

Service Security Overview

Reliability, Protection, Secure Access



- ✓ **99% or better service availability**
- ✓ **Industry standard secure SSL data encryption**
- ✓ **Multi-level account permissions and access control**

Mindjet Catalyst® is a cloud-based service that helps users visually connect ideas, information and people to increase efficiency, team communication and collaboration. Catalyst is easily accessed from MindManager® or through a web browser anytime, anywhere.

We built Catalyst with service reliability and security in mind. Mindjet has successfully completed a SAS 70 Type II compliance audit for Catalyst, which means that an independent auditing firm has validated that Mindjet has the processes and safeguards in place to protect the assets and data entrusted to our systems.

Reliability and Protection

- **Protected Colocation Facility** – Mindjet Catalyst is hosted by Savvis®, Inc., a global leader in cloud infrastructure and hosted IT solutions for enterprises. Savvis has nearly 2,500 unique clients, including 33 of the top 100 companies in the Fortune 500. Savvis also conducts SAS 70 Type II audits on its colocation facility.
- **Data Security Measures** – Mindjet has a formal InfoSec policy dictating the handling of customer data. Access to the DB systems is restricted to a small subset of Operations staff. All data is encrypted in transit.
- **Secure Document Sharing** – Catalyst uses 128-bit SSL 3.0 TLS 1.0 communication to help protect all files shared on the Catalyst service. Once stored in Catalyst, your company's data is sandboxed within Catalyst and scanned at upload time with multiple industry-leading anti-virus software packages. Real-time collaboration sessions are protected with the same SSL security as document collaboration.
- **User Authentication** – Users are authenticated via a centralized LDAP-style directory around which Catalyst is designed.
- **Strong Password Support** – Catalyst supports the use of strong passwords selected by individual team members, which are stored in an encrypted fashion on the Catalyst service. Mindjet employees have no access to passwords once encrypted.
- **Session-Based Transaction Protection** - Individual user sessions are identified and re-verified with each transaction, using a unique token created at each user sign in. Sessions will time out after a period of inactivity to help prevent unauthorized access.
- **Service and Data Protection Measures** – Catalyst is protected 24x7x365 by multiple firewall mechanisms, virus scanning software and is continuously monitored by security experts. Mindjet has implemented full redundancy of all system components including load-balanced hardware, power, and Internet connectivity and uses RAID storage technology to help maintain high levels of data protection and service reliability.

- **N+1 Redundancy and Environmental Controls** – The Catalyst data center facilities have multiple HVAC units with high volume, zoned temperature control systems, multiple UPS (Uninterruptible Power Source) systems, generators and short notice diesel refueling available should power outages occur. Environmental controls that help protect our data center include fire suppression devices and seismic isolation equipment.
- **Intrusion Detection** – Catalyst deploys IDS systems to monitor and detect potential attacks.
- **Scheduled Off-Site Backups** – Data stored in the Catalyst service is backed up at daily, weekly and quarterly intervals and stored in a secure Iron Mountain® location off-site to help ensure service reliability and integrity.
- **Incident Response Processes** – Mindjet has instituted Major Incident (MI) and RCA (Root Cause Analysis) processes.

Permissions and Privacy

- **Multi-Level Account Permissions** – Account owners determine access to Catalyst accounts, with each account invitation tied to specific users you control. Owners determine which users can create workspaces. Owners can suspend account membership and user privileges at any time, making data previously shared inaccessible.
- **Private, Team, and Inter-Company Workspace Support** – Workspaces can be configured as private document repositories, invisible to other team members, or set up as team workspaces where multiple users can collaborate and work interactively. Workspace ownership and management can be shared among multiple users to facilitate collaboration.
- **Multi-Level Access Control** – Each workspace supports unique access control lists, clearly identifying which users have the ability to manage the workspace and its users, which members have the ability to edit and upload files, and which team members have read-only permission.
- **Account Data and Privacy Protections** – Mindjet Catalyst is PCI-compliant when protecting account owner credit card data.
- **Data Separation** - Catalyst is built with a granular security model that enforces the ability of customers to restrict access to their data stored in our SaaS environment. No one customer can view the data of another.

