Autodesk® BIM 360® Security Whitepaper

March 2018

AUTODESK

Table of Contents

Introduction

Autodesk® BIM 360® is a cloud-based construction project management platform designed to improve performance across a project's lifecycle. As a secure, cloud-based product, Autodesk BIM 360 offers the benefits of collaboration in the construction space while safeguarding customer data. The BIM 360 application is designed and built using best-in-class cloud software practices and powered by Amazon Web Services (AWS), the world's leader in cloud infrastructure. We have designed our services to be scalable and secure, thus providing our customers with a resilient and safe application. We know our customers' business is relying on us and we take that responsibility seriously.

Document Purpose and Scope

The purpose of this document is to outline Autodesk BIM 360 operations, software development, and security measures implemented in the environment. The scope of this whitepaper is limited to the following BIM 360 applications and services:

- BIM 360 Documents Management (Docs)
- BIM 360 Field Management (a.k.a. Next Generation Field)
- BIM 360 Model Coordination (a.k.a. Next Generation Glue®)
- BIM 360 Project Management and BIM 360 Insight

Cloud Operations

The 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 BIM 360.

High Availability

Our commitment to high availability enables customers to enjoy the full power of BIM 360.-To achieve high availability, BIM 360 employs redundant systems in its supporting infrastructure and distributes the load across a scalable fleet of instances. The Autodesk BIM 360 system consists of several web/application servers, background job processing systems, report execution systems, and data stores and file storage. These services are spread across a pair of AWS Availability Zones (AZ). Each AZ is an independent data center within a territory, so the use of multiple AZs shields BIM 360 applications from outages. To ensure a high level of service, the BIM 360 service targets availability of over 99.5%.

Business Continuity & Data Center Redundancy

Autodesk has a Business Continuity Plan and a disaster recovery process that relies on AWS Availability Zones (AZ). To support the process, BIM 360 is deployed across a pair of AWS Availability Zones (AZ). Each AZ is in a separate data center, and data is replicated between them.

Power System Redundancy

To maintain 24/7 operations, redundant electrical power systems are installed in data centers. In te event of a failure, an uninterruptible power supply (UPS) automatically provides backup to primary electrical systems. Generators at each data center provide long-term backup power if an outage occurs.

Internet Connectivity Redundancy

Autodesk BIM 360 uses a redundant, multi-vendor system to maintain Internet connectivity to each of the data centers.

Data Replication

Customer data is replicated between data centers in separate locations. Replication prevents the possibility of data loss or delay in service if failover to a backup data center is required.

Physical Infrastructure Security

BIM 360 applications run in secure data centers powered by Amazon AWS. The data centers are protected from unauthorized physical access and environmental hazards by a range of security controls.

- **Facilities access control.** Data centers are guarded 24/7 by professional physical security staff. Data center entrances are guarded by mantraps that restrict access to a single person at a time. Only employees with a legitimate business need are provided with data center access and all visits are logged electronically. All visitors and contractors must present identification to be admitted and are escorted by authorized personnel at all times.
- **Video surveillance.** The perimeter of each data center and rooms that contain computing and support equipment are protected by video surveillance. Video surveillance is preserved on digital media so that recent activity can be viewed on demand.
- **Fire prevention.** Fire detection and suppression systems, such as smoke alarms and heat-activated wet pipes, are installed throughout each data center to protect rooms that contain 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 that may be subject to failure if strict environmental ranges are violated. Monitoring is in place by both systems and personnel to prevent dangerous conditions, such as overheating, from occurring. Control systems automatically adjust temperature and other environmental measurements to keep then within acceptable ranges.

Operations Incident Management

BIM 360 has an incident management policy that defines best practices for driving incident resolution. The policy is guided by the Information Technology Infrastructure Library (ITIL) Version 3 framework. The BIM 360 incident management policy emphasizes logging incident remediation steps and performing root cause analysis to build a knowledge base of actionable procedures. The goal of the 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. Please visit the Autodesk Trust Center for more details.

Patch Management

The Cloud Operations 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 are approved by authorized Cloud Operations personnel. The BIM 360 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, Cloud Operations personnel complete thorough regression testing before deploying the patch. The Change Management team tracks the deployment of patches to production systems.

Change Management

The Cloud Operations team has a change management policy, which includes the following processes and procedures:

- **Request For Change (RFC) form**. 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 Operations team creates detailed backout plans prior to deploying a change so that they can restore system state if a change causes a service disruption. Backout plans include executable instructions, defined in scripts, that restore system state with minimal manual steps.
- **Defined maintenance windows**. The Cloud Operations team specifies scheduled,

emergency, and extended maintenance windows. They schedule planned maintenance during off-peak hours.

- **Test plan**. The Cloud Operations 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 Operations and Product QA teams execute the tests to check that at-risk functionality 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 has implemented a capacity management policy. As part of the capacity management policy, BIM 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.

