Therefore™ Online White Paper

www.therefore.net

Therefore™

PEOPLE PROCESS INFORMATION

VERSION: 2022 - 01

Table of Contents

1. **Introduction** 4

2. **Architectural Overview** 5

2.1 The Host - Microsoft Azure 5

2.1.1 Defense in Depth 5

2.1.2 Infrastructure Protection 6

2.1.3 Network Protection 7

2.1.4 Data Protection 8

2.2 The Virtual System 8

2.2.1 Tenant Structure 10

3. **The Datacenters** 11

3.1 Certifications 11

4. **Data Management** 14

4.1 Data Security 14

4.2 Data Backup 14

4.3 Data Migration 15

5. **The System - Therefore™ Online** 16

5.1 User Licenses 16

5.2 Additional Licenses 17

5.3 Configuration and Security 17

5.4 Core Applications 18

5.4.1 Therefore™ Solution Designer 18

5.4.2 Therefore™ Console 18

5.4.3 Therefore™ Navigator 18

5.4.4 Therefore™ Viewer 18

5.4.5 Therefore™ Capture Client 18

6. **Technical FAQ** 19

1. Introduction

"Cloud Computing" is an emerging and evolving technology, transforming how IT services, including software applications, are delivered. The technology is centered on the idea of pooling and utilizing shared IT resources amongst numerous organizations, by harnessing the power of the internet and advanced data centers to deploy a spectrum of IT services.

This paradigm shift from locally owned to remotely shared IT infrastructures provides an array of benefits, along with some potential concerns. Some of the advantages realized with cloud computing include cost savings through the sharing and optimization of IT resources, improved performance, greater IT flexibility and scalability, as well as the savings found in not having to employ and invest in personnel to maintain an onsite IT infrastructure. The concerns associated with cloud computing revolve mainly around data security, and the fact that customer data is stored remotely, not within the confines of the customer's location. Like any technology, the advantages and concerns of cloud computing must be evaluated and weighed. Despite the concerns, cloud computing is a viable option for many organizations, and the trend is growing.

Cloud Computing provides an alternative method of delivering Therefore™'s information management solution, with a new cloud-based version, Therefore™ Online. The features and interface are indistinguishable to the end user; the difference lies in where your information is stored. With Therefore™ Online, information is stored in a highly protected data center hosted on the Microsoft Azure platform, rather than on the end user's onsite servers.

The purpose of this white paper is to clearly illustrate the framework and security measures taken with Therefore™ Online, as to give customers a clear understanding and assurance of how their data is being managed.

2. Architectural Overview

2.1 The Host - Microsoft Azure

Therefore Corporation GmbH has partnered with Microsoft, a leading global IT service provider, to host the operations and infrastructure for Therefore™ Online. Utilizing the services of a professional datacenter allows the performance and security of Therefore™ Online to be optimized to the fullest extent. Customers can be assured that all of their data will be held within the Microsoft Azure datacenter in their respective region.

Microsoft's cloud platform, called Microsoft Azure, is a hosted infrastructure that provides processing, storage, network capacity, security, monitoring, back-ups and other fundamental computing resources. A customer specific virtual system environment is operated within the large scale resources of Microsoft datacenters. By utilizing virtualization technology, combined with pooling and automating all of the datacenter resources, Microsoft is able to provide an efficient and agile infrastructure for Therefore™ Online.

2.1.1 Defense in Depth

Defense-in-depth is a security best practice and it is an approach Microsoft uses across their cloud services and infrastructure. Applying controls at multiple layers can involve sometimes employing overlapping protection mechanisms, developing risk mitigation strategies, and responding quickly and effectively to attacks when they occur. Using multiple security measures of varying strength—depending on the sensitivity of the protected asset—results in improved capacity to prevent breaches or to lessen the impact of a security incident.

Microsoft assesses and addresses every part of the service stack – from the physical controls, to encrypting all data that moves over the network, to locking down the host servers, to keeping malware protection up-to-date, to ensuring applications themselves have appropriate safeguards in place. Maintaining a rich set of controls and a defense-in-depth strategy ensures that if any one area should fail, there are compensating protections in other areas.

Just in Time and Just Enough Administration is an important part of Microsoft's approach. This technology enables organizations to present operators with only the amount of access required to perform specific tasks.

In addition, Microsoft has built unique assets in their Digital Crimes Unit and Malware Protection Center—the work they are doing around the cloud ecosystem is continuously applied to protecting customers and their data.

2.1.1.1 Security Incident Response

An important part of Microsoft’s security capabilities include their response processes. The Security Incident Management (SIM) team responds to potential security issues when they occur, operating around the clock. The SIM processes are aligned with ISO/IEC 18044 and NIST SP 800-61.

