DEVICE SECURITY OVERVIEW

i-SENSYS, i-SENSYS X AND imageRUNNER

Canon

00 Contents

INTENT OF THIS DOCUMENT

Canon recognises the importance of information security and the challenges that your organisation faces. This document provides several information security facts for i-SENSYS, i-SENSYS X and imageRUNNER devices (from here on referred as ‘Canon devices’). It provides details of the security technology for networked and stand-alone environments, as well as an overview of the product technologies related to document and data security.

This document is primarily intended for the administrative personnel of a customer charged with responsibility for the configuration and maintenance of the Canon devices. This document is designed to provide you with adequate information to understand more clearly the security related configuration capabilities* offered by Canon devices and enable you to discuss with Canon or Canon partner the most appropriate settings for your specific business environment.

It should be noted that not all device hardware has the same level of capability and different system software may provide different functionality. Once decided, the suitable configuration settings can be applied to your device or fleet. Please feel free to contact Canon or a Canon partner for further information and support.

Canon does not warrant that use of the information contained within this document will prevent malicious attacks or prevent misuse of your Canon devices.

*Security feature support varies by model; please refer to the Appendix attached to this document and to User Manuals for model-level detail:

https://oip.manual.canon/portal-eu-af-me-ru/frame_htmls/home.html

The features reviewed in this document include standard and optional solutions for Canon’s devices.

Specifications and availability are subject to change without notice.

01
Introduction

Overview

Security Market Overview

In today’s digital world, risks to networks and connected devices come in more forms and from more directions than ever before. From identity theft and intellectual property loss, to infection by viruses and malware, IT administrators are tasked with adequately protecting information and assets from threats from the outside as well as within.

Nearly every day destructive threats emerge and undiscovered vulnerabilities are exposed, proving that you can never be too secure. IT administrators need a holistic security strategy that can be applied at every level of the organisation — from servers, desktops and devices such as printers and Multifunction devices (MFPs) to the networks that connect them all.

Increased governmental regulations add an additional layer of strict compliance standards that must be met. Legislation such as Sarbanes-Oxley Act (SOX) and General Data Protection Regulation (GDPR) require businesses to ensure the security, privacy, accuracy and reliability of information receives the utmost attention.

Imaging & Printing Security Overview

Today’s printers and multifunction devices share many similarities with general purpose PCs. They contain many of the same components such as memory capability. Like any other device on the network, sensitive information may be passed through these units and potentially stored on the device. However, many businesses printers and multifunction devices are not given the same attention concerning information security.

This document has been designed to provide detailed information on how Canon devices can address a wide variety of security concerns.

Key Security Concentration Areas

Canon recognises the vital need to help prevent data loss, protect against unwanted device use, and mitigate the risk of information being compromised. As a result, all Canon devices systems include security features to help safeguard information. These security capabilities fall into four key areas:

- Device Security
- Data Security
- Network Security
- Security Monitoring / Management Tools

02 Device Security

i-SENSYS, i-SENSYS X and imageRUNNER Platform Security

Canon devices are built upon a platform that provides strong capabilities related to security and productivity. The architecture centers on an operating system powered by an embedded OS. The source version used by Canon devices has been hardened* by removing all unnecessary drivers and services so that only the ones essential to its operation are included.

The nature of embedded operation systems and the hardening* of the operating systems reduce the exposure to exploits as compared to a desktop or server version of a PC operating system. Some of the security related activities include testing of Canon devices during various phases of the development process to address potential vulnerabilities prior to production.

*Hardening is the process of making an operating system more secure. This requires the configuration of the system and network settings specific to the requirements of the environment in which the system is being used; in addition, unused files are deleted and the latest patches are applied

Authentication

Select Canon devices include authentication options which administrators can use to ensure that only approved walk-up and network-based users can access the device and its functions, such as Print, Copy or Scan and Send feature. Beyond limiting access to only authorised users, authentication also provides the ability to control usage of colour output, and total print counts by department or by user.

Device-Based Authentication

Department ID Mode

An embedded feature within select Canon devices, the Department ID Management Mode permits administrators to control device access. If Department ID authentication is enabled, end users are required to enter a password up to seven digits long before they can access the device. Up to 300 Department IDs can be configured and each can be configured with device function limitations, such as limiting printing, copying, and faxing, as well as restricting access to colour printing.

