SECURITY WHITEPAPER

PRISMAsync print server

PRISMA sync

PRISMA

Canon

EXECUTIVE SUMMARY

Protecting valuable customer data has become a key part of any print provider's business. Today's high-end printers are usually connected to networks, other devices and the cloud. This offers great ease of use and productivity, but also provides inherent security risks. PRISMAsync print server is designed with efficiency and safety as priorities: a fast, secure data funnel.

PRISMAsync has a unique security architecture:

- Data security: customer data is never shared outside the printer, unless the system administrator gives permission. Machine and configuration data are shared only with permission.

- Software security: PRISMAsync includes only the essential software for print functionality. These software packages run 'sandboxed' – confined to specifically allocated disc and memory space, with only the minimum in required network communication.

- Network security: PRISMAsync permits access only to authorised users, communicates through secure protocols and interfaces and is selective in which applications to connect.

- Access security: PRISMAsync has a robust user roles and permissions system that defines exactly who has access to what and can also be connected to local user management.

- Device security: Unlike most other print servers, PRISMAsync runs on a dedicated device and uses a long-term service branch of Microsoft® Windows without unnecessary applications. McAfee® Embedded Control is available as a powerful security multiplier, blocking any unauthorised changes to software and operating system.

PRISMAsync print server: ready to provide maximum security from the moment you first turn it on.

CONTENTS

DOCUMENT VERSIONING

VERSION	DATE
Mark 7	Nov 28, 2019
Mark 8 & up	March 1, 2022

1 INTRODUCTION

This security whitepaper provides information about how the PRISMAsync print server fits into a network in terms of security features and system architecture. It explains the measures Canon takes to help you address the major security risks inherent in today's highly networked business environments on each of the relevant conceptual levels. Our security policy, and the products developed based on it, allow you to create a secure environment for printing, scanning and copying. If any new security threats arise, we are able to identify and address them quickly – thanks to our active involvement with customers, government agencies and security organisations. Because of these measures, you can be confident that PRISMAsync contributes to a safe and secure IT environment.

As print provider, you are entrusted with your customers' valuable data. Whether you are printing bank statements with personal information, reports and drawings that have commercial value or documents with sensitive content, you want to be certain that nobody else can get access to that data on your devices. At Canon, security is an integral part of product development. We take a pro-active approach to ensure the highest possible security level. Our design inspiration comes from concepts that go well beyond legally required security levels.

The PRISMAsync print server is designed from the inside out for security and peace of mind. Unlike other print servers, PRISMAsync is a dedicated solution that is an integral part of the printer. It is not a standalone personal computer that operators could also use for their email, break-time games and other office activities. PRISMAsync is maximally shielded from the outside world, without unnecessary features that may provide access to hackers or viruses. In addition, PRISMAsync can only be operated directly from the user interface of the printer or other secure interfaces.

2 PRISMASYNC: HIGHLY SECURE EASE OF USE

Often, people seem to think the only goal of security is to keep people out of a system or a network. But security is both about keeping the wrong people out and giving the right people enough access and ease of use to achieve their goals. This is known as the CIA triad – the balancing act between the confidentiality of stored and processed data, the integrity of that data and the availability of data and services. In addition, there are matters of compliance to keep in mind, for instance with regulations such as the EU General Data Protection Regulation (GDPR).

A properly secure print server should provide user-friendly access to print functions while protecting user, job and machine data. Its very purpose is to quickly and efficiently receive, translate and export data from users to the printer, so the requested documents are printed right away at the right quality. The print server should be kept safe from intrusions from the outside, the data on the print server and on its way to it should be safe from interruptions, spying or tampering, and there should be as few potential route of infection for the print server as possible.

For that reason, the PRISMAsync print server is designed to be secure from the inside out. Data security is guaranteed on all conceptual levels. Accessing data is only possible through controlled PRISMAsync interfaces.

