Online Services Security v2.1

Contents

1 Introduction

At Canon, security is at the heart of what we do; our products and services are implemented using robust and tested security technologies to provide the most secure services to our partners and customers.

This document outlines Canon's security for Online Services that are hosted using Canon's Cloud platform. It defines how applications and customer data are managed, the protection controls used to give well-defined identity & access management and data transmission & encryption. An overview of the network design and management is also provided.

2 Cloud Infrastructure

In order that we bring the power of the Cloud to your business, Canon partners with the best Cloud providers to ensure that you are provided with fully enabled Cloud services that support your business needs.

Our partners are certified to the highest industry security standards to offer you the assurance that rigorous internal standards are used for maximum security. From inception, every service has been designed and built with Canon Europe IT and Canon Europe Information Security Department teams using our internal standards to ensure full compliance with our robust security and design principles.

2.1 Data Centre Locations

Canon's Cloud platform is managed in Belgium with datacentres located in France. No checks are in place for Client data in transit.

Should there be the need to locate data in-country, further discussion would be required and additional cost would apply.

2.2 Data Centre Compliance

The Data Centres used to support our service are compliant with number of standards, including those relevant for Canon's Online Services:

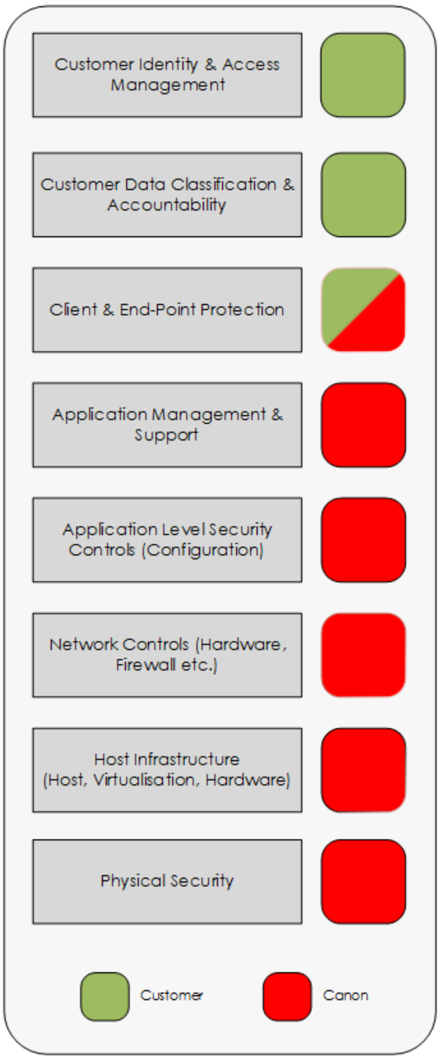
- ISO27001
- ISAE3402/SSAE16 SOC1 (underlying Cloud solution is audited to ISAE3402)
- T Section 101 SOC2

2.3 Roles and Responsibilities

We operate under a shared security responsibility model where, working with our Cloud provider, there is responsibility for physical data centre security, virtualization layer, hardware security and Operating System security, including secure configuration and anti-virus.

It is expected that the customer takes responsibility for the management of users accessing the service and the protection of the client endpoint devices used.

The figure to the right gives a more detailed breakdown of this shared security responsibility approach.



