# INFORMATION SECURITY IN ACTION!

IN A WORLD WHERE CYBER THREATS ARE GETTING SMARTER AND COMPLIANCE IS GETTING TOUGHER, HOW WILL YOUR BUSINESS KEEP INFORMATION SAFE?

# INDEX

Data is the treasure of every modern organisation. It supercharges your finance department, it gives your executive team predictive powers, and it imbues your employees with greater business intelligence.

This precious resource must be kept safe at any cost.

As the value of this treasure keeps rising, so too does the number of foes trying to take it: malicious attackers lie in wait outside to steal information when you least expect it. Meanwhile, double agents may seek to take the treasure for themselves.

But it doesn't take an enemy to bring down an organisation.

A great power watches over the land, ensuring that everyone follows the rules of data compliance.

But even though the laws are strict, and the punishments are severe, it's also never been easier to make a mistake.

Modern day businesses are not a walled city; increasingly, they're not even in one location at all. Hybrid working means employees are storing, sharing and collaborating on information across more locations than ever before.

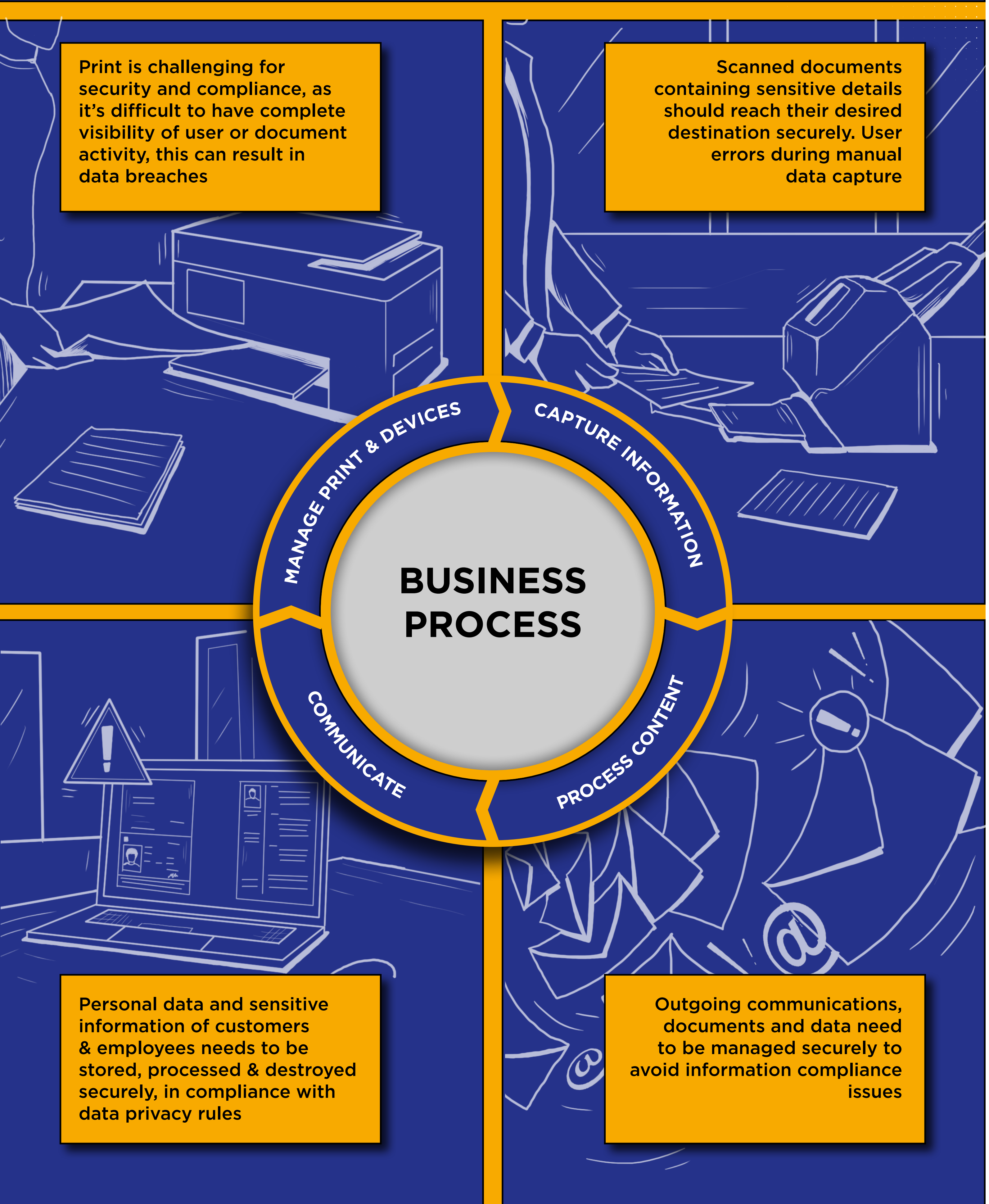
In such a complicated working environment, keeping your information safe and your processes compliant can seem like an impossible challenge.

You need a trusty partner who can secure your treasure, protect you from villains and help your people stay compliant against all odds.

Let's explore how Canon and our secret weapons can help you take on the challenge.

# CHALLENGES IN THE DOCUMENT LIFECYCLE

Documents are created, copied, stored and shared during their lifecycle within your organisation, all these stages pose challenges for keeping the data within them secure and compliant.



Print is challenging for security and compliance, as it's difficult to have complete visibility of user or document activity, this can result in data breaches

Scanned documents containing sensitive details should reach their desired destination securely. User errors during manual data capture

BUSINESS PROCESS

MANAGE PRINT & DEVICES

CAPTURE INFORMATION

PROCESS CONTENT

COMMUNICATE

Personal data and sensitive information of customers & employees needs to be stored, processed & destroyed securely, in compliance with data privacy rules

Outgoing communications, documents and data need to be managed securely to avoid information compliance issues

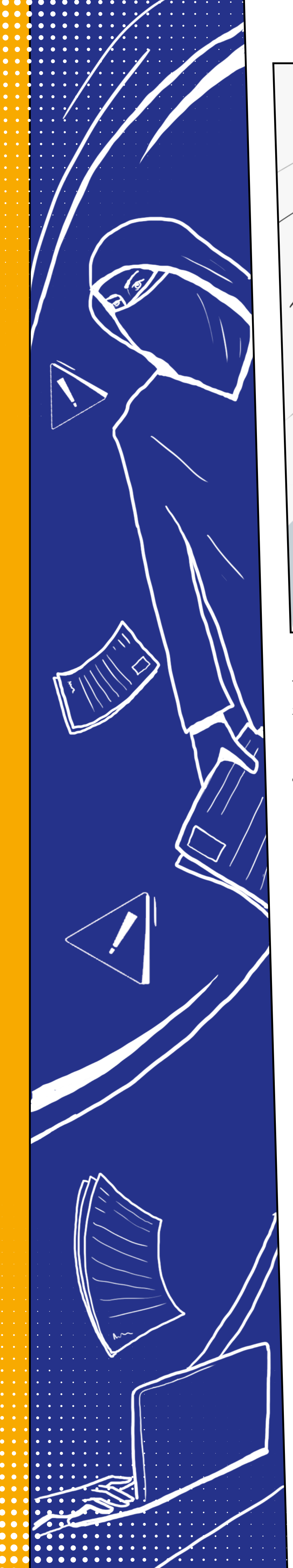
# CHALLENGE 1

## THE SECRET STRATEGY

Organisation X has a big secret: it's set to embark on a new adventure. The leadership team has decided to invest in a new area of business in the hope of gaining new power and discovering untold riches.

It's essential that these plans stay under wraps until they're made public. The news would reveal Organisation X's intention to its rivals, forewarning them that there's a new competitor on the horizon. Meanwhile, employees at Organisation X have a lot at stake – could there be new opportunities in their department? New areas of business to explore? Or are their jobs under threat?

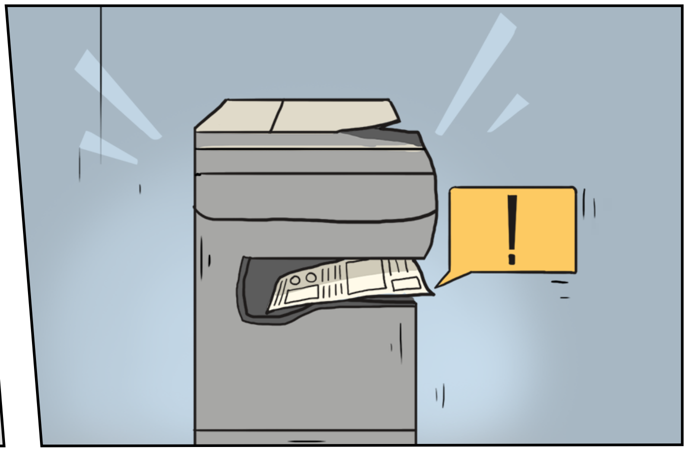
The senior leadership team must proceed carefully if they are to ensure their plans stay out of the hands of conspiring employees and external foes. Throughout the budgeting and announcement process, they must avoid a range of traps, from insider threats to malware and network attacks. Can they keep their secret safe?



The comms team has drafted a press release reflecting the organisation's new strategic direction. The information is still top secret, and the announcement is being written and approved by a small group of senior executives. Selma the Finance Director has asked to review a physical copy of the document. Polina her assistant is ready to print it for her.