02 Device Security

Single Sign-On Hybrid (SSO-H) Login

Single Sign-On Hybrid (SSO-H) is a Multifunctional Embedded Application Platform (MEAP) login service that can be used stand-alone with user data registered locally on the device or in conjunction with an Active Directory (AD) network environment. Available on select Canon devices, SSO-H supports the following modes:

- Local Device Authentication – with credentials stored in the device
- Domain Authentication – in this mode, user authentication can be linked to an Active Directory environment on the network
- Domain Authentication + Local Device Authentication

When used in Domain Authentication mode, a user must successfully authenticate using valid credentials on the system's control panel, Remote UI utility, or web browser when accessed via a network prior to gaining access to any of the device functions.

SSO-H can support up to 200 trusted domains plus the users that belong to the same domain as the device. Select Canon devices also ship with SSO-H, which supports direct authentication against an Active Directory domain using Kerberos or NTLMv2 as the authentication protocol. SSO-H does not require any additional software to perform the user authentication as it is able to directly communicate with the Active Directory domain controllers.

Universal Login Manager (ULM)

ULM is a server-less login application which provides an easy and convenient solution for user authentication. Ideal for small to medium size businesses, ULM's simple user authentication includes card log-in (requires an additional option), PIN code, or user name and password, using local or Active Directory (AD), with minimal IT requirements. ULM delivers simplified tracking, allowing organisations to obtain a simple overview of user or device usage activity.

User Authentication (UA)

The User Authentication (UA) is a Multifunctional Embedded Application Platform, known as MEAP login service which is available on the select Canon models. User Authentication combines the SSO-H and Department ID functions available on other Canon models. UA can manage up to 5,000 user accounts within 1,000 department codes.

02 Device Security

uniFLOW* Authentication

When combined with optional uniFLOW, Canon devices can securely authenticate users through contactless cards, chip cards, and PIN codes. uniFLOW supports various types of cards using its own reader as well as others through potential custom integrations.

*includes uniFLOW/uniFLOW Online/uniFLOW Online Express

Password-Protected System Settings

As a standard feature, select Canon device's setup screens support administrator password protection to restrict device setting changes from both, the control panel and Remote UI tool. System Administrators can set network information, system configuration, enable, and disable network and printing protocols among many other options.

Canon highly recommends setting an administrator password at time of installation since it controls critical device settings.

Remote UI Default Password Change

To ensure good security practice, unique passwords should be used for each device or require the user to change the default password to a unique password before use. This prevents trivial remote access to the device until the default password/PIN for the Administrator/System Manager account is changed. This changes the ability to access the Remote UI through your web browser when the default password/PIN currently set on the device. Depending on the device, access to the RUI will be prevented or the RUI will be disabled until the default password is changed.

Scan and Send Security

On devices that have Scan and Send enabled, information being sent from the device may be considered confidential and sensitive. For these devices, there are additional security features to prevent confidential information from being accessed by an unauthorized person.

Address Book Password

Administrative passwords can be set for Address Book Management functions. By setting a password for an Address Book, the ability to Store, Edit, or Erase individual and group e-mail addresses in the Address Book is restricted. Therefore, only individuals with the correct password for an Address Book will be able to make modifications.

This is not the same functionality when password protecting an Address Book. Administrators who are looking to Import/Export an Address Book, can select to set a password when exporting the File. That password is then required to Import the Address Book. The Address Book Import/Export function is available through the Remote UI utility.

Destination Restriction Function

Select Canon models allow System administrators to control where information can be sent using a destination restriction function. Data transmission to a new destination through the Scan and Send and Fax functions can be restricted, prohibiting transmissions to locations other than the destinations registered or permitted.

By restricting sending of faxes, e-mails and files to new destinations, data can only be sent to previously registered destinations. As you can no longer enter or send to new destinations, setting this mode with an Address Book PIN increases security when sending.

Print Driver Security Features

Print Job Accounting

A standard feature in Canon’s printer drivers, print job accounting requires users to enter an administrator-defined password prior to printing, thereby restricting device access to those who are authorised to print. Printing restrictions can be set using Department ID credentials.

Custom Driver Configuration Tool

Administrators can create custom driver profiles for users to limit access to print features and specify default settings, thereby protecting the device against unauthorised use, enforcing internal policies and better controlling output costs. Settings that can be defined and enforced include secure print, custom print profiles, as well as hiding any desired functions.

USB Block

USB Block allows the System Administrator to help protect the Canon devices against unauthorised access through the built-in USB interface allowing for the USB Memory Media connection. In addition, access to the device’s USB interface for desktop access and the device’s host mode for other USB devices can each be permitted or disabled.

