The Quick-Start Guide to Print Security

How to maximise your print environment and minimise security threats

The Hidden Security Threat

What's the first thing that comes to mind when you hear the words 'IT security'?

If you're like most people, you'll probably think of malware, email scams and passwords that are easy to crack. Or maybe the high-profile cases of hacking we've seen in recent years, or the WannaCry cyber attack which affected the NHS.

But there's another aspect that often flies under the radar: print security.

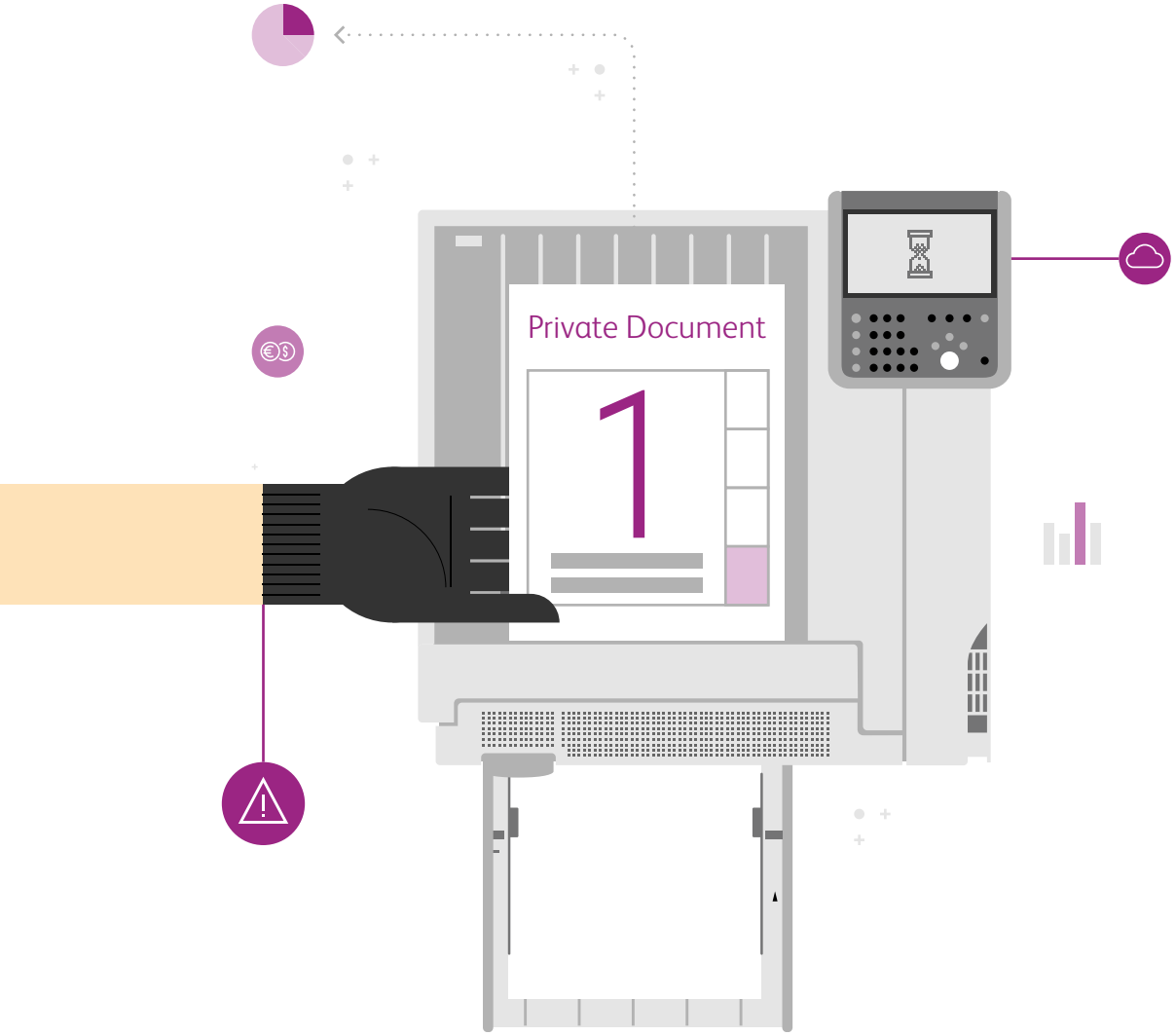
These days, multifunction printers (MFPs) are more like powerful computers. They're connected to your network and the cloud, accessed wirelessly by mobile devices, and capable of scanning, routing, storing and sharing documents.

But the flipside of all that power and flexibility is a big increase in security risks if the printer isn't securely configured.

This quick-start guide will highlight some of the most important issues, and give you the inside track on how to ensure your print environment is smart and secure.

Let's dive right in.

The Top 3 Threats



UNCOLLECTED DOCUMENTS

It's estimated that 25% of print jobs are never picked up by the users who printed them.[1] That's a big waste both of resources (paper and toner) and effort (somebody has to remove the documents and get rid of them).

But even more importantly, it's a significant security threat.

That uncollected print job could be sensitive confidential information, such as personal details of staff or patient information.

1. Nuance – Based on Nuance Customer data / Internal Study of Help Desk Calls

The Top 3 Threats

UNSECURED DATA

Even if every print job is collected, you're still not out of the woods.

