Powered by Cartadis

Optimize and Secure your Print Flows with Gespage

White Paper

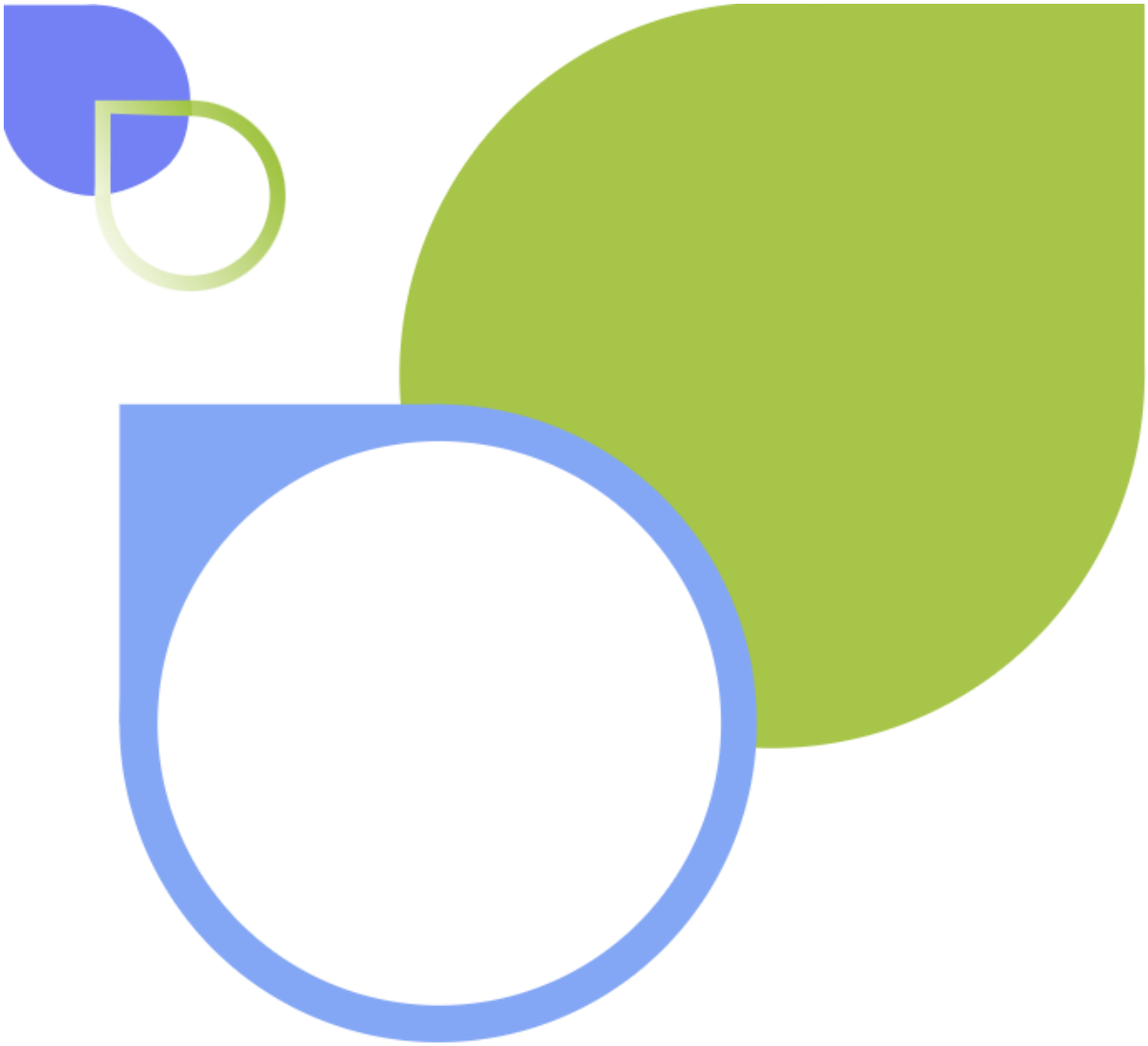


Table of Contents

1. Introduction

Did you know that 67% of organizations experience data loss each year due to unsecured printing? Faced with this major challenge, Gespage effectively secures your print workflows by ensuring complete protection of sensitive information while optimizing costs and facilitating compliance with international regulations such as GDPR.

