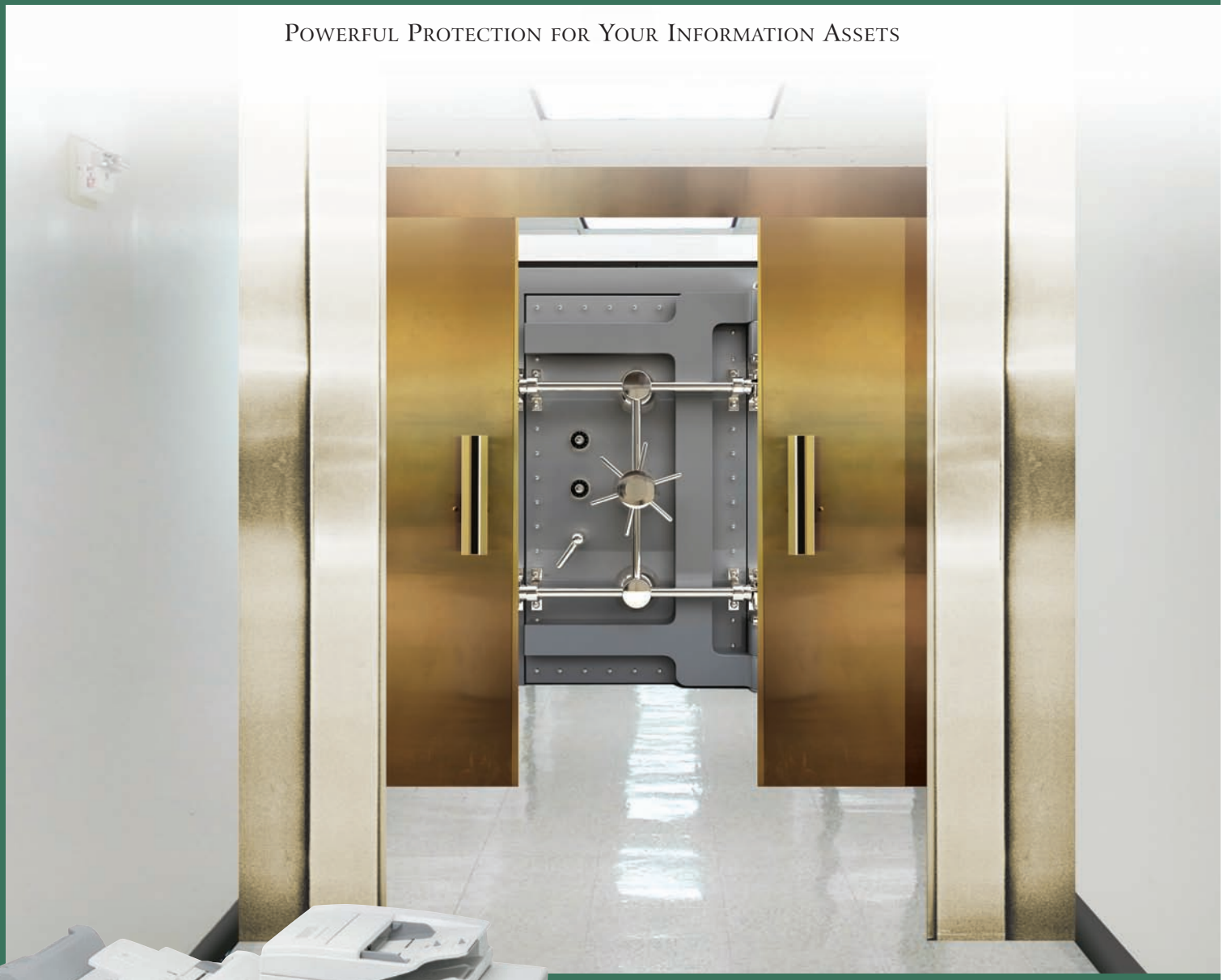
SHARP®

The Sharp Security Suite

Powerful Protection for Your Information Assets



2007 BERTL's BEST www.bertl.com

PICK of the YEAR 2006

2006 BERTL's BEST www.bertl.com

DATA SECURITY

THE LEADER IN DIGITAL INFORMATION SECURITY

Technology makes an ever-increasing contribution to profitability in today's highly competitive business landscape. However, the same technology that enables high productivity in the workplace can easily be compromised if not sufficiently secured. The consequences of inadequate protection could be financial loss, identity theft, risk to intellectual property, or even fines and criminal charges in the most severe cases.

