AUTODESK

White paper sulla sicurezza di Autodesk® Fusion 360

Ottobre 2022

Sommario

1. INTRODUZIONE 2

1.1 SCOPO E AMBITO DEL DOCUMENTO 2

2. SICUREZZA DI AUTODESK 2

3. PROGETTAZIONE DI FUSION 360 3

3.1 FORMAZIONE DEI DIPENDENTI 4

4. SICUREZZA DEL PRODOTTO FUSION 360 4

4.1 SICUREZZA DELLE COMUNICAZIONI 4
4.2 CRITTOGRAFIA E CIFRATURA 4
4.3 AUTENTICAZIONE 4
4.4 SICUREZZA DEI DATI 5
4.5 VERSIONI DELLE PROGETTAZIONI 5
4.6 SICUREZZA DELLA COLLABORAZIONE BASATA SU HUB E SU GRUPPO 5
4.7 CONDIVISIONE PUBBLICA 6

5. INFRASTRUTTURA CLOUD 6

5.1 ELEVATA DISPONIBILITÀ 6
5.2 REPLICA E RIDONDANZA DEI DATI 6
5.3 RIDONDANZA DEL SISTEMA DI ALIMENTAZIONE 6
5.4 RIDONDANZA DELLA CONNETTIVITÀ INTERNET 6
5.5 SICUREZZA DELLE INFRASTRUTTURE FISICHE 7
5.6 CONTROLLO DELL'ACCESSO ALLE STRUTTURE 7
5.7 PREVENZIONE DEGLI INCENDI 7
5.8 CONTROLLI CLIMATICI 7

6. GESTIONE DEGLI INCIDENTI OPERATIVI 8

7. GESTIONE DELLE PATCH 8

8. GESTIONE DELLE MODIFICHE 8

9. GESTIONE DELLA CAPACITÀ 9

10. AVVISI E MONITORAGGIO 10

11. ZERO INATTIVITÀ DURANTE LE INSTALLAZIONI CLIENT 10

12. CONTROLLI OPERATIVI DI AUTODESK FUSION 360 11

13. SICUREZZA DI AUTODESK 11

13.1 ANALISI DELLA VULNERABILITÀ E TEST DI PENETRAZIONE 12
13.2 SICUREZZA DELLA RETE 12
13.3 CRITTOGRAFIA 12
13.4 PRIVACY 12

14. RISORSE 12

1. Introduzione

Autodesk® Fusion 360™ è il primo strumento CAD, CAM e CAE 3D del suo genere. È in grado di collegare il processo di sviluppo dei prodotti in un'unica piattaforma basata sul cloud, compatibile con Mac e PC. Gli strumenti di Fusion 360 consentono di esplorare le idee progettuali in modo semplice e veloce attraverso un set di strumenti sicuro e integrato con opzioni che vanno dalla progettazione concettuale alla realizzazione, fino a includere browser Web e dispositivi mobili.

1.1 Scopo e ambito del documento

Lo scopo di questo documento è spiegare le operazioni di Autodesk, il processo di sviluppo del software e le misure di sicurezza implementate nell'ambiente. In questo documento, con Autodesk Fusion 360 si intende sia il software client Fusion 360 sia il software di accesso al browser Fusion 360.

Il framework di sicurezza di Autodesk si basa sugli standard di settore per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni sui clienti.

Fusion 360 è progettato per garantire elevata disponibilità e scalabilità, fornendo ai clienti un servizio cloud veloce e resiliente. Il fornitore di servizi hosting cloud di Autodesk è Amazon Web Services (AWS), leader nell'infrastruttura cloud. Autodesk si affida al modello di responsabilità condivisa del fornitore di hosting AWS, che include l'infrastruttura composta da hardware, software, reti e installazioni che eseguono i servizi cloud AWS. Per ulteriori informazioni, consultare: https://aws.amazon.com/it/compliance/shared-responsibility-model/.

2. Sicurezza di Autodesk

Il framework di sicurezza di Autodesk si basa sugli standard di settore per garantire procedure di protezione coerenti che consentono costruire e operare in modo sicuro e di rimanere sicuri.

