Cloud Print Services, 2022

The Cloud Print Services Market Landscape, 2022
Excerpt Report: Xerox

QUOCIRCA

Cloud Print Services, 2022

Executive summary

The cloud has underpinned the digital transformation journey for many organisations as they adapted to decentralised work models over the past two years. As we move into the era of hybrid work, organisations are increasingly focused on building a resilient, future-proof IT infrastructure. The high availability, flexibility, and scalability of the cloud is helping businesses become more agile, while also better preparing them for cyberattacks through advanced data compliance and security. In addition to flexibility and scalability, the cloud can also help organisations reduce costs – both financial and environmental – compared to operating a traditional on-premises environment.

Print manufacturers and ISVs are bringing cloud-based options to the market to cater for the different public, private and hybrid cloud approaches being pursued by customers. Cloud print services and solutions encompass the remit of serverless printing platforms, cloud-based remote monitoring platforms, and hybrid cloud print management platforms, which may be managed internally or by third-party managed print services (MPS) providers. Cloud print services may also include other adjacent services and solutions around digitisation, workflow, security and collaboration.

This report highlights key market trends for cloud print services, covering offerings from both manufacturers and independent software vendors (ISVs). It draws on multiple primary research studies conducted by Quocirca in 2022.

Key findings include:

- **Cloud adoption continues to increase, underpinning the digital transformation journey.** According to Quocirca's latest research, 20% expect their IT infrastructure to be fully in the cloud by 2025, a rise from 6% today. A further 41% expect it to be mostly in the cloud, a rise from 21% today. This is creating momentum in the cloud print services market, as more organisations recognise the benefits of eliminating or minimising their reliance on on-premises print servers.
- **Cloud print services help overcome the complexity and inefficiencies of managing a traditional print infrastructure.** Conventional print management is typically reliant on on-premises print servers and incurs a high IT administrative burden to manage driver installation, device configuration and compliance, device monitoring, reporting and management, server and queue management, firmware updates, and app deployment and maintenance. Cloud-based print management can reduce the IT burden and, where print servers are eliminated, also lower the financial and environmental costs associated with procuring and managing print servers.
- **Cloud print adoption continues to accelerate.** Overall, 43% of organisations have already implemented a cloud print management platform, with a further 37% reporting that they have plans to do so in the next two years. The US is the most mature in relation to cloud printing adoption (56%), with Germany trailing at 32%. The finance sector is the most advanced vertical (56%).
- **Cloud print adoption aligns with customer sustainability goals.** By reducing or eliminating print servers, organisations can lower costs and reduce environmental impact through lower energy usage. Quocirca's Sustainability Trends reports revealed that 80% of organisations had already implemented or planned to implement cloud printing as part of their sustainability strategy.
- **Organisations are looking for support from MPS on their cloud print journey.** Of respondents, 40% said moving to a cloud print management platform was a top benefit of MPS adoption. Notably, the use of cloud-based print management is more common amongst organisations that have been using MPS for some time or have moved beyond the initial stages (60%). However, organisations that are managing some element of their print infrastructure in-house are more likely to have made the transition to a cloud-based print management platform.
- **Organisations recognise the enhanced security of cloud printing platforms.** Over half (52%) of respondents considered cloud printing to be more secure than an on-premises platform. Cloud security is a major consideration, with 42% indicating they were operating a zero trust architecture for their IT environment. Ensuring cloud platforms conform to zero trust principles is now a major consideration, and as IT environments become increasingly distributed, a zero trust approach is becoming more important.

© Quocirca 2022

Contents

© Quocirca 2022

Methodology

End-user analysis

This report highlights key market trends and provides an overview of the competitive landscape, including both manufacturers and independent software vendors (ISVs). It is based on Quocirca's annual MPS study (203 ITDMs), and references our Print 2025 study carried out in March 2022 (521 ITDMs and 1,021 office workers) and Zero Trust study carried out in February and March 2022 (202 ITDMs). Where useful, data has also been drawn from other studies carried out by Quocirca.

Vendor analysis

To participate in this study, vendors were required to submit a written response to Quocirca's request for information on cloud services and solutions. This report covers only vendors that agreed to participate in this study. It includes:

Manufacturers: Canon, HP, Konica Minolta, Lexmark, Ricoh, Xerox
ISVs: directprint.io, EveryonePrint, ezeep, Kofax (Printix), MPS Monitor, MyQ, NT-ware, PaperCut, Process Fusion, Vasion (PrinterLogic), Y Soft

Definitions

Cloud computing

Public cloud computing is on-demand delivery of IT resources over the internet, generally with pay-as-you-go pricing. Instead of buying, owning and maintaining physical data centres and computing hardware, customers are given access to technology services such as computing power, storage, networks and databases as needed from a cloud provider. The cloud can offer faster innovation, flexible resources and economies of scale. The public cloud enables a business to trade fixed capital expenses (such as data centres and physical servers) for variable operational expenses, and only pay for IT as it is consumed. Elasticity enables a business to increase and decrease the amount of resources as business needs change.

The three main types of cloud computing include Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service. Each type of cloud computing provides different levels of control, flexibility and management.

- **Infrastructure-as-a-Service (IaaS).** IaaS contains the basic building blocks of cloud IT. It typically provides access to networking features, computers (virtual or dedicated hardware) and data storage space. It is the responsibility of the organisation using IaaS to install and manage any software (which generally includes operating systems) on top of the physical or virtual hardware platform. IaaS provides the most flexibility and management control over IT resources. However, it offers the least cost off-loading, as the user must still bear most of the technical operations and other costs around implementing and maintaining the software layer.
- **Platform-as-a-Service (PaaS).** PaaS removes the need to manage the underlying infrastructure (usually hardware and operating systems), allowing IT to focus on deployment and management of applications. This means a business does not need to manage resource procurement, capacity planning, software maintenance, or patching.
- **Software-as-a-Service (SaaS).** SaaS is a method for delivering software applications or services over the internet, on demand and typically on a subscription basis. SaaS cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, such as software upgrades and security patching.

Cloud computing models

There are four ways to deploy cloud services:

- **Public cloud:** Public clouds are owned and operated by third-party cloud service providers, which deliver computing resources such as servers and storage over the internet. All hardware and other supporting infrastructure are managed by the cloud provider. Examples of public cloud providers are AWS, Microsoft Azure, Google Cloud Platform, IBM Cloud, Rackspace and VMware Cloud. Large public clouds such as Azure and AWS offer a mix of IaaS, PaaS and SaaS, although their biggest strengths tend to lie in the PaaS space.
- **Private cloud:** A private cloud refers to cloud computing resources used exclusively by a single business or organisation. A private cloud can be physically located in the company's on-site data centre or within a colocation facility operated by a third party, while the business still owns and operates the computing and storage hardware, along with some aspects of networking hardware. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.
- **Hybrid cloud:** Hybrid clouds combine public and private clouds, bound together by technology that allows sharing of data and applications between them. This gives a business greater flexibility and more deployment options, and helps optimise the existing infrastructure, security and compliance. The most common method of hybrid deployment is between the cloud and existing on-premise infrastructure to extend and grow an organisation's infrastructure into the cloud, while connecting cloud resources to internal systems.
- **Multi-cloud:** A multi-cloud environment aims to eliminate reliance on any single cloud provider or instance. A typical multi-cloud architecture utilises two or more public clouds, as well as private clouds. Companies use multi-cloud environments to distribute computing resources and minimise the risk of downtime and data loss. They can also increase the computing power and storage available to a business.

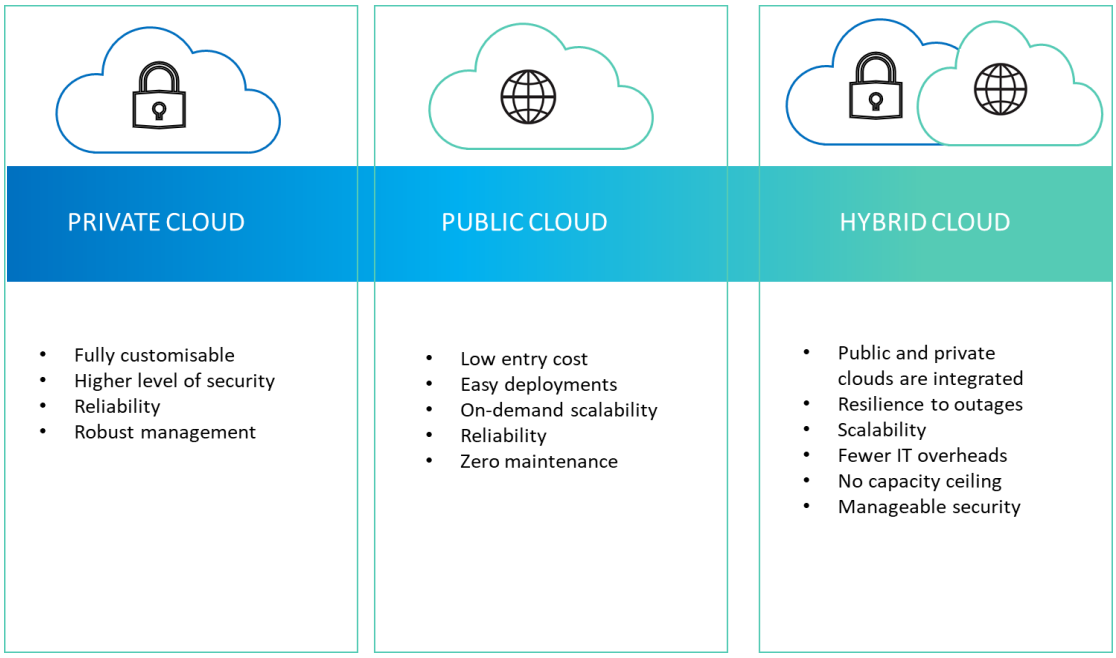


Figure 1. Cloud models

Multi-tenant vs. single-tenant cloud

In a multi-tenant cloud environment, a public cloud provider runs a single instance of an application or service that is used by multiple different customers. However, it gives each customer a separate, secure space for storing data and projects. Each user can access only its own stored information, and the cloud provider's complex suite of permissions and security prevents other customers from accessing this content or the content or details of any ongoing processes. Since a multi-tenant cloud architecture means the same servers are hosting multiple users, it is critical for public cloud customers to thoroughly understand the performance and security offerings of their cloud provider.

