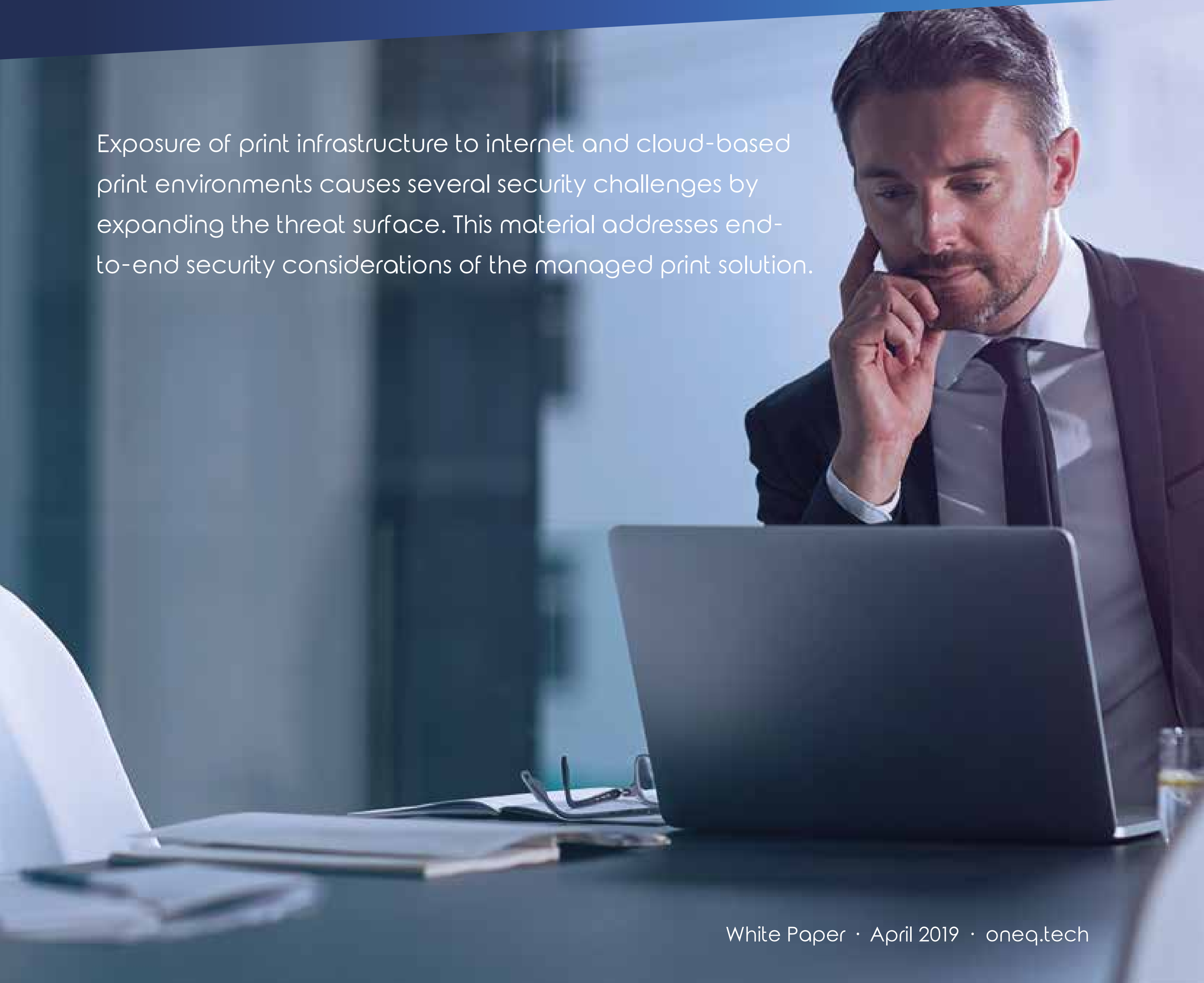
White Paper:

Security & Compliance in Managed Print Solution



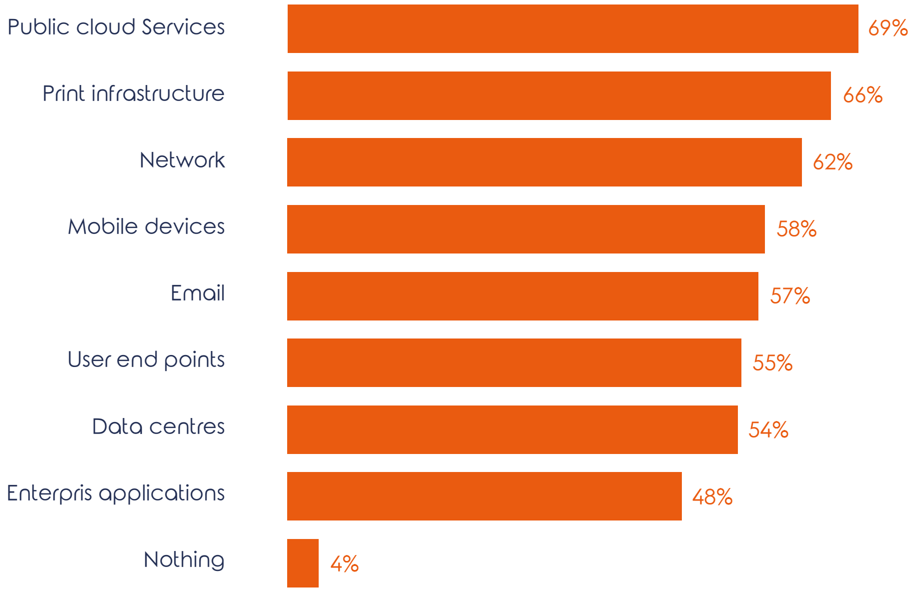
Exposure of print infrastructure to internet and cloud-based print environments causes several security challenges by expanding the threat surface. This material addresses end-to-end security considerations of the managed print solution.

Table of contents

Importance of Print Security

According to Quocirca, the cyber-attack surface is increasing for many organisations as connected Internet-enabled endpoints proliferate. These include both legacy and the new breed of smart printers and multi-function printers (MFPs). Consequently, businesses must take a proactive approach to print security as these print devices can provide an open door to corporate networks. By taking steps to analyze the potential vulnerabilities of print environments, businesses can mitigate risks without compromising productivity.

Figure 1: Rating of IT risks that may lead to security breaches (% ranking as a top 5 concern) (Ref.: Quocirca, Global Print Security Landscape, 2019)



Global Print Security Landscape

A global market analysis on print security ranks the print infrastructure 2nd among risks of security and data breaches.

61% of large enterprises suffered at least one data breach because of insecure printing (Quocirca's Print Security 2019).

Printing Environment

A printing environment may provide a mix of printing and scanning functionalities.

Using Web print, users upload documents using a web portal in order to print. Login validation is optional. In Driver print, users can perform the print from their programs and workstations or laptops. This may perform with or without driver installation using a print server, optionally with one or multi-factor authentication. With Email print users can send documents for printing from mobile devices, by sending an email with documents attached, to a specified email address configured for this purpose. This may optionally secure with login credentials or PIN Codes etc.

"Users can access and download their files through a Smart Scan client application or using a web browser."

With Mobile print, users can send documents to print using an App on Apple iPhones and iPads, or Android smartphones and tablets, or Windows Phone devices. This can also utilise optional authentication method(s).

Using the other technique Google Cloud Print, users can send print jobs from Chromebook, phone or tablets, Google Apps like Gmail, Google Docs, Google Sheets, or using any other application or device that supports Google Cloud Print.

Scanning jobs may include Smart Scan as a simple and secure method for users to scan their documents on MFPs and receive them directly into a folder on their own computer. Users can access and download their files through a Smart Scan client application or using a web browser. Using Scan to Workflow the scanned images of your documents will seamlessly be routed to one or more target corporate applications such as ERP or HRMS systems or alternatively to shared folders or emails, document management systems. The built-in features of the solution may analyse the images and the content to forward it to the right destination.

