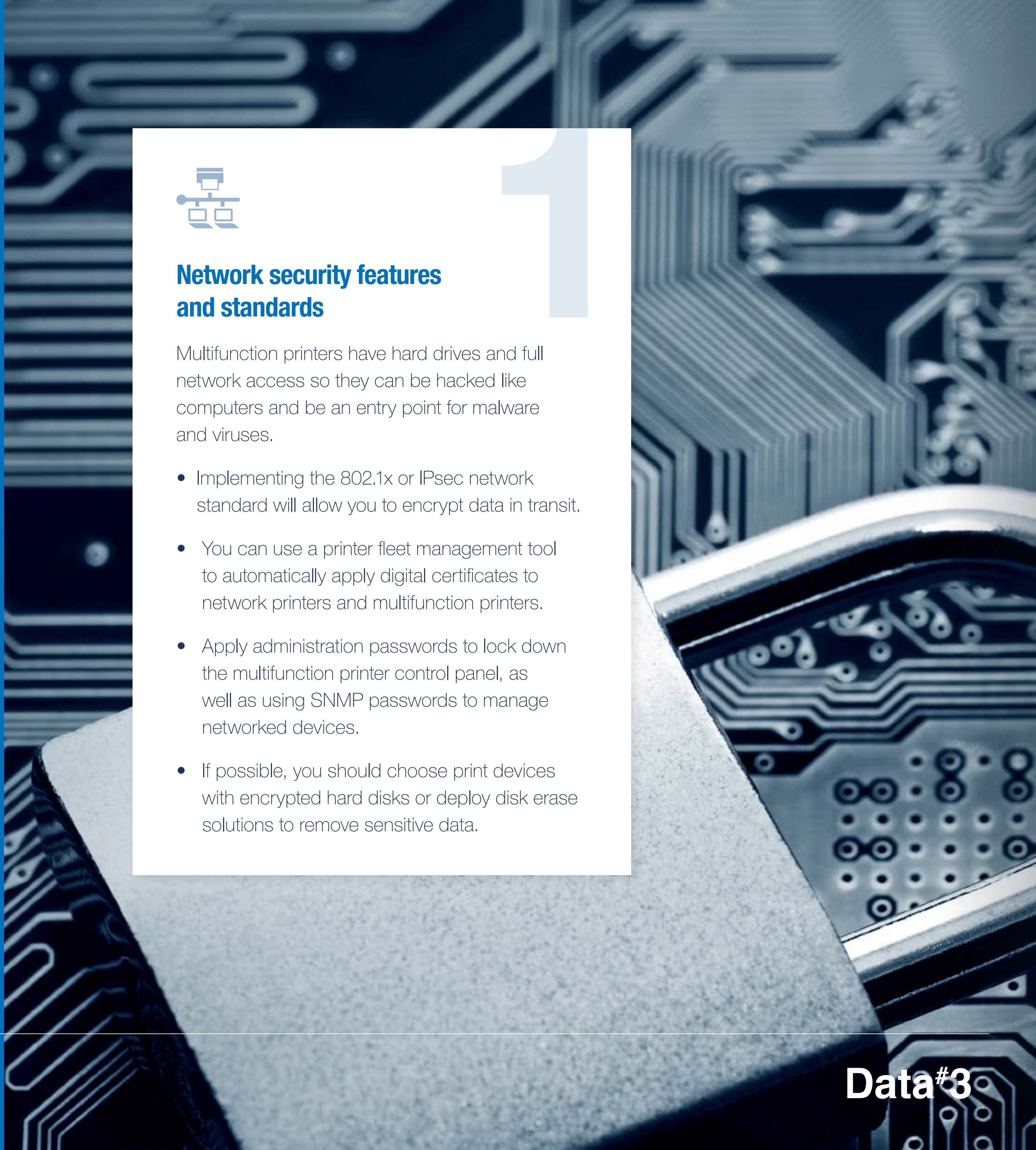
# Data#3

## The six printer security hotspots every business should check

# INTRODUCTION

Today's multifunction printer does more than simply print. It scans, sends and stores potentially sensitive information. Innovations surrounding networked printers help streamline business processes and increase productivity. At the same time, implementing those additional features may leave your fleet vulnerable to attack.

If your printer fleet connects like your computer fleet connects, it should be protected in the same way. In conjunction with HP, we've identified six printer security hotspots that all businesses should be reviewing to ensure they're protected. Within each hotspot, we've provided a checklist for you to quickly assess your printer security practices and guide any remedial action you should take.



1

## Network security features and standards

Multifunction printers have hard drives and full network access so they can be hacked like computers and be an entry point for malware and viruses.