There are six phases to the SIM incident response process:

- **Preparation** – SIM staff undergo ongoing training to be ready to respond quickly and effectively when a security incident occurs.

- **Identification** – looking for the cause of an incident, whether intentional or not, often means tracking the issue through multiple layers of the Microsoft cloud computing environment. SIM collaborates with members from internal Microsoft teams to diagnose the origin of a given security incident.
- **Containment** – once the cause of the incident has been found, SIM works with all necessary teams to contain the incident. Containment methods are based on the business impact of the incident.
- **Mitigation** – SIM coordinates with relevant product and service delivery teams to reduce the risk of incident recurrence.
- **Recovery** – continuing to work with other groups as needed, SIM assists in the service recovery process. This phase often includes suggestions and recommendations for additional monitoring and penetration testing to validate mitigation efficacy.
- **Lessons learned** – after resolution of the security incident, SIM convenes a joint meeting with all involved personnel to evaluate the event and to record lessons learned during the incident response process.

2.1.2 Infrastructure Protection

Microsoft Azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical data centers that house it all. Azure addresses security risks across its infrastructure.

Physical security: Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

Monitoring and logging: Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Update management: Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure uses a combination of Microsoft and third-party scanning tools to run OS, web application, and database scans of the Azure environment.

Antivirus and antimalware: Azure software components must go through a virus scan prior to deployment. Code is not moved to production without a clean and successful virus scan. In addition, Microsoft provides native antimalware on all Azure VMs. Customers can install Microsoft Antimalware for Cloud Services and Virtual Machines or another antivirus solution on VMs, and VMs can be routinely reimaged to clean out intrusions that may have gone undetected.

Penetration testing: Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of their customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their own—and only their own—applications hosted in Azure.

DDoS Protection: Azure has a defense system against Distributed Denial-of-Service (DDoS) attacks on Azure platform services. It uses standard detection and mitigation techniques. Azure's DDoS defense system is designed to withstand attacks generated from outside and inside the platform.

2.1.3 Network Protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Because Azure's shared infrastructure hosts hundreds of millions of active VMs, protecting the security and confidentiality of network traffic is critical. In the traditional datacenter model, a company's IT organization controls networked systems, including physical access to networking equipment. In the cloud service model, the responsibilities for network protection and management are shared between the cloud provider and the customer. Customers do not have physical access, but they implement the logical equivalent within their cloud environment through tools such as Guest operating system (OS) firewalls, Virtual Network Gateway configuration, and Virtual Private Networks.

Network isolation: Azure is a multitenant service, meaning that multiple customers' deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

Virtual networks: A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks.

VPN and Express Route: Microsoft enables connections from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs. For even better performance, customers can use an optional ExpressRoute, a private fiber link into Azure data centers that keeps their traffic off the Internet.

Encrypting communications: Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises data centers. More information on the provisions specifically related to Therefore™ Online can be found in the Data Security section.

2.1.4 Data Protection

Azure allows customers to encrypt data and manage keys, and safeguards customer data for applications, platform, system and storage using three specific methods: encryption, segregation, and destruction.

Data isolation: Azure is a multitenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware.

Protecting data at rest: Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily and cost effectively streamline key management and maintain control of keys used by cloud applications and services to encrypt data. More information on the provisions specifically related to Therefore™ Online can be found in the Data Security section.

Protecting data in transit: For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS between devices and Microsoft datacenters, and within datacenters themselves. More information on the provisions specifically related to Therefore™ Online can be found in the Data Security section.

Encryption: Customers can encrypt data in storage and in transit to align with best practices for protecting confidentiality and data integrity. For data in transit, Azure uses industry-standard transport protocols between devices and Microsoft datacenters and within datacenters themselves. You can enable encryption for traffic between your own virtual machines and end users. More information on the provisions specifically related to Therefore™ Online can be found in the Data Security section.

