Autodesk® Cloud documents

Security White Paper

November 3, 2011

Autodesk Cloud documents

Autodesk® Cloud delivers a broad range of web-based features, products, and services. This white paper specifically addresses the security of the Autodesk Cloud documents service.

This paper explains how security is an integral component of the Autodesk Cloud documents service and how Autodesk addresses information security, physical security, and operational security pertaining to the service. The policies described in this paper are in effect as of the time of authorship. Some specific details may change over time as we release new service features and enhancements.

Organizational Security

Autodesk employs a full-time Information Security team responsible for Autodesk Cloud documents and other services. The team members are experts in information, application, and network security. This team is responsible for maintaining the defense systems, developing security review processes, and building a customized security infrastructure for the Autodesk Cloud documents service. It also has a key role in the development, documentation, and implementation of Autodesk's SaaS Operations security policies and standards.

Employee Lifecycle

Autodesk has established formal policies and procedures to delineate the minimum standards for logical access to the Autodesk Cloud documents platform and infrastructure hosts. Autodesk maintains policies requiring Autodesk SaaS Operations staff with potential direct access to customer data to undergo a background check. The policies also identify functional responsibilities for the administration of logical access and security.

Key Architecture Design Points for Autodesk® Cloud documents

Compute Cloud

Autodesk® Cloud documents leverages services from recognized and dependable third-party cloud infrastructure providers. These services, characterized by redundant computing environments and dynamic resource allocation, enable customers to access their data virtually anytime and anywhere from Internet-capable devices. Our third party providers' compute environments allow CPU, memory and storage resources to be shared and utilized by many customers, while also offering security benefits.

Shared Responsibility Environment

Moving IT infrastructure to third-party service providers creates a shared responsibility model between Autodesk SaaS Operations and our third-party providers. Our providers operate, manage and control the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. Autodesk SaaS Operations maintains the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the third-party provided security group firewall for Autodesk Cloud documents. Autodesk SaaS Operations takes additional measures to enhance security and/or meet more stringent compliance requirements by leveraging technology, such as host-based firewalls, host-based intrusion detection/prevention, encryption and key management.

Security Group Firewalls

Our third-party providers use firewall settings where application-specific instances are protected by one or more security groups, named sets of rules that specify which ingress (i.e., incoming) network traffic should be delivered to the instance. Security groups give basic firewall-like protection for running instances. Similar instance types are grouped and a security group rule set is developed based on the perceived functionality of the group of instances.

Host-Based Firewalls

Our third-party infrastructure provider instances are further protected by a host-based firewall. Using this firewall allows the definition of rule sets, which are named lists of rules that are searched sequentially until a rule is found that terminates the search. The rule sets are defined on a per-instance basis and are dictated by the functionality of the instance.

Security Patch Management

Security Patch management is an integral part of operations and is necessary to provide systems that are immune to known vulnerabilities. Autodesk SaaS Operations utilizes a centralized patch collection repository for Autodesk Cloud documents to manage the distribution and installation of security patches. The patches are first installed in the staging environment. Post successful validation, the patches are rolled on to the production environments.

Logging Management

Autodesk Cloud documents servers are configured to log locally as well forward the logs to a centralized logging server. The logs are sent in real time and over an encrypted channel.

Monitoring

Autodesk SaaS Operations security monitoring program for Autodesk Cloud documents is focused on information gathered from server-specific traffic, employee actions on systems, and outside knowledge of vulnerabilities.

Security for Autodesk Cloud documents is monitored with the aid of centralized monitoring, correlation, and analysis systems that proactively manage the large amount of information generated by devices within the environment, providing pertinent and timely monitoring and alerts.

Incident Management

Autodesk SaaS Operations maintains an incident management process for security events that may affect the confidentiality, integrity, or availability of Autodesk Cloud documents systems or data managed by the Autodesk SaaS Operations team. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation.

Key Autodesk SaaS Operations staff members are trained in forensics and in handling evidence in preparation for an event, including the use of third-party and proprietary tools.

Operating System Security

Autodesk SaaS Operations production servers for Autodesk Cloud documents are based on a stripped and hardened version of server operating systems that have been customized to include only the components necessary to run Autodesk® Cloud documents, such as those services required to administer the system and deliver user traffic. The system is designed for Autodesk SaaS Operations to be able to maintain control over the entire software stack and to help provide a secure application environment.

Using a robust change management system for Autodesk Cloud documents to provide a centralized mechanism for registering, approving, and tracking changes that impact all systems, Autodesk SaaS Operations minimizes the risks associated with making unauthorized modifications to the standard Autodesk SaaS Operations OS templates.

Physical and Environmental Security

Our third-party providers have many years of experience in designing, constructing, and operating large-scale data centers. These data centers are housed in non-descript facilities. Physical access is strictly controlled both at the

perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Regulatory Compliance

Autodesk SaaS Operations endeavors to obtain industry-leading certifications and outside assessments on an ongoing basis. Autodesk has initiated the process to obtain a SSAE 16 SOC2/SOC3 attestation for its background operations and will continue to seek similar attestation for specific Autodesk Cloud services in an ongoing basis. A SSAE 16 SOC2/SOC3 audit is an independent assessment by an outside audit firm that validates the subject company's adherence to its defined controls and confirms that these controls are operating effectively. When complete, the audit firm provides a report that details the company's compliance with these controls.

Independent Security Assessment

In addition, Autodesk SaaS Operations has obtained an independent security assessment for its background operations. This report includes external and internal network penetration testing and vulnerability assessment of the control environment and is conducted by an independent security organization annually.

For more information about Autodesk® Cloud documents or other services, please visit www.autodesk.com/cloud