Thru. Security White Paper

INFORMATION SECURITY

Version 2.10 | 2024 January

Thru manages and runs its MFT applications and services on Azure SOC 2 certified data centers.

Introduction **4**
Identity Management **4**
Role-Based Access Control (RBAC) 4
Authentication 4
Data Security **4**
Encryption 4
Key Management 5
Data Retention and Destruction Policies 5
Network Security **5**
DDOS Protection 5
Web Application Firewall 5
Threat Detection **5**
Antimalware 5
Security Management, Monitoring and Governance **6**
Detailed Audit 6
Data Monitoring 6
Network and Log Monitoring 6
Thru Data Centers **6**
Examples of Azure Data Center Certifications 6
Thru Service Availability 7
Thru Business Continuity **7**
Software Updates and Maintenance **7**
Penetration Testing **8**
Vulnerability Scans **8**
Thru Certifications & Third-Party Assessments **8**
Service Level Agreement & Recovery Objectives **9**
Thru Cloud Architecture **9**
Version History **10**

[Page intentionally left blank]

Introduction

This document details the security practices at Thru to ensure data stored and transferred by Thru meets the highest standards to minimize risk and exposure. We follow the zero-trust security model and adhere to the following frameworks and certifications: NIST, SOC2 and ISO/IEC 27001. Thru is hosted in Microsoft Azure data centers and we adhere to a defense in depth (DiD) model outlined in the document.

Identity Management

Thru's identity management tools enable authentication and authorization for entities attempting to access Thru. The system supports role-based access control and enforces the principle of least privilege. Single Sign On (SSO) access is available using SAML 2.0

Role-Based Access Control (RBAC)

Role-based access controls are available allowing admins to control access based on a user's role. This can be configured in the GUI admin section or via APIs.

Authentication

Thru provides several methods for explicit authentication for users, systems and APIs that access Thru. Please refer to the following table.

Entity	Authentication Method
Thru API	Tokens provided by Thru for authentication.
Thru Applications	*Federated Identity Management* With Identity providers via SAML 2.0 for web applications and OpenID Connect for native applications *Username/Password & Multi-Factor Authentication (MFA)* MFA is available as part of Identity Providers implementing SSO and directly in File Sharing portal.
SFTP & FTPS	Username, password and or key and certificate authentication.
Thru Node	HTTPS connection to the cloud supports TLS protocol 1.2 and later.

Data Security

Thru provides separation of customer metadata and storage.

Encryption

Thru's system provides end-to-end encryption for data files in transit and at rest. For additional security, file payloads may also be encrypted.

In Transit

Data in transit over HTTPS is protected using TLS 1.2 and later; transit over SFTP is protected using SSH; transit over FTP is protected using TLS.

At Rest

All data stored in the Thru cloud platform is encrypted by AES 256-bit FIPS-compliant encryption keys. Encryption policies isolate storage per tenant and protect customer data from access by platform administrators and data center operators.

File Payload

PGP encryption option is supported for managed file transfer payloads.

Key Management

SSH and PGP keys can be generated or imported and managed via administration web portals

SSL client certificate support for FTPS connections.

Keys for files encrypted at rest are stored in cloud platform key vault and can be managed by the customer in case of deployment of Thru service in private cloud.

Keys used in at-rest file encryption are protected by Azure Key Vaults utilized in Thru cloud service.

Data Retention and Destruction Policies

Data retention rules can be set by the Thru Admin. Customers who no longer subscribe to the Thru service will have their data deleted, which will be unrecoverable.

Network Security

Thru network security features prevent unauthorized access and SFTP/FTPS connections are allowed only under whitelisting rules.

DDOS Protection

Distributed denial-of-service (DDoS) protection at every Azure data center hosting Thru.

Web Application Firewall

Web Application Firewalls are deployed to filter HTTPS traffic on the Thru service perimeter.

Threat Detection

Antimalware

Data transferred into Thru is scanned by Azure Cloud Defender to protect against malware. The feature provides protection and remediation. Thru's Automated File Transfer service scans files up to 250MB.

