TRINTECH

Trintech
Cloud Security
Frequently Asked Questions

DOCUMENT SUMMARY

Trintech's Information Security team has created a list of frequently asked questions about our cloud security processes and the physical, administrative, and logical controls we have set in place.

Please note that all information in this document applies to the following Trintech and Adra Software-as-a-Service (SaaS) solutions:

- Trintech Cadency and CadencyDirect
- Trintech ReconNET, T-Recs, UPCS, Smart Analysis, and SmartTreasury
- Adra Accounts and Receivables

For information related to Trintech's cloud offerings around the globe and how they may differ, please contact your Trintech account representative.

TABLE OF CONTENTS

Data Access

Data Residency

Encryption

Data Backups

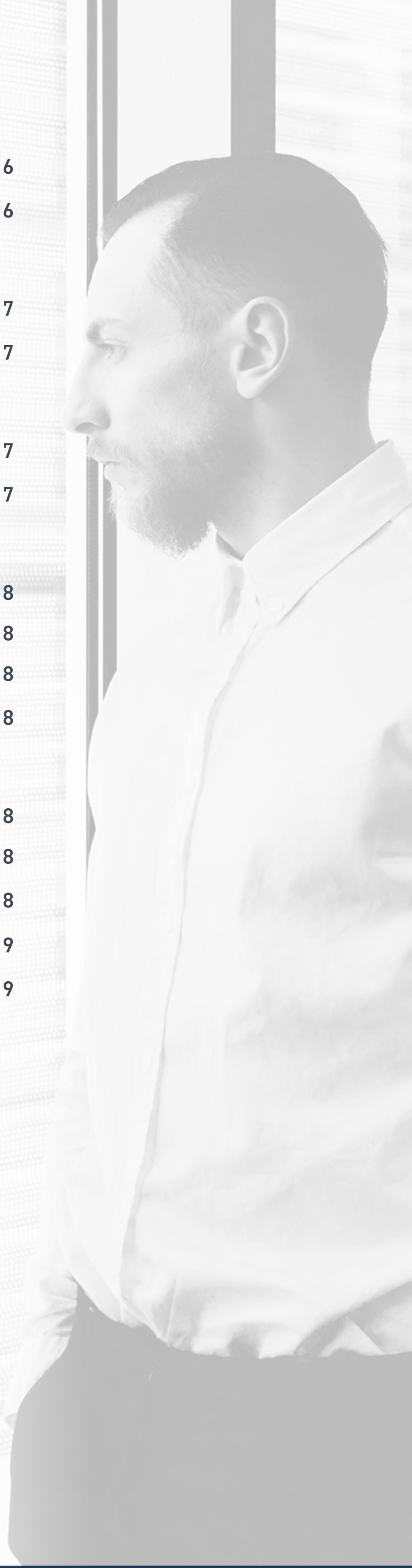
Logging

Vulnerability Management

Software Updates

Compliance and Auditing

Miscellaneous Questions



DATA ACCESS

Who can access customer data?

Customers have complete control over who accesses their data. Access to client data is limited by our role-based access control, which is based on the principle of least privilege, and in accordance with our documented policies and procedures to ensure only a limited subset of employees have access to client data in our production environment.

Which authentication methods are available to customers?

Trintech's Identify and Access Management (IAM) strategy includes SAML 2.0 based Single Sign On (SSO) support as a core capability of key Trintech products. This includes Cadency, CadencyDirect, ReconNET, T-Recs, and other products.

Trintech cloud solutions fully support Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) for customers who elect to configure this on the Identity Provider (IDP) side of the SAML SSO integration.

What password policies are customers able to use?

Customers set their own password policies, either in their instance or in the external directory service. Trintech does not manage customer passwords.

How do Trintech staff access the cloud infrastructure?

Only Trintech personnel with defined and approved production support roles may access the infrastructure supporting customer environments and data. These personnel do not have access to the application's front end of customer non-production or production environments.

Access is limited to the performance of specific tasks, such as troubleshooting in the context of incident response, and maintenance in the context of approved change execution. Access is monitored and logged. Permissions are controlled, reviewed, and audited.

> “We have an absolute commitment to our customers' security. It's why we complete annual, independent third-party audits. Security is baked into everything we do.”

DATA RESIDENCY

Where is customer data hosted?

Each customer's production, non-production environments and data are hosted only within the regional data center pair selected by the customer. Regional data center pairs are pre-defined by Trintech.

Where are the data centers located?

Trintech provides services from regional data center pairs in the United States, United Kingdom, Germany, and Australia.

Are customers able to have their data stored in a single data center?

By design, customer data is hosted within a regional pair of data centers configured to provide both high availability and resiliency. This approach means it is not possible to host customer data in a single data center.

Are customers able to pair Trintech's vendor data centers with one of their own?

Trintech provides leading compliance, security, and availability built on a highly standardized platform. Achieving industry-leading availability and security would not be feasible, nor technically achievable, using resources outside of Trintech's own environment. For this reason, we are unable to permit customers to use their own data centers.

Is a customer's data transferred around the world?

No. Data remains in the customer's designated regional data center pair. Transfers are made in accordance with customer contractual and relevant legal obligations.

ENCRYPTION

How is data encrypted in transit?

Data in transit is encrypted using industry standard secure protocols such as HTTPS (TLS 1.2+, 2048-bit SSL certificates) and SSH.

How is data encrypted at rest?

Data at rest is encrypted using AES-256. Randomly generated symmetric keys are protected by customer-specific public/private key pairs stored in a secure appliance (FIPS 140-2 Level 2/3 certified HSM).

All customer data stored on disk, on tape, or offsite, including backups, is encrypted at rest. This includes all server roles: file transfer, integration, application, reporting, and database servers.

How often are encryption keys rotated?

