Service Security Overview

Mindjet: Reliability, Protection, Secure Access

Multi-level account permissions and access control

The Mindjet web app is a cloud-based service that helps groups visualize their best ideas and plans, securely manage and share files, get teams on the same page and access information anywhere, at any time.

Forrester®'s Rob Koplowitz indicated in his 2011 report that 43% of information workers work from multiple locations over the course of a month, and that 42% work outside of the corporate firewall. Work is decentralized, moving faster and likely to keep changing at a rapid pace to keep up with the similarly frenetic pace of change in communications, business and technology. The Mindjet web app addresses the needs of this changing workforce.

We built the Mindjet web app with service reliability and security in mind. Mindjet has successfully completed a SAS 70 Type II compliance audit for Mindjet Catalyst (the predecessor to the Mindjet web app), and is pursuing the new SOC2 standard for the Mindjet web app, which is the replacement for SAS 70. For SOC 2, this means that an independent auditing firm will validate that the Mindjet web app has the processes and safeguards in place to provide users a high level of assurance that Mindjet's data center is secure, highly available and operating under a consistent set of high integrity processes.

Reliability and Protection

Protected Colocation Facility

The Mindjet web app infrastructure is hosted at market leading, world class data center providers. These providers sustain high service level agreements, extreme power densities, and military grade security including biometrics and regulatory compliance.

Data Security Measures

The Mindjet web app 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

The Mindjet web app uses 128-bit SSL 3.0 TLS 1.0 communication to help protect all files shared on the Mindjet service. 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 the Mindjet web app is designed.

Strong Password Support

The Mindjet web app supports the use of strong passwords selected by individual team members, which are stored in an encrypted fashion on the Mindjet service. Mindjet employees have no access to passwords once encrypted.

Reliability and Protection

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

The Mindjet web app is protected 24x7x365 by multiple firewall mechanisms, and is continuously monitored by security experts. Mindjet has implemented full redundancy of all system components including load balanced and clustered hardware, power, and Internet connectivity, and uses redundant storage technology to help maintain high levels of data protection and service reliability.

N+1 Redundancy and Environmental Controls

The Mindjet web app data center facilities have multiple HVAC units with high volume, zoned temperature control systems, multiple UPS (Uninterruptible Power Supply) 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

The Mindjet web app deploys IDS systems to monitor and detect potential attacks.

Scheduled Off-Site Backups

Data stored in the Mindjet web app service is backed up at a location off-site to help ensure service reliability and integrity.

Incident Response Processes

Mindjet implements Major Incident (MI) and RCA (Root Cause Analysis) processes.

Permissions and Privacy

Multi-Level Account Permissions

Specific account roles determine access to the Mindjet web app items. Owners and administrators determine which users can create folders or files, and can suspend account membership and user privileges at any time, making data previously shared inaccessible.

Private, Team, and Inter-Company Support

Folders and files can be configured for private access invisible to other team members, or set up as team assets where multiple users can collaborate and work interactively. Folder or file ownership and management can be shared among multiple users.

Multi-Level Access Control

Account type, roles in the account, and object permission levels determine access control. Each folder and file supports unique access control lists, clearly identifying which users have the ability to manage individual objects and its users.

Account Data and Privacy Protections

The Mindjet web app is PCI-Compliant when protecting account owner credit card data.

Data Separation

The Mindjet web app is built with a granular user authorization model that enforces the ability of customers to restrict access to their data stored in our SaaS environment. Documents and data are partitioned by account to prevent unauthorized access in a secure multi-tenant infrastructure.