Print represents a greater security threat than organisations realise. Typical security and compliance risks include paper documents being taken from the printer before they are collected by the user, or forgotten about altogether, exposing sensitive or confidential information to unauthorised people.

Innovation has also opened the doors to an array of new security threats. Modern multi-function printers are as powerful as a PC, packed with a hard drive, memory and central processing unit (CPU), and are often connected to the internet. As a result, it's possible for printer firmware to be targeted by hackers attempting to gain access to the network and corporate data.



## SECRET WEAPONS

### imageRUNNER ADVANCE DX C5800

The imageRUNNER ADVANCE DX C5800 is built with security embedded as standard. Polina can only print the document by logging in at the device using her identity card, which means nobody else can access the document queued to print and it is not left waiting in the device tray.

The device also offers Trellix McAfee Embedded Control, which protects against zero-day and advanced persistent threat (APT) attacks by blocking execution of unauthorised applications through intelligent whitelisting. To prevent an attacker from obtaining the press release through a network attack, McAfee Embedded Control safeguards against program tampering.

Finally, the imageRUNNER ADVANCE DX C5800 supports Security Information Event Management (SIEM) integration, which makes it easier for organisations to include printers in their existing security monitoring systems (Syslog, for example). These systems can recognise and flag security events across a fleet of devices in real time, alerting the company of any issues or threats as they happen.

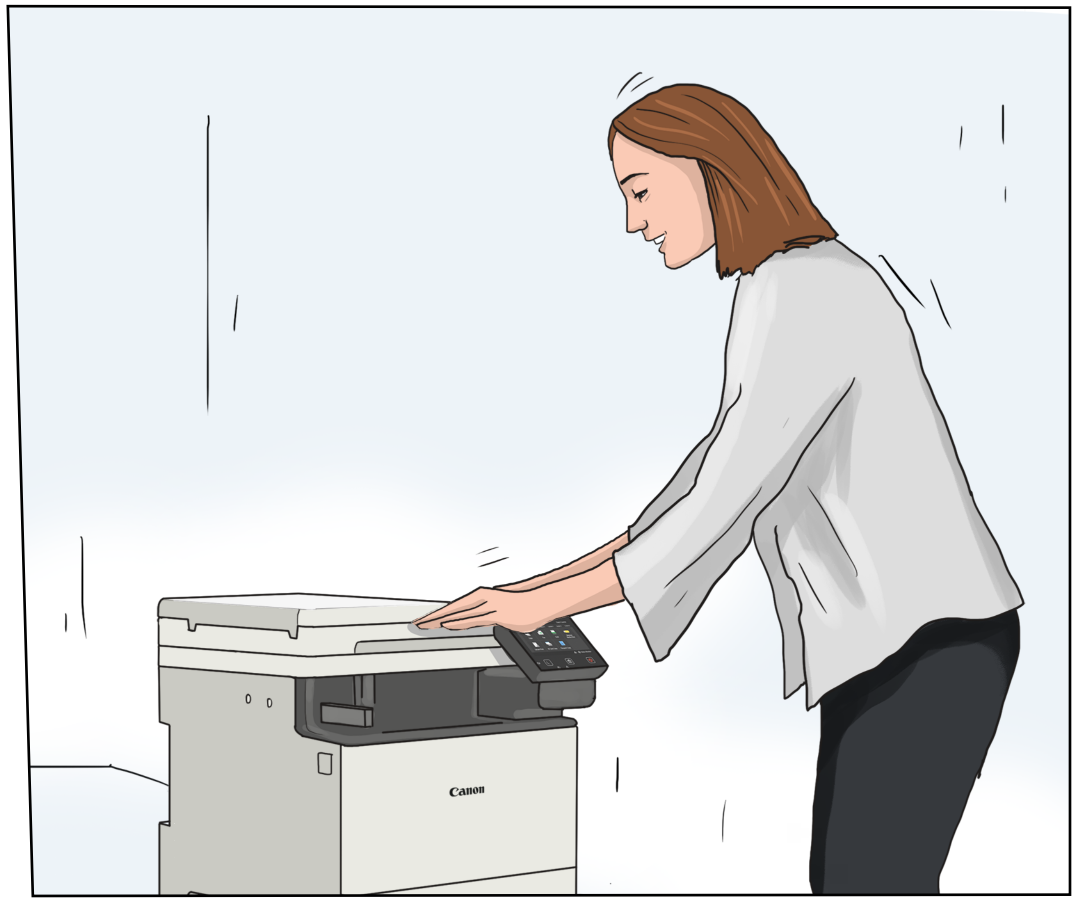
### Device Hardening Service

With Canon, security starts before you've even bought a device. We configure imageRUNNER ADVANCE MFDs to strengthen their safety, including reinforcement of in-built security controls and blocking of non-essential functions and unsecured ports. The configured device is checked and verified before it is shipped.

### imageWARE Secure Audit Manager Express

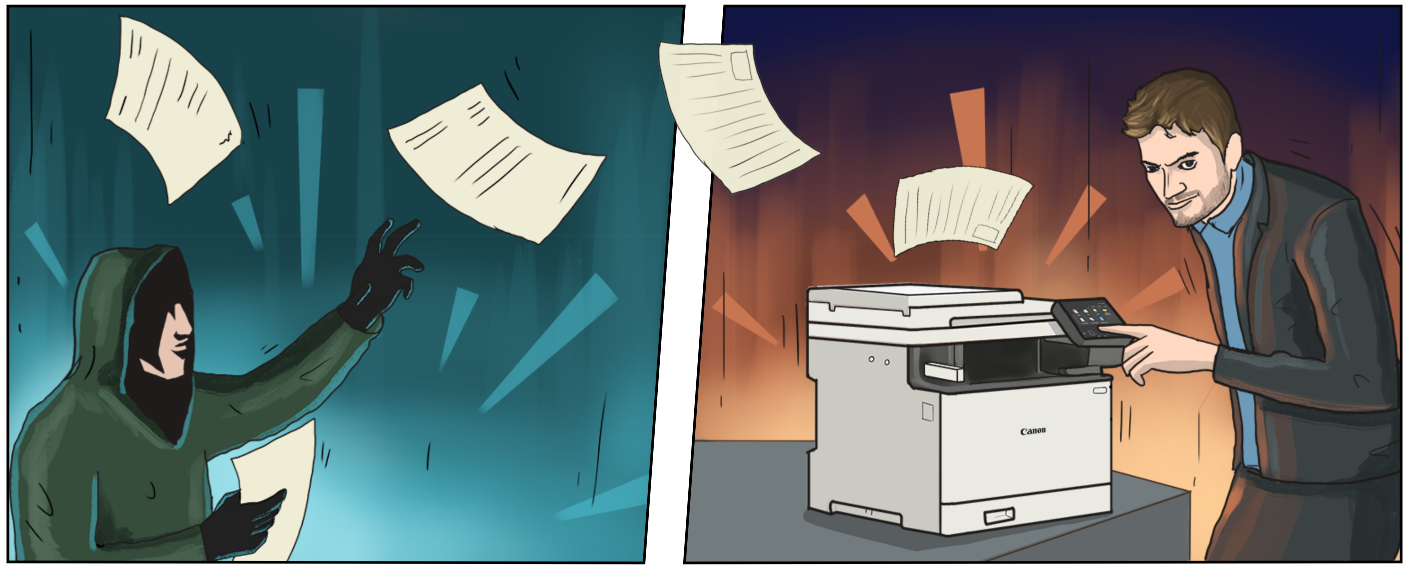
This network device security solution gives Company X oversight of their document-related activities. It can capture, archive, and audit the activities that occur on Canon devices. When Polina prints the press release, imageWARE Secure Audit Manager Express triggers an email alert to IT saying that a high-risk document is being printed. This helps Organization X to stay abreast of any unauthorised employees or parties trying to copy or print sensitive information.

Selma has reviewed the press release and provided some written comments. Polina needs to share the feedback with Pierre, the PR Manager responsible for the announcement. As Pierre works from home, Polina will need to create a digital copy to send him. Scanning documents and emailing them directly from the device creates an opportunity for the attacker to intercept the document.



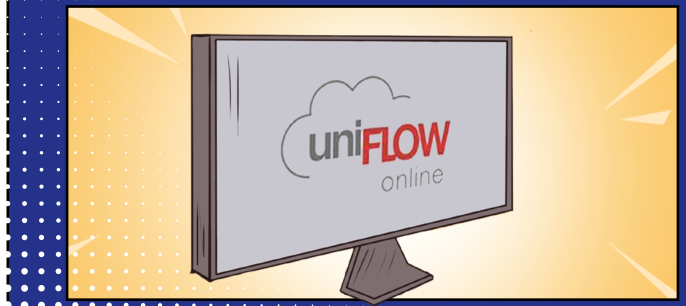
Today's scanning devices are often internet-connected, allowing users to email documents straight to a recipient, or save them in cloud destinations. As a result, there are more opportunities for digital information to be at risk, so it's crucial that scanning devices have robust security features. Without secure functions, a scanner is vulnerable to tampering – an internal user could change email routing queues to direct an email job to an unauthorised user, for example. Or, without encryption, a document could simply be opened, edited or printed.