© Quocirca 2022

The alternative to multi-tenant cloud architecture is single-tenant cloud, in which a server hosts only one customer, or tenant, who has sole access. In a single-tenant architecture, the customer has greater control over multiple capabilities, including data, performance, security and storage. However, this can reduce resource flexibility, as the cloud instance will have been provisioned for the specific customer.

In essence, the difference can be seen as:

- Single-tenant cloud: architected to provide the envisaged resource requirements for a single, specific company. All hardware and application code is costed to support that company. To allow for any resource overruns, the single-tenant cloud owner needs to provide and cost in the respective server, storage and network overhead to allow for demand on resources. These resources are unlikely to be regularly needed, but need to be kept running and will involve additional costs, such as for licensing, alongside power and maintenance costs. If the initial design is wrong, there may be insufficient resources when the application or service needs it, which could lead to the service being hindered or failing completely.
- Multi-tenant cloud: architected to support multiple customers that may have counter-cyclical needs in their applications, based on geographical location or when they run certain services, such as payroll, data consolidation or reporting. As such, applying a small amount of resource overheads will generally be sufficient to meet the needs of all customers – and the cost for this can be shared amongst customers.

The cloud print ecosystem

A cloud-based print management platform can be delivered as a part of or independently from an MPS. It can be deployed as a private or hybrid model, in which print servers are located in the cloud, eliminating the need for on-premise hardware (serverless printing) or for the software to be hosted on-premise (private cloud). Serverless printing enables direct IP printing from workstations to network printers, which removes the complicated set-up of having a dedicated print server.

The cloud print services and solutions ecosystem is diverse, covering vendors that deliver cloud MPS and cloud-based software and solutions. This is categorised as follows:

- **Printer/copier manufacturers –** Traditional OEMs such as Brother, Canon, HP Inc., Konica Minolta, Kyocera, Lexmark, Ricoh, Sharp and Xerox.
- **Channel partners such as MPS providers –** These are a channel to market for some printer and copier vendors, and may offer cloud print services and solutions as part of a wider MPS or cloud offering.
- **ISVs –** These are companies that write and market software for facilitating tasks and processes. There is a thriving market for ISVs that focus on print management solutions, including directprint.io, EveryonePrint, ezeep (powered by ThinPrint), Kofax (Printix), MyQ, NT-ware (uniFLOW), PaperCut, Process Fusion (UniPrint), ThinPrint, Vasion (PrinterLogic), and Y Soft.

© Quocirca 2022

Introduction

The rise of the cloud

As the post-pandemic world takes shape, the cloud has become the foundation for speed, agility and resilience for many companies. It delivers flexibility and on-demand scalability, enabling businesses to emerge stronger and more adaptable, while plugging gaps in their resilience measures. Organisations that adapted to the pandemic best had already taken steps to modernise their IT environment and were able to rapidly scale resources to support a remote workforce.

As organisations ramp up their digitisation journeys and remote working becomes a permanent feature for many, cloud initiatives are set to accelerate through 2022 and beyond. According to Quocirca's latest research, 20% expect their IT infrastructure to be fully in the cloud by 2025, a rise from 6% today. A further 41% expect it to be mostly in the cloud, a rise from 21% today (Figure 2).

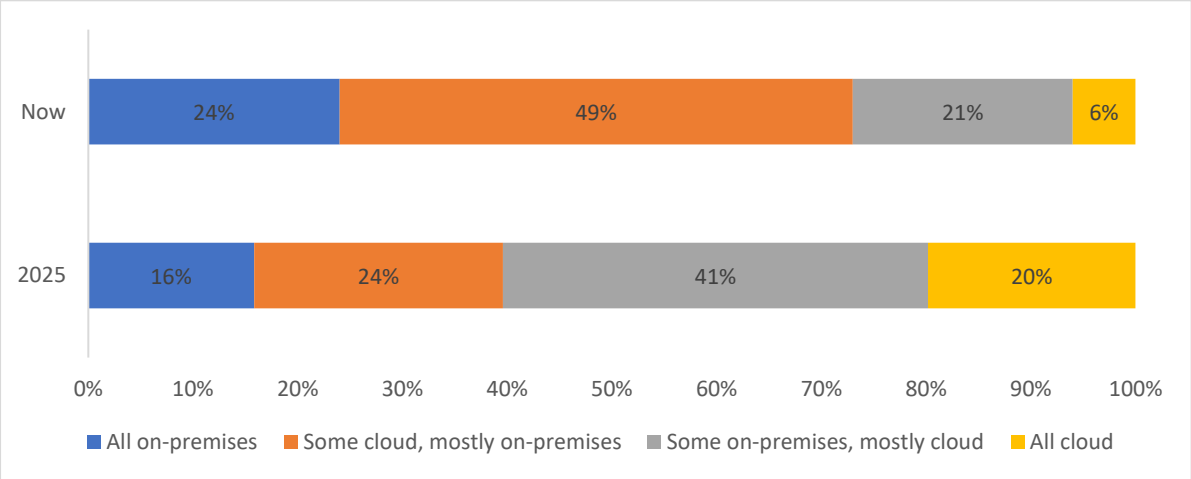


Figure 2. Which statement best reflects your organisation's total IT environment (infrastructure, applications, data, etc., excluding client devices)?

There are many drivers for organisations considering a move to cloud computing. Alongside the move from capital expenditure (CapEx) to operational expenditure (OpEx), it can be appealing to offload variable costs such as maintenance to a third party as part of a predictable monthly subscription. There is strong perception that public clouds will be better maintained and updated as time progresses – so far, this has proven to be the case, but will need to be watched carefully as the market matures. Needs around data sovereignty are also being better met by large public cloud providers, as users can choose where data is stored around the globe.

However, a full cloud platform may only be suitable for new organisations that were 'born in the cloud', having no existing IT platform. Alongside these organisations, some perceive their existing platform as having reached the end of its useful life and, as such, believe a migration to the cloud can be a strategic move in a single transformation. For the majority, however, the cloud will be a journey: existing investments in on-premise infrastructure, combined with the constraints of many existing enterprise applications, will lead to a hybrid platform, with some aspects remaining on-premise for some time while other functions are moved directly to cloud and new or replacement functionality is provided from the cloud over time.

Many organisations are operating a hybrid model for the cloud as they look to maintain a mix of on-premise and cloud infrastructure. In order to increase scalability, reduce costs or avoid vendor lock-in, organisations may adopt a multi-cloud strategy – using multiple and often less connected cloud services. The cloud is not an either/or model, and an organisation's choice of approach has to be based on costs, performance, security, compliance, and governance requirements.

© Quocirca 2022

Meanwhile, edge computing – computing that is processed at or near the data source, or "edge", of the network – is creating momentum for the distributed cloud. The growth of internet-connected devices (including printers) and impact of ever-faster network technology such as 5G is set to drive demand for edge computing solutions in 2022 and beyond.

Cloud print services momentum

As organisations embrace the hybrid work model, they are under increased pressure to manage and secure printing across both home and office environments. By turning to cloud print management, organisations not only reduce the IT burden associated with managing print in-house through using a third-party MPS provider, but can also better track and monitor print usage across the hybrid workplace. While office print volumes are likely to continue a downwards trajectory, given fewer employees are in the office, there is a greater need to ensure document security with more remote workers printing across multiple locations.

Cloud printing continues to gain momentum. Overall, 43% have already implemented a cloud print management platform, a significant rise from 29% in 2021. A further 37% are planning to do so, which means 80% are expecting to use cloud-based print management. Notably, the use of cloud-based print management is more common amongst organisations that have been using MPS for some time or have moved beyond the initial stages (60%). The US is the most mature in relation to cloud printing adoption (56%), with Germany trailing at 32%. The finance sector is the most advanced vertical (56%). To enable remote workers to route print jobs to printers in the office, 45% of respondents indicated that they had implemented remote job submission to office devices, which rises to 52% in the US and 56% in the financial sector.

Cloud in the zero trust security era

Traditional security approaches that focused on the perimeter of the network have become ineffective, and must now accommodate an ever-changing, diverse set of users and devices, as well as much more prevalent threats targeting previously 'trusted' parts of the network infrastructure. For larger organisations in particular, securing cloud-based remote employees will require a move to a zero trust security model resembling a secure access service edge (SASE) architecture.

The rapid shift to the cloud has led to security gaps and increased vulnerabilities. As the remote work landscape proliferates to encompass more devices at the edge, network security is increasingly challenging. Remote workers are using laptops and printers with fewer controls in place connected to home networks, often with default security credentials, which leaves them exposed to cyberattacks.