Organizations spend significant capital to protect digital assets from threats, yet frequently overlook one of the most integral devices in use today — the office Multi-Function Peripheral (MFP). The more advanced and integrated MFPs become, the greater the risk to confidential information during the document's life cycle when it is being copied, printed, scanned or faxed. For a comprehensive security strategy to be effective, it is imperative for organizations to demand a greater level of protection from MFP vulnerabilities.

Sharp was the first to address security in digital imaging and received the first Common Criteria Validation for an MFP in 2001. Even today, Sharp remains the highest rated company in validated MFP products and is regarded as one of the industry's greatest security innovators. Businesses and government agencies worldwide have come to depend on this level of assurance, which Sharp pioneered and for which it continues to set the benchmark.

The Risks to Office Multifunction Peripherals

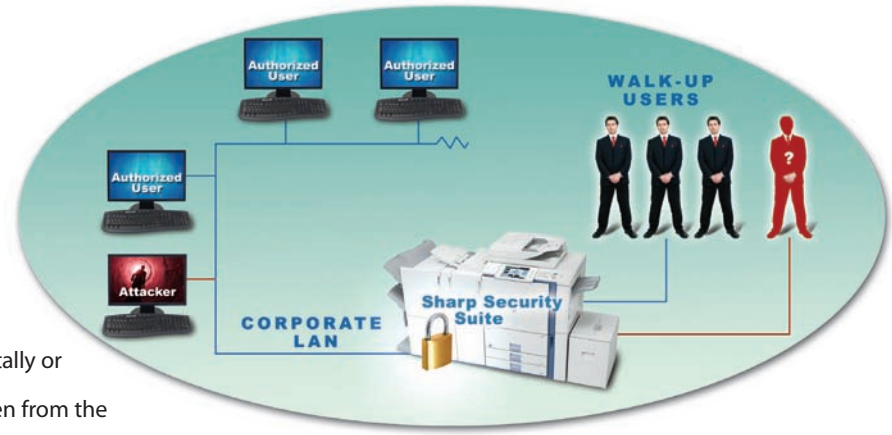
An MFP is a powerful asset in your office's environment. Left unsecured however, an MFP can pose one of the greatest threats to your organization. Just consider the types of documents that are copied, printed, faxed or scanned on a daily basis — personal information, financial statements, confidential reports, e-mails, memos, customer data, and employee information.

Intellectual property, private and personal information becomes portable once processed by an MFP, and is extremely susceptible to malicious use from both internal and external threats. While not all risks to confidential information are considered malicious, the potential for significant damage from inadequate protection can be only a matter of time.

Common Vulnerabilities

Some of the most common vulnerabilities associated with an unsecured MFP include:

- Loss of productivity
- Regulatory non-compliance
- Loss of access
- Stolen information
- Lawsuits
- Unauthorized use

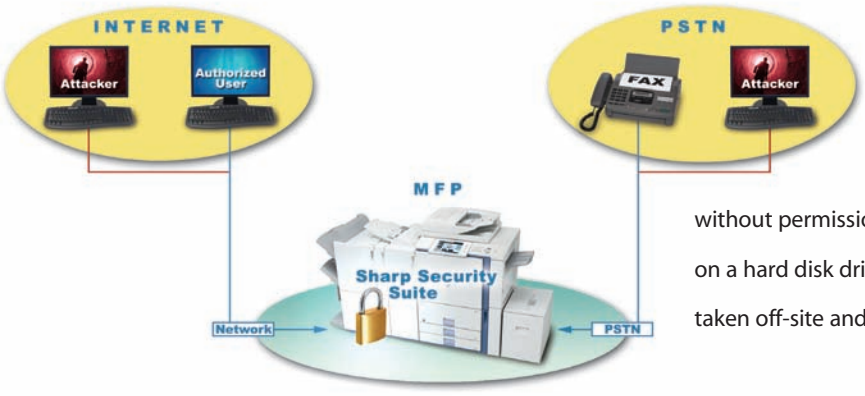


Internal Threats

At the device, confidential information can be accidentally or even purposefully copied from stored documents, taken from the output tray or faxed without authorization. Any information stored on a local desktop computer or accessible through the Local Area Network (LAN) can be printed without authorization.