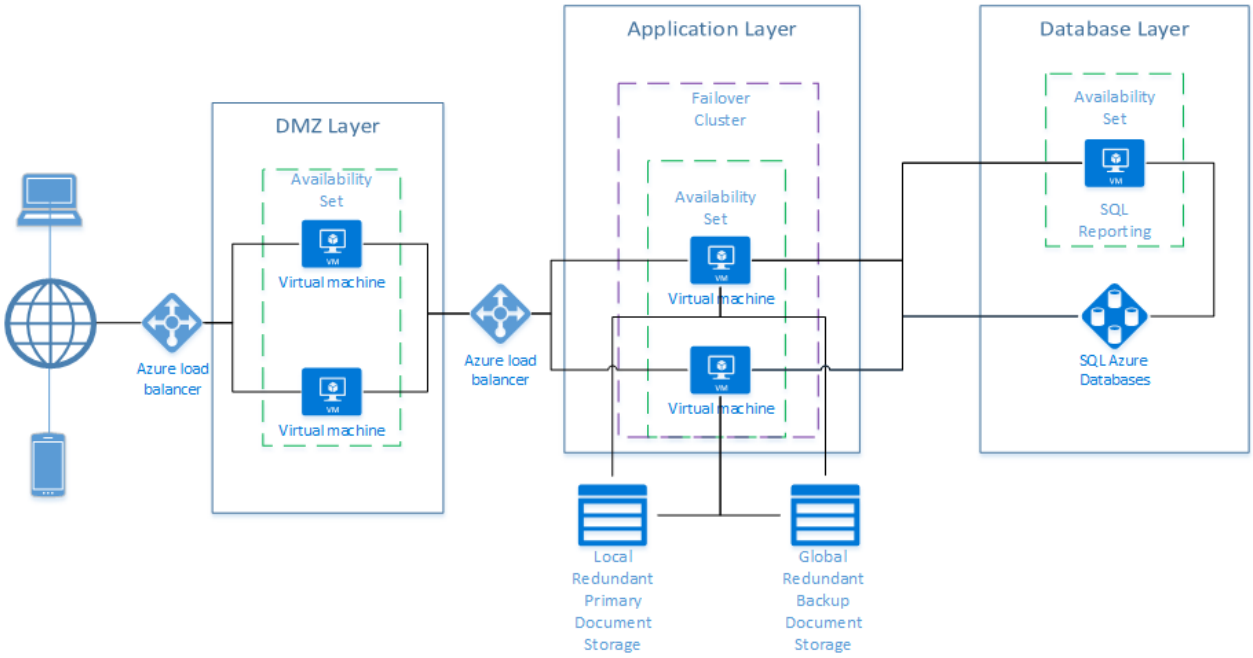
Data redundancy: Data may be replicated locally, or within a selected geographic area for redundancy.

2.2 The Virtual System

Virtualization technology is the underpinning of the Microsoft Azure platform and Therefore™ Online's architecture. Therefore™ Online is a highly suitable system to offer as a hosted service due to its multi-tenant capability. A single instance of the software running on a server in the datacenter can be securely provisioned amongst multiple client organizations, enabling them to operate in their own customized virtual application space. This configuration also has the additional benefit of allowing security updates and software upgrades to be centrally managed by Therefore Corporation.

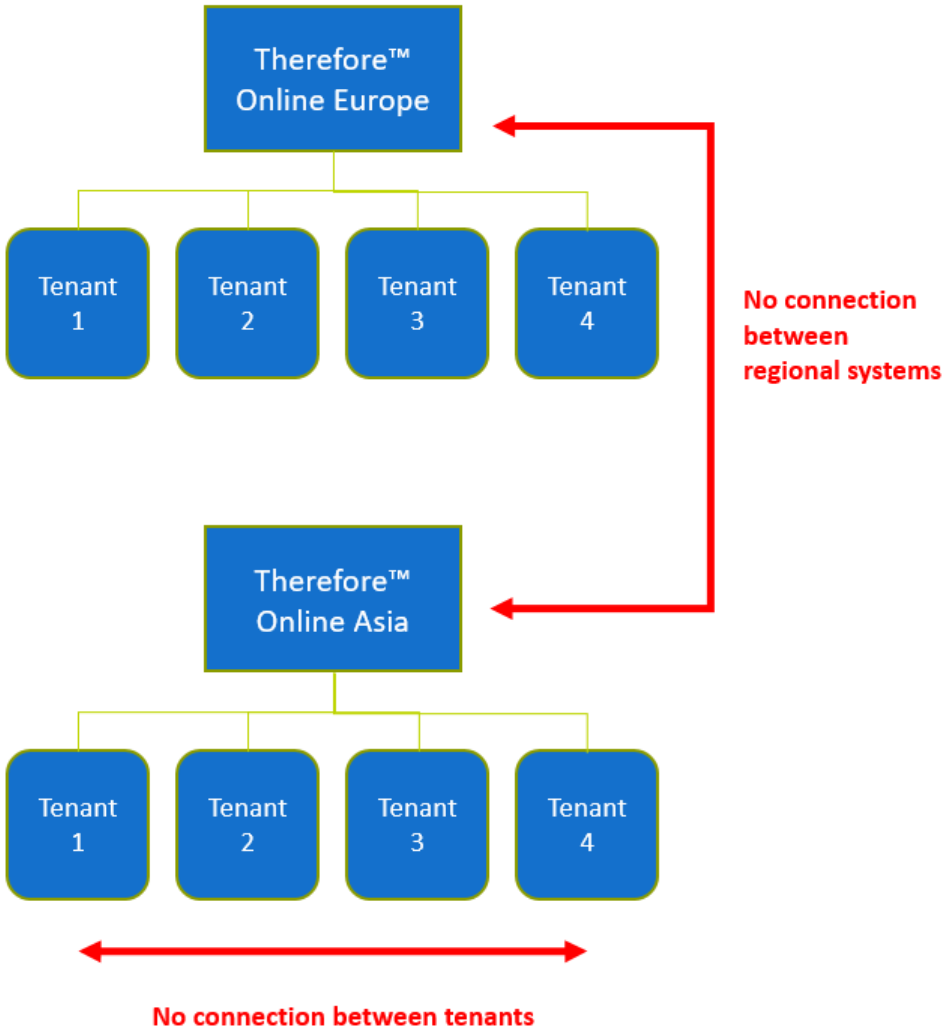
The virtual machines are hosted in virtual containers, also known as virtual systems. These virtual systems have been optimally designed for use with Therefore™ Online, incorporating high resilience and strict security measures, to provide a secure and stable environment. All data transferred between a virtual machine and a Therefore™ Online user is protected. System data is fully encrypted. Azure SSE (Storage Service Encryption) is used to encrypt data at rest using 256-bit AES encryption, one of the strongest cyphers available. In transit, data is encrypted using HTTPS and SMB 3.0.

