



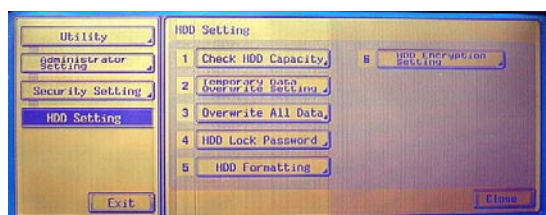
BUYERS LABORATORY INC.

Solutions Report—European Edition



A Buyers Laboratory Document Imaging Software Assessment

Konica Minolta Hard Drive Overwrite Function with Optional Encryption



Overall	★★★★★
Functionality	★★★★★
Encryption	★★★★★
Type of Jobs Protected	★★★★☆
Number of Overwrites	★★★★☆
Ease of Setup	★★★★★
Speed of Overwrite	★★★★★
Pricing*	★★★★☆

*Based on U.S. price structures

SOLUTIONS

Overview

In the last three years, virtually every manufacturer of copiers and MFPs has introduced some form of security for its devices. Common features include network authentication (users enter a user name and password in order to access the device), secure print (requires a password at the control panel to release a secure job) and data overwrite capability, which erases data stored in the MFP's memory or hard drive by overwriting it with a series of characters. The latter is generally available as an optional upgrade.

Buyers Lab has evaluated the hard drive overwrite function of a range of MFP vendors and has found that they vary considerably from vendor to vendor. For example, while the function is usually offered only as an optional upgrade from other vendors, Konica Minolta is taking a different approach. Instead of offering the hard drive overwrite capability as an optional upgrade, the company has embedded the function – and indeed, almost all of its security features – into the firmware itself, meaning users don't have to pay additional money for hard drive overwrite/sanitising capabilities. Overwrite is performed immediately upon completion of all copy, scan, fax and print jobs. In contrast, the sanitisation function is used only when a device is at the end of its useful life in a department, as it removes all settings from the machine in addition to removing all data.

The only security functions for Konica Minolta MFPs that are still chargeable options are a removable hard drive for the bizhub PRO 1050 and hard drive encryption capability (128-bit AES encryption) on any bizhub MFP.



“Our security is in our firmware,” said Olaf Lorenz, General Manager, Product Marketing Division - Konica Minolta Business Solutions Europe. “bizhub OP machines will all feature standard hard drive overwrite. It will be available for any machine available in the field as a no-charge upgrade. No hardware is involved and no memory has to be upgraded. The set specification will be 99 percent the same across the entire bizhub OP product line.”

BLI recently evaluated the hard drive overwrite function of Konica Minolta's security firmware as installed on the bizhub C450 model equipped with the latest firmware. The tested unit was configured with the Emperon Print System, which features a 40-GB hard drive. As of the time of testing, the bizhub C450 was under evaluation to achieve ISO 15408 Common Criteria certification at Evaluation Assurance Level (EAL) 3 (see “Understanding Common Criteria Certification” in this report), and Lorenz said that all bizhub products will be submitted for this certification going forward.

Konica Minolta's hard drive overwrite function offers exceptional value in that it is included as standard instead of offered as an option for which other vendors charge from \$400 to \$995. Because Konica Minolta offers the overwrite function as standard, buyers can add the encryption option and get the added security offered by both capabilities for a price that, at \$450, is among the lowest for hard drive overwrite options BLI has evaluated, which range in price from \$400 to \$600. Only two of the optional hard drive overwrite kits evaluated thus far offer encryption as part of the option, and both are priced higher. In addition, while its three overwrites after every job is competitive, it offers a choice of up to seven overwrites for “sanitising” the hard drive when the unit is being removed from a customer's location, which is more overwrites than offered by some competitive systems. Moreover, Konica Minolta's system offers superior ease of setup and use as compared to some competitive systems.

Value analysis was based on U.S. price structures and prices vary according to the country where the device is purchased.



Functionality



■ ENCRYPTION



As noted above, while the hard drive overwrite functions of two other vendors encrypt all information before storing it to the hard drive, Konica Minolta is like most vendors in that it does not support this functionality as standard. However, hard drive encryption is available as an option. In this way, only users who desire this extra level of protection need pay for it.

