Intapp Secure Cloud

Architectural overview and reliability

The Intapp Secure Cloud is designed from the ground up to meet the needs of legal, financial, and professional services firms and their clients requiring the highest level of security and control over their data. Our cloud model incorporates the key elements of secure computing and exceeds common regulatory requirements while preserving firms' control over data access.

This document describes the availability architecture of the following Intapp OnePlace products:

- Intapp CRM
- Intapp Experience
- Intapp Intake
- Intapp Conflicts
- Intapp Terms
- Intapp Pricing
- Intapp Time
- Intapp Flow

The Intapp Secure Cloud possesses a unique architecture built specifically to meet the needs of regulated industries. Cloud deployment delivers many unique benefits, including a secure infrastructure, a simplified process for releasing critical application updates, and proactive monitoring to maximize performance and responsiveness. This architecture leverages the Amazon Web Services (AWS) secure cloud infrastructure, which is the largest and most successful public cloud provider for services and enterprises and provides a highly secure and resilient infrastructure. NASDAQ, the U.S. Food and Drug Administration, NASA Jet Propulsion Laboratory, and Orion Health also rely on AWS for their line of business applications.

AWS data centers

Intapp selected Amazon for its excellent uptime track record.

AWS state-of-the-art data centers utilize innovative architectural and engineering approaches. The AWS platform and infrastructure benefit from Amazon's many years of experience designing, constructing, and operating large-scale data centers.

AWS data centers include automatic fire detection and suppression equipment to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by various types of sprinkler systems, including wet-pipe, double-interlocked pre-action, and gaseous systems. Data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, 7 days a week. Uninterruptible power supply (UPS) units provide backup power for critical and essential loads in the facility in the event of an electrical failure, and generators provide backup power for the entire facility.

Climate control maintains a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Both personnel and systems monitor and control temperature and humidity at appropriate levels.

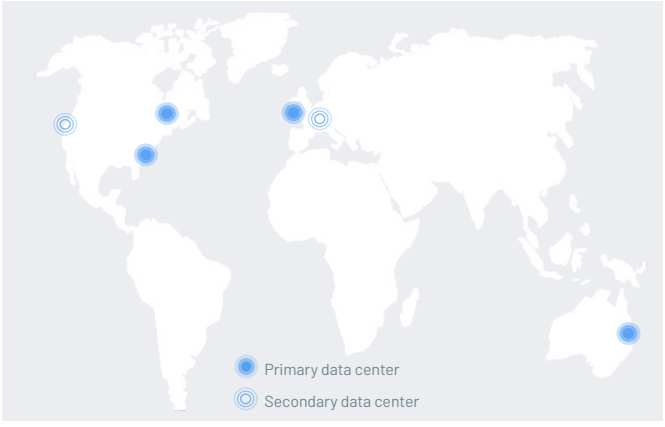
AWS monitors electrical, mechanical, and life-support systems and equipment to immediately identify any issues. Preventative maintenance is performed to maintain the continued operability of equipment.

Finally, security is top of mind for Amazon. AWS data centers are housed in nondescript facilities, and physical access is strictly controlled by professional security staff both at the perimeter and at building ingress points utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data-center floors. All visitors and contractors are required to present identification, and are signed in and continually escorted by authorized staff.

Intapp Secure Cloud high availability

Intapp uses commercially reasonable efforts to make online service available 24 hours a day, 7 days a week, except for planned downtime necessary for system maintenance and feature releases.

The Intapp Secure Cloud is hosted in multiple locations worldwide. Customers can select their service delivery region of preference: U.S., E.U., Australia, and Canada.



The Intapp global data center footprint

To achieve high availability for the Intapp Secure Cloud, Intapp uses a resilient architecture with components provisioned in multiple AWS availability zones within the selected region, with an automated failover process in place in the event of a failure of one of the availability zones.

Amazon automatically provisions and maintains a synchronous standby replica of the tenant's database — a key component — in an alternate availability zone. The primary database instance is synchronously replicated to the replica to provide redundancy, eliminate I/O freezes, and minimize latency spikes. In the event of a planned or unplanned instance outage, AWS services automatically switch to a standby database replica in another availability zone.

For other components enabled in multiple availability zones, the Intapp Secure Cloud leverages multiple active nodes in different availability zones, and traffic will be rerouted among them in the case of individual node failure.