- **Costruire in modo sicuro**: l'integrazione della sicurezza nei nostri prodotti dal basso verso l'alto è fondamentale per proteggere l'investimento dei nostri clienti nei prodotti e nei servizi Autodesk. Integriamo la sicurezza in tutte le fasi dello sviluppo del software.

- **Operare in modo sicuro**: costruiamo la sicurezza direttamente nelle nostre infrastrutture. Il nostro approccio olistico include l'installazione client di strumenti di protezione degli endpoint, requisiti di applicazione di patch e protezione avanzata standardizzati, controlli per la gestione di identità e accessi e attività di sicurezza offensiva.

- **Rimanere sicuri**: in Autodesk la sicurezza è incentrata su tre obiettivi principali che proteggono la riservatezza, l'integrità e la disponibilità delle informazioni:

    - Riservatezza: le informazioni sono accessibili solo alle persone autorizzate.
    - Integrità: le informazioni sono complete e accurate.
    - Disponibilità: i dati sono accessibili e disponibili ai clienti.

Il Chief Security Officer (CSO) è responsabile dello sviluppo, dell'implementazione e della governance della strategia e del programma di sicurezza e garantisce che i criteri e gli standard di sicurezza vengano applicati a tutti i prodotti e gli ambienti Autodesk. Il team di sicurezza e il CSO sono supportati dai dirigenti e dal Consiglio di amministrazione di Autodesk.

3. Progettazione di Fusion 360

Il team di progettazione di Fusion 360 è responsabile della progettazione, dell'implementazione e del test del software client e dell'applicazione dei servizi cloud di Fusion 360.

La progettazione, la codifica, il test e la manutenzione di Fusion 360 si basano su un processo di sviluppo software agile. Durante le fasi di progettazione, gli architetti producono e rivedono documenti di progetto dettagliati per valutare la funzionalità e la scalabilità della progettazione. Durante le fasi di implementazione, gli ingegneri e gli architetti software eseguono revisioni dei codici tra colleghi per rilevare le deviazioni dalle pratiche di sviluppo dell'applicazione Fusion 360. Tutto il codice prodotto durante il processo include test delle unità funzionali e le storie dell'utente non vengono completate finché il personale del controllo qualità non ha verificato l'accettazione e la definizione dei criteri di completamento. Anche il test delle prestazioni di Fusion 360 è integrato nel ciclo di vita di sviluppo. Il team di Fusion 360 esegue test di carico durante lo sviluppo per identificare già nelle prime fasi del processo modifiche che potrebbero influire negativamente sulle prestazioni.

3.1 Formazione dei dipendenti

L'importanza della sicurezza delle informazioni viene sottolineata come parte dell'orientamento di tutti i dipendenti neo-assunti di Autodesk. I dipendenti devono leggere, comprendere e seguire un corso di formazione sul Codice di condotta aziendale. Il Codice richiede che ogni dipendente operi in modo lecito, etico, con integrità e nel rispetto reciproco e nei confronti di utenti, partner e concorrenti dell'azienda.

I dipendenti di Autodesk devono seguire le linee guida aziendali in materia di riservatezza, etica aziendale, utilizzo appropriato e standard professionali. I nuovi dipendenti devono firmare un accordo di riservatezza. Il nuovo orientamento dei dipendenti pone in rilievo la riservatezza e la privacy dei dati dei clienti.

Per implementare pratiche ottimali di sicurezza, Autodesk ha introdotto un programma annuale di certificazione della sicurezza del software (SSCP, Software Security Certification Program) per i dipendenti con mansioni relative a progettazione e infrastruttura cloud.

4. Sicurezza del prodotto Fusion 360

In Autodesk Fusion 360 sono integrate funzionalità di sicurezza che vanno dalla comunicazione con i servizi cloud a funzionalità di protezione e collaborazione a livello di prodotto che sono controllabili dall'utente.

4.1 Sicurezza delle comunicazioni

Tutte le comunicazioni tra Autodesk Fusion 360 e i servizi cloud richiedono connessioni HTTPS sicure.

4.2 Crittografia e cifratura

La comunicazione tra i servizi di Fusion 360 e quelli di back-end e all'interno di questi ultimi avviene su un canale crittografato.

