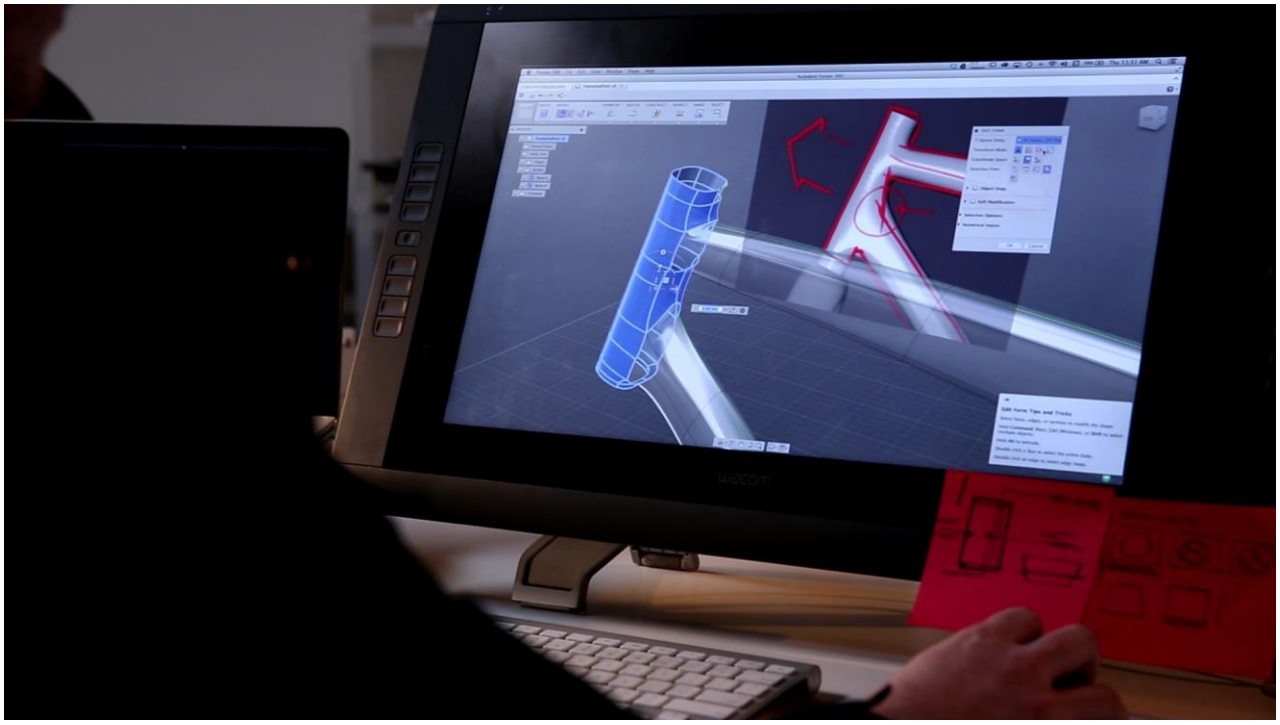
Autodesk Fusion 360 Security Whitepaper



Published: August 2015

For the most current information, please visit the Autodesk Trust Center at:

http://www.autodesk.com/trust/overview

Contents

Introduction

The Autodesk® Fusion 360™ service is a cloud based 3D CAD/CAM tool for product development that combines industrial and mechanical design, collaboration, and machining in a single package. Autodesk Fusion 360 tools enable fast and easy exploration of design ideas with a secure and integrated concept-to-production toolset that extends to include web browsers and mobile devices through Autodesk's cloud computing platform.

To keep customer information highly available, Autodesk Fusion 360 runs on a scalable infrastructure that enables the service to remain responsive as demand increases.

Document Purpose

The purpose of this document is to explain Autodesk Fusion 360 operations, the software development process and security measures.

Autodesk Fusion 360 Engineering

The Autodesk Fusion 360 Engineering team is responsible for designing, implementing, and testing the Autodesk Fusion 360 client side software and the cloud services application provided in the cloud.

The design, coding, testing, and maintenance of the Autodesk Fusion 360 application is based on an agile software development process. During the design sprints, detailed design documents are produced and reviewed by architects to assess functionality and scalability of the design. During implementation sprints, peer code reviews by software engineers and architects are conducted to detect deviations from Autodesk Fusion 360 application development practices. All code produced during the process includes functional unit testing and no user story is complete until quality assurance personnel has verified the acceptance criteria. Performance testing of Autodesk Fusion 360 is also integrated into the development lifecycle. The team conducts load tests throughout the development sprints to identify changes that negatively affect performance as early as possible in the process.

