Catalyst Security Overview

Security is a top priority at Catalyst. In our 15 years in operation, we have hosted thousands of matters on behalf of some of the largest companies and law firms in the world without a single security compromise or incident. In September 2013, a third-party security assessment concluded that the Catalyst Insight system was free from any known security vulnerabilities.

Our Data Center Locations

Catalyst’s production servers are located in secure cages at four colocation facilities. Three of the facilities are in the United States and one is in Japan to serve our Asia clients.

The three U.S. facilities are all located in the greater Denver area, near Catalyst’s corporate headquarters. Two are operated by ViaWest and one by Latisys. The Japan facility is operated by Equinix.

Data Center Operations and Physical Security

All of our colocation facilities are Tier 3 or higher data centers guaranteeing at least 99.982% availability. All are SOC 1/SSAE 16/ISAE 3402 Type II or SAS 70 Type II certified. In addition, all of our facilities meet or exceed these specifications:

- Round-the-clock security. Facilities 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 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 connections with at least six different telecommunication companies. Although Catalyst purchases secondary and tertiary Internet connectivity from our colocation vendors, our primary connectivity in Colorado is directly to Level 3 Communications.
Our physical installations at these facilities include 44 rack-mount server cabinets and 1,400 physical and virtual servers. More than 40 servers are dedicated entirely to servicing the incoming application requests from our clients.

Within our data centers, only electronically badged Catalyst employees and authorized, escorted Catalyst guests 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 uses Nagios to monitor our IT infrastructure, including servers, switches, applications and services. Using Nagios, Catalyst systems engineers and developers create tests that are run against the subsystems of network devices and servers to check on their operating status and detect potential problems. Currently, we monitor over 1,100 hosts devices and more than 19,000 individual services.

In the event that a subsystem responds out of spec, Nagios performs a predefined action. Actions can include taking corrective action, sending out an email notification, or paging an individual or group of individuals. Additionally, Nagios records the operating status information through these tests so that changes in behavior or performance trends can be identified.

We monitor all of our systems using Symantec intrusion detection and intrusion prevention software. This includes real-time file-integrity monitoring to identify changes to files and real-time configuration monitoring to identify policy violations, suspicious administrators and intruder activity.

System Interconnectivity and Disaster Recovery

All Catalyst colocation facilities in the U.S. are interconnected via private redundant gigabit Ethernet connections. High availability is achieved through redundancy for all network devices and server nodes. Our Japan data center is connected by an Internet Protocol Security (IPsec) tunnel across the Internet to our U.S. facilities.

For the purpose of disaster recovery (DR), all client data for Catalyst CR (case configuration, documents and associated metadata) is replicated and/or backed up between colocation facilities.
Application Security

Catalyst’s first line of defense is limiting the protocols through which clients can connect with our systems and infrastructure. For instance, Catalyst’s applications (Insight, CR, XE and custom applications) allow access only through our firewall on port 443 (HTTPS). The application servers for these products are configured to respond only on port 443 and only to an SSL-encrypted HTTP call. Our SSL certificates are signed by a publically recognized certificate authority and are signed with a minimum 1024-bit encryption.

Data Delivery

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

- Secure FTP (FTPE) using a minimum 1024-bit encrypted certificate signed by a publicly recognized certificate authority
- Secure Copy (SCP/SFTP) using a client-supplied certificate for encrypted communications
- Hard drive with TrueCrypt-encrypted data volumes

Our FTP, FTPE and SCP/SFTP servers receive the files and hand them off to automation.
Access to Client Data

Only Catalyst employees have access to client data and that access is on a need-to-know basis. Many of our key employees have been with us for well over a decade and many of our “newcomers” have been with us for at least five years.

Employees of our data centers generally have no access to our servers or data unless authorized by Catalyst to provide remote-hands services. Any such physical access is restricted to the servers and does not include login access to the data.

U.S.-EU Safe Harbor Certified

Catalyst has committed to handling data coming from EU countries in accordance with the Safe Harbor Principles and is registered with the U.S. Department of Commerce as a member of the Safe Harbor network. Catalyst's Safe Harbor certification can be found by clicking on this link. Our privacy policy can be read here.

Employee and Contractor Security Policies

All Catalyst employees and contractors are required to accept and sign our standard nondisclosure and confidentiality agreement when they are hired. If an employee or contractor is found to have violated the agreement, we take appropriate disciplinary measures, up to and including dismissal.

In addition, Catalyst employees are required to follow our Information Security Policy, which governs confidentiality, computer systems and protection of data, and our Media Handling Policies and Procedure, which governs handling and recording data.

Catalyst offices are secured using a combination of employee ID key card access with pin code and video cameras at each entrance.

System Reliability

Apart from regularly scheduled maintenance, our site rarely experiences downtime. Our goal is to limit application unavailability due to causes within our control to less than one consecutive hour in any calendar month (other than during scheduled maintenance windows). On average over an annual basis, our infrastructure uptime exceeds 99.9 percent.

Return or Destruction of Client Data

Unless otherwise requested, Catalyst maintains file archives for 60 days. Before we delete any archives, clients are contacted to arrange for the return or destruction of those files. Original media received from the
client is returned or stored (in lieu of the Catalyst copy) as may be directed by the client. If the client desires destruction of original media, Catalyst uses industry-standard methods for erasing data. A proof of destruction certificate will be issued to clients.

**Third-Party Security Audits and Certifications**

In 2013, Catalyst Insight underwent a rigorous IT security and risk assessment performed by Blue Lava Consulting, a specialist in global compliance and IT risk assessment. Blue Lava concluded that Catalyst had taken the necessary steps to protect intellectual property and client information and that the Catalyst application was free from any known security vulnerabilities.

Catalyst's original security schema was designed by the chief security officer of AIG as a prerequisite to hosting the company’s confidential case and claim data. Subsequently, our security was inspected and approved by a security team from American Express (which hired an ethical hacker as part of the process), and it has since been reviewed and approved by a number of major corporations in fields such as insurance, finance and technology.

As a prerequisite to our hosting classified data relating to a major terrorist trial, the U.S. Department of Justice conducted an extended examination of our security systems and procedures and approved them in a report to the U.S. district judge in charge of the case. We have been approved to host data in several federal criminal cases, including one in which the presiding judge entered public findings regarding our security and ordered the Bureau of Prisons to allow a prisoner direct access to our repositories.

Please [contact us](#) to learn more.