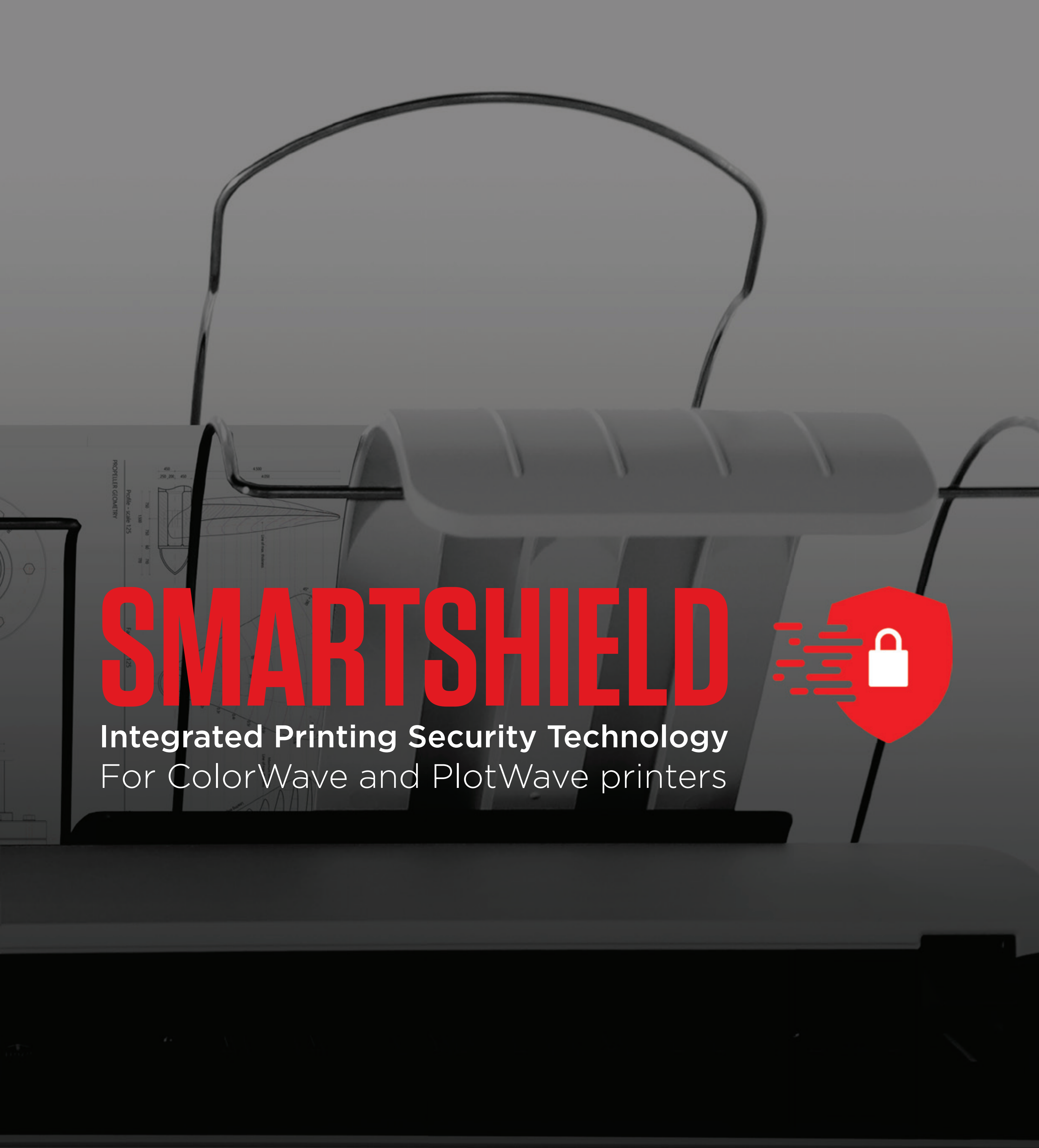


SMARTSHIELD

Integrated Printing Security Technology

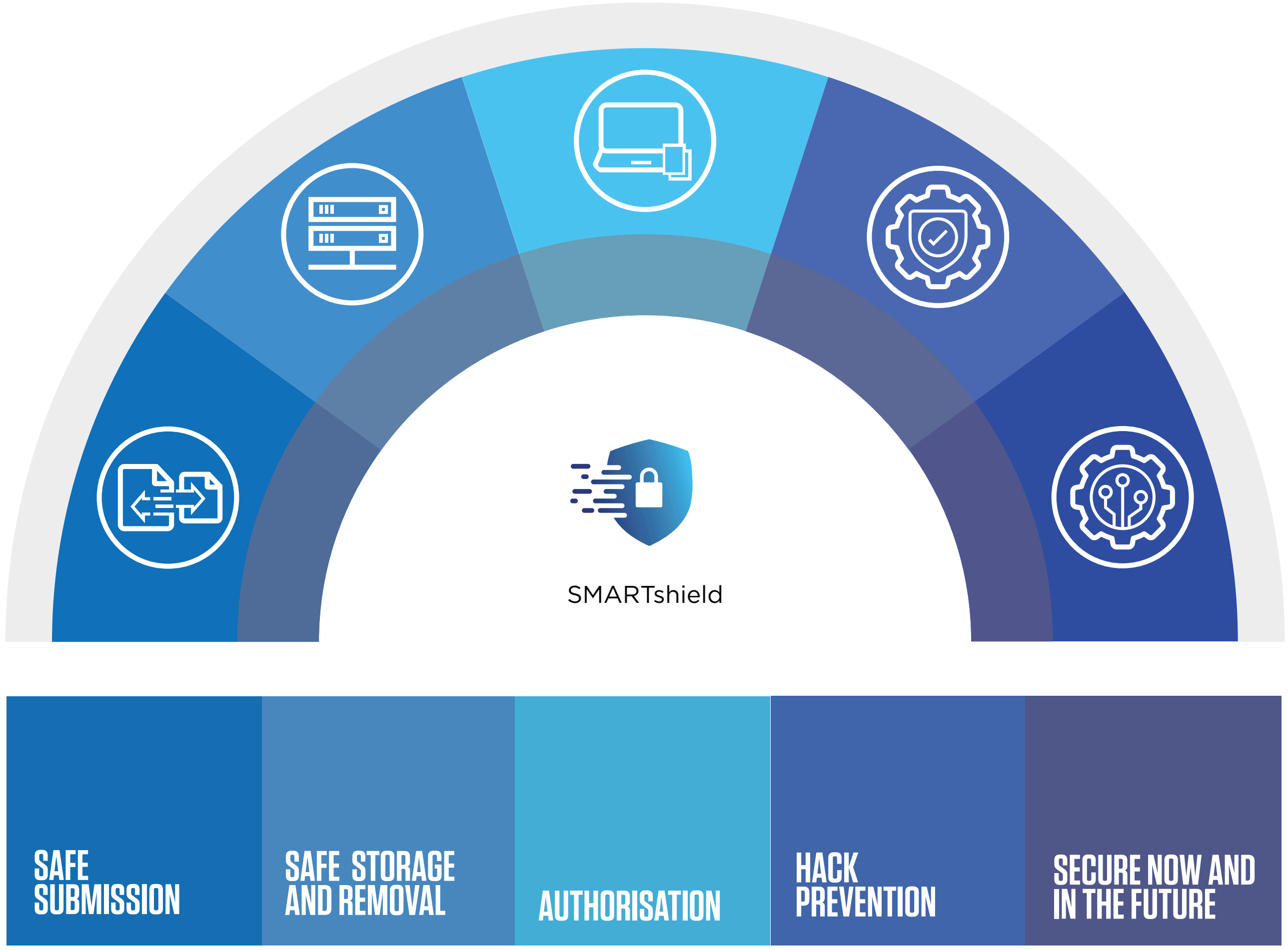
For ColorWave and PlotWave printers

Canon

FIRST-CLASS PRINTING SECURITY

Our market-leading Large Format printers address the security concerns of technical document users who handle confidential customer data.

SMARTshield is a suite of security features embedded in the total print workflow of the latest PlotWave and ColorWave systems. Designed to keep your systems safe: today and in the future.



More than ever, businesses and government organisations with Large Format printers need to protect their most important, confidential, and sensitive information within their office and on their networks. This includes information sent from individual workstations and other devices to the printer as well as data stored on the printer. It is also essential that systems are protected against any unauthorised access to print data, printed information and the end-user's own IT infrastructure via printers. For these reasons organisations need a secure Large Format printer that makes life easier for the IT administrator, users and management.