In a business world where data is a valuable asset, print workflow management and security are becoming critically important. Too often overlooked, the print environment can become a gateway for security breaches or a source of costly inefficiencies.

Gespage, Cartadis' flagship print management solution, addresses these challenges with a comprehensive and innovative approach.

This white paper explores how Gespage helps you optimize your print workflows while increasing security and reducing costs, all while complying with regulations such as GDPR.

According to Quocirca's "Print Security Landscape 2024" report, print security remains a major challenge for organizations. Here are some key statistics from the report:

- **Print-related data breaches**: 67% of organizations reported data losses over the past 12 months due to unsecured printing practices, up from 61% in 2023.
- **Confidence in the security of the printing infrastructure**: Only 43% of organizations say they are fully confident in the security of their print infrastructure.
- **Costs of data breaches**: Mid-sized companies are particularly affected, with breach costs reaching 1 million pounds.
- **Importance of printing for business**: 71% of businesses believe that printing will be very important to their operations over the next 12 months.
- **Satisfaction with print security**: Only 16% of companies say they are "very satisfied" with their print security in 2024, a figure that has been declining since 2022.

These data underscore the critical importance of strengthening security measures around print infrastructures to protect organizations' sensitive information.

2. Low-level security of the entire infrastructure

It is important to recognize that print workflow security requires securing the entire printing infrastructure.

It starts with the printer, then continues through the company's network architecture, and ends with the print server.

2.1 Securing Printers

Multifunction printers come with a multitude of protocols and services and are often overloaded with features that are not necessary in a specific business environment.

To minimize vulnerabilities, it is essential to place them in monitored locations, implement a secure printer configuration, and regularly update its firmware.

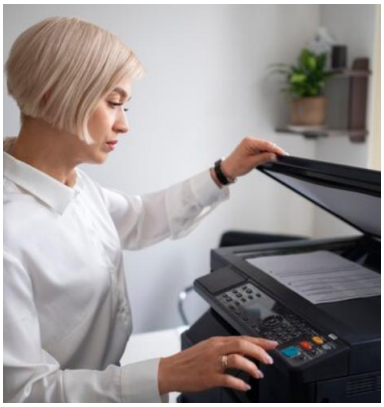
Below we provide standard best practice recommendations for securing printers. **We also recommend contacting your printer or MFP vendor for their specific security recommendations.**

Securing the location

The risk of attacks can be significantly increased if printers are placed in vulnerable areas where they may be misused. Installing printers in secure locations accessible only to authorized personnel is a simple solution to reduce security risks.

Educational institutions and campuses are particularly at risk, especially when printers are easily accessible to students.

To enhance physical security, the following measures can be implemented:



- **Securely fix the printer** to the building to prevent theft or unauthorized handling.
- **Disable USB ports** to prevent access to unauthorized external devices.
- **Secure network connections**, for example by securing network cables to prevent tampering.
- **Lock the paper trays** in order to limit theft or prevent misuse.

Password management

Default administrator passwords are often known, exposing devices to potential intrusions. Therefore, it is crucial to replace these passwords upon installation and change them regularly. Additionally, choose complex passwords to protect critical settings, such as network configuration, from hacking attempts or unauthorized changes.

Securing protocols and services

When configuring your printer, it is recommended to disable protocols and services that are not used in your infrastructure. Here are some of these as an example:

- **Printing protocols** : A printer can support various printing protocols (IPP, JetDirect, LPD, AirPrint, FTP, etc.). It is recommended that the most frequently used protocols implemented in your infrastructure are IPP and JetDirect.
- **Remote control** : This option may cause security issues, it is recommended to enable it only for limited periods of time and only when necessary.
- **Storing print data :** Some printers allow print jobs to be stored on their internal memory for later reuse. While convenient, this feature can pose risks if confidential documents are accessed without proper protection. A strict policy should define what types of documents can be stored and enforce password protection. When this feature is not necessary, it is recommended to disable it or use an automatic data deletion option.

Encryption of sensitive data

Modern devices often include advanced features, such as full hard drive encryption using standards such as AES (Advanced Encryption Standard). Enabling this option is recommended to ensure that all data stored on the device is protected from unauthorized access.