The Print Security Ecosystem

The Print systems are quite complex and covering multiple devices, networks, and operating systems. There are three main areas which should be analysed and hardened for end to end security: Device security, Data security and Document security. A range of features should be implemented in printer and MFP by device manufacturers. Data threats may target any sort of print or scan data in transit or at rest. The entire lifecycle of the print job is vulnerable to exposure and data breaches, either on hard-disk (MFP) or on transit across the network, a hard-copy of printed document or any unauthorised access to the printer by an insider or outside-world attack.

As an example, non-compliance to GDPR can result in massive fines of up to 4% of global revenue or 20 million euros, whichever is greater.

Business risks:

- Compliance issues
- Damaged reputation
- Financial loss

Range of attacks can endanger print environment:

- Ransomware
- DoS / DDoS
- Botnet
- Malware / cloud database exfiltration
- Man-in-the-Middle
- SQL injection, Cross-Site forgery, Cross-Site Scripting (Web pages)

Security & Compliance measures

Various compliance standards regulate security and data protection of one or few elements of managed print environment from printing devices, MFPs to data transport and cloud computing infrastructure.

This may focus on nature of business or industries or being popular in a region of the world such as GDPR for EU citizens, or data protection regulations under HIPAA.

The GDPR covers data protection of personal data for EU citizens. This means implementing controls over EU citizen and employee data when it is processed, no matter where in the world. The definition of personal data covers a wide range. With reference to Article 4 of the GDPR definition of "personal data" is: "any information relating to an identified or identifiable natural person".

For further details refer to GDPR definition of terms on Article 4: Definitions[1].

A few 'data subject rights' are covered under GDPR. These including, the right to be informed, right of access, the right to rectify incorrect data, the right to have data forgotten (erasure), the right to restrict data processing, right of portability of data (movement), the right to ask to how data is processed, the rights in relation to automation of data processing.

> "...definition of 'personal data' is: 'any information relating to an identified or identifiable natural person'."

The HIPAA[2] is primarily targeting to modernise the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare industries should be protected from fraud and theft.

Today's printers and multi-functional devices can have hard drives the size of high-spec laptops. As conduits for corporate information being printed, faxed etc. they retain data subject to legal and regulatory compliance, such as the Data Protection Act[3] and PCI-DSS[4].

[1] GDPR Article 4: Definitions https://gdpr-info.eu/art-4-gdpr/

[2] HIPPA: Health Insurance Portability and Accountability Act

[3] U.K. Data Protection Act 1998 (DPA 1998); https://whatis.techtarget.com/definition/UK-Data-Protection-Act-1998-DPA-1998

[4] What's new in PCI-DSS and PA-DSS version 3.0? https://www.computerweekly.com/podcast/Podcast-Whats-new-in-PCI-DSS-and-PA-DSS-version-30

One Q targets end-to-end Print Security

It is highly recommended to assess your print environment for the security and vulnerability areas. The below table reviews end to end security challenges and proposes solutions. Please contact us for the assessment questionnaire.

Concern & How to address

Concern: Unclaimed print jobs

- Pull Printing plus 2FA[5]: Card Reader, QR Code, etc.
- Card-in-touch (job file deletion if MFP out-of-paper)[6]

Concern: Compliance & Regulatory

- GDPR – PCI DSS – HIPPA – FIPS

Concern: Data Privacy

- Local file storage (One Q PM, Connect Server CS)
- Encrypted file storage & database
- Privacy printing by mandatory pull printing

Concern: Data transport

- SSL/TLS with Cert.: IPPS, One Q PM (Local, p2p to MFP), One Q PM (Server upload), HTTPS
- IPSec VPN with SSL Cert., IKEv.1 & 2.
- IPSec AES-256 data encryption

Concern: Security management tools (SIEM, UEBA, etc.)

- Integration with 3rd party security analysis tools such as SIEM or UEBA (Syslog, Audit Logs, Event Logs, etc.)