The optional SC-503 hard drive encryption kit encrypts all data stored on the hard disk drive, with selections including encryption priority or overwrite priority. It utilises the 128-bit Advanced Encryption Standard (AES) algorithm, which is a block cipher adopted as an encryption standard by the U.S. government. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. The AES

algorithm is sufficient to protect classified information up to the secret level. (Top secret information will require use of either the 192- or 256-bit key lengths.)

When the HDD encryption kit is attached and combined with the Temporary Data Overwrite function which comes standard with the machine, users will have a choice of not only “Mode 1” or “Mode 2” but also “encryption priority” or “overwrite priority.”

With encryption priority, data on the bizhub’s hard drive is completely overwritten and encrypted, including deleted data as well as remaining data stored on the hard drive. In contrast, overwrite priority completely overwrites deleted data, but does not encrypt it (though data stored on the hard drive is still encrypted).

Konica Minolta bizhub OP products with the newest firmware installed automatically encrypt all scanned documents into encrypted PDF format when they are sent from the machine to the destination. Data transmitted over the network is via encrypted PDF format, with recipients required to enter a password before they can open or print the encrypted file. The PDF Encryption function comes standard with the bizhub OP models and does not require the optional HDD encryption kit



Administrators can set encryption levels for scanned PDFs at Low or High, and can enable or disable the requirement for passwords and other permission for the encrypted PDF document.



■ TYPES OF JOBS PROTECTED



The Temporary Data Overwrite function, which is the standard firmware-based data security function on the tested unit overwrites all copy, print, scan and fax jobs, with data overwritten as soon as the job is completed. In addition, jobs archived on the drive are automatically overwritten upon deletion. It offers administrators a choice of two different types of overwriting methods supporting standards such as US Navy (NAVSO P-5239-26) (Mode 1), US Department of Defense (DoD 5220.22-M) (Mode 1) and US Air Force (AFSSI5020) (Mode 2).

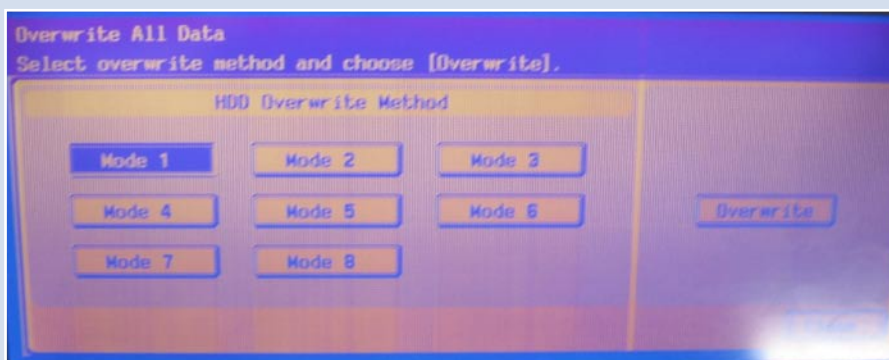
Jobs stored on the hard drive can be encrypted with the optional hard drive encryption kit. Data stored in RAM and ROM is not overwritten, which is on par with most competitive kits tested. Of the seven competitive kits tested by BLI thus far, three overwrite data stored in RAM, one of which also overwrites data stored in EEPROM. According to Lorenz, any data left in RAM is overwritten by the next job. Image data never touches Flash memory or ROM.



■ NUMBER OF OVERWRITES



The maximum number of overwrites available after each job is three, which is competitive with other systems. Users can choose between two methods of overwriting. But unlike with many systems, Konica Minolta’s hard drive overwrite function enables data to be overwritten up to seven times during sanitising.



At the control panel, administrators can select one of eight different overwrite methods.

During sanitising, administrators can select one of eight different methods of overwriting, with each mode meeting different security standards (10 standards in all). For example, one mode meets the standards set by the Japan Electronic and Information Technology Association, as well as the Russian Standard (GOST); another is the National Security Agency (NSA) standard; and another meets standards for the National Computer Security Center (NCSC-TG-025), U.S. Navy (NAVSO P-5329-26) and U.S. Department of Defense (DoD 5220.22-M). The number and type of overwrites performed varies according to the device itself, as well as by the method of overwriting selected by the administrator.

