KONICA MINOLTA

SECURITY WITHOUT SACRIFICE

INFORMATION
SECURITY

Giving Shape to Ideas

SECURITY IS THE KEY ELEMENT OF KONICA MINOLTA'S OVERALL STRATEGY

"Konica Minolta offers a comprehensive range of solutions across access control, data security, network security and scanning security, with functionality varying across device. … Konica Minolta claims to have the widest range of ISO15408 fully certified MFPs in the market."

Source: Quocirca (2017): Business and IT Analysis "Print security: An imperative in the IoT era – A market perspective on print security", p. 14.
This independent report was written by Quocirca Ltd., a primary research and analysis company specializing in the business impact of information technology and communications (ITC).

INDUSTRY-LEADING SECURITY STANDARDS

In the digital age, we have seen global communications undergo unprecedented growth – and the potential of damaging security breaches has soared in parallel. In any business environment, the daily activities of printing, scanning, copying, emailing and faxing as the elementary components of work processes and workflows make MFPs indispensable at many levels. As a consequence, it is paramount that these devices are given the protection needed to withstand the ongoing threats to security.

Konica Minolta's comprehensive range of standard security features and options form a powerful source on which professional solutions can be based: solutions to both detect and prevent security violations, and avoid knock-on financial and/or reputational damage at the corporate as well as the private individual level. Konica Minolta has pioneered this field and remains the industry's leader.

Konica Minolta devices are certified almost without exception in accordance with the Common Criteria ISO 15408 framework. These are the only internationally recognized standards for IT security testing for digital office products. Printers, copiers and software compliant with Common Criteria certification have all passed a strict security evaluation and are able to satisfy and deliver the kind of security levels that a prudent business operation should seek and rightfully expect.

DATA STAY WHERE THEY BELONG – IN THE RIGHT HANDS!

Generally MFPs offer a huge range of functions and features. All these features represent a wide range of potential security leaks. Therefore a lot of security mechanisms are included in the system offering secure access control, document and data security and network security. With bizhub devices data stay where they belong.

Access control/Access security

Despite the topic of security being high on the agenda in both public and corporate domains, MFPs are often ignored as being any kind of security risk. While some risks are perhaps identified, they are often simply neglected, especially where sensitive documents and information are concerned. This is especially risky for those MFPs and printers located in public areas, where they can be accessed by staff, contractors and even visitors.

Because the advanced features available on today's MFPs deliberately make it easy for information to be copied and distributed within and beyond actual and virtual corporate boundaries, the first logical step is to prevent unauthorized persons being able to operate an MFP. Preventive measures are needed to firstly control access to MFPs, and secondly to establish some kind of security policy reflecting how the devices are actually used in real life. Obviously none of these measures should restrict or limit the user-friendliness of the systems. Konica Minolta is prepared for this, offering various security features and solutions.

Document security/Data security

Reflecting the fact that MFPs can easily be accessed if located in public areas, it is necessary to implement appropriate data security policies. After all, the situation is that confidential data, for example stored on the MFP hard disk over a period of time or simply confidential documents lying in the MFP output tray as printouts, is initially unprotected and could fall into the wrong hands. Konica Minolta offers a comprehensive range of tailored security measures to ensure document and data security.

Network security

Today's business environment is characterized by connected systems, automatic data collection and transmission to downstream systems handling the data afterwards. Konica Minolta office devices are designed to integrate into network environments. For example, network printers and multifunctional peripherals (MFP) have evolved to the point that they act as sophisticated document processing hubs integral within the network, with the ability to print, copy and scan documents and data to network destinations, as well as send emails, for example. This scenario also means that this office technology must cope with and comply with the same security risks and policies as any other network device, and represents a risk if unprotected. Therefore, Konica Minolta ensures that all equipment complies with the strictest security standards, which are achieved by multiple features in order to close potential security leaks by using the network connection.

WITH ITS COMPREHENSIVE RANGE OF SECURITY FEATURES, KONICA MINOLTA PROVIDES PROFESSIONAL SOLUTIONS FOR THE DETECTION AND PREVENTION OF SECURITY BREAKS.