A SECURE SYSTEM IN A SECURE COMPANY

The CIA triad shows there is often a trade-off between security and ease of use. Security procedures are necessary to keep any system safe. However, especially in work environments with a high workload, end users tend to prefer systems that are open and easily accessible – even to the point of taking security risks that make using the system a little easier. PRISMAsync is devised to be both easy to operate and secure, respecting the time and interests of operators and not burdening them with overly complex demands. Regardless, security is as good as its weakest chain.

We strongly recommend that end users combine PRISMAsync security features with other safeguards to secure the system and network well. The optimum in security can only be reached if your entire company practices secure operations: a strong password policy that includes regular updating of passwords, quick response to available updates, and good security around the physical environment of the printer, any Public Key Infrastructure (PKI) and Near-Field Communication (NFC) smart keys, and your computing network. Security is a state of mind.

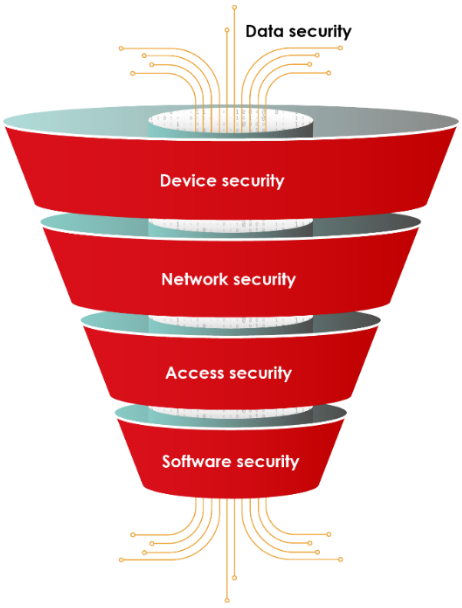
3 PRISMASYNC SECURITY ARCHITECTURE

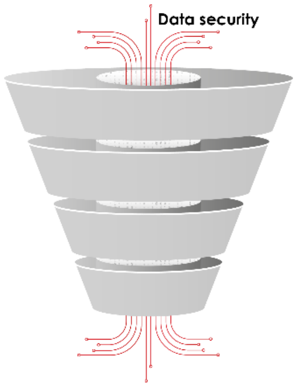
PRISMAsync is designed to be more than just a controller. It is a firewall between the network your printer is on and the printer itself. Once your data and that of your customer enters PRISMAsync, our software architecture ensures its security through:

Device security – secure device architecture
Network security – secure communications
Access security – limiting data access to the right people
And software security – secure software programs and applications

The crucial difference between most other print servers for production printers and PRISMAsync is that the other print server software usually runs on a PC with a standard Microsoft Windows operating system, which may allow installation of other software. PRISMAsync, in contrast, is a dedicated hardware/software solution that is embedded in the printer, operated through dedicated user interfaces and is not used for other tasks.

Another difference is that PRISMAsync is set up fully secure before delivery. There is no need to configure the hardware to ensure security before first-time use. You can rest assured knowing that you are adding a piece of hardware to your network that is secure out-of-the-box, rather than one that a company's IT team will need to invest time into configuring.





3.1 DATA SECURITY

Protecting your customer's data is the heart of security. Your organisation and your customers need to be able to trust your security measures. Print servers such as PRISMAsync deal with different types of data, which require different security approaches.

- **Customer data** is the content of the documents that are printed, scanned or copied. This includes job names and instructions for printing and finishing the document.
- **Machine data** concerns machine performance information, such as toner levels, nozzle status and media use.
- **Configuration data** describes the way PRISMAsync is configured, which may include usernames and passwords.

Customer data flows through the print server to the printer. Machine data and configuration data stay on PRISMAsync. In PRISMAsync, the different data types are processed and stored entirely separately.

Customer data is the content of the documents. This includes job names and instructions for printing and finishing the document. Customer data cannot be viewed outside the printer, unless the system administrator allows it to be. For instance, by allowing PRISMAsync Remote Manager to show customer data on a different location. The rest of this whitepaper will explain the security features that guarantee the safety of customer data.