[5] 2FA: two-factor authentication

[6] The card must be touched and left on the reader during print job. If the printer goes out of paper, then the whole print job including the file should be erased from printer hard disk. In the absence of this feature the next person can receive the remainder of print output from previous person, after topping up papers in the tray.

Concern & How to address

Concern: Authorized Access

- Two-Factor Authentication: Short ID / Pin Code, Card or Badge, Windows Login, Fingerprint, NFC, QR, etc.
- Digital certificates on MFP (enrolled by VDMS)
- Tracking of printed jobs (all printing sources)

Concern: Isolation of customer data

- SSO/IDM token-based authentication (CAS)
- 'One Q PM' to keep the print job locally

Concern: Latent images on MFP hard disk

- Supports of MFP device manufacturer
- (Same day print/copy job removal)

Concern: Multi-layered Print Security

- One Q Assessment questionnaire

Concern: Fleet monitor & manage

- Fleet firmware/OS updates
- One Q Care FMS (SaaS)
- Device Onboarding: Auto-configure new MFPs when added to the network
- Compliance audit reporting of print fleet security

Concern: Document Security

- Automated certificate management (MFPs, Clients)
- One Q VDMS print server (for MFP)
- ADCS (MS Win Server), KeyStore Explorer (Linux Server)
- Deploy MICR, Watermarks, etc. to deter counterfeit, fraud, or document tampering

Concern: Certificate management

- Automated certificate management (MFPs, Clients)
- One Q VDMS print server (for MFP)
- ADCS (MS Win Server), KeyStore Explorer (Linux Server)

Concern: Document Security

- Deploy MICR[7], Watermarks, etc. to deter counterfeit, fraud, or document tampering

[7] MICR: Magnetic ink character recognition code, known in short as MICR code, is a character-recognition technology used mainly by the banking industry to ease the processing and clearance of cheques and other documents.

Concern & How to address

Concern: Device security (MFP)

- Run-time intrusion & malware detection
- BIOS code self-healing
- Firmware Whitelisting
- Detect malware "calling home"
- Encrypted storage with secure erase – print job encryption & cleanup
- Disable unused physical ports (USB, Network)
- Support identity and CA certificates

Concern: Cloud Cybersecurity

- Option for Local Storage of print data (Isolation)
- Use SSL/TLS (HTTPS) encryption to secure data communication across Internet connections
- Any traffic on open ports should be encrypted
- Isolate authentication data by use of SSO / token-based authentication techniques across multiple cloud-provider or multiple cloud IAMs[8] (Office 365, SalesForce, etc)
- Auto-Scaling can mitigate impact of large traffic (DDoS attack)

Concern: Data Loss (DLP)

- Databases should have regular daily backups (Server config, logs, audit data, User data print jobs, etc.)
- Backups to be stored encrypted in geo-redundant locations
- Implement DR & HA[9] for VDMS servers: Clustering, Grid

Concern: BYOD & Mobile Printing

- Personal and BYOD devices must be secured with SSL certificates
- Consider options to allow connect to the printer without accessing the company network: Wi-Fi Direct, Bluetooth, NFC touch-to-print

Concern: API

- Implement multiple layers of security for Public APIs; use authentication tokens which may bind with IP address whitelisting to only receive API calls from trusted sources

[8] IAM: Identity Access Management

[9] DR: Disaster Recovery, HA: High Availability

About One Q Technologies A/S

We are a team of enthusiastic and passionate professionals, who are working on making secure printing efficient and simple for enterprise customers worldwide. The company was founded in 2004 under the name Ubiquitech, until changed to One Q in August 2017. Our software is based on cloud technology, easy and simple to deploy and manage. We do however give our customers the freedom of choice if you still want One Q installed on-premise using Windows, Linux and other platforms. We offer services to our customers worldwide through a network of skilled and certified partners, making them valuable and essential contributors in assisting customers from pure interest to seeing the benefits of the implemented solutions.

For more information, visit oneq.tech.