Data integrity and disaster recovery

Intapp performs daily backups of each database in geographically separated data centers.

In the case of data corruption, restoration after failed upgrade, or data loss, Intapp can perform a point-in-time restoration up to 15 days back.

Intapp also provides a comprehensive disaster recovery plan that addresses the actions Intapp will take in the event of an extended service outage. In a catastrophic event where a complete AWS region is taken offline, Intapp would redeploy the affected Intapp Secure Cloud cluster into a different AWS region within the same geography.*

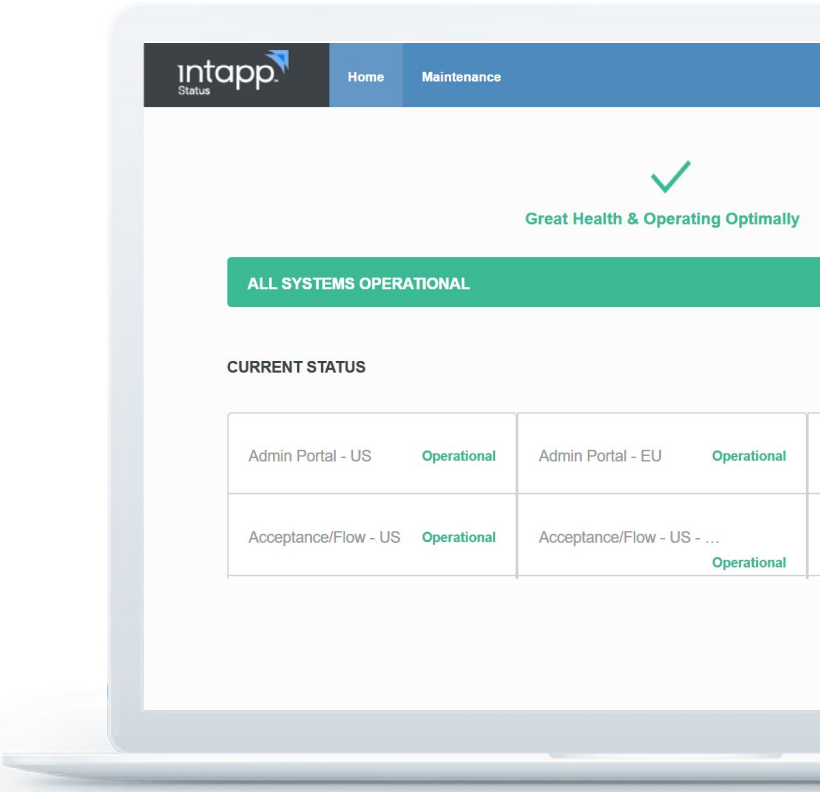
Intapp tests its disaster recovery plan each time that it is revised — but not less than once every 12 months — using any of several industry standard testing methods. A limited-functionality instance is maintained for up to 90 days after a subscription ends, unless otherwise specified. Intapp can discuss the results of the most recent disaster recovery test upon request.

*Restoring to a different AWS region is not available for customers in Australia and Canada geographic regions.

Failure scenario	Recovery time objective (RTO)*	Recovery point objective (RPO)
Host failure	N/A	N/A
Data center failure	15 minutes	1 minute
Region failure**	8 hours	4 hours

*RTO: time required to deploy the application to the new region and perform any required network end-point failover. Intapp DevOps standard operating procedure for this process in case of major outage is no more than 8 hours, which includes communication to affected customers.

** Does not apply to Australia and Canada geographic regions.



Service level agreement

Intapp provides financial backing to our commitment to achieve and maintain service levels.

Maintenance process

Unlike on-premises deployments, software and solutions delivered via the Intapp Secure Cloud are maintained directly by Intapp. Fixes and upgrades are introduced into production on a regular, automated basis after going through a rigorous development, integration, and testing process.

Proactive monitoring

Intapp specifically monitors service availability, response times, and database load, as well as CPU and network performance. Intapp has implemented synthetic transaction monitoring and health checks to ensure platform services are available to each application.

In the event of service degradation, Intapp has implemented processes and tools to react rapidly. Moving beyond simple pings to check uptime, Intapp leverages best-of-breed monitoring and alerting systems that allow support teams to proactively be alerted of any performance issues as experienced by users. The service level is publicly shared in real time on the Intapp Secure Cloud status website at https://status.my.intapp.com.