Machine data is what your service technician needs to know to keep your print system in optimal condition. Still, even this data may be valuable

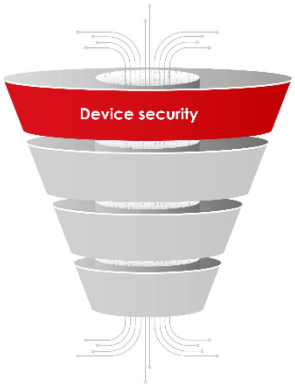
in the wrong hands, for instance by offering your competition insight in your performance. PRISMAsync is set up so that machine data can only be communicated to a secure service laptop or, if the system administrator grants permission, to Remote Service. Remote Service communicates through a fully secure channel and is linked to your service number. It is a worldwide service to increase uptime, offering preventive capabilities such as remote diagnosis and assistance. Remote Service is ISO/IEC 27001 certified (by the International Organisation for Standardisation and the International Electrotechnical Commission), demonstrating a high level of precautions to secure your machine data.

Configuration data can be accessed and changed by the system administrator or similar, custom, high-level user profiles. This is the data that describes how PRISMAsync is set up. It contains printing defaults, hot folders, colour configuration etc. Since PRISMAsync can be allowed to connect to your network, configuration data can also include passwords

The system administrator can change, add and delete user accounts and passwords and determine how data backups should be handled:

- Exclude customer data from the backup
- Include customer data in the backup, encrypted with an additional passphrase
- If customer data is included, export of backups can be:
    - Disabled completely, so the data – even in backup form – stays on the print server
    - Allowed by system administrator only
    - Allowed by system administrator and service operators

For security reasons, it is impossible to export customer data unencrypted.



3.2 DEVICE SECURITY

The PRISMAsync print server consists of more than just the print server software. Since it runs on a device embedded in the printer itself, extra attention has been paid to securing this Microsoft Windows-based environment. The design choices in hardware, operating system and crucial software provide the rock-solid foundation of PRISMAsync security.

EMBEDDED IN THE PRINTER

PRISMAsync print server is embedded in the print engine and set up for full security before delivery. This has some definite advantages. Because the print server cannot be used for other tasks – email, job preparation, web browsing, YouTube, social media, etc. – it does not need the full complement of software and accessibility features of a regular office computer. This mitigates many of the existing security risks.

SECURE BIOS AND OPERATING SYSTEM

We use a non-commercial off-the-shelf version of Microsoft Windows operating system that comes with prolonged support. This version is hardened (stripped to the essential services that are needed for the PRISMAsync purposes) and therefore is not affected by most of the vulnerabilities reported for the COTS (commercial off-the-shelf) Windows version. All vulnerabilities reported by Microsoft for the Windows OS are evaluated by Canon to determine whether they are relevant and whether a patch needs to be applied to our products.

To prevent any unauthorised access to both BIOS and operating system, each PRISMAsync print server is installed with randomised, strong administrator passwords that prevent any entry. The only connections anyone can make with the system are through the PRISMAsync print server and service software. As the Windows administrator passwords are randomised at installation, no one knows these system passwords. This is a good security measure because nobody needs access to the BIOS or operating system.

SECURED USB AND MASS STORAGE DEVICES

Plugging in USB devices is an easy way for a system to get infected with a virus or malware. By design, PRISMAsync print server is set to provide limited permissions to USB sticks and other mass storage devices, so they cannot be used to install anything.

It is also possible to restrict USB access even more, blocking all USB devices outright. Note that this also blocks devices such as USB keyboards and the use of PKI smart cards (which require a card reader) for key operators and service personnel.

MCAFEE EMBEDDED CONTROL

A powerful multiplier for the security of the PRISMAsync print server is the McAfee Embedded Control licence (also known as the Integrity Checker). This is a standard part of the PRISMAsync resale licence for some series of Canon printers and an optional security add-on for others. Unlike a virus scanner, which can create a security risk if you do not keep it constantly updated with the latest virus definitions, McAfee Embedded Control has a detailed map – a ‘fingerprint’ or ‘safe list’– of all the files on the print server and prevents any unauthorised changes, whether by malware, viruses or unauthorised users. It is constantly checking the integrity of the files against the known fingerprint, and will block and report any tampering or unauthorised change. The use of McAfee Embedded Control is possible because PRISMAsync is a closed system, where the software only changes after installation of a curated and signed software update. After each update, your print server also receives an updated fingerprint map.