The wider adoption of home printing is already impacting security confidence amongst IT decision-makers. Quocirca's Print Security 2022 study revealed that just 26% were completely confident in the security of their print environment as offices reopened. Additionally, 66% stated that they were very or somewhat concerned that employee-owned printers presented a risk to their organisation. Organisations must protect cloud data from phishing attacks, malware, ransomware and a host of other vulnerabilities.

Zero trust security ensures that the same controls applied to the corporate network also extend to the home or remote worker. This means organisations need visibility and security controls across the print infrastructure to support a zero trust model. According to Quocirca's 2022 zero trust study, 42% of organisations have implemented a zero trust security architecture, with only 1% stating that they have no plans to do so. Amongst organisations using MPS, 31% of respondents said it was very important that their MPS provider could provide services around zero trust security for their print infrastructure; this rises to 48% in the US and 49% in the financial sector.

Ultimately, a layered approach to security is necessary to address the varying security needs of businesses. This should include multi-factor authentication/identity access management, device security and remote monitoring, and reporting tools that can track not only user behaviour, but also device anomalies such as DDoS attacks. Although cloud print management platforms that support zero trust principles are emerging, approaches taken vary and organisations should carefully evaluate claims.

© Quocirca 2022

Sustainability and the cloud

Shifting to the cloud can enable organisations to reduce their environmental impact and improve their sustainability credentials. Sustainability is moving higher on the corporate agenda; Quocirca's Sustainability 2022 research revealed that 75% of respondents were prioritising reducing their environmental impact – with 74% stating that reducing paper usage was either very or somewhat important and 80% planning to implement or already having implemented cloud printing as part of their sustainability initiatives.

The cloud is a big winner here: data centres are heavy overall users of energy, and privately owned data centres are notoriously inefficient. Public cloud data centres are by their very nature more efficient, and hyperscale providers such as AWS, Google and Microsoft are driving their cloud infrastructure efficiency and higher resource utilisation to be more energy efficient than an enterprise data centre. The ability to share resource overhead across many different customers is useful here. Similarly, large-scale platforms can make the most of economies of scale with cooling and power backup systems. Also, massive public data centres can be positioned where renewable energy sources are present, such as hydro or geothermal, whereas privately owned data centres tend to have to be built near the point of use.

However, even at a private cloud level, virtualisation of the underlying physical equipment can also provide higher levels of sustainability. Rather than having to size physical resources for each application, organisations will be able to share resources across multiple workloads – just not to the level a massive, multi-tenanted public cloud facility can offer.

© Quocirca 2022

How cloud printing supports a hybrid work model

Print infrastructure has been slower than other parts of IT in moving to the cloud. However, as is being increasingly recognised, such a move presents tremendous opportunities to lower both financial and environmental costs, provide massive improvements around information security, and better support a hybrid working environment, including those still working from home. It also offers distinct improvements over the efficiencies and capabilities of operating a traditional print infrastructure that uses on-premise print servers.

The complexity of traditional print management

Managing traditional and diverse print infrastructure is costly. Dedicated print servers can provide a range of benefits, including centralised print management, automatic driver updates, high availability, control over a user's printer profile, and integrated reporting. However, on-premise print servers are expensive to purchase and manage, and need to be continuously maintained by the IT department. Such management does not always keep pace with the increased prevalence of cyberthreats that organisations face.

Print management tasks include the initial provisioning of the printers themselves, followed by maintenance of print drivers and associated software. In a traditional mixed-fleet print infrastructure, there are typically multiple print queues for each brand of MFP, along with many print drivers, which require various types of management and support. The impact of a print server going down can be disruptive and costly. However, high-availability redundancy is generally not in place.

The proliferation of home printers in response to broader remote working requires solutions that enable remote submission of print jobs to office printers, a more complete approach to information and device security, and more comprehensive analytics on printing across the home and office environment. Even within the office, there are increased security implications, particularly in organisations that operate a broad and diverse range of print devices; this is made worse as the hybrid work environment creates a much more complex and diverse environment.

The hidden costs of print servers

Quocirca research identifies that, on average, servers costs £1,900 each to provision, with annual running costs of £1,500. The same research indicates that the average organisation operates approximately three print servers.

This means each organisation has a capital outlay of close to £6,000 to provision its print servers, followed by £4,500 per annum in operating costs, just to run print jobs on site.

These costs mount up for larger organisations operating thousands of printers.

Addressing print infrastructure complexity with cloud print management

In a cloud-based print infrastructure, networked printers and MFPs are retained at the customer site, while print servers are hosted in the cloud and managed by a third-party provider. Increasingly, such services are expanding to embrace remote workers, not just to enable job submission to office-based printers, but also to manage the usage of printers in the home environment. Cloud print management consolidates print management tools into one platform, allowing configuration, users, printers and policies to be managed remotely. This eliminates the need for internal IT maintenance and individual driver installation.

Cloud print management tools offer secure printing, remote job submission and mobile printing. For instance, a global print queue can avoid the need for multiple print drivers and queue management. In addition, cloud-based print management can offer stronger access controls, security and compliance, with firmware updates, fleet management, and reporting all handled by the provider.

Cloud print management can operate within a private hosted or hybrid model. Print jobs may be sent to the cloud or retained locally. In smaller organisations that have very few workstations or printers, a serverless model may be a better approach, where everything to do with the management of print jobs is managed directly in the cloud. It can also appeal to enterprises that are consolidating servers, looking to reduce print costs and lower the IT administrative burden. For organisations with tighter security regulations that are not looking to eliminate their print servers, a hybrid solution allows ease of use for administrators while still allowing for consolidation and cost savings, as certain data around the print job is managed by on-premise servers while the metadata around the job itself is managed in the cloud, deployed under a single management platform.

© Quocirca 2022

Cloud print momentum

As organisations embrace the hybrid work model, they are under increased pressure to manage and secure printing across both home and office environments. By turning to cloud print management, organisations not only reduce the IT burden associated with managing print in-house through using a third-party MPS provider, but can also better track and monitor print usage across the hybrid workplace. While office print volumes are likely to continue a downwards trajectory given fewer employees are in the office, there is a greater need to ensure document security with more remote workers printing across multiple locations.

Cloud printing continues to gain momentum. Overall, 43% have already implemented a cloud print management platform. A further 37% are planning to do so, which means 80% are expecting to use cloud-based print management. Notably, the use of cloud-based print management is more common amongst organisations that have been using MPS for some time or have moved beyond the initial stages (52%). The US is the most mature in relation to cloud printing adoption (56%), with Germany trailing at 32%. The finance sector is the most advanced vertical (56%). To enable remote workers to route print jobs to printers in the office, 45% of respondents indicated that they had implemented remote job submission to office devices, which rises to 52% in the US and 56% in the financial sector.

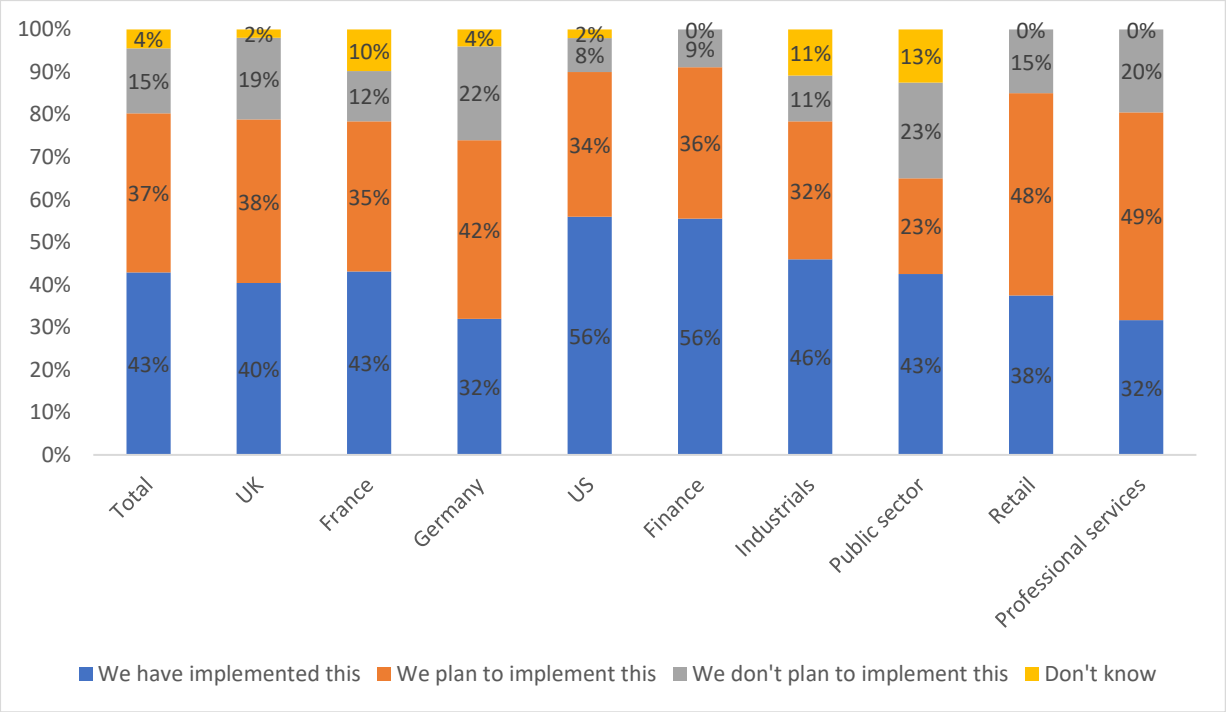


Figure 3. Plans to implement a cloud print management platform (MPS 2022 study – organisations using MPS)

Those using a hybrid MPS approach are also more likely to move to the cloud in the future. It is apparent that those with a fully outsourced MPS model are either being held back by the MPS provider or just not incentivised enough to move away from the tried and tested on-premise approach. For MPS providers, this is both a problem and an opportunity: the maintaining, support and evolution of on-premises systems is expensive and fraught with problems. The cloud provides a far easier and cost-effective means of supporting customers, yet many will not want to move to a new platform unless there is enough incentive to do so. The MPS provider must be able to move their on-premise customers to the cloud at a speed that meets both its own needs and the overall cloud plans of the customer to provide a more effective and lower-cost overall offering.

