SHARP®

IMAGER™ **security** solutions

Protect Your Business with Sharp's Comprehensive Document Security Solutions

"IT Friendliness" Award

BERTL's BEST 2005 Winner
Best Security Solutions

Digital
iMAGER™
Advanced Workgroup System

an overlooked security risk:
the office multifunction peripheral (MFP)

Today's office technology makes it incredibly easy for people to reproduce information. Unrestricted access to networked printers, multifunction devices, e-mail and the internet can put your business at considerable risk. With an increased emphasis on information and document security, every business and government agency needs to monitor and control network activity—including connected digital MFPs and network printers.

How are networked MFPs vulnerable?

Whenever pages are printed, copied, scanned or faxed, archived or e-mailed, your digital device retains data in the internal memory, which can be retrieved by unauthorized personnel just like the data on any PC's hard disk. Additionally, internal users who have unrestricted access to the device, or even sensitive documents inadvertently left in the paper tray, can lead to security breaches and information leaks.

Is your confidential information vulnerable?

Yes. With today's technology, there's been a significant increase in identity and intellectual property theft. Whether it's personal or financial information, health records, or protecting sensitive corporate data, it's critical to deploy a solution that provides heightened security and minimizes risk. Plus, with new federal, state, and local regulations regarding privacy and confidentiality, including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm Leach Bliley Act (GLB), information and document security are now a high priority for every business.

For additional information visit:
www.sharpusa.com/security

Protect all of your data with Sharp's Security Solutions.

At Sharp, we recognize the importance of information and document security. Sharp's advanced print controllers provide standard and optional security features that integrate seamlessly with Sharp's Digital IMAGER™ line of printers and MFPs. Our scalable solutions address a wide array of security concerns—including user authentication and document transmission. Whether you're in the financial, healthcare, accounting, legal or public sectors, Sharp's IMAGER Security Solutions offer a flexible menu of options that greatly reduce the risk of a security breach, thereby increasing your peace of mind.

Your greatest asset is information. Protect it with Sharp's Data Security Kit and IMAGER Security Solutions.

health
records
financial information
corporate
data
identity

The Sharp Data Security Kit:
the cornerstone of optimum security

Secure the Image Data:
Be sure you leave nothing behind.

Designed to protect your confidential information, Sharp's Data Security Kit works as a "digital shredder," offering several layers of advanced security. With both encryption and overwrite features, Sharp's Data Security Kit helps protect your confidential information from even the most sophisticated threats.

Data Encryption:
With 128-bit encryption, Sharp's Data Security Kit encrypts image data in the MFP before it's written to Hard Drive, RAM or ROM for print, copy, scan, or fax functions. This first layer of security provides peace of mind even while your documents are still active.

Automatic and Manual Memory Clear:
You can choose to have the Data Security Kit automatically overwrite all memory when the MFP is powered up, and/or after each print/copy/scan/fax job. Or, at any time, you can also choose to manually clear all memory for added versatility and control.

Data Overwrite:
Random numbers overwrite the information written to memory when a document is printed, copied, scanned or faxed. For the highest levels of security, Sharp's Data Security Kit can be set to perform up to seven overwrites—more than any other competitor to date.

• Hard disk overwrite for print, copy and scan functions
• RAM overwrite for print, copy and scan functions
• Flash ROM overwrite for fax function

don't just get security.
Get Sharp Security.

Sharp's Security solutions can help protect your company's most critical asset—information. With a "layered" security approach, including the Common Criteria Validated Data Security Kit, you'll get a flexible security solution designed specifically for your business— as well as the outstanding reliability of an award-winning digital MFP.

Standard Level	Heightened Level Includes Standard Level Solutions	Optimum Level Includes Heightened Level Solutions
Human Resources, General Office	IT Departments, Financial, Accounting, Healthcare, Insurance	Federal Agencies, Military, Research & Development, Legal
• Benefits • Confirm User Access Protect User Output	• Benefits • Eliminate the Latent Document Image Safeguard User Access	• Benefits • Audit User Activity Protection of Documents Even After Distribution
• Solutions • Secure the User (User Auth, Account Codes) Secure the Output (Confidential/PIN Printing)	• Solutions • Secure the Image Data (Data Security Kit) Secure the Network Access (IP/MAC Filtering)	• Solutions • Secure the Audit Trail (Equitrac Office™) Secure the Document Rights (FileSECURE™)

Sharp offers scalable document and information security solutions designed to meet a variety of security needs.

increase document protection
in a wide range of applications

Secure the User:
Control who is accessing your MFP.
Sharp IMAGERs **Account Codes** can be used to limit access to the device to only authorized users. For additional scan security, select Sharp IMAGERs can be configured to require that **users authenticate** onto the network before accessing the scanning functionality. This eliminates "anonymous" Scan to E-mail access. Additionally, you can have every Scan to E-mail saved in a custom mailbox, thereby providing a complete auditable record.

