BioEx Tech Security

July, 2017

A Backbone Built on IBM

BioEx Tech is built on top of IBM's Cloudant platform, allowing us to harness top-tier security features, some of which aren't even available in South Africa. We made this decision to ensure that regardless of client size or budget, data would be safe, segmented, and compliant.

Customer proven

Customers have been using the Cloudant DBaaS in production environments since 2009. Today Cloudant is used as the back-end data layer for hundreds of mission-critical applications in financial services, government, e-commerce, telecommunications, healthcare, and other security-minded industries.

Innovative, Distributed Database Protection

Can you imagine backing up a live, 100-node database cluster that spans multiple data centers? Or how about setting access permissions for specific fields in a NoSQL JSON database? Cloudant automates tough big-data security challenges like these, and continues to lead the way in NoSQL and DBaaS security innovation.

Top-Tier Physical Platforms

The Cloudant DBaaS is physically hosted on Tier-1 cloud infrastructure providers such as IBM (SoftLayer) and Amazon. Therefore your data is protected by the physical and network security measures employed by our hosting partners, including (but not limited to):

- Certifications: Compliance with SSAE16, SOC1, ISAE 3402, ISO 27001, CSA, and other standards
- Identity and access management
- 24/7 physical security of data centers and network operations center monitoring
- Server hardening
- Full-system virus scanning and systems patching

Secure Access Control

There are a multitude of security features built into Cloudant that allow you to control access to data:

- **Authentication –** Cloudant is accessed via a RESTful API; the user is authenticated for every HTTPS or HTTP request Cloudant receives.
- **Authorization –** Grant read, write, admin permissions to specific databases.
- **"In-flight" Encryption –** all access to Cloudant is encrypted via HTTPS. Enterprise customers can use custom SSL certifications.
- **At-rest Encryption –** data stored on disk in Cloudant can be encrypted
- **API Access –** Cloudant is accessed programmatically via a RESTful API over secure HTTP (HTTPS). API keys can be generated via the Cloudant dashboard.
- **Access Logs –** All access to Cloudant is logged for auditing purposes
- **IP Whitelisting –** Cloudant Enterprise customers can whitelist IP addresses to restrict access to only specified servers and users.
- **CORS –** Enable CORS support for specific domains via the Cloudant Dashboard.

Protection Against Data Loss or Corruption

Cloudant has a number of features to help you maintain data quality and availability:

- Redundant and durable data storage – By default Cloudant saves to disk three copies of every document to three different physical nodes in a cluster. This ensures that a working failover copy of your data is always available, regardless of failures.

- Data Replication & Export – You can continuously replicate your databases between clusters in different data centers, or to an on-premise Cloudant Local cluster or Apache CouchDB. Another option is to export data from Cloudant (in JSON or CSV format) to other locations or sources (such as your own data center) for added data redundancy.

- Backup – Cloudant Enterprise users can request that their databases be incrementally backed up to a cluster of their choice to protect against data corruption or deletion. Backup will allow for database restores from a previous time, and document level compare and restore via the Dashboard.

Please feel free to speak to us on info@bioextech.co.za should you have any security questions.

HIPAA

Cloudant Enterprise, when hosted on IBM Softlayer, meets the required IBM controls that are commensurate with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy Rule requirements. These include appropriate administrative, physical, and technical safeguards required of Business Associates in 45 CFR Part 160 and Subparts A and C of Part 164.

International Organization for Standardization (ISO)

ISO certificationCloudant is certified under the International Organization for Standardization (ISO) 27001 standard, which defines the best practices for information security management processes. The ISO 27001 standard specifies the requirements for establishing, implementing, and documenting Information Security Management Systems (ISMS) and the requirements for implementing security controls, according to the needs of individual organizations. The ISO 27000 family of standards incorporates a process of scaling risk and valuation of assets, with the goal of safeguarding the confidentiality, integrity, and availability of the written, oral, and electronic information. Cloudant is audited by a third-party security firm and meets all of the requirements for ISO 27001

SOC 2 Certification

SOC 2 certificationIBM provides SOC 2 reports for Cloudant. These reports evaluate IBM's operational controls with respect to criteria set by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. The Trust Services Principles define adequate control systems and establish industry standards for services providers such as SoftLayer to safeguard their customers' data and information.