The Therefore™ Online virtual system architecture is constructed as a three-layer system protected by a firewall. The first layer, or Demilitarized Zone (DMZ), is for front end web services, which are load balanced for optimum web performance. These VMs run on Microsoft™ Windows 2016 Server. The second layer is dedicated to the Therefore™ Server. Two virtual machines are available in a failover cluster, which ensures high availability as the system will seamlessly switch to the other VM should one fail. The third layer consists of a virtual machine running the SQL Reporting Service and the SQL Azure Databases. This configuration emulates conventional hardware architecture, where the DMZ acts as a buffer to the internal segment housing the virtual machines, safeguarding it from direct access to the internet.



2.2.1 Tenant Structure

Therefore™ Online uses multi-tenancy technology to provide a cloud-based version of Therefore™ running on the Microsoft Azure cloud platform. Tenants are completely separate. A tenant's data is only accessible to that tenant's users. Each tenant belongs to the main regional Therefore™ Online system. There are no sub-tenants.



3. The Datacenters

The facilities hosting Therefore™ Online are located within different regional datacenters throughout the world. Within each region, data is copied to both datacenters to ensure redundancy in case of large-scale accessibility failures at one of the locations. Data stays within the customer's region is never transferred to another region. For example, a U.S.-based customer's data will always remain within the two Americas datacenters, while a Europe-based customer's data will always remain within the two Europe datacenters.

Europe:
The Microsoft Azure datacenters for the Europe Therefore™ Online system are located in the Netherlands and the Republic of Ireland.

Americas:
The Microsoft Azure datacenters for the Americas Therefore™ Online system are located in the United States (Iowa and Virginia) and Canada (Toronto and Quebec City).

Asia:
The Microsoft Azure datacenters for the Asia Therefore™ Online system are located in Singapore, Hong Kong, Central India (Pune) and South India (Chennai).

Australia:
The Microsoft Azure datacenters for the Australia Therefore™ Online system are both located in Australia (New South Wales and Victoria).

3.1 Certifications

Microsoft Azure meets a broad set of international as well as regional and industry-specific compliance standards, such as ISO 27001, FedRAMP, SOC 1 and SOC 2. Azure's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations.

Comprehensive, independently verified compliance: Azure is designed with a compliance strategy that helps customers address business objectives and industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Microsoft Azure offers the following certifications for all in-scope services.

CDSA: The Content Delivery and Security Association (CDSA) provides a Content Protection and Security (CPS) standard for compliance with anti-piracy procedures governing digital media. Azure passed the CDSA audit, enabling secure workflows for content development and distribution.

CJIS: Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy. Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy, which commits Microsoft to adhere to the same requirements that law enforcement and public safety entities must meet.

CSA CCM: The Cloud Security Alliance (CSA) is a nonprofit, member-driven organization with a mission to promote the use of best practices for providing security assurance within the cloud. The CSA Cloud Controls Matrix (CCM) provides detailed information about how Azure fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2, and is published in the CSA's Security Trust and Assurance Registry (STAR).