External Threats

From across a Wide-Area Network (WAN), the Internet or a Virtual Private Network (VPN), information such as stored documents, scan data or print data can be intercepted. In the worst case, a user from the outside can obtain confidential information, unleash a Denial of Service (DOS) attack, or even place a virus on the device via the network or a phone line. Through a FAX line, or corporate LAN, communications could be intercepted or sent without permission anywhere in the world. Even MFP data stored on a hard disk drive or in memory could be compromised or even taken off-site and stolen if not protected.



PROTECTING YOUR ASSETS FROM VULNERABILITY

The Sharp Security Suite is effective at preventing unauthorized access to your most confidential information because security has been designed from the ground-up. At the core of the device is a proprietary embedded operating system that is resistant to attack from malicious code and virtually untouchable by viruses, worms or trojan horses. Around this impenetrable core, Sharp MFPs utilize a multi-layered approach to protection — providing better control over the users, devices, ports, protocols and applications that access your Sharp MFPs.

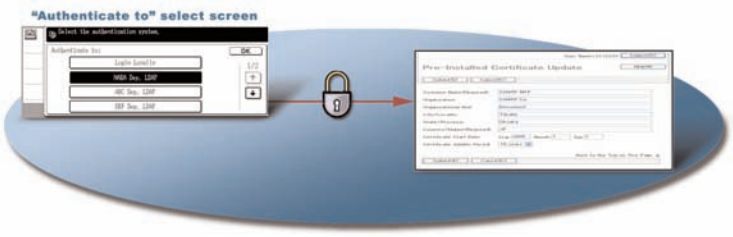
DATA SECURITY

The optional Data Security Kit (DSK) protects and controls the major MFP systems and subsystems (print, copy, scan, fax jobs, network settings, operating system, memory components, local user interface, engine and job controller).

The DSK uses the Advanced Encryption Standard (AES) algorithm on all data before it is written to RAM or Flash memory and the disk. The DSK also provides overwriting routines for deleted data, to ensure that all information is virtually irretrievable by unauthorized users.

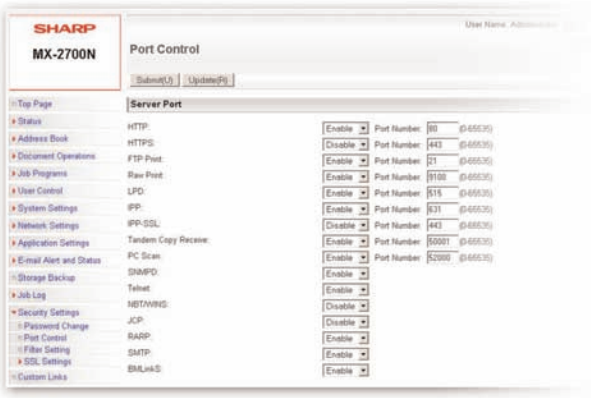
ACCESS CONTROL SECURITY

To limit unauthorized access to each device, Sharp MFPs can utilize account codes, user/group profiles, passwords, or external user accounts contained in an LDAP or Active Directory server. All user credentials are transferred using a proven combination of Kerberos, SSL or Digest-MD5 encryption to help avoid interception.



