Canon
CANON SOLUTIONS AMERICA

Canon Office Cloud

SECURITY WHITE PAPER

CANON OFFICE CLOUD

A FedRAMP-authorized Service

SMART CHANGE STARTS HERE.

TABLE OF CONTENTS

INTRODUCTION

The Federal Risk and Authorization Management Program, FedRAMP, promotes the adoption of secure cloud services across the U.S. government, providing a standardized approach to security assessments for cloud service offerings. FedRAMP's guiding principle is re-use: do once, use many times. This saves money, time, and effort for both agencies and Cloud Service Providers.*

This document provides a high-level security overview of Canon Office Cloud, a FedRAMP-authorized (moderate level) Managed Print Service. Canon Office Cloud represents a multi-tenant Software-as-a-Service (SaaS) solution, as defined by NIST's SP 800-145. The system is intended solely for use by United States Federal, State, Local, and Tribal Governments, Government Consultants, and Federally Funded Research and Development Centers (FFRDC) (referred to throughout the following sections as "customers"). Canon Office Cloud is supported by an enterprise-class cloud computing architecture that is delivered on the Microsoft Azure Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) platforms.

Moderate Impact accounts for the majority of CSOs that receive FedRAMP authorization and is most appropriate for CSOs where the loss of confidentiality, integrity, and availability would result in serious adverse effect on an agency's operations, assets, or individuals. Serious adverse effects could include significant operational damage to agency assets, financial loss, or individual harm that is not loss of life or serious life-threatening injuries.

SERVICE DESCRIPTION

Canon Office Cloud is built using FedRAMP-compliant Microsoft® Azure IaaS and PaaS offerings. The suite comprises two feature sets, NT-ware uniFLOW Online (uFO) and Netaphor SiteAudit (SA). uFO's core capabilities revolve around users and includes tracking and managing their print or scan jobs. SiteAudit's core capabilities revolve around printing and scanning devices, which includes fleet management, device discovery, security monitoring, meter collection, ink/toner monitoring, and supplies replenishment. Together, these two feature sets provide end-to-end, cloud-based services supporting a managed print strategy.

uniFLOW Online is a cloud-based printing and scanning solution for organizations of all sizes. uFO offers the following user-centric features:

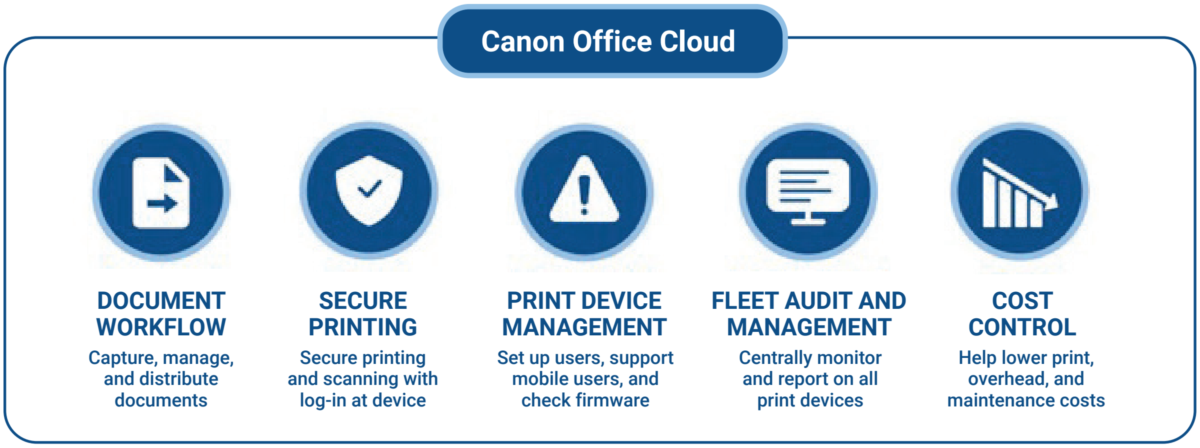
- **Flexible Authentication** – such as support for PIV/CAC/SIPR, Proximity Card, and PIN.
- **Secure Print Feature** – a local client keeps print jobs on the customer's local network.
- **Print From Anywhere Functionality** – jobs can be printed from PCs or email-based printing and "follow" users to any printer.
- **Document Scanning** – allows users to scan documents to themselves and to FedRAMP-authorized cloud storage services.