Select Canon models also can be set to restrict USB usage for memory but allow USB usage for peripherals such as card readers. Canon’s USB feature provides the capability to view and print from the devices only for non-executable files, such as .pdf, .jpg and .tiff. Executable files cannot be performed on the device, which helps protect against viruses and malware.

Security Measures to Protect Against Malware and Tampering of Firmware/Applications

Security measures to protect against malware/firmware tampering have been implemented, that do not allow for installation or execution of programs without a digital signature applied by Canon when updating firmware, executing processes or installing applications. In order to further assist in the prevention of data disclosure due to unknown attacks/springboard attacks, additional security enhancements have been made for select Canon devices.

Verify System at Startup*

Once enabled, the Verify System at Startup function runs a process when the machine starts or when an application (in Application Library) is executed. The process verifies that the system or application has not been tampered. If tampering of one of these areas is detected, it will either prompt for a firmware update or application reinstall. Standard cryptographic technologies (hash, digital signature) are used for verification.

When this function is turned on, Warm-up time after powering on (WUT) is increased because the verification process is performed when the device is started. However, it does not affect the time to wake up from sleep mode or the restore time for quick startup, because the verification process is performed at device startup.

*Selected models only

03 Data Security

Protecting your organization's confidential information is a mission that Canon takes seriously. From your documents, faxes and e-mails to the underlying data in memory, Canon has built in many controls to help ensure that your information does not become compromised.

Data Storage

Canon's i-SENSYS, i-SENSYS X and imageRUNNER devices do not contain a built-in hard disk drive (HDD). Instead some of the Canon devices use embedded Multi Media Card (eMMC) mass storage that use NAND-based flash memory.

To prevent physical reading of stored data, PCB mounting without PIN feet (BCA) and Flash memory sealing (meaning memory element cannot be removed) are done, to reduce the risk of critical data loss at the printer. To further protect data, encryption by the device firmware is performed when writing any data to the memory media.

Document Security Capabilities

Watermark

To discourage the unauthorised copying or sending of confidential information, the option to embed user-defined text within the background of any print or copy job can be utilized. Users can define custom or preset watermarks to appear in any position on copied output.

Encrypted PDF*

The Encrypted PDF mode enables users to encrypt, set password and define permissions for PDF files that are sent to an e-mail address or file server for enhanced security. Only users who enter the correct password can open, print, or change the received PDF file.

Encrypted PDF mode can be used only if an e-mail address or file server is specified as the destination. If a fax number, I-fax address, or inbox is specified as the destination, a user cannot send the job as an encrypted PDF file. Encrypted PDF files can be saved using the 128bit AES algorithms or the 256bit AES algorithms.

Digital Signature PDF (Device Signature)*

Within Scan and Send, users can add digital signatures that verify the source and authenticity of a PDF document. When recipients open a PDF file that has been saved with a digital signature, they can view the document's properties to review the signature's contents including the name of the device that created the document, the Certificate Authority, system product name, serial number and the Time/Date stamp of when it was created. The Device Signature PDF use the device signature certificate and key pair inside the machine to add a digital signature to the document, which enables the recipient to verify the device that scanned it.

*Select models only, may also require additional option(s).

03 Data Security

Secure Printing

Secure Print*

Secure Print is a print function that holds a job in queue until the user enters the appropriate password at the device. This ensures that the user is in proximity of the printer before the document is printed and minimizes unattended documents left at the device. The i-SENSYS, i-SENSYS X and imageRUNNER device requires the user to set a password in the print driver window when sending a print job from a connected PC. The same password is also required for releasing the job at the device. Secure print jobs can be set to delete within a specified time frame.

Encrypted PDF*

The Encrypted PDF mode enables users to encrypt, set password and define permissions for PDF files that are sent to an e-mail address or file server for enhanced security. Only users who enter the correct password can open, print, or change the received PDF file.

Encrypted PDF mode can be used only if an e-mail address or file server is specified as the destination. If a fax number, I-fax address, or inbox is specified as the destination, a user cannot send the job as an encrypted PDF file. Encrypted PDF files can be saved using the 128bit AES algorithms or the 256bit AES algorithms.

*Select models only, may also require additional option(s)

uniFLOW Secure Print

uniFLOW is an optional modular software designed to help reduce costs, improve productivity and enhance security. From a security perspective, uniFLOW contributes to secure printing capabilities by holding jobs at the server until released by the user at any compatible device. From their desktop, users print documents by choosing a single Universal driver. At the chosen device, users can be authenticated using a wide variety of supported methods, access the uniFLOW client application from the device’s control panel, and release their job from their queue of pending documents.

