printix

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

Executive Summary

Technology is offering the modern enterprise new ways of working. Cloud-computing has extended the reach of our offices and our staff allowing us to work more productively. Our enterprise print environment has entered the era of cloud and is part of the extended infrastructure of our business. Cloud-based print environments are open to the same cybersecurity struggles that the rest of the business faces. The threats that we have to deal with on a daily basis, such as data breaches, Distributed Denial of Service DDoS, and even ransomware are now impacting our print environment too. The laws and regulations that we use to guide us in how we deal with these security issues and what we have to do to meet customer and government expectations are being strengthened to include the expanding threat matrix that Internet-enabled devices and the Internet of Things (IoT) have introduced. Regulations such as the GDPR and HIPAA have data protection at their heart, and systems that utilize cloud computing technology have to be incorporated into our overall drive to compliance.

This paper looks at the types of threats a cloud-based print infrastructure has to anticipate and what types of steps can be taken to mitigate those threats. It 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.

Part one

The Cloud Print Management Industry Today

The word 'data' is one which has entered the collective dictionary of our era. Data is everywhere and it comes in many forms, from digital to physical. What each form has in common is that it has a lifecycle and may also transform from one form of data to another. This is what happens with a modern, smart, 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 has to overcome the challenges of security and compliance expected by a number of data protection regulations.

The Cyber Threat Landscape – What Cloud Print Management Is Up Against

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

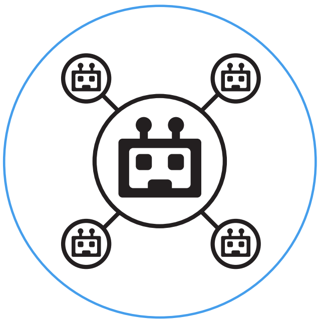
In order to mount an effective response to the cyber security threats impacting on enterprises of all types and sizes, we must have a complete understanding of the nature of these threats. We can break it down into several areas that are of particular concern to web applications and those utilizing data through services like cloud-based print management:

Data threats: The Breach Level Index, which collates data exposure across industry, recorded almost 2 billion breached data records in the first half of 2017. Only 4.6% of those records were encrypted (1). Data is a commodity and cybercriminals target data and not just personal data. Information is king and intellectual property theft 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 (2). Cloud-based print management is open to data focused attacks across the entire lifecycle of the print job. This includes the key areas:

- On disk - during processing of the print job, the data is available on the printer's hard disk and therefore vulnerable to exposure.
- Across the network - any unencrypted communication of data 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.

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 as part of their vector of chaos. An example is the DDoS vulnerability that security firm Trustwave found in Brother printers recently (3). This vulnerability was in found in the web front-end of the printer leaving it open to access control threats. Access control of Internet-enabled devices is a key vector that cyber criminals take advantage of when not correctly implemented or configured. The result is prevention of the use of the service or even the possibility of hijack of the service.

Ransomware: When we hear the word ransomware, we usually equate it with a PC or mobile phone being locked and/or our data being maliciously encrypted. We are then forced into a ransom situation - a fine being demanded for retrieval of encrypted data. Printers, especially a cloud-based print infrastructure, are also potential targets for ransomware. In fact, ransomware is expected to become one of the biggest threats to cloud-based services in 2018 (5). Printers are part of the flow and lifecycle of data, and as such are a target for ransomware and a potential source of disruption.



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 (4). 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.

Security Vulnerabilities in Older Servers: Some older server operating systems and associated software are no longer supported in terms of 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.

Costs of Cybersecurity and Data Exposure

The cost of a data exposure or service disruption can be profound. It can mean financial cost, cost of disruption, and even cost of reputation. The Ponemon Institute (6) carries out annual reviews of the costs to industry of cybercrime. In their 2017 survey, they found the average cost, per organization, per data breach, was $3.62 million. They also found that it took, on average, 191 days to identify a breach, and 66 days to contain it. The predictions going forward are not comfortable reading; Juniper Research has predicted that cybercrime will cost businesses $8 trillion by 2022 (7).

Having an SaaS platform to support cloud-based print management offers your organization a highly efficient way to manage and utilize print services across your organization. However, you have to use smart methods to manage the security of the service. In a mid-year survey for 2017, Cisco identified a key area in the fight against enterprise cybercrime as being the secure management of endpoints and infrastructure:

“Many companies underestimate the risk (and the number) of blind spots in their enterprise network, endpoint, and cloud infrastructure.” (8)

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

The balance of redress against the cybercriminal network has begun.