* *Source: https://www.fedramp.gov/program-basics/*

- **Cost Management** – allows designated users to track print, scan, and copy costs, allowing for reporting and chargeback within the organization.

SiteAudit is a cloud-based fleet management tool that complements the user-centric features of uFO. Importantly, SiteAudit features can be provided by Canon as a fully managed service to customers. SiteAudit offers the following device-centric features:

- **Supply replenishment** – outsource automatic replenishment of ink, toner, and more.
- **Metering** – track ink and toner levels and get visibility into critically low levels.
- **Security Monitoring** – alert for new devices, insecure devices, or devices where security settings have changed.
- **Device Discovery** – identify MIB-compliant print and scan devices.
- **Inventory Change Tracking** – track asset information, moves, adds, changes, and printer age.
- **Service Performance Analysis** – track fleet health including response time, uptime, and service level agreements (SLAs).



Canon Office Cloud

DOCUMENT WORKFLOW
Capture, manage, and distribute documents

SECURE PRINTING
Secure printing and scanning with log-in at device

PRINT DEVICE MANAGEMENT
Set up users, support mobile users, and check firmware

FLEET AUDIT AND MANAGEMENT
Centrally monitor and report on all print devices

COST CONTROL
Help lower print, overhead, and maintenance costs

AZURE SERVICES IN USE FOR CANON OFFICE CLOUD

Canon Office Cloud is deployed, operated, and managed using Microsoft Azure Commercial. Azure services are used for supporting networking, computing, data persistence, encryption, configuration, and monitoring. All Azure services in use are FedRAMP authorized as part of the Microsoft Azure ATO package.

DATA AND METADATA ELEMENTS

NIST SP 800-53 describes metadata as information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels). Customer data and metadata is fully accounted for in the Office Cloud FedRAMP Authorization Boundary and approved system interconnections.

Canon Office Cloud collects the minimum data and metadata elements necessary to provide customers with a fully functional product that supports a managed print strategy. This includes basic information such as Organization/ Customer Name, Email Addresses, and Canon Office Cloud authentication data (tokens) for users of the application, Customer ID, multifunction peripheral (MFP) device name/model, MFP device vendor/manufacturer, MFP Private IP address and FQDN, Private IP address and FQDN of each uniFLOW SmartClient registered with uniFLOW Online, MFP MAC address, MFP device serial number, MFP consumables information (toner, ink, etc.), and MFP alerts (low on consumables, other types). There is also basic metadata associated with print and scan jobs including the username, spool time, color, copies, pages, page format, and location of spool file. Other types of metadata include customer tenant activity logs, system logs, security alerts, and vulnerability information.

CUSTOMER RESPONSIBILITY

Canon Office Cloud is a FedRAMP Moderate impact service that does not store customer files or documents used for printing and scanning. Customers are responsible for making decisions on the enabling, disabling, and configuration of certain Canon Office Cloud features, which is typically performed by a customer application administrator as part of the initial setup and deployment. Examples of these features include whether to enable or disable mobile printing, how long print jobs can stay idle before being deleted, whether to enable or disable integration with third-party SaaS services (e.g., Box®, OneDrive®, and Google® Drive), how to configure their identity provider, and how to configure their email provider.

MULTI-TENANCY

Canon Office Cloud is a multi-tenant SaaS designed to securely handle data from various Federal customers while enforcing logical controls to keep each customer's data separated from the others. Customers connect to Office Cloud using domains that are specific for their subscription, which requires authentication. Customer data within Azure Storage is logically isolated from public data using storage accounts which use unique namespaces. For Blob and Table storage, customers each have their own unique tables and blob containers, which logically isolates one customer's data from another's and prevents cross-contamination. For data stored in Azure SQL Database, each customer has a separate database which also logically isolates their data and helps prevent cross-contamination.