If proper security isn't in place, documents with sensitive and confidential data moving around your network – via a cable or wirelessly – can still be intercepted. And don't forget that Multifunction printers (MFPs) nowadays also have hard drives to cope with complex print jobs. If data on the drive isn't deleted after printing, it could be open to abuse.

80 Trusts in the UK were hit by the WannaCry attack,[2] and 60% of all breaches are carried out within a matter of minutes.[3] So tightening up print data security isn't an optional extra – it's an absolute must.

2. https://news.sky.com/story/a-year-after-wannacry-is-nhs-better-prepared-11368864
3. Verizon 2015 data breach investigations report

The Top 3 Threats

MOBILE APPS, MOBILE USERS, MOBILE THREATS

Mobile devices now outnumber people across the world, and are expected to grow exponentially[4] to 11.6 billion by 2021. Bring your own device (BYOD) is becoming the norm, as people connect smartphones, tablets and laptops to the company network.

If NHS Trusts don't provide a simple, cross-platform printing solution for these users, they may decide that a third-party app is what they need. And that's a big threat, because unauthorised apps could seriously compromise network security.

34.4% of breaches worldwide are hitting the healthcare industry.[5]

4. Cisco Visual Networking Index

5. https://www.healthcareglobal.com/public-health/gdpr-healthcare-ready

It’s Time to Take Control

The consequences of a printing security breach are too serious to ignore, and prevention is always better than cure.

A structured, multi-pronged approach will ensure that your print environment is protected to the highest possible levels. You’re going to need a mix of at least five capabilities.

It's Time to Take Control

Secure printing means that confidential documents never lie unattended in paper trays. Print jobs are sent securely to the printer, and released only when the user enters a passcode or swipes an ID card.

Image overwrite is used by advanced printers or MFPs to electronically 'shred' documents that are held on the hard drive as part of print processing. This shredding can be carried out automatically, manually or on a schedule.

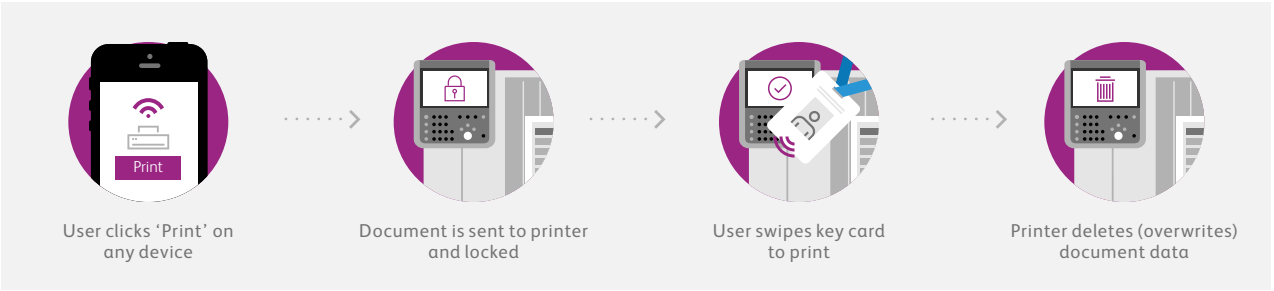
Data encryption keeps prying eyes from seeing sensitive information as it moves to and from your printer.

Network security prevents unauthorised remote access to your printer and protects confidential data as it moves across the network.

User authorisation allows you to grant or deny access to specific MFP functions such as scanning or access to patient data.
If you've already got access controls in place for other tech, this is how you integrate your MFPs into those policies.

41%

UK public sector NHS Trusts believe paper processes are a security risk.[6]



6. 2016 Survey carried out by Coleman Parkes for Xerox

Don't be a Soft Target

Trusts today realise the importance of having the latest version of software in the fight against security threats.

But it's crucial not to overlook printer software when designing your print security strategy.

Next-generation multifunction printers (MFPs) are equipped with embedded antivirus software, so you're safe against malware and other potential threats. They also have automatic firmware update functionality, so no user intervention is required.

GET TO KNOW YOUR USERS

It's easy to think that all security threats are malicious and come from outside the organisation. But in fact 35% of data breaches are internal, and simply the result of human error.[7]

User analytics will let you see who's accessing, sharing, scanning and printing documents. This user-centric view of your print environment will allow you to design policies and profiles to tighten your security – and control your costs.

7. 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute

Take Your Print Security to the Next Level

Print security is often neglected when Trusts assess potential threats. But print data breaches have serious consequences – for patient confidence, your credibility, and your finances.

Advanced print security solutions are available today to let you balance flexibility with security, control with ease of use.

They allow you to fully exploit the latest trends and technologies – such as mobile working and mobile printing – without compromising confidentiality or exposing you to unnecessary threats.

They harness the incredible power of MFPs, using next-generation technology to help you to stay smart and secure.

To find out more about print security solutions, talk to a Managed Print Services (MPS) partner today.

About Xerox

Xerox Corporation is a technology leader that innovates the way the world communicates, connects and works. We understand what's at the heart of sharing information - and all of the forms it can take. We embrace the integration of paper and digital, the increasing requirement for mobility, and the need for seamless integration between work and personal worlds. Every day, our innovative print technologies and intelligent work solutions help people communicate and work better. Discover more at www.xerox.com and follow us on Twitter at @Xerox.

For more information visit **www.xerox.com**.