Average cost:
$3.62 million
per data breach

191
days to identify a breach

66
days to contain a breach

Cybercrime will cost
$8 trillion
by 2022

Trends in Printing – Using Smart Cloud Management Platforms for Printing

Before looking at the use of secure cloud-based print management platforms we should explore why this type of service has evolved.

Cloud managed services have been embraced by companies of all sizes. There are a variety of reasons why a company goes down the third-party service route for an infrastructure requirement. But in general, cloud managed services are expected to show a growth (CAGR) of 9.60% between 2017 and 2022 with an estimated global market value of US $86.47 billion by 2022 (9). This explosion of growth in cloud managed services is down to, amongst other things: efficiency of service, reach of services across an often remotely distributed workforce, and cost benefit.

Cloud managed services have extended their reach to printing. Printing is an oft-misunderstood area of business but is an intrinsic critical infrastructure of a business, albeit a less obvious one than energy or finance. However, for the business depending on it, the output can be super-critical. In a recent survey by Quocirca they found that 61% of large enterprises suffered at least one data breach because of insecure printing (10)

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.

Because of changing technology, including the increase in cloud-based infrastructures, modern companies are experiencing a transformation. They are witnessing change across various areas, including:

Incidence of remote working increasing, and workers using shared office space

Bring Your Own Device (BYOD) becoming more prevalent

Complicated administration of a diverse IT infrastructure across hardware, software operating systems

Vendor-specific printing requirements within a complex IT infrastructure

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.

Right Scale's "2017 State of the cloud" survey (11) found that 85% of enterprises were running applications across multiple clouds. Cloud computing platforms like Microsoft Azure allow businesses to become more efficient, and printing may be business process that can be most simplified using the cloud.

