KONICA MINOLTA

7 COMMON MISTAKES WHEN IMPLEMENTING CLOUD PRINT AND HOW TO AVOID THEM

Use of cloud technology is commonplace but the extent of its use varies massively. Print is rarely invited to the cloud party and often overlooked as legacy. A missed opportunity.

Your print infrastructure can be securely moved to the cloud and in doing so you will not only make printing easier for users and better support mobile working, you will relieve your IT teams of the need to manage a myriad of print servers.

Here's some Dos and Don'ts you need to consider:

1

MISTAKE

Not planning for the future

Getting tied into solutions that do not allow for flexible procurement in the future can become an obstacle for sustainable growth.

SOLUTION

Build in flexibility

Consider any future changes to your organisation and your IT network infrastructure when implementing a cloud print solution. For example, the platform needs to be scalable so any new applications can be accommodated in addition to legacy applications. Ideally, your contract should also be flexible enough to grow and change with your organisation.

2

MISTAKE

Insufficient internet connectivity

Even temporary interruptions to an internet connection can cause costly downtime of the print infrastructure.

SOLUTION

High availability by default

Make sure your internet connection isn't flaky and that it's fast enough. This means that there should be no single points of failure with local failover potential when offline. Effectively moving to the cloud should enable you to have a high availability architecture by default (ideally with an SLA).

3

MISTAKE

Being fooled by cloud wash — is it really cloud?

There are many print management solutions that claim to be "cloud", but in essence they are hosted on-premise solutions. These solutions have many limitations that are often not acceptable in terms of IT security and connectivity requirements.

SOLUTION

Look for SaaS

Ideally, a cloud print service should be a Software-as-Service (SaaS)[1] model, not require a VPN, have automatic updates (patching), not require LDAP[2] connectivity to cloud identity management[3] solutions (e.g. Azure Active Directory) and not require an on-premise server (or mini-PC) for connectivity to the MFP embedded client.

4

MISTAKE

Not having cloud SLAs in place

Your provider should offer clear SLAs and there shold be clarity in terms of what your provider is responsible for and what you need to take care of.

SOLUTION

Clarity over responsibilities

A Service Level Agreement (SLA) gives a clear understanding about what is included in the service from the provider's side and what needs to be taken care of you. Typical agreements consist of solution availability, support times, plans for expected downtime and data ownership, as well as disaster recovery and backup.

5

MISTAKE

Neglecting security

Be aware your data is the most valuable thing you own! Ensure you protect it at all times, even if it is print-related data.

SOLUTION

Check for the highest security standards

- Zero Trust Policy[4]
  - The data centre is certified in accordance with ISO 27001[5]
  - Data centres locations (high requirements related to GDPR compliance)
  - End-to-end encryption for your data
- Main data centre and backup data centre in different places in case of a disaster
  - 24/7 monitoring
  - Uninterruptable power supply approach in place
  - Automatic security updates

6

MISTAKE

Forgetting about people

Often modernisation and improved user experience go hand in hand. However, with something as traditional as printing, there may be significant resistance to change.

SOLUTION

Print as usual

Essentially, to minimise disruption to end users and reduce adoption curves, a cloud print platform should enable users to continue as if nothing had changed. The key is how and when you communicate any changes to your users, being sure to stress the benefits to them.

1 Software-as-a-Service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted
2 LDAP (Lightweight Directory Access Protocol) is an open and cross-platform protocol used for directory services authentication
3 Cloud identity management can manage user access to WiFi networks, connect cloud servers and facilitate authentication
4 Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network
5 ISO/IEC 27001 is an international standard on how to manage information security. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS).

GET YOUR FREE IMPLEMENTATION PLAN

Now that you are well aware about which mistakes to avoid, learn how to smoothly migrate your print infrastructure from on-premise to cloud.

Infographic by
Konica Minolta Business Solutions Europe GmbH

Giving Shape to Ideas