FDA 21 CFR Part 11: The US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 lists requirements for the security of electronic records of companies that sell food and drugs manufactured or consumed in the United States. The compliance reports produced by Azure's independent third party SSAE and ISO auditors identify the procedural and technical controls established at Microsoft and can be used to satisfy the requirements of CFR Title 21 Part 11. Microsoft is able to show how relevant controls within these reports have an impact on compliance with the FDA 21 CFR 11 regulations.

FedRAMP: Azure has been granted a Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) at a Moderate impact level based upon the FIPS 199 classification. FedRAMP is a US government program that provides a standard approach to security assessment, authorization, and monitoring for cloud services used by federal agencies and thereby saves the taxpayer and individual organizations the time and cost of conducting their own independent reviews.

FERPA: The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of student educational records. Microsoft agrees to use and disclosure restrictions imposed by FERPA.

FIPS 140-2: Azure complies with the Federal Information Processing Standard (FIPS) Publication 140-2, a US government standard that defines a minimum set of security requirements for products and systems that implement cryptography.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

IRAP: Azure has been assessed against the Australian Government Information Security Registered Assessors Program (IRAP), which provides assurance for public sector customers that Microsoft has appropriate and effective security controls.

ISO/IEC 27018: Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

ISO/IEC 27001/27002:2013: Azure complies with this standard, which defines the security controls required of an information security management system.

MLPS: Multi-Level Protection Scheme (MLPS) is based on the Chinese state standard issued by the Ministry of Public Security. Azure operated by 21Vianet adheres to this standard, which provides assurance for both the management and technical security of cloud systems.

MTCS: Azure has achieved Level-1 certification with the Multi-Tier Cloud Security Standard for Singapore (MTCS SS), a cloud security standard covering areas such as data security, confidentiality, business impact, and operational transparency, developed under the Singapore Information Technology Standards Committee.

PCI DSS: Azure is Level 1 compliant with Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0, the global certification standard for organizations that accept most payments cards, as well store, process, or transmit cardholder data.

SOC 1 and SOC 2: Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements. The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.

TCS CCCPPF: Azure operated by 21Vianet is among the first cloud providers in China to pass the Trusted Cloud Service certification developed by the China Cloud Computing Promotion and Policy Forum (CCCPPF).

UK G-Cloud: The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received OFFICIAL accreditation from the UK Government Pan Government Accreditor.

The most up-to-date list of Azure compliance offerings can be found on Microsoft's website: https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

4. Data Management

4.1 Data Security

Therefore™ Online has been designed with security as a primary focus.

Data Encryption
System data is fully encrypted. Azure SSE (Storage Service Encryption) is used to encrypt data at rest using 256-bit AES encryption, one of the strongest cyphers available. In transit, data is encrypted using HTTPS and SMB 3.0.

DMZ Layer
The DMZ layer is the only part of the system that can be accessed externally. No data is stored on the DMZ layer; it is used as a relay for sending/retrieving data from the application and database layers, where the data is stored. These layers cannot be accessed directly from the outside, for example by a hacker.

Secure Connections
To ensure maximum security, only secure connections are allowed when accessing the system.

HTTPS (Inbound Port: 443): Standard communication protocol.

FTPS (Inbound Port: 21 and 50,000 - 50,001): FTP over TLS file transfers for the Content Connector.

Secure Socket (Inbound Port: 8091): MFP file transfers.

Secure Network Design
Every virtual machine running in the system is protected by a firewall. Inbound from the Internet, Azure DDoS Protection helps shield against large-scale attacks against Azure. Public IP addresses (endpoints) are used to determine which traffic can pass through the cloud service to the virtual network. Native Azure virtual network isolation ensures complete isolation from all other networks and that traffic only flows through user configured paths and methods. These paths and methods are the next layer, where NSGs, UDR, and network virtual appliances are used to create security boundaries to protect the application deployments in the protected network.

4.2 Data Backup

All customer data is redundantly backed up in the datacenter as is standard with the Therefore™ Online service. Data is copied to multiple disks, so if one disk or even multiple disks fail, customer data remains intact in the datacenter. Customer databases are stored in SQL Azure, with redundancy systems handled by Microsoft's strict uptime and availability policies.

All data in Therefore™ Online is protected and backed up with both LRS (Locally Redundant Storage) and GRS (Globally Redundant Storage). Primary storage is LRS-enabled for the highest performance when saving and retrieving documents. Data saved to the primary storage is simultaneously replicated across 3 separate nodes, each of which are further replicated several times. On the other hand, backup storage is GRS-enabled. In this case, data is first saved in the primary datacenter, where it is replicated 3 times. Then the data is replicated asynchronously to the secondary datacenter, where it is also replicated three times. This highly redundant configuration ensures that dozens of copies of system data are continuously maintained across different secure storage locations. GRS-enabled storage guarantees that data remains protected even in the case of a complete regional outage or disaster in which the primary datacenter is not recoverable.