From an external perspective, an attacker could also gain access through the network and make changes to email directories, allowing a document to be sent to recipients outside the organisation. Or they could intercept a document transmitted over HTTPS if it and its data are not encrypted.



## SECRET WEAPONS

**i-SENSYS X C1333iF**
Selma is ready to scan the document using the i-SENSYS X C1333iF. This multi-functional device (combining print and scan functionality) offers secure scanning features that help keep information safe. The moment it is switched on, its Verify System at Start-up feature checks whether there have been any attempts to compromise the device's integrity, and can alert Selma if it has been tampered with. Selma then has to log in using an identification card, ensuring there is a record of who is copying or sharing information. Finally, the i-SENSYS X C1333iF's IEEE802.1X support provides an authentication mechanism, so when it connects to the company LAN or WLAN, it provides confirmation of its authenticity.



**uniFLOW Online**
When Selma scans the contract, uniFLOW Online creates an encrypted PDF and offers optional password protection. These prevent unauthorised users from viewing, editing or printing the document, protecting the information from anyone who attempts to intercept it.

Tobias has heard that the company may be moving in a new direction. As the head of one of the teams which is struggling under the current strategy, he knows this might mean serious cuts to his budget this year, or even a threat to jobs.

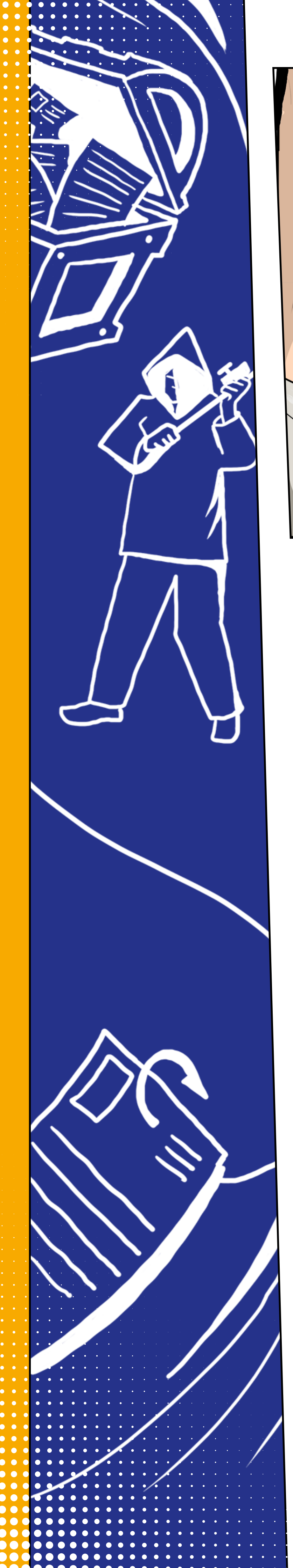
Tobias is frustrated by the news, so he plots to confirm the veracity of the rumours and possibly warn colleagues. As he thinks he knows where the senior leadership would store their financial documents, he begins a secret search for anything that might be associated with the new plans.

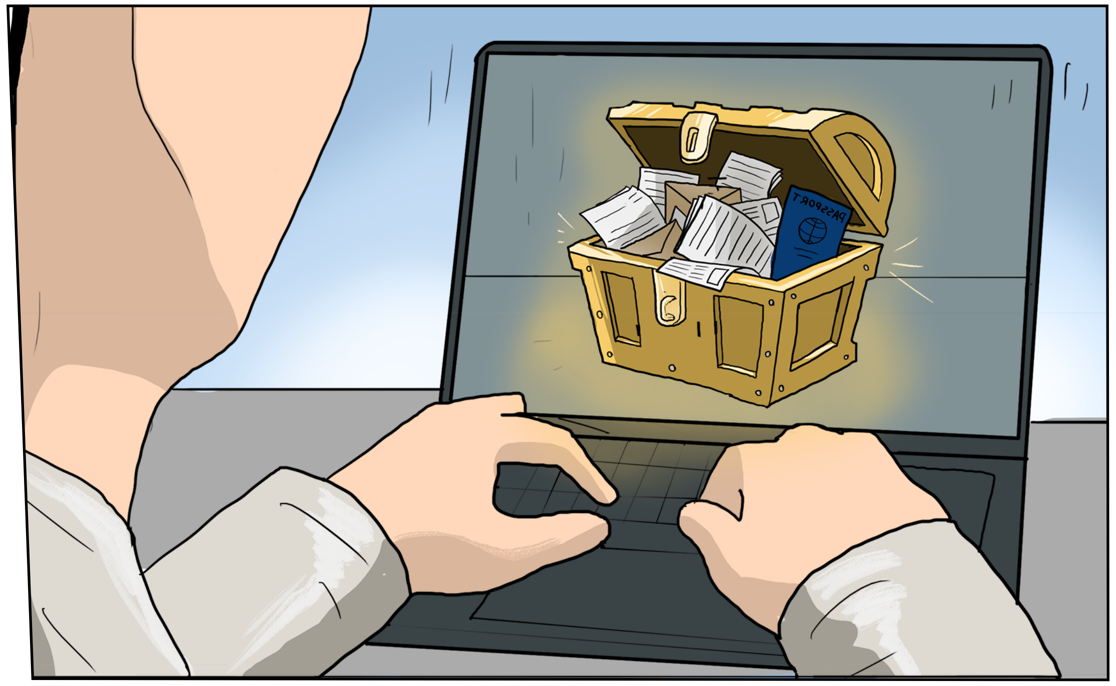
Organisations create and store more and more information every year. With many now also operating hybrid models, this information is spread across an increasing number of locations, both physically and virtually. As a result, it's common for organisations to struggle with haphazard storage strategies, with employees using everything from filing cabinets to personal cloud storage services such as Dropbox to house company data. What's more, employees frequently deal with sensitive information such as contracts, staff bank details and corporate financial results. Even with critical data like this, it's almost impossible for IT teams to ensure best practice information management when documents are stored in such a way.

## SECRET WEAPONS

**Therefore Online**
With robust in-built security, Therefore Online allows organisations to set automated policies around who can access documents and how information is stored, shared or edited. Access controls prevent unauthorised employees such as Tobias from opening private or sensitive documents like the press release.

Therefore Online is cloud-based, ensuring that the location of a user doesn't impact accessibility; authorised users who are working from home or on the go can still access essential documents. Any interaction with a document is tracked, ensuring that information is tightly managed and visible end-to-end, providing a digital audit trail.

