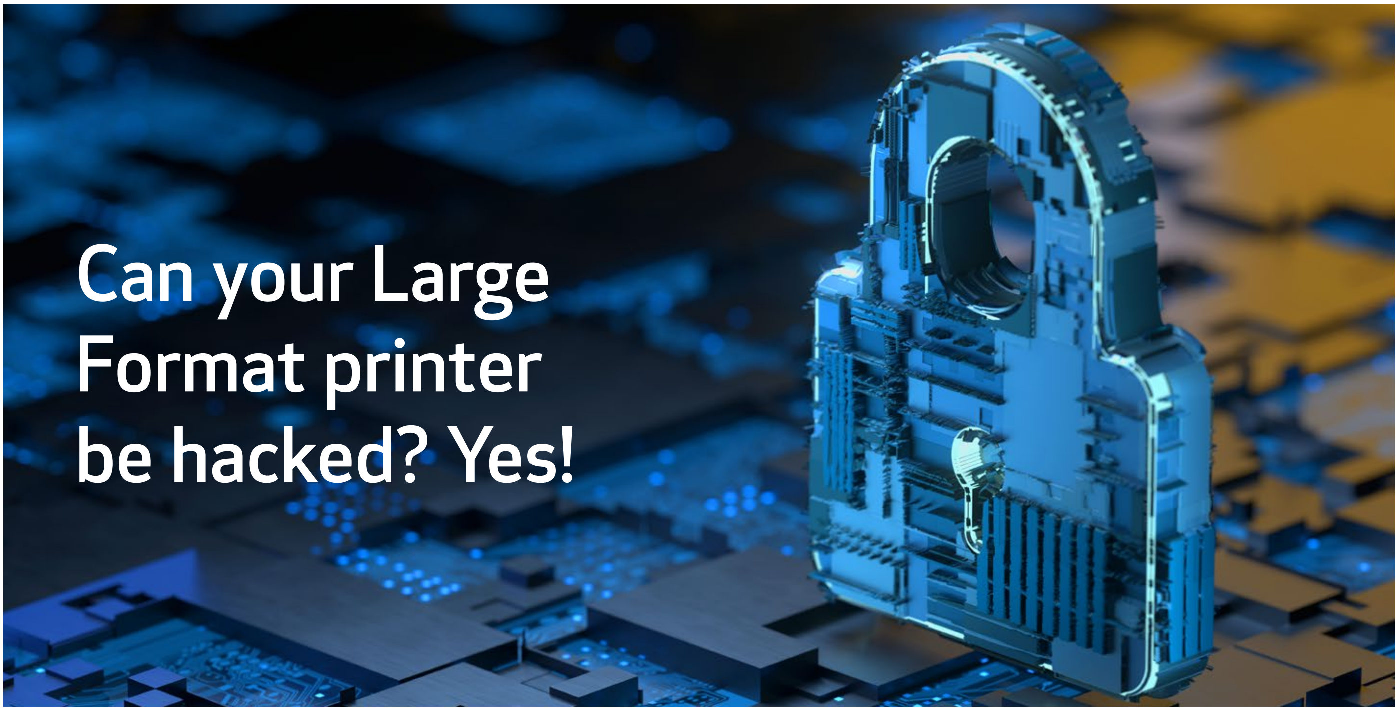
Canon

CANON SOLUTIONS AMERICA

IS YOUR LARGE FORMAT PRINTER A POTENTIAL TARGET FOR HACKERS?

SMART CHANGE STARTS HERE.



Can your Large Format printer be hacked? Yes!

If printers are connected to a company's network, they are just as vulnerable to cyber attacks as a computer. Printers may be even more susceptible given they are often times unprotected and overlooked as a network access point.

Vulnerabilities of Old Operating Systems

- End of security patch support
- Lack of integration into security infrastructure
- No smart card support
- No disk encryption
- No data erasure provision
- No certification support
- Gaps in encryption protocols
- Shared or hard coded passwords

Implications of an Unsecured Printer

- Confidential data stolen or sold
- Ransomware attack
- Monetary theft – payment details stolen
- Botnets - data theft and cyber attacks cause malfunctions and wreak havoc
- Cause malfunctions to wreak havoc
- Command your printer to randomly print
- Command your printer to shut off
- Device "bricking" – renders it useless
- Data deletion

More than ever, businesses and government organizations with Large Format printers need to protect their most important, confidential, and sensitive information within their office and on their networks. And if you are still operating on a device that is no longer receiving Security patch support, you may be more vulnerable than you realize.

SO HOW CAN YOU MITIGATE THESE POTENTIAL RISKS AND THREATS?

With Integrated Printing Security Technology

For ColorWave and PlotWave printers

This includes protecting 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 unauthorized access via printers to print data, printed information, and the end user's own IT infrastructure. For these reasons, organizations need a secure Large Format printer that makes life easier for the IT administrator, users, and management.