SMARTshield, is a fully integrated printing security technology that is in all our Large (Wide) Format Printers , and is designed specifically to address such needs.

SMARTshield features multiple security measures designed to keep data and information safe from unwanted eyes.

With SMARTshield, all your security risks in every stage of the workflow process are addressed.

SMARTshield secures you now and in the future.

SAFE SUBMISSION

Protect data while sending files to your printer – from any device.

Thanks to ClearConnect workflow applications, users can submit files from their desktop or any mobile device. With this level of flexibility and mobile access, It is essential that valuable data is submitted securely to the printer at all times and from all devices.

- Internet Protocol Security (IPSec) compatibility
- IPv6 and IPv4 compatibility
- HTTPS

SMARTshield

SAFE STORAGE AND REMOVAL

Protect confidential data stored on the hard drive of the printer.

It is important to protect confidential data stored at the printer from being stolen or accidentally leaked from the company or department. SMARTshield encrypts data and restricts access with user identification, to make sure all your data is kept safe. By erasing data correctly, users can be sure their confidential files are unavailable to unauthorised colleagues.

- Secure File Erase
- E-Shredding
- Removable hard disk
- Secure Boot
- Data encryption
- HDD destruction at the end of the contract

SMARTshield

AUTHORISATION

SMARTshield user authorisation restricts access to confidential files for unauthorised users.

Additionally, by requiring users to authenticate, you can keep tighter control of their activities. It's also possible to limit the features and protocols they can access and monitor the expenses incurred per user.

- Control panel access lock
- Secure printing via domain credentials (Active directory)
- Secure printing via smartcard (excl. reader)
- Print files only available in your Smart inbox
- Scan to your personal home folder
- Print from your personal home folder
- Disable ports and interfaces
- Third-party software such as uniflow

HACK PREVENTION

One of the greatest security challenges for any business is keeping hackers out. With so much valuable data being printed, it's essential to restrict access to the printer and data stored on the controller (or hard drive).

And you want to be sure that your printer cannot be hijacked and used against your network. SMARTshield addresses the challenge of hack prevention on a number of fronts:

- Disabling unused protocols
- SNMP v3
- IEEE 802.1x compatibility
- McAfee antivirus (optional)
- McAfee Whitelisting Application control (optional)

SECURE NOW AND IN THE FUTURE

Security is not a static situation. Hackers are constantly trying to find new ways to access your valuable information. SMARTshield has been designed to keep your information secure: today and in the future.

And of course, our security specialists are constantly monitoring the latest risks to help ensure your data and your printers stay safe. Current features include:

- Windows 10 IoT Enterprise LTSC controller software
- Support at least up to 2029 or beyond
- Remote controller security updates
- On Remote service

We understand your security concerns, and have put together a suite of features to address the risks your business faces at every stage of the workflow process.
Not just today, but also in the future.

Canon is your partner for a safe printing environment.

SMARTshield

SMARTSHIELD COMPATIBLE

SMARTshield is integrated in the following systems:

ColorWave 3600

ColorWave 3800

PlotWave 3000 series

PlotWave 5000 series

PlotWave 7500

SMARTSHIELD IN DETAIL

SAFE SUBMISSION

Internet Protocol Security (IPsec) compatibility
IPsec is a protocol that provides authentication, data confidentiality and integrity in the network communication between the controller and other devices.

IPv6 and IPv4 compatibility
Internet Protocol version 4 (IPv4) is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. It uses 32 bit addresses. IPv6 is the most recent version and uses 128 bit addresses and can therefore address many more devices.

HTTPS
To protect the network traffic for WebTools Express, Publisher Express and Publisher Select using the HTTP protocol from being intercepted or altered, the HTTPS protocol can be used instead of HTTP traffic with the controller. Moreover, trusted certificates from a Certificate Authority can be embedded in the controller to prevent a man-in-the-middle attack, where a malicious party which happens to be on the path to the controller server pretends to be the controller.

SAFE STORAGE AND REMOVAL

Secure file erase
Automatically remove print, scan and copy jobs from the smart Inbox after the user defined time. The files erase is secure when enabling E-Shredding.

E-shredding
The e-shredding feature is a security feature which allows the system to overwrite any user print/copy/scan data after it has been deleted from the system. This feature prevents the recovery of any deleted user data including file content and file attributes, for instance if the disk is stolen.