ACCESS CONTROL & SECURITY – SAFE PATH TO KONICA MINOLTA **MULTIFUNCTIONAL SYSTEMS**

Advanced features available on today's MFPs, make it easy for information to be copied and distributed within and beyond actual and virtual corporate boundaries. The first logical step is to prevent unauthorized persons from operating an MFP at all. Preventive measures are needed firstly to control access to MFPs, and secondly to establish some kind of security policy reflecting how the devices are actually used in real life. Konica Minolta achieves this without restricting the user-friendliness of the systems in any way.

User authentication methods

The authentication path starts by setting down a policy defining and configuring users and groups allowed to work with an MFP device. This can include limitations to access rights, namely that some users are authorized while others are not, to use various functions such as color printing.

Authentication information can be stored either on the MFP (encrypted) or draw on existing data from the Windows Active Directory. Konica Minolta provides three basic technologies for user authentication:

Personal password
The password, an alphanumeric code with up to 8 characters, is entered at the MFP panel. These codes can be created for administrators and users. An important aspect is that they can be centrally managed.

ID card authentication
Most Konica Minolta devices can be fitted with an ID card reader. ID cards offer convenience and speed; it is simply a matter of placing the ID card on or near the reader interface to access and also to log out of the system.

Biometric finger vein scanner
This state-of-the-art design is an advance on more common fingerprint scanners. The system works by comparing the image of the scanned-in finger vein patterns with those in the memory. The finger vein is a biometric characteristic that is almost impossible to falsify, which makes it extremely reliable to identify a person based on an individual physical feature. Unlike fingerprint systems, the finger vein cannot be scanned without the person actually being present and alive. The biometric finger vein scanner means there is no need for people to remember passwords or carry cards.

Account tracking for more transparency

Since user control for security requires every user to log in to the output device, the data generated represents an efficient means of monitoring at a number of levels such as user, group and/or department. Whichever of the device functions is used, monochrome or color copy, scan or fax, b/w or color printing, they can all be tracked individually, either at the machine or remotely. Analysis and trending of this data provides robust information about MFP usage from a number of different viewpoints: the data can be applied to ensure compliance and to trace unauthorized access; above all, it allows usage to be monitored across the whole fleet of printers and MFPs in a corporate/business/ office landscape.

Individualize access with function restrictions

It is possible to limit various MFP functions on an individual user basis. All of the Konica Minolta access control and security functions not only offer greater security against threats that can result in financial and reputational damage; they can also be used as the basis for better governance and enhanced accountability.

Log information

Log information for access and usage of individual devices not only enables immediate detection of security breaches, it also facilitates accounting and cost allocation to users and departments. The administrator can individually review audits and job logs for different machine functions, including b/w and color printing and/or copying, incoming and outgoing faxes, and scanning. Many print controllers on Konica Minolta devices contain electronic job logs that record all print jobs sent to the output device. In addition, Konica Minolta's Job Log Utility can provide comprehensive electronic tracking logs of user activity.

DOCUMENT & DATA SECURITY – CONFIDENTIAL DATA AND INFORMATION SECURED BY KONICA MINOLTA

As MFPs and printers are often located in public areas, where they can be easily accessed an appropriate implementation of data security policies is essential. Sensitive data stored on the MFP hard disk over a period of time as well as confidential documents lying in the MFP output tray as printouts, are initially unprotected and might therefore fall into the wrong hands. To avoid this and ensure complete document and data security, Konica Minolta offers various security measures to secure user details and output contents.

Protect documents with secure printing

Output devices are considered a security risk that should not be underestimated: at the simplest level, documents lying in the output tray can after all be seen and read even by passers-by. There is no easier way for unauthorized persons to gain access to confidential information. The secure print functionality is a way of ensuring document confidentiality as the author sets a password as a security lock prior to the printing. Protected documents cannot be printed until the correct password is entered. This is a simple and very effective way of preventing confidential documents being accessed by the wrong person.