Our fully integrated printing security technology that is housed in the Canon ColorWave and PlotWave Series is designed specifically to address such needs, with multiple security measures designed to help keep data and information safe from unwanted eyes. Potential security risks in every stage of the workflow process are addressed.

Help support your data security initiatives now and in the future.

SAFE SUBMISSION SAFE STORAGE AND REMOVAL

Help 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 always submitted securely to the printer, from all devices.

Help 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. Encrypt data and restrict access with user identification, to help ensure all your data is kept safe. By erasing data correctly, users can help keep confidential files out of the hands of unauthorized individuals.

AUTHORIZATION HACK PREVENTION

User authorization helps restrict access to confidential files for unauthorized users.

Additionally, by requiring users to authenticate, you can keep tighter control of their activities. You want to be sure that the printer features and protocols that users can access cannot be hijacked and used against your network.

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.

SECURE NOW AND IN THE FUTURE

Security features have been designed to help keep your information secure today and going forward.

Security is not a static situation. Hackers are constantly trying to find new ways to access your valuable information.

Our security specialists are constantly monitoring the latest risks to help ensure your data and your printers stay safe.

We understand your security concerns and have put together a suite of features to help address the risks your organization faces at every stage of the workflow process, with ongoing updates to address evolving threats.

SECURITY IN DETAIL

SAFE SUBMISSION	
Internet Protocol Security (IPsec) Compatibility	IPsec is a protocol that helps provide 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 internet working 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 helps 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	
Safe Storage and Removal	Automatically removes print, scan, and copy jobs from the Smart Inbox after the user-defined time period. Secure File Erase helps to keep jobs secure when enabling E-Shredding.
E-Shredding	Allows the system to overwrite any user print/copy/ scan data after it has been deleted from the system. This feature helps prevent the recovery of any deleted user data including file content and file attributes, for example, 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	A security standard to help 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 Canon 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 customer's request, the internal hard disk drive of the POWERsync controller can be removed at the end of the contract and physically destroyed by the customer, ensuring no customer print data remains on the printer once it has left the customer's premises.

mirror_mod.use_y = True
mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active

AUTHORIZATION

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 smart card.
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 helps prevent the print from being accidently taken by others.
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 their home directory on the network as configured for the user’s 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 their home directory on the network as configured for the user’s account on MS Windows Active directory.
Disable Ports and Interface	To help secure the POWERsync controller from unauthorized 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. This gives users additional functionalities and helps 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	Provides 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 other devices.
McAfee Antivirus	Optional. McAfee antivirus software can be installed on the POWERsync controller as an additional measure to help protect against virus infections.
McAfee Whitelisting Application Control	Optional security feature, activated via a license. When activated and enabled, it creates a detailed list of all the files on the controller and helps prevent any unauthorized change, whether by malware, viruses, or unauthorized users. It is constantly checking the integrity of the files against the list and will help block any tampering or unauthorized 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 at least 2029. Microsoft will support of Windows 10 IoT Enterprise LTSC until January 2029. 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 physical interaction of a service engineer at the printer.

WHY CANON SOLUTIONS AMERICA.

Canon Solutions America recommends forward-thinking strategies to help achieve the highest levels of information management efficiency for your unique business needs. Using superior technology and innovative services, we then design, implement, and track solutions that help improve information flow throughout your organization while considering the environment, helping to result in greater productivity and reduced costs.

There are many reasons why you should choose Canon Solutions America as your provider for document management solutions. Benefits include:

- A Canon U.S.A. Company
- Business Services
- Professional Services
- Global Monitoring Capabilities
- Certified Training and Support
- Flexible Finance Options
- Single-Source Solutions Provider
- Managed Document Services
- Nationwide Coverage
- Customized Industry Solutions
- Genuine Canon Parts and Supplies
- Diverse Range of Input-to-Output Technology

But that's not all. As a company that is dedicated to your needs, we support our solutions with highly skilled professionals and advanced diagnostic systems to maintain peak performance. And with ongoing consultation, we can further your document management capabilities to help ensure the highest level of satisfaction and productivity.

Canon
CANON SOLUTIONS AMERICA

Large Format Solutions
100 Park Blvd., Itasca, IL 60143

CSA.CANON.COM
1-800-714-4427 | us.info@csa.canon.com

Canon is a registered trademark of Canon Inc. in the United States and elsewhere. ColorWave and PlotWave are registered trademarks or trademarks of Canon Production Printing Netherlands B.V. in the United States and elsewhere. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged. Neither Canon Inc. nor Canon U.S.A., Inc. nor Canon Solutions America, Inc. represents or warrants any third-party product or feature referenced hereunder. Specifications and availability subject to change without notice. Not responsible for typographical errors. Canon Solutions America does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, CCPA, GDPR, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Some security features may impact functionality/performance; you may want to test these settings in your environment.