Security Management, Monitoring and Governance

Thru has several tools to support a framework of authority and accountably for your data. By using Thru, your organization has a centralized view in the GUI for all file transfer activities. Alerts are available to notify administrators or users of a range of events or non-events such as inactivity. Reports can be generated for specific purposes to view historical data.

Detailed Audit

In the event of a security related incident, Thru's detailed audit of all actions, changes and file transfers will assist in detecting the root cause of the problem. The Thru portal provides file transfer status activity reporting, in real-time and historical. All changes to the data in the system are logged and available for audit via the activity screens. Additional reports can be created by integration via Management API.

Data Monitoring

Ability to monitor events with a vendor SIEM solution for added security.

Thru file delivery and activity dashboard and alerts can be viewed in Thru management portal or file transaction data can be retrieved by third-party applications that consume Thru API. More information is provided on thruinc.com/secure-file-transfer/#monitoring.

Network and Log Monitoring

Thru uses Azure and third-party network and log monitoring tools within the Thru cloud environments. Health metrics of the service and infrastructure are monitored as part of the service and used for internal performance tuning.

Thru Data Centers

Thru is deployed on a multi-tier network architecture and hosted in Azure data centers which have multiple certifications.

Examples of Azure Data Center Certifications

- System and Organization Controls (SOC): 1, 2 and 3
- ISO 27001
- HITRUST
- PCI DSS
- HIPAA

Thru Service Availability

Thru is deployed in the following Azure regional data centers with high availability configurations: US, UK, DE, AU. High availability of critical services is implemented via load balancing, replication, or failover clustering. Thru File Sharing application is configured and deployed in a single availability zone in a specific region. Automated File Transfer application is deployed across multiple availability zones in each region.

Thru MFT storage is deployed in Zone-redundant Azure storage accounts (ZRS). Zone-redundant storage replicates the files synchronously across three Azure availability zones in the Thru service region. Each availability zone is a separate physical location with independent power, cooling, and networking. ZRS offers durability for storage resources of at least 99.9999999999% (12 9's) over a given year.

Customer metadata stored in databases is managed by Azure SQL managed instances and is continuously backed up with point in time restore availability for 7 days. Database backups are stored with geo replication.

Region(s) of deployment to be selected by customer which will be stated in the Service and Usage licensing Agreement (SULA)

(!) Note: Thru instances are unique to each regional datacenter, if all the availability zones in a region were to fail, the Thru service would be unavailable. Multi-region redundancy is not part of the standard Thru service.

Thru Business Continuity

Business operational services and infrastructure are cloud-based and tolerant to any event restricting staff from accessing physical office or office network.

Software Updates and Maintenance

Thru MFT service is deployed in multiple regions and the software is updated as required during weekly scheduled maintenance windows (early Sunday night local time zone of the region). Maintenance notifications are published on Thru service status page status.thruinc.com with emails sent to administrators:

a) One (1) hour before maintenance starts,

b) at the start, and

c) at the end of the maintenance.

Duration of the maintenance is defined by

a) the scope of the update and

b) impact on integrating file transfer APIs and protocols.

For critical integrations and data flows, the maintenance schedule can be planned and adjusted in advance with Thru customers in the region.

Small scope incremental updates may not require downtime of file transfer APIs and protocols connecting to Thru during the maintenance window.

Larger scope updates may require maintenance in APIs and protocols connecting to Thru. If emergency maintenance is required, the customer will receive two (2) hours advance notice. Thru's 99.9% Service Level Agreement only applies to unplanned service outages.

Penetration Testing

Customers are welcome to perform penetration tests, but this procedure requires explicit written consent from Thru. Customers must complete the *Thru Penetration Test Request Information form*.

Vulnerability Scans

Thru process for vulnerability scans, frequency, and access to reports.