4.3 Data Migration

If requested, the customer can migrate all of their data into their sole possession, using the Therefore™ Export Utility. Whether it's to move the customer to the on-premise version of Therefore™, move to another document management solution, or upon completion of the customer's contract, the customer can migrate their own documents from Therefore™ Online. The XML meta file can also be migrated for use in importing meta data into a new system.

Upon completion of the customer contract and data migration to the customer, the tenant is deleted and all data is securely erased. Microsoft follows strict standards for overwriting storage resources before reuse, as well as physical destruction of decommissioned hardware.

5. The System - Therefore™ Online

Therefore™ Online is a full-featured information management solution, delivering state of the art software, from the cloud. In addition to providing intelligent information management, Therefore™ Online comes standard with workflow functionality, enabling organizations to optimize their business processes. The Therefore™ Online system and functionality are indistinguishable from its counterpart, the on-premise version of Therefore™. The only major difference between the on-premise and online version is the location of the customer's information. With Therefore™ Online, data is remotely stored in a highly protected datacenter, as opposed to being stored on-site at the customer's location.

Therefore™ Online is offered as a single edition, nearly identical to the Business and Enterprise Editions available with the on-premise version of Therefore™. It is subscription-based, with the option of choosing a monthly or yearly plan. Highly scalable and customizable, Therefore™ Online allows customers to make changes to the system as their business dictates. Customers can begin with just a single user license if they choose, and add as many as they need throughout the term of their contract.

Note: Emails from the Therefore™ system may have failed to send. Users may have seen error messages in the Therefore™ Solution Designer when trying to send a test email. This happened only to customers who had configured Therefore™ to send emails from a custom email address (by changing the "SMTP sender" in Therefore™ Solution Designer settings) rather than the default one (<tenantname>@thereforeonline.com).

Due to changes in security policy, changing the "SMTP sender" field to a custom email address is no longer allowed. In order to ensure an orderly transition, this feature will remain active until the 1st of March, but will deactivated for all tenants at that point. To continue sending emails from the Therefore™ system, two options are available:

1. Use the default "SMTP sender" (<tenantname>@thereforeonline.com) to send emails.
2. Configure Therefore™ to send emails using your own SMTP server. This can be configured in the Therefore™ Solution Designer: https://www.therefore.net/help/2020/en-us/sd_r_theobject_settings_general.html

If you want to use your own "From" address (SMTP sender) Therefore recommends using your own SMTP server to send emails. This allows you to keep using your own custom "From" email address while maintaining full control of your email domain and settings.

5.1 User Licenses

There are three types of user licenses available with Therefore™ Online:

- **Named User License:** this user license is specifically assigned to an individual employee for their use only. This type of license is ideal for a user who regularly needs access to the system.

- **Concurrent User License:** this user license is shared among all users of the system (excluding those who have a Named User License). When a 'concurrent' user logs-on to the system, they essentially 'borrow' a license from the system server 'pool' and return the license (automatically) when logging off. When all available licenses are currently being used by other users, additional users will be denied access until an active user logs off and releases their license.

- **Read Only License:** this user license is designed for customers who would like to offer users very limited access to the documents in the Therefore™ repository. As the name suggests, the user will only be able to read or view the documents. Read only licenses are frequently used when Therefore customers wish to make Therefore documents available via a web portal (Therefore Web Access) to their own customers as part of a paid for service.

5.2 Additional Licenses

Additional types of licenses are also available with Therefore™ Online:

- **Capture Client License:** this license allows the Therefore™ Capture Client to be used to process paper or electronic information.

- **MFP Application License:** this license allows the Therefore™ MFP Application to be used together with a Canon ImageRUNNER or Canon imageRUNNER ADVANCE.

- **eCopy Application License:** this license allows a user to save documents directly from eCopy ShareScan into Therefore™.

- **Universal Connector License:** this license allows the use of the Therefore™ Universal Connector for integrating third-party applications with Therefore™. Only one license is needed system-wide.

- **Content Connector License:** this license allows the use of the Therefore™ Content Connector for importing electronic documents into Therefore™. Only one license is needed system-wide.

- **Portal License:** this license allows the use of the Therefore™ Portal for granting access to information to external parties. Only one license is needed system-wide.

- **Exchange Connector License:** this license allows the use of the Therefore™ Connector for Microsoft Exchange Server for integrating Microsoft Exchange with Therefore™. Only one license is needed system-wide.

