The Print Security Landscape, 2022

Securing the remote and hybrid workforce

Report Excerpt: MyQ

January 2022

QUOCIRCA

Executive summary

Quocirca's Global Print Security Landscape 2022 report reveals that many organisations are struggling to keep up with print security demands in today's hybrid work environment. Home printing is creating new security concerns, exacerbated by shadow purchasing of devices. SMBs and mid-size organisations are finding it harder to keep up with print security challenges leading to a higher incidence of print-related data loss. This is leading to a lower confidence, particularly among SMBs, in the security of their print infrastructure. However, in Quocirca's Print Security Maturity Index, those organisations classed as leaders that have implemented a range of technology and policy measures are seeing lower levels of data loss and have higher confidence in the security of their print infrastructure. Print manufacturers and channel partners must strengthen their security propositions for organisations of all sizes to help customers mitigate risk in the new era of hybrid work.

The study is based on the views of 531 IT Decision Makers (ITDMs) in the US and Europe. 23% of the respondents were from SMBs (250 to 499 employees), 29% from mid-size organisations (500 to 999 employees) and 47% from large enterprises (1,000+ employees).

The following vendors participated in this study:

Manufacturers: Brother, Canon, Epson, HP, Kyocera, Konica Minolta, Lexmark, Ricoh, Xerox
ISVs: EveryonePrint, Kofax, MPS Monitor, MyQ, PaperCut, Ringdale

Key findings

- **Remote working is here to stay and is creating an expanded threat landscape.** Pre-pandemic approaches to securing the print environment focused around a primarily static, office-based workforce now need to move to supporting workers who spend some time in the office, and some in the home environment. On average, 44% of employees are expected to work remotely as offices fully reopen. Hybrid work creates significant security challenges for IT teams to manage as the exploitable attack surface increases. The proliferation of shadow IT and unsecured home networks means that organisations need to rethink their security posture around the print environment.
- **IT security remains the top investment priority over the next 12 months.** 53% of respondents say it is one of their highest three priorities. MPS (managed print services) are second in importance (41%) followed by managed IT services (38%) and cloud services (35%). 70% of organisations expect to increase their print security spend over the next 12 months, with only 11% expecting a decrease.
- **A reliance on printing creates a need for effective print security.** Despite rapid digitisation over the course of the pandemic, many organisations remain reliant on printing. Printing will remain critical or very important for 64% of organisations in the next 12 months. 44% anticipate that office print volumes will increase, and 41% that home print volumes will do likewise. Printers and networked MFPs pose a security risk not only in terms of printed documents being accessed by unauthorised users, but also as an ingress point to the network if left unprotected.
- **Just a quarter (26%) feel completely confident that their print infrastructure will be secure when offices fully reopen.** Organisations are struggling to keep up with print security demands: more than half (53%) say it has become considerably or somewhat harder to do so. 67% of respondents are concerned about the security risks of home printing, compared to 57% who are concerned about office print security.
- **Print security is lower on the security agenda than other elements of the IT infrastructure.** Top security risks are considered to be cloud or hybrid application platforms, email, public networks and traditional endpoints. Employee-owned home printers come in as the 5th top security risk (24%) ahead of the office print environment (21%). This suggests both a lack of awareness and complacency in not

fully appreciating the security vulnerabilities around printing, which remains an integral endpoint in the IT environment.

- **There are marked differences between MPS users and non-MPS users.** Organisations that use an MPS provider foresee much greater growth in print volumes and are most confident in the security of their print environment – despite having a higher awareness of the risks. They are also twice as likely to state that keeping up with print security challenges has become somewhat or a lot easier. The visibility and control provided by an MPS appears to ease the security burden for users, increase assurance that they can ramp up print volumes if needed, and reduce complacency, therefore lowering the likelihood of being blindsided by a security incident.

- **In the past 12 months, over two thirds (68%) of organisations have experienced data losses due to unsecure printing practices.** This has led to a mean cost per data breach of £631,915. Such quantified financial losses are bad enough for organisations to manage, but they also state many other negative impacts, such as a loss of business continuity and ongoing business disruption after the breach. Customer loss is reported to be the biggest impact for SMBs. Large organisations are less likely to have suffered a print-related data loss, with 36% reporting no breaches compared to 24% of SMBs. The public sector is the most affected vertical. Vulnerabilities around home printers were cited as the top reasons for data loss – such as home workers not disposing of confidential information securely, and interception of documents stored in the home printer environment.

