IBM Newsroom

IBM Cloud Delivers Quantum-Safe Cryptography and Hyper Protect Crypto Services to Help Protect Data in the Hybrid Era

IBM brings hybrid cloud leadership together with quantum and security research expertise to stay at the forefront of quantum cybersecurity

ARMONK, N.Y., Nov. 30, 2020 /PRNewswire/ -- IBM (NYSE:IBM) today announced a series of cloud services and technologies designed to help clients maintain the highest available level of cryptographic key encryption protection to help protect existing data in the cloud[1] and prepare for future threats that could evolve with advances in quantum computing. Pioneered by IBM Research scientists, the company is now offering quantum-safe cryptography support for key management and application transactions in IBM Cloud®, making it the industry's most holistic quantum-safe cryptography approach to securing data available today.

The new capabilities include:

- **Quantum Safe Cryptography Support**: Through the use of open standards and open source technology, this service enhances the standards used to transmit data between enterprise and Cloud, helping to secure data by using a quantum-safe algorithm.
- **Extended IBM Cloud Hyper Protect Crypto Services**: New capabilities are available to enhance privacy of data in cloud applications, where data sent over the network to cloud applications and sensitive data elements like credit card numbers, are stored in a database that can be encrypted at application-level – supported by the industry's highest level of cryptographic key encryption protection with 'Keep Your Own Key' (KYOK) capability.

"As our reliance on data grows in the era of hybrid cloud and quantum computing capabilities advance, the need for data privacy is becoming even more critical. IBM now offers the most holistic quantum-safe approach to securing data available today and to help enterprises protect existing data and help protect against future threats," said Hillery Hunter, Vice President and Chief Technology Officer, IBM Cloud. "Security and compliance remain front and center for IBM Cloud as we continue to invest in confidential computing and our leading encryption capabilities to help enterprises of all kinds – especially those in highly regulated industries – keep data secured."

Preparing for future threats with Quantum-Safe Cryptography Support

While quantum computing aims to solve complex problems even the world's most powerful supercomputers cannot solve, future fault-tolerant quantum computers could pose potential risks, such as the ability to quickly break encryption algorithms and access sensitive data. To mitigate these risks IBM has developed a clear strategic agenda to help protect the long term security of our platforms and services. This agenda includes the research, development and standardization of core quantum-safe cryptography algorithms as open source tools such as CRYSTALS and OpenQuantumSafe. It also includes the governance, tools and technology to support our clients as they start on the same journey to a more secure future.

Today, as the next step in that agenda, IBM is bringing itsindustry-leading encryption capabilities built by IBM Research cryptographers to help clients with a quantum-safe cryptography approach for their data-in-transit within IBM Cloud. The capabilities are designed to help enterprises prepare for future threats and can be useful against attacks in which malicious actors harvest encrypted data today with the intent to decrypt it later as quantum computing advances.

IBM Key Protect, a cloud-based service that provides lifecycle management for encryption keys that are used in IBM Cloud

services or client-built applications, has now introduced the ability to use a quantum-safe cryptography enabled Transport Layer Security (TLS) connection – helping to protect data during the key lifecycle management.

In addition, IBM Cloud is also introducing quantum-safe cryptography support capabilities to enable application transactions. When cloud native containerized applications run on Red Hat® OpenShift® on IBM Cloud or IBM Cloud Kubernetes Services, secured TLS connections can help application transactions with quantum-safe cryptography support during data-in-transit and protect from potential breaches.

Protecting sensitive data with IBM Cloud Hyper Protect Crypto Services

Enterprises also need to mitigate risks from external and internal threats, as well as to address regulatory compliance.

Today, IBM Cloud is also delivering new capabilities to help secure application transactions and sensitive data using IBM Cloud Hyper Protect Crypto Services, which offer the industry's highest level of cryptographic key encryption protection by providing customers with 'Keep Your Own Key' (KYOK) capability. Built on FIPS-140-2 Level 4-certified hardware – the highest level of security offered by any cloud provider in the industry for cryptographic modules[2] – this allows clients to have exclusive key control, and therefore authority over the data and workloads protected by the keys.

Designed for application transactions where there is a deeper need for more advanced cryptography, IBM Cloud clients can keep their private keys secured within the cloud hardware security module while offloading TLS to IBM Cloud Hyper Protect Crypto Services to help establish a secure connection to the web server. They can also achieve application-level encryption of sensitive data, such as a credit card number, before it gets stored in a database system.

Continuing to address the security demands of clients and highly regulated industries

IBM has been investing in confidential computing technologies for over a decade and today delivers production-ready confidential computing to help clients protect data, applications and processes.

Furthering its commitment to security and compliance, IBM continues to collaborate with its industry peers to make further progress in standardization initiatives. For example, security best practices on IBM Cloud are now available as a Center for Internet Security (CIS) Foundations benchmark for IBM Cloud, and IBM Research cryptographers are key contributors to the QSC algorithms that are short listed in the National Institute of Standards and Technology (NIST).

IBM, the IBM logo, and IBM Cloud are trademarks or registered trademarks of IBM Corp., in the U.S. and/or other countries.

Red Hat® and OpenShift® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

About IBM Cloud

For further information visit: www.ibm.com/cloud/

CONTACT:
Kate Gazzillo
IBM Communications
kate.gazzillo@ibm.com

[1] Encryption keys and cryptographic operations are protected with highest level certified HSM - with Hyper Protect Crypto services: FIPS 140-2 Level 4.

[2] Based on IBM Hyper Protect Crypto Service, the only service in the industry built on FIPS 140-2 Level 4-certified hardware. 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.

SOURCE IBM

---

https://newsroom.ibm.com/2020-11-30-IBM-Cloud-Delivers-Quantum-Safe-Cryptography-and-Hyper-Protect-Crypto-Services-to-Help-Protect-Data-in-the-Hybrid-Era