In fact, McAfee Embedded Control makes a virus scanner unnecessary. With McAfee Embedded Control, your device is secure from most viruses or malware because McAfee Embedded Control continuously checks for differences with the approved software and files and blocks any attempts to take advantage of known exploits. This keeps your device safe even if it is running legacy Microsoft Windows versions that are no longer supported. The other PRISMAsync design choices already provide great security. By adding McAfee Embedded Control, your security becomes ironclad.

THREAT DETECTION AND LOGGING

PRISMAsync is set up by design to monitor and log intrusion attempts and incorrect logins. Automatic IP blocking is available.

In addition, audit logging (see the Access Security chapter for more information) can provide another layer of monitoring. McAfee Embedded Control can be set to export its threat detection logs to the audit log, allowing them to be accessible when needed.

DISC ENCRYPTION AND PHYSICAL PROTECTION

To protect data at rest, encrypted PRISMAsync hard drives cannot be read even if they are physically taken from the machine. In many Canon printer types, the PRISMAsync print server is physically embedded within the printer, making it almost impossible to remove it from the printer. With other printers, such as the Canon imagePRESS series, PRISMAsync runs on a separate computer. In that case, the PRISMAsync hardware comes with a metal security eye that can be locked with a chain to prevent opening up the computer to take out the hard disc or even taking the entire PC. There is also the option to order a cabinet with a lock.

E-SHREDDING OF DATA

A print server is not intended to be an archive of all printed jobs. That is why it is best practice to set up PRISMAsync to remove job data from the print server after printing. Making sure that data is removed within the proper time frame is also an important part of staying compliant with regulations such as the GDPR. The e-shredding function, available through a licence and compliant with the NIST SP 800-88 standard, securely erases printed jobs from the printer. This prevents the possibility of recovering data from printed jobs.

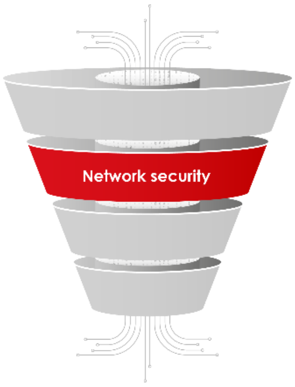
When e-shredding is enabled, three types of data are e-shredded: the submitted Page Description Language (PDL) data, bitmaps generated by the ripping of the job, and thumbnails that are generated for job previewing.

E-shredding is a continuous process that runs in the background, during and right after printing. You can configure the number of e-shredding passes between one and three, with one as the default.
E-shredding is immediate, depending on the number of passes and the system load at that moment.

There are three shredding moments. First, immediately after the job is printed, unless the printed queue (history) is enabled. In that case, e-shredding starts after the job is deleted from the printed queue. Second, when job settings are changed and the job requires a re-rip. In that case, bitmaps of the previous rip are e-shredded. Lastly, e-shredding occurs when a job is explicitly deleted from the queues or DocBoxes.

DECOMMISSIONING

If it ever becomes necessary to decommission your Canon printer, the decommissioning function will destroy all data on the PRISMAsync print server permanently, preventing any recovery. To make sure the PRISMAsync print server – and thus the printer – is not rendered unusable by accident, decommissioning requires the participation of Canon service personnel.



3.3 NETWORK SECURITY

Today's printing environments are highly connected. By transferring data through networks, you get access to functionalities, capabilities and analysis methods that would otherwise be out of reach. However, setting up a connection and transferring data inevitably introduces additional security risks that need to be addressed.

PROTECTING DATA IN TRANSIT

To prevent data packages from being intercepted or copied, PRISMAsync permits only authorised users and groups to access the print engine and make prints, limiting device communications to designated IP addresses and controlling the availability of individual network protocols and ports as desired.