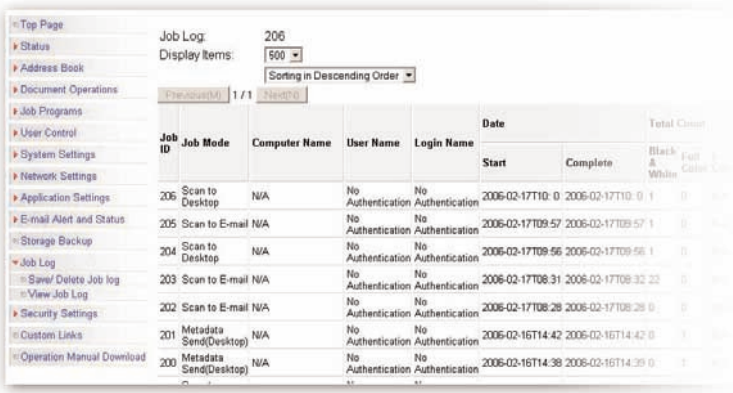
NETWORK SECURITY

Sharp MFPs feature an intelligent network interface that can limit access to specific computers on a network by IP or MAC address, and selectively enable or disable any protocol or service port on each device. All communications to and from the MFP can utilize Secure Socket Layer (SSL) for secure transmission over the network, and most devices also support SMB, IPv6*, IPSec* and SNMPv3.



*Q4 2007

Multi-Layered Security



Fax Security

The architecture of Sharp MFPs provides a logical separation between the fax telephone line and LAN. It is, therefore, virtually impossible for attackers to gain access to the internal systems of the MFP or the local network.

Document Security

Protection for all sensitive documents can be assured through Sharp encrypted PDF files for scanning and printing, or using SSL (Secure Socket Layer) protocols for scanning, printing, E-mail and setup.

Audit Trail Security

The Sharp MFP internal audit trail, and/or third party application software such as Equitrac Office,® provides comprehensive auditing of all user activity. Certain federal regulations parameters, such as 'to', 'from', 'when' and 'file name' can be logged, reviewed and archived for conformance.

Robust Security Solutions for Any Organization

Sharp MFPs have been rigorously tested and validated to provide the highest level of security protection available today. Sharp remains the first and only company to receive the highest achievable level of Common Criteria Validation for a complete MFP solution — Evaluation Assurance Level 4 (EAL4). While other vendors obtain certification for only individual components of an MFP at the lowest validated level, Sharp is committed to delivering the most comprehensive security solutions possible.

Security for the Public Sector and Government Sectors

With stronger control over all information access and dissemination, the highest level of privacy can be confidently assured for any governmental agency or department. Sharp MFPs have passed the most rigorous evaluations for commercial products available today, and meet the strictest requirements set forth in the National Security Telecommunications and Information Systems Security Policy (NSTISSP) #11 and DoD Directive 8500.1.

Private Sector Regulations and Privacy

Sharp MFPs provide robust, complete control over information access, transmission and tracking to facilitate compliance with stringent mandates. This will mitigate risk and help avoid any penalties or law suits for non-compliance.

By implementing the Sharp Security Suite, Sharp MFPs can help banks and investment institutions to meet the privacy requirements of the Gramm-Leach-Bliley (GLB) Act. Insurance and health providers can maintain Health Insurance Portability and Accountability (HIPPA) Act compliance with confidence. Businesses across all industries will benefit from the strict controls over financial information required under the Sarbanes-Oxley (SOX) Act.

Sharp MFP Security Levels

How Secure do you need to be?

Standard Level

Who should use it?

- General office
- SOHO
- Public offices

Benefits

- Confirm user access
- Protect user output
- Adds resistance to attack from malicious codes and viruses

Applications

- Access Control Security (accounts codes, PIN printing)
- Network Security (IP/Mac Filtering, Port/Protocol Management)

Heightened Level
(Includes Standard Level)

Who should use it?

- Enterprise companies
- Human Resources
- Financial
- Accounting
- Healthcare
- Insurance
- Legal
- Education

Benefits

- Virtually eliminates latent document images
- Helps protect stored documents
- Access control authentication
- Helps protect documents in transit
- Audit user activity

Applications

- Data Security Kit (DSK)
- Access Control Security (LDAP and active directory authentication)
- Document Security (document encryption)
- Network Security (data and traffic encryption)
- Audit Trail Security (internal and third party log file)

Optimum Level
(Includes Heightened Level)

Who should use it?

