KONICA MINOLTA

RETHINK PRINT SECURITY

SECURE YOUR PRINTERS, PROTECT YOUR BUSINESS

Giving Shape to Ideas

PRINT INFRASTRUCTURE — A GAP IN SECURITY?

Like any responsible organisation, you work hard to protect your data and your business against the risk of security breaches that could lead to reputational, legal or financial losses. You'll be using firewalls, anti-virus software and other security technologies to secure your network, email system, cloud services and mobile devices.

But what about your printers? It's often the case that when users print, copy or scan a document, they're entrusting business-critical, confidential or sensitive information to their organisation's print infrastructure. And although print infrastructure is rated as a top-5 IT security risk, organisations may not know where to start when it comes to securing their printers.

RATING OF IT RISKS THAT MAY LEAD TO SECURITY BREACHES*

69%
Public cloud services

66%
Print Infrastructure

62%
Network

58%
Mobile devices

57%
Email

*Quocirca 2019 - Global Print Security Landscape, 2019

What are the risks of unsecured printers?

An unsecured printer could:

- Give attackers access to the valuable business data that's stored on your printer's hard drive whenever a document is printed, copied or scanned
- Provide attackers with a gateway onto your network that lets them penetrate your organisation
- Allow viruses from infected documents to pass into or outside your organisation

Advanced security for Konica Minolta devices

To help you close this chink in your defences, Konica Minolta has developed a range of security features for its bizhub i-Series range of multifunction printers (MFPs). By using them to protect your print infrastructure, you'll keep your data, your organisation, and those you do business with safe from threats and attacks.

3
LAYERS OF PROTECTION WITH KONICA MINOLTA

Built-in and optional security features for our bizhub i-Series devices help you safeguard your data and your business. Our engineers are on hand to help you configure all these features to meet the needs of your organisation.

1

bizhub SECURE:
Protect data stored on the MFP's hard drive

bizhub SECURE is designed to secure the MFP and its hard drive to safeguard your data. It can be activated on your MFP before we deliver it or once it's installed on your site. Here's how you benefit:

Password protection. You can use secure passwords to protect document data, the bizhub hard drive, and the security settings on the MFP itself:

- Protect sensitive documents by storing them in a password-protected box or folder on the MFP's hard drive
- Set a password to lock down the bizhub hard drive
- Set your own administrator password to prevent unauthorised changes to security settings

Protection for data in temporary storage. You can protect document data while it's temporarily stored on, or passes through, the MFP using encryption and overwriting. So your organisation's data can flow safely with no risk of security breach.

Time-limited data storage. You can limit the length of time document data is held in temporary storage on the MFP's hard drive, so it's not left vulnerable to attack.

Hard drive encryption. Your MFP's hard drive can be encrypted, so that even if the MFP or its hard drive gets stolen, the data stored on it remains inaccessible and secure.

bizhub SECURE features at a glance:

—

Password protection of the bizhub hard drive

—

Encryption of bizhub hard drive contents

—

Timed auto-deletion of data stored in electronic folders on the MFP

—

Prevention of unauthorised changes to secure settings by creating your own administrator password

—

2

bizhub SECURE Notifier App: Monitor your MFP's security settings

The bizhub SECURE Notifier App lets you keep an eye on your printer's security settings using the bizhub control panel.

If a change is made, the app notifies the system administrator by email, so that prompt action can be taken if the change was unauthorised.

The bizhub SECURE Notifier App comes with bizhub SECURE as standard.

3

BitDefender: Protect against viruses and malware

BitDefender Antivirus can be installed on any bizhub i-Series MFP to protect your organisation against document-borne viruses and malware. With BitDefender, you:

- Create a safe operating environment for your users
- Ensure the data and documents handled by your bizhub are safe
- Prevent the spread of potential risks outside your organisation

BitDefender works by performing real-time scans of incoming and outgoing data — including print jobs, scans and PDFs — checking for potential viruses and other malware. You can see the scans on the MFP's control panel.

If BitDefender detects anything suspicious, it blocks the job in question and notifies the administrator.

Bitdefender

BitDefender® features at a glance:

—

Automated and scheduled real-time scanning of data transmitted and received

—

Automatic updates to ensure protection against the latest known viruses

—

READY TO KNOW MORE?

If you'd like to know more about protecting your data and your business with security features for your Konica Minolta devices, please get in touch, we're here to help.

business@konicaminolta.co.uk

KONICA MINOLTA

READY TO KNOW MORE?

If you'd like to know more about protecting your data and your business with security features for your Konica Minolta devices, please get in touch — **we're here to help.**

business@konicaminolta.co.uk

Konica Minolta Business Solutions UK Ltd, Miles Gray Road, Basildon SS14 3AR
www.konicaminolta.co.uk

03/2020