© Quocirca 2022

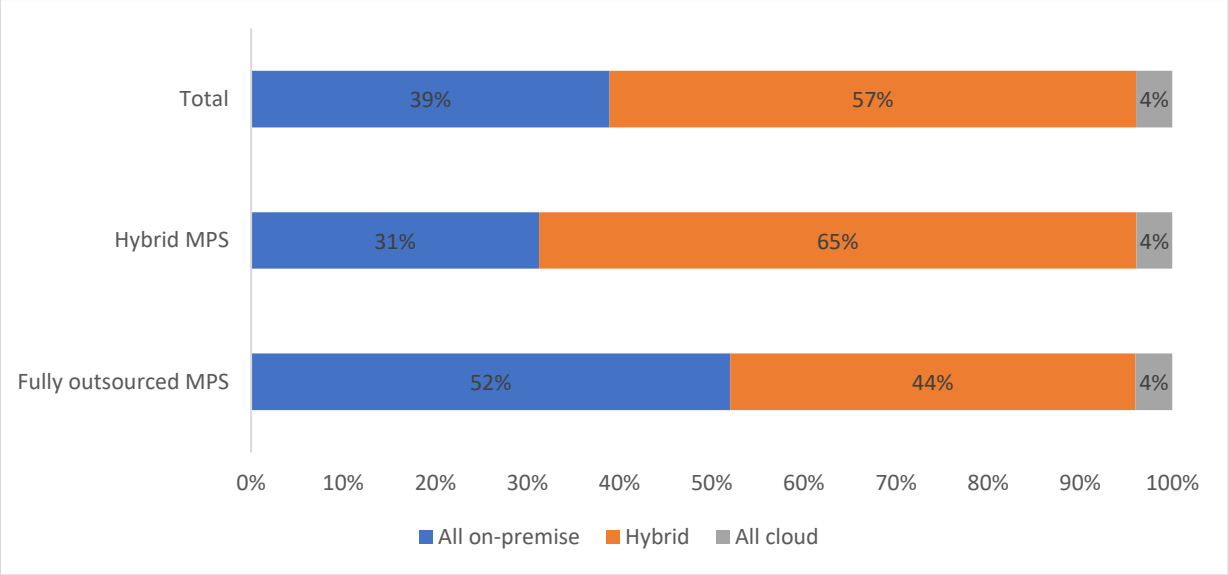


Figure 4. Which statement best reflects your organisation's print environment?

Overall, 39% of respondents are still operating a fully on-premise print management platform This rises to 52% of those using a fully outsourced MPS model. It seems that organisations that are partly managing their print environment in-house are more likely to be more positive about shifting to the cloud, while those using a fully outsourced MPS provider are slower to move.

This is an opportunity for MPS providers to transition these organisations – however, in many cases traditional MPS providers may not have a broad cloud portfolio. In some instances, those using a hybrid approach to MPS may be using third-party cloud print management solutions that are not under the remit of the MPS provider. Indeed, 40% of organisations said that moving to a cloud print management platform was a top benefit of MPS adoption.

© Quocirca 2022

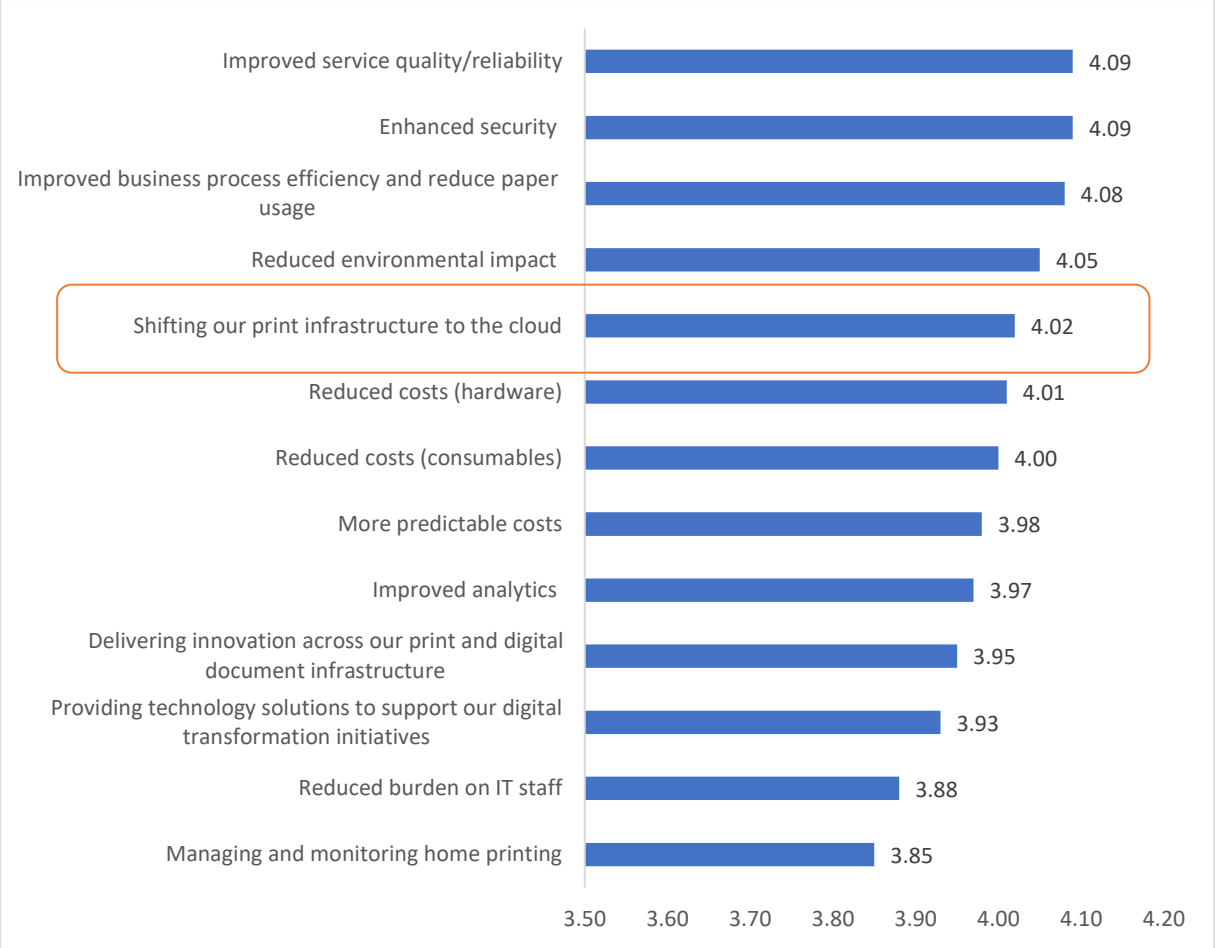


Figure 5: Importance of MPS benefit (rated on a scale of 1 to 5 where 1 is not important and 5 very important)

Organisations using MPS are looking for providers that can support their transition to the cloud. Of respondents, 40% indicated that it was a key driver for MPS adoption, with its overall importance score reaching 4.02 out of 5 from respondents (Figure 5).

© Quocirca 2022

In terms of expectations from MPS providers, 38% overall stated that they would be more likely to select a provider that offered cloud print services, which puts cloud print services in second place after workplace services (Figure 6). US respondents were most likely to prioritise cloud print services as an additional service (54%), compared to less than one-third of respondents in the UK and Germany.