4.3 Autenticazione

Per accedere ad Autodesk Fusion 360 sono necessarie credenziali, ossia l'ID Autodesk, l'ID utente e la password. Le credenziali sono protette durante la trasmissione di rete e conservate solo come hash con salt.

In Fusion 360 gli utenti finali possono utilizzare l'autenticazione a più fattori durante l'accesso. Gli utenti che scelgono di attivare questa funzionalità possono utilizzare il proprio dispositivo personale protetto (ad esempio il telefono cellulare) per ricevere un codice da utilizzare insieme alla password.

4.4 Sicurezza dei dati

Tutte le progettazioni di Fusion 360 sono salvate nel cloud in un archivio crittografato. La soluzione di archiviazione utilizza lo standard di crittografia avanzata a 256 bit (AES-256) per crittografare i dati.

A livello locale, le progettazioni memorizzate nella cache si basano sulle autorizzazioni a livello di utente del sistema operativo per il controllo degli accessi.

4.5 Versioni delle progettazioni

Per ogni progettazione, in Autodesk Fusion 360 viene conservata la cronologia delle versioni. Il controllo delle versioni protegge l'integrità dei dati consentendo agli utenti di eseguire il ripristino alle versioni precedenti e fornendo un elenco verificabile contenente informazioni su ogni modifica dei file.

4.6 Sicurezza della collaborazione basata su hub e su gruppo

I progetti forniscono una semplice base per concedere o limitare l'accesso alle progettazioni di Autodesk Fusion 360 ad un gruppo di collaboratori. Gli inviti ai progetti sono approvati dal proprietario o dal moderatore del progetto e garantiscono un rigoroso controllo sui membri che concedono l'accesso a nuovi utenti.

Le aziende possono scegliere di utilizzare gli hub del team per esercitare la proprietà e il controllo di accesso su tutti i progetti creati dai membri. Le impostazioni relative alla privacy del progetto, quali progetti aperti, chiusi e segreti, consentono una collaborazione controllata. Con gli hub del team, i membri possono scegliere di limitare l'accesso ai collaboratori che sono stati invitati al progetto. Gli hub del team consentono inoltre agli amministratori del cliente di disattivare gli account degli ex-dipendenti e di trasferire la proprietà del progetto ad altri membri del team.

4.7 Condivisione pubblica

Con la condivisione pubblica, gli utenti possono collaborare con parti interessate esterne che non dispongono di un ID Autodesk o di un diritto per Fusion 360. Gli utenti di Fusion 360 creano un collegamento che fornisce un accesso in sola lettura alla progettazione. Possono inoltre abilitare le funzionalità di download/esportazione. Gli utenti possono revocare in qualsiasi momento la condivisione pubblica offerta da questo collegamento.

5. Infrastruttura cloud

Il team di infrastruttura cloud è responsabile di definire ed eseguire le procedure per la gestione del rilascio delle applicazioni, gli aggiornamenti dell'hardware e del sistema operativo, il monitoraggio dello stato del sistema e altre attività necessarie per la manutenzione di Autodesk Fusion 360.

5.1 Elevata disponibilità

Autodesk Fusion 360 è progettato per raggiungere un elevato livello di disponibilità mediante l'utilizzo di sistemi ridondanti nell'infrastruttura di supporto e la distribuzione del carico in un parco di istanze scalabili.

5.2 Replica e ridondanza dei dati

La replica dei dati dei clienti viene eseguita tra le zone di disponibilità di Amazon Web Services (AWS). La replica limita la possibilità di perdita di dati o di un ritardo nella ripresa del servizio qualora fosse necessario eseguire il failover in un centro dati di backup.

5.3 Ridondanza del sistema di alimentazione

I centri dati AWS contengono sistemi di alimentazione elettrica ridondanti per la manutenzione delle operazioni 24 ore su 24, 7 giorni la settimana. I gruppi di continuità (UPS, Uninterruptible Power Supplies) forniscono automaticamente backup ai sistemi elettrici primari in caso di guasto. I generatori in ciascun centro dati forniscono un'alimentazione di backup a lungo termine nell'eventualità di un'interruzione di servizio.