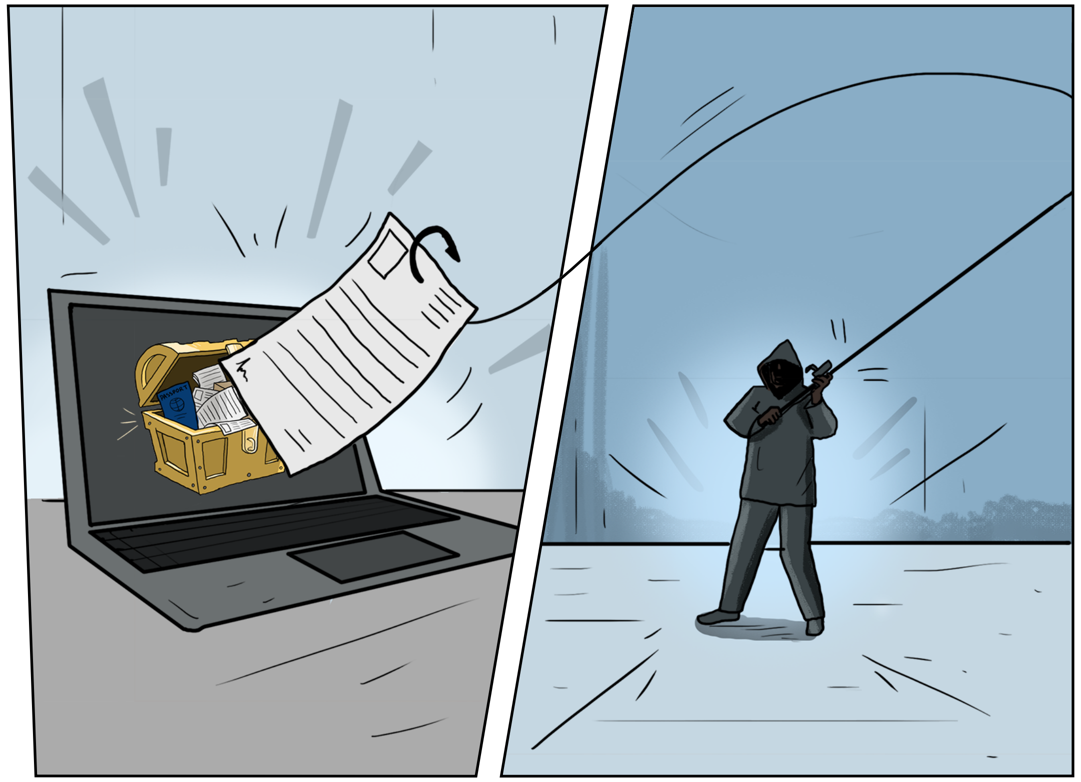




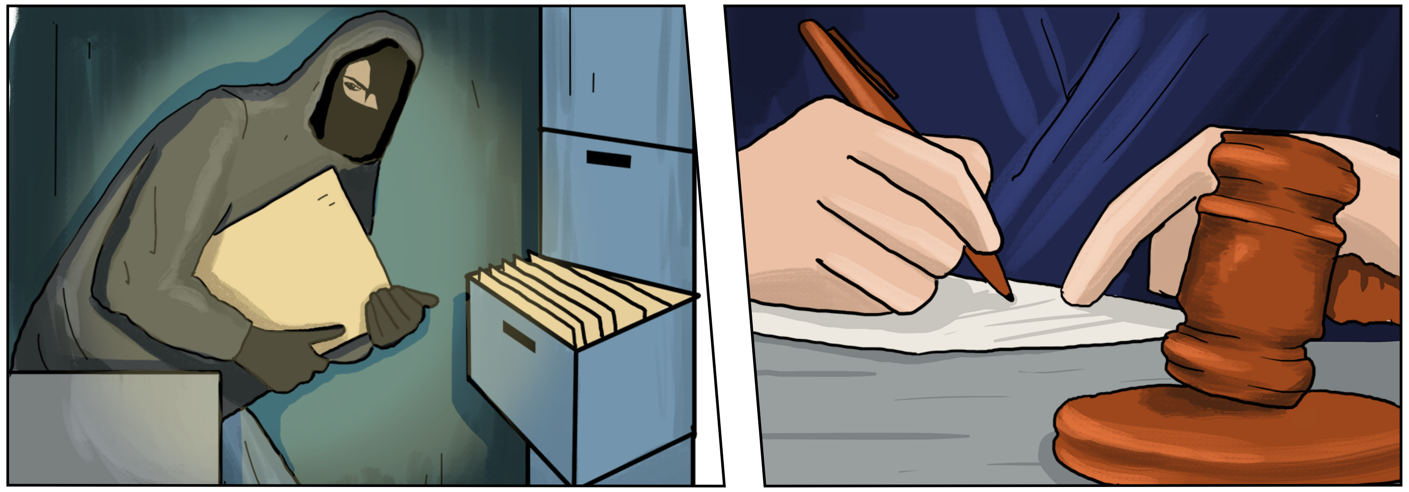
Pierre is preparing to send out the announcement under embargo to recipients including key shareholders and selected journalists. It's essential that the document is only sent to these contacts; he cannot risk it ending up in the wrong hands.

Meanwhile, he needs to be careful about the extra information Organisation X is keeping secret. The company database contains countless gems: sensitive data about the recipients, including their email addresses, telephone numbers and in the case of the journalists, passport details from previous press trips.

This data is a potential honeypot for thieves who could use these credentials to leak the announcement early, or, if they were so inclined, use details of individuals in the database to perform identity theft or orchestrate phishing attacks.



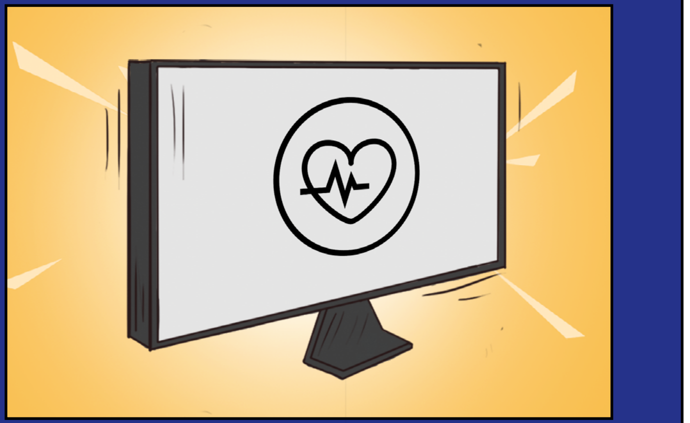
Businesses frequently hold highly personal and confidential information about their customers, partners and other parties they work closely with. This information is not just contained on company servers but is included in outgoing communications such as bank statements, invoices and correspondence with these parties. Holding this information represents a risk to the business, as if it was lost or stolen by attackers, it would expose the business to significant fines and reputational damage. Meanwhile, if an organisation does communicate with these contacts, it's crucial that personal information within those communications only reaches the recipient.



## SECRET WEAPONS

### Office Health Check

Office Health Check helps organisations review their IT environment to ensure it is secure from the start. Global cyber security expert NCC Group will conduct a remote analysis of the organisation's internal and external IT infrastructure, including communication channels and ports, to reveal any vulnerabilities. By identifying any issues, the organisation can avoid them being exploited by a potential attacker, preventing the interception of Pierre's communications, or the journalist or stakeholder data being stolen from Organisation X's databases.



### uniFLOW sysHub

uniFLOW sysHUB gives users tight control and oversight of their customer communications, making it easier for Pierre to ensure that the communication reaches the right destination. This solution consolidates internal communications processes and applications into one workflow, managed from a single point of operation. uniFLOW sysHUB then automates this workflow to make it more efficient and reduce the risk of error. Every step of the workflow is logged and stored in a sysHUB library for later review and to support audit trails, making it difficult for a member of staff to deliberately leak a document without it being recorded. Meanwhile, Pierre can check the proof of delivery to ensure the communication has reached the right person.

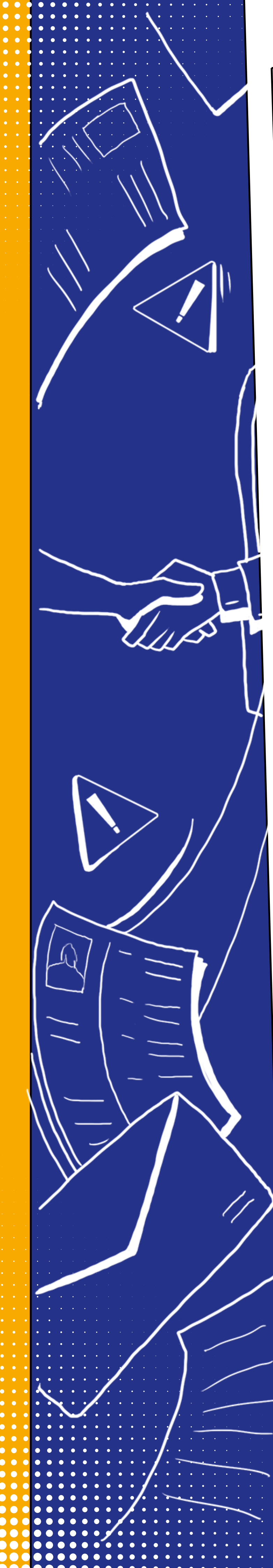
# CHALLENGE 2

## THE CONFIDENTIAL HIRE

Organisation Y needs to attract new workers to power its expanding kingdom. Its workforce used to be based in a single location, but thanks to hybrid working, its intrepid employees roam across the land. The busy HR team have had to quickly adapt. New employees are now enrolled through virtual hiring and onboarding processes. The HR team must have eyes everywhere, communicating across great distances to share confidential documents related to new joiners.

With the HR team's great power comes great responsibility: they have in their possession a mountain of valuable and sensitive information, from employee payroll details to health status and performance records. They know that it falls to them to keep this information safe and in line with compliance legislation. The auditors are always on the horizon and the HR team know they will be expected to demonstrate how information is stored and shared. This is not easy. While the HR team work hard, they don't have superpowers. It's easy for accidents and errors to lead the team into trouble.

Without the right technology solutions in place to save the day, this could spell trouble for Organisation Y.

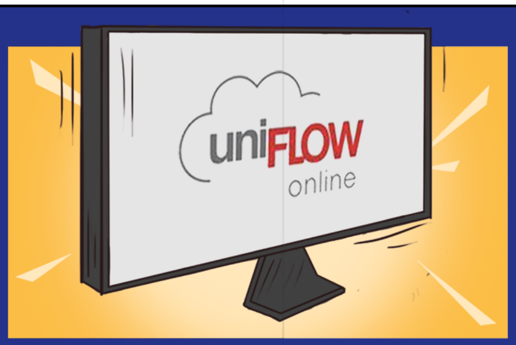


After a successful interview process, Organisation Y has agreed to hire a new employee. The candidate has visited the head office to deliver their passport and sign their contract with Fatima, the Hiring Manager. Fatima wants to make copies of the documents for her own records and to share with the head of HR who is working from home. It's easy for Fatima to accidentally enter the wrong recipient, or to save the document to a location which is accessible by anybody. If the wrong person did receive it, they could simply open the captured documents to reach the information.

Organisations have a responsibility to ensure that any scanned documents are only seen by those authorised to view them. A simple error could lead to potential data loss or breach which could have a severe impact on compliance. If the organisation does not realise they have experienced a serious breach and do not report it, the data protection regulator can issue a fine of up to 4% of the organisation's global turnover.

