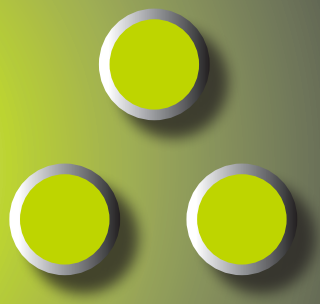
Therefore™ Online



White Paper: Information in the Cloud

Table of Contents

White Paper Objectives 2
Introduction 3
Architectural Overview 4
The Host – Fujitsu America 4
The Infrastructure – Reliability through Redundancy 4
The Virtual System 5
The Datacenter 7
Certifications 7
Facility Security 8
Data Management 9
Data Security 9
Data Backup 9
Data Migration 9
The System – Therefore™ Online 10
User Licenses 10
Configuration and Security 11
Applications 11
Therefore™ Solution Designer 11
Therefore™ Console 11
Therefore™ Navigator 12
Therefore™ Viewer 12
Therefore™ Capture Client 12
Conclusion 13

White Paper Objectives

Your information is the cornerstone of your organization, which requires the proper security and accessibility in order to conduct business effectively. With that philosophy in mind, we at Canon set out to offer our customers a highly secure, yet convenient way to intelligently manage their information, without the need to invest in costly IT infrastructure. With Therefore™ Online, you can easily and securely manage your information, from the cloud.

The purpose of this white paper is to layout the general framework and security measures implemented with Therefore™ Online. Our goal is to educate readers of all the actions taken in order to provide optimal performance and data security, when using the new cloud-based information management solution now distributed by Canon.

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 enables Canon to offer customers 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 by Fujitsu in the United States, rather than on the end user's on-site 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.

Architectural Overview

The Host – Fujitsu America

Therefore Corporation GmbH has partnered with Fujitsu America, Inc., a leading global IT service provider, to host the operations and infrastructure for Therefore™ Online. By utilizing the services of a professional datacenter, Canon is able to optimize the performance and security of Therefore™ Online. Customers can be assured that all of their data will be held within Fujitsu's datacenter located in the United States.

Fujitsu's IaaS (Infrastructure as a Service) platform, called *Fujitsu Cloud IaaS Trusted Public S5,* is the Fujitsu 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 the Fujitsu datacenter. By utilizing virtualization technology, combined with pooling and automating all of the datacenter resources, Fujitsu is able to provide an efficient and agile infrastructure for Therefore™ Online.

The Infrastructure – Reliability through Redundancy

Perpetual infrastructure uptime is essential for the legitimate operation of a professional cloud service. Downtime could affect a customer's ability to access its resources; therefore the appropriate measures must be implemented across all facets of the datacenter in order to mitigate the existence of any "single point of failure" and maintain high availability of the cloud service.

In order to provide consistent availability, Fujitsu has implemented a policy of full-redundancy throughout all of their datacenters. The Fujitsu facilities are comprised of large server rooms, located in separate fire sections throughout the datacenter, which are equipped with complete redundancy of all critical components. Servers, storage, network devices, power supply equipment, and cable routing, among other components, are completely redundant in order provide reliability and prevent any "single point of failure".

In the event of a component failure, such as a crash of a physical server hosting a virtual machine, automatic failover functions are instantly enabled, migrating the virtual machine from the failed server to an operational server. In fact, a failure does not even have to occur before a virtual machine is migrated to another physical server. When there are indications of pending physical problems on a particular server, all virtual machines are proactively allocated to other operational servers automatically. All services and information in the virtual machine's memory will be retained, and the end user is unaware that this failover and migration has even occurred.

In addition to a redundancy of servers, the storage element of the *Fujitsu Cloud IaaS Trusted Public S5* is also fully redundant. All data is stored in a RAID 5 configuration using Fujitsu ETERNUS Storage Array, and additional protection is provided using mirroring between storage cabinets. The data is mirrored to separate disk arrays before management software uses "data-striping" to randomize data location. If a single disk, volume, disk tray or entire array is lost, a user's data is still completely intact and accessible. All data saved in physical storage is protected by a secure encryption scheme equivalent to 128-bit Advanced Encryption Standard (AES).

FGCP Core Technologies

- Fujitsu PRIMERGY Servers
- Fujitsu ETERNUS Storage Array (RAID 5)
- Fujitsu SR-S / SR-X Gb Network switches
- Xen for Hypervisor
- Cisco ASR 1006 Internet Router & firewall