- **Quocirca's Print Security Maturity Index reveals that only 18% of the organisations can be classed as Print Security Leaders**, meaning they have implemented six or more security measures. The number of leaders rises to 22% in the US and falls to 12% in France, which also has the highest number of laggards (37%). Print Security Leaders are likely to spend a higher amount on print security, experience fewer data losses, and report higher levels of confidence in the security of their print environment. When compared by vertical, finance has the largest percentage of leaders (23%).

- **Less than a third (28%) of ITDMs are very satisfied with their print supplier's security capabilities.** This drops to 20% in the public sector. US organisations are most satisfied, with those in Germany least happy. ITDMs who use an MPS have far higher satisfaction levels (42% are very satisfied) than those who don't (20%).

- **Most ITDMs turn to managed security service providers (MSSPs) for print security advice.** MSSPs are the primary source of security guidance for 35% of organisations overall, rising to 40% in the US. Just 18% of ITDMs overall would turn to an MPS provider for print security guidance, while 21% would consult a print manufacturer. This points to an opportunity for MPS providers and channel partners to collaborate more closely with MSSPs.

- **CIOs and CISOs differ in their views on the future of print, and their handling of security challenges relating to the hybrid print environment.** CISOs are more bullish, with 53% and 58% respectively expecting a rise in office and home print volumes, compared to 42% and 40% of CIOs. Notably, CIOs (32%) and CISOs (33%) show the most concern around home printing compared to other IT respondents, ranking it as their second top security risk. CIOs also seem to be finding it harder than CISOs to keep up with print security challenges – 61% stated that they were finding it considerably or somewhat harder, compared to only 44% of CISOs, where 29% also stated that they were finding it somewhat or a lot easier.

Buyer recommendations

Print devices continue to become more sophisticated, with greater intelligence being built into even low-end consumer printers. Such intelligence can be used by those with malicious intent to access a print environment, and if that then provides direct access back into the corporate environment, chaos could ensue. Organisations must therefore pay far closer attention to protecting the print environment, particularly when looking to the continuation of hybrid working.

Organisations need to look at investing in the following areas to ensure that the print environment is secured to the same levels expected across any other area of the IT platform.

- **Conduct in-depth print security and risk assessments.** Most organisations have these in place for the overall IT environment, but the print platform often seems to be left out. Given the increasing threat landscape associated with hybrid work, organisations must ensure that the print infrastructure is fit for purpose across device, document and network security. This can be carried out internally, or by third parties such as managed security service providers (MSSPs) or managed print service (MPS) providers. New assessments must fit in with the broader IT security and risk assessments.
- **Implement a zero trust architecture.** Zero trust operates on the basis of 'never trust, always verify', assuming that an environment will be compromised and no device should ever be fully trusted. Organisations have started to implement zero trust environments, but mainly within the constraints of their owned and managed IT environment. This now needs to be extended to the wider hybrid environment, embracing home workers and all the devices that are being used for work purposes across that environment – including print devices.
- **Provide defined and authorised printers for home workers.** Individuals still require access to printed output when working from home. However, basic consumer printers do not come with the capabilities they may require, such as print speed and quality, and will not generally adhere to the needs of the organisation – such as security and manageability. Organisations should move to defining classes of printer that individuals can use, depending on need. These should then be supplied and provisioned by the organisation, along with the means of managing and controlling what business content the individual prints on the device.
- **Revise BYOD policies to include employee printers.** For many organisations, supplying and provisioning printers to all employees working from home may not be practical. Existing bring-your-own-device (BYOD) policies must now be updated to cover the home environment – moving to a BYOO (bring your own office) approach, with policies covering desktop/laptop PCs, tablets, mobile devices, desk phones and print devices. An effective BYOD/BYOO policy will help ensure that each individual's environment adheres to an organisation's basic security needs.
- **Evaluate content security solutions.** Content management systems based around document metadata, where documents are classified based on their sensitivity – along the lines of 'Public', 'Commercially sensitive', and 'Internal use only' for example – allow specific policies to be set, such as '*this document cannot be printed*' or *'this document can only be printed on an approved printer*'. This enables home-based employees to use their own printers for routine jobs without the risk of restricted documents ending up in their wastebins.
- **Implement pull printing.** Requiring a PIN or a Bluetooth or NFC token to release a job at a printer means that the print job owner has to be present before the job is printed out. Pull printing is most useful in shared access environments, as is the case for many office printers. However, it could also be applied to allow home users to submit print jobs securely via the cloud to office printers, or even their own printer – enabling them to be tracked at a central level. Jobs that the owner forgets about are held, and can be securely deleted if not printed out after a defined period of time.
- **Continuously monitor through reporting and analytics.** Risk assessments, tuning content security and configuring SIEM (security information and event management) systems all require insight provided by gathering reports from across an organisation's network, including its extension into employees'