Performance and Scalability

To provide a high level of availability, performance and load tests are executed throughout the software development lifecycle.

BIM 360 Operational Security Controls

BIM 360 has several security controls that protect 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 BIM 360.

- **Background checks.** Background checks are required for employees before they are granted access to the computing resources and support systems used by BIM 360.
- **Test execution**. Once deployment is complete, the Cloud Operations and Product QA teams execute tests to check that functionality identified as at-risk remains available.
- **Administrative functionality.** BIM 360 administrative tools provide a flexible way for administrators to manage users, role-based permissions, and other access controls for end users.
- **Redundant technologies.** Redundant technologies such as load balancers and clustered databases limit single points of failure.

BIM 360 Engineering

The BIM 360 Engineering team is responsible for designing, implementing, and testing the BIM 360 application. The design, coding, testing, and maintenance of BIM 360 is based on a software development process that includes security processes as needed.

During the design stage, detailed design documents of user stories are produced and are reviewed by architects to assess functionality and scalability of the design. The design phase uses a joint application design process where architects and software engineers assess the functionality, scalability, and performance characteristics of the user stories.

During implementation, engineers and architects conduct peer code reviews in order to detect deviations from BIM 360 application development practices.

All code produced during the process includes unit testing, integration, and QA verification. No user story is complete until quality assurance personnel verify the acceptance criteria.

As part of the development lifecycle, BIM 360's performance team conducts load tests throughout the development sprints to catch changes that negatively affect performance as early in the process as possible.

Employee Training

All Autodesk employees must affirm the importance of information security as part of new-hire orientation. Additionally, 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, we have introduced a yearly security training program for all BIM 360 engineers.

BIM 360 Product Security Controls

Autodesk BIM 360 has built-in security features that allow customers to create detailed identity and access management policies. Customer administrators and users can use BIM 360's security tools to manage ownership of their workspace items and set sharing permissions on their reports.

Authentication and Encryption in Transit

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

Data Security

All BIM 360 customer uploaded files are stored in the cloud on encrypted storage. The storage solution uses 256-bit advanced encryption (AES-256).

Administrative Controls

BIM 360 provides customer administrators with security features for creating identity and access management policies.

- **Provisioning user**s: Administrators can create and deactivate users.
- **Using role-based security**: BIM 360 roles allow administrators to customize access control levels, to provide fine grained controls to restrict access. A role is a collection of permissions to data and functionality that relate to a job function.

  By providing a flexible way of assigning permissions-based on roles, BIM 360 adheres to the principle of least privilege, which requires that each user's access to data and functionality be limited to what they need to complete their assigned tasks.

User Controls

Users can control access to the items, reports, and files they own with exception to administrative restrictions. Users can also use file versioning to restore previous versions of files they have attached to workspace items.

Identity Federation Standards

BIM 360 supports Single Sign On (SSO) with customer systems for all users.

Cloud Security

Our dedicated Cloud Security team is focused on identifying and enforcing security within the Autodesk BIM 360 cloud environment. The 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 security assessments as needed.
- Monitoring cloud services for possible security issues and responding to incidents as needed.

Vulnerability Scans, Penetration Testing, and External Audits

The Cloud Security team conducts regular security scans and penetration testing of BIM 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 (physical or logical), and hardening procedures. Stand-alone hardware firewalls are deployed at the perimeter of the cloud at our data centers. All ports are blocked, except those required to serve customer requests.

Encryption

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

Security Standards and Compliance

- Autodesk BIM 360 has selected industry standard – SSAE-16 AT 101 SOC 2 attestation to validate our security posture.

- Autodesk BIM 360 is ISO 27001, ISO 27017 and ISO 27018 certified.

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 additional information on topics referenced in this document.

- To learn more about Autodesk, please visit: http://www.autodesk.com.
- For more information on our comprehensive security framework, please visit: https://www.autodesk.com/trust/security.
- BIM 360 applications are hosted in AWS. As such, security and infrastructure are a shared responsibility between Autodesk and Amazon. For more information about Amazon security, please review the Amazon Security Whitepaper.

The information contained in this document represents the current view of Autodesk, Inc. as of the date of publication, and Autodesk assumes no responsibility for updating this information. Autodesk occasionally makes improvements and other changes to its products or services, so the information within applies only to the version of Autodesk BIM 360 offered as of the date of publication.

This whitepaper is for informational purposes only. Autodesk makes no warranties, express or implied, in this document, and the information in this whitepaper does not create any binding obligation or commitment on the part of Autodesk.

Without limiting or modifying the foregoing, Autodesk BIM 360 services are provided subject to the applicable terms of service located at http://www.autodesk.com/company/legal-notices-trademarks/terms-of-service-autodesk360-web-services.