Forced Hold Printing

Select Canon models come with an enhancement of the “Secure Printing” function, where IT administrators can enforce secure print for all, or select users. The setting only needs to be changed in the Settings/Registration screen on the local device UI. Print driver settings do not need to be changed.

Rules can be set up based on certain conditions (unknown owner, owner name, IP address, and/or port) to hold as a regular document, print immediately or cancel). Administrators can set how long documents in job hold will be held (from 10 min – 72 hours) and can choose whether to auto delete after printing or keep until expiration or manual deletion.

With Forced Hold Printing, IT Administrators can help reduce the amount of wasted prints, by requiring users to release their jobs after submitting them to the printer, which can reduce the amount of uncollected printouts. Forced Hold Printing also helps to ensure that the user receives their desired output the first time, by allowing the user to preview their job, change print settings from the hold queue, and even print a sample file before printing an entire job.

Fax Security

Canon i-SENSYS/imageRUNNER MFPs that support fax can be connected to the Public Switched Telephone Network for sending and receiving of fax data. In order to help maintain the security of customer’s networks in relation to this potential interface, Canon has designed its devices to function in accordance with the following security considerations:

Super G3 Fax Board Communication Mechanism

The modem on the Super G3 Fax Boards does not have Data Modem capability, but only Fax Modem capability. As a result, TCP/IP communication through the phone line is impossible. In addition, there is no functional module such as a Remote Access Service that enables communication between a phone line and a network connection within the device.

Fax Transmission

The PC Fax function can fax documents from the PC, using a Fax driver that runs on the PC. However, data transfer from the PC to the device and data transfer (FAX transmission) from the phone line via the G3 FAX board are structurally separated.

Fax Received

Although a received fax document can be automatically forwarded to a network, it is not possible to breach the network as these capabilities are afforded following completion of facsimile communication. Since the data stored is in a format proprietary to Canon, there is no threat of virus infection. Even if the device receives a data file pretending to be a FAX image data but contains a virus, the received data must be decoded first. While trying to decode the virus the phone line will be disconnected with a decode error and the received data will be discarded. The Super G3 Fax Boards cannot receive data files, but are capable of receiving and decoding facsimile transmissions. As a result, virus-laden files sent to the i-SENSYS, i-SENSYS X and imageRUNNER MFP via its phone line connection cannot be processed.

Other Fax Features

Allow/Restrict Fax Driver Transmissions

Device can be configured to allow (default) or restrict sending fax transmissions via a PC Fax driver.

Fax Forwarding

The Fax Forwarding function allows Canon MFPs to forward inbound fax transmissions to specific recipients stored in the address book. This is done by setting predetermined conditions or storing faxes in memory for later printing rather than permitting incoming messages to be left in an open output tray.

Fax Destination Confirmation

To help prevent faxed documents from being inadvertently sent to the wrong destination, select Canon MFPs offer a Confirm Entered Fax Number feature for additional protection. When enabled on the device by an administrator, users will be prompted to re-enter the recipient’s fax number prior to sending in order to confirm that it matches the original one specified. If the fax numbers do not match, the user will be prompted to enter the original number again and re-confirm.

04
Network Security

Network and Print Security

Canon devices include a number of configurable network security features that assist in securing information when network printing is deployed. Network security features include the ability to permit only authorised users and groups to access and print to the device, limiting device communications to designated IP/MAC addresses, and controlling the availability of individual network protocols and ports as desired.

Enabling/Disabling Protocols/Applications

Through Canon's device setup, network administrators are provided with the ability to configure the specific device protocols and service ports that are accessible. As a result, unwanted device communication and system access via specific transport protocols can be effectively blocked. The ability to disable unused TCP/IP ports, further secures the Canon devices. Disabling ports may affect the available functions and applications on the device.

IP Address Filtering

IP Address Filtering is a function to permit or reject reception and/or transmission of packets from specified IP Addresses. Administrators can decide to enable IP Filtering and can specify filtering options (Permit/Reject). The default value of all options for this feature is "Disable" (permit reception).

The setup required for filtering involves configuration of the default policy (either Reject or Permit), followed by registration of the IP addresses to be exempt.

If the default policy is to "Permit," then the IP addresses you want to reject must be registered. Conversely, if the default policy is to "Reject," then the IP addresses you want to permit must be registered. The default value for the default policy is to "Permit" for both reception and transmission.

