SMARTSHIELD

Integrated printing security technology
IT security features for the years ahead
For colorWAVE and plotWAVE printers

INTREGRATED SECURITY FOR THE YEARS AHEAD

Our Large Format printers are designed to help address the security concerns of technical document users who handle confidential customer data.

SMARTshield integrated printing security technology is a range of IT security features embedded in the print workflows of the latest plotWAVE and colorWAVE T-series printers. To help keep your systems safe: now and for the years ahead.

Protect your information

More than ever, you need to protect your most important, confidential, and sensitive information within your Large Format printers workflows and on your networks. This includes information sent from individual workstations and other devices for printing 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 your own IT infrastructure via printers. This is why you need a secure Large Format printer that makes the life of your IT administrator, users and management easier.

Secure print workflow

SMARTshield supports you in creating, managing and submitting print jobs securely from a variety of devices and sources, to help safeguard data at every stage of the print workflow process.

SMARTshield incorporates multiple IT security features designed to keep users data and information safe from unwanted eyes.

In tackling their security concerns, customers are looking for ways to:

- Keep data from being captured from the network while in submission
- Keep data that’s stored on the printer secure
- Stop hackers accessing printers
- Stay compliant with the latest security standards
- Avoid confidential drawings being taken from the printer by unauthorised staff

Secure submission

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

Thanks to integration with your plotWAVE and colorWAVE T-series workflow eco-system, users can submit files from their desktop or any mobile device. With this level of flexibility and mobile access, it's essential that valuable data is submitted securely to the printer at all times and from all devices. To help protect data and user credentials while sending files to the printer, SMARTshield offers:

- Internet Protocol Security (IPSec) compatibility
- IPv6 and IPv4 compatibility
- HTTPS
- TLS/SSL protocols

Secure storage

To help protect confidential data stored at the printer from being stolen or accidentally leaked from the company or department, SMARTshield includes:

- Secure File Erase
- Secure Boot
- Removable hard disk
- Data encryption
- HDD (Hard disk drive) destruction at the end of the contract
- E-shredding

Authorisation

To ensure users identify themselves and to keep you in control of the activities, features, expenses and protocols each user is permitted to use, SMARTshield offers robust user authentication features including:

- Control panel access lock
- Password/PIN code printing
- Secure printing via domain credentials (Active directory)
- Secure printing via smartcard (excl. cards and reader)

- Only access to your personal print files in the Smart inbox
- Scan to your personal home folder
- Print from your personal home folder
- Lightweight directory access protocol (LDAP) user authentification
- Disable ports and interfaces
- Third-party software such as uniFLOW[1]

Hack prevention

To help keep hackers out and so prevent the printer from being hijacked and used against your network, SMARTshield incorporates:

- Disabling unused protocols
- Network management security features through SNMP v3
- File encryption
- IEEE 802.1X compatibility
- Trellix antivirus support
- Trellix whitelisting (optional)

IT security features

To help you keep up with hackers constant efforts to find new ways to access your valuable and confidential information, and to help ensure you conform with new legal requirements, the SMARTshield offering includes:

- **Microsoft Windows 10 Enterprise LTSC 2021 controller operating system** Supported up to 2032
- **SMARTshield CIP (Continuous Improvement Process) – Audit/ Implement/Validate/Release** SMARTshield CIP is a continuous process in which a cycle of audits (internal and external) is used to highlight potential areas of improvement. Security checks, fixes, patches and updates are an ongoing process with stringent validation and testing procedures to help keep your data security up-to-date
- **External annual security audit programme** We use an external security consultancy company to periodically conduct penetration testing, to verify the effectiveness of SMARTshield. Testing is primarily based on the Open Testing Worldwide Application Security Project (OWASP)
- **Automatically triggered notifications** for Microsoft security patches, to be installed to the administrator's specifications, so your administrators can install them from their desks, when and how they choose
- **Microsoft security patches** will be made available for the economic life of the T-series printers[2]

[1] Basic uniFLOW software is included as standard. Optional additional functionality is available for purchase. Consult your Canon representative.

[2] The expected economic life of plotWAVE and colorWAVE printers is 7 years based on Canon service data.