Removable Hard disk
The optional Removable HDD Kit enables administrators to physically remove the device's internal hard disk so it can be locked down in a secure place after working hours. The drive can then easily be reinstalled for use during normal working hours.

Secure boot
Secure Boot is a security standard to make sure that the device boots using only software that is trusted. When the printer starts, the controller software checks the signature of each piece of boot software.

Data encryption
The hard disk encryption-of the POWERsync controller encrypts all files present on the entire drive (including the operating system and all data; used space encryption). The encryption mechanism is based on a Trusted Platform Module (TPM) and Microsoft BitLocker mechanism which is compliant to FIPS 140-2 certification. The AES 256 encryption method is used.

HDD destruction at the end of the contract
At the customer's request, the internal hard disk drive of the POWERsync controller can be removed and physically destroyed, ensuring no customer print data remains on the printer once it has left the customer's premises.

AUTORISATION

Control panel access lock
When enabling the access management function, the ClearConnect user control panel can only be accessed after unlocking via domain credentials or smartcard.

Secure printing via domain credentials (active directory)
The 'sensitive' print jobs sent by the job owner are not printed until the job owner authenticates on the system user panel with the correct user credentials and releases them for printing.

Secure printing via smartcard (excl. Reader)
The 'sensitive' print jobs sent by the job owner are not printed until the job owner authenticates on the system user panel by swiping and inserting the smart card and releases them for printing.

Print files only available in your Smart inbox
When disabling 'direct print' in WebTools Express, the print file will wait in your Smart Inbox until activated from the ClearConnect user panel or WebTools Express. This function prevents the print being accidently taken by other office workers.

Scan to your personal home folder
The Scan to Home Folder function is available with the user name and password authentication method. After entering authentication on the printer panel, the user can scan a file to his home directory on the network as configured for his own account on MS Windows Active directory.

Print from your personal home folder
The print from Home Folder function is available with the user name and password authentication method. After entering authentication on the printer panel, the user can print from his home directory on the network as configured for his own account on MS Windows Active directory.

Disable ports and interface
To secure the POWERsync controller from unauthorised access all unused ports and network interfaces are disabled.

Third party software such as uniFLOW
The PlotWave and ColorWave printing systems with a ClearConnect user interface can be integrated in uniFLOW environments of the customer. This gives users additional functionalities and help them to control and reduce printing and copying costs, increase document security and improve employee productivity.

HACK PREVENTION

Disabling unused protocols
Network administrators are provided with the ability to configure the specific protocols that are accessible. As a result, unwanted device communication and system access via specific transport protocols can be effectively blocked.

SNMP V3
The secure version of SNMP which provides authentication and integrity between the Network Management Station (NMS) and the managed printers.

IEEE 802.1X device authentication
To provide a port-based authentication mechanism (according to IEEE802.1X standard) allowing a device to be authenticated by a central authority in order to communicate on the network with the other devices.

McAfee antivirus (optional)
Optional possibility to install McAfee antivirus software on the POWERsync controller as additional measure to protect against virus infections.

McAfee Whitelisting Application control (optional)
Optional security feature, activated via a license. When activated and enabled, it creates a detailed list of all the files on the controller and prevents any unauthorised change, whether by malware, viruses or unauthorised users. It is constantly checking the integrity of the files against the list, and will block any tampering or unauthorised change.