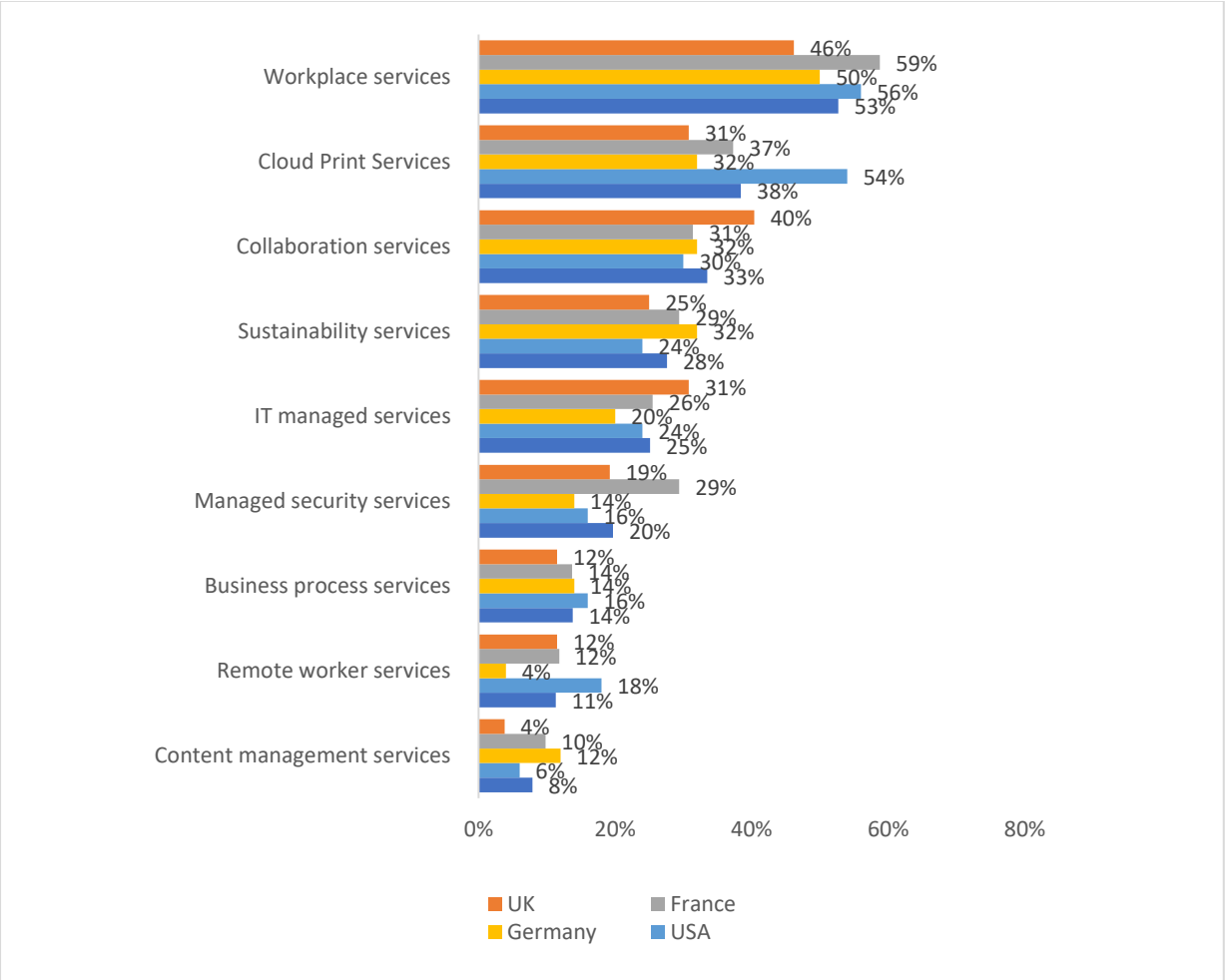


Figure 6. What additional services would be more likely to make you select an MPS provider? (Top 7 shown)

Cloud security

Increased use of the cloud across all business sizes creates the need for robust security measures to protect users and keep data and business operations safe from cyberattacks. The public cloud, while removing the need for organisations to manage the underlying hardware, also takes away some ability to manage security. However, this does not eliminate the responsibilities of the user around security for the total environment.

Public cloud environments have proven to be secure at a base level. However, security breaches have happened due to poor application or service implementation by users.

Cloud printing considered more secure than on-premise

Overall, Quocirca's research shows that there is a stronger perception around how much more secure the cloud is than on-premise platforms for print management. Of survey respondents, 87% considered the cloud to be 'a lot more secure' (52%) or 'somewhat more secure' (35%) than an on-premise platform. No respondents felt that a cloud platform would be 'a lot less secure' than an on-premise one, with only 3% perceiving it as 'somewhat less secure' (Figure 7).

Large public cloud operators not only can afford to attract the best security experts as employees, but also know that they must keep them current as to what sort of threats they will be dealing with. Although a security breach within a single-tenanted environment may be catastrophic to a single company, such a breach in a multi-tenanted environment could bring the provider to its knees: it is imperative that the provider maintains suitable levels of security, at both the technical and physical levels, around as much of its platform as possible.

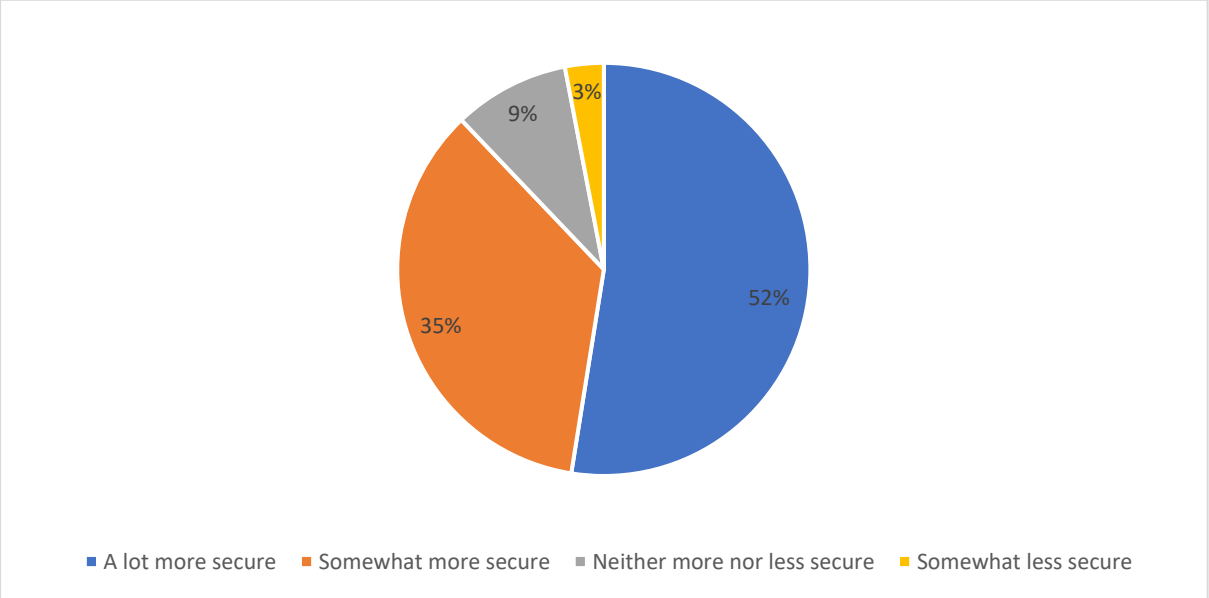


Figure 7. Do you consider using a cloud print service provider more or less secure than an on-premise print environment?

MPS and zero trust

'Zero trust' is a security model that states that nothing across an IT platform should be trusted implicitly – every device, network connection, user, application/service, data source, etc., needs to be regarded as a possible source of malicious activity, and security must be applied accordingly. In Quocirca's research, 81% of respondents stated that they understood that zero trust was a security model, as opposed to a single product or set of solutions. Already, 49% of respondents have stated that zero trust is 'critically important' to their organisation's security posture, with a further 42% stating that it is 'very important'; 42% had already implemented a zero trust approach, with a further 14% in a pilot or proof-of-concept stage and 28% at the early evaluation stage.

Organisations perceive a need for a different approach to security from the historical 'walled garden' (securing the perimeter) or 'onion skin' (layers of security) models. Adoption of the cloud means large areas of the underlying hardware and operating systems are outside of the organisation's security control, while greater decentralised working means much activity is occurring across home and public networks with essentially insecure devices.

Those that use an MPS provider are looking for help from the provider around zero trust. Overall, 74% of respondents saw provision of zero trust services from an MPS provider as 'very important' (31%) or 'fairly important' (43%) (Figure 8). The financial sector is the most focused on this, with 49% seeing it as 'very important'.

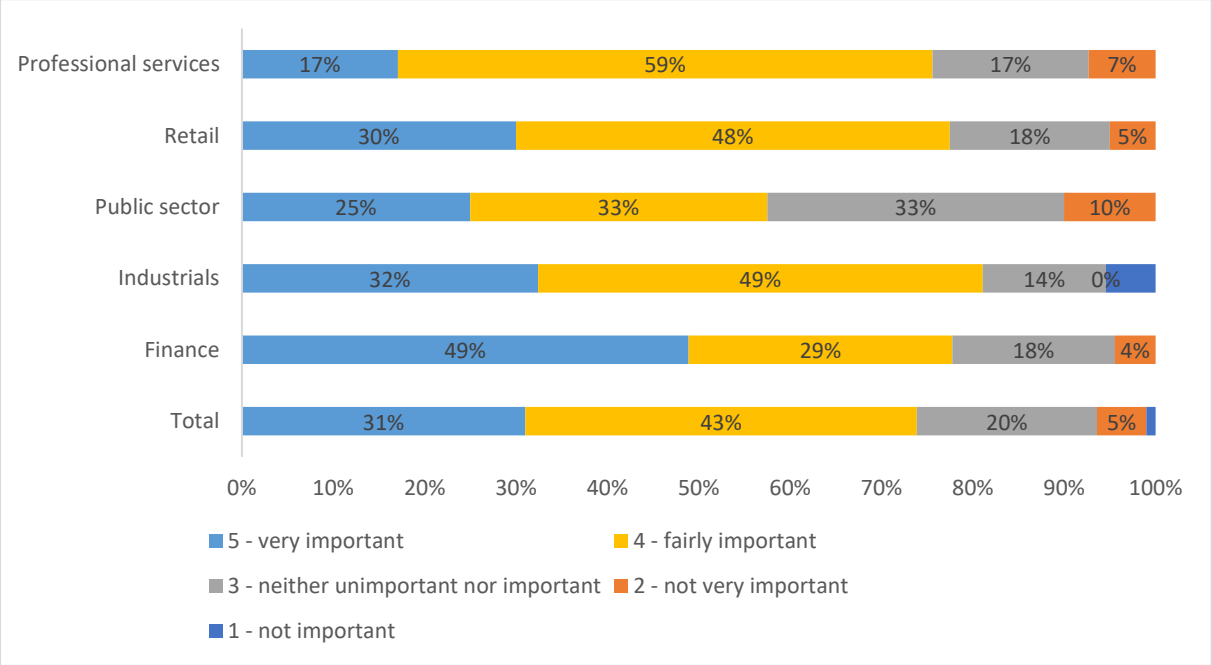


Figure 8. How important is it that your MPS provider can provide services around zero trust security for your print infrastructure?