So how many overwrites is sufficient? BLI’s research indicates that the U.S. DoD originally recommended a three-pass overwrite algorithm standard for classified information but withdrew this requirement a few years ago due to a disagreement in the security community regarding how many times data on a hard disk should be overwritten, with some positing that one pass is good enough. According to Lorenz, “In a normal office environment, one is fine. A financial organisation might want three or four. For Area 51,” he said, jokingly referring to the rumored extra-terrestrial landing site in New Mexico, “they’d probably want data overwritten seven times.”



Ease of Use

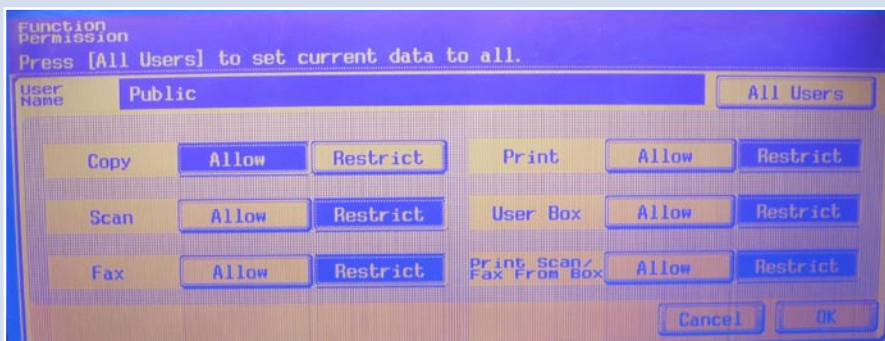


■ INSTALLATION ★★★★★

Installing the standard data security features is simple and consists of downloading and installing the firmware upgrade for machines not currently running the most recent version of the software. Although this generally requires a service visit, a service visit is typically required for other vendors' systems as well. No hardware is required, unlike with some other systems. Moreover, as it is considered routine maintenance and is part of the service contract, it does not cost customers additional money. The download and installation process takes about 20 minutes. It should also be noted that for units that ship with the latest version of the firmware (which Konica Minolta expects for all current bizhub models by Fall 2006), no installation is required.

■ ADMINISTRATOR SETUP ★★★★★

Only administrators can turn features on or off, with access via an eight-character alphanumeric password entered at the control panel. While this is a typical password length, note that a few systems offer longer, and therefore, more secure passwords of up to 12 or 32 characters. Administrators can only access and program the overwrite capability from the control panel. Some competitive kits allow administrators to access the overwriting functionality from the Web utility in addition to the control panel. Administrators can enable or disable specific functions (such as walk-up scan) and assign usage limits, as well as select the method of automatic overwriting used by the device. Setup of selections took only eight keystrokes, which is in contrast to other systems BLI evaluated, which typically require 13 or more keystrokes.



Specific functions can be allowed or restricted by administrators. In the example shown, any walk-up user can make a copy, but all other functions require user authentication.



■ SPEED OF OVERWRITE

★★★★★

Because the data overwrite is automatic after every printed or copied job, and occurs in the background while the machine is operational, BLI was unable to time the overwriting process on Konica Minolta bizhub units. (With some other units, users were blocked from using the control panel during the overwrite process, which can take up to six seconds for a typical office document or up to 32 seconds for a 120-page document.) However, in testing this overwrite solution, the machine remained operational at all times, with users able to continue printing, copying or programming jobs with no noticeable slowdown in any functionality.

The speed of overwrite during sanitising depends on the method used (i.e., the number of overwrites, from one to seven) and varies from a low of 31 minutes to a high of approximately three hours and 40 minutes, according to Konica Minolta.