5.4 Ridondanza della connettività Internet

Viene utilizzato un sistema multi-fornitore ridondante per mantenere la connettività Internet a ciascuno dei centri dati.

Il software client Autodesk Fusion 360 dispone anche di una modalità offline che consente agli utenti di continuare ad accedere a copie locali della progettazione e di lavorare ad esse quando non sono connessi ad Internet.

5.5 Sicurezza delle infrastrutture fisiche

L'applicazione Autodesk Fusion 360 viene eseguita in centri dati protetti da AWS, che applicano una serie di controlli di sicurezza contro accessi fisici non autorizzati e rischi ambientali. Segue una sintesi di alcuni controlli fisici e ambientali. Per una panoramica completa dei processi di sicurezza AWS, vedere qui.

5.6 Controllo dell'accesso alle strutture

I centri dati AWS sono protetti 24 ore su 24, 7 giorni la settimana dal team di sicurezza fisica professionale. Il perimetro di ogni centro dati, così come le stanze che contengono le installazioni informatiche e di supporto, è protetto da videosorveglianza. La videosorveglianza è mantenuta su supporti digitali per poter visualizzare l'attività più recente su richiesta. Gli ingressi ai centri dati sono protetti da porte blindate che limitano l'accesso ad una sola persona alla volta. Tutti i visitatori e gli appaltatori devono presentare prova di identità per essere ammessi ed essere sempre scortati da personale autorizzato. Solo i dipendenti con un'esigenza aziendale legittima possono accedere al centro dati e tutte le visite sono registrate elettronicamente.

5.7 Prevenzione degli incendi

I sistemi di rilevamento e soppressione degli incendi, quali rilevatori di fumo e impianti sprinkler attivati dal calore, sono installati in ogni centro dati per proteggere i locali contenenti apparecchiature informatiche e sistemi di supporto. I sensori di rilevamento antincendio sono installati nel soffitto e sotto un pavimento rialzato.

5.8 Controlli climatici

I controlli climatici del centro dati proteggono server, router e altre attrezzature soggette a guasti qualora vengano violati valori ambientali ben definiti. È in atto un monitoraggio da parte dei sistemi e del personale per prevenire condizioni pericolose, come il surriscaldamento. I sistemi di controllo applicano automaticamente le regolazioni per mantenere la temperatura e altre misurazioni ambientali entro soglie accettabili.

6. Gestione degli incidenti operativi

Autodesk applica una politica di gestione degli incidenti che definisce le pratiche ottimali di risoluzione degli incidenti. La politica di gestione degli incidenti di Autodesk richiede la registrazione di tutte le fasi di ripristino e l'utilizzo dell'analisi delle cause primarie per costruire una base di conoscenza delle procedure applicabili. L'obiettivo della politica di gestione degli incidenti di Autodesk non è solo di chiudere gli incidenti in modo rapido ed efficace, ma anche di raccogliere e distribuire informazioni sugli incidenti, in modo che i processi possano essere migliorati costantemente e le risposte future possano essere guidate dalle conoscenze accumulate.

7. Gestione delle patch

Il team di infrastruttura cloud dispone di una politica di gestione che garantisce un'efficace installazione client delle patch. Ove possibile, è disponibile un'automazione per verificare la presenza di nuove patch e preparare elenchi di installazioni client che possano essere approvati dal personale autorizzato per le infrastrutture cloud. La politica delle patch definisce inoltre i criteri per determinare l'impatto di una patch sulla stabilità dei sistemi. Se si rileva che una patch ha un impatto potenzialmente elevato, viene condotto un test di regressione prima dell'installazione client della patch. La gestione delle modifiche consente di monitorare l'installazione delle patch nei sistemi di produzione.