Autodesk Fusion 360 Product Security

Autodesk Fusion 360 has built-in security features that range from its communication with the cloud services, to product level security/collaboration features that the users can control.

Communications Security

All communication between Autodesk Fusion 360 client software and cloud services requires secure HTTPS connections.

Encryption & Ciphers

Communication between Autodesk Fusion 360 and backend services and within the backend services is over the encrypted channel to provide communication security.

Authentication

Credentials, consisting of an Autodesk ID, user ID and password, are required to access Autodesk Fusion 360. Credentials are secured during network transmission and stored only as a salted hash generated by the SHA-2 cryptographic hash function.

Data Security

All Autodesk Fusion 360 designs are saved in the cloud on encrypted storage. The storage solution uses 256-bit Advanced Encryption Standard (AES-256) to encrypt data.

Locally, cached designs rely on the Operating System user level permissions for access control.

Design Item Versioning

For every item, Autodesk Fusion 360 maintains a version history. Versioning protects the integrity of data by allowing changes to be rolled back by promoting earlier versions, and provides an auditable list containing information about each file modification.

Hub and Group based Collaboration Security

Projects provide a simple basis for granting or limiting access to Autodesk Fusion 360 designs for a set of collaborators. Invitations to projects are approved by the owner or moderator of the project, thereby allowing strict control over invitees inviting further invitees.

Companies can opt for Team hubs, which allow the company to exercise ownership & access control to all projects created by members. Project privacy settings like open, closed & secret projects allow for controlled collaboration. In Team Hubs, members can choose to add collaborators only to invited projects. These collaborators can only access the projects that they are invited to. Team hubs also allow the company hub admin to deactivate accounts of ex-employees & transfer project ownership to other members of the team.

Public Sharing

Public sharing is a way to collaborate with an outside stakeholder who does not have an Autodesk ID or Fusion 360 entitlement. The user can create a link which provides read only access to the design, and optionally provide download/export access via this link. Further, at any time, the user can revoke the public sharing offered by this link.

Cloud Operations

Autodesk's Cloud Operations team is responsible for defining and executing procedures for application release management, hardware and operating system upgrades, system health monitoring, and other activities required for the maintenance of Autodesk Fusion 360.

High Availability

Autodesk Fusion 360 is designed to achieve a high level of availability by employing redundant systems in its supporting infrastructure and distributing load across a scalable fleet of instances.

Data Replication

Replication of customer data is performed between data centers in different locations. Replication limits the possibility of data loss or a delay in service resumption if fail-over to a backup data center is required.

Data Center Redundancy

Similar physical infrastructure is maintained in different data centers to provide protection against events such as data center failure.

Power System Redundancy

Redundant electrical power systems are installed in data centers to maintain operations 24 hours a day, 7 days a week. Uninterruptible Power Supplies (UPSs) automatically provide backup to primary electrical systems in the event of a failure. Generators at each data center provide long-term backup power if an outage occurs.

Internet Connectivity Redundancy

A redundant multi-vendor system is used to maintain Internet connectivity to each of the data centers.

The Autodesk Fusion 360 client software also has an offline mode to allow users to continue to access and work on local copies of their design when they are not connected to the internet.

Physical Infrastructure Security

The Autodesk Fusion 360 application runs in secure data centers that are protected from unauthorized physical access and environmental hazards by a range of security controls.

Facilities Access Control

Data centers are guarded 24 hours a day, 7 days a week by professional physical security staff. The perimeter of each data center, as well as rooms that contain computing and support equipment are protected by video surveillance. Video surveillance is preserved on digital media that allows recent activity to be viewed on demand. Data center entrances are guarded by mantraps that restrict access to a single person at a time. All visitors and contractors must present identification to be admitted and are escorted by authorized personnel at all times. Only employees with a legitimate business need are provided with data center access and all visits are logged electronically.

Fire Prevention

Fire detection and suppression systems, such as smoke alarms and heat-activated wet pipes, are installed throughout each data center to guard rooms containing computing equipment and support systems. Fire detection sensors are installed in the ceiling and underneath a raised floor.

Climate Controls

Data center climate controls protect servers, routers, and other equipment subject to failure if strict environmental ranges are violated. Monitoring by both systems and personnel is in place to prevent dangerous conditions, such as overheating, from occurring. Adjustments that keep temperature and other environmental measurements within acceptable ranges are made automatically by control systems.

Operations Incident Management

Autodesk has an incident management policy, which defines best practices for driving incident resolution. The Autodesk incident management policy emphasizes logging of remediation steps and the use of root cause analysis to build a knowledge base of actionable procedures. The goal of the Autodesk incident management policy is not only to quickly and effectively close incidents, but also to collect and distribute incident information so that processes are continuously improved and future responses are driven by accumulated knowledge.