- Federal agencies, DOD, state offices
- Research & Development

Benefits

- Helps protect from attackers on fax lines
- Provides assurance claims
- Better user access control authentication

Applications

- Common Criteria Validation (CC DSK)
- Fax security (separation between fax and network lines)
- Network security (SSL Digital Certificate)

Common Criteria Validation

Common Criteria
Validated
Sharp Data Security Kit
MX-FRX1, Ver. M10 MX-FRX2, Ver. M10 MX-FRX3 Ver. M10

The Spectrum Benchmark

Common Criteria is an international standards evaluation program developed in the early 1990s to validate the Information Assurance claims of manufacturers. It provides a high level of confidence in the Security functions of the products evaluated. Today, Common Criteria Validation is recognized worldwide as a benchmark for technology products, and has become a requirement for the United States government and many others.

What is ISO 15408?

ISO 15408 (International Standard Organization 15408) refers to a set of evaluation standards for security products and systems established by the Common Criteria. This set of criteria is simply referred to as ISO 15408.

The World's First and Highest Rated MFPs

In 2001, Sharp became the world's first MFP manufacturer to achieve Common Criteria Certification for a data security kit and has since maintained the leadership position in the industry. As of March 2007, Sharp can claim no known vulnerabilities in the National Vulnerability Database (NVD) for an MFP. Sharp's commitment to continuous improvement has led to the release of the third-generation of Common Criteria validated MFPs, which have undergone a comprehensive review and achieved a level of EAL3+ and EAL4.

More Rigorous Testing Means Greater Assurance

Common Criteria evaluations for commercial security products range from EAL1 to EAL4. While many MFP manufacturers still only achieve EAL2 Validation for their products, Sharp MFPs are measured against a higher level of criteria for more meaningful results in real-world applications. To achieve a level of EAL3 and above, greater disclosure of product information must be provided to the government-controlled testing laboratory.

