services have also helped enterprises meet key compliance requirements relating to whether their data will be secured in the public cloud. This includes GDPR, ISO 27K, IRAP Protected and SOC 2 Type 1 reports. In addition, the devices are HIPAA ready.

Today, IBM delivers production-ready Confidential Computing, to protect data, applications and processes at scale for a broad spectrum of clients. Clients like Daimler and companies including ISVs, and SaaS vendors in fast moving markets like digital asset custody and other financial areas are already working with us to keep

their enterprise-class data protected. We have also brought this same technology to Apple CareKit via the IBM Hyper Protect Software Development Kit (SDK) for iOS available in the Apple CareKit open source GitHub community. This SDK helps developers build healthcare applications that are HIPAA-Ready running on Apple devices with features that address unauthorized party access to their data in the IBM Cloud.

Over the last few months, we have made several announcements showcasing momentum in this area:

- **IBM Cloud for Financial Services:** Built on IBM public cloud, our financial services cloud offering is powered by the same industry-leading Confidential Computing security found in IBM Z. Delivered via IBM Hyper Protect Services, it features 'Keep Your Own Key' encryption capabilities backed by FIPS 140-2 Level 4 certification, making the IBM public cloud the industry's most secure and open public cloud for business.
- **IBM Secure Execution for Linux:** Announced in April 2020, IBM Secure Execution for Linux, is a Trusted Execution Environment enabling clients to isolate large numbers of workloads with granularity and at scale, designed to help protect from internal and external threats across the hybrid cloud. Secure Execution is designed for data integrity protection.
- With IBM z15, clients can gain security advantages to protect data with memory and scale. Announced in September 2019, IBM z15 offers up to 16TB of secured memory.
- Protecting containerized workloads with IBM Cloud Data Shield: With IBM Cloud Data Shield, you can protect the data in your containerized workloads, that run on Kubernetes Service and Red Hat OpenShift clusters, while your data is in use. OpenShift support was introduced this year. Data Shield leverages hardware based secure memory encryption based on Intel SGX technology.
- Open industry leadership and open source with Red Hat: We announced Project Enarx which aims to make it simple to deploy workloads to a variety of Trusted Execution Environments (TEEs) in the public cloud, on your premises or elsewhere. Red Hat is also part of the industry consortium, Confidential Computing Consortium, to drive open standards and approach in this space.
- **Fully Homomorphic Encryption Toolkits:** We are taking innovative steps to protect data in use such as through Fully Homomorphic encryption. In June we announced new toolkits enabling MacOS and iOS developers to experiment with Fully Homomorphic Encryption (FHE) to keep data protected and processed simultaneously. Later this month, we will be announcing a new FHE toolkit for Linux, bringing FHE to multiple Linux distributions for IBM Z and x86 architectures.

With the growing adoption of hybrid cloud environments, Confidential Computing could not be more important. IBM has taken the first step to bring true Confidential Computing to clients, but we can't take our foot off the gas. Now is the time for the industry to follow suit to deliver on the next gold standard for security.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice and represent goals and objectives only.

FIPS 140-2 Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a comprehensive envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

https://newsroom.ibm.com/confidential-computing