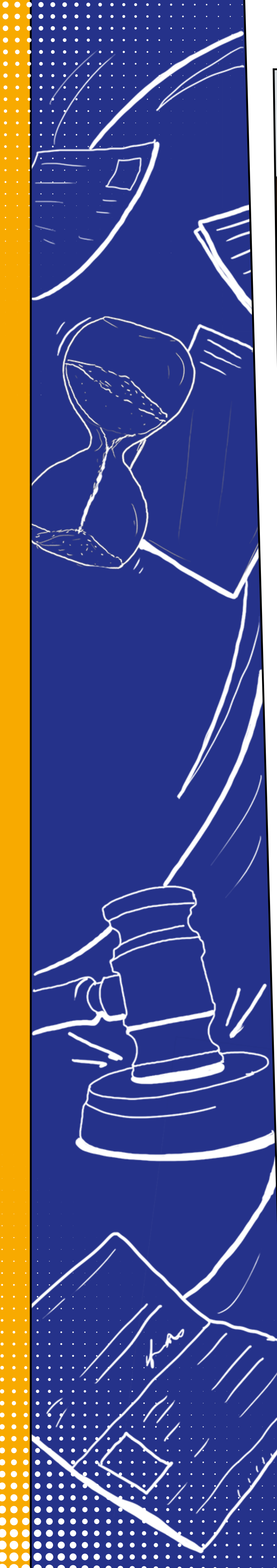
## SECRET WEAPONS

**uniFLOW Online**
uniFLOW Online offers built-in Secure Scan Workflows which allow Organisation Y to pre-configure specific scan workflows for each user. Document workflows such as HR Onboarding are already pre-defined, preventing Fatima from saving the scan of a new employee in an incorrect destination.



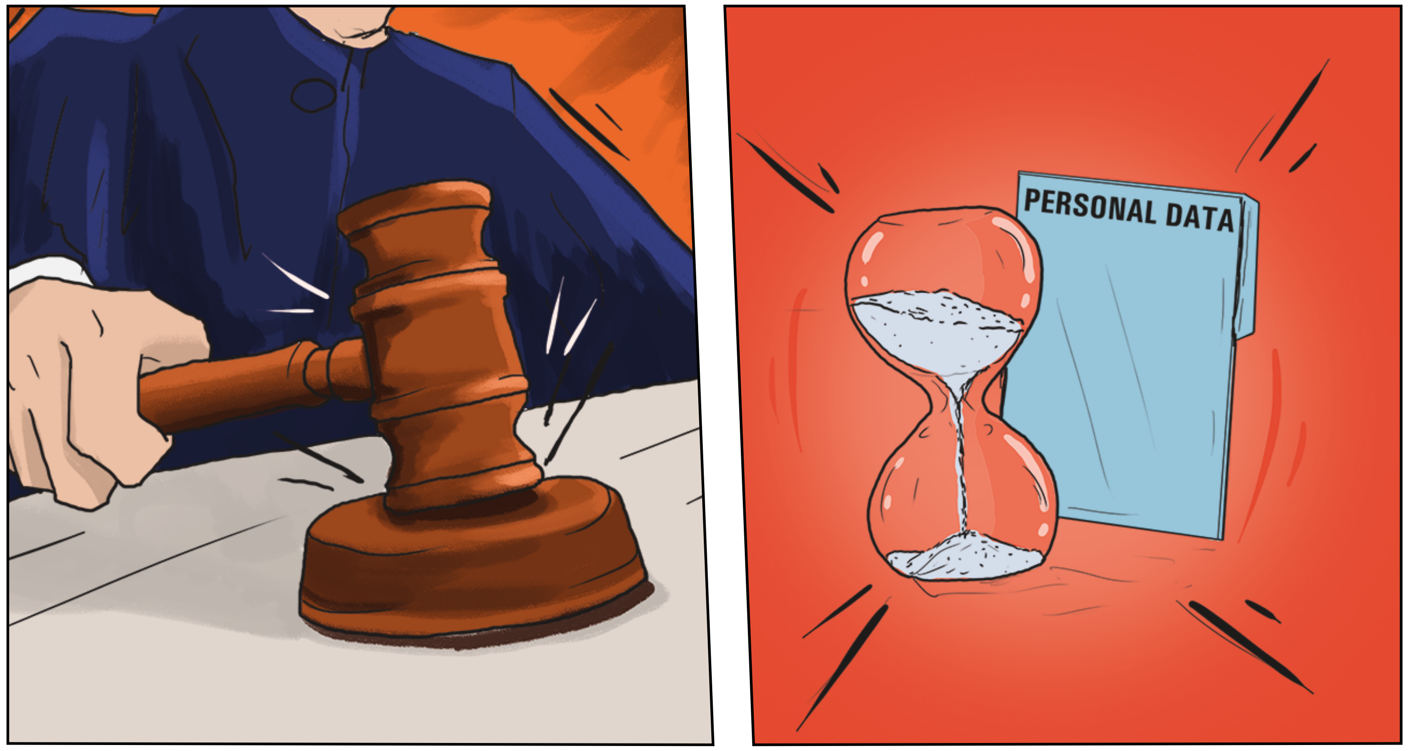
**imageFORMULA S150**
Fatima is ready to scan the document using the imageFORMULA S150. This scanner offers secure features that help keep information safe: it requires any user to log in using an identification card, ensuring that only Fatima can access the document which has been captured. It also automatically applies encryption to the digitised version, meaning that only a recipient with a password can read it, edit it and print it. imageFORMULA S150 devices also offer options to send documents through secure protocols such as scan to FTPS, SFTP and SMTPS.

**IRISPowerscan**
The company also has IRISPowerscan, which means that once the documents are digitised, they are automatically identified as a passport and contract. The software corrects any scan faults such as skews and uses Optical Character Recognition to recognise key details such as the employee's name and passport number. This information is added to indexing, making it easier for the organisation to find it in future. What's more, IRISPowerscan automatically routes the contract and passport scans to the right secure storage location on the company system.



During the recruiting process, several employees – including Fatima and Nick, a colleague – were involved in interviewing the candidates and reviewing CVs. Both employees are based virtually, working in different locations across Europe. Both Fatima and Nick have copies of the candidates' CVs and notes on their interviews stored on their personal laptops and in shared Dropbox locations. Once the new candidate has been offered the job, Fatima and Nick can easily forget to delete any of these documents.

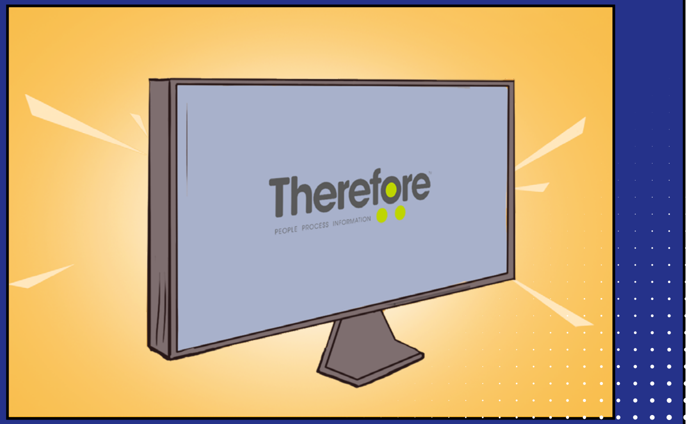
Recently tightened legislation means that compliance has never been so important. Laws such as the GDPR have introduced specific rules governing how information must be stored – for example, organisations must not retain personally identifiable information for longer than it is strictly required. Yet many organisations still struggle with haphazard storage strategies, without official locations to store documents, or the ability to locate documents saved to their own servers. Should an ex-employee, or indeed a previous candidate, make a subject access request to the organisation, it would be very difficult for the company to declare what information they hold. In addition, for audit purposes, the organisation would struggle to demonstrate that they have control over where personally identifiable information is being stored.