■ PRICING

★★★★★

Of all the hard drive overwrite capabilities BLI has evaluated thus far, Konica Minolta's is the only one included standard. It is standard on all bizhub OP products. As of now, the newest firmware release (which enables the standard security features) is in the process of rolling out to Konica Minolta bizhub OP products including the monochrome bizhub 420, 500, 600 and 750 and the colour bizhub C300, C350, C351, C352 and C450 machines starting in July. Konica Minolta anticipates that all current bizhub machines will have the newest firmware releases by the fall of 2006. In contrast, the hard drive overwrite function offered by other vendors is an option generally ranging in price from approximately \$400 to \$600, and in one case, as high as \$995. Konica Minolta's strategy of offering security capabilities as standard demonstrates a strong commitment to security.

The fact that overwrite is standard means that users can also get optional hard disk drive encryption, priced at \$450, for a price that is comparable to that of optional kits that provide only overwrite functionality. BLI evaluated the standard Konica Minolta hard drive overwrite capability with the optional encryption capability included.

Value analysis was based on U.S. price structures and prices vary according to the country where the device is purchased.

Security Kit Demand

Lorenz told BLI he is heavily involved with major bid account sales. "Almost every bid that I see that's technologically oriented contains some questions about security," he said. "It could be from a financial institution, or government account, or hospital. In medium to large businesses, security is the word on the tip of everybody's tongue."



For example, he said, “I was in a meeting yesterday with a large insurance company. They were asking about security. I went to a bank and they were asking specific questions about security. Customers are becoming educated. They’re asking things about hard drive overwrite, such as how many times and what method is used.”

“More and more MFP products are used for electronic distribution of private, sensitive and confidential documents,” Lorenz says. Because of the nature of the jobs that get stored on the hard drive or distributed over the network, as well as the enhancements in the technology that distributes documents electronically, people are concerned that our ‘hubs of business’ that store and move electronic data have to comply with legislation that’s been enacted.

“I think our security helps sell the products,” he said, “especially in a major account, where the RFP says you have to have hard drive overwrite or user authentication. If you don’t have it, you’re out. With some customers, if we hadn’t had those features we wouldn’t have made the sale.”

Other bizhub Security Features

In addition to hard drive overwrite and hard disk sanitising, other security features available for Konica Minolta bizhub MFPs include:

Network Authentication with Support for LDAP — This capability ensures that all scan, fax and e-mail jobs are tagged to an authorised user. To perform one of these actions, the user must log onto the device with a user name and password, which is checked against a network server that holds the user’s credentials. In addition to allowing the administrator to control access to the device, network authentication also provides a way to track where and from whom documents have been sent. Authentication is via Windows Active Directory, Novell NDS and NT RAM Manager.

Standard Secure Mode — This mode can be enabled so that if the machine is in secure mode and someone tries to access it with a password unsuccessfully three times in a row, the machine will lock down. This requires that the machine be shut down and powered back up again, which is a deterrent to anyone trying to guess at passwords. If an authenticated user walks away and forgets to log out, after a preset amount of time the device reverts to secure mode and requires a password again.

Standard Scanning Encryption — This feature encrypts all scanned documents sent over the network as PDFs, which protects against the possibility of data being compromised during transmission.

IP Address Filtering — This feature allows administrators to tell the MFP to only accept communication from approved IP addresses, and to block specific IP addresses from accessing the device if required. A first level of defense against unauthorised use of the system, this can be applied to up to five different IP ranges.



Administrators can enable or block specific IP addresses from accessing the bizhub from the control panel.

Port Disablement — This lets users enable or disable ports, depending on their needs.

Hard Drive Lock — The hard drive is electronically keyed to the specific machine in which it is installed. If the hard drive is removed for any reason, it will not work on another machine unless a long (about 20 digits) passcode is entered. If the hard drive is not unlocked with its passcode, it will automatically lock down, even if installed in another Konica Minolta bizhub product.

Access Control — With this function, administrators can limit usage according to function. For example, the system can be set so any walk-up user can output black copies but only certain users can make colour copies (by entering a password).

Secure Watermark — Standard on colour bizhub products (the bizhub C250, C300 and C352), this feature adds a watermark to a secure document when a copy is made, adding administrator-specified text such as “Do not distribute.”

Secure Print — This feature allows users to apply a PIN that must be entered at the control panel to release and print sensitive documents. This is standard on Konica Minolta bizhub machines running at 20 ppm and higher.