8. Gestione delle modifiche

Il team di infrastruttura cloud si avvale di una procedura di gestione delle modifiche che include le seguenti attività:

- **Modulo di richiesta di modifica (RFC, Request For Change).** Per tutte le modifiche è necessario inviare un modulo RFC. Il modulo include il nome dell'autore della modifica, la priorità della modifica, la giustificazione aziendale della modifica e la data di implementazione della modifica richiesta.
- **Piani di backout.** Il team di infrastruttura cloud crea piani di backout dettagliati prima dell'installazione client, per consentire il ripristino dello stato del sistema se una modifica

provoca un'interruzione del servizio. I piani di backout includono istruzioni eseguibili definite negli script che ripristinano lo stato del sistema con un minimo di passaggi manuali.

- **Finestre di manutenzione definite.** Il team di infrastruttura cloud specifica le finestre di manutenzione pianificate, di emergenza ed estese. Programma la manutenzione pianificata fuori dalle ore di massimo utilizzo.

- **Piano di test.** Il team di infrastruttura cloud definisce un insieme di test per verificare che la funzionalità sia accessibile dopo l'installazione client di una modifica.

- **Esecuzione del test.** Al termine dell'installazione client, il team di infrastruttura cloud e il team QA di Autodesk Fusion 360 eseguono i test per verificare che la funzionalità identificata come a rischio rimanga disponibile.

9. Gestione della capacità

Poiché l'accesso dei clienti ai servizi cloud viene fornito su richiesta tramite un modello self-service, i modelli di traffico sono altamente variabili e soggetti a picchi di utilizzo. Quando si verifica un picco, la disponibilità di un servizio può essere compromessa se il pool di risorse di elaborazione che alimenta il servizio è esaurito. Per mantenere un elevato livello di disponibilità, il team di infrastruttura cloud implementa una politica di gestione della capacità. Queste pratiche includono:

- **Frequente registrazione dell'utilizzo delle risorse.** L'utilizzo delle risorse di Autodesk Fusion 360 viene raccolto ad intervalli regolari da una varietà di componenti di infrastruttura, incluse istanze virtuali, volumi di archiviazione virtuale e dispositivi di rete virtuali. Le statistiche di utilizzo sono memorizzate in un repository di gestione della capacità.

- **Pianificazione della capacità.** Il team di infrastruttura cloud utilizza la gestione della capacità per generare un piano di capacità dettagliato, che documenta gli attuali livelli di utilizzo e modella i livelli futuri in base all'analisi statistica e all'impatto dei prossimi

miglioramenti alle funzionalità aziendali. Il piano di capacità viene aggiornato in base alle esigenze o se vengono rilevate modifiche significative ai modelli di utilizzo.

- **Allocazione delle risorse.** Le risorse di calcolo sono allocate in base alle richieste dei clienti. Le risorse di calcolo "pre-riscaldate" sono sempre disponibili. Nel caso di un picco di attività, vengono create istanze di nuove risorse. Ad esempio, è possibile ottenere la disponibilità delle risorse del browser di Autodesk Fusion in meno di 10 minuti.
- **Monitoraggio delle attività.** Le plance di comando e gli avvisi di attività sono definiti nei servizi back-end e permettono agli ingegneri di osservare l'attività del sistema ed eseguire esami e analisi successivi all'incidente.

10. Avvisi e monitoraggio

Per fornire il più breve tempo medio di riparazione, Autodesk utilizza sistemi automatizzati per monitorare Fusion 360, convalidando lo stato di integrità del servizio. Ogni singolo componente, dal database ai servizi, viene monitorato individualmente.

Nel caso di un evento con un impatto sul servizio, vengono generati avvisi e il team di infrastruttura cloud riceve una notifica tramite un processo di escalation.

Lo stato del servizio descrive inoltre la correlazione tra i servizi Autodesk. Un servizio come Autodesk Fusion 360 è altamente sensibile al servizio ACM (controllo degli accessi). Ogni servizio deve essere resiliente quando un servizio dipendente non funziona e deve degradarsi lentamente fino a non funzionare più senza causare la perdita dei dati del cliente.

Lo stato del servizio Fusion 360 viene visualizzato pubblicamente dal servizio Plancia di comando Integrità di Autodesk: https://health.autodesk.com.

11. Zero inattività durante le installazioni client

Quando le patch vengono applicate all'ambiente di produzione, viene adottato un approccio di installazione client Blue-Green per il browser di Autodesk Fusion e altri servizi Fusion 360. Questo per evitare che i clienti si trovino in una situazione di inattività del servizio.

