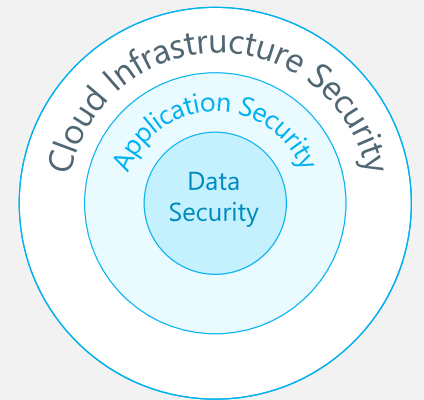


# Thru. Data Security and Compliance

Thru provides a secure and scalable cloud service for manual file sharing and automated file transfer. We adhere to a multi-layer defense-in-depth model, which reduces the attack surface and contains security breaches at multiple levels. Security layers protect Thru's cloud infrastructure, application and customer data.



## Cloud Infrastructure Security

### Deployment

Thru is deployed in Microsoft Azure data centers which are compliant with the following standards (see also [Microsoft Azure documentation](#)):

- SSAE 18 / ISAE 3402 (previously SAS 70)
- SOC 3 SysTrust
- ISO 27001
- PCI Level 1 Service Provider Certified
- Tier III Standards Compliant

### Antivirus Protection

- Real-time scanning of code and data areas
- Ongoing antivirus engine and signature updates
- Automatic quarantine of infected files

### Monitoring

We monitor global infrastructure and security events with SIEM (security information and event management) software 24/7.

### Network Protection

- High availability for all network components
- Multiple zones deployed for access controls and traffic logging
- Firewalls with stateful inspection
- Intrusion protection / detection software
- OWASP-compliant web application firewalls filter web traffic
- Dedicated VPN tunnels with multi-factor authentication for access into production systems by operations personnel
- Domain access control by Active Directory in each deployed geography
- Whitelisting and connection management of Thru's server endpoints protects against security scanning and denial of service attacks

# Thru. Data Security and Compliance

## Application Security

### Authentication

- Required to access any part of Thru
- Strong credential policies for web portals and native applications
- Multi-factor authentication support
- Federated authentication with identity providers via SAML 2.0 and OpenID Connect
- SFTP / FTPS endpoints are protected by password, key and certificate-based authentication

### Web Portal Security

Protection against OWASP Top 10 web application security risks. Portals are scanned for security vulnerabilities on a regular basis.

### Public API Protection

Secured by OAuth 2.0 framework.

### Authorization

Role-based security to control access to application actions, workflows and data entities following the principle of least privilege.

## Data Security

### Data in Transit

Data transfer protected by secure transfer protocols: HTTPS / TLS 1.2 / 1.3, FTPS, SFTP.

### Data at Rest

All data stored in Thru is encrypted by AES 256-bit encryption.

### Data Replication

Data is replicated to multiple zones via cloud provider infrastructure.

### Payload Encryption

PGP encryption is supported along with key management in the administration portal.

### Data Retention

Multi-level retention policies delete the file data from transient storage after transfer completion.

## Security Scanning and Penetration Testing

- Weekly automated scanning of Thru's cloud infrastructure in all service geographies
- Weekly automated vulnerability assessments of Thru platform
- Periodic penetration testing by third-party security vendors

## Secure Software Development Life Cycle

- Static application security testing is performed in all phases of Thru's SDLC with triage and remediation
- Dynamic application security testing is performed at the testing and release SDLC phases using automated cloud security tools

## General Data Protection Regulation Compliance

Your administrators can

- Require user agreements before sending or receiving files
- Allow users to request removal of personal information from Thru

For more information about GDPR compliance, please see our [Privacy Policy](#).