panoply.io

Secure Automated Data Management

Panoply provides end-to-end data management-as-a-service. Its unique self-optimizing architecture utilizes machine learning and natural language processing (NLP) to model and streamline the data journey from source to analysis, reducing the time from data to value to as close as possible to none. The ultimate database administration tool, Panoply eliminates the need to truncate and/or enrich data while providing uncompromised security for customers' sensitive data.

Data Center Security

Panoply utilizes the Amazon cloud's flexible and secure cloud infrastructure to store data logically across multiple AWS cloud regions and availability zones. AWS ensures the highest level of data security and protection, in keeping with industry and government requirements and best practices. AWS infrastructure follows IT security best practices and adheres to leading compliance standards such as: HIPPA, PCI-DSSI, SOC 2, SOC 3, FISMA and FedRAMP.

All data centers that run Panoply's platform are secured and monitored 24/7, and physical access to AWS facilities is strictly limited to select AWS cloud staff. (For more information about AWS secure architecture and compliance certifications, visit: **http://aws.amazon.com/security**.)

SHARED RESPONSIBILITY

As with any AWS cloud-hosted solution, responsibility for security is shared between Panoply and AWS. Amazon is responsible for the security of the AWS cloud, with its data centers and network architecture built to meet the requirements of the most security-sensitive organizations.

Panoply is responsible for managing the servers on the cloud, leveraging AWS services to ensuring the security and integrity of customers' data through a variety of measures such as encryption, access management, and more.

Data Protection

Customers retain control of which security measures they choose to implement to protect their own content, platform, applications, systems and networks – just like they would for applications in an on-site data center.

Panoply is built on top of AWS, and uses the latest security patches and encryption capabilities provided by the underlying platform, such as hardware-accelerated RSA encryption. Panoply uses AWS Hardware encryption for all of the data stored on Redshift and uses AES-256-ctr with **AWS KMS** keys for encrypting all connection details and data source information.

The system employs SSL encryption for data in transit, so customers can securely upload their data to Panoply. Archived data is encrypted and hosted in separate Simple Storage Service (S3) buckets, which are secured via durable AES 256-bit encryption.

ENHANCED PRIVACY

Panoply offers additional layers of security, such as columnar encryption that lets customers encrypt their data, however they can choose, to use private keys (not stored on Panoply's servers), thus giving customers full control over their data. When Panoply's encryption is implemented, the keys are rotated on a daily basis.

Customers may choose to not load all of their data into Panoply by omitting specific columns from the data. This is useful for anonymity in cases where the actual contents of the data are not relevant for analysis (for example, credit card information).

Access Management

Panoply implements **two-step verification**, which requires all users to manually unlock the data using a text message sent to their phone. Customers can also require their colleagues to change their passwords at configurable intervals.

Panoply's permissions model lets customers restrict access to specific tables, views or columns for hierarchical security protocol. Panoply's platform enables customers to set read-only permissions and lock down their data so it can't be exported. To prevent former employees from retaining access to data, user management options include the ability to automatically expire users after a configurable amount of time, requiring manual renewal of their accounts before they can resume access to the data.

Panoply enables customers to audit their company's data access patterns and identify any suspicious activity. Panoply does not have access to any of its clients' raw data or encryption keys.

Test and Risk Assessment

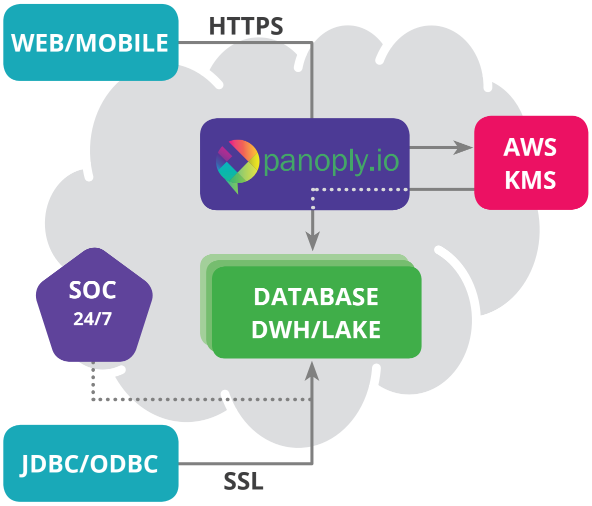
Security is a top priority in the implementation of all R&D processes, across all system layers, from the physical layers up to the application layer. Strict development processes, coding standards, and a rigorous testing platform ensure adherence to industry-standard, best practices for security. In addition, Panoply's testing protocol includes code reviews and tests for quality assurance.
As part of Panoply's ongoing risk assessment process, our security professionals meet with the R&D leaders on a monthly basis to review risk assessments, system security configurations, and policies. In addition, the teams discuss and review new projects and their potential impact on security.

Network Security

Panoply takes every precaution to ensure that every layer involved in data transfer is secured by best-of-breed technologies. The company's network is segmented using AWS security groups, VPCs, ACLs, and additional custom measures. In addition, our security operations center (SOC) is kept up to date with security alerts that are analyzed and addressed in real-time.

Access to the Panoply systems are monitored, logged, and analyzed 24x7. Anomaly detection is used to identify strange connections to data, for example, someone running a query from a new computer, or a different country than usual. Customers may choose to completely block these queries or manually approve them.

Panoply ensures end-to-end encrypted security of data and access



panoply.io

Our Office Locations

TEL AVIV
Isserles, 22
67014 Tel Aviv, Israel

+972 54 977 7862

SAN FRANCISCO
1161 Mission St.
San Francisco, CA 94103

+1 415 233 2811

@panoplyio | panoply.io