Zero trust drivers

Overall, the biggest driver behind the adoption of zero trust security models is to protect sensitive data, with 38% of respondents citing this as one of their most important criteria. Securing cloud deployments comes second at 29%, with securing the complete digital attack surface third at 27% (Figure 9).

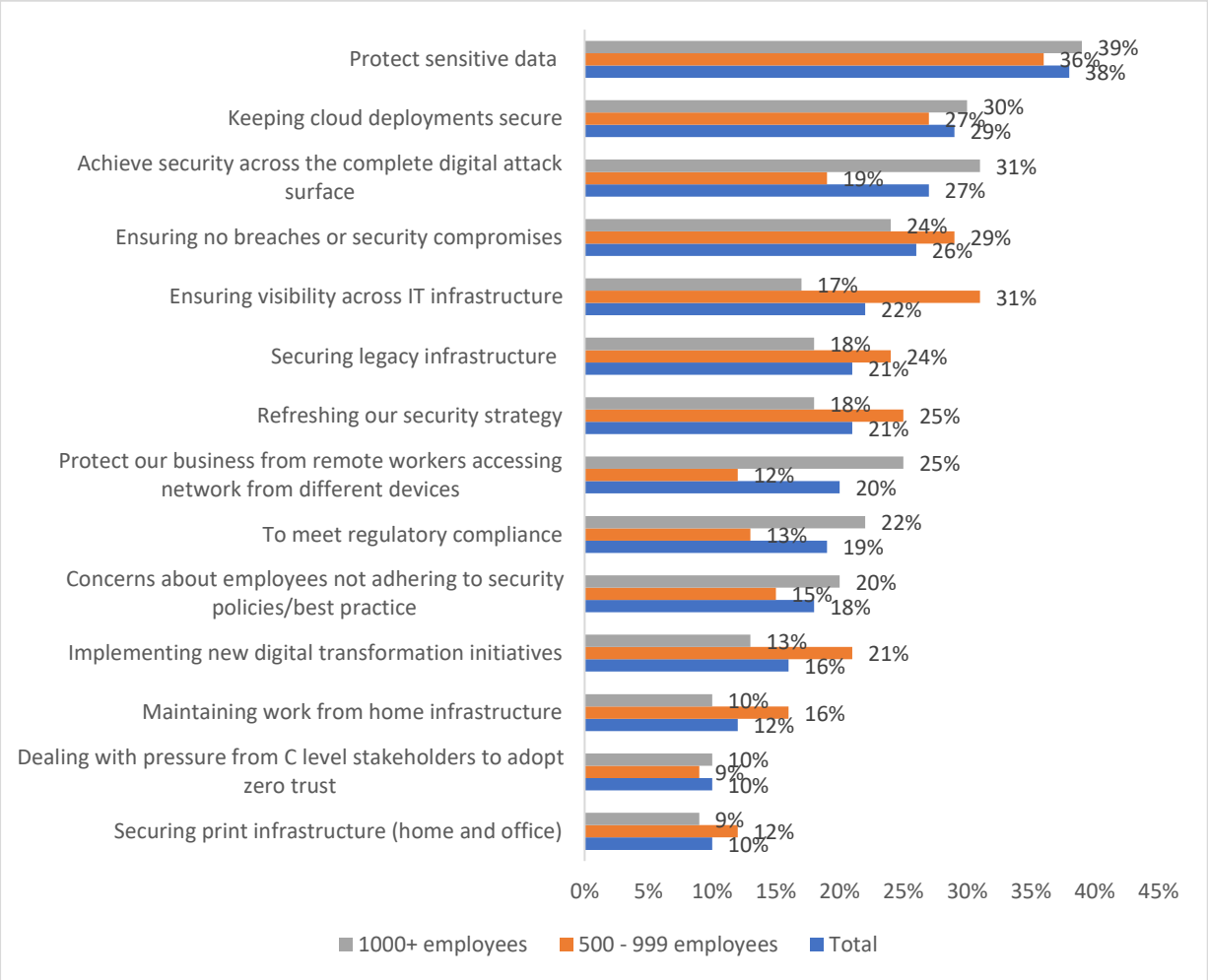


Figure 9: What are the main reasons for deploying zero trust?

Organisations are changing their whole approach to security. The focus is now moving towards a data-centric model. With cloud-based print management, this can be a strong message: the underlying platform is already perceived as and proven to be secure, and the ability to ensure that the print management system is continually updated against security threats is an improvement on on-premise implementations, which are often not updated as regularly as they should be.

Cloud-based print management systems can also interoperate with printer hardware far more effectively: areas such as printer drivers can be updated directly via the cloud, firmware can be modified to provide greater protections against device security threats, and devices that have been compromised can be airlocked from the platform until the problem can be automatically or manually remediated. Also, print jobs can be much better handled. Jobs can be routed to the best-possible device to ensure optimum levels of efficiency and effectiveness, encrypted to prevent man-in-the-middle attacks; and prevented from printing via insecure printers.

© Quocirca 2022

Buyer recommendations

Although the cloud print services market is still evolving, movement to the cloud is unstoppable. An increasing number of print manufacturers are offering fully managed cloud print services, while independent software vendors (ISVs) are a good solution for organisations operating a mixed-fleet environment or not using a fully outsourced MPS.

Ensuring that a chosen solution fits in with an organisation's needs now and in the future is key. Solutions must not force an organisation into moving faster than it desires toward cloud deployment, and neither must they hold back any organisation that wants to move at speed into the cloud. A portfolio that offers private, public and hybrid models will enable organisations to transition as their on-premise and cloud needs adapt. For those already on their cloud journey, it will be crucial to choose a provider that will be able to keep pace.

- **Serverless or hybrid.** Smaller organisations with few workstations or printers may find a serverless model with no on-premise print servers a better approach to saving money on print server costs and overheads. It can also appeal to enterprises that are consolidating servers, looking to control print costs and lower the IT administrative burden. Organisations not looking to eliminate their print servers, or that have security concerns, may find a hybrid solution the better choice. With a hybrid solution, some aspects of key print jobs are still managed by hardware on-premise, with other aspects managed via the cloud, deployed under a single management platform; this allows ease of use for administrators, as well as consolidation and cost savings.
- **Multi-tenant platform.** Single tenant-hosted solutions are more expensive than multi-tenanted ones, but provide better overall control and nominally better security capabilities. However, they can create availability risks due to manual maintenance and update processes. Multi-tenant solutions are generally highly configurable and also include solid security managed by the service provider. Multi-tenancy can also help to keep costs down due to costs being shared across multiple individual tenants.
- **VPN requirements.** Some cloud printing solutions are hosted on a cloud server, but still require a virtual private network (VPN) tunnel into the network, which limits accessibility. This can add overheads in terms of the performance of the connection, cost of the VPN, and costs of installation and management of the VPN client on desktops and mobiles. It can also create an unnecessary security weakness: if the VPN is compromised, it will affect the whole on-premise network.
- **Document security**. The print platform should allow either compression and encryption of print jobs, or local handling of at least some part of the job, rather than sending all the data and metadata around print jobs to the cloud to be spooled. Most cloud-based platforms can keep print jobs on the local network behind the firewall, maintaining higher levels of overall information security. Any data sent between the client and the cloud should be encrypted to prevent the stream from being captured via a man-in-the-middle attack.
- **Identity access management and multi-factor authentication.** Evaluate the capabilities for pull printing, which allows print jobs to be released only to authenticated users, regardless of location. Cloud printing can enable users to release print jobs from any networked printer or MFP. Consider a cloud printing platform that enables users to authenticate at any device using smart card release, other forms of near field communication/Bluetooth, biometrics, or PIN printing. Identity management is becoming a much stronger focus for many providers, with integration into existing identity access management (IAM) systems on offer.
- **Zero trust support.** The print environment can no longer be viewed as a separate environment to the rest of the IT platform. As the attack surface offered by intelligent devices both in the home and at the office increases, such devices are being targeted as a means of accessing an organisation's network. Buyers must ensure that any chosen system fits with their organisation's security posture and existing security tools – not just for now, but also for the future. Quocirca recommends ensuring that any chosen solution adheres to the zero trust model.
- **Native driver support.** While a universal print driver (UPD) can offer simplicity, buyers should consider solutions that offer native driver support that can use the full functionality of the MFP. Efficiencies and cost savings can be made when the driver supports the full functions of the MFP, such as double-sided printing, multi-page up, collation, and multi-drawer support for different paper qualities/types. However,

many UPDs are improving rapidly and offer good support for the most-used functionalities. Quocirca expects that such improvements will continue, and UPDs will be updated regularly, particularly on multi-tenanted cloud MPS platforms.

- **Reporting and analytics.** Traditional print management solutions offer extensive reporting on printer utilisation, device performance, consumables usage (toner, paper), and service information. In a serverless environment, this reporting may be limited. Quocirca is seeing this change, however, as cloud printing platforms mature and more data is drawn from print devices to be analysed and reported on. The increasing demand for home printers to be included as part of an organisation's overall IoT environment means print devices must be able to participate directly, but also remain affordable for organisations to offer to employees working from home or for on-premise home IoT 'hubs'. These hubs can act as a means of collecting and dealing with data needs such as edge devices. However, it may be possible to do this using PC-based software – it will be up to print OEMs and the channel to furnish such software as part of their offerings.