5.3 Configuration and Security

Therefore™ Online employs a multi-tenancy architecture, meaning there is a single instance of software installed and running on a server, which serves multiple client organizations, called "tenants". Utilizing multi-tenant architecture, Therefore™ Online is designed to virtually partition its data and configuration, so that each client organization works in a customized virtual application, completely independent from another tenant.

Additional security measures can be implemented on the client side, by the administrator, in the Therefore™ Solution Designer. The administrator of the system can restrict user/group rights and permissions to specific 'Categories' of documents (for example the admin. can deny access, allow read, allow annotate, allow modify, etc.) or even deny access to documents based upon the values in some specific Index field (such as 'Owner' or 'Salary').

Therefore™ Online also has built in Version Control (all old versions of a document are saved and can be accessed) and can maintain a complete Audit Trail of all user activity and document access. This allows its use in secure application areas where access to documents must be monitored and controlled.

5.4 Core Applications

5.4.1 Therefore™ Solution Designer

The Therefore™ Solution Designer is the main application for the administration of a Therefore™ system. This is where the administrator(s) can manage the various components that comprise the system, including user/group permissions, category/folder creation, document retention policies and workflow design, among other system configurations.

5.4.2 Therefore™ Console

The Therefore™ Console application is an administration tool-set that allows the monitoring of status and events occurring on the Therefore™ Server. It does so by linking to the Therefore™ Server Service, which is the central controlling service of the Therefore™ Information Management System. All user activity, all access to media, and the migration of documents to archive storage media is controlled by this service. Therefore™ Online also provides an Audit Trail feature, accessible from the Console, for auditing users, documents and workflows.

5.4.3 Therefore™ Navigator

The Therefore™ Navigator is a tool for searching and retrieving documents saved to Therefore™ Online. It also manages workflow process tasks, and is the starting point for users to display and edit documents in the Therefore™ Viewer. The primary function of the Navigator is to find and retrieve the information a user is seeking. There are a variety of search methods available, which can be chosen depending on the method most convenient for the user.

5.4.4 Therefore™ Viewer

The Therefore™ Viewer is used for displaying and editing documents that have been saved to Therefore™ Online. The Viewer enables you to view, print or annotate documents created in over 400 file formats, even if the user does not have the document's native application installed on their PC. However, if the user wishes to make revisions to a document, the document's native application must be installed locally, in order to make edits using the native applications inherent functionality.

5.4.5 Therefore™ Capture Client

The Therefore™ Capture Client is used to scan and save documents to Therefore™ Online. It is typically used with a document scanner, although it can also be used to import documents from a hard disk. The Capture Client allows for customized settings to be defined in a Profile, which can automatically apply image enhancement settings, assign a category, capture index data via barcodes or OCR, and split pages into separate documents when batch scanning.

6. Technical FAQ

This section contains a list of the most frequently asked technical questions about Therefore™ Online.

What are the system requirements and/or bandwidth requirements?

When performing system actions from a client, internet access is required. A standard broadband connection is the minimum recommended, though faster connections will generally yield better system performance. A loss of internet connection will not cause data to be lost when it is at rest. Simply reconnect once the internet connection is reestablished.

What are the client requirements?

Therefore™ client OS: Windows 10, 8.1, and 7 SP1

Therefore™ Web Access browsers:

- Microsoft Edge
- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Opera
- Safari

Does Therefore™ Online require a constant internet connection?

Yes, an internet connection is required to perform most system actions.

Do I need any special software to access Therefore™ Online?

No. All normal Therefore™ client applications, including web, mobile, and MFP connections, will work with Therefore™ Online.

Where/how is the data stored?

Both documents and metadata are stored in the regional datacenter. All data is backed up in the local datacenter and the backup datacenter, in a different geographic location.

How does ADFS Single Sign-On work with Therefore™ Online?

Please refer to the document "ADFS Single Sign-On with Therefore™ Online", available on the Therefore Extranet or from your local Canon/reseller representative.

How do I integrate with a 3rd party database?

Please refer to the document "Best Practice to Connect to an External Database", available on the Therefore Extranet or from your local Canon/reseller representative.

Can I access the SQL database directly to create tables?

No, the customer has to use table replication to create a table.

How do I create my own SQL reports in Therefore™ Online?

We recommend creating reports in a local test or demo system first and then uploading them to Therefore™ Online via the Solution Designer.

How do I add an existing SQL report (.rdl) to Therefore™ Online?

The Therefore™ Solution Designer offers the functionality to import and export SQL reports. This is also available for Therefore™ Online.

Can I change SMTP server settings to my own/my customer's email server?

Yes, every tenant is created with preconfigured SMTP settings, but these can be changed to use your own SMTP server.

Which ports need to be opened for the Therefore™ MFP App?

