

*Work Like Tomorrow.™*

## Meeting Data Security and Compliance Requirements Using a Smart Cloud Print Infrastructure



printix  
a **KOFAX** company

**KOFAX**



# Contents

Executive Summary.....	3
<b>Part One: Cloud Print Management Within a Zero Trust Framework.....</b>	<b>5</b>
What is Zero Trust?.....	6
Zero Trust and the Cloud Print Management Space.....	6
Hybrid Working and Print Management .....	7
The Cyber Threat Landscape - What Cloud Print Management Is Up Against .....	7
Plugging the Trust Gap in Printing.....	10
Costs of Cybersecurity and Data Exposure.....	10
The Era of the Zero Trust Printer .....	11
Trends in Printing - Using Smart Cloud Management Platforms for Printing.....	12
<b>Part Two: Secure Cloud Print Management Services to Meet the Compliance and Security Challenge.....</b>	<b>14</b>
Cybersecurity and Cloud Threats of Cloud-Based Print Platforms .....	15
Crossing the Hurdle of Compliance and Print – GDPR, and Other Data Protection Regulations.....	16
What Is the GDPR and Other Privacy Regulations? .....	17
HIPAA for Health Data Protection .....	18
Zero Trust Privacy and Printers.....	18
Five Steps to a Compliant Print Environment.....	19
Creating a Secure Print Environment – Meeting the Compliance Challenge.....	20
Examples of Requirements for a Secure Cloud-Based Print Management Platform.....	21
About Printix .....	23



## Executive Summary

Recent years have resulted in challenges to business operations and working conditions. The Covid-19 pandemic cemented the home working movement, adding new layers of security requirements above and beyond network and cloud security. The enterprise print environment, already part of cloud-first digital transformation projects, became a stalwart of home working. The hybrid office-home work environment persists, with the cloud facilitating this shift.

A report from Deloitte shows that cloud and home/hybrid working are changing the face of the office.

 **87% of IT decision-makers identified the pandemic as a key driver of increased cloud uptake and expect a decline in on-premises workloads by 2025.<sup>1</sup>**

<sup>1</sup><https://www2.deloitte.com/us/en/insights/topics/digital-transformation/cloud-infrastructure-strategy.html>

Cloud-based print management has data at its core, and like all digital data-rich systems, cloud printing must deal with cyber-attacks that target data. In addition, the hybrid work environment has added to the security challenges.<sup>2</sup> Since the pandemic, zero trust has entered the business lexicon as a guiding principle in controlling access to data. In the world of printing, access is key to robust security.



As well as security principles and guidelines, the laws and regulations guide and enforce organizations in security and privacy best practices. These regulations are essential to meet customer and government expectations. Many of these regulations have been or are in the process of being updated. These updates reflect the expanding threat matrix introduced by Internet-enabled devices and hybrid working. Regulations such as the EU's NIS2 and HIPAA have data protection at their heart, and systems that utilize cloud computing technology must be incorporated into our overall drive to compliance.

This paper looks at the types of threats targeting a cloud-based print infrastructure and what preventative actions mitigate those threats. The paper also looks at how Cloud-based printing fits in with the expectations of data protection under the GDPR and other compliance measures such as HIPAA.

<sup>2</sup>[http://www.virtualstarmedia.com/downloads/Forrester\\_zero\\_trust\\_DNA.pdf](http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf)

# PART ONE

## CLOUD PRINT MANAGEMENT WITHIN A ZERO TRUST FRAMEWORK

### ZERO TRUST CONSIDERATIONS OF PRINTING



**Three-Quarters  
(74%)**

of enterprises expect cloud print vendors to support zero trust



**> One-Quarter  
(27%)**

of employees work entirely remotely



**One Third  
(32%)**

are hybrid workers

The word 'data' has entered the collective dictionary of our era. Data is everywhere and exists in many states, from digital to physical. What each state has in common is that it has a lifecycle and may also transform from one form of data to another. This happens with a modern, intelligent, Cloud-based print management platform - it takes digital data, processes it, and transforms the digital data into a physical form. In doing so, Cloud-based print management platforms transform our business by allowing us to print from any device connected to the cloud. Best of breed Software-as-a-Service (SaaS) solutions that provide Cloud-based print management platforms can be private, public, or hybrid. These modern print platforms have revolutionized how an enterprise manages printing to the point where it is fully optimized and highly cost-effective. However, as with all data services, Cloud-based print management fits squarely in a zero trust security model.