Secure the Output:
Protect your documents from roving eyes.
Sharp's **Confidential Print** feature minimizes the risk of sensitive documents being removed from the paper tray by unauthorized users. By utilizing a PIN number in both the Print Window and the MFP's LCD panel, users have greater control over when their documents are printed.
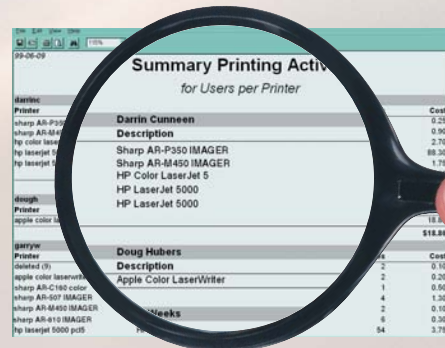
For an enterprise-wide solution, Equitrac Office offers **Secure Document Release** which holds sensitive documents on the print server—not the device itself—until an authorized user logs in and releases them directly to the MFP. This provides an added layer of security by requiring user log-in before releasing the document to the device.

Secure the Network Access:
Control how your MFP is accessed.
Enhance network security with Sharp's **Secure Network Interface Card (NIC)**. This security-enabled Ethernet card provides IP filtering, allowing administrators to restrict user access to the network printer or MFP and its embedded home page. It also enables administrators to disable protocols and close ports, thereby greatly reducing vulnerability to both external and internal threats.

Secure the Audit Trail:
Track network activity and usage.
With the ability to monitor all print and copy activity **Equitrac Office provides comprehensive reports for auditing** and details activity by user, device, department or billing code. Easily track every page that is printed and copied, and deter unauthorized use of network printers and MFPs.

Secure the Document Rights:
Protect and track files—
no matter where they are stored or sent.
AirZip's **FileSECURE** provides **persistent security** to sensitive information, enabling you to protect it everywhere it goes and every time it is accessed. All files are protected with both AES 256-bit encryption and file access permissions (View, Print, Copy and Control). Privileges can be easily designated to take effect and/or expire at specific times. The permissions can be modified after distribution, and each use of protected information is tracked. With this communication tool, secured files can now be distributed with confidence and used only as you permit.

To learn more about Sharp's Digital IMAGER and Sharp's suite of Security Solutions, call your Authorized Sharp Dealer today.

Sharp. **Leading the industry** with the first Common Criteria Validated Solution for document and information security

What is Common Criteria?

Common Criteria is an internationally recognized standard for evaluating the security claims of information systems, hardware, and software vendors (consistent with ISO 15408). By validating the claims of a manufacturer, these evaluations provide the highest certification standards—enabling businesses to streamline the selection process of printer/copier/scanner/fax systems.

Recognized by Federal agencies across the country, you can rely on Common Criteria validation to help you navigate today's security-conscious landscape—and get the best security solution for your business.

A Global First in the Industry

Sharp leads the industry with the first Common Criteria validated office equipment solution that addresses the document security needs of today's information age. As other companies are just beginning to address the security of their products, Sharp's third generation Common Criteria validated solutions are sophisticated, and protect your printed, copied, scanned, faxed and e-mailed documents.

Don't just get security. Get Sharp security.

Sharp's continuing high standards for office equipment security enable IT professionals to safely deploy digital office solutions—in any government or business environment.

In the United States, the Common Criteria program is administered by NIAP—the National Information Assurance Partnership—a collaboration between the National Security Agency and the National Institute of Standards and Technology.

Sharp Data Security Kit
Common **C**riteria
Validated
AR-FR4
Version M.20

The validation obtained by this product concerning the information security is the result of the evaluation based on the standard and method prescribed by the Target of Evaluation. It certifies that the product conforms to the security assurance requirements.

Sharp Network and Document Security Reference Chart

General Information	AR-M237/M277 Series	AR-M350/M450 Series	AR-M355/M455 Series	AR-M550/M620/M700 Series	AR-BC260 Series	AR-BC320 Series
Speed (PPM)	23/27ppm	35/45ppm	35/45ppm	55/62/70 ppm	26 b/w /17color ppm	32 b/w /26color ppm
Functions[1]	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax
Printer Controller	AR-P17	Standard[2]	Standard[2]	Standard[2]	Standard	Standard
Network Interface Card	AR-P17[3], AR-NC5J[3]	Standard[4]	Standard[4]	Standard[4]	Standard	Standard
Network Scanning Expansion Kit	AR-NS2	AR-NS2	AR-NS3	AR-NS3	AR-NS2	Standard
Facsimile Expansion Kit	AR-FX7	AR-FX5	AR-FX12	AR-FX8	AR-FX10	AR-FX10
Hard Disk Drive	-	AR-HD3	Standard[5]	Standard	Standard	Standard