Media Access Control (MAC) Filtering*

MAC address filtering is useful for smaller networks where administrators can manage controls for specific systems, regardless of the subnet to which they happen to be connected. For environments using Dynamic Host Configuration Protocol (DHCP) for IP address assignments, MAC address filtering can avoid issues that are caused when DHCP leases expire and a new IP address is issued to a system. As with IP address filters, MAC address filters can be used to allow or deny access to specific addresses.

MAC address filters take a higher priority than the IP address filters; so necessary devices can be allowed or denied, even if the printer's IP address would dictate otherwise. Canon devices support MAC address filtering for received packets (RX) and transmitted packets (TX).

*Not available on Wi-Fi

04 Network Security

TLS Encryption

Canon devices support Transport Layer Security (TLS), which is a connection-type transport layer protocol for HTTP security. It provides authentication and encryption, as well as detects alterations.

Many organisations are quite diligent about protecting data as it is transferred between PCs and servers or from one PC to another. However, when it comes to transmitting that same data to and from the MFP or printer device, it is this may not be the case. As a result, it may be possible to capture data as it is sent to the printer via the network. Canon helps mitigate this by providing Transport Layer Security (TLS) for support of some transmissions to and from the Canon device, such as Internet Printing Protocol (IPP), Internet-fax (I-fax) and Remote UI).

IPv6 Support

IPv6 support, which is available in all Canon devices, provides a more secure network infrastructure, improved traffic routing and easier management for administrators than IPv4.

IPSec Support

Canon devices support IPSec, which allows users to utilize IPSec (Internet Protocol Security) to help ensure the privacy and security of information sent to and from the device while in transit over unsecured networks.

IPSec is a suite of protocols for securing IP communications. IPSec supports secure exchange of packets at the IP layer, where the packets in the data stream are authenticated and encrypted. It encrypts traffic so that the traffic cannot be read by parties other than those for whom it is intended, it also ensures that the traffic has not been modified along its path, that it is from a trusted party and protects against replay of the secure session. The IPSec functionality of the device only supports transport mode, therefore authentication and encryption are only applied to the data part of the IP packets.

Wireless LAN

Most Canon devices support wireless networking. Wireless LAN is IPv6 compliant and supports the latest wireless encryption standards, including WEP, WPA and WPA2.

IEEE 802.1X (Wireless and Wired supported)

Canon devices support IEEE 802.1x, which is a standard protocol for port-based Network Access Control. The protocol provides authentication to devices attached to a LAN port and establishes a point-to-point connection only if authentication is successful.

IEEE 802.1X functionality is already supported by many Ethernet switches, and can prevent guest, rogue, or unmanaged systems that cannot perform a successful authentication from connecting to your network.

SNMP & Community String

Simple Network Management Protocol (SNMP) is a protocol for monitoring and controlling communication devices in a network by using Management Information Base (MIB).

SNMPv1 uses information called “community” to define the scope of SNMP communication. As this information is exposed to the network in plain text, your network may be vulnerable.

With SNMPv3, you can implement network device management that is protected by more robust security features.

Community Strings are like passwords for the management elements of network devices:

There is a community string which is used for read-only access to a network element. The default value for this community string for most network devices is often “public”. Using this community string an application can retrieve data from the Canon device’s Management Information Base (MIB) elements.

There is also a read-write community string, and its default value is usually “private.” Using the read-write community string, an application can change values for MIB variables.

Canon devices use public and private as the default SNMP community strings, but these may be renamed to a user-defined value. In addition, Canon model’s systems support SNMPv3, which provides greater security by protecting data against tampering, ensuring access is limited to authorised users through authentication and encrypting data sent over a network.

Scan and Send -Virus Concerns for E-mail Reception

For i-SENSYS, i-SENSYS X and imageRUNNER Multifunction Devices (MFPs) with Scan and Send capabilities enabled, when data is received, the email text is separated from any file attachments and only JPEG/TIFF image files are printed and transferred. The device will discard any attachments of a different file format in e-mail message upon receipt, including attached viruses.

Scan and Send-enabled devices support POP and SMTP as e-mail reception protocols.

Mail Server Security

When the Scan and Send on i-SENSYS, i-SENSYS X and imageRUNNER MFPs is enabled, the internal mail service is enabled and supports the POP, SMTP APOP, SMTP over TLS, POP over TLS protocols. To protect the service against attack or improper use, administrators can enable additional security features such as SMTP Authentication.

