

Hard Disk
Security
Printers,
multifunction
printers, and
copiers



Hard Disk Security for Printers, MFPs, and Copiers

What Resellers need to know to advise their customers.



Hard disk security

Risks, safeguards, and solutions

It's common knowledge that computers store information on hard disk drives.

What's not as well known is that some printers and most multifunction printers (MFPs) and copiers also contain hard disk drives that record and store data. Residual data that may remain on the disk after printing, copying, etc. could pose a risk.

Your customers' data at risk

Recent reports on the *CBS Evening News* and *60 Minutes* demonstrated the security risks to data stored on MFP hard disk drives. In their reports they recovered dozens of pages worth of confidential information stored on MFPs, warehoused in several used equipment facilities.

The purpose of this document is to help Xerox Resellers become experts on hard disk security. Understanding the potential risks and safeguards—and the advantages Xerox products provide—will help position you as a valued consultant for your customers.

Printer, MFP and copier hard disks

Digital information is transmitted to a printing device through a computer, over a network, by scanning, or through a telephone line. Most of the time this data is stored on a hard disk drive so the device can print quickly and multitask—provide more than one function (print/copy/scan) at the same time.

How to tell if your printer or MFP has a hard disk drive?

First, go to www.xerox.com/security and click on the *Data Protection: Image Overwrite, Encryption and Disk Removal* link to download the PDF. This document includes a list of Xerox products, indicates whether a hard disk is standard or optional, and