Security Features

	AR-M237/M277 Series	AR-M350/M450 Series	AR-M355/M455 Series U / N Series	AR-M550/M620/M700 Series	AR-BC260 Series	AR-BC320 Series
SECURE THE USER						
Account Codes	Yes	Yes	Yes	Yes	Yes	Yes
User Authentication	LDAP	LDAP[14]	LDAP	LDAP	LDAP	LDAP
External Access Control	Optional[8,9,10]	Optional[8,9,10]	Optional[8,9,10]	Optional[8,9,10]	Optional[8,9,10]	Optional[8,9,10]
SECURE THE OUTPUT						
Confidential Print	Yes	Yes[6,7]	Yes	Yes	Yes	Yes
Secure Document Release	Optional[8,9]	Optional[8,9]	Optional[8,9]	Optional[8,9]	Optional[8,9]	Optional[8,9]
SECURE THE IMAGE DATA			U Series / N Series			
Commercial Data Security Kit	AR-FR12U	AR-FR4U	AR-FR22U / AR-FR21U	AR-FR11U	AR-FR23U	AR-FR20U
Common Criteria Data Security Kit	AR-FR12M[11]	AR-FR4M20	AR-FR22[11] / AR-FR21[11]	AR-FR11[11]	Not Applicable	Not Applicable
EAL Validation Level	EAL3+	EAL4	EAL3+ / EAL3	EAL3	-	-
DATA SECURITY KIT (DSK) FEATURES						
Functions[1]	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax
Encrypts Image Data	Fax Data Only	Yes[12]	Yes[12]	Yes[12]	No	No
Hard Disk Overwrite	Not Applicable	Yes	Yes	Yes	Yes	Yes
RAM Overwrite	Yes	Yes	Yes	Yes	Yes	Yes
FAX ROM Overwrite	Yes	Yes	Yes	Yes	Yes	Yes
HARD DRIVE OVERWRITE FEATURES	Not Applicable					
Encryption Key	-	Yes	Yes	Yes	Yes	Yes
# Overwrites	-	Up to 7	Up to 7	Up to 7	Up to 7	Up to 7
Overwrite Method	-	Random Data	Random Data	Random Data	Random Data	Random Data
Auto. Overwrite after each job	-	Yes	Yes	Yes	Yes	Yes
Auto. Overwrite at Start Up	-	Yes	Yes	Yes	Yes	Yes
Manual Overwrite	-	Yes	Yes	Yes	Yes	Yes
DOCUMENT FILING	Not Applicable	Not Applicable			Not Applicable	Not Applicable
Protection method without DSK	-	-	Folders and/or Document level password protection	Folders and/or Document level password protection	-	-
Protection method with DSK	-	-	Adds encryption	Adds encryption	-	-
SECURE THE NETWORK CONNECTION						
IP Filtering	Yes	Yes	Yes	Yes	No	No
MAC Address Filtering	Yes	Yes	Yes	Yes	No	No
Port Management	Yes	Yes	Yes	Yes	No	No
Password Protected Setup	Yes	Yes	Yes	Yes	Yes	Yes
SECURE THE AUDIT TRAIL						
Copy Audit Trail	Optional[8,9]	Optional[8,9]	Optional[8,9]	Optional[8,9]	Optional[8,9]	Optional[8,9]
Print Audit Trail	Optional[8]	Optional[8]	Optional[8]	Optional[8]	Optional[8]	Optional[8]
SCAN AUDIT TRAIL						
Scan to E-mail Auto Archive	Yes	No	Yes	Yes	Yes	Yes
FileSECURE™ Reporting	Optional[13]	Optional[13]	Optional[13]	Optional[13]	Optional[13]	Optional[13]
SECURE THE DOCUMENT						
Automatic Scan Secure	Optional[13]	Optional[13]	Optional[13]	Optional[13]	Optional[13]	Optional[13]
FileSECURE™	Optional[13]	Optional[13]	Optional[13]	Optional[13]	Optional[13]	Optional[13]
FILESECURE™ FEATURES						
Encryption Key	AES 256-bit	AES 256-bit	AES 256-bit	AES 256-bit	AES 256-bit	AES 256-bit
Privilege Levels	View, Print, Copy, Control	View, Print, Copy, Control	View, Print, Copy, Control	View, Print, Copy, Control	View, Print, Copy, Control	View, Print, Copy, Control
Time Availability Control	Yes	Yes	Yes	Yes	Yes	Yes
Recall	Yes	Yes	Yes	Yes	Yes	Yes
Reporting	Yes	Yes	Yes	Yes	Yes	Yes
Compression	Yes	Yes	Yes	Yes	Yes	Yes

1) Some functions require optional equipment.
2) Standard on N series. AR-M350/M450 U series requires (AR-P14) Printer Controller, AR-M355/M455 U series requires (AR-P21) Printer Controller, AR-M550/M620/M700 U series requires (AR-P19) Printer Controller.
3) RJ45 Network Interface included with the printer controller, certain operating systems and protocols may require (AR-NC5J) option.
4) Standard on N series. AR-M350/M450 U series requires (AR-NC5J) Network Interface Card (NIC), AR-M355/M455 U series and AR-M550/M620/M700 U series NIC is included with Printer Controller Option.
5) AR-M355/M455 also available without Hard Drive (AR-P20).
6) Requires AR-HD3.
7) Confidential Print feature is disabled when Data Security Kit is installed.
8) Requires Equitrac Office.
9) Requires PageCounter.
10) Requires Secure Document Release.
11) Available 2005.
12) FIPS 197 AES 128 Bit Encryption.
13) Requires FileSECURE™.
14) LDAP is not supported when AR-FR4M20 is installed.

SHARP
be sharp