

Autodesk® Buzzsaw® Security Overview

Introduction

Autodesk Buzzsaw is designed to help safeguard customers' data—while giving them the business benefits of collaboration. Providing a secure data environment is at the core of what Autodesk Buzzsaw does.

Offering industry-leading levels of performance and availability, Autodesk Buzzsaw is at the forefront of a growing trend of providing software as a service (SaaS). In fact, Gartner Group predicts that by 2010, 30 percent of new software will be delivered by the SaaS model (December 2005). Many organizations choose Autodesk Buzzsaw recognizing that its proven on-demand infrastructure provides high levels of security—often keeping their data more secure than it is within their own companies.

Making security a top priority, Autodesk has built an infrastructure for Autodesk Buzzsaw that includes the following features:

- A fault tolerant environment with no single point of failure
- Replicated storage for customer data in geographic locations more than 6,000 miles apart
- Comprehensive protection to help prevent unauthorized user access

Supported by a team of security experts dedicated to providing 24x7 data and systems protection, Autodesk Buzzsaw deploys only proven, best-of-breed security technologies.



Security Architecture

With a proven security model, the Autodesk Buzzsaw architecture helps assure the highest degree of protection for customer data. The “defense-in-depth”, or layered, approach to security developed by Autodesk employs the following technologies and configurations:

Physical Security

Physical access to the data center facility is strictly controlled. Security precautions include a 24-hour onsite security presence, surveillance monitoring of the facility, and biometric access and exit scans.

Communication Security

All data passed between the user's client and Autodesk Buzzsaw systems is encrypted with industry standard Secure Sockets Layer (SSL) technology. By encrypting data and authenticating certificate owners, Autodesk helps ensure that each communication session between the client and the Autodesk Buzzsaw application is secure.

Perimeter Security

Autodesk Buzzsaw utilizes security best practices at the perimeter network to filter out unnecessary and potentially harmful traffic. Multiple layers of firewalls strictly control access to Autodesk Buzzsaw's network from the Internet as well as from Autodesk's management networks. Additionally, network intrusion systems monitor both external and internal traffic and report on possible attack attempts.

System Security

Autodesk tightly controls and limits administrative access to a small group of specialized personnel on the Autodesk operations team. Customers own their data; Autodesk does not view customer data. Autodesk employees only access customer data to perform backups, system maintenance, and security monitoring. Autodesk maintains all systems at current vendor recommended patch levels and configures all systems using recognized security best practices.

Application Security

A user name and password combination—encrypted using SSL during transmission—strictly controls user login to Autodesk Buzzsaw. In addition, site administrators can enforce complex password rules and other configurable security features in accordance with their organizations' security policies.

Auditing

To help maintain the highest levels of security at all times, Autodesk performs regular audits. Security logs are regularly reviewed to identify possible attacks.

All equipment undergoes assessment, promoting best practice adherence. In addition, Autodesk regularly solicits independent, third-party security assessments of both the Autodesk Buzzsaw infrastructure and application.

High Availability

Autodesk Buzzsaw customers expect their data to be available when they need it. The Autodesk Buzzsaw architecture helps achieve this customer requirement, taking advantage of redundancy at every level. There are no single points of possible failure in the architecture.

Data Center Capabilities

Environmental and physical safeguards at our data centers include multiple independent power grids, full UPS protection, backup generators, and redundant HVAC units. Autodesk sources Internet bandwidth from multiple providers via redundant circuits, so that if one network goes down, impact to our customers' business is minimized.

Disaster Recovery and Business Continuation

Even in the midst of a disaster, Autodesk customers expect to continue normal business operations. Autodesk protects customer data by geographically separating Autodesk data centers by more than 6,000 miles.

To protect customer data in the event of a disaster, Autodesk's business continuance data center houses an exact duplicate of the primary data center infrastructure. This helps ensure that all data entered into Autodesk's systems

before an event-triggered disaster will be available after activation of business continuance procedures.

In addition, all software as well as network, server, and data storage equipment has been implemented in a fault tolerant configuration. As a result, Autodesk Buzzsaw can restore service rapidly after a disaster.

Monitoring and Operational Practices

To provide high levels of system and data availability, Autodesk employs a comprehensive set of system monitors and operational practices. Thanks to proper monitoring and practices, Autodesk can predict problems, correcting them before users are impacted or service is interrupted.

The Autodesk operations team follows industry best practices for operational routines and procedures, including incident management, problem management, change management, configuration management, and release management.

For More Information

Further detailed information on the security measures employed by the operations team for Autodesk Buzzsaw is available upon request. Please call 866-815-3501 (415-356-0700 outside the United States) or send e-mail to bcs.sales@autodesk.com. A non-disclosure agreement will be required to receive detailed information.

Disclaimer: While we have made every effort to provide accurate information, none of the statements or information in this document shall be construed as a warranty or guarantee. We disclaim all warranties, express or implied, with respect to this Security Overview, including but not limited to, warranties of merchantability, fitness for a particular purpose or non-infringement, and any warranty concerning the accuracy, timeliness or completeness of the information contained herein. We reserve the right to change, revise, enhance or discontinue the products, programs or services described in this Systems Security Overview at any time without notice.

The contents of this Security Overview do not constitute a contract. This Security Overview is provided for informational purposes only, and does not include the conditions, limitations and exclusions that apply to our services. Only a signed agreement setting forth the precise terms and conditions of service constitutes a contract.

Autodesk and Buzzsaw are trademarks or registered trademarks of Autodesk, Inc., in the USA and/or other countries. All other brand names, product names, or trademarks belong to their respective holders.

© 2007 Autodesk, Inc. All rights reserved.