

USERS:

- Have more confidence their documents are being sent to the right person each time.
- Are assured that their sensitive and confidential documents are well protected.
- Are comfortable knowing their compensation information won't leak to others accidentally.

IT ADMINISTRATORS:

- Have more power to prevent security breaches.
- Can manage all security measures centrally and remotely.
- Appreciate solutions that help secure information and protect users.

BUSINESS DECISION MAKERS:

- Can be much more confident that their companies' assets are secure.
- Keep internal business plans secret to help maintain competitive advantages.
- Have confidence to bring in contractors, because all internal information is protected.

Ensure that all users print securely:

uniFLOW Output Manager enables your business to provide access to high-quality print capabilities while drastically reducing security concerns.

With this solution, all print jobs can be set up so they are held at the uniFLOW server until a user provides authorized identification at a device. This prevents unauthorized persons from accessing or retrieving confidential documents.

uniFLOW integrates easily with many identification systems including fingerprint readers, magnetic card readers, contactless card readers, and keyboard entry.

Give your users direct access to print, scan, and copy devices — with powerful security measures in place to ensure that all print-related activities fall within your organizational guidelines.

This Canon solution features:

- Canon imageRUNNER device
- uniFLOW Output Manager
- eCopy ShareScan



“Are we sure people aren't sending sensitive documents outside the company from our MFP devices?”

“Did someone else pick up my confidential printout?”



“Can the contract files we send be opened by anyone other than the intended client?”



SECURITY

Secure Your Company's Print, Copy, Scan, and Send Activities

Most business leaders want their people to have every resource that can be an advantage toward helping their companies succeed. MFP print devices are certainly one of those potential resources.

Yet while they deliver a wide variety of powerful functionality, unfettered access to the devices and the documents that pass through them can raise serious security concerns.

Canon security solutions help ensure that authorized users can easily gain access to the print-related features they need, while everyone is assured that document information is well protected.

Security shortcomings can invite problems:

With Canon SECURITY solution:

No way to track who sends documents, and few leak deterrents.

Contractor: Internal price list emailed to unauthorized recipient. No way to determine who sent job.

Intern: Marketing plans scanned, then accidentally faxed to wrong destination. Strategic campaign information is leaked.

**Negotiation power compromised.
Internal strategies no longer secret.**

Comprehensive deterrents help you restrict access and prevent leaks.

Contractor: User must authenticate at the device, otherwise no access to send functionality.

Intern: Authenticated users can send documents only to users from a pre-approved list of recipients.

Confidential documents printed, but picked up by wrong person.

HR Specialist: Company compensation plan picked up by unauthorized employee.

Office Associate: Sensitive employee medical records discovered by colleague.

**Conflicts stir among employees.
Company potentially open to lawsuits.**

Confidential documents can be authorized and released for print by user at MFP.

Supervisor: Company compensation plan released to print by authorized user entering his ID at device. No more prints laying out on the printer.

HR Specialist: Card reader checks user's ID and verifies clearance to access and release medical records for print.

Electronic document files freely accessible, and sent out from MFP.

Service Rep: Without user authorization at device, contract is scanned to email and sent to wrong client.

Supervisor: User receives sensitive, unsecured PDF by mistake, and is able to open it without a password.

**Clients learn your security is weak.
Insecure strategic information can leak.**

Only authorized users can access and send protected electronic document files.

Office Associate: With proper authorization at device, contract is scanned to email and sent only to the right client.

Supervisor: If a user were ever mistakenly sent a confidential PDF by someone else, password protection would prevent them from opening it.

Business Decision Maker

- ✗ Strategic business information can be accessed and exposed to clients, partners, vendors, or competitors.
- ✗ Confidential documents can be mistakenly sent to unauthorized recipients.
- ✗ Any sensitive hard-copy document can be scanned and sent to anyone.

Business Decision Maker

- ✓ Users gain wide access to the print capabilities they need.
- ✓ Sensitive documents can be released for print only by authorized users at the device.
- ✓ Document information is well protected, company-wide.