Key rotation occurs at least annually. Trintech can accommodate schedules designed to meet customer specific policies and regulatory requirements (e.g., quarterly, monthly, etc.).

DATA BACKUPS

How and when is data backed up?

Trintech utilizes industry standard backup tools to perform automated daily backups. This includes weekly full backups, and daily differential or incremental backups on all days when weekly full backups do not occur.

Backups are performed at the file, operating system, and database levels. Schedules are designed to meet Business Continuity and Disaster Recovery (BC/DR) targets in the event of a disaster, such as contractual 1 hour Recovery Point Objectives (RPOs) and 4-hour Recovery Time Objectives (RTOs).

How long does Trintech store backed up data?

Trintech retains backups of customer production environments and data for 28 days.

While Trintech does not allow customers to define custom backup retention requirements, Trintech products allow customers the flexibility to retain data within the product for as long as customers' internal policies and/or regulatory requirements dictate (e.g., 1 year, 7 years, etc.).

Are backups encrypted?

At rest encryption described above applies to all backups.
This includes all customer data stored on disk, on tape, or offsite.

> “We are trusted by over 3,500 companies across 100+ countries — including the majority of the Fortune 100.”

LOGGING

Are customers able to see Trintech's firewall and infrastructure logs?

Trintech does not share audit logs with our customers because they contain sensitive information pertaining to Trintech other customers.

As detailed in customer contracts, in the event of an actual suspected security incident, Trintech will provide customers with log information upon removal of information with the potential to identify other Trintech customers.

How long are the logs available?

Both infrastructure and application logs are retained in a centralized logging and Security Event and Incident Management (SEIM) tool. Logs are available online within the tool for a minimum of 30 days and retained for a minimum of 2 years.

VULNERABILITY MANAGEMENT

Are customers able to perform a penetration test on their Trintech instance?

Upon signature of our Security Testing Agreement, we will allow limited vulnerability scanning and penetration testing. This agreement provides the scope and conditions of any testing against Trintech's environment. Without this signed agreement and coordination of testing activities, any attempted attack (real or simulated) will result in Trintech executing its incident response plan, including the notification of law enforcement. If security testing is something you require, please discuss with your account team.

How should customers respond if they discover a vulnerability?

Trintech does not condone any attempts to actively audit our infrastructure. However, we recognize that vulnerabilities in our systems, products, or network infrastructure may be occasionally discovered incidentally. Please follow the Responsible Disclosure instructions on the Trintech Trust Center.

SOFTWARE UPDATES

Are software updates and patches automatic?

Trintech applies patches based on the risk level associated with the vulnerability and in accordance with our contractual obligations.

When do customers need to upgrade their instances?

Trintech collaborates with customers and partners to ensure that upgrades to new release versions (with added customer value and performance/stability improvements) occur on a regular basis and our customers are always on the most current version. Trintech notifies customers of all releases via our usual communication channels, and we encourage all of them to upgrade when a new version and/or a patch is available.

COMPLIANCE AND AUDITING

Are customers able to audit Trintech?

As a SaaS vendor, and in keeping with common industry practice, Trintech permits qualifying customers to conduct one annual onsite audit in accordance with their contractual terms, at our Plano corporate headquarters.

Are customers able to find out more about compliance & standards?

Customers under NDA can view extensive security policies, standards, procedures, reports, and other relevant documents from the Trintech Trust Center portal.

Is Trintech's information security policy documentation obtainable?

Yes, if you are a customer. Trintech has a very detailed set of information security policies and standards that are based on ISO 27001 and assessed as part of this certification. Trintech's information security policy is reviewed and approved by the CISO at least annually and is owned by the director of governance, risk management, and compliance at Trintech. This information is available according to the terms of your subscription agreement.

Is Trintech ISO 27001 certified?

Yes. Trintech's Cadency product is ISO 27001 certified as of 2021

> “We've worked hand-in -hand with customers for years to ensure our compliance standards are consistently up-to-date and comprehensive.”

MISCELLANEOUS QUESTIONS

Are customers able to install their own hardware & software in Trintech's cloud?

Like most cloud providers, it is not possible for customers to install their own hardware or software in the Trintech cloud.

Does Trintech have a disaster recovery plan?

Yes, Trintech operates a disaster recovery (DR) program for customer environments. It is updated and tested at least annually, and the results are documented.

What happens to a customer's data if they stop being a customer?

Upon notification of expiration or termination to Trintech, Trintech works with each customer to return and remove all customer data. Returned data includes both file attachments and database backups made available for download via secure protocols.

How can customers access their database dump?

Customer's file attachments are provided in the format originally uploaded to Trintech (e.g., Excel, PDF, etc.). Database backups are provided in a standard file format. Both may be downloaded from a managed file transfer (MFT) site within the Trintech data center where the customer's production environment resides.

What is Trintech's data destruction process?

Upon written request to Trintech Support, typically after notice of termination and/or return of customer data, Trintech can provide written confirmation that customer specific encryption keys have been securely deleted; that all encrypted online copies of customer data have been removed; and that all encrypted backup copies of customer data will be removed within 30 days. Trintech's data destruction process is in accordance with NIST SP800-88.

The content of this document is provided for general informational purposes only, is not legal advice and shall not be considered expert advice on which anyone should rely for any reason. There is no warranty of any nature for the content of this document including, without limitation, as to completeness, accuracy, usefulness, or timeliness. This document is subject to change at any time including, without limitation, variance or supplementation without notice of any kind to anyone. The content of this document may or may not apply to individual reader situations and, in all cases, individual readers should seek expert advice including, without limitation, legal and technical advice to address specific questions or concerns relevant to their situation without reliance of any nature on the content of this document. Trintech Inc. shall not be liable in any way for use of the content of this document by any individual or organization.