3.3.1 SECURE CONNECTIONS

An important part of network security is establishing secure connections. PRISMAsync works with several connection protocols and interfaces. To reduce the opportunities for attack, PRISMAsync only enables the network ports that are in use; all other ports are automatically disabled.

HTTPS

You can configure PRISMAsync to only communicate over computer networks through HTTPS, an encrypted, secure extension of the Hypertext Transfer Protocol (HTTP), to protect the privacy and integrity of your data. HTTPS helps ensure that the other party is authentic and safeguards against eavesdropping or tampering with data. Moreover, trusted certificates from a Certificate Authority can be embedded in the print server to prevent a man-in-the-middle attack, where a malicious party which happens to be on the path to the print server pretends to be the print server.

IPPS

PRISMAsync can also use the special Internet Printing Protocol Secure (IPPS) to communicate with other applications. This network printing protocol was designed especially for communication with print servers and other devices and applications, for instance on other computers, mobile phones, tablets, etc. IPPS can be used to submit and stop print jobs, check printer status, view the progress of the print job, and other actions. IPPS connections can be used on your local network and on the internet, and support access control, authentication and encryption.

IPSEC

Internet Protocol Security (IPsec) is another encryption protocol that provides integrity and privacy in network communication. The secure IPsec network protocol suite authenticates and encrypts the packets of data sent over an internet protocol network and is used in Virtual Private Networks (VPNs). In an IPsec connection, sender and receiver establish mutual authentication before exchanging any data. IPsec secure communication is also how the different computers within a single Canon printer communicate, for instance the three computers within the iX-series. Like HTTPS, IPsec can also work with trusted certificates from a Certificate Authority.

PORT-BASED AUTHENTICATION (IEEE 802.1X)

PRISMAsync supports the use of Port-Based Network Access Control (PNAC), specifically IEEE 802.1X (from the Institute of Electrical and Electronic Engineers), for authenticating devices that want access to a local network. The device requesting access provides the required credentials – username and password, or a permitted certificate – to the network switch or access point (the 'authenticator'), which can allow or prevent the new device from participating in network data traffic. The authenticator then checks with a trusted server whether to allow the new device onto the network and which settings to use.

3.3.2 SECURE APPLICATIONS

Another important part of network security is being selective in which applications you connect to. A secure connection is meaningless for your network security unless the third party you are connecting to also follows good security practices.

SHARING CUSTOMER DATA: PRISMASYNC REMOTE MANAGER

PRISMAsync Remote Manager enables you to view customer data – print jobs – on other devices than the printer, and potentially to download it. Remote Manager is a web interface hosted on the PRISMAsync print server, which other computers can connect to through a secure HTTPS connection. PRISMAsync Remote Manager can be configured to be accessible only to authorised users. Each user can be granted different levels of access as needed. Data is stored and kept at PRISMAsync until an explicit download is requested. It is possible to disable downloading.

With PRISMAsync Remote Manager, you can control multiple PRISMAsync print servers and print engines. Remote Manager clusters them in groups, to facilitate backing up data or doing load balancing during busy times. To add an engine with a PRISMAsync print server to a cluster, it needs to pair with another PRISMAsync print engine in that cluster. The other cluster engines will automatically accept the new member. This pairing can only be done by a system administrator, and clusters are secured with cluster keys.

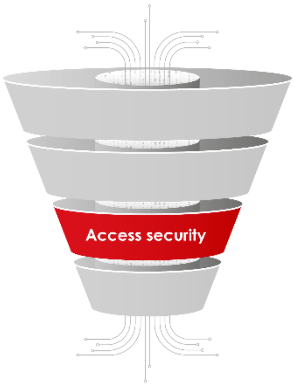
SHARING MACHINE DATA: REMOTE SERVICE AND OTHER APPLICATIONS

Machine data is valuable and can be used by several optional applications. Only one port in PRISMAsync is used to share machine data, even when multiple applications interact with the server. The system administrator must grant permission for communication between PRISMAsync and these software tools.