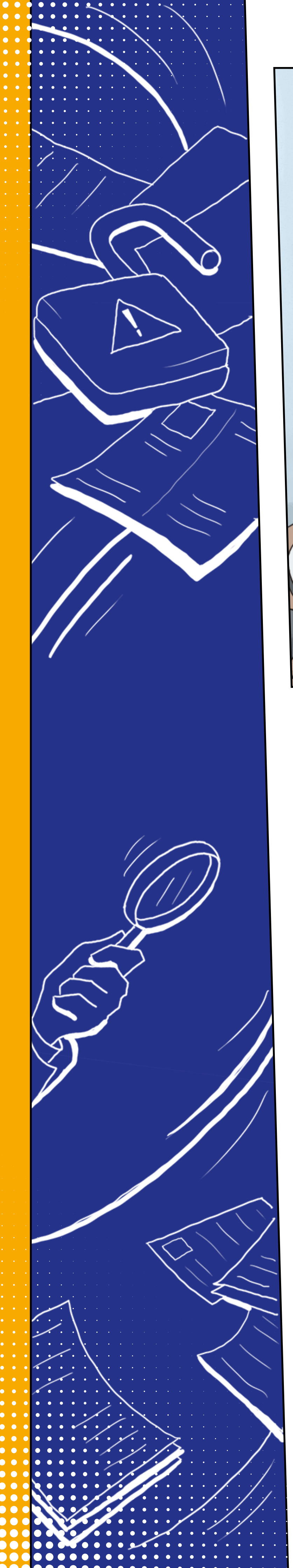


## SECRET WEAPONS

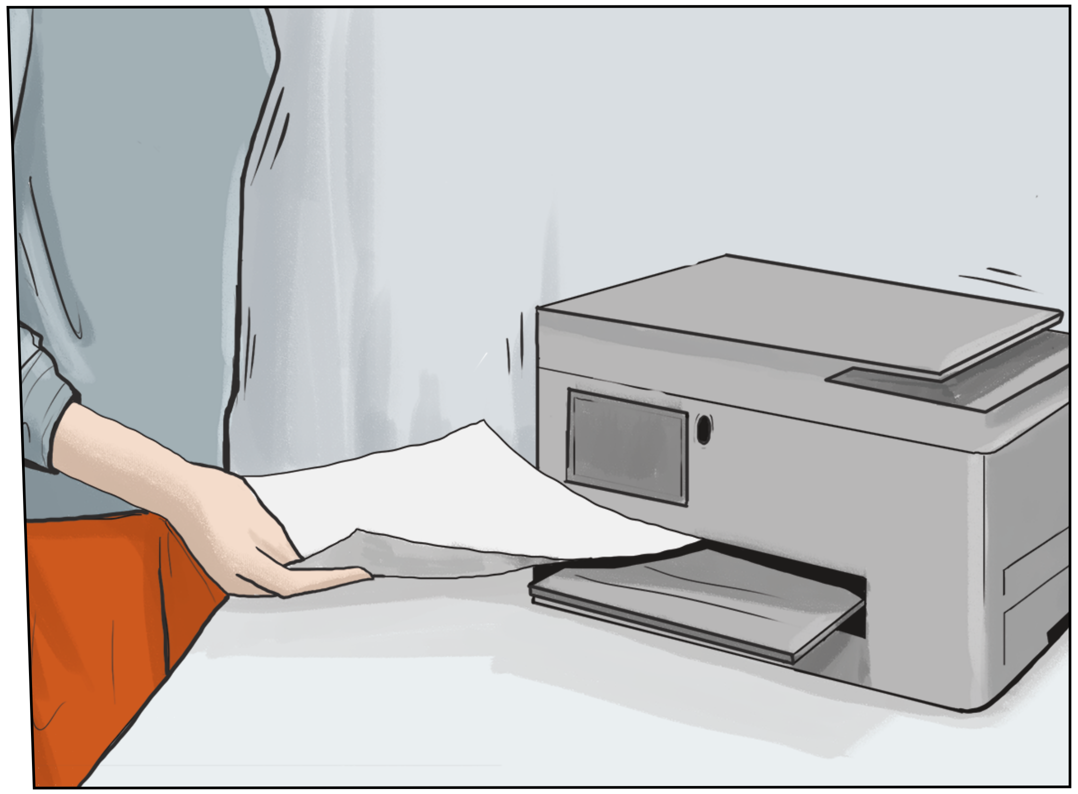
**Therefore Online**
With robust in-built security, Therefore Online allows organisations to set automated policies around who can access documents and how information is stored, shared or edited. It tracks every interaction with a document that takes place, keeping information tightly managed and visible end-to-end, which makes the audit process much more straightforward.

Organisation Y can also set automatic retention policies to ensure that old documents which contain sensitive information are deleted after an appropriate retention period, delivering compliance. As Therefore Online is cloud-based, even when teams are off site, they can still upload documents and be assured that they are safe and secure.





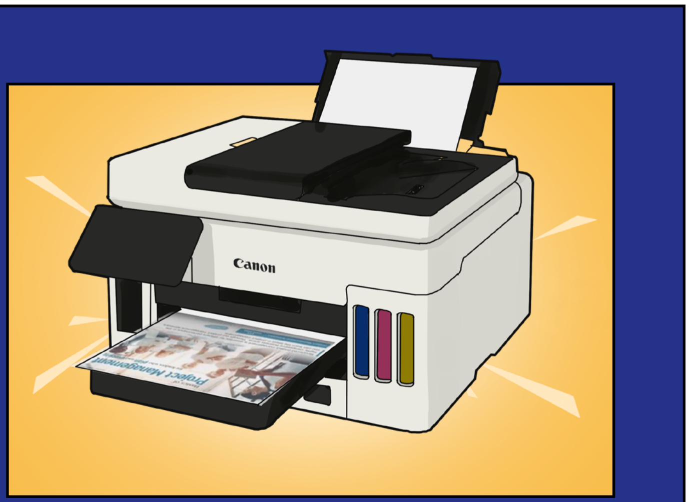
Ingrid, the employee's new line manager, is working from home and preparing to run an induction interview at the office the next day. She wants to print a copy of the letter confirming the new hire's salary, along with other forms, to share with them during that process. Ingrid has only recently started working from home and has not been supplied with a work printer, so she is using her own personal device.

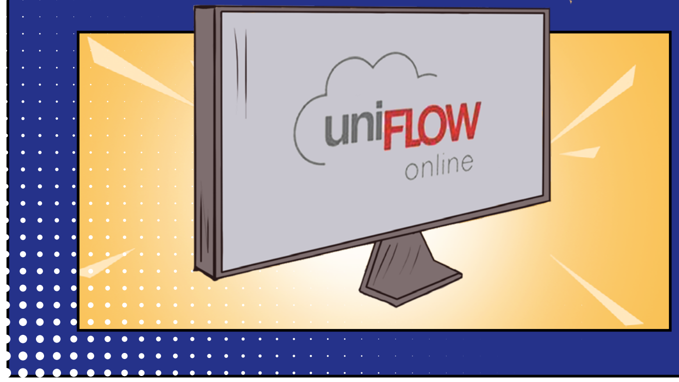


It's easy for organisations to forget that printers play a big part in the security and compliance of workflows, with the devices holding valuable data and documents. As part of legal compliance obligations, organisations are expected to provide audit trails which report how sensitive information is being used. This requires them to have greater visibility and tracking of how documents interact with devices. However, as Ingrid is using her own personal printer, it is not connected to the corporate network – there is no traceability, no record of the data stored in the device and no guarantee that it is secure.

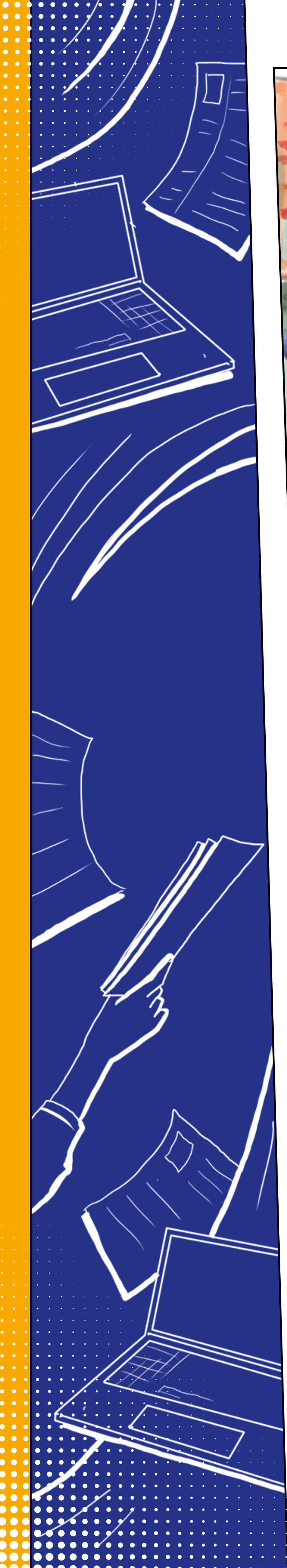
## SECRET WEAPONS

**MAXIFY GX6050**
This efficient desktop printer produces high-quality prints for home workers, but it also helps to keeps documents secure and compliant thanks to its embedded integration with uniFLOW Online. The Scan to Myself feature prevents Ingrid from sending documents to anyone but her own e-mail or personal folder, to avoid her accidentally sending on business documents to personal contacts. The secure print job release function means that Ingrid only prints documents when she's ready, meaning sensitive business documents aren't left at the device.