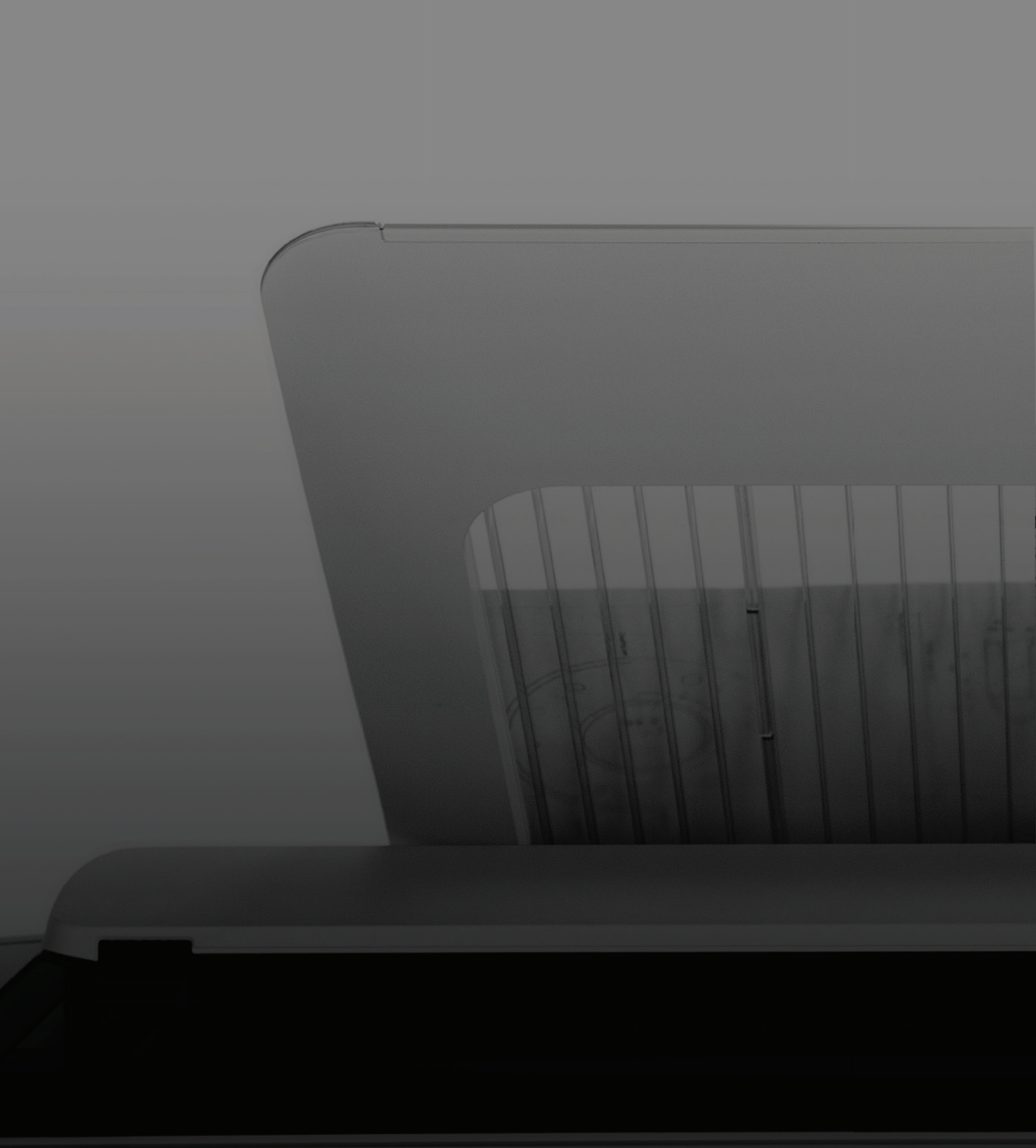
SECURE NOW AND IN THE FUTURE

Windows 10 IoT Enterprise LTSC controller software
The POWERsync controller in the printer uses Windows 10 IoT Enterprise LTSC.

Support to 2029 or beyond
Microsoft guaranties the support of Windows 10 IoT Enterprise LTSC to 2029 or beyond. This means security updates will be provided within this time period.

Remote controller security updates
Via WebTools Express, the system administrator can remotely upload and install security updates. This enables quick reaction and high uptime, as it is not necessary to arrange a physically interaction of a service engineer at the printer.

On Remote Service
On Remote Service is a service developed by Canon to ensure the highest uptime for your Canon system. As a controller embedded application, Remote Service offers you support at a distance including remote diagnostics, remote meter reading and remote assistance. The result is increased system availability, reduced administration, improved first-time service fixes, quicker response times and above all, peace of mind.



No part of this publication may be copied, modified, reproduced or transmitted in any form or by any means, electronic, manual, or otherwise, without the prior written permission of Canon Production Printing. Illustrations and printer output images are simulated and do not necessarily apply to products and services offered in each local market. The content of this publication should neither be construed as any guarantee or warranty with regard to specific properties or specifications nor of technical performance or suitability for particular applications. The content of this publication may be subject to changes from time to time without notice. Canon production printing shall not be liable for any direct, indirect or consequential damages of any nature, or losses or expenses resulting from the use of the contents of this publication.

Canon Inc.
global.canon
Canon Europe
canon-europe.com
English edition