Remote Service is a service tool that is standard on almost all Canon printing systems and print servers. Authorised service organisations use this online tool – with your permission – to distribute, gather and interpret machine data. Remote Service optimises uptime, offers a quick service response and reduces maintenance time. Remote Service only has access to machine and configuration data, and does not share those with third parties. Remote Service is ISO/IEC 27001 certified, providing the assurance that the Canon organisation and Remote Service is transparent, pro-active and focused on security.

PRISMAlytics Dashboard is an application that enables operators to monitor the performance of printers over time, for instance to measure ink usage or uptime over time. PRISMAlytics Dashboard only has access to machine and configuration data – and not ever customer data. The machine and configuration data in PRISMAlytics Dashboard are never shared with third parties.

PRISMAsync Remote Control is a tool running on smartphone operating systems that alerts operators when an intervention is needed (such as refilling paper) even when they are not nearby. PRISMAsync Remote Control only has access to machine and configuration data, and does not share those with third parties.



3.4 ACCESS SECURITY

A basic security principle is restricting information to only those who need it. PRISMAsync print server has a sophisticated, flexible system for defining user roles and permissions. You can define up to 100 users and 100 user groups with specific access rights, including numerous options such as access to strictly personal jobs, access to all jobs, access to the control panel, full access to administrator tasks, etc. Each user can be part of several user groups. Regular prompts to change passwords help enforce a strong password policy.

PRISMAsync can be added to a domain controller, making it possible to use the Lightweight Directory Access Protocol (LDAP) access protocol for user and group authentication. It is also possible to give users access to the printer through PKI smart cards or NFC cards, which carry user authentication data and can be used to sign in more quickly.

By default, PRISMAsync Print Server comes with 6 factory-defined user groups: operators, key operators, central operators, maintenance operators, system administrators and service operators, each with different privileges. For the full specifications of the PRISMAsync access control options, please refer to the security data sheet available from Canon.

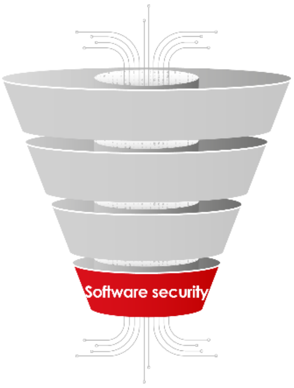
AUDIT LOGGING

Audit logging can be enabled to track all activities done on the device and modifications to the system. The traces, optionally including those from McAfee Embedded Control, are then sent to an external server set up for that purpose. For many companies, audit logging is required for compliance reasons. But it also provides an extra layer of security. More details on how to configure audit logging, and the details of the information that is recorded, are available in the PRISMAsync manual.

SERVICEABILITY

To allow your print engine to be serviced without sharing the administrator passwords with service personnel from outside the company, it is possible to enable SAM key access. These USB-based keys give access to those parts of the system that are necessary for servicing without exposing user, customer or job data.

SAM key validity can be determined by the machine itself though an algorithm, so it does not require an account or a password. SAM keys need to be validated by Canon at regular intervals and can be invalidated remotely. This provides additional protection against loss and fraudulent use.



3.5 SOFTWARE SECURITY

Some software is essential for any print server: to create bitmaps for the print engine, a print server uses Page Description Language (PDL) software and a Raster Image Processor (RIP). The PDL describes the appearance of the printed page on a high level and the RIP rasterises the PDL data into a bitmap. This software is an essential part of every print server. However, all interactions carry a security risk: incoming and outgoing data may be intercepted, and data that is being read or written may be found and read by other software, whether on the same computer or over a network.

SANDBOXING

To prevent any unauthorised person or program from accessing the crucial functions and working data of the PRISMAsync print server, the PDL, RIP and all other necessary processes are 'sandboxed'. The data they process is confined to disc and memory space allocated specifically for this purpose. Communication with the network and other running software is heavily restricted. This prevents data from leaking, viruses from spreading and unauthorised agents from listening in – even if they have bypassed all other security measures. The only connections allowed into and out of a sandboxed program are those necessary to run the specific process, e.g. receiving incoming jobs and sending bitmaps to the print engine.

