Security Overview

Protecting client data is a top priority at Catalyst. In over 18 years of operation, we have been consulted and have in turn provided legal technology services for thousands of clients and have hosted terabytes of data on behalf of some of the largest companies and law firms in the world—without a single instance of a security compromise or incident that put our client or their data at risk. We engage a reputable security company to conduct regular penetration, vulnerability and application security examinations.

We employ effective security standards at every layer of our business as our solution requires security measures be taken at every level of our application including the end-user-level in order to adequately safeguard our clients' data.

SOC 2 Compliant

Catalyst completes an annual SOC2 audit conducted by Coalfire Systems. The auditor's report is available upon request.

Physical Location

Catalyst's production systems are located at five top-tier colocation facilities. Three of the facilities are in the United States and two are in Japan to serve offshore clients.

Catalyst offices are secured using a combination of employee key card and video cameras at each entrance. Visitors and vendors are required to sign in.

Similar to one of our U.S. colocation facilities.

Data Center Operations and Security

Catalyst chooses colocation facilities that are Tier 3 or better, guaranteeing at least 99.982% availability. All are SOC2 compliant, using the NIST or ISO frameworks.

In addition, all of our facilities meet or exceed these specifications:

- Round-the-clock security. Facilities are staffed 24x7x365 with locked private cages and access verification.
- Video monitoring of all entrances and throughout the building, with surveillance recordings stored digitally for 30 days.
- Uninterruptible power. At least two power grid connections, battery banks, and N+1 diesel generators are covered by fuel delivery contracts.
- Multiple load-balanced HVAC systems that keep the climate at the optimum temperature and humidity levels.
- Fire detection and suppression. FM200 non-halon fire suppression systems.
- System monitoring. Systems are monitored by staff of both Catalyst and our colocation facilities.

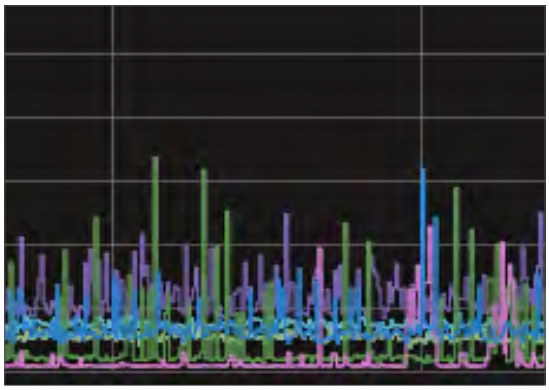
With regard to connectivity, all of our sites are carrier neutral and have access to multiple telecommunication companies. Catalyst contracts with multiple carriers for bandwidth.

Within our data centers, only electronically badged Catalyst employees have direct, physical access to our systems. Employees of the colocation facility have no access to our cabinets, servers or data unless authorized by us to provide services.

Infrastructure Monitoring

Catalyst monitors all of the infrastructure, including servers, switches, applications and services. Currently, we monitor over 1,500 devices and more than 20,000 services.

The monitoring software can respond to events by implementing corrective actions in addition to the baseline communication updates.



Catalyst has a dedicated team that monitors tens of thousands of endpoints.

System Interconnectivity

All Catalyst colocation facilities in the U.S. are interconnected via private, redundant ethernet connections.

System Security

Catalyst routinely applies vendor patches across all devices and makes use of baseline security scanning to ensure that all devices are in the preferred configuration. Catalyst employs external security teams to evaluate the application and delivery platform.

Application Security

Catalyst's first line of defense is limiting the protocols through which clients can connect with our systems and infrastructure. For example, Catalyst's applications allow access through our firewall (HTTPS), and application servers for those products will only respond to an SSL-encrypted HTTP call. Documents can only be accessed from our dedicated object storage network through an "auth ticket," which provides unique, time-limited credentials to access the document but nothing beyond.

Catalyst offers optional two-factor security to clients who wish to have an additional layer of security. With two-factor security, the user is prompted to supply an additional token for authentication, as a supplement to name and password.

Data Handling

Delivery: For delivering data to Catalyst in bulk, clients can choose from a number of secure delivery methods:

- **FTPS:** Catalyst offers FTP with enhanced security known as FTPes or FTPS. The servers use SSL to encrypt the transport. To use FTPes, make sure your FTP client supports this option.
- **SCP:** Catalyst also offers SCP for clients that prefer this means of encrypting a transport.
- **Physical Drives**: We accept delivery by hard drives or other magnetic media but recommend they be encrypted using TrueCrypt-encrypted data volumes or an equivalent alternative.

Return: Upon request, Catalyst will return data to clients. The data can be transferred via our network delivery or by encrypted hard drive.

Access to Client Data

Catalyst conforms to the principles of least privilege. Only employees with a justified business purpose are granted access to data.

Employee and Contractor Security Policies

All Catalyst employees and contractors are background checked and required to accept and sign our standard nondisclosure and confidentiality agreements before being given system access. If an employee or contractor is found to have violated the agreement, we take appropriate disciplinary and legal measures, up to and including dismissal and prosecution.

In addition, Catalyst employees are required to follow our comprehensive suite of Security Policies, which govern confidentiality, computer systems, access, protection of data and more. Our Media Handling Policies and Procedures govern handling and recording data.

Privacy Shield Framework

Catalyst has committed to handling data coming from EU countries in accordance with the EU and Swiss Privacy Shield Framework. Catalyst is registered with the International Trade Administration (ITA) within the U.S. Department of Commerce. Catalyst's privacy policy and Privacy Shield provisions can be read here.

Please contact us to learn more.