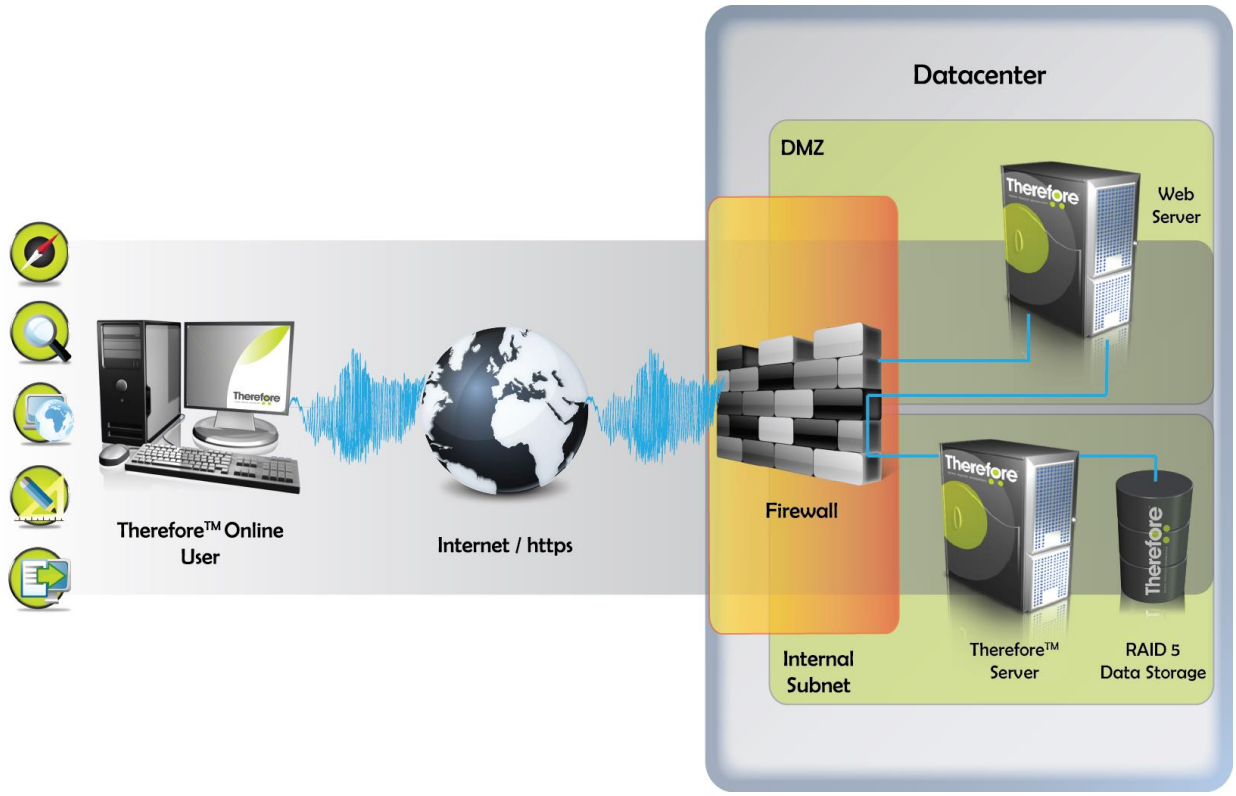
Network redundancy is also evident in the architecture of the *Trusted Public S5*, contributing to the overall reliability of the cloud service. VLAN technology controls the data path between the Eternus Storage Array and the Primergy Servers with resilience throughout and no single points of failure. If a switch, router, or cable fails, there will always be an alternative path in operation. Under-floor LANs are also fully redundant, as well as WAN network connections which are linked via two separate carriers.

The Virtual System

Virtualization technology is the underpinning of the *Fujitsu Trusted Public S5* platform and Therefore™ Online 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. Data is carried via HTTPS – which combines standard HTTP communication with SSL/TLS protocols. A Secure Site SSL Certificate, with an encryption rate equal to 128 bits is used for the encryption. HTTPS provides encrypted communication and secure identification typically used for online payment and sensitive corporate transactions.

The Therefore™ Online virtual system architecture is constructed as a two-tier system protected by a firewall, as shown in the diagram below. The first tier, or Demilitarized Zone (DMZ), is for front end web services, which are load balanced for optimum web performance. This runs on a Microsoft™ Windows 2008 web server with IIS set up as a virtual machine. The second tier is a secure internal subnet dedicated to the Therefore™ Server and Microsoft™ SQL database server, as well as the RAID 5 data storage array. By placing these components in a separate network segment, it provides an additional layer of security. 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.



Therefore™ Online Service Infrastructure

The Datacenter

The facility hosting Therefore™ Online is located within the United States, at Fujitsu's Sunnyvale, California datacenter. Every *Fujitsu Trusted Public S5* datacenter is designed and constructed to provide a highly resilient, highly secure environment that maximizes availability.

While it's important to have a secure physical and virtual environment, it's just as important to know whom you let into your environment. The *Fujitsu Cloud IaaS Trusted Public S5* is an enterprise-ready trusted public cloud service. This means that the cloud service, while shared with other organizations, is not available to just anyone. The cloud service is only open to recognized organizations, not to individuals. Registration and acceptance to the *Trusted Public S5* is limited to registered companies, charities, and public sector organizations.

Acceptance is contingent upon meeting specific criteria, including an identity and credit check. This level of screening helps to further protect the cloud environment from unethical organizations and malicious activity.

Certifications

Fujitsu's Sunnyvale facility is a Tier III rated datacenter, certified Gold for both design and operation. It provides an annual service availability rate of 99.95%.

The datacenter is HIPPA certified, as well as, ISO9001 certified, which meets high standards for quality management systems.