NO ADMINISTRATOR RIGHTS

Another integral security feature of PRISMAsync is that individual programs running on PRISMAsync have no administrator rights or write permissions when communicating over the network, for instance for receiving jobs or communicating that a job is complete. This is a redundant measure: in the highly unlikely event that a part of the PRISMAsync software were to be compromised, it cannot infect or change other components.

SOFTWARE SCANNING AND SECURE SOFTWARE DEVELOPMENT

PRISMAsync was developed from the ground up with security in mind and with the functionality to help you stay compliant with the law. As part of that, Canon uses static and dynamic software analyses. To ascertain yourself of the security status of the PRISMAsync software, you can do the same analyses yourself. We use:

- SonarQube and TFS for code review
- Nessus and Qualys® for vulnerability scanning and dynamic application security testing (DAST); this is repeated quarterly at Canon

4 UPDATES AND UPGRADES

Every computer system needs to be updated and upgraded regularly to be maximally secure. This is the responsibility of your system administrator or key operators. However, PRISMAsync has several features that make updates and upgrades better and easier.

UPDATES

Security and maintenance patches are free of charge during the period of the service contract. The PRISMAsync development team is continuously monitoring the international threat situation and any news about new vulnerabilities. We do our best to make updates available in a timely fashion throughout the print server's supported life, whether created by us or Microsoft. Updates are signed either by Canon or Microsoft, and only those signed updates can be installed on PRISMAsync.

UPDATE SCREENING

The PRISMAsync development screens Microsoft Windows updates, filtering out the many non-security-related updates that have no bearing on the performance of your PRISMAsync print server. Because PRISMAsync runs on a locked-down version of Windows, many functionality updates can safely be left out. As a result, you experience less unscheduled downtime installing updates and rebooting your printer, and a much lower risk that the update breaks something important and has to be rolled back. Installing all available Windows updates is not only useless but may actively increase security and functionality risks.

THIRD-PARTY VULNERABILITIES

Occasionally, vulnerabilities arise from third-party open source software. Canon uses the WhiteSource open source scanning software to track known vulnerabilities and provide patches for them through our PRISMAsync update channels.

UPDATE TIMING AND AUTOMATIC UPDATES

For important security threats, Remote Service will make sure that you receive the update as soon as possible. From PRISMAsync 7.1 onwards, the system will prompt and offer updates automatically, making it even easier to respond quickly to the availability of a new security update.

Canon only guarantees security for systems that are up to date with all security patches.

UPGRADES

Functional upgrades of the system are made available for sale regularly – at least once per year –

or are included in your service contract. These upgrades usually also include important security upgrades. Older systems, for which no patches and updates are released anymore, need to be upgraded to or replaced by a newer version for continued support.

5 CONCLUSION: INSIDE-OUT SECURITY

The model of data security as a vault, where keeping others out means you are safe, is no longer good enough in today's world. In our highly networked business environment, customer data is continuously received, processed and printed or scanned, processed and uploaded. A print server is open to the world. Therefore, we designed PRISMAsync print server to be intrinsically accessible and secure – a leak-proof funnel, providing efficiency and productivity.

As an embedded print server, PRISMAsync is shielded from unnecessary changes and functionalities such as email or social media, and even from unnecessary Windows updates. Even more importantly, the design choice to run all processes sandboxed from each other minimises the risk that data can be shared or accessed in any unintended ways.

Canon is proud that our embedded PRISMAsync print server provides maximum security for your valuable customer data from the moment it is delivered. PRISMAsync is safe from the first time you turn it on. After that, Canon continues to provide updates and upgrades, and supports print providers in maintaining the print server's high level of security.

Although security is never 'done,' Canon PRISMAsync can support decision makers as an intrinsically secure element in any well-thought-out security strategy.

Canon