homes. SIEM systems themselves can often provide this information, as can other log management tools.

- **Formalise processes to respond to print security incidents.** Accept that leaks are likely to happen – and plan how to deal with the repercussions. Most of the respondents to Quocirca's research had at least some security measures in place, and a reasonable belief that their print environment was secure, but 68% still experienced at least one print-related data loss in the past 18 months. Organisations must put appropriate processes in place to respond to data breaches by dealing with the possible legal and reputational damage caused, while building back business capabilities in the shortest possible time.
- **Use cloud routing for certain print jobs.** While a lot of printing is informal and needs to be near to the user to be effective – for example, printing a report in order to review it – other print jobs are part of larger business processes, and the user who submits the job may never see the output. For example, letters to be mailed to customers, marketing output, and forms that make up part of a broader process may be better printed at a more suitable printer. Employees can securely submit such jobs from home to a cloud print service, which can check the veracity of the submission, and seek secondary authorisation before allocating the job to the most suitable print resources available. Even within the office environment, such routing can help in minimising print wastage by making sure that certain print jobs go to the most suitable printer.

Please note that this is a report excerpt. The full report is available at https://quocirca.com/print-security-2022/

Vendor Profile: MyQ

Quocirca opinion

MyQ has made strong inroads in the print management market, continuing to enhance its security features. MyQ's print management solutions are designed to secure corporate documents in digital and physical form during capture, processing, distribution, printing or copying.

MyQ has developed both its MyQ X and MyQ Roger platforms to meet the requirements of customers' zero trust architectures especially in the areas of user identity, user and device authentication, authorisation policies and ensuring secure work and communication between personal and IoT devices and cloud services.

In the past twelve months, in addition to launching the MyQ Roger multi-tenant, fully-fledged public cloud platform, the developer has also introduced several new mobile applications, continued to enhance its mature MyQ X solution and significantly increase its focus on penetration and security testing, which is conducted by independent external labs and security experts.

Key security highlights

MyQ X
MyQ solutions manage print, scan, capture and document management workflows, but differ in their ability to operate in a cloud environment. MyQ X is optimised for high availability virtual servers as well as a private cloud infrastructure, and also supports Universal Print by Microsoft. It can be installed on-premise, in-house, or in a private cloud environment equipped with a Microsoft operating system. Built as a public cloud SaaS product, MyQ Roger has a multi-tenant architecture, with a secure and isolated dataspace for each customer.

Total print management solution
The MyQ X on-premise server solution has evolved from a platform originally designed to reduce print costs with features such as monitoring, accounting, rules, user rights and restrictions, advanced reports and payment gateways; to become a total management solution covering print (including mobile print), scan and capture, OCR and fleet management. MyQ X comes with high-end security features, personalisation options for maximum efficiency and accurate cost reporting.

The MyQ X server product has undergone a major overhaul of all integrated applications in supported printers to significantly speed up and refine the monitoring and accounting system. Next year will see a major change to the server architecture to enable parallel running and load distribution across multiple servers, as well as a completely redesigned central management, set up and monitoring system. In addition, individual components will be optimised for operation in a cloud environment.