443 and 8091

How do I configure access to the Therefore™ Mobile App in Therefore™ Online?

The connection details are included in the tenant creation notification sent to the responsible technician.

How do I restart the Therefore™ services?

Therefore™ Online customers cannot restart the Therefore™ services, as this is never required from their side. They can restart their own tenant via the Therefore™ Console.

How do I integrate with a 3rd Party ERP?

Depending on the type of the integration, there are several different options such as: WebAPI, API, and Table Replication. Contact your local technical resource for more information.

Can Therefore™ Online integrate with Office 365? How do I save documents in Office365 to Therefore™ Online?

Therefore™ Online can integrate with a local installation of Office 365 through the standard Therefore™ integration for Microsoft Office. However, this integration does not work with browser-based Office 365 applications like Word Online, PowerPoint Online,etc.

Does each tenant have its own database server or are all tenants on a single database server but with an allocated database instance?

Each tenant has its own database, but the tenants share SQL servers.

How can I upload documents from a Therefore™ on-premise server to Therefore™ Online?

Documents in a Therefore™ on-premise server can be exported with the Therefore™ Export Utility and then imported into Therefore™ Online with the Therefore™ Document Loader.

How do I upload documents to Therefore™ Online with the Therefore™ Content Connector?

The Content Connector can monitor a folder on an FTP server and then save documents uploaded to this folder to Therefore™ Online. Here's how it works:

- Documents are uploaded to the Therefore™ Content Connector using an FTP connection. Connection details and credentials are provided by Therefore Corporation when a Content Connector license is activated on a Therefore™ Online system.
- Each tenant is restricted to one FTP account to use for uploading files to the Therefore™ Content Connector.

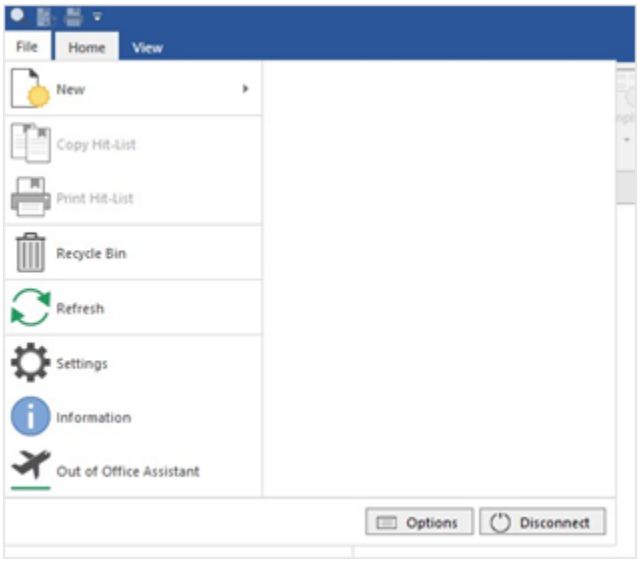
- Auto-uploading documents from a local server to the Therefore™ Online FTP server can be achieved by using scripting for the WinSCP tool: https://winscp.net/eng/docs/scripting. Use of the WinSCP tool is at the customer's discretion; Therefore Corporation does not officially provide support for scenarios involving this tool.
- Alternatively, you can also use Cloud Storage in combination with Therefore™ Online. For example, you can use OneDrive without the need for an additional sync tool.

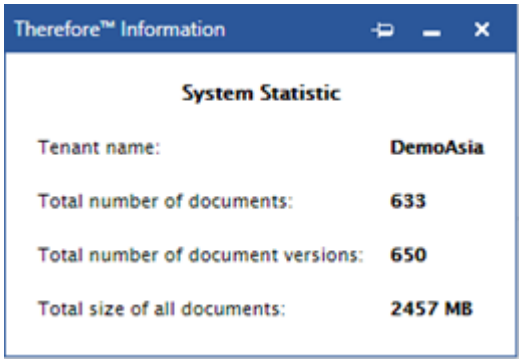
How do I import documents in cloud storage devices into Therefore™ Online?

The Therefore™ Content Connector can be used to monitor and download documents from cloud storage devices, and then import them into Therefore™. Please refer to online help for details: http://www.therefore.net/help/2018/en-us/sd_t_intergrations_contentconnector_savingcloudstorage.html

How do I check the storage utilization in Therefore™ Online?

Open Therefore™ Web Access (the Therefore™ web client in a browser), click on "File" then select "Information". This option is visible only to users with "Operator" permission.





Do I need any special training to sell, configure, or use Therefore™ Online?

No. If you already know how to sell, configure, or use a regular Therefore™ system, Therefore™ Online will be no different, other than making it easier for you to get started!