SMARTSHIELD CONTINUOUS IMPROVEMENT PROCESS

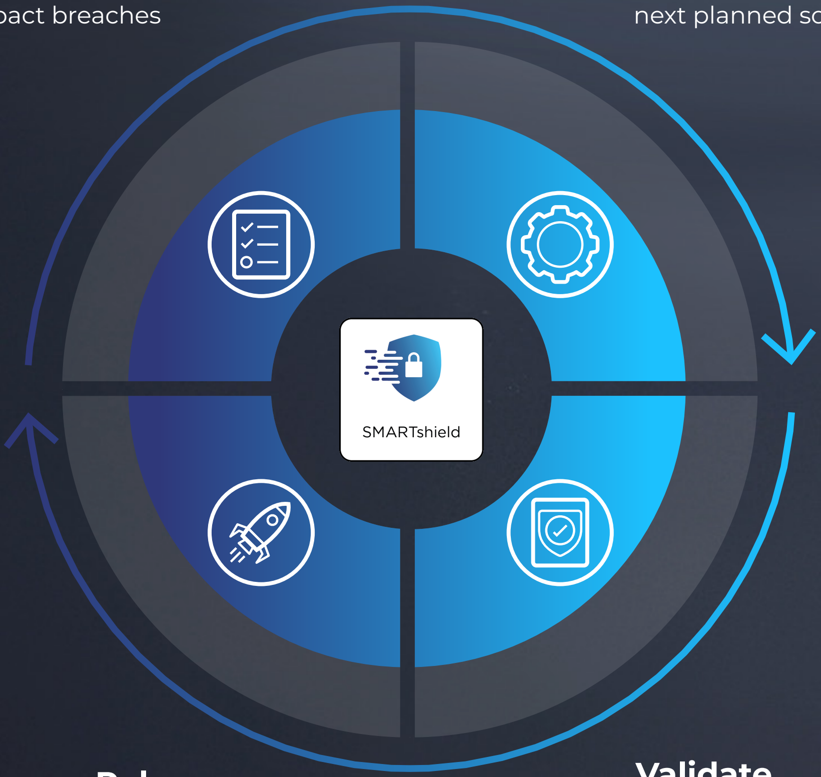
SMARTshield helps safeguard security throughout your plotWAVE and colorWAVE T-series print workflow eco-system.

Audit

Continuous monitoring of vulnerabilities[1]
Annual Security Audit Program[2]
Monitoring of new legislation
Monitoring of high impact breaches

Implement

Implement the security fixes via a patch on the current software release, or via an update in the next planned software release



Release

Release the new version of the controller or software to the market
Automatic[3] Microsoft security patch dispatch and installation on the POWERsync+ controller

Validate

Internal validation of the implemented solutions

[1] Canon continuously monitors security vulnerabilities in the wider security landscape to understand if there is the need to apply patches. https://cpp.canon/products-technologies/security/

[2] An external security consultancy company is used to periodically conduct penetration testing to verify the effectiveness of SMARTshield functionality. Testing is primarily based on the Open Worldwide Application Security Project (OWASP) top application security risks. https://owasp.org/

[3] In order to have access to the automatic dispatch of Microsoft security patches, there must be an active connection of the POWERsync+ controller with the Canon service platform: PRISMAservice. Manual downloads of Microsoft security patches are available via https://downloads.cpp.canon

SMARTSHIELD IN DETAIL

Safe submission

Internet Protocol Security (IPsec) IPv6 and IPv4 compatibility	IPsec is a protocol that provides authentication, data confidentiality and integrity in the network communication between the controller and other devices. 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 PRISMAproduce Tech 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

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

Authorisation

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.
Password/PIN code printing and secure printing via domain credentials (Active directory)	The 'sensitive' print jobs sent by the job owner are not printed until the job is selected and released with the correct password or PIN code.
Secure printing via smartcard (excl. reader) Print files only available in your Smart inbox	'Sensitive' print jobs sent by the job owner are only printed when the job owner authenticates on the system user panel by swiping or inserting the smart card releasing them for printing. 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 personal home folder	The Scan to Home Folder function is available with user name and password authentication. After entering authentication on the printer panel, the user can scan a file to their own account in their Microsoft Windows Active directory configured on the network.
Print from personal home folder	The print from Home Folder function is available with user name and password authentication. After entering authentication on the printer panel, the user can print a file from their own account in their Microsoft Windows Active directory configured on the network.
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 a customer's uniFLOW environment, to give additional functionalities and help 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 provides authentication and integrity between the Network Management Station (NMS) and managed printers.
IEEE 802.1X compatibility	Provides a port-based authentication mechanism (according to IEEE 802.1X standard), to allow a device to be authenticated by a central authority in order to communicate on the network with the other devices. Optional possibility to install Trellix antivirus software on the POWERsync$^+$ controller as an additional measure to protect against virus infections.
Trellix antivirus (optional)	Optional security feature, activated via a license. When activated and enabled, Trellix whitelisting creates a detailed list of all the files on the controller and prevents any unauthorised change, whether by malware, viruses or unauthorised users.
Trellix whitelisting (optional)	It is constantly checking the integrity of the files against the list, and will block any tampering or unauthorised change.

IT security

Windows 10 IoT Enterprise 2021 controller software supported up to 2032	The POWERsync$^+$ controller in the printer uses Microsoft Windows 10 IoT Enterprise 2021. Microsoft guaranties the support of Microsoft Windows 10 IoT Enterprise 2021 with security updates up to 2032.
SMARTshield CIP (Continuous Improvement Process)	SMARTshield CIP is a continuous process in which a cycle of audits (internal and external) is used to highlight potential areas of improvement. Security checks, fixes, patches and updates are an ongoing process with stringent validation and testing procedures to help keep your data security up-to-date.
External annual security audit programme	We use an external security consultancy company to periodically conduct penetration testing, to verify the effectiveness of SMARTshield. Testing is primarily based on the Open Testing Worldwide Application Security Project (OWASP)
Automatically triggered notifications for Microsoft security patches	To be configured to the administrator's specifications, so administrators can install them from their desks when and how they choose.
For the economic life of the T-series printers	Microsoft security patches will be made available for the economic life of the T-series printers

Seamless integration with the plotWAVE and colorWAVE T-series workflow eco-system

Integration with plotWAVE and colorWAVE T-series	To help you safeguard security throughout your print workflows.

Disclaimer 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 representation, 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 Europe
canon-europe.com
English edition