- Automated network scans of Thru cloud infrastructure via Qualys cloud infrastructure security testing.
- Automated vulnerability assessments of production Thru software platform via Qualys Web Application Scanning (WAS) tool.
- Periodic manual penetration testing via third-party security companies.
- Qualys reports can be requested once an NDA is in place. Third party pen test reports cannot be shared, as they are requested and run by Thru customers.

Thru Certifications & Third-Party Assessments

Thru has been assessed by third-party vendors and complete results reports are available upon request:

- CyberVadis: 794 / 1000 for a rating of Developed.
- Security Scorecard: 97% Security Score.

Thru is currently in the process of SOC 2 Type 1 certification. (Expected by Q2 2024.)

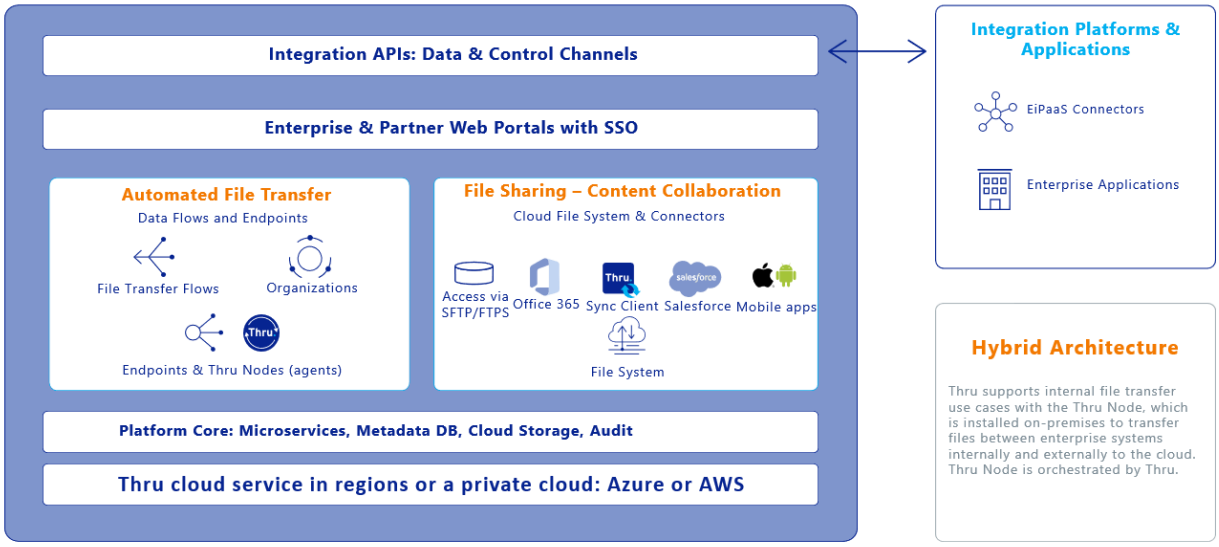
Service Level Agreement & Recovery Objectives

Thru service includes a 99.9% uptime Service Level Agreement (SLA) with details described in the master service agreement (MSA).

Thru recovery time objective (RTO) is 48 hours maximum.

Thru recovery point objective (RPO) is 1 hour.

Thru Cloud Architecture



Version History

Version	Date	Description	Modified By
1.0	05/10/2022	Initial White Paper Drafted	Ian Snead
1.1	06/22/2022	Reviewed and updated	Sergey Arutiunov
2.1	07/05/2022	Reorganized and reformatted document	Monica Otte
2.2	07/26/2022	Additional refinement of new format and information	Monica Otte
2.3	10/26/2022	Added security assessment information	Monica Otte
2.4	02/14/2023	Added storage resiliency section	Monica Otte
2.5	03/09/2023	Storage resiliency correction	Monica Otte
2.6	05/23/2023	Update certification information	Monica Otte
2.7	07/14/2023	Added recovery information	Monica Otte
2.8	10/13/2023	Reworked and updated	Alexei Godek
2.9	12/06/2023	Updated antimalware section	Monica Otte
2.10	01/09/2024	Update dates to 2024 where applicable	Monica Otte