NO LOOPHOLES WITH HDD SECURITY

Most printers and MFPs are equipped with hard disks and memory that retain many gigabytes of possibly confidential data, collected over long periods. Dependable safeguards must therefore be in place to ensure the safekeeping of sensitive corporate information. In Konica Minolta systems, a number of overlapping and intermeshing features provide this assurance:

- **Auto delete function**
  The auto delete function erases data stored on the hard disk after a set period.

- **Password protection of internal HDD**
  The read-out of data, obviously including confidential data, on the hard disk requires password entry after HDD removal. The password is linked to the device. The data is therefore not accessible after the HDD is removed from the device.

- **HDD overwriting**
  The most secure method of formatting a hard disk is by overwriting the data. This is performed in accordance with a number of different methods conforming to various (e.g. military) specifications.

- **HDD encryption**
  On HDDs fitted to Konica Minolta devices the stored data can be encrypted using the Advanced Encryption Standard (AES) supporting a 256-bit key length. This feature satisfies corporate data security policies. Once an HDD is encrypted, the data cannot be read/retrieved, even if the HDD is physically removed from the MFP.

Printing with individual authentication

Touch & Print is based on authentication via finger vein scanner or ID card reader while ID & Print requires user authentication via ID and password. The job at hand is printed immediately after the user authenticates at the MFP by placing his ID card on the unit card reader or by ID confirmation using the finger vein scanner. The advantage of this particular feature is its speed: it waives the need for additional security print ID and password.

Curb unauthorized copying

The copy protection feature adds a watermark to prints and copies during the printing process. The watermark is barely visible on the original print, but if the document is copied, it moves from the background into the foreground to indicate that it is a copy.

Remain in control with Copy Guard

Copy Guard/Password Copy adds a concealed security watermark to the original during printing to prevent this from being copied. While barely visible on the protected original, it is not possible to copy this document again, because the device is blocked for this operation. The Password Copy feature can override Copy Guard and allows copies to be made when the correct password is entered at the MFP panel.

Smart PDF encryption

Encrypted PDFs are protected by a user password: permission to print or copy the PDF and permission to add PDF contents can be configured during the scanning phase at the MFP.

Useful PDF digital signature

With this feature, a digital signature can be added to the PDF during scanning. After a PDF is written, this allows monitoring any changes.

User box security

User boxes are available for single persons and/or for groups. They allow for any documents to be securely stored on the MFP hard disk before output of the print or copy job. User boxes can be protected using an eight-digit alphanumeric password. When the right password is entered, it is possible to access/view documents in the box. This system effectively limits access to confidential documents and data to those authorized.

Secure fax reception

When activated, any faxes received are kept confidential in a protected user box.

NETWORK SECURITY – SAFE NETWORK COMMUNICATION WITH KONICA MINOLTA

Konica Minolta's office devices are based on a concept of communication and connectivity. This complies with strict security standards concerning user access, encryption of data and protocols used for information transmission. Therefore, you can ensure your data will arrive to the desired destination secure and trustworthy.

User Authentication

Besides governing access to output devices, user authentication also prevents unauthorized users from accessing the network. With this feature, which can be configured to authenticate to the network or locally at the machine, every authorized user has a unique user ID and password.

SSL/TLS encryption

SSL and TLS encryption protects communication to and from output devices, covering online administration tools, the Enterprise Server and Active Directory transmissions, for example. This communication type prevents from man-in-the-middle attacks where the attacker would be able to record the data communication.

IPsec

Konica Minolta devices also support IPsec for the complete encryption of any network data transmitted to and from the multifunctional system. The IP security protocol encrypts the whole network communication between the local intranet (server, client PC) and the device itself.

IP address filtering

An internal basic firewall provides IP address filtering and control of protocol and port access. IP address filtering can be set at the machine: the network interface card of the multifunctional system can be programmed to only grant access to a specific IP address range from client PCs.

Ports and protocols secured by administrator

Ports and protocols can be opened, closed, enabled and disabled via the administration mode at the machine or remotely via Web Connection or Device Manager. As protection against unauthorized tampering with machine and network settings, the administrator mode itself is accessed by a 16-digit alphanumeric password, which can only be changed by the service engineer or from within the administration area.

