Canon

APPLICATION FORM

INVOICE

LAB TEST RESULTS

DEPOSITION

TOP SECRET PROJECT

CLIENT LIST

STRATEGIC PLANS

imageRUNNER ADVANCE Security Solutions

Safeguard Against Internal Information Theft

imageRUNNER
ADVANCE

Are Security Vulnerabilities in Your Office Technology Putting Your Company at Risk?

You Believe Your Network Is Secure – but What About MFPs?

Chris, we may have a serious security breach. Jane Doe says her private information has been shared.

Which devices were involved? Can you find evidence of which employees are likely responsible?

I'm sorry, sir. We'd be guessing. I just don't have much to go on here.

IT administrator suspects that an MFP device may have been involved in the leak—a potential compliance violation.

Management demands more information about the leak.

Sensitive, confidential client information has leaked, and they have no material way to investigate it.

Do You Know When MFPs Are Used to Image Your Confidential Information?

TOP SECRET PROJECT

.PDF

Back at her desk, she saves an electronic version of the file.

A walk-up user prepares to scan a confidential document back to her desktop PC.

A month later, she has a new job working for a competing company.

She still has top secret, proprietary information from her previous company. Will she share it with her new employer?

Are Internal Leaks Originating from Your On-Premises Devices?

CLIENT LIST

A walk-up user prepares to scan and print a document that lists vital contact information for the company's clients.

A competing company receives the list of client contacts.

The original company starts to lose business and clients. They are at a loss to explain why. But they never learn about the breach of their client list.

Now You Can Safeguard Your Company Against Internal, Document-Related Security Vulnerabilities

Locate Breaches or Compliance Violations Associated with Network Devices

Chris, we may have a serious security breach. Jane Doe says her private information has been shared.

> "Find any activity that involves documents for Jane Doe."

IT administrator suspects that an MFP device may have been involved in the leak—a potential compliance violation.

He performs a search of the job folders for document activity involving likely attributes about the record.

He locates a handful of job logs that meets that criteria, and he can now review the accompanying OCR text files to identify the user.

Deter Document-Related Information Leaks with Notifications

TOP SECRET PROJECT

Export Folder

SERVER

held a new perspective on product X18 and a competitive edge for

TEXT

.PDF   JOB LOG

held a new perspective on product X18 and a competitive edge for

E-MAIL

A walk-up user prepares to scan, send, print, or copy confidential hard-copy pages.

When OCR is performed on page images, a sensitive word is discovered. The suspicious activity log and document is stored on a server and an e-mail notification is sent.

IT administrator has been alerted to the suspicious activity. He can investigate the incident immediately.

Prevent Document-Related Information Leaks from Occurring

CLIENT LIST

John Doe
34 Upside Street
Dayton, OH

TEXT

.PDF   JOB LOG

?

Possible attempted scan of proprietary client list

E-MAIL

A walk-up user prepares to scan and print a document that lists vital contact information for the company's clients.

During the activity, a sensitive item is discovered in the text of the associated document, so the job is stopped. An e-mail alert is also sent to the IT administrator.

No copies were made, but the IT administrator is alerted to the suspicious activity. He can now investigate and confront the user immediately.

Information Theft Threats May Be Real. Now, So Are the Solutions.

In today's connected and competitive business environment, it's more important than ever to defend your company's documents. Corporate espionage and information theft can be very real concerns.

Traditionally, information security has been about protection from external attacks. In fact, the findings from global security study on information leakage reveal that the data and revenue loss caused by internal employee behavior can be much more severe than external threats. Among business decision makers, there may be a growing awareness of these kinds of threats. Unfortunately, many companies still fail to safeguard against attacks from the inside. Consider taking a closer look at these security solutions:

imageWARE Secure Audit Manager Express

Canon imageWARE Security Audit Manager Express is document security software that acts as a deterrent against employees who may potentially leak valuable information from your company. imageWARE SAM Express can track all documents being sent to—or scanned from—devices on your network and provide an audit trail that can be reviewed when needed.

All search features can be managed through a simplified log viewer that enables your IT administrator to easily search information relating to any security breach. The simple act of having this security technology in place can help provide greater accountability, transparency, and peace of mind for any organization.

imageWARE Secure Audit Manager Express with uniFLOW

When you combine content tracking with notification functionality, information leakage can become a thing of the past.

Canon imageWARE Secure Audit Manager Express with uniFLOW can be implemented to operate behind the scenes. It will keep track of document-related activity and can be set to notify your IT administrator when a specific keyword is printed, scanned, faxed, copied, or sent. With this feature, your IT administrator can be made aware of crucial information breaches as they occur so you can head off potential leaks.

uniFLOW

uniFLOW offers robust security features designed to help you prevent information leaks and compliance violations. With the uniFLOW security solution, you can capture every print and/or send activity and process the image data for key words before storing it in a document management system.

If any attempt is made to print and/or send a document featuring any of your critical key words such as internal project names, codes, or confidential client information, the device activity will stop and your IT administrator can be immediately notified via an alert message.

Canon
*image*ANYWARE

1-800-OK-CANON
www.usa.canon.com

Canon U.S.A., Inc.
One Canon Plaza
Lake Success, NY 11042

LET YOUR BUSINESS RUN

COLOR DOCUMENT MANAGEMENT DOCUMENT DISTRIBUTION PRODUCTIVITY SECURITY

OUTPUT MANAGEMENT DEVICE MANAGEMENT USABILITY ACCESSIBILITY ENVIRONMENT