Dedicated data security solutions

Some manufacturers also offer comprehensive sets of security features bundled into "data protection kits." These kits, which include options for secure data deletion, encryption, and sensitive print management, can be essential in environments requiring an important level of protection. Ensure these kits are installed and properly configured if your organization manages critical data.

Printer firmware updates

Finally, it is essential to regularly ensure that the printer firmware is up to date.

Printer and MFP manufacturers are increasingly focusing on security by regularly releasing updates to address identified vulnerabilities. Therefore, it is essential to implement a policy of periodically updating the firmware of your printers and MFPs to benefit from essential fixes and security improvements.

In particular, the encryption protocols used by printers are constantly evolving. Regular firmware updates ensure that your devices use modern and robust encryption protocols, thus strengthening protection against potential attacks.

Modern systems automatically negotiate the most robust security protocol when communicating between devices. For example, solutions like Gespage are designed to work with the latest TLS algorithms while maintaining compatibility with devices that have not yet been updated. This ensures an optimal balance between security and functionality.

Recommendations:

- Schedule regular **checks of firmware versions** for all your devices.
- Identify printers using outdated protocols and **prioritize updating them**.
- If possible, **automate** update processes to minimize the risks associated with outdated firmware.

By following all these best practices, you will strengthen the resilience of your printing infrastructure against emerging threats while optimizing compatibility and performance.

With Gespage, you also benefit from dedicated technical support and an active community, guaranteeing fast and efficient assistance.

Furthermore, we remind you that it is essential that you contact your printer and MFP supplier when setting up specific configurations.

2.2 Network security

Multifunction printers require network access to communicate with Gespage or receive prints. However, if improperly configured, these connections can open vulnerabilities in your infrastructure. Careful management of access and protocols is essential to ensure optimal security.

Isolation of devices on the network

Create dedicated subnets or use VLANs to isolate your printers from other segments of your infrastructure. Allow only the print server to communicate with the MFPs. This control can be enforced with access control lists (ACLs) and IP filtering rules. This significantly reduces the potential for exploitation if a device is compromised.

The details of the network flows used between Gespage and the printers and MFPs are available in the **Gespage network flow matrix** available on the Gespage knowledge base (link).

If this setup is not possible in your network configuration, it is usually possible to restrict printing to the print server's IP address in the printer settings. This configuration is particularly recommended in paid environments.

Encryption of network connections

Enable HTTPS connections on your printers to protect sensitive data transmissions. Configure your devices to use the latest versions of TLS protocols, which offer a high level of security. Older standards should be disabled as they are vulnerable to attacks.

By default, Gespage requires the use of at least the TLS 1.2 protocol by printers and MFPs.

Using Certificates to Secure TLS

To prevent man-in-the-middle attacks, configure your devices to require valid certificates for TLS connections. If the risk is low, a self-generated certificate may be sufficient while still ensuring encrypted communications.

Depending on your printer or MFP model, setting up a certificate requires additional specific settings in the Gespage eTerminal. These specific features are documented in the Gespage manuals and knowledge bases.

By combining these measures, you can transform your printing infrastructure into a resilient network, capable of meeting daily needs while minimizing security risks.

2.3 Gespage On-Premise Print Server

The Gespage print server and application server (which can be hosted on the same server) are strategic elements of your infrastructure. They centralize printing resources.

System Updates and Protection

It is essential that your servers hosting the application server and the Gespage application server are secure. This security is based on IT best practices. This includes:

- **Regular operating system updates** : Ensure your operating system is up to date to address vulnerabilities. These updates should be performed following best practices for prior backup.
- **Antivirus and firewall** : Enable real-time protection and configure firewalls to limit unauthorized access.

- **Regular updates of printer drivers** : Regularly ensure that printer drivers are up to date by contacting your printer supplier to find out which drivers are recommended for your environment.
- **Secure administrator access** : Administrator access to the operating system must be strictly reserved for authorized members of the IT team responsible for server administration.

Secure network configuration

With Gespage, print servers can be placed in isolated subnets and protected by firewalls. This ensures that internal IP addresses are not accessible from the outside. Gespage can also limit communication between the server and printers, reducing the attack surface.