Mobile first with MyQ Roger
Launched as a result of changing business needs due to the pandemic, the new MyQ Roger digital workplace assistant was designed to empower users to self-serve in terms of printing and defining scanning workflows, and help them work more efficiently. A key differentiator is its mobile-first concept, meaning users can easily customise and personalise smart scanning workflows on every compatible printer using their smartphones, or perform pull-printing from their cloud or local storage.

MyQ Roger is designed to eliminate any unnecessary traffic to the cloud and back, to reduce negative impact on local internet connection, and to be highly cost-efficient when it needs to consume cloud computing resources. Print jobs can be stored on any capable print devices, documents can be pull-printed on any printer connected to the local network, can be stored in personal cloud storage repositories such as OneDrive or Google Drive, on desktop PCs or the Universal Print spooler if it is used for printing.

Future plans for MyQ Roger include the addition of monitoring and accounting functionality, online payments using print devices, and integration with a range of third-party systems.

Security features overview

Key features include:

- **Mobile-first concept.** All settings and customisation can be done via a smartphone, which also supports Face ID or biometric user authentication.
- **Direct cloud storage integration.** Integration with OneDrive or Google Drive cloud storage ensures secure handling of user documents. Documents are securely downloaded directly to the printer or stored directly in the user's cloud storage without any intermediate layers.
- **BYOD with zero trust.** MyQ mobile apps, cloud services and integrated apps on print devices communicate with each other over secured channels based on latest TLS & certificates standards. No requirement for special Wi-Fi networks or VPN tunnels.
- **Touchless remote control.** MyQ can control printing, scanning, and copying functions completely remotely via a mobile phone, without having to touch the printer's LCD panel.
- **Voice assistant integration.** Printing, scanning, and copying functions can be controlled by the human voice.
- **Dynamic QR login.** User authentication can be conducted via dynamically changing QR codes which prevent copying/misuse of codes. TLS 1.2 and all relevant certificates are verified for each user session using SSL Labs, where MyQ Roger's overall rating is A+ (equivalent to internet banking security).
- **Universal Print integration.** MyQ securely downloads documents directly to the printer only when the user wishes to print it.
- **Pull-printing based on a local printer mesh.** When printing on a local network, MyQ can temporarily store a print document on any printer. In addition, all printers can pass a document to each other for printing as soon as a user logs on to any device.
- **Encryption.** Documents are stored on the printer in encrypted form. The encryption key is distributed by secured channels and is different for each tenant (customer). MyQ meets the latest security and encryption standards for secure communication on a public network or to access personal cloud storage.
- **Scanning on the go**. Documents can be safely captured on the go without a printer. By pressing the same button as on the printer, documents can be scanned using the smartphone camera and MyQ will then perform the same scenario with the document as if it were using a multifunction device.
- **Secure storage.** Content of scans or **copies** is securely stored in a central digital archive of copied and scanned documents.
- **Watermarks, digital signatures, timestamps**. Provides audit trail of when and by whom physical and digital documents are printed or acquired.
- **User authentication.** When a user is authorised with the Roger server, it issues a unique Access token – a series of bytes that is impossible to breach. During the life of the token users can access MyQ Roger functions without having to re-enter credentials each time they perform another action. Tokens also offer a second layer of security to the connection. MyQ Roger also supports Refresh tokens, which have a longer life span than Access tokens.
- **Data access and retention.** When connecting the MyQ Roger application to the user's OneDrive for Business, the user grants MyQ Roger the right to browse and save to print or scan folders. Printed or scanned documents are not transferred through the MyQ Roger server, document data exchange happens only between the user's connected cloud service and the MFP. All data retention is subject to governing laws and regulations (e.g. GDPR).

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 has played an influential role in advising clients on major shifts in the market. Our consulting and research is at the forefront of the rapidly evolving print services and solutions market, trusted by clients who 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:
This report has been written independently by Quocirca. During the preparation of this report, Quocirca has spoken to a number of suppliers involved in the areas covered. We are grateful for their time and insights.

Quocirca has obtained information from multiple sources in putting together this analysis. These sources include, but are not limited to, the vendors themselves. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in any information supplied.

Although Quocirca has taken what steps 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.

All brand and product names are trademarks or service marks of their respective holders.