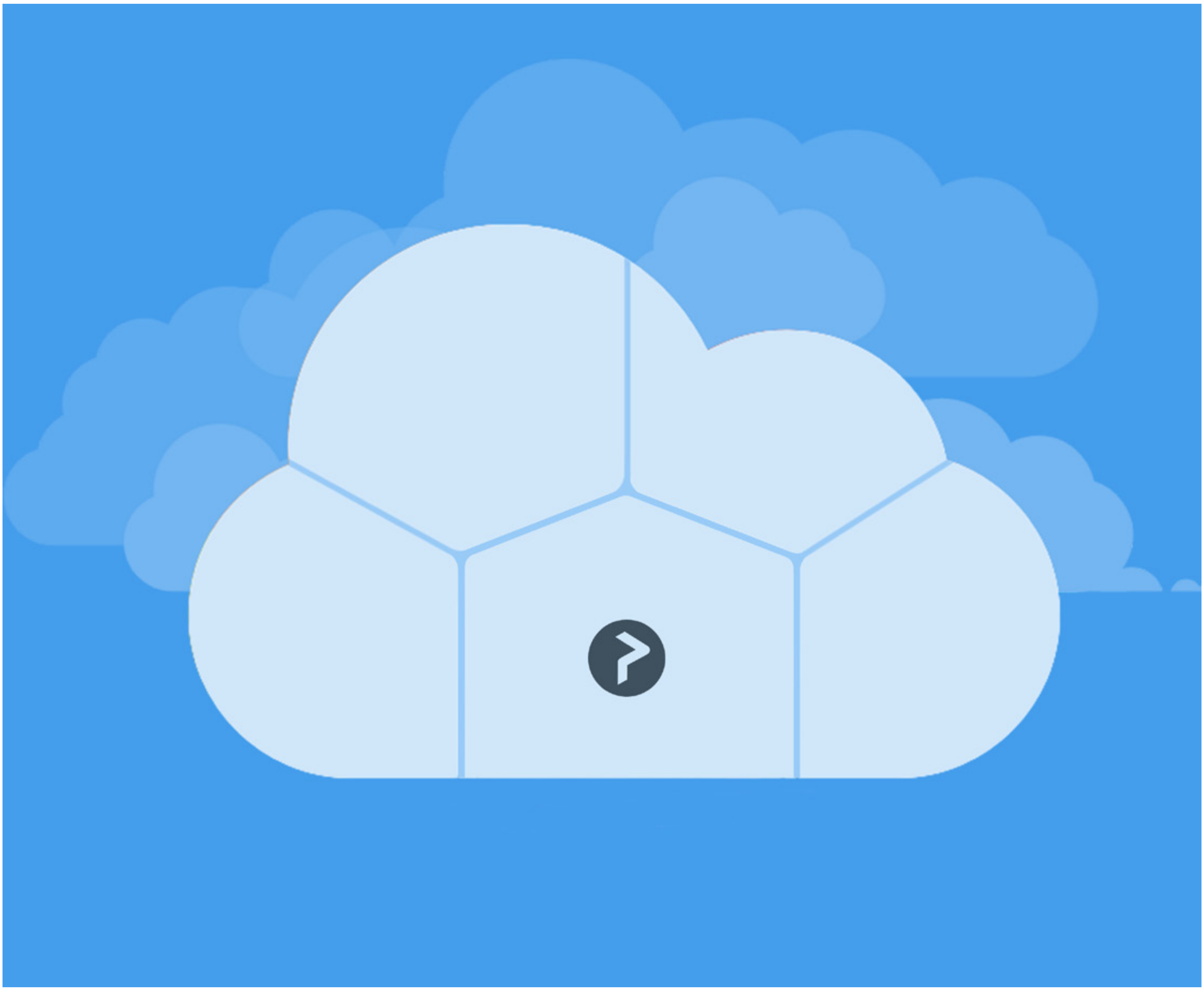
Part two

Secure Cloud Print Management Services to Meet the Compliance and Security Challenge

Previously, we set out the type of security environment that an enterprise has to deal with. The hostile cyber security situation that an enterprise finds itself in today has to be met with knowledge and a plan of how to mitigate the impact of an attack. Having a thorough understanding of the threat landscape offers a way to redress the balance against attacks. With a smart and secure approach to cloud-based print management we can have the efficiency afforded by cloud computing, without the cost of a cyber attack.

In addition, the compliance and regulatory frameworks we rely on to guide our security choices are being adjusted to accommodate new technologies; this includes the extended use of Internet-enabled devices and the massive explosion of big data.

Fortunately, much work has been and is being done in the field of cyber security threat mitigation. This work extends to the field of secure cloud-based print management platforms and below we have identified a number of key areas of concern and their associated solutions.



Cybersecurity and Cloud Threats of Cloud-Based Print Platforms

The table below is a guide to best practice when using a cloud-based print management platform.

Issue/Area of concern	Solution
Man in the Middle attack (MitM) - cloud-based systems are open to interception of data communications	Use SSL/TLS (HTTPS) encryption to secure communication of data across Internet connections. Option to isolate the data communications by keeping sensitive data within an organization's own network. The Printix solution allows print data to be stored locally.
Data exposure via cloud application attacks such as cloud database exfiltration	SaaS solutions should allow that print data stays local if required. Data should automatically reside in the cloud only when it is needed to manage the print infrastructure. This will also reduce the impact of a cloud-based malware infection that can then exfiltrate data. 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.
Access control to data and print jobs	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. 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.
Open ports	Some ports need to be open to communicate. However, a cloud-based platform should not require any open inbound ports in the firewall. Any port traffic should be encrypted.
Unencrypted data and loss	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.
Inadvertent theft from printers	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.
System behavior	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.

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

The expanding and increasingly sophisticated cybersecurity threat landscape has resulted in the upgrade of compliance and regulatory frameworks across the world. Data privacy and security mandates such as the General Data Protection Regulation (GDPR) which comes into force on May 25, 2018 sets out stringent rules on the processing of data. Other such as the Health Insurance Portability and Accountability Act (HIPAA) have specific regulatory requirements around the protection of health data. The GDPR is understandably causing anxiety among organizations the world over. The regulations expect that a number of data rights are adhered to for all EU citizens. This means implementing controls over EU citizen and employee data when it is processed, no matter where in the world. Non-compliance can result in massive fines of up to 4% of global revenue or 20 million euros, whichever is greater.

What is the GDPR About?

The GDPR is about data, and specifically personal data. However, the definition of personal data varies widely. Article 4 of the GDPR defines a number of terms, including personal data as:

"any information relating to an identified or identifiable natural person" (12)

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

"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;"

This puts printing firmly in the spotlight of the GDPR. Print environments are awash with data. Often this data will contain the personal information described by the GDPR. 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. The GDPR also sets out a series of 'data subject rights' with respect to how data is managed, controlled and accessed.

A good rule of thumb is to only record data needed to do the processing of a given task. This will help when you evaluate the impact of GDPR on your organization during the assessment phase. It will also reduce the load on the organization for data protection and the data subject rights expected to be upheld under GDPR.

These data subject rights are:

Informed: The right to be informed
Access: The right of access
Correct: The right to rectify incorrect data
Erasure: The right to have data forgotten
Restriction: The right to restrict data processing
Movement: The right to portability of data
Processing: The right to object to how data is processed
Automation: The rights in relation to automation of data processing

HIPAA for Health Data Protection

The HIPAA legislation came into force back in 1996 to add safeguards, including data privacy and security to the use of 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 can 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.

