Data Security at Catalyst

Our Infrastructure

All Catalyst Services operate on Microsoft Azure servers that comply with strict international standards. These standards include ISO 27001, ISO 9001, ISO 27017, ISO 27018, C5, Cyber Essentials Plus, DOD DISA L2,L4,L5, FedRAMP, FIPS 140-2, PCI DSS, SEC 17-a-4, SOC 1,2 and 3.

Access to infrastructure at Catalyst is securely controlled via VPN. Access to critical third-party software providers used by Catalyst are limited to senior level employees only and protected by 2-factor authentication.

Data is stored in the EU or US (depending our customer's request) on Microsoft Azure servers and is continuously backed up. Our datacenters are protected by physical access controls, intrusion and fire detection systems and 24/7 professional security staff.

Connections to Catalyst Services are encrypted using 256-bit SSL with integrity assured by the SHA2 ECDSA algorithm.

Monitoring

We have continuous resource and infrastructure access monitoring in operation 24/7, 365 days a year. Any alerts generated by our monitoring system are sent to senior team members immediately and actioned.

Data Isolation and Protection

All customer data is protected with unique security credentials at each level of transit including data upload, file storage, web application, data processing, and database. Each customer's data is stored in separate dedicated databases to ensure complete isolation of your data. All customer data is backed up every night and stored for thirty days. Production databases maintain point-in-time transaction logs for restoration between scheduled backups.

Data Privacy

Our servers on Microsoft Azure comply with applicable EU data protection laws and the incorporates the Article 29 Working Party Model Clauses. You can find more information here

Also see our Privacy Policy for more information.

Additional Security Options

By default, Catalyst offers leading data security technologies and procedures. However, should customers wish to enhance this further, we offer additional security options. These include:

- IP whitelisting
- On-premise deployments

Vulnerability Reporting

If you have discovered a security concern, please email us at security@getcatalyst.in. We'll work with you to make sure that we understand the scope of the issue, and that we fully address your concern. We consider correspondence sent to security@getcatalyst.in our highest priority, and work to address any issues that arise as quickly as possible.

Please act in good faith towards our users' privacy and data during your disclosure. We won't take legal action against you or administrative action against your account if you act accordingly: White-hat researchers are always appreciated.