Data Security and Privacy

Overview

The security and privacy of our customer data is a top priority at Cyrus. We adhere to state of the art industry practices for security and privacy on the cloud and fully leverage the capabilities of our underlying platform (Google Compute) to secure your data, both when it is stored on a drive, and while it is transferred between your location and the Cyrus cloud instance.

Data Privacy

Your data inside of Cyrus is private to your account. Data of an individual user cannot be viewed by any other user, even within the same customer organization. Cyrus does not have data sharing capabilities - sharing of user data requires you to export it out of Cyrus and import it into another user's account.

Cyrus employees are not allowed to view the contents of your user files or to export them out.

In order to provide technical support, especially for troubleshooting purposes, a specific subset of Cyrus employees may be permitted to access your files directly to transfer them between secure drives within our system. However, even in these cases such Cyrus employees are not permitted to view the contents of your files. Cyrus maintains a list of permitted employees, which can be provided upon request.

In rare instances, permitted employees may have to gain access inside of your data files because you have explicitly requested assistance inside of a Cyrus "session" – these would be separately requested service calls as part of an open service ticket, and not part of normal operations.

Authentication

Cyrus offers two options for authentication.

1. Cyrus integrates with your LDAP/Active Directory authentication system, if your firm uses such authentication internally.
2. Alternatively, if your organization does not use LDAP, the standard secure authorization protocol is the open source OAuth 2.0 standard. Cyrus will adhere to new OAuth standard versions as they become available over time.

Many organizations are offering two-factor authentication to prevent unauthorized intrusion. Cyrus can offer two-factor authentication if required, please notify us if you are interested in this option.

Intellectual Property

We at Cyrus appreciate and respect the value our clients place on their Intellectual Property as a strategic business asset. A common concern is the impact of cloud usage on subsequent patentability of molecules due to the USPTO's rules pertaining to the publication of patentable material. All Cyrus software and databases are entirely self-contained inside Cyrus's private cloud instance. Your data never leaves our network onto any public resource where it could be construed to be "published" with regard to USPTO standards of publication. For example, we run BLAST software internally against internal databases that are frequently updated, and not on the public BLAST servers.

Data Security

Cyrus operates on a cloud infrastructure provided by the Google Cloud Platform (GCP). Standard user accounts operate within the Cyrus network of compute instances, storage instances, and shared networking.

The Google security model is an end-to-end process, built on over 15 years of experience focused on keeping customer data safe on Google applications like Gmail and Google Apps. With Google Cloud Platform your applications and data take advantage of the same security model.

The protection of your data is a primary design consideration for all of Google's infrastructure, products and personnel operations. Their scale of operations and collaboration with the security research community enable Google to address vulnerabilities quickly or prevent them entirely.

We believe that Google can offer a level of protection that very few public cloud providers or private enterprise IT teams can match. Because protecting data is core to their business, Google makes extensive investments in security, resources and expertise at a scale that others cannot. This investment, coupled with Cyrus's strict adherence to these standards, frees you to focus on your business and innovation. Data protection is more than just security. Google's strong contractual commitments enables Cyrus to make sure you maintain control over your data and how it is processed.

Over five million organizations across the globe, including 64 percent of the Fortune 500, trust Google with their most valuable asset: their information. Google will continue to invest in their platform so you can benefit from Cyrus services in a secure and transparent manner.

Encrypting all data in transit and at rest

All communications to servers in Cyrus cloud instance over the open internet (data in motion) are SSL/TLS encrypted to protect data in transit between the Cyrus client running in your browser and servers in our cloud instance.

Files that are not being actively used, or "at rest" (a.k.a. stored on a drive) are encrypted using 256-bit AES server-side encryption. This is done by Google before writing data to disks (https://cloud.google.com/storage/docs/concepts-techniques#encryption).

Data Usage

GCP customers own their data, not Google. The data that you put into our systems is yours. Neither Google nor Cyrus mine customer data to provide advertisements, or sell or share the data with third parties. Google offers their customers a detailed data processing amendment that describes their commitment to protecting customer data. It states that Google will not process data for any purpose other than to fulfill their contractual obligations. Furthermore, if customers delete their data, Google commits to deleting it from their systems within 180 days. Finally, Google provide tools that make it easy for their customers and partners to take their data with them if they choose to stop using their services, without penalty or additional cost imposed by Google.

Learn more about the Google Cloud Platform security model in this in-depth whitepaper: https://cloud.google.com/security/whitepaper