04 Network Security

SMTP Authentication

To prevent unauthorised users from making use of the device's internal SMTP server, administrators can enable SMTP Authentication and designate a username and password to connect to the server. In addition, administrators can enable TLS for all SMTP send and receive operations.

POP Authentication Before SMTP

As an additional layer of security, Canon MFPs support the ability for administrators to enable or disable the POP Authentication before SMTP feature. POP Authentication before SMTP forces a successful login to a POP server prior to being able to send mail via SMTP.

05 Security Monitoring & Management Tools

Canon provides tools to help organisations enforce their internal company policies and meet regulatory requirements. Whether a single Canon device is deployed, or forms part of a fleet, these solutions provide the ability to audit usage and limit access to features and functions enterprise-wide—at the group and user-level.

Security Policy Settings

As document, user, and information security become more important to organisations, administrators need to be sure that the various settings are organised in an accessible location that can be password protected and managed. Canon devices have a common web interface called the Remote User Interface, where administrators are able to do the following:

- Set passwords for access to device settings, including security settings
- Access and review current security settings
- Edit and save changes to security settings

Enterprise Management Console

imageWare Enterprise Management Console (iWEMC) is a highly scalable web-based management utility for administrators that delivers a streamlined, centralized point of control for all devices installed across an enterprise. The software makes it easier for organisations to securely manage one or more systems remotely across a network. To aid in implementing and managing a printer and MFP infrastructure, iWEMC facilitates the secure distribution of device configuration information and address books using TLS encryption.

Device Configuration Management Plug-in

Allows administrators to configure device and interface settings as required and push the settings out to multiple devices. Provides the ability to back-up or restore detailed device settings to help save significant time and resources for IT departments.

Device Firmware Update Plug-In

Allows administrators to push out firmware updates to the fleet.

06 Conclusion

Since initially introduced, the Canon printers and MFPs have grown in both the breadth and depth of features and functions. As with any networked device, imaging and printing devices must be included within the broader context of the company's overall security strategy to help ensure the confidentiality, integrity and availability of information.

When properly deployed, the devices can be effectively protected against vulnerabilities from either malicious or unintentional use. Combined with advanced monitoring and management tools for auditing and centralized administration, the systems can meet the demand for increased productivity and strong security.

Each customer's needs are different, and while the security of corporate data is ultimately the responsibility of the customer, Canon can offer additional services and expertise to enhance the security levels, from device initial set-up to its end of life. While these suggestions assist in enhancing device security, internal company security policies should ultimately dictate which security measures are appropriate for implementation within a specific environment.

Security-related services

Canon offers services focused on enhancing the protection of your information, especially useful when there's

1. **Device hardening service**

Offering pre-configuration of security focused settings and functions on your i-SENSYS, i-SENSYS X and imageRUNNER device before it is delivered and connected to your network.

2. **Data removal service**

Offering permanent deletion of both physical and digital data when devices reach end-of-life, including documented evidence upon completion of service.

Canon is committed to helping our customers meet their objectives related to security of their critical information and is continuing to develop new technologies in this area. For more information, please contact your Canon representative or Canon partner, or visit **https://www.canon-europe.com/support/product-security.**

Please find model-level detail regarding security support in the Appendix attached to this document: Security Matrix

07 Disclaimer

The information provided in this document is the most current information available at the time of its creation. Canon hereby expressly disclaims all warranties of any kind, express or implied, statutory or non-statutory, in relation to the information provided in this document: Edition No.1, Sep 2020.

In no event shall Canon, Canon's subsidiaries or partners, affiliates, their licensors, distributors or dealers be liable for any direct, special, consequential, incidental or indirect damages of any kind (including without limitation loss of profits or data or personal injury), whether or not Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers have been advised of the possibility of such damages, and Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers shall not be liable for any claim against you by a third party arising out of the use or performance of canon's products or information referenced herein.

Regulatory Disclaimer:

Statements made in this document are the opinions of Canon Europe. None of these statements should be construed to customers or Canon Europe's partners as a legal advice, as Canon Europe does not provide legal counsel or compliance consultancy, including without limitation, Sarbanes Oxley or the GDPR. Each customer must have its own qualified counsel determine the suitability of a particular solution for the regulatory and statutory compliance.

All specifications and availability are subject to change without notice.

08
Appendix

Security Matrix

Canon Inc.
canon.com

Canon Europe Ltd.
canon-europe.com

English Edition