The complete details of the network flows used by Gespage as well as by your infrastructure (printers, user workstations, etc.) are available in the network flow matrix, which can be consulted on the Gespage knowledge base (link).

End-to-end encryption

All network communications with the Gespage application are encrypted via secure protocols : no data circulates in clear text.

Advanced management of print queues and access rights

With Gespage, managing rights on print queues is simplified:

- **Secure release of prints** : Integrate secure release functions after user authentication.
- **Access control** : Configure permissions to limit the functions accessible on printers to their needs only.
    - **Limit access** to printers using company letterhead.
    - **Set up specific groups** to prevent abuse or unauthorized access.

Password management and personalized administrator access

It is strongly recommended to change the default Gespage administrator password after commissioning, then to renew it regularly, respecting good security practices (complex, unique and confidential password).

Additionally, enabling custom administrator credentials is recommended so that each action is tracked and associated with a specific user. This customization allows you to create dedicated access for an external technician performing occasional maintenance on the server.

Finally, it is possible to restrict administration rights per user, to limit access only to the necessary functionalities according to the responsibilities of each administrator.

Gespage maintenance and security updates

Cartadis regularly provides updates to the Gespage application. These updates are made available under the maintenance contract. It is important to note that the user must, at their own expense, download and install these updates within a reasonable time.

These updates are essential to correct vulnerabilities identified throughout the life of the product.

These updates should be performed following best practices for prior backups and having carefully read the release notes beforehand. Indeed, some major updates may require assistance from a Gespage-certified technician.

To be informed of Gespage updates, we invite you to follow the news published on the Gespage website or contact your Gespage solution provider (link).

2.4 Gespage Stratus Print Server (SaaS)

Gespage Stratus is the SaaS print management solution, hosted in a secure private cloud by Cartadis, designed for small and medium-sized organizations.

Gespage Stratus is a single-tenant server application, fully managed by Cartadis.

Each dedicated instance guarantees enhanced security and optimal performance.

Data location

Sovereign and secure hosting: The solution is hosted by OVHcloud, ensuring, from an architectural point of view, GDPR compliance and maximum security for customers in France and abroad (ISO standards ISO/IEC 27001, 27017 and 27018 and SecNumCloud / Trusted Cloud).

System Updates and Protection

It is essential that your user workstations or servers hosting Gespage services locally (Gespage Agent, Gespage Connector, etc.) are secure. This security is based on IT best practices. This includes:

- **Regular operating system updates** : Make sure the operating system is up to date to patch vulnerabilities.
- **Antivirus and firewall** : Enable real-time protection and configure firewalls to limit unauthorized access.
- **Regular updates of printer drivers** : Regularly ensure that printer drivers are up to date by contacting your printer supplier to find out which drivers are recommended for your environment.

Secure network configuration

When deploying Gespage Stratus, network access can be restricted to only those communications strictly necessary for the solution to function properly. This approach significantly reduces the area exposed to attacks.

The complete details of the network flows used by Gespage Stratus as well as by your infrastructure (printers, user workstations, etc.) are available in the network flow matrix, which can be consulted on the Gespage knowledge base (link).

End-to-end encryption

All communications between printers, user workstations and the cloud are encrypted via secure protocols : no data circulates in clear text.

Advanced management of print queues and access rights

With Gespage, managing rights on print queues is simplified:

- **Secure release of prints**: Integrate secure release functions after user authentication.
- **Access control**: Configure permissions to limit the functions accessible on printers to their needs only.
    - **Limit access** to printers using company letterhead.
    - **Set up specific groups** to prevent abuse or unauthorized access.

Password management and personalized administrator access

It is strongly recommended to change the default Gespage administrator password after commissioning, then to renew it regularly, respecting good security practices (complex, unique and confidential password).

Additionally, enabling custom administrator credentials is recommended so that each action is tracked and associated with a specific user. This customization allows you to create dedicated access for an external technician performing occasional maintenance on the server.

Finally, it is possible to restrict administration rights per user, to limit access only to the necessary functionalities according to the responsibilities of each administrator.

Gespage maintenance and security updates

The Gespage Stratus application is regularly updated to the latest version. Cartadis manages updates during short-term maintenance periods.