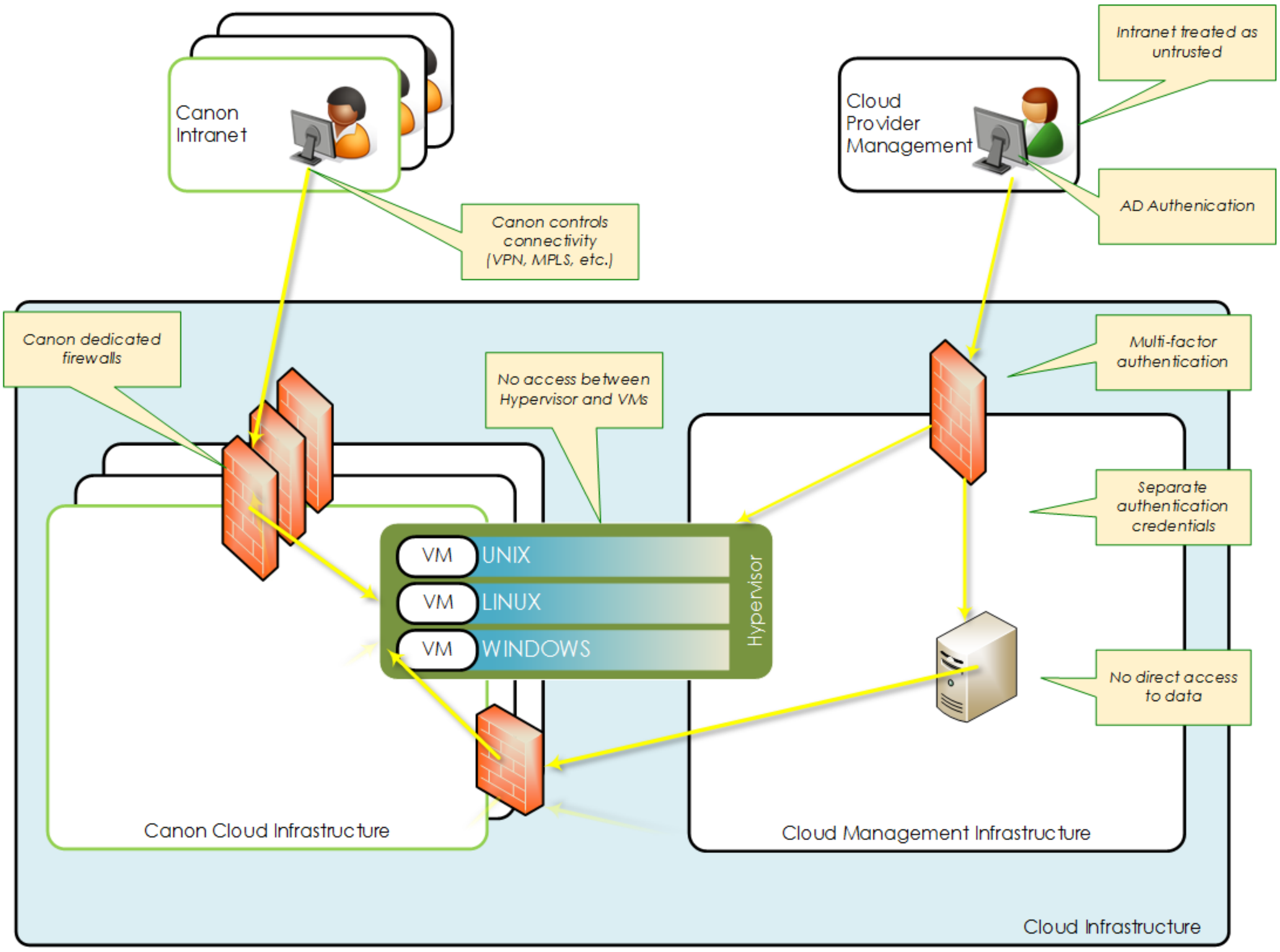
Customer Identity & Access Management	🟩
Customer Data Classification & Accountability	🟩
Client & End-Point Protection	🟩🟥
Application Management & Support	🟥
Application Level Security Controls (Configuration)	🟥
Network Controls (Hardware, Firewall etc.)	🟥
Host Infrastructure (Host, Virtualisation, Hardware)	🟥
Physical Security	🟥

🟩 Customer 🟥 Canon

3 Network Security

3.1 Network Setup & Access Points

Access to the Canon Cloud platform is stringently controlled to ensure relevant security levels are implemented. Please refer to the figure below for an overview of the network setup and access points.


Canon Intranet
Cloud Provider Management
Intranet treated as untrusted
AD Authenication
Canon controls connectivity (VPN, MPLS, etc.)
Canon dedicated firewalls
No access between Hypervisor and VMs
Multi-factor authentication
Separate authentication credentials
VM
UNIX
VM
LINUX
VM
WINDOWS
Hypervisor
No direct access to data
Canon Cloud Infrastructure
Cloud Management Infrastructure
Cloud Infrastructure

The diagram above shows the paths and separation used to provide management of the underlying infrastructure. Support personnel accessing the management infrastructure is logged.

3.2 Network Security Features

The Canon Cloud service has been designed in such a way to offer the following security features:

- Use of dedicated Virtual Local Area Networks (VLANs)
- Security zoning with DMZ in place
- Logical segmentation of subnets
- Controlled routing principles
- LIS (Leveraged Internet Services) for controlled exposure to the Internet
- Load balancers (global)
- Uptime and performance that is optimised

A single network compartment is used with data separation provided by zoning to control data accessibility protected by firewall rules. Logical separation and isolation of individual network traffic reduces the risk of customer data being exposed to unauthorised access during transport across the infrastructure. Dedicated server operating system instances within the dedicated virtual networks separate Canon environments.

Network Intrusion Detection and Network Intrusion Prevention (NIDS/NIPS) services inspect all public Internet traffic to the Cloud infrastructure. Industry-standard attack filters are deployed to detect, report and block known network security threats before harm can be affected to the infrastructure.

Default passwords on managed systems and equipment used to provide services are changed when placed into production.

A vanilla operating system image is installed into the Managed Server infrastructure to run a hardening script which adjusts the configuration to a predefined hardened state to force effective settings, patch levels and active services. Any changes to this configuration are managed through a Change Request.