Datacenter Specifications

- Location – Sunnyvale, CA
- Power Density – 100W per sq. ft.
- Power Resiliency
  - 8 x 750 kVA UPS (N+1)
  - 1 x 1000 kVA & 4 x 1500 kVA generators (N+1)
  - A/B/C/D distributed load power to the racks
  - 1 x 235 kVA Hydrogen Fuel Cell (Clean Energy)
- Power Capacity
  - Utility – 5.5 MW
  - Generator – 6MW (4.5MW N+1)
- Cooling
  - 3 x 900 ton & 1 x 650 ton water based chillers with dual path cooling (N+1)
  - In-room ducted CRAC units with plenum return (hot isle/cold aisle)
  - Roof-top air-side economizers
- Monitoring & Management
  - Air-conditioning & humidity Halogen-gas
  - Fire sprinkler & leak detection systems
  - CCTV cameras & card reader access points
  - Siemens Building Management System (BMS)
  - Advanced power monitoring & management system
  - CCTV throughout facility
- Physical Security
  - Security zones & multi-layered authentication
  - Two or Three factor identity authentication
- Communications
  - Multiple Fiber circuits with multiple carriers (OC12s and OC192)
  - Redundant fiber paths

It also holds the ISO27001, which is the international standard for Information Security Management Systems. This certification defines industry best practice for security management, and certification is only awarded after rigorous independent audit.

In addition, the datacenter is annually audited in accordance with the Statement of Auditing Standards No.70-Type II (SAS70-Type II) by a third party auditing firm.

The datacenter is also subject to annual Payment Card Industry Data Security Standard (PCI DSS) inspection with diagnosis of Internet connection environment vulnerabilities. This is carried out regularly in order to ensure adherence to PCI DSS requirements.

Facility Security

All Fujitsu datacenters are managed 24 hours a day, 7 days a week, 365 days a year, by highly experienced and trained operations staff. Fujitsu implements a spectrum of security technologies at all of their datacenters, in order to maintain the integrity of the facility. 24-hour onsite security controls, integrated Building Management, perimeter security controls, as well as Security and CCTV systems are just some of the security measures implemented. Digital surveillance is employed throughout the datacenter to prevent unauthorized access, including biometric access points in conjunction with proximity card readers, for all employees.

The biometric access points consist of palm vein authentication devices, which use palm vein patterns to authenticate authorized personnel from entering secure sections of the datacenter. This biometric authentication is used in combination with Radio Frequency Identification (RFID) tags that are assigned to every datacenter employee. The RFID tags not only provide an additional layer of authentication into secure sections of the facility, but also track the location of every employee within the facility. Employees have specific restrictions imposed on the sections, server rooms, racks, and other locations within the datacenter that they can access, by way of predefined privileges according to their roles. Tailgating detection technology is also instituted throughout secure access areas of the datacenter, which help prevent unauthorized persons from entering or leaving restricted areas by closely following (tailgating) employees that do have access.

In addition to all of the security measures described above, CCTV surveillance video is also present at all access points. The video surveillance records the entering and leaving of rooms, the locking and unlocking of racks, determines employee/visitor location, and other necessary security information, which is collected and archived for a predetermined time on a dedicated server.

Data Management

Data Security

Customer data is protected throughout all processes and locations which it resides, using a number of different encryption methods respectively. At its resting state, when data is stored within the Fujitsu ETERNUS Data Storage Array, it is encrypted using a custom encryption scheme equivalent to 128-bit Advanced Encryption Standard (AES). This encryption helps ensure the integrity of the data, by preventing it from being decipherable in the unlikely event that an unauthorized person accesses the storage array.

Customer data is also protected while in transit. When a Therefore™ Online user is accessing their system, they are communicating with a web server and associated virtual machine located in the datacenter, via the Internet. In order to protect this communication, all data is carried using HTTPS protocol. HTTPS combines standard HTTP communication with SSL/TLS protocols, providing not only website authentication, but also bidirectional encryption of communications between a client and server. That communication is further protected by a dedicated firewall, configured to only allow authorized users access to the virtual machine.

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 using RAID 5 configuration, so if one disk or even multiple disks fail, customer data remains intact in the datacenter. Customer databases are also copied to multiple disks, so in the event of a system disk failure, the Therefore™ virtual machine would be immediately restored as well as the database, maintaining system availability.

Data Migration

If requested, the customer can have all of their data migrated 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, all documents will be migrated back to the customer. 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, all data is securely erased by Fujitsu using the "zero write" method. This method consists of overwriting all of the data regions that had been used, once a customer virtual system is returned and when physical storage is discarded.

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, virtually identical to the Enterprise Edition 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.

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.

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.

Core Applications

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.

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.

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.

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.

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.

Conclusion

Cloud computing technology continues to grow in both consumer and business markets alike, and we at Canon aim to provide our customers with the option of utilizing such technology in order to advance their business.

Canon and Therefore Corporation, in partnership with Fujitsu America, are proud to offer this new format of information management solution, Therefore™ Online, for customers that wish to take advantage of the benefits of cloud computing. We hope this white paper addresses any potential concerns you might have about cloud computing and information management, as well as clearly illustrates all of the measures taken to keep your information protected.