Supplier recommendations

Quocirca's research shows that cloud usage continues to increase. Although there are new players in the print market that are 100% cloud-based, a full shift toward a cloud-only model for those offering mature on-premise services is still not advisable: while it can play well for providers whose customer base is predominantly small and medium-sized organisations or 'born in the cloud' companies, not all organisations are moving to the cloud at the same speed. A mixed capability of an equally functional cloud and on-premise solutions will allow customers to move along the cloud journey at their own pace – with the channel's help. Building that equally functional cloud environment may take time, however: maintaining a more functional on-premise offering while this happens will help ensure that customers will stick with your company.

Alongside the technical issues around moving to an equally functional cloud service, many within the channel remain unprepared to move to cloud. The move from upfront capital and licensing fees, plus ongoing maintenance, to subscriptions, has not been easy, with some parts of the channel preferring to stick with what they know rather than make such a move. Others have struggled to define what type of cloud model best suits them, with some early movers deciding to go for a dedicated cloud, only to find that this means they incur heavy ongoing management costs that are difficult to pass on to the customer. These providers have found that dedicated clouds are more expensive and less flexible than multi-tenanted, public cloud environments, and many have had to move away from their dedicated platforms, incurring additional costs and effort.

Print manufacturers have a critical role to play in helping the channel overcome these challenges. Any supplier of cloud-based print services and solutions should consider the following:

- **Educate the customer.** The cloud is undoubtedly a major part of most organisations' strategies now. However, the print environment has been slower than other areas of the IT infrastructure in its move to the cloud. Nevertheless, recent Quocirca research shows that the speed of both the print channel and its customers in moving to the cloud for MPS services has accelerated strongly. To build on this momentum, customers still need educating on why a move to cloud-based MPS makes sense – arguments around availability, more manageable costs, and better updating of available functionality should be used as preliminary discussion points with any customer (or prospect) still wary of such a move. While many businesses may be familiar with the benefits of MPS, the market for cloud print services and solutions is broad and diverse. The growing acceptance of the cloud – be it IaaS, SaaS or PaaS – will enable providers to build propositions that can support existing cloud strategies.
- **Address the multi-cloud needs of businesses.** Although the ultimate goal around cloud usage may be a hybrid or single cloud model, the current reality for the majority of enterprises is a multi-cloud model. Those selling cloud-based print management solutions must recognise that each variant of the cloud offers its own advantages and obstacles to adoption. Any cloud print infrastructure proposition must address the varying needs of businesses as their cloud journey progresses.

© Quocirca 2022

- **Ensure security is adequately addressed.** Vague statements around security performance will no longer satisfy buyers, who are now more security-aware than ever, as a more decentralised work environment has focused on acute security concerns. Look to zero trust models to develop and message solutions across your portfolio.
- **Look to integrate with existing security platforms**. Identity access management (IAM) and security information and event management (SIEM) systems are widespread in the market and offer mature solutions. For this reason, Quocirca advises that those in the print market do not aim to provide their own solutions in this area. Instead, the channel should look to integrate into systems that are already strong in the enterprise environment, such as Okta and Ping Identity. At a minimum, multi-factor authentication (MFA) systems should be implemented, preferably using mobile device-based apps.
- **Continue the shift from a traditional to a consultative mind-set.** Providing guidance on how to leverage different types of cloud services and technology is critical. Moving from where a customer is currently to where they need to be in the future will require a lot more discussion and planning. The future of the channel is no longer a 'sell it and forget' model that depends on the customer to automatically renew maintenance annually, but one that works with the customer to uncover extra areas where more value add can be built in over time – and so extra revenue accrues to the provider. This requires a shift in mind-set from selling products to offering solution-based services, as well as the subscription model that comes with this.
- **Enhance trusted partner status to deliver differentiated value services.** Cloud print service providers have a significant opportunity to provide other value-added services and solutions to support a customer's digital transformation journey. Workplace services, particularly in the areas of collaboration, videoconferencing, managed desktops and workflow, can be low-hanging fruit in which good margins can be made. Other areas, such as managed security and other larger IT services, are also possible. Service providers can generate greater profitability by offering additional managed services that deepen customer engagement. Managed services can also increase the share of business that comes from recurring revenue, delivering healthier margins and revenue growth over time. Such services do not need to be home grown by the channel partner: the advantage of the cloud is that it allows cloud-based service providers to share and consume each other's functionality easily.

© Quocirca 2022

Vendor landscape – Cloud MPS vendors

Quocirca has created a vendor landscape for the cloud print services market that includes the major MPS providers offering cloud-based services. For inclusion, each vendor must have a mature managed print services (MPS) offering that it has extended to the cloud environment. Quocirca excluded vendors that did not have a mature cloud-based print services offering, as well as those only offering simple cloud print and capture software solutions. Independent software vendors (ISVs) have not been included in this vendor landscape.

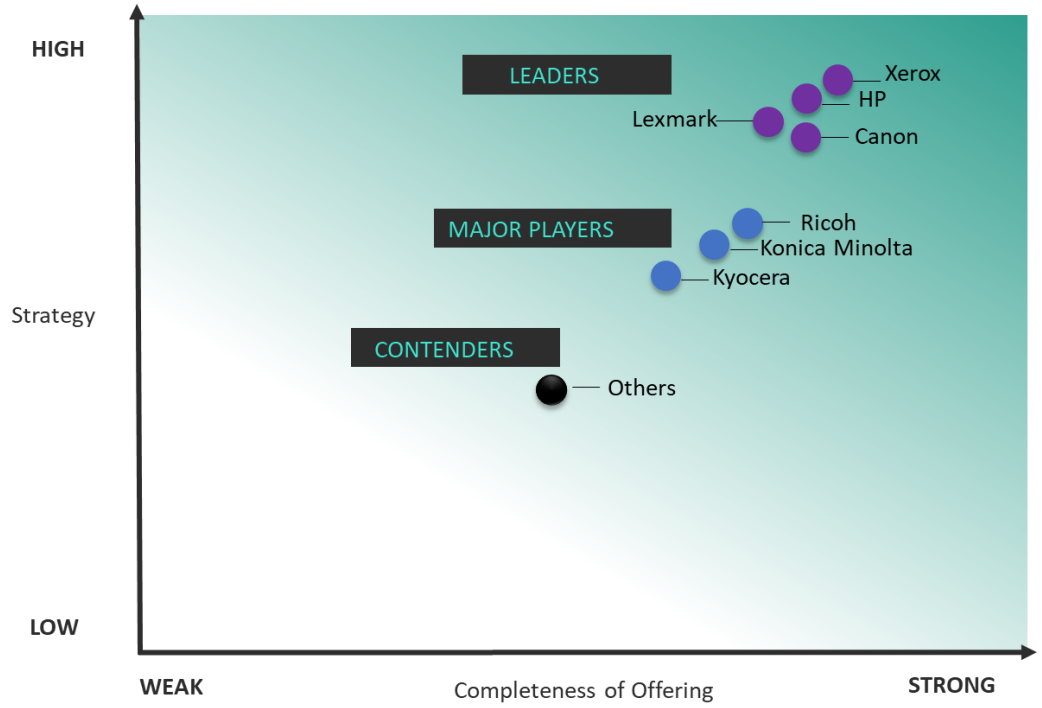
This evaluation of the cloud print services market is intended as a starting point only. Please note that Quocirca's scoring is based on an unweighted model, and prospective buyers should use this as guidance alongside the more detailed vendor profiles to assess suppliers based on their specific requirements. Quocirca has based this landscape on vendors' completeness of offerings and strategies across the following key areas:

- **Overall cloud strategy and vision** – the comprehensiveness of the vendor's MPS strategy, the quality of its overall value proposition and its future roadmap.
- **Maturity of offerings** – how long the vendor has been active in the market and how developed its offerings are.
- **Geographic reach** – A vendor's geographical reach, either via direct engagement or through partners or channels.
- **Breadth and depth of service offering** – provisioning, deployment and implementation of cloud-based print services, as well as support for hybrid cloud models.
- **Multivendor support** – support for a mixed-fleet environment.
- **Digital workflow automation** – adjacent cloud-based services to optimise print and digital workflow automation.
- **Cloud security and zero trust** – approach to zero trust and cloud security models.
- **Analytics and reporting** – the breadth and depth of capabilities to provide analytics and reporting.
- **Channel tools** – flexible cloud platforms to support channel partners.

Figure 10 represents Quocirca's view of the competitive landscape for printer and copier vendors that deliver enterprise MPS.

- **Market leaders** – vendors that lead the market in both strategic vision and depth of service offering. Leaders have made significant investments in their service portfolio and infrastructure, and are supported by strong delivery capabilities.
- **Major players** – vendors that have established and proven offerings supported by demonstrable customer success.
- **Contenders** – vendors with service offerings that are currently being aligned on a global or European basis. Contenders are typically investing in resources, infrastructure and partnerships to expand their market coverage.

© Quocirca 2022



This information is provided as a visual representation only and should be combined with other sources to determine the suitability of any vendor product or service.

Figure 10: Quocirca Cloud Print Services Landscape, 2022

Vendor Profile: Xerox

Quocirca opinion

Xerox has a broad range of cloud-based device management, print management and productivity tools, and solutions that can be delivered on-premise, in a private cloud, or via a Xerox-native cloud application. Its portfolio includes Xerox Device Manager, Xerox Device Agent, Workplace Cloud Fleet Management Solution, Fleet Management Portal, Xerox Services Portal, Support Assistant, and CareAR. Secure cloud print management solutions include Workplace Suite, Workplace Cloud, Virtual Print Management, Workplace Cloud Print Tracker, Digital Hub and Cloud Print, and third-party solutions. Cloud productivity solutions include Workflow Central, Apps, DocuShare, Capture and Content Services, and Campaigns on Demand. Xerox also provides cloud-enabled MPS advanced analytics.