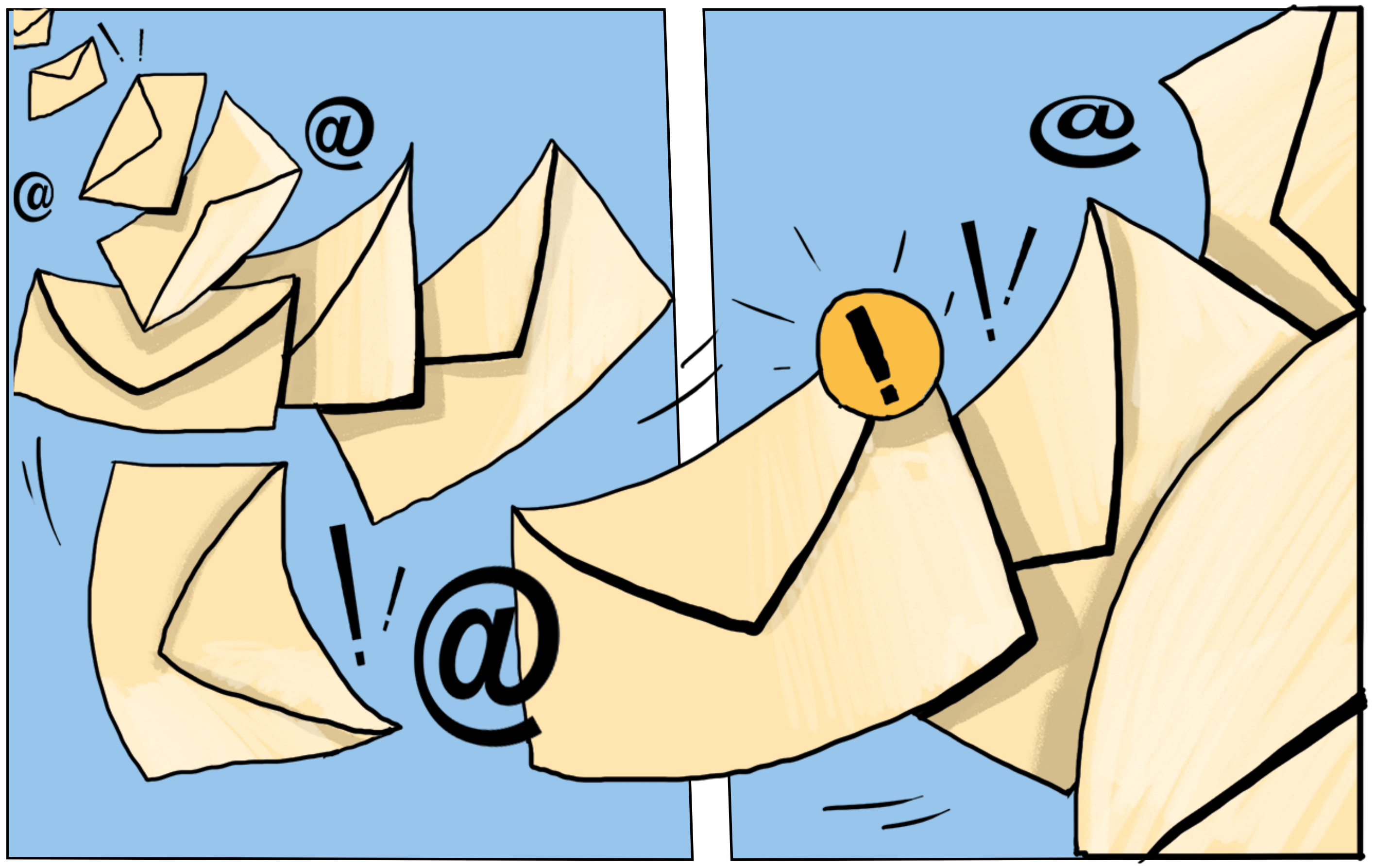
**uniFLOW Online**
This embedded software integrates the MAXIFY GX6050 with the organisation's environment, allowing Organisation Y's IT team to track Ingrid's printing activity and accurately report back on how sensitive information is being used, even when she's working from home.



It's the end of the new employee's first month and Fatima from HR is preparing to send out payslips. Unfortunately, the new employee has the same forename as another member of staff. Fatima accidentally sends each payslip to the wrong recipient, meaning that they are both able to see how much the other is paid.

The organisation has breached the employees' confidentially; technically, they have grounds to take the company to an employment tribunal. Moreover, having seen their colleague's payslip, the new employee is now challenging their own salary with HR and may no longer feel comfortable staying in their role.

Communication is a high-risk stage of any document workflow as it involves sharing information, whether that's internally with employees, or externally with customers, suppliers and other stakeholders. In a standard audit, organisations will be expected to demonstrate how sensitive information is shared with other parties. Given the huge volume of communications that an organisation makes in any given week, it's essential to have solutions in place that take the pain out of tracking and tracing these processes.



## SECRET WEAPONS

**uniFLOW sysHub**
uniFLOW sysHUB gives users tight control and oversight of their internal communications, making it easier for Fatima to keep HR communications confidential. The solution consolidates internal communications processes and applications into one workflow, managed from a single point of operation. uniFLOW sysHUB automates this workflow to make it more efficient and to reduce the risk of error. In this example, Fatima would not be able to accidentally send confidential information to another employee.

Every step of the workflow is logged and stored in a sysHUB library for later review and to support audit trails, meaning that Fatima can check the proof of delivery to ensure her communication has reached the right person.

# HOW CAN WE HELP?

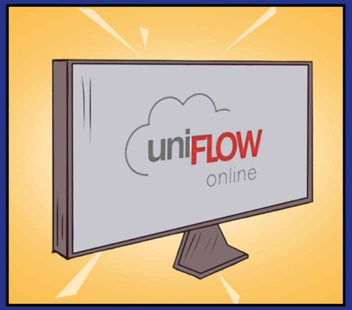
Every business wants to keep their information secure and compliant. But as Organisation X and Y have shown, it's a hostile landscape out there. Not only are organisations fighting more villains than before, but tougher legislation means that the stakes are high when mistakes are made. It can seem like a losing battle, but it doesn't have to be. The secret is having the right technology and partner on your side.

Canon is a leader in the IDC MarketScape for print and document security solutions and services, as well as in the Quocirca Print Security Landscape. Our hardware, software and services are designed to help your organisation run as efficiently and effectively as possible in a complicated world. No matter where your people are based, or where you are on your digital transformation journey, our technology supports every working environment.

With our 'secure by design' approach, we take the hard work out of keeping information safe. Our solutions are built to prevent attacks, protect data and maintain and safeguard compliance, so you can take advantage of new capabilities without adding more work for your team.

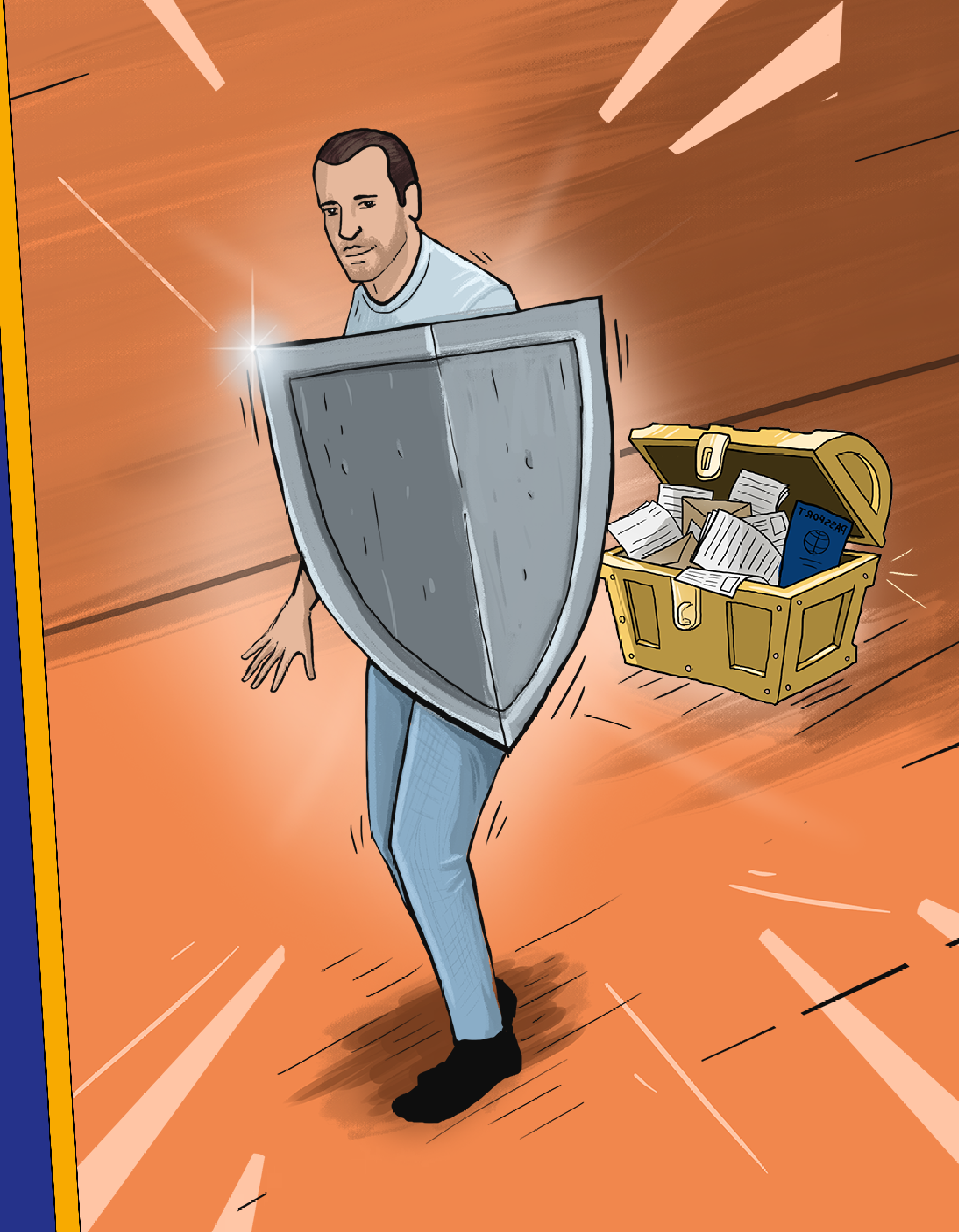
**PRINT AND SCAN DEVICES**
Our print and scan portfolio is equipped with the latest security features to safeguard critical data at every stage of document workflow. All Canon products are security checked at the design and development phases, as well as prior to release.

