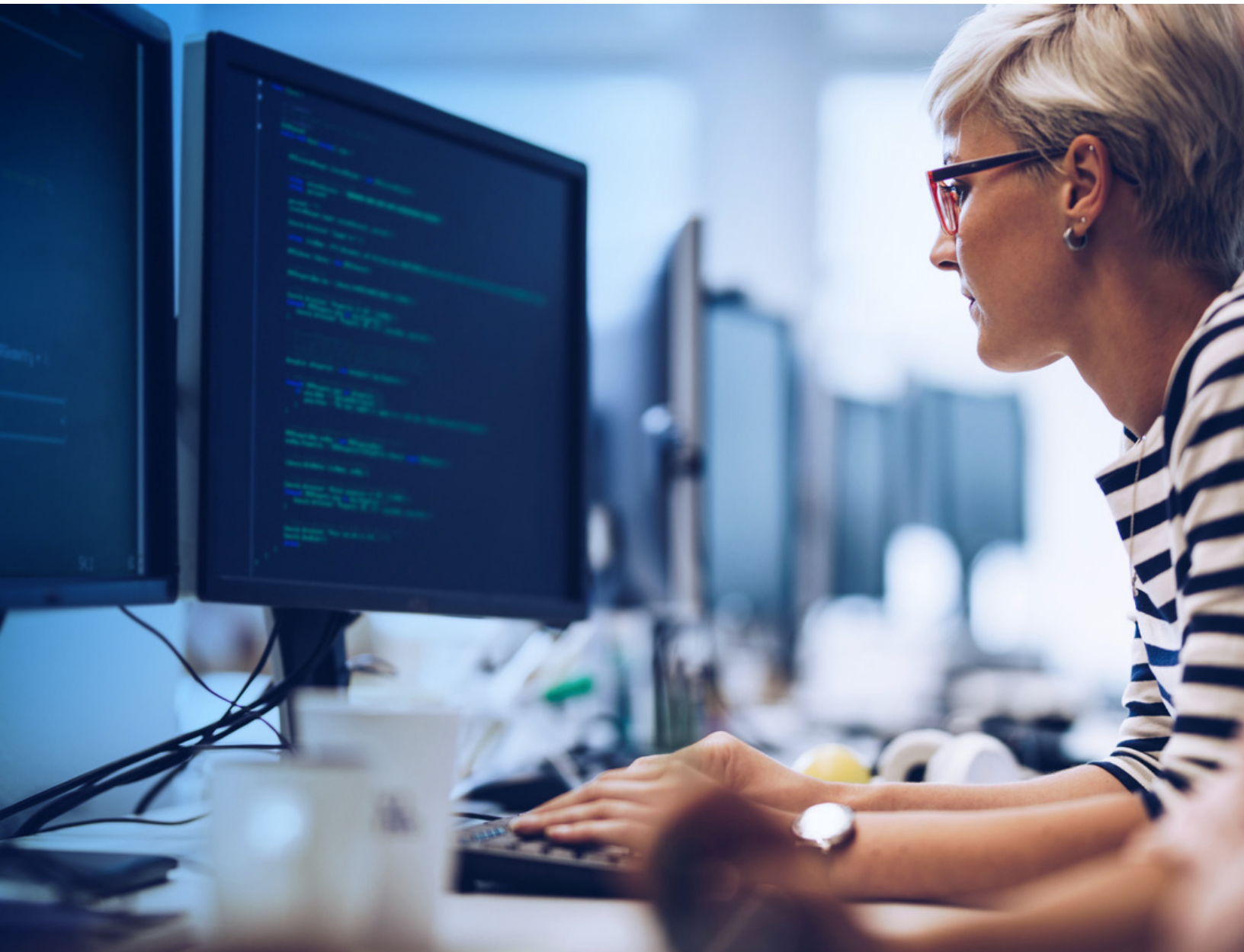
# The Intapp Secure Cloud

## 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.

The Intapp Secure Cloud possesses a unique architecture built specifically to meet the needs of regulated industries. Cloud deployment delivers many unique benefits, including 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) and Microsoft Azure secure cloud infrastructure, the largest and most successful public cloud for services and enterprises and provides a highly secure and resilient infrastructure.

### AWS and Azure Data Centers

Intapp selected AWS and Azure due to their excellent uptime track records. State-of-the-art data centers use innovative architectural and engineering approaches, and benefit from many years of experience designing, constructing, and operating large-scale data centers.

To reduce risk, data centers include automatic fire detection and suppression equipment, including 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 in the event of an electrical failure for critical and essential loads in the facility, and generators provide backup power for the entire facility.

Within data centers, 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 equipped to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity to maintain appropriate levels.

Data centers monitor 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. 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 using video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication at least twice to access data-center floors. All visitors and contractors must 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. To achieve high availability for the Intapp Secure Cloud, Intapp uses a resilient architecture with three redundant levels for all solutions (with the exception of DealCloud for Financial Services).

At the first level (HA1), the Intapp architecture is fault-tolerant and uses multiple, active processing nodes for each service. Traffic will reroute among the nodes in the case of an individual node failure. Thus, a single-host failure, including the database, will not cause downtime.