Sharp Network and Document Security Reference Chart

General Information	AR-M237/M277 series	AR-M257/M317 series	AR-M355/M455 series	MX-M350/M450 series	AR-M550/M620/M700 series	MX-M550/M620/M700 series	MX-M850/M950/M1100 series	MX-2300N/2700N series	MX-3501N/4501N MX-3500N series	MX-5500N/6200N/ 7000N series
Speed (PPM)	23/27ppm	25/31ppm	35/45ppm	35/45ppm	55/62/70 ppm	55/62/70 ppm	85/95/110 ppm	23/27 b/w / 23/27color ppm	35/45 b/w / 35color ppm	55/62/70 b/w / 41color 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	Print/Copy/Scan/Fax	Print/Scan/Copy/Fax	Print/Scan/Copy/Fax	Print/Scan/Copy/Fax
Printer Controller	AR-P17	AR-P27	Standard [2]	Standard [2]	Standard [2]	Standard [2]	MX-PBX2, MX-PKX4	Standard	Standard	Standard
Network Interface Card	AR-P17 [3] , AR-NC5J [3]	AR-P27	Standard [2]	Standard [2]	Standard [2]	Standard [2]	Standard	Standard	Standard	Standard
Network Scanning Expansion Kit	MX-NSX1	MX-NSX1	MX-NSX1	MX-NSX1	MX-NSX1	MX-NSX1	MX-NSX1	Standard	Standard	Standard
Facsimile Expansion Kit	AR-FX7	AR-FX7	AR-FX12	AR-FX12	AR-FX8	AR-FX8	MX-FXX1	MX-FX1	MX-FX2	MX-FX3
Hard Disk Drive	-	-	Standard [4]	Standard [4]	Standard	Standard	Standard	Standard	Standard	Standard
Security Features										
Access Control Security										
Account Codes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Comprehensive embedded user access control	No	No	No	No	No	No	Yes	Yes	Yes	Yes
User Authentication	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP
Confidential Print	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Follow You Printing™	Optional [5,6]	Optional [5,6]	Optional [5,6]	Optional [5,6]	Optional [5,6]	Optional [5,6]	Optional [5,6]	Optional [5,6]	Optional [5,6]	Optional [5,6]
External (3rd party) access control	Optional [7]	Optional [7]	Optional [7]	Optional [7]	Optional [7]	Optional [7]	Optional [7]	Optional [7]	Optional [7]	Optional [7]
Fax Security										
Confidential FAX	-	-	-	-	-	-	Yes	Yes	Yes	Yes
Separation between FAX and Network connections	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Filter Junk Fax	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data Security			U Series N Series	U Series N Series						
Commercial Data Security Kit	AR-FR12U	AR-FR24U/AR-FR25U	AR-FR22U AR-FR21U	MX-FRX7U MX-FRX6U	AR-FR11U	MX-FRX5U	MX-FRX8U[8]	MX-FRX1U	MX-FRX2U	MX-FRX3U
Common Criteria Data Security Kit	AR-FR12M	AR-FR24[9]/AR-FR25[9]	AR-FR22 AR-FR21	MX-FRX7[9] MX-FRX6[9]	AR-FR11	MX-FRX5[9]	MX-FRX8[9]	MX-FRX1	MX-FRX2	MX-FRX3[9]
EAL validation level	EAL3+	EAL3+	EAL3+	EAL3	EAL3	EAL3	EAL3	EAL3+	EAL3+	EAL3+
Data Security Kit 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	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax
Encrypts Image Data	Fax data only	Fax data only	Yes[10]	Yes[10]	Yes[10]	Yes[10]	Yes[10]	Yes[10]	Yes[10]	Yes[10]
Hard Disk Overwrite	Not Applicable	Not Applicable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RAM Overwrite	Yes	Yes	Yes[12]	Yes[12]	-	-	-	-	-	-
FAX ROM Overwrite	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to (DOS) Denial of Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to common Virus attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Document Control (Anti-Copy)	-	-	-	-	-	-	Yes	Yes	Yes	Yes
Lock user after 3 retries	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hard Drive Overwrite Features	Not Applicable	Not Applicable								
Encryption Key	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
# Overwrites	-	-	Up to 7	Up to 7	Up to 7	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	Random Data	Random Data	Random Data
Automatic Overwrite after each job	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automatic Overwrite at Start up	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Manual Overwrite	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Document Filing	Not Applicable	Not Applicable								
Protection method without DSK	-	-	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection
Protection method with DSK	-	-	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption
Network Security										
IP Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MAC Address Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Port Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password Protected Setup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPSec, IPv6	No	Yes[8]	No	Yes[8]	No	Yes[8]	Yes	Yes[8]	Yes[8]	Yes[8]
SNMPv3 and SMB Support	No	No	No	Yes[11]	No	Yes[11]	Yes	Yes	Yes	Yes
SSL	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Audit Trail Security										
Embedded Log File	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Equitrac® Copy Audit Trail	Optional[5,6]	Optional[5,6]	Optional[5,6]	Optional[5,6]	Optional[5,6]	Optional[5,6]	Optional[5,6]	Optional[5,6]	Optional[5,6]	Optional[5,6]
Equitrac® Print Audit Trail	Optional[5]	Optional[5]	Optional[5]	Optional[5]	Optional[5]	Optional[5]	Optional[5]	Optional[5]	Optional[5]	Optional[5]
Scan Audit Trail										
Scan to E-mail	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Document Security										
Scan Encrypted PDF file	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Print Encrypted PDF file	No	No	No	No	No	No	Yes	Yes	Yes	Yes

1 Some functions require optional equipment.
2 Standard on N series. MX-M350/M450 U series requires (MX-NBX3) Printer Controller, AR-M355/M455 U series requires (AR-P21) Printer Controller, MX-M550/M620/M700 U series requires (MX-NBX1), 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 MX-M350/M450 U come without Hard Disk (MX-NBX2 provides Printing and Scanning capabilities), AR-M355/M455 also available without Hard Drive (AR-P20)
5 Requires Equitrac Office® or Equitrac Express®.
6 Requires Equitrac for Sharp's MFPs or PageControl
7 3rd party applications for Sharp OSA platform
8 Availability - Late 2007
9 Availability - 2008
10 FIPS 197 AES Encryption.
11 Only for SMB.
12 For MFP without hard disk.

ENERGY STAR

SHARP®

SHARP ELECTRONICS CORPORATION
Sharp Plaza, Mahwah, NJ 07430-1163
1-800-BE-SHARP • www.sharpusa.com

Design and specifications subject to change without notice. Sharp, Sharp OSA and all related trademarks are trademarks or registered trademarks of Sharp Corporation and/or its affiliated companies.