Where required, a web interface closing functionality allows the disabling of the web interface, i.e. Web Connection, for all users. This limits web access to administrators, providing reliable protection against unauthorized persons tampering with settings, configurations, etc.

SMTP Authentication

SMTP Authentication (Simple Mail Transfer Protocol) provides advanced email security. When activated, SMTP will authorize a machine to send email. For those customers who do not host their email services, the use of an ISP mail server is possible and is supported by the machine. SMTP authentication is required by email service providers and for the prevention of spam. For secure communication it is also possible to combine POP before SMTP, APOP, SMTP authentication or encryption using SSL/ TLS.

S/MIME encryption

To secure email communication from the multifunctional system to certain recipients, the system supports S/MIME (Secure/ Multipurpose Internet Mail Extensions). S/MIME encrypts the email message and content with a security certificate. S/MIME certificates or encryption keys (public key) can be registered for email addresses stored in the system's address book. S/MIME encrypted emails can only be opened by the owner of the decryption key (private key).

Changing "From" address

When user authentication is activated, it is not possible to change the 'From' address. Despite the 'Changing From Address' function being enabled, The 'From' address of a scan-to-email job will always be the logged-in user's email address. This feature prevents spoofing and provides audit trails for administrators.

Manual Destination Prohibit

With the 'Manual Destination Prohibit' function, the direct input of an email address or scan destination is impossible. If this function is activated, only registered destinations from the internal system address book or LDAP can be used.

Fax line security

Advanced fax line security is ensured by the fax connection using only the fax protocol for communication – no other communication protocols are supported. Konica Minolta devices block any intrusion attempts as threats, including intrusions of a different protocol over public telephone lines, as well as any attempt to transmit data that cannot be decompressed as fax data.

Fax rerouting

Fax rerouting allows automatic forwarding of incoming faxes to any destination within the internal address book, including for example email addresses, or to the user boxes on the device's internal HDD. Storing incoming faxes in a user box is considerably safer, as there are no printed faxes to be seen in the output tray. This rerouting can also make the communication faster, as faxes reach their recipients sooner. Last but not least, it also helps to save paper – recipients can decide whether printing a fax is really necessary.

Network access control

Most Konica Minolta devices support the IEEE802.11x standard for network access control to WANs and LANs. These standards ensure a secure network by shutting down any network communications (e.g. DHCP or HTTP) to unauthorized devices, with the exception of authentication requests.

BE PREPARED FOR
THE EVERYDAY SECURITY RISKS!

It is important to remain aware of the fact that today no company or organization is immune to security risks – security breaches happen everywhere, all the time! However, prudent businesses look ahead and take the necessary precautions before it is too late. They ensure that the confidential data held by the hard disk and memory of digital printers, copiers and all-in-one equipment cannot be accessed in the first place, let alone tampered with.

Security-conscious company owners and managers ensure that their network is protected and that unauthorized access to information on the company's intranet is barred. Conscientious managers are also aware that the printers and copiers installed throughout the company can easily constitute the most serious of security gaps. If left unattended in the output tray, confidential information might get into the wrong hands and could easily leave the company, for example via scan to email or fax transmissions. Nevertheless, prudent managers and IT specialists guard against these risks by reliably limiting access to devices to those authorized and by guarding against the unattended output of any kind of prints.

Konica Minolta supports its customers' efforts to protect against security risks by allocating extensive engineering resources to the advanced development of security-related features for bizhub MFPs and printers. Konica Minolta thus provides customers with the technology required in today's security-conscious environments.

Whether a customer is concerned about network intrusion, data theft or compliance with regulations, or whether the issue centers on limiting access to devices or functionalities, Konica Minolta bizhub technology offers professional solutions for the detection and the prevention of security breaches. This is the level of comprehensive protection that customers from all industries and public authorities now expect.

KONICA MINOLTA

CK Document imaging
Tél. +352 26 380 1 | **Fax** +352 26 380 380
2, rue Léon Laval - Z.A. Am Bann
L-3372 Leudelange
ck-documentimaging.lu