Patch Management

Where possible, automation is in place to check for new patches and prepare deployment lists that can be approved by authorized Cloud Operations personnel. Patching policy also defines criteria for determining the impact of a patch on systems stability. If a patch is identified as having a possibly high impact, regression testing is completed before the patch is deployed. Change Management tracks deployment of patches to production systems.

Change Management

The Cloud Operations team has a change management policy which includes the following activities:

- Requiring the submission of a Request For Change (RFC) form, that includes the name of the change initiator, the change priority, the business justification for the change, and a requested change implementation date.
- Cloud Operations team creates detailed back out plans prior to deployment so that system state can be restored if a change causes a service disruption. Back out plans include executable instructions defined in scripts that restore system state with a minimum of manual steps.
- Defining maintenance windows. Scheduled, emergency, and extended maintenance windows are specified by the Cloud Operations team and regularly planned maintenance is scheduled during off-peak hours.

- Defining tests to verify that functionality is accessible after the deployment of a change.
- Once deployment is complete, the Cloud Operations and Autodesk Fusion 360 QA team execute the tests to check that functionality identified as at-risk remains available.

Capacity Management

Because customer access to cloud services is provisioned on-demand through a self-service model, traffic patterns are highly variable and subject to usage spikes. When a spike occurs, the availability of a service can be negatively impacted if the pool of computing resources powering the service is exhausted. To maintain a high level of availability, the Cloud Operations team implements a capacity management policy. These practices include:

- Frequent recording of resource use – Autodesk Fusion 360 resource use is collected at frequent intervals across a range of infrastructure components, including virtual instances, virtual storage volumes, and virtual network devices. Usage statistics are stored in a capacity management repository.
- Building a capacity plan documenting current resource use and forecasting future requirements - the capacity management repository is used by the Cloud Operations team to generate a detailed capacity plan that documents current levels of use and models future levels based on statistical analysis and the impact of upcoming enhancements to business functionality. The capacity plan is updated as needed or if significant changes to usage patterns are detected.

Autodesk Fusion 360 Operational Controls

Autodesk Fusion 360 provides protection of sensitive customer data from unauthorized access.

- **Physical restrictions to data centers** – Physical restrictions to data centers prevent unauthorized parties from accessing the hardware and support systems used by Autodesk Fusion 360.
- **Background checks** – Background checks are required for employees with physical access to the computing resources and support systems used by Autodesk Fusion 360.
- **Data replication** – Data replication copies customer data across redundant data centers so that business continuity can be maintained if a fail-over between facilities occurs.
- **Redundant technologies** - Redundant technologies such as load balancers and clustered databases limit single points of failure.

Cloud Security

The Cloud Security team is a dedicated group of information security specialists focused on identifying and enforcing security within the Autodesk Fusion 360 cloud environment.

The Cloud Security team's responsibilities include:

- Reviewing the security of cloud infrastructure design and implementation.
- Defining and ensuring implementation of security policies including identity and access management, password management and vulnerability management.
- Driving compliance with established security procedures by conducting internal reviews and audits.
- Identifying and implementing technologies that secure customer information
- Engaging third-party security experts to conduct information security assessments
- Monitoring cloud services for possible security issues and responding to incidents as needed
- Conducting annual reviews of security policy.

Vulnerability Scans and Penetration Testing

The Cloud Security team conducts scans and penetration testing of Autodesk Fusion 360 services. Security scans and penetration-testing cover a wide range of vulnerabilities defined by the Open Web Application Security Project (OWASP) and SANS top 25.

Network Security

Network security is enforced using a combination of physical and logical controls, including encryption, firewalls, and systems hardening procedures. Stand-alone hardware firewalls are deployed at the perimeter of the cloud. All ports except those required to serve customer requests are blocked.

Encryption

Network traffic containing sensitive information, such as credentials, application session information, access tokens and user profiles, is transmitted securely over the Internet to the perimeter of our environment.

Security Standards and Attestations

Autodesk Fusion 360 security controls will be reviewed by an independent auditor and listed in AT Section 101 SOC 2 audit report in the future.

Resources

The following resources provide general information about Autodesk and other topics referenced in the main section of this document.

- Autodesk - To view information about Autodesk, visit http://www.autodesk.com.
- Autodesk Trust Center - To view information about Autodesk Trust Center, visit http://trust.autodesk.com.
- Autodesk Fusion 360 – To view information about Autodesk Fusion 360 service, please visit http://fusion360.autodesk.com