- Implementing the 802.1x or IPsec network standard will allow you to encrypt data in transit.
- You can use a printer fleet management tool to automatically apply digital certificates to network printers and multifunction printers.
- Apply administration passwords to lock down the multifunction printer control panel, as well as using SNMP passwords to manage networked devices.
- If possible, you should choose print devices with encrypted hard disks or deploy disk erase solutions to remove sensitive data.

2

## Fleet management

Lack of central control of printers and the inability to automate policies can lead to inefficient, incomplete, and time intensive efforts by IT to establish and maintain security settings on printers.

- Consider applying a user authentication solution to track all printing activities and maintain corporate security and compliance standards.
- Deploy a printer fleet management tool to ensure your devices are up-to-date with the latest device protection and security features.
- You should establish a standard level of security configuration and secure user policies. Once established, leverage fleet management tools that provide centralised visibility and control with the ability to automatically apply these to new devices.
- By including printers as part of your IT ecosystem, and using security information and event management (SIEM) software, you can detect and take corrective action on printer security alerts.

3

## Mobile print security

Allowing workers to print from mobile devices is a convenience and can also increase productivity. In the absence of a user-friendly mobile device strategy, employees may implement workarounds that could violate established security policies. If mobile printing is important to your organisation you should:

- Use a managed mobility solution that includes print client authorisation with secure authorisation tokens. This should integrate with VPN or MDM solutions as well as provide specific end user set-up and policy settings.
- Limit mobile printing to authorised users only and deploy a user authentication solution with passphrase, PINs or LDAP authentication to allow mobile device printing.
- Apply your overall print security policy to your mobile device printing.
- Consider peer-to-peer wireless printing that allows users to print without connecting to the network, or the same subnet as the printers.

4

## Document security

Output trays are an easy way for sensitive data to fall into the wrong hands. Unprotected output trays could lead to confidential documents (such as birth certificates, prescriptions etc.) being stolen and used in malicious activities such as identity theft. Options for increasing physical document security include:

- Installing output trays with physical locks.
- Using a chemical reacting toner that can dramatically reduce the potential for fraudulent alteration of documents.
- Appling a private or pull-print solution to authenticate users before releasing the print job to the output tray.
- Embedding fraud protection such as UV inks, water marks, custom logos, signatures and security fonts into documents.

5

## User authentication and access control

Without requiring user credentials, it's possible for sensitive documents to be retrieved and distributed by any user - anyone who can access printer settings can exploit permissions. Consider:

- Implementing user authentication methods such as passphrase, PIN, LDAP authentication, proximity cards, smart cards or biometric access controls. All are effective ways to prevent sensitive documents from falling into the wrong hands.
- Only allowing IT staff and other authorised individuals to set-up and configure printer settings.
- Restricting certain printer features by user or department to reduce costs and security risks.
- Assigning printer feature permissions to individuals or groups as well as lock out walk-up features such as copying.

6

## Printer hard drive security

Printing and imaging devices store user credentials and other sensitive data that can be accessed if not encrypted or periodically erased.

- Consider hard drive encryption to prevent the theft of information stored on the printer's hard drive.
- If disposing of a printer, ensure that the data on the printer's hard drive is erased or otherwise removed.
- Even if using encryption, erasing the printer's hard drive every day is one of the simplest ways to reduce the risk of printer security breaches.
- Control who has access to networked printer settings with passwords.

As an end-to-end IT solutions provider, Data#3 is more than just a print company focused on increasing cost-per-page services. Our approach to managed print includes big data and analytics as well as security, optimisation of your printer fleet, workflow management and cost management as part of a full IoT solution.

We're changing what a managed print service should be.

**For more information visit data3.com.au/secure-managed-print or contact Data#3 today.**

**1300 23 28 23**
www.data3.com.au

**Brisbane (Head Office)**
67 High Street
TOOWONG, QLD
4066, Australia

**Melbourne**
Level 4,
55 Southbank Boulevard
SOUTHBANK, VIC
3006, Australia

**Sydney**
107 Mount Street
NORTH SYDNEY, NSW
2060, Australia

**Launceston**
23A Earl Street
LAUNCESTON, TAS
7250, Australia

**Adelaide**
84 North Terrace
KENT TOWN, SA
5067, Australia

**Canberra**
Level 3,
65 Canberra Ave
GRIFFITH, ACT
2603, Australia

**Hobart**
16 Collins Street
HOBART, TAS
7000, Australia

**Perth**
Level 2, 76 Kings Park Road
WEST PERTH, WA
6005, Australia

**Fiji**
Suva Business Centre
217 Victoria Parade
Suva, Fiji

**Follow Us:**

twitter.com/Data3Limited

facebook.com/Data3Limited

linkedin.com/company/Data3

youtube.com/Data3Limited

Data#3