3. Gespage Security Model: A Three-Phase Framework

In an environment where data security is a priority, print management must incorporate rigorous measures to protect sensitive information and ensure optimal compliance. **Gespage**, a leading-edge print management solution, is designed to meet these requirements while optimizing your printing processes.

3.1 Securing the printing infrastructure

Protect your communications and data

With Gespage, all transmissions between components, such as servers, administration interfaces, and printers, are secured using the HTTPS protocol. This approach ensures that sensitive information, such as printed documents or credentials, remains protected from interception.

Regarding stored data, Gespage allows flexible management by using databases compatible with your internal standards, while supporting regular backups to avoid any loss.

Advanced features for optimal security

Gespage integrates robust security measures to meet current challenges:

- **Process isolation** : Gespage runs in isolated processes to minimize interaction with the system kernel. This ensures that critical tasks do not require excessive permission, such as administrator access.
- **Secure APIs** : Calls to Gespage public APIs are protected by authentication tokens, ensuring reliable and controlled communication.
- **Secure web pages** : Gespage protects its interfaces against attacks such as SQL injection, cross-site request forgery (CSRF), and cross-site scripting (XSS).
- **Authentication via directory services :** Gespage integrates with services like LDAP, Active Directory, and Entra ID to authenticate users, eliminating the need to store passwords directly. Local accounts, such as those for guest printing, are protected by strong encryption.

GDPR Compliance with Gespage

Gespage complies with European data protection standards, ensuring that personal information is treated with the highest level of confidentiality. This includes access rights management, data encryption, and configurable policies for deletion when necessary.

Maintain a secure printing system with Gespage

A reliable and secure printing infrastructure relies on the adoption of good IT practices:

- **Regular audits** : Perform periodic checks to identify potential vulnerabilities.
- **Automated backups**
    - In the case of a Gespage On-Premise server, ensure that the Gespage databases are regularly backed up to a secure external server to avoid any data loss.
    - In the case of a Gespage Stratus server, the automated backup is managed by Cartadis.
- **Updates and fixes** : Keep your Gespage solution up to date to benefit from the latest security patches.
- **Disaster recovery plan** : Regularly test your recovery plan to ensure continuity in the event of an incident.

With its advanced features and focus on security, Gespage is much more than a print management tool: it is a strategic solution to protect your data and optimize your printing operations.

3.2 Securing print flows

In many traditional printing environments, jobs are sent directly to printers for immediate processing. However, a substantial portion of these prints are often discarded, creating not only unnecessary waste but also privacy risks when sensitive documents are left unattended.

With Gespage, the secure print release feature ensures that jobs remain pending in a queue until the user physically authenticates at the printer to release them. This approach offers several advantages:

- **Enhanced confidentiality** : Sensitive documents are only printed when the user is present to retrieve them.
- **Reduction of unnecessary printing** : Unnecessary jobs are never printed, saving paper and ink.
- **Increased security** : Sensitive documents never remain exposed on printers.

Setting the print job retention time

Abandoned prints are not the only risk : prints pending on the server can also be accessed by malicious people if security is not ensured.

Although the measures described in the "Low-level security of the complete infrastructure" section can limit this risk, it is recommended that you automatically delete print jobs that have been queued for too long.

This helps protect sensitive data and reduce the load on the print server,

With Gespage, you can define how long a print job remains pending before being automatically deleted.

Print2Me printing with Gespage

For even more flexibility, Gespage integrates Print2Me printing, a mobile solution that allows users to send their jobs to a single queue and retrieve them from any printer on the network. By authenticating themselves via methods such as RFID badges (on a card reader such as Cartadis TCM4) or a print code, users can easily retrieve their print jobs to the device of their choice.

Why choose Gespage for your secure printing?

Gespage does not just offer basic features. Its intuitive interface and advanced capabilities, such as centralized management and detailed print tracking, make this solution a strategic choice for optimizing your print workflows while ensuring maximum security.

By integrating features like secure release and Print2Me printing, Gespage helps businesses reduce costs, improve document confidentiality, and simplify print resource management.

3.3 Securing printed output

With Gespage, you can secure your prints while ensuring complete traceability thanks to advanced features such as log management or watermarks.