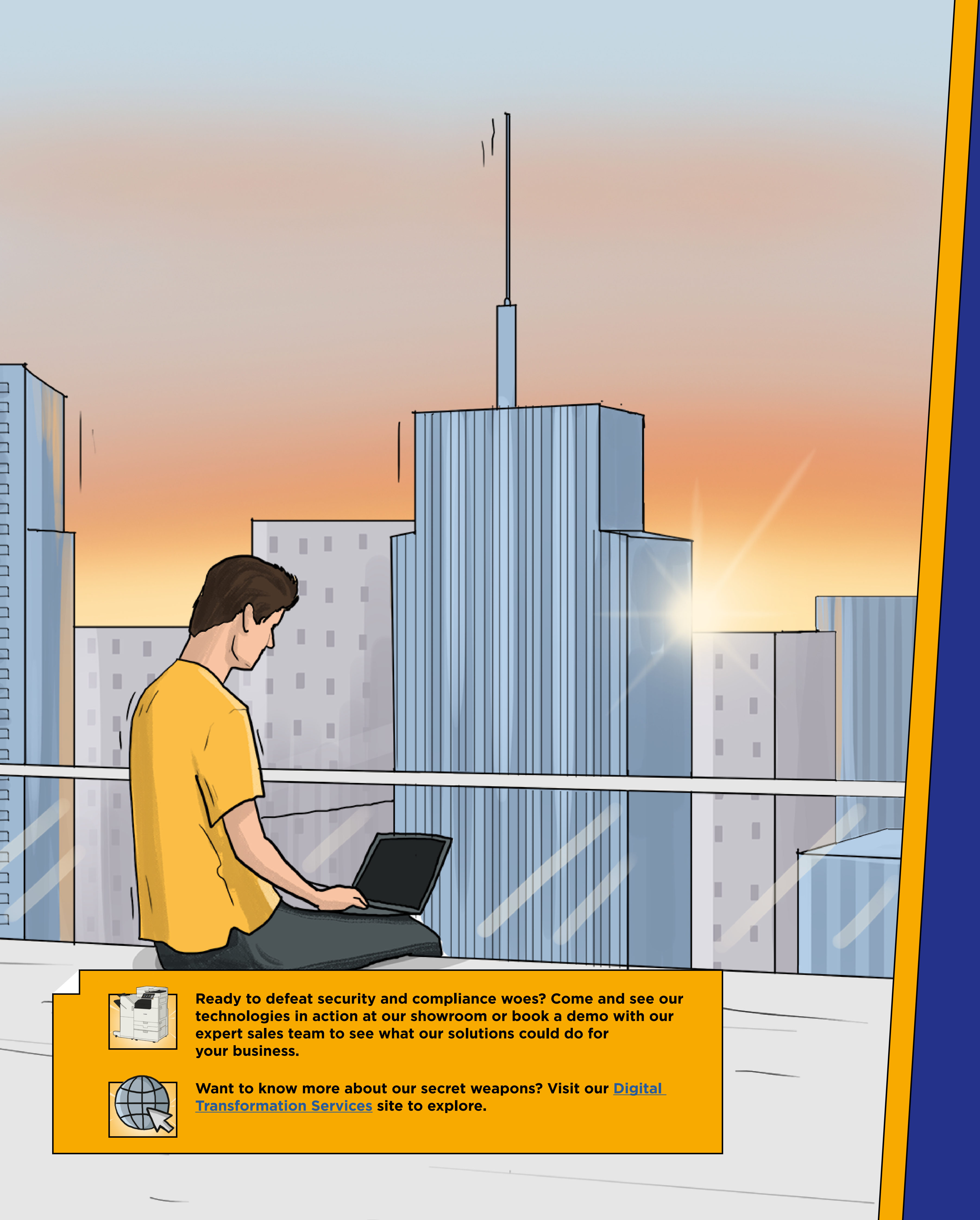
We continue to build strong partnerships with industry leaders, such as Trellix and Microsoft, to ensure the widest possible coverage and compatibility when securing device fleets. And we have a dedicated product security incident response team.



**SOFTWARE**
We understand that information isn't bound by location, which is why we offer software which protects data wherever it goes. And we work with external organisations such as IOActive to conduct penetration tests at the release stage and for major software updates.

**SERVICES**
We offer security services designed to help you maintain data protection compliance and protect your sensitive data throughout the lifetime of your print and scan infrastructure.





Ready to defeat security and compliance woes? Come and see our technologies in action at our showroom or book a demo with our expert sales team to see what our solutions could do for your business.

Want to know more about our secret weapons? Visit our Digital Transformation Services site to explore.

# ABOUT CANON

Canon is imaging. We use that imaging to make a difference and enable change.
For our customers as they undertake digital transformation and work in new ways.
For wider societal change with our ongoing sustainability focus as part of our corporate heritage and culture.

Finally, we are changing as we invest in new markets, products and technologies, so we are here for the long term for the benefit of all; our customers, our people and the wider society.

## CANON IS BUILT ON 4 KEY PILLARS:

### Innovation

A long history of image-led innovation delivering cutting edge technology for over 80 years. Pioneering industry-firsts and a strong commitment to future developments in technology.

### Support

A diverse portfolio of services to ensure top quality and customer satisfaction. Inhouse expertise working towards enhancing efficiency and committed to unlocking potential for our customers.

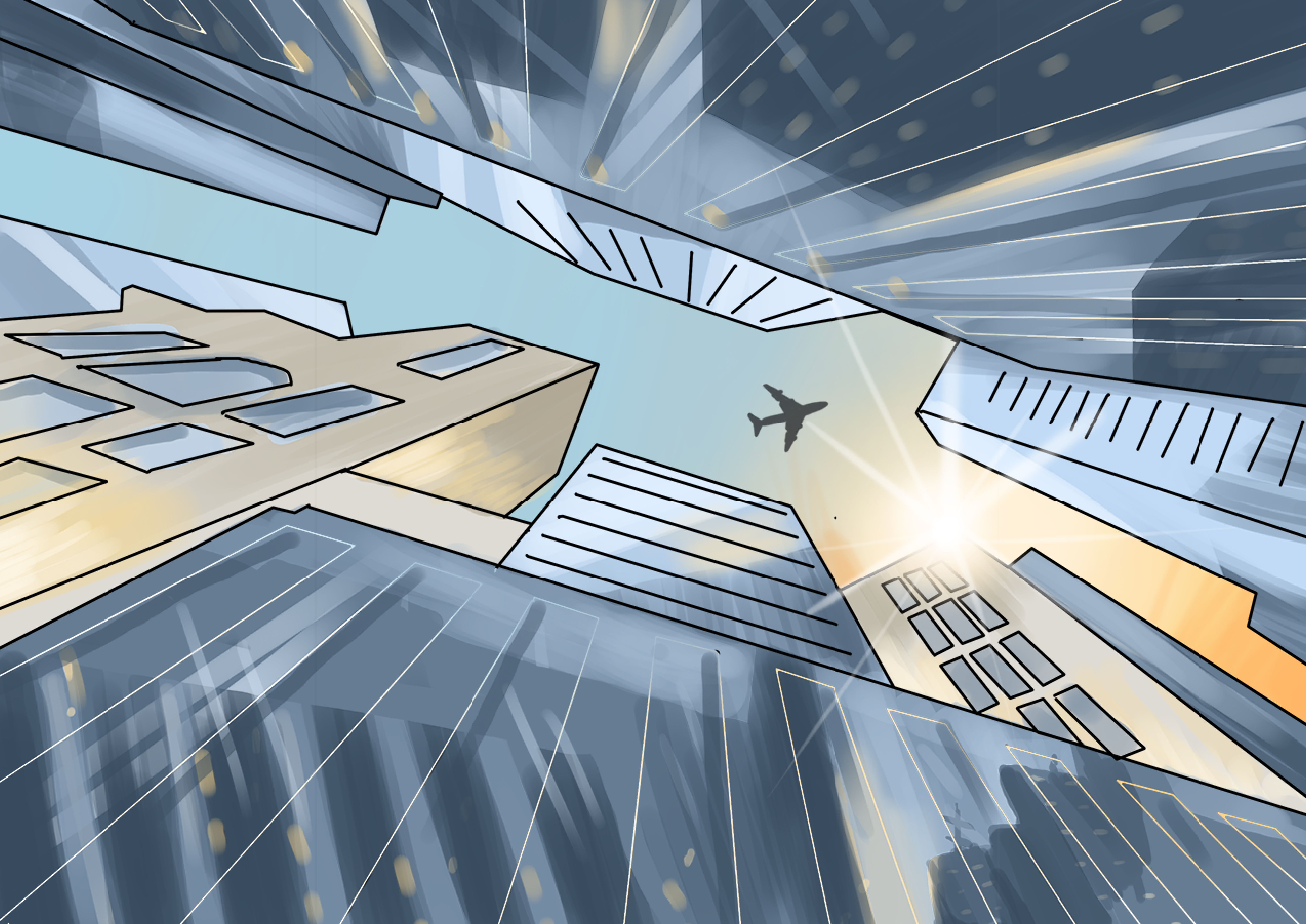
### Security

Canon solutions and services help secure all documents and sensitive data, whether in paper or digital format across the document lifecycle. Secure by design, the devices, solutions and services are built with security in mind.

### Sustainability

Canon has aligned its sustainability practices with the UN's Sustainable Development Goals (SDGs) such as commitments to reduce CO2 omissions across the product lifecycle by downsizing packaging and consolidating distribution centres.

**ALL OF THESE ELEMENTS COMBINED MAKE CANON THE RIGHT PARTNER FOR YOU.**



**Canon Inc.**
Canon.com

**Canon Europe**
canon-europe.com
English Edition

**Canon Europe Ltd**
4 Roundwood
Avenue,
Stockley Park,
Uxbridge
UB11 1AF, UK