At the second level (HA2), all components are provisioned in multiple availability zones within the selected region. The hosting providers automatically provision and maintain 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 provide redundancy, eliminate I/O freezes, and minimize latency spikes. An automated fail-over process is in place in the event of a failure of a service or one of the availability zones.

At the third level (HA3),* Intapp solutions store a copy of the customer data in a region at least 100 miles away from the production data centers. Intapp provides a comprehensive disaster recovery plan that addresses the actions we'll take in the event of an extended service outage. In a catastrophic event where a complete region is taken offline, Intapp would redeploy the affected Intapp Secure Cloud cluster into a different region within the same geography. Intapp tests its disaster recovery plans each time they're revised, but not less than once every 12 months, using several industry-standard testing methods.
Note that restoring to a different region isn't available for customers in Australia and Canada geographic regions due to hosting provider limitations.

DealCloud for Financial Services maintains a similar high availabilty setup. The first level (HA1) is identical to the HA1 setup for the other solutions. The protection for data center and regional failures are merged; DealCloud for Financial Services systems are set up to replicate customer data in near real-time from the primary region to the secondary region.

The secondary region is a warm site that can be activated by the Intapp DevOps team to become the primary site. The near real-time replication should result in nearly no data loss; however, Intapp also has the ability to restore from remote daily backups in case of data corruption due to the primary site outage. Intapp performs tests of its disaster recovery plan as described for the other solutions.

*Data Center Availability for Intapp Solutions*

| Failure Scenario** | Recovery Time | Recovery Point |
|---|---|---|
| **Host Failure** | N/A | N/A |
| **Data Center Failure** | 15 minutes | 1 minute |
| **Region Failure** | 8 hours*** | 4 hours |

*Data Center Availability for DealCloud for Financial Services*

| Failure Scenario | Recovery Time | Recovery Point |
|---|---|---|
| **Host Failure** | N/A | N/A |
| **Data Center or Region Failure** | 6 hours | 24 hours |

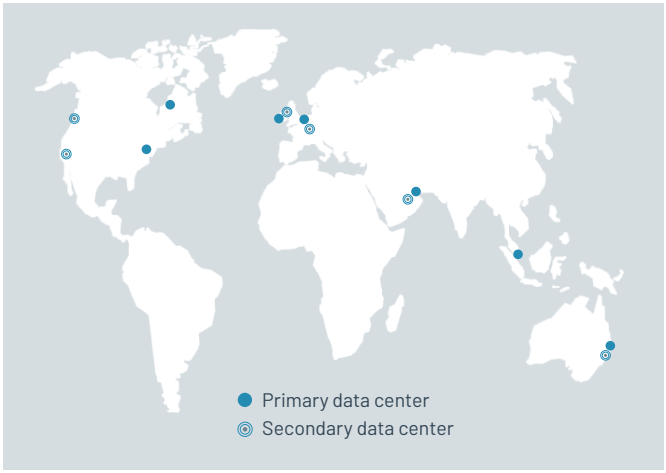
* HA3 not applicable in Canada and Australia; hosting providers maintain only one region in each country (Sydney and Montreal, respectively).

** Does not apply to Australia and Canada geographic regions due to hosting provider limitations.

*** 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.

## Data Location

The Intapp Secure Cloud is hosted in multiple locations worldwide. Customers can select their service delivery region of preference: U.S., E.U., UAE (DealCloud for Financial Services only), APAC (DealCloud for Financial Services only), Australia (excluding DealCloud for Financial Services), and Canada (excluding DealCloud for Financial Services).




*Intapp Global Data Center Footprint*

| | Primary Data Centers | Secondary Data Centers |
|---|---|---|
| | **AWS-Hosted Solutions** | |
| **United States** | U.S. East, Northern Virginia, us-east-1 | U.S. West, Oregon, us-west-2 |
| **Europe** | Europe, Ireland, eu-west-1 | Europe, Frankfurt, eu-central-1 |
| **Canada** | Canada Central, Montreal, ca-central-1 | — |
| **APAC** | Asia Pacific, Sydney, ap-southeast-2 | — |
| | **Azure-Hosted Solutions** (except DealCloud for Financial Services) | |
| **United States** | U.S. East, Virginia | U.S. West, California |
| **Europe** | West Europe, Netherlands | North Europe, Ireland |
| **APAC** | Australia East, New South Wales | — |
| **Canada** | Canada Central | — |
| | **DealCloud for Financial Services** | |
| **United States** | U.S. East, Virginia | U.S. West, California |
| **Europe** | West Europe, Netherlands | North Europe, Ireland |
| **APAC** | Singapore | Australia East, New South Wales |
| **Middle East** | UAE, Dubai | UAE, Abu Dhabi |

### Data Integrity

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. (DealCloud for Financial Services retains backups of up to 1 year.)

### Data Retention

A limited functionality instance is maintained for up to 90 days after a client's subscription ends, unless otherwise specified.

### 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. Intapp publishes its maintenance policy at intapp.com/maintenance.

### 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 status.my.intapp.com.