Autodesk® Fusion 360 Security Whitepaper

September 25, 2018

Contents

Introduction

Autodesk® Fusion 360™ is the first 3D CAD, CAM, and CAE tool of its kind. It connects your entire product development process in a single cloud-based platform that works on both Mac and PC. The Fusion 360 tools enable fast and easy exploration of design ideas with a secure and integrated concept-to-fabrication toolset that extends to include web browsers and mobile devices.

Document Purpose and Scope

The purpose of this document is to explain Autodesk Fusion 360 operations, the software development process, and security measures implemented in the environment. In this document Autodesk Fusion 360 refers to both the Fusion 360 client software and the Fusion 360 browser access software.

Fusion 360 Engineering

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

The design, coding, testing, and maintenance of Fusion 360 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, software engineers and architects conduct peer code reviews to detect deviations from 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 verify the acceptance and Definition of Done criteria. Performance testing of Fusion 360 is also integrated into the development

lifecycle. The Fusion 360 team conducts load tests throughout the development sprints to identify changes that negatively affect performance as early as possible in the process.

Employee Training

All Autodesk employees must affirm the importance of information security as part of new-hire orientation. Employees are required to read, understand, and take a training course on the company's Code of Conduct. The code requires every employee to conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors.

Autodesk employees are required to follow the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. New employees must sign a confidentiality agreement. New employee orientation emphasizes the confidentiality and privacy of customer data.

To implement security best practices, Autodesk has introduced a yearly Software Security Certification Program (SSCP) for everyone in the Engineering & Cloud Infrastructure functions.

Fusion 360 Product Security

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

Communications Security

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

Encryption & Ciphers

Communication between Fusion 360 and backend services and within the backend services is over an encrypted channel.

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.

Fusion 360 provides end users with the option to use multi-factor authentication when logging in. Users who opt to enable this feature can use their authorized secure personal device (e.g. cell phone) to receive a code to use in conjunction with their password.

Data Security

All 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 Versioning

For every design, Autodesk Fusion 360 maintains a version history. Versioning protects the integrity of data by allowing users to roll back to earlier versions and providing 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, assuring strict control over members granting access to new users.

Companies can opt for Team Hubs, which allow them to exercise ownership and access control to all projects created by members. Project privacy settings, such as open, closed, and secret projects, allow for controlled collaboration. With Team Hubs, members can choose to restrict access to collaborators who have been invited to the project. Team Hubs also allows customer administrators to deactivate accounts of ex-employees and transfer project ownership to other members on the team.

Public Sharing

With Public Sharing, users can collaborate with outside stakeholders who do not have an Autodesk ID or Fusion 360 entitlement. Fusion 360 users create a link that provides read-only access to the design. Users also have the option to enable download/export features. At any time, the user can revoke the public sharing offered by this link.

Cloud Infrastructure

The Cloud Infrastructure team is responsible for defining and executing procedures for application release management, hardware and operating system upgrades, system's 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 and Redundancy

Replication of customer data is performed between Amazon Web Services (AWS) Availability Zones (AZs) . Replication limits the possibility of data loss or a delay in service resumption if fail-over to a backup data center is required.

Power System Redundancy

AWS data centers contain redundant electrical power systems 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 on AWS secure data centers that are protected from unauthorized physical access and environmental hazards by a range of security controls. Some physical and environmental controls are summarized below. A full overview of AWS Security Processes is available at https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

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 that 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

The Cloud Infrastructure team has a patch management policy that helps ensure effective patch deployment. Where possible, automation is in place to check for new patches and prepare deployment lists that can be approved by authorized Cloud Infrastructure personnel. The 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 Infrastructure team has a change management policy which includes the following activities:

- **Request For Change (RFC) from.** An RFC form must be submitted for all changes. The form includes the name of the change initiator, the change priority, the business justification for the change, and a requested change implementation date.
- **Backout plans.** The Cloud Infrastructure team creates detailed back out plans prior to deployment so that system state can be restored if a change causes a service disruption. Backout plans include executable instructions defined in scripts that restore system state with a minimum of manual steps.
- **Defined maintenance windows.** The Cloud Infrastructure team specifies scheduled, emergency, and extended maintenance windows. They schedule planned maintenance during off-peak hours.
- **Test plan.** The Cloud Infrastructure team defines a set of tests to verify that functionality is accessible after the deployment of a change.
- **Test execution.** Once deployment is complete, the Cloud Infrastructure 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 Infrastructure 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.

- **Capacity planning.** The Cloud Infrastructure team uses capacity management 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.
- **Resource allocation.** Computational resources are allocated as customers request them. Pre-warmed computation resources are always available. If a spike of activity occurs, new resources are instantiated. For example, availability for Autodesk Fusion browser resources is usually achieved in less than 10 minutes.
- **Activity monitoring.** Activity dashboards and alerts are defined across the backend services, allowing engineers to observe the system activity and to execute post incident examinations and analysis.

Alerts and Monitoring

In order to provide the shortest possible Mean Time to Remediation, Autodesk uses automated systems to monitor Fusion 360, validating the health state of the service. Each single component, from the database to the services, are individually monitored. In the case of an event impacting the service, alerts are generated, and the Cloud Infrastructure team is notified through an escalation process.

The service health also describes the interrelation between Autodesk services. A service like Autodesk Fusion 360 is highly sensitive to the ACM service (Access Control). Each service has to be resilient when a dependent service fails and should gracefully fail when it can no longer operate without any data loss for the customer.

The state of the Fusion 360 service is publicly displayed by Autodesk's Health Dashboard Service: https://health.autodesk.com.

Zero Downtime during Deployments

As patches are applied to the production environment, a Blue-Green deployment approach is taken for Autodesk Fusion browser and other Fusion 360 services. This helps to ensure that customers do not experience any downtime of the service.

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 failover between facilities occurs.
- **Redundant technologies**. Redundant technologies such as load balancers and clustered databases limit single points of failure.

Autodesk Security

The Autodesk Security team is a dedicated group of information security specialists focused on identifying and enforcing security practices within the Autodesk cloud environment. The Autodesk Security team's responsibilities include:

- Reviewing the security posture of Autodesk's 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 Autodesk's security policy.

Vulnerability Scans and Penetration Testing

Fusion 360 services undergo an annual penetration test and regular scans for security threats and vulnerabilities. The application also undergoes static analysis and third-party library scans. 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. Additionally, AWS provides network security controls that protect their physical data centers. For more information, see their security whitepaper: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

Encryption

All network traffic is encrypted when transmitted over the Internet to the perimeter of the Autodesk cloud environment. Sensitive information, such as credentials, application session information, access tokens and user profiles, is encrypted at rest.

Privacy

Autodesk is transparent on how customers' personal data is collected and used. Read the Autodesk Privacy Statement to learn more.

Resources

The following resources provide general information about Autodesk and other topics referenced in the main section o 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 Fusion 360, please visit http://fusion360.autodesk.com