BIM 360 and Cloud Security

Prabhu Gunasekaran
Autodesk

Thandavan Boobalan
Autodesk

Learning Objectives

- Data encryption, privacy, and access control
- Physical data center security
- Disaster recovery
- Vulnerability scans, penetration testing, external audits, and two-factor authentication.

Description

The BIM 360 cloud-based design and construction project management platform is designed to improve performance across a project’s lifecycle. Confidentiality, integrity, and availability of customer data is vital to business operations. We know our customers’ businesses are relying on us and we take that responsibility seriously. But how?

Speaker(s)

Prabhu Gunasekaran (Technical Specialist, Autodesk) works to bring every person on every team, in the construction industry, closer together, to help them win in the future of connected construction. A Civil & Structural Engineer, with over 8 years of experience in the Engineering Procurement & Construction Industry, working in multiple project execution teams, driving them towards technology adoption and digital transformation.

Thandavan Boobalan (Technical Specialist, Autodesk) carries 9 years of Experience in Pre-sales, Training & Technical Support on BIM for MEP Products, and our manufacturing product portfolio. In his earlier assignments he worked as BIM Implementation Engineer & BIM Coordinator for projects across Middle East region.
Data Encryption, Privacy & Access Control

BIM 360 is designed with privacy in mind. All files uploaded to BIM 360 are stored in the cloud on encrypted storage. The storage solution uses the 256-bit advanced encryption (AES-256). Network traffic containing sensitive information, such as credentials and session tokens, is transmitted securely encrypted using Transfer Layer Security (TLS) encryption technology.

Authentication & Encryption
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. Communication between clients and backend services is over the encrypted channel to provide communication security. The services are scanned regularly by industry-leading tools to ensure that they continue to meet the highest standards. The services support TLS v1.2 connections with secure cipher suites.

All BIM 360 customer uploaded files are stored in the cloud on encrypted storage. The storage solution uses 256-bit advanced encryption (AES-256), one of the strongest block ciphers available. The entire encryption, key management, and decryption process is inspected and verified internally on a regular basis as part of our existing audit process. A small amount of metadata containing project attributes such as filenames, are stored unencrypted to facilitate searching of projects and other management operations.

Administrative Controls
BIM 360 provides customer administrators with security features for creating identity and access management policies.
- Provisioning Users
- Using role-based security

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. BIM 360 also supports two-factor authentication to add a second level of authentication to a user account during login.

Privacy
Autodesk is transparent on how customers’ personal data is collected and used. Read the Autodesk Privacy Statement to learn more. You can also reference the Privacy section of the Autodesk Trust Center.
Physical Data Center Security

All data is stored in secured data centers powered by Amazon Web Services. The data centers are protected from unauthorized physical access and environmental hazards by a range of security controls.

Facilities access control
AWS 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 always escorted by authorized personnel.

Video surveillance
The perimeter of each AWS 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 AWS 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
AWS 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 them within acceptable ranges.

Disaster Recovery

Autodesk has a Business Continuity Plan and a disaster recovery process that relies on AWS Availability Zones (AZ). Autodesk BIM 360 services are spread across multiple AWS regions and 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.

Each AWS AZ is in a separate data center, and data is replicated between them. Replication prevents the possibility of data loss or delay in service if failover to a backup data center is required. As part of deployment across multiple AWS AZs, redundant electrical power systems are installed to maintain 24/7 operations, with uninterrupted power supply (UPS) and generators for long-term backup power if an outage occurs. A redundant, multi-vendor system is used to maintain Internet connectivity to each of AWS’s data centers.
Cloud Security

Vulnerability Scans, Penetration Testing & External Audits
Autodesk’s dedicated Cloud Security team conducts regular security scans, penetration testing and external audits 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 Autodesk’s cloud environment. All ports are blocked, except those required to serve customer requests.

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 modules and services are ISO 27001, ISO 27017 and ISO 27018 certified.

For more information on the latest attestation status of BIM 360 and related services, please review the “Compliance” section on Autodesk Trust Center.