## What is Zero Trust?

Zero trust pivots upon data. At the core of zero trust is that any access point must be under continuous authentication to ensure that the person or device attempting access is authorized. A zero trust architecture covers people, devices, networks, and workloads. For example, cloud print management and physical printers are part of a zero trust architecture.



## Zero Trust and the Cloud Print Management Space

Today, cloud print management solutions are integral to the broader zero trust infrastructure. The principles underpinning the zero trust print approach can help to secure the wider cloud printer framework within an expanded threat surface. IT decision makers hold this view: Quocirca's "Managed Print Services Market Landscape Report, 2022" found that almost three-quarters (74%) of enterprises expect cloud print vendors to support zero trust.<sup>3</sup>


<sup>3</sup> <https://print2025.com/reports/quocirca-mps-2022-market-landscape/>



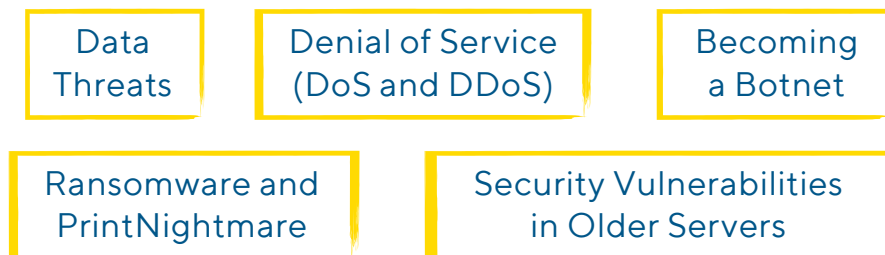
Three-quarters (74%) of enterprises expect cloud print vendors to support zero trust.<sup>3</sup>

## Hybrid Working and Print Management

Quocirca researchers found that over one-quarter (27%) of employees work entirely remotely, and almost one-third (32%) are hybrid workers. In addition, the pandemic shifted worker expectations on where and how they managed their work life. Gartner has described this situation as the "everywhere enterprise."<sup>4</sup> In terms of printing, remote workers, home workers, and satellite offices have meant that cloud print management has become a standard way to manage printer use.

 Quocirca researchers found that over one-quarter (27%) of employees work entirely remotely, and almost one-third (32%) are hybrid workers.<sup>4</sup>

## The Cyber Threat Landscape - What Cloud Print Management Is Up Against



The last few years have seen unprecedented and sophisticated cyber security attacks. The attacks span several areas, from DDoS to ransomware and data exposure. As a result, any Cloud-based system is at risk, across the spectrum, of threats and cyber security vectors. For example, a cloud-based print management service is essentially a web application that manages data and can be at risk of attacks such as those threatening the service execution itself and attacks which target the lifeblood of the service - data.

<sup>4</sup><https://blogs.gartner.com/bob-gill/2020/06/09/emergence-of-the-everywhere-enterprise/>

The Quocirca research mentioned above shows the impact of poor printer security on an organization:



**68% of organizations have experienced data losses due to unsecured printing practices, and the average cost of a print-related data breach is 755K (euros).**

To mount an effective response to the cyber security threats impacting enterprises of all types and sizes, we must have a complete understanding of the nature of these threats.

### **Data Threats**

In 2021, almost 22 billion breached data records were exposed, stolen, or breached.<sup>5</sup> Data is a commodity, and cybercriminals target all data types, from personal data to company intellectual property. Intellectual property theft, including trade secrets and copyrighted material, is a major global issue. The “IP Commission Report,” a survey commissioned by the U.S. government, found that although trade secret theft is hard to access, it is likely to comprise between 1 and 3% of the GDP of a country.<sup>6</sup>

Cloud-based print management is open to data-targeted attacks across the entire lifecycle of the print job. This includes the key areas:

- **On disk** - During the print job’s processing, the data is available on the printer’s hard disk and, therefore, vulnerable to exposure.
- **Across the network** - Any unencrypted data communication is liable to exposure.
- **Hard-copy** - Once printed, the hard-copy data is vulnerable if left unattended.
- **Unauthorized access** - Stolen or misused credentials can allow print jobs to be re-routed, changed, or intercepted.

<sup>5</sup><https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end>  
<sup>6</sup>[http://www.ipcommission.org/report/IP\\_Commission\\_Report\\_Update\\_2017.pdf](http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf)



## Denial of Service (DoS and DDoS)

Web applications are a perfect target for hackers. Printers are part of a growing focus by cybercriminals on Internet-enabled IoT devices incorporating vulnerable devices into a 'DDoS Swarm.' The swarm is infected with malware bots that are then used to cause a DDoS attack. Cybercriminals are using the search engine 'Shodan', to find accessible TCP ports, often used for raw TCP/IP printing jobs. Printjack is an example of a cyber-attack that uses Shodan and infects printers with malware. Printjack attacks can also be used to steal information during print job transfers across unsecured networks.<sup>7</sup>

## Becoming a Botnet

Carrying on from the DDoS attack example, another area of concern is the botnet army. A bot is a device that has been infected with a specific type of malware. It then becomes part of a larger network of bots - a botnet. This network is used to perform DDoS attacks against other online services. Internet-enabled printers have already been unwitting victims of this type of attack; in one case, 150,000 consumer printers were used to create a botnet - the hacker claiming that they were demonstrating how easy it was to do so.<sup>8</sup> These were general consumer Internet-enabled printers. This type of threat means there is a distinct possibility that your organization could become an unwilling pawn in a cyber-criminal attack on another organization.

## Ransomware and PrintNightmare

Ransomware is the number one scourge of enterprise the world over; in 2021, 71% of companies were infected by ransomware.<sup>9</sup> Ransomware is typically associated with data being maliciously encrypted; however, printers are now being co-opted into the fraudster's armory. For example, in 2021, Egregor Ransomware hijacked printers and churned out ransomware notes.

One of the most shocking printer-related security issues is the PrintNightmare spooler vulnerability. The software flaw in the Windows Print Spooler service affects windows 7+. The flaw was originally identified by the US Cybersecurity & Infrastructure Security Agency (CISA).<sup>10</sup> The vulnerability allows a hacker to execute malicious code on a vulnerable system, modify data, and even create new privileged admin accounts.

## Security Vulnerabilities in Older Servers

PrintNightmare is an example of a vulnerability that has been patched. However, some older server operating systems and associated software are no longer supported with security patches. This creates a dangerous situation whereby a hacker can compromise a server. Printix offers a Cloud Print Management Service, which removes the need for print servers and so manages this security gap.

<sup>7</sup><https://www.bleepingcomputer.com/news/security/researchers-warn-of-severe-risks-from-printjack-printer-attacks/>

<sup>8</sup><https://www.cybersecurity-insiders.com/cyber-attack-launched-on-150000-printers-working-worldwide/>

<sup>9</sup><https://cyber-edge.com/cdr/>

<sup>10</sup><https://www.kb.cert.org/vuls/id/383432>

## **Plugging the Trust Gap in Printing**

A best practice in printing is to focus on core weaknesses in access control and trust. Many print-focused cyber-attacks mentioned above begin with compromised credentials and unauthorized access. These weak points are used alongside any flaw in the software and hardware of a cloud print environment. Robust access control methods can help to alleviate many insecurities in cloud printing. Secure printing that encompasses hybrid working and cloud-hosted apps and infrastructures must be considered an ecosystem. Layers of security, based on zero trust principles, are used to build a trusted print infrastructure. These security layers include:

- Zero trust approach to access control
- Strong user authentication at all access points
- End-to-end encryption during print events
- Print rules that verify users when they access printers
- Segmentation applied to printers, facilitated through a smart cloud-based print management model

## **Costs of Cybersecurity and Data Exposure**

The cost of data exposure or service disruption can be profound. It can mean financial losses, the cost of remediation of disruption, non-compliance fines, and lost reputation. The Ponemon Institute and IBM performs annual reviews of data breaches' costs. Their 2022 survey found that the average cost per organization per data breach per data breach had increased by 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022.

Interestingly, the report also found that zero trust pays: organizations that don't deploy zero trust pay an extra \$1 million in breach costs compared to those using a zero trust model.<sup>11</sup>

 **The average cost per organization per data breach per data breach had increased by 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022.**

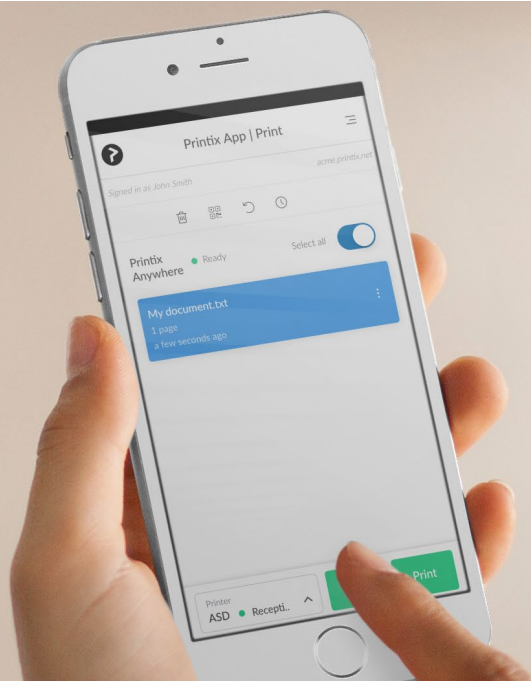
<sup>11</sup><https://www.ibm.com/uk-en/security/data-breach>

## The Era of the Zero Trust Printer

The era of zero trust print management will remove the vulnerabilities inherent in complex work environments. An SaaS platform handling cloud-based print management offers your organization a highly efficient way to manage and utilize print services across your organization. However, you must apply smart methods to manage the security of the service. Printing must not be left out of the security puzzle: the era of the zero trust printer brings a robust way to mitigate cyber-attacks. Printers are an enterprise architecture endpoint. With 68% of enterprises experiencing a cyber-attack from a compromised endpoint, adding zero trust into the print infrastructure helps alleviate these attacks.<sup>12</sup>

The cybercrime landscape is one of the biggest challenges of an enterprise, no matter what size or sector: it is one of the defining features of our modern age. This is within a business world that takes advantage of some of the most exciting, innovative, and enabling technologies. Technologies such as IoT, Cloud services, and intelligent computing are built around data and the optimized use of it. Technologies like innovative cloud-based print management give our business an edge over the competition, allowing our organization to be agile and responsive. But they come at a cost - cybercrime. In response, the world of regulations and compliance is hardening its stance.

<sup>12</sup><https://engage.morphisec.com/2020-endpoint-security-risk-study>



# Trends in Printing - Using Smart Cloud Management Platforms for Printing



## Growth Trends

Cloud-managed services are used by companies of all sizes: the market for cloud print management is expected to show a growth rate of almost 19%, with a predicted market value of USD 5.04 billion by 2029.<sup>13</sup>

This explosion of growth in cloud-managed services is down to, amongst other things:

- The efficiency of service
- The reach of services across an often remotely distributed workforce
- Cost benefit

## Strong Relationship Between Printers and Data

Printing is an oft-misunderstood area of business but must be considered part of a company's critical infrastructure, albeit less evident than energy or finance. However, the output can be super-critical for any business with a printing dependency. The Quocirca survey that identified 68% of enterprises suffered insecure printer-related data breaches highlights the strong relationship between printers and data.

<sup>13</sup><https://www.adroitmarketresearch.com/industry-reports/print-management-software-market>

## **Simplify to Secure**

Managing enterprise printing services using a secure Cloud-based platform can offer enterprises of all sizes a way to simplify their print infrastructure. This is becoming more important as organizations become increasingly complex. In addition, more simplicity in services means more simplicity in managing cybercrime.

## **Digital Transformation and the Printer**

Technology changes and the increase in uptake of cloud-based infrastructures are driving digital transformation. Other drivers of this transformation of the enterprise include:

- Remote and home working
- Workers using shared office space
- Bring Your Own Device (BYOD) becoming more prevalent since the pandemic
- Complicated administration of a diverse IT infrastructure across hardware, software, and operating systems
- Vendor-specific printing requirements within a complex IT infrastructure

## **The Zero Trust Printer**

The zero trust principles of ‘always verify, never trust’ fit perfectly with the printer. Printers are endpoints, and control over access to and privileges in the use of the printer must follow a zero trust model.

The application of a cloud-based print management platform simplifies and streamlines this matrix of complex needs. This is why more companies are turning to smart cloud-based print management solutions like Printix.

Printix is secure-by-design, enforcing access control and establishing user privileges using a zero trust model.

According to Flexera’s “State of the Cloud 2022” report, 80% of enterprises use a hybrid cloud.<sup>14</sup> Cloud computing platforms like Microsoft Azure allow businesses to become more efficient, and printing may be a business process that can be most simplified using the Cloud.

<sup>14</sup><https://www.flexera.com/blog/cloud/cloud-computing-trends-2022-state-of-the-cloud-report/>

## PART TWO

# SECURE CLOUD PRINT MANAGEMENT SERVICES TO MEET THE COMPLIANCE AND SECURITY CHALLENGE

Previously, we set out the type of security environment affecting an enterprise. The hostile cyber security must be dealt with from a position of knowledge. This intelligence is used to plan mitigation measures to minimize the impact of an attack. In other words, having a thorough understanding of the threat landscape offers a way to redress the balance against attacks.

Placing cloud print management within the controls of a zero trust model builds the layers of protection needed to prevent modern cyber-attacks.

This zero trust model helps in compliance with data protection regulations. Many regulation frameworks have been updated recently or are being updated to accommodate changes in this threat landscape. For example, the EU's NIS regulation is about to be updated to NIS2.<sup>15</sup> This will impact printer manufacturers. Consumers of print services are also affected by regulations, including GDPR in the EU and HIPAA in the USA.

Fortunately, much work has been done in cyber security threat mitigation. This work extends to secure cloud-based print management platforms, and below we have identified several critical areas of concern and their associated solutions.

<sup>15</sup>[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS\\_BRI\(2021\)689333\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)





## Cybersecurity and Cloud Threats of Cloud-Based Print Platforms

The table below guides best practices when using a Cloud-based print management platform.

Issue/Area of Concern	Solution
<p>Man in the Middle attack (MitM) - Cloud-based systems are open to interception of data communications</p>	<p>Use SSL/TLS (HTTPS) encryption to secure communication of data across Internet connections.</p> <p>Option to isolate the data communications by keeping sensitive data within an organization's own network.</p> <p>The Printix solution allows print data to be stored locally, thus avoiding MitM attacks.</p>
<p>Data exposure via Cloud application attacks such as Cloud database exfiltration</p>	<p>SaaS solutions should ensure print data stays local, if required. Data should automatically reside in the Cloud only when it is needed to manage the print infrastructure.</p> <p>This will also reduce the impact of a Cloud-based malware infection that can then exfiltrate data.</p> <p>A Cloud-based print management platform should allow for local storage by design. Whereby, print data only leaves the customer network if specifically required to do so. In which case, robust encryption measures must be in place.</p>
<p>Access control to data and print jobs</p>	<p>Zero trust principles should be followed and users, devices, and workloads, verified continually.</p> <p>Role-based access controls should be in place to control who does what in terms of printing. Passwords should always be secured using salted password hashing techniques.</p> <p>Options to use existing login credentials, for example via Active Directory, Office 365, etc., will allow credential management to be offset to that service and come under the policy control of the service.</p>

<sup>16</sup><https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

Issue/Area of Concern	Solution
Open ports	<p>Some ports need to be open to communicate. However, a Cloud-based platform should not require any open inbound ports in the firewall.</p> <p>Any port traffic should be encrypted.</p> <p>Segmentation should be used wherever possible.</p>
Unencrypted data and loss	<p>Make sure that data is encrypted (using a robust algorithm such as AES 256) throughout the touch points of the lifecycle of the print. This includes both hard-disk and across the network.</p>
Inadvertent theft from printers	<p>As well as having the ability to encrypt data across the system, having a granular level of control can add an extra dimension of security. For example, allowing the user to release a print job when they are ready to receive it can reduce the likelihood of interception and inadvertently leaving documents on a printer.</p>
System behavior	<p>Creation of audit logs on system and user behavior is important for both compliance reasons, and for intelligence to spot security issues. Audit logs should be able to identify who printed what, when, and where.</p>

## **Crossing the Hurdle of Compliance and Print – GDPR, and Other Data Protection Regulations**

The expanding and increasingly sophisticated cybersecurity threat landscape has resulted in upgrading compliance and regulatory frameworks worldwide. Data privacy and security mandates, such as the General Data Protection Regulation (GDPR), set out stringent rules on the processing of data. Other such as the Health Insurance Portability and Accountability Act (HIPAA), have specific regulatory requirements around protecting health data. Non-compliance fines can be rigid, with non-compliance with the GDPR, for example, resulting in massive fines of up to 4% of global revenue or 20 million euros, whichever is greater.





66% of home workers had printed confidential work documents on their personal printer.



## What Is the GDPR and Other Privacy Regulations?

Data privacy regulations have become normalized across large parts of the world. The most infamous is the GDPR. Another is the California Consumer Privacy Act (CCPA). 71% of countries have data protection and privacy legislation in place.<sup>16</sup> Privacy revolves around data, specifically personal or consumer data. However, the definition of these forms of data varies widely. For example, Article 4 of the GDPR defines several terms, including personal data:

“any information relating to an identified or identifiable natural person”

The article goes on to describe the processing of this data as follows:

“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;<sup>17</sup>”

Print environments are data-driven. Often this data meets the remit of the personal information described by the regulation. This can be anything that identifies an individual, including employees, customers, clients, and partner company employees. If the data has the potential to be exposed, either maliciously or accidentally, it has to be shown to be protected.

A recent survey found that in the UK, 66% of home workers had printed confidential work documents on their personal printer and may be in non-compliance with local data protection laws.<sup>18</sup>

<sup>17</sup><https://gdpr-info.eu/art-4-gdpr/>

<sup>18</sup><https://goshreduk.tumblr.com/post/641368333191675904/working-from-home-the-hidden-risks-of-printing>

## HIPAA for Health Data Protection

The HIPAA legislation came into force in 1996 to add safeguards, including data privacy and security, to electronic health data. The sections of HIPAA that are of particular interest to organizations processing health data are the 'Security Rule' and the 'Privacy Rule':

### **Privacy Rule**

This rule came into force on April 14, 2003. It covers national standards to ensure that patient data is under the control of the patient.

### **Security Rule**

This rule came into force on April 20, 2005. It covers national standards on how to store and transmit patient data covering methods to establish the confidentiality, integrity, and availability of electronic health data.

HIPAA requires that printers, as endpoints, must be protected. However, since many hospitals will have hundreds of printers, security management can become complex.

## Zero Trust Privacy and Printers

A print environment needs as much attention as other parts of an organization's IT infrastructure when looking at GDPR, HIPAA, and other data security compliance.

Because many companies work across jurisdictions, meeting a complex web of data protection and privacy regulations could become a nightmare. A good strategy is ensuring that your printer endpoints and the print cloud management system are aligned with a robust security strategy that uses zero trust principles.





## Five Steps to a Compliant Print Environment

The following steps can help in an understanding of how cloud-based printing platforms can adhere to data protection and privacy regulations:

### **Step 1: Identify Where Printing Fits**

Include the print environment in an overall regulation strategy plan. A data mapping exercise should include the entire print infrastructure - see step 2.

### **Step 2: Understand Data Processing in Your Print Environment**

Look at data processing concerning printing. Understand the data flow across the platform and where the data touch points and vulnerabilities lie. This process may need to be regularly performed as new data or processes are added or new threats arise.

Note that in the case of HIPAA, any business associates that process health data will also need to come under the umbrella of HIPAA compliance.

### **Step 3: Document and Audit**

Understanding how the print environment and data processing intertwine allows it to be documented. Part of many privacy regulations is the evidence of compliance; an organization must show its data processing processes and procedures. They should also provide evidence on which security and privacy measures are used to adhere to security requirements.

### **Step 4: Gap Analysis**

A print environment audit will allow an analysis of gaps around regulatory compliance.

### **Step 5: Report**

Documenting compliance with GDPR, CCPA, and other regulations like HIPAA, is half the battle. If an organization understands the risk areas of using a Cloud-based print management platform, it can map those areas and their links to the safety measures in place. Documentation is a vital part of proving compliance.



## Creating a Secure Print Environment – Meeting the Compliance Challenge

When an organization implements a secure, cloud-based print management platform that can work with cloud services like Microsoft Azure, it will inherit several security features. Intelligent print management SaaS solutions, like Printix, offer the levels of control required by data protection and privacy regulations. They also have an in-built granular audit to monitor your print environment. Access control measures, such as those offered by Active Directory integration, extend the control to the whole ecosystem, and build in the type of control of data exposure that GDPR and other data protection frameworks insist upon. This fits neatly into a zero trust architecture with verification of people and endpoints at its heart.

### Using a Data Protection Impact Assessment

Privacy regulations typically specify that a Data Protection Impact Assessment (DPIA) is carried out. This is a wide-reaching look at the entire data infrastructure of an organization or organizational area and should always include your print environment. It is good practice to use a DPIA even outside of the regulatory requirements as it provides insight into data vulnerabilities. Once a DPIA has been carried out, it is easier to assess the risk in specific areas and create a mitigation strategy. A specifically designed secure cloud-based print management platform provides several built-in measures to close the vulnerability gap. For example, having the option to use pull-printing means a user only releases the print job once they have been authenticated, thereby significantly reducing the exposure of sensitive data.

### Privacy by Design (PbD)

PbD is about having a secure privacy environment built into the design and implementation of any system that handles data. The use of a secure cloud-based print management platform, like Printix, explicitly designed to address data security, works to the principles of PbD to meet the exacting compliance requirements of privacy and other data protection regulations.



## Examples of Requirements for a Secure Cloud-Based Print Management Platform

Below, we have picked out several questions that customers are asking about the features and functions of a secure, Cloud-based print management platform like Printix. Hopefully, these will give you an idea of the type of questions to ask when exploring a SaaS print solution:

**Question:** *How can a SaaS print solution isolate customer data?*

**Answer:** Authentication and authorization security models, based on industry standards like OAuth, can ensure that customer data is isolated and only accessible by authorized parties.

**Question:** *How can access to data be controlled?*

**Answer:** Data access is granular and based on a per tenant basis. Database access is controlled by a database administrator (DBA).

**Question:** *Can I store my customer data in the EU?*

**Answer:** Local laws often mean that data storage often needs to be a specified jurisdiction, like the EU. Because Printix uses Microsoft Azure as its infrastructure provider, data is stored in an Azure data center in The Netherlands. Other data centers may also need to be available but assurance that data is stored in the EU should be forthcoming. Printix can store a company's data in any regions required to meet the requirements of local regulations and laws.

**Question:** *What type of encryption do you use and where is it used?*

**Answer:** Encryption should be a well-known, tested and trusted algorithm such as Advanced Encryption Standard (AES) with a key length of 256 bits.

SSL/TLS (HTTPS) should be offered to protect data communications. Data transport should also be encrypted.

Database entries should be encrypted where necessary.

**Question:** *What type of disaster recovery can you offer?*

**Answer:** Databases should have regular daily backups. The backups need to be stored encrypted on alternative locations other than the main data center. Other disaster recovery processes for data loss or data corruption need to be offered.

Even if the Printix Cloud-based print management platform is down you can still print.

**Question:** *What kind of authentication and access control procedures are offered?*

**Answer:** Access control using secure methods such as SSH and with 2-Factor Authentication (2FA) should be offered. Systems must require authentication/ authorization before a user can have access. Sensitive tasks such as deleting a tenant MUST require two-factor authentication (2FA).

Integration with third party identity systems, such as Active Directory, Azure Active Directory or G Suite should be offered.

**Question:** *What sorts of policies are able to be used in the print environment?*

**Answer:** Data wiping: Tenant data should be able to be wiped after 90 days. If you want your data to be deleted before the typical disabled period is over, you should be able to request expedited deprovisioning.

Print data: Should not go outside of the company network unless using a Cloud connection, in which case data should encrypted and a deletion date set.

**Question:** *What other security measures should be used?*

**Answer:** Firewalls should be used to protect the production environment. Regular internal audits should be performed to make sure the production environment is kept secure.

A wide range of automated tests, both stress tests, unit tests and GUI-tests should be performed whenever a new release is made.

**Question:** *How can the threat of a DDoS attack be mitigated?*

**Answer:** Bad traffic should be filtered and diverted if a DDoS attack occurs. For the period of the attack the solution should be able to handle increased scaling to mitigate the impact of the significantly larger amount of traffic during a DDoS attack.

**Question:** *What measures are offered for incident response in the system?*

**Answer:** Audit logs including system security logs should be created on a regular basis and error-rates in the monitoring system should generate notifications.



## About Printix

Printix, a Kofax company, is a secure, cloud-based print management platform that works in seamless concert with Microsoft Azure AD.

Using Single Sign-On (SSO) with M365, each user gains fast, automatic access to printers, ready configured via Printix cloud administration. This significantly reduces workload for IT support staff. Printix is flexible, allowing easy removal of print servers with no impact on users. Printix is an intelligent system allowing for provision of data-driven analytics with enhanced reporting. This flexibility extends to 'Printix AI' which automatically manages users and printers as they move and print, between or across multiple office locations.

Printix is the glue that holds the secure print environment together in an increasingly complex enterprise network.



## About Kofax

Kofax enables organizations to Work Like Tomorrow™—today.

Kofax Intelligent Automation software platform and solutions digitally transform document intensive workflows. Customers realize greater agility and resiliency by combining our process orchestration, cognitive capture, RPA, output management, analytics and mobile capabilities to speed time-to-value and increase competitiveness, growth and profitability while mitigating compliance risk.

For more information, visit [kofax.com](https://www.kofax.com).



*Work Like Tomorrow.™*