12. Controlli operativi di Autodesk Fusion 360

In Autodesk Fusion 360 i dati sensibili dei clienti sono protetti dall'accesso non autorizzato.

- **Restrizioni fisiche ai centri dati.** Le restrizioni fisiche ai centri dati impediscono l'accesso di persone non autorizzate ai sistemi hardware e di supporto di Autodesk Fusion 360.
- **Controlli delle referenze.** Per i dipendenti che hanno accesso fisico alle risorse di calcolo e ai sistemi di supporto di Autodesk Fusion 360 sono richiesti controlli delle referenze.
- **Replica dei dati.** La replica dei dati consente di copiare i dati dei clienti tra centri dati ridondanti, in modo da poter mantenere la continuità aziendale in caso di failover tra le installazioni.
- **Tecnologie ridondanti**. Tecnologie ridondanti, quali i bilanciatori di carico e i database in cluster, limitano punti di errore singoli.

13. Sicurezza di Autodesk

Il team di sicurezza di Autodesk è formato da un gruppo di specialisti in sicurezza delle informazioni responsabile di identificare e applicare le pratiche di sicurezza all'interno dell'ambiente cloud di Autodesk. Le responsabilità del team di sicurezza di Autodesk includono:

- Consultare la posizione di sicurezza della progettazione e dell'implementazione delle infrastrutture cloud di Autodesk.
- Definire e garantire l'attuazione delle politiche di sicurezza, inclusa la gestione dell'identità e dell'accesso, la gestione delle password e la gestione delle vulnerabilità.
- Promuovere il rispetto delle procedure di sicurezza consolidate mediante revisioni e audit interni.
- Identificare e implementare tecnologie che proteggano le informazioni dei clienti.

- Incaricare esperti di sicurezza di terze parti di condurre valutazioni sulla sicurezza delle informazioni.
- Monitorare i servizi cloud per potenziali problemi di sicurezza e rispondere agli incidenti in base alle esigenze.
- Eseguire revisioni annuali della politica di sicurezza di Autodesk.

13.1 Analisi della vulnerabilità e test di penetrazione

I servizi di Fusion 360 sono sottoposti ad un test di penetrazione annuale e a scansioni periodiche per individuare le minacce e le vulnerabilità relative alla sicurezza. L'applicazione è sottoposta anche ad analisi statiche e a scansioni delle librerie di terze parti. Le scansioni di sicurezza e i test di penetrazione coprono un'ampia gamma di vulnerabilità definite da Open Web Application Security Project (OWASP) e SANS top 25.

13.2 Sicurezza della rete

La sicurezza della rete viene applicata mediante una combinazione di controlli fisici e logici, tra cui crittografia, firewall e procedure protezione avanzata dei sistemi. Inoltre, AWS fornisce controlli di sicurezza di rete per proteggere i centri dati fisici. Per ulteriori informazioni, vedere Procedure ottimali per la sicurezza, l'identità e la conformità.

13.3 Crittografia

Tutto il traffico di rete viene crittografato durante la trasmissione su Internet al perimetro dell'ambiente cloud di Autodesk. Le informazioni riservate, quali credenziali, informazioni sulle sessioni dell'applicazione, token di accesso e profili utente, sono crittografate quando inattive.

13.4 Privacy

Autodesk è trasparente per quanto riguarda la raccolta e l'utilizzo dei dati personali dei clienti. Per ulteriori informazioni, leggere l'Informativa sulla privacy di Autodesk.

14. Risorse

Le seguenti risorse forniscono informazioni generali su Autodesk e su altri argomenti a cui si fa riferimento nella sezione principale del presente documento.

- **Autodesk**: per informazioni su Autodesk, visitare il sito Web all'indirizzo https://www.autodesk.it.
- **Autodesk Trust Center**: per informazioni su Autodesk Trust Center, visitare il sito Web all'indirizzo https://www.autodesk.it/trust/overview.
- **Autodesk Fusion 360**: per informazioni su Fusion 360, visitare il sito Web all'indirizzo http://fusion360.autodesk.com.