Periodic penetration testing of the management infrastructure is performed at least once per calendar year. Periodic assessments or audits of the Canon Cloud environment are performed.

Patches are applied as deemed necessary by Canon and our hosting partner.

3.3 Zoning & Firewalls

Security for the Canon Cloud infrastructure is primarily done through network segmentation controlled by firewalls. A four-tier zoning system is in place, featuring the following properties:

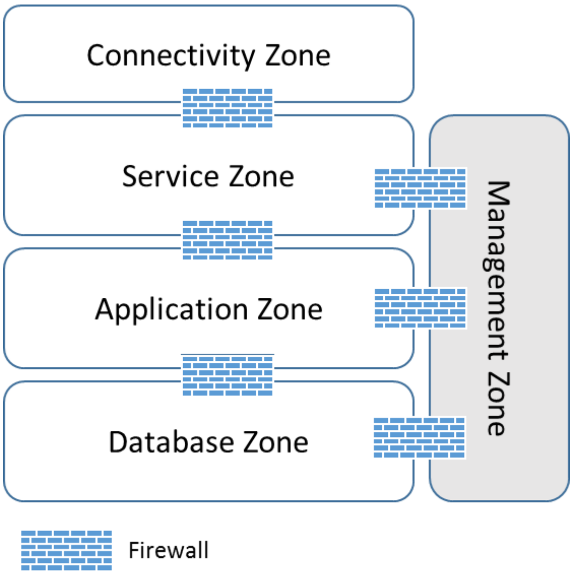
- Connectivity zone: this is the only zone that allows for external connections into the compartment.

- Service (DMZ) zone: this zone contains outer facing systems providing an additional layer of security for Internet facing connections.

- Service (Semi Trusted) zone: contains outer facing application servers such as application and web servers.

- Database (Trusted) zone: is reserved only for data and internal systems such as databases. This is where customer data is stored.

- Management zone: provides management and IT infrastructure services such as identity management.



This zoning design ensures that customer data is protected with the most appropriate level of security possible within the network environment.

Any environments that are created in the network above are also subject to DTAP classification (Development, Test, Acceptance, Production) to ensure the integrity of the environments in which customer data is stored/processed is maintained.

4 Server Security

4.1 Authentication Controls

Access controls are applied to the Cloud infrastructure, allowing only authorised designated users. Customer access rights will be implemented for local server accounts based upon Canon requests.

Restricted administrative access to the Cloud environment is accomplished by verifying authorised users' identities with multi-factor authentication to reduce the risk of inappropriate access. Actively managed processes and tools are used to enforce system policy compliance.

4.2 Storage Features

Industry standard storage strategies and controls are used to secure data in the Storage Area Network so that the Canon service is restricted to the allocated storage.

As per the standard service offered, the following security features are available for storage:

- Fibre channel based SAN with SAN zoning to prevent communication across the fabric and LUN masking
- Disk storage scrubbed with multi-pass overwrite (3 passes)
- Resilience across dual data centres

Securely erase data before reuse of media and securely dispose of media that is physically decommissioned and not reused.

4.3 Data Encryption

Data encryption in the Canon Cloud environment is available at the backup level. The SAN storage environment ensures that customer data is segregated and cannot be shared between customers. The network setup described in **3 Network Security** outlines the additional measures that are in place to protect data.

4.4 Backup Schedules

Backup schedules that apply are as follows:

- Incremental daily backups of files (excluding databases) using on-site virtual storage technology
- Weekly full backups of files (excluding databases) using on-site virtual storage technology
- Retention of on-site file backups for fifteen (15), thirty (30) or forty-five (45) days; and
- Upon request, restoration of files from on-site backups.

To protect and restrict access to data stored on tape media, encryption is used with personnel needing unique IDs where technology permits.

4.5 Malware Protection

Anti-virus

- McAfee anti-virus protection is provided for servers

Malware Protection

- Malware protection provided for servers

OS Hardening Scripts

- Pre-hardened OS images are installed on all servers

4.6 Physical & Personnel Security

The weakest link in the security chain is always the people you trust: personnel, development staff, vendors, essentially anyone that has privileged access to your system. Our holistic security approach attempts to minimize security risk brought on by the "Human Factor".

Information is divulged only on a ‘need-to-know’ basis with authorisation expiring upon the expiry of the requirement. Having a clear and well defined incident reporting process shall prevent threats to propagate and to reoccur.

The data centres are operated in accordance with best practices, including:

- Access control by key card or biometric scanner
- Site monitoring includes indoor/outdoor video surveillance and on-site security personnel on a 24 by 7 basis
- Redundant power and cooling infrastructure
- Diverse network access points
- ITIL-based operations