Advanced print tracking with Gespage

Gespage records every detail of print jobs:

- Who printed (username).
- What was printed (document name).
- When and where (time, printer used).

These detailed logs are accessible through an intuitive interface, allowing administrators to detect unusual behavior and ensure transparency of printing activities. Additionally, Gespage offers scheduled reports that can be sent automatically to ensure ongoing monitoring.

Embedded watermarks

Gespage offers custom watermarks, displaying information such as the user's name or the print date directly on the document. This feature acts as a visual reminder that each document is traceable.

Tracking Gespage configuration changes

Gespage provides a detailed event log that allows you to track all configuration changes made, and the ID of the administrator who made them.

It is also possible to subscribe to an administrator email alert on some of these events.

4. Compliance with international regulations

4.1 Data protection and GDPR compliance

Regulation (EU) No. 2016/679, known as **the General Data Protection Regulation (GDPR)**, is the European reference text for the protection of personal data. It strengthens and unifies data protection for individuals within the European Union. It came into force on **May 25, 2018**, and applies to any organization collecting or processing personal data of European Union residents, whether located within or outside the EU.

The GDPR's primary objective is to restore control over the personal data of citizens and residents while simplifying the regulatory environment for businesses operating internationally through unified regulations. It also regulates the export of personal data outside the European Union.

To be compliant with GDPR, organizations must meet several requirements:

- **Securing IT systems** : Ensure the protection of personal data against unauthorized access.
- **Respect for the rights of the persons concerned**: Provide individuals with the ability to access their data, correct erroneous information, or request its deletion (right to be forgotten).
- **Informed consent**: Obtain explicit consent before any data collection or processing.
- **Secure design**: Implement compliant systems from the design stage (principle of “privacy by design”).

These requirements also apply to printing systems. An unsecured printing system can represent a major point of vulnerability for an organization, allowing unauthorized access to sensitive data or the loss of documents. For example :

- **Discontinued printed documents** on printers.
- **Data stored on MFP hard drives** or in the servers' print queues.

A GDPR-compliant system must therefore include traceability, secure authentication, and access rights management features to minimize these risks.

4.2 Gespage solution compliance

Gespage helps you comply with the European GDPR directive.

The following features of Gespage allow this safety:

• Print management is secure. Securing the printing system involves securing the print flow from end to end (from the moment the user sends their print job to the document being printed at the point of print).

• Authentication and on-device release (Print2me) prevents "orphan" prints and therefore the loss of printed documents. Documents are only printed when the user comes to the printer and authenticates.

• Automatic purging of unprinted print spools also prevents lost data.

• Print spools remain pending on the print server and are not saved on the Multifunction Hard Drive.

• User information is immediately available through data export. An individual can therefore easily request and obtain access to all information about them.

• A user's information is automatically deleted (directory synchronization) when they leave the structure. Only print history remains saved for calculating statistics.

• Ability to anonymize usernames : A setting is available in the Gespage administration to automatically request the anonymization of usernames, either systematically or after the departure of an employee. Individuals therefore have the right to be forgotten regarding information concerning them.

• Ability to hide document names in print queues : Gespage offers an option to hide document titles in queues, thus strengthening the confidentiality of sensitive information even before printing.

5. Best practices for integrating Gespage into your organization

It is important to define a good printing policy from the outset to optimize the machine fleet as much as possible and to improve the quality of service for your users.

When you want to implement restrictive rules (limiting user credits, forcing black and white printing, etc.), we recommend using Gespage in observation mode for the first two months. At the end of this analysis period, it will then be easier to choose the right printing policy.

Printer/MFP locations may be reviewed to optimize your fleet's operating rate. In addition, redirection rules will be implemented to promote quality usage for your fleet.

A deployment that promotes the security of the printing infrastructure can be summed up in these three points :

- Analysis of previous print volumes and identification of risks.
- Phased rollout to minimize disruptions.
- Training sessions to ensure safe adoption.

6. Conclusion: A strategic tool for the future of your printing infrastructure

Gespage is not just a software solution : it is a strategic lever for improving security, reducing costs, and aligning your infrastructure with current standards.

The security of the printing environment is therefore a shared responsibility; understanding the End User License Agreement is essential for compliant and secure use of Gespage.