Cloud-first development path

Xerox believes underlying cloud infrastructure is an essential enabler to future solutions for the increasingly distributed workforce. Rather than simply moving an on-premise server application to an Azure, AWS, or Google private cloud, Xerox is on a cloud-first development path. By architecting its solutions to be multi-tenant, native cloud applications, it provides customers with a true SaaS, 'IT touchless' solution. In addition to the multi-tenant cloud deployment option, Xerox can support clients' private cloud implementations.

Its cloud-first development path strategy allowed Xerox to pivot very quickly to support homeworkers early in the COVID-19 pandemic. Cloud-native applications are ideal for the distributed workforce because they have low to no footprint (no VPN), can be sold in a true SaaS commercial model – customers pay for only what they use, are scalable to enable organisations to grow and expand, are IT touchless – there are no software upgrades or security patches to manage, enable zero trust security, and deliver globally consistent reporting and analytics.

Cloud-native MPS

Xerox has long been on the path to enable agile, digital services for enterprise and SMB clients beyond traditional print management capabilities. It further expanded its offer in 2020 to support customers in designing and maintaining a high-performing workplace no matter the location of that workplace (corporate office, home/remote office, or a combination of both).

Xerox's cloud technologies support a changing workforce and digital transformation with flexible and scalable services that adapt to unexpected and future workforce requirements. Cloud device management optimises the IT infrastructure with low or no on-premise footprint and simplified IT staff effort. Cloud print management better supports mobile and home workers while also simplifying IT requirements. Cloud productivity solutions such as Workflow Central enable workers to tap into ConnectKey technology from anywhere, with any device.

Xerox MPS supports client zero trust initiatives by providing end-to-end security and connectivity in the cloud. The company is also looking to invest in tighter SIEM integrations and refine federated cloud service integrations such as Oauth2, SAML, OpenID. Additionally, it is researching options and integrations across continuous diagnostics and mitigation (CDM), extended detection and response (XDM), content disarm and reconstruction (CDR) and threat intelligence.

Analytics

Xerox has created a new dashboard for overall reporting. The MPS Advanced Analytics dashboard is a step-change in its analytics toolset strategy. It provides clients with self-serve, always-on insight into the global printer fleet, users/documents, and security via a single pane of glass. Architected on Microsoft BI, the web-based tool is organised into logical modules aligned with the functional interests of client user roles, such as IT operations manager, security director, sustainability manager and contract manager. By consolidating information into one cloud-hosted dashboard, Xerox is providing even greater insight and value to customers.

Cloud services and solutions portfolio

Xerox Smart Fleet Management

Xerox's device/supplies management service is built upon a single, global, cloud-native platform, enabling faster implementation that results in quicker benefits, such as cost reductions and increased productivity. This

automated, proactive management service automatically discovers networked printers (both Xerox and non-Xerox) and provides monitoring, management and security policy compliance services supported by a full range of reporting and analytics tools.

Smart Cloud Fleet Management
Cloud fleet management is enabled by a combination of Xerox Services Manager (XSM), which provides the globally hosted multi-tenant, cloud-based asset database at the hub of the Xerox MPS technology platform, and device management tools – Xerox Device Manager (XDM), Xerox Device Agent (XDA), Xerox Device Direct (XDD), and Xerox Workplace Cloud Fleet Management Solution (WCFM).

- **Xerox Services Manager** – XSM is an intelligent, global cloud incident management hub that supports the full chain of custody of an activity, from inception to closure. XSM provides a sole source of record for all device events (such as consumable requests and fault alerts) as captured by its device management tools or other event-logging systems, such as the Xerox Services Portal, Fleet Management Portal, and the Xerox Service Desk. XSM also manages device meter readings and can be easily connected to third-party help desks through Xerox's Help Desk Integration Connector Tool. XSM uses artificial intelligence to automate, predict and proactively provide device maintenance, and determine when new supplies are needed. Using standardised global methodologies, more than 80% of incidents are managed proactively.

- **Xerox Device Manager** – XDM can be installed on-premise or hosted in the customer's private cloud. It is predominantly used in enterprise environments, while XDA (a lighter version of XDM) and WCFM (hosted in a multi-tenant cloud) are often used in SMBs. XDD technology (included with Xerox devices) is particularly useful for remote locations, including home workers.

Xerox Workplace Cloud Print Tracker
Xerox Workplace Cloud Print Tracker extends print monitoring into the home office, helping organisations strengthen security and monitor print costs remotely. Jobs sent using a company laptop can be centrally tracked with cloud service analytics tools, which shows what is being printed in the home as well as the office.

Key features include:

- Easy set-up with exceptionally low IT overhead
- Reporting and analytics
- Cost recovery enablement for prints related to project codes or for simple reimbursement
- The ability to (remotely) define cost-saving default print settings

Xerox Workplace Cloud/Xerox Workplace Suite
Xerox Workplace Cloud delivers authentication, print management, cost control and mobility workflows. As a true cloud-architected platform, it is ideal for clients that want to reduce local network infrastructure or manage printers across multiple locations and networks. For clients with unique data control needs that prefer a more traditional solution delivery model, Xerox Workplace Suite can be privately hosted and features similar print management and mobility features to those of Workplace Cloud.

Xerox Workplace Cloud provides traditional print management capabilities, such as pull-printing, card and PIN release, accounting, printing from mobile devices, print rules and reporting, content monitoring, and security. Next-generation features include touchless workflows, analytics, network-sensing print path optimisation and location-independent print tracking. Workplace Cloud also integrates with Microsoft Universal Print to provide added functionality.

A Xerox Workplace Cloud account also enables IT teams to authorise, control and track business-related data printed on registered home printers. When working between home and the office, Workplace Cloud allows users to send jobs from home, and securely release them at the office at their next planned trip, or as the need arises. Alternatively, users can send jobs from home directly to an office printer, where office-based workers can

© Quocirca 2022

perform central batch tasks such as sending out content for postal delivery or important paper-based dispatches. A new delegate mode allows users to delegate central office workers to release secure jobs when they are needed. New content security features ensure policies are followed by monitoring and flagging documents with words or terms that are tagged as sensitive.

Virtual Print

Virtual Print adds new capabilities to the Xerox Workplace Cloud technology: including infrastructure cost assessment which enables customers to understand current print management infrastructure cost and create business cases for internal stakeholders; and premium post-sale support to relieve IT of the burden of print infrastructure management. Serviced by the Xerox Virtual Print Operations Center, customers have access to support expertise to ensure the availability of the Xerox cloud infrastructure, end-user support and ongoing day to day service management.

Xerox Workflow Central Platform

Xerox Workflow Central Platform is a SaaS cloud-hosted software platform, hosted within Microsoft Azure, which offers automation workflows for digital or physical documents. It enables customers to tap into Xerox ConnectKey technology from anywhere, with any device. For example, a user can translate a letter into their native language, or even turn it into an MP3 file to listen to; redact a customer report, removing a personal date, before sharing safely; or summarize a lengthy report for faster consumption of the key points. Hybrid workers can access the platform via mobile, PC, ConnectKey MFP, and any Xerox personal MFP from anywhere using the Xerox Print and Scan Experience PC application. Customers sign up to a company-wide subscription, with unlimited devices and users.

DocuShare Go

DocuShare Go is a SaaS cloud-hosted collaborative content services platform that supports business-centric processes by utilising the latest AI and machine learning technology. The platform helps customers with digital capture and conversion of paper content, storage and retrieval of digital files, and team sharing with real-time document collaboration. Hosted within AWS infrastructure, it adheres to the latest compliance standards while supporting encrypted data at rest and in motion to ensure full end-to-end security.

Xerox Digital Hub and Cloud Print Services (DH&CPS).

Xerox Digital Hub and Cloud Print Services is a multi-layered solution for organisations that require fast, cost-controlled printing services, including design, production, and delivery of print and digital collateral materials. An easy-to-use web storefront provides anytime access to customisable marketing materials, as well as real-time status and cost reporting for increased visibility and efficiency.

Xerox Digital Mailroom Service

Xerox Digital Mailroom Service automates the capture of all incoming mail and correspondence, whether delivered on paper, in an email, via fax or at the point of origination, and sends structured electronic information to business processes, systems (such as DocuShare) and remote workers.

© Quocirca 2022

About Quocirca

Quocirca is a global market insight and research firm specialising in analysing the convergence of print and digital technologies in the future workplace. Since 2006, Quocirca played an influential role in advising clients on major shifts in the market.

Our consulting and research are at the forefront of the rapidly evolving print services and solutions market, trusted by clients that are seeking new strategies to address disruptive technologies. Quocirca has pioneered research in many emerging market areas. More than 10 years ago we were the first to analyse the competitive global market landscape for managed print services (MPS), followed by the first global competitive review of the print security market.

More recently Quocirca reinforced its leading and unique approach in the market, publishing the first study looking at the smart, connected future of print in the digital workplace. The Global Print 2025 study provides unparalleled insight into the impact of digital disruption, from both an industry executive and end-user perspective.
For more information, visit www.quocirca.com.

Disclaimer:
Although Quocirca has taken every step it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data.

© Copyright 2022, Quocirca. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Quocirca. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.