Secure Fax — While firewalls work at the network periphery to prevent unauthorised access to a customer’s environment, unprotected fax connections in multifunction devices can be an open “back door” into the network. Konica Minolta devices protect access through the fax line with the capability to detect whether an incoming transmission is a valid fax reception and block access from other



incoming calls. Administrators can also block fax reception from unrecognisable phone numbers. Finally, incoming faxes can be routed to specific destinations (i.e., administrators can set all fax receptions from a specific phone number to automatically route to a pre-set e-mail address or user mailbox, or to multiple destinations), so sensitive faxes do not have to sit in the public access bin as they are received.

Removable Hard Drive — An optional upgrade available only for the bizhub PRO 1050, the removable hard drive can be locked into the device or removed for storage in a secure location.

Understanding Common Criteria Certification

With the proliferation of MFPs, the security risks these products pose to the network—whether through the telephone line connection or the retention of sensitive data on their hard drives—is justifiable cause for concern on the part of IT directors and business owners. To address the needs of government customers who are required to purchase products that adhere to certain security standards, as well as commercial customers concerned about security, office product vendors increasingly are having their products Common Criteria-certified.

The Common Criteria Evaluation and Validation Scheme is sponsored by a U.S. government program established by the National Information Assurance Partnership (NIAP), which is a collaboration between the National Security Agency (NSA) and the National Institute of Standards and Technology. Designed to meet the needs of both manufacturers and users, the program consists of evaluations conducted by accredited third-party commercial laboratories to evaluate products in accordance with the “International Common Criteria for Information Technology Security Evaluation” (ISO 15408), or Common Criteria for short. The program was established because so many commercial products that implement security features are used throughout all departments of the government.

According to the NIAP Web site (www.niap.nist.gov for U.S.-based certifications or www.commoncriteriaportal.org/public/consumer/ for non-U.S. certifications), the Common Criteria present a “general model for evaluation” and specify seven predefined Evaluated Assurance Levels (EALs), against which products’ functions are tested and evaluated. The Web site states that, “In general, the Department of Defense views EALs 1 and 2 as basic level assurance, Levels 3 and 4 as medium-level assurance and Levels 5 through 7 as high-level assurance.” We learned from our research that only EALs 1 through 4 are covered by an agreement whereby participating countries agree to recognise evaluations performed using the Common Criteria methodology in any of the other countries participating in the agreement. The reason for this is that the large



majority of commercial products are not designed for uses that would require these higher level certifications. Although NIAP does have testing methodology for these higher levels, there is not agreement on the methodology in the international community. In addition, the NSA is involved in these evaluations to protect classified information. The difference in the levels relates to how much time and digging into the design of the product is involved. Level 4, for example, requires that the vendor provide the lab with low-level design information, while a Level 2 evaluation allows the vendor to describe the way their product works in more general terms.

Does Certification Mean You're Secure?

Just because a product is Common Criteria-certified does not mean it has the government's stamp of approval as a secure device. What's important to realise is that Common Criteria certification simply means that the product evaluated was evaluated in accordance with the established methodology by a NIAP-accredited Common Criteria Testing Laboratory for specific security functionality specified by the vendor in a document called a "security target." The security target of every validated product, as well as the validation report, is available on the Web site, along with the list of all validated products and products under evaluation. Buyers are encouraged to review and compare vendors' security targets prior to making an acquisition in order to understand the security functionality of the product.

The security targets should help buyers understand exactly what a vendor is claiming to be Common Criteria-certified. For example, the Common Criteria certification earned by some products also covers the fax aspect of those products, validating the vendor's claim that the network cannot be accessed through the fax line.

The certifications cover exactly what is specified in the security targets and validation reports. So, if it's an MFP used in conjunction with a security option, the product that earns the certification is the exact configuration tested, with the exact same firmware. Later versions of a product would either have to be retested in order to earn certification, or through NIAP's Assurance Continuity program, a vendor would have to submit documentation regarding what changes have been made to the validated product and then, depending on what the changes are, the validation may be updated to cover the new version of the product, which will be indicated on the Web site, or it may be decided that the new version requires reevaluation in order to obtain certification.