Five Steps to Help Map Print Environments to GDPR and HIPAA Compliance

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. The following steps can help in an understanding of how cloud-based printing platforms fit into GDPR or HIPAA compliance measures:

Step 1: Identify where printing fits: Include the print environment in an overall GDPR or HIPAA 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 with respect to printing. Understand the data flow across the platform and where the data touch points and vulnerabilities lie. This is a process that may need to be regularly performed as new data or processes are added. 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: Having an understanding of how the print environment and data processing intertwine allows it to be documented. Part of GDPR compliance is showing that an organization understands their data processing processes and procedures, and are putting measures in place to adhere to GDPR security requirements. Similarly, a HIPAA risk assessment can show evidence that you have a security plan in place.

Step 4: Gap analysis: An audit of the print environment will allow analysis of gaps around GDPR or HIPAA compliance in that area.

Step 5: Report: Documenting compliance with GDPR , 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 then map those areas and their links to the safety measures in place. Documentation is a key part of becoming compliant.

Meeting GDPR compliance includes how to meet security expectations around sensitive data and mitigate risk and exposure of data. Other regulations that include data security, such as industry specific ones like PSD2 and HIPAA, will be at least partly encompassed by going through the rigors of GDPR compliance.

Creating A Secure Print Environment – Meeting the Challenge

When an organization chooses to implement a secure, cloud-based print management platform that can work in concert with cloud services like Microsoft Azure, they will inherit a number of security features. Intelligent print management SaaS solutions like Printix offer the levels of control required by GDPR and other regulations like HIPAA. They also have in-built granular audit that allows you to monitor your print environment. Access control measures such as those offered by Active Directory integration extend the control out to the whole ecosystem and build in the type of control of data exposure that GDPR and other data protection frameworks insist upon.

Using a Data Protection Impact Assessment: The GDPR requirements 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 GDPR requirements as it allows you to understand where there may be data vulnerabilities. A DPIA can also help with HIPAA compliance and understanding where gaps may lie. Once done it is easier to make an assessment of the risk in that area and create a mitigation strategy. Using a specifically designed secure cloud-based print management platform provides a number of built in measures designed 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 greatly reducing the exposure of sensitive data.

Privacy by Design (PbD) is the foundation stone of the GDPR: 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, designed specifically to address data security, like Printix, provides the PbD tools to meet the exacting compliance requirements of GDPR and other data protection regulations.

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

Below, we have picked out a number of questions that are being asked by customers 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 an 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 needs to be a specified jurisdiction, like the EU. Printix uses Microsoft Azure as its infrastructure provider and data is stored in an Azure data center in The Netherlands. Other data centers may also need to be available and assurance provided that data is stored in the correct jurisdiction. Printix can store a company's data in any region required, to ensure data residency and 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 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 be 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 is a secure, cloud-based print management platform that works in seamless concert with Microsoft Azure AD.

Using Single Sign-On (SSO) with Office 365, 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.

References:

(1) Gemalto, Breach Level Index Report H1 2017:
http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

(2) The National Bureau of Asian Research, IP Commission Report 2017:
http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

(3) Trustwave, Denial of Service Vulnerability in Brother Printers:
https://www.trustwave.com/Resources/SpiderLabs-Blog/Denial-of-Service-Vulnerability-in-Brother-Printers/

(4) PC World, Hacker hijacks thousands of publicly exposed printers to warn owners:
https://www.pcworld.com/article/3166052/security/hacker-hijacks-thousands-of-publicly-exposed-printers-to-warn-owners.html

(5) Computer Weekly, Ransomware to hit cloud computing in 2018, predicts MIT:
http://www.computerweekly.com/news/450432488/Ransomware-to-hit-cloud-computing-in-2018-predicts-MIT

(6) The Ponemon Institute, 2017 Cost of Data Breach Study:
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

(7) Juniper Research, The Future of Cybercrime & Security:
https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security/enterprise-threats-mitigation

(8) Cisco, 2017 Mid-Year Cybersecurity Report: *https://engage2demand.cisco.com/cisco_2017_midyear_cybersecurity_report*

(9) Transparency Market Research, Global Cloud Managed Service Market Driven by SME's Strive to Reduce CAPEX:

https://www.transparencymarketresearch.com/pressrelease/cloud-managed-services-market.htm

(10) Quocirca, Print Security: An Imperative In The IoT Era: *http://quocirca.com/content/print-security-imperative-iot-era*

(11) Right Scale, 2017 State of the Cloud:
https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey

(12) GDPR, Article 4: *https://gdpr-info.eu/art-4-gdpr/*