PRINT AND SCAN MANAGEMENT

Firewall and Proxy Changes

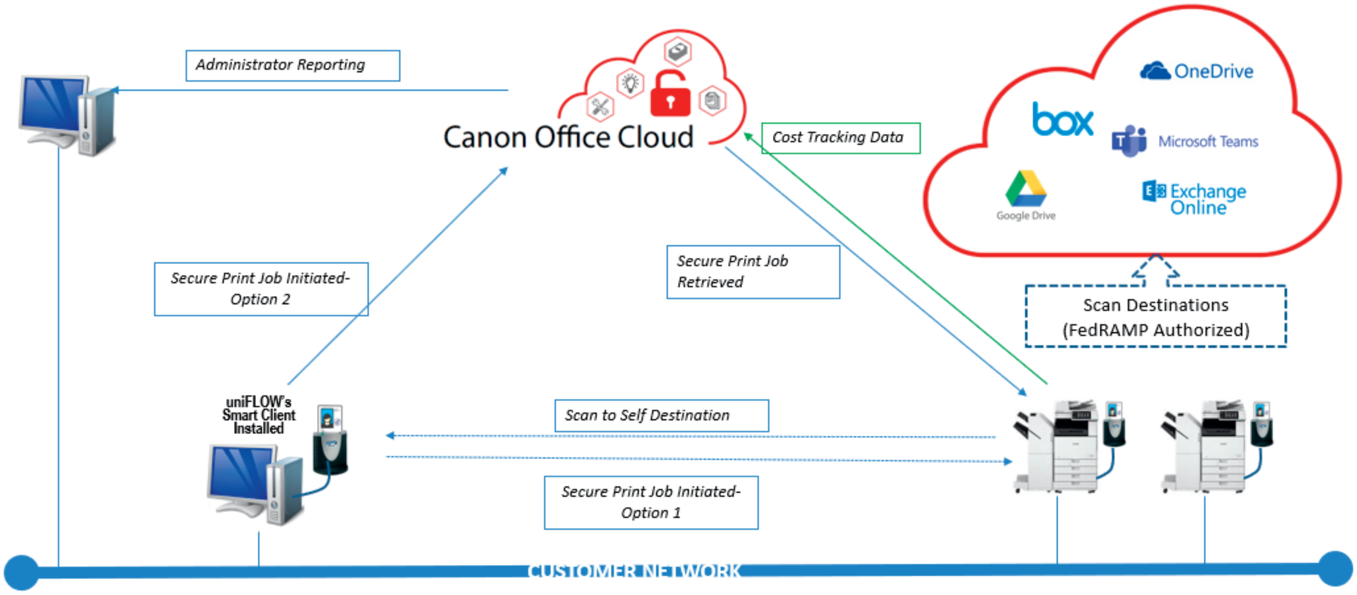
In a typical organization, there is no need to change any of the existing firewall or proxy rules. All communication between the uniFLOW Online service and the components on the company network takes place via HTTPS (port 443, outbound), which is usually allowed for normal website access.

Document/Job Encryption

Print jobs are secured via an AES-256 RSA encryption process for uniFLOW SmartClient to Canon imageRUNNER ADVANCE devices or to uniFLOW Online (if configured). Other printing is done via unencrypted TCP 515/9100 communication but stays within the local customer network. Furthermore, documents and jobs within the Microsoft Azure cloud storage are also encrypted.

Printing via uniFLOW SmartClient

One of the key components of the uniFLOW Online system is the uniFLOW SmartClient. The uniFLOW SmartClient for Windows allows print jobs to be stored on users' local workstations rather than being sent over the internet to uniFLOW Online. By default, for Windows printing, all print jobs stay within the company network and do not travel externally. As an option (#2), jobs can be sent to Canon Office Cloud, via TLS 1.2, where the user can then release the job at any compatible Canon device.


Administrator Reporting
Canon Office Cloud
Cost Tracking Data
OneDrive
box
Microsoft Teams
Google Drive
Exchange Online
Secure Print Job Initiated- Option 2
Secure Print Job Retrieved
Scan Destinations (FedRAMP Authorized)
uniFLOW's Smart Client Installed
Scan to Self Destination
Secure Print Job Initiated- Option 1
CUSTOMER NETWORK

Users authenticate at the Canon imageRUNNER ADVANCE DX device utilizing their government issued CAC/PIV card to access secure print and scan features.

Canon Office Cloud – uniFLOW Online Data Flow

Scanning

Communication with linked/external services is all done via CSI (Connectivity Services Interface) connectors. Communication protocol, encryption levels, and certificates exchange are initiated by the external service.

uniFLOW Online CSI uses OAuth 2.0 to authenticate to external systems. The identities stored to connect to these scanning endpoints are held inside uniFLOW Online, and these have the same data protection as offered in general by uniFLOW Online. The identities can be removed by the user who owns them or by an administrator.

All scan job content is deleted once it is successfully uploaded to the third-party system or mailed out, respectively. Meta-information and accounting information about the scan job may be kept on a per-tenant basis.

uniFLOW Online temporarily stores the scanned images in its file storage for the lifetime of the scan job.

- If the processing and sending of a scan job are not completed successfully due to errors, such as conversion errors or connection errors from the device to uniFLOW Online or from uniFLOW Online to the external system, the scan files are kept for a maximum of 14 days. If during these 14 days, the number of stored scan files for a user exceeds 150, the oldest jobs are deleted regardless of when they were created.
- For scan workflows of the "Scan to Myself" variety, the option to store scan files in uniFLOW Online and make them available for download rather than send them as email attachments is available. For all of the use cases described above, the data stored in uniFLOW Online is held in an encrypted state at all times.

The uniFLOW Online REST API is used to upload the scanned data via HTTPS from the devices into uniFLOW Online, and this benefits from all the security the uniFLOW Online REST API provides:

- HTTPS is enforced.
- The devices identify and authorize against uniFLOW Online using OAuth 2.0.
- The user must be authenticated at the device to be able to scan.

DEVICE MANAGEMENT

SiteAudit performs a discovery using SNMP. The discovery allows both inclusion and exclusion of IP addresses. Discovery over SNMP v1/v2c and SNMPv3.

- Each included network, range, static IP on the list determines the addresses in that list.
- Each excluded network, range, static IP determine if any of these addresses are excluded.

SiteAudit can perform broadcast scans, specific IPV4 address, IPV4 range, or DNS name list to find devices that are explicitly included as one of the discovery addresses.

SiteAudit scans the following ports to find printers:

Port	Description
161 SNMP	Verifies if SNMP is enabled
SNMP	Used to collect data
80 and 8080	HTTP to see if there is an embedded web server HTTP is used to collect data
9100 and 1650	Print protocol for printers, used to collect data
631	IPP print protocol, used to collect data
135	RPC, used to detect a Windows host for local printers
47545 (CPCA) and 9300 (NPAP)	May also be used if the printer supports those protocols
Ports 21 (FTP) and 23 (Telnet)	Identifies potential security vulnerability

Encryption and Authentication Compliance

SiteAudit implementation of SNMP v3 is compliant with the following:

- SHA-1 and SHA-256, SHA-384, SHA-512, MD5, DES, AES-128
- Compliance with: FIPS 140-2, TLS v1.2

Data Collected

Data collected consists of printer asset information, counters, supplies, and error information. A sample of the collected data is listed below. Compliance with: FIPS 140-2, TLS v1.2

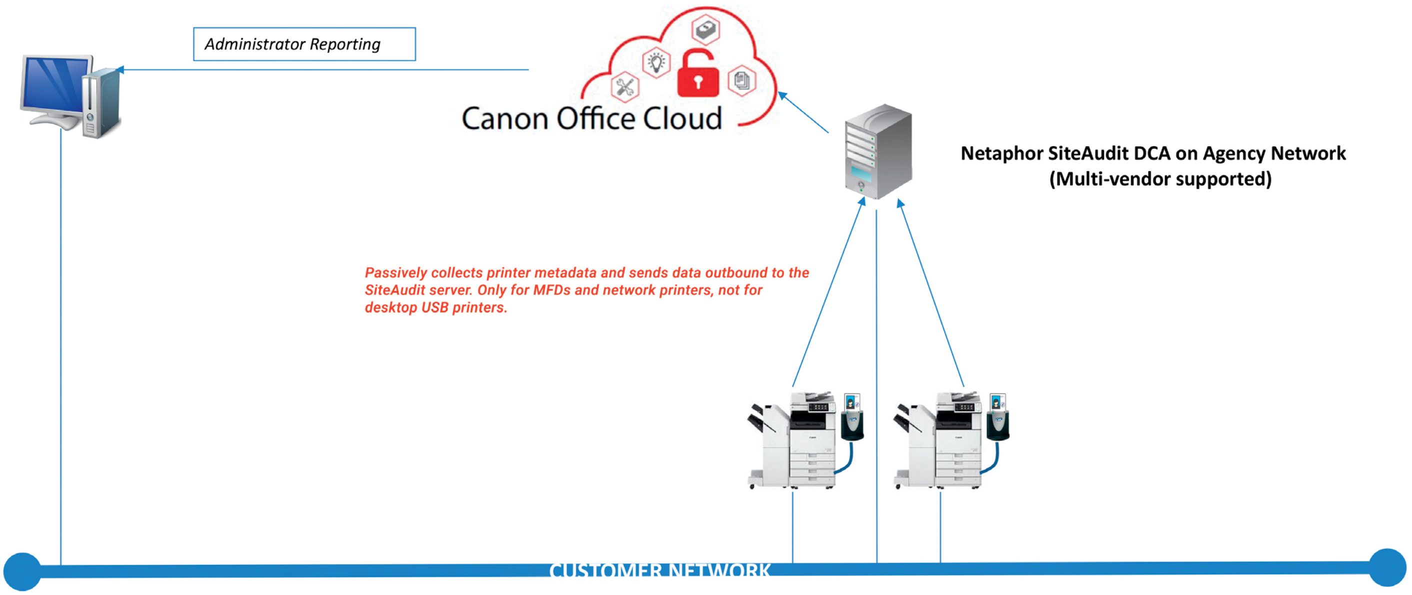
Asset Information	Supplies	Counters	Errors
Manufacturer	Supplies Remaining Level %	Total Pages	Alert Code
Model	Original Supply Level	B/W All	Severity Level
IP Address	Percentage of w/Supplies Used	B/W Print	Training Level
Printer Name	Date Toner Detected	B/W Copy	State
Product Number	Replaced On Date	B/W Large	Resolution Status
Serial Number	Supplies Description	Color All	Incident Description
Asset Tag	Supplies Type	Color Print	Incident Duration
Location	Supplies Part Number	Color Copy	Service Level Agreement Name
Printer MAC Address	Supplies Serial Number	Color Large	Contact
Host MAC Address	Supplies Installation Date	Large/Small	Total Errors
		Copied	Uptime
		Print	Last Successful Communication
		Fax	Last Notified
		Scanned	Device Status (Ready/Error/Warning)

Common Questions about Data Collection

Device Data Collection: Only device data is collected. Information, such as user accounts on the device for print retrieval or secure print or the list of jobs on devices, is not collected.

No information such as user passwords, credit card information, SSN, etc., are collected or stored by SiteAudit.

External communication outside the firewall is under control of the customer. The only external communication is via notification email or scheduled reports. The customer can control which notifications are sent and to whom. The same is true for scheduled reports.



Passively collects printer metadata and sends data outbound to the SiteAudit server. Only for MFDs and network printers, not for desktop USB printers.

Users authenticate at the Canon imageRUNNER ADVANCE DX device utilizing their government issued CAC/PIV card to access secure print and scan features.

Canon Office Cloud – Netaphor SiteAudit Data Flow

SUMMARY

Offering two robust robust services, Canon Office Cloud can help improve document and print security, manage print related costs, and improve overall device management with the added benefit of FedRAMP authorization.

Canon Office Cloud has met all relevant FedRAMP security, process, and continuous monitoring requirements. FedRAMP-authorized systems are already validated against a known set of standards that can be verified, helping to reduce internal security evaluation requirements.

Canon Office Cloud is available to (1) U.S. federal, state, local, tribal, educational, and territorial government entities, and (2) entities which handle data that is subject to government regulations and requirements. Validation of eligibility may include confirmation of handling data subject to International Traffic in Arms Regulations (ITAR), law enforcement data subject to the FBI's Criminal Justice Information Services (CJIS) Policy, or other government-regulated or controlled data and are only granted access to the services through a formal contracting process.

Canon

CANON SOLUTIONS AMERICA

1-800-815-4000 **CSA.CANON.COM**

FedRAMP

Canon offers products that contain certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of features discussed herein will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel to determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment. Subscription to a third-party service required. Subject to third-party service providers terms and conditions. Canon makes no representations or warranties with respect to third-party products. Neither Canon Inc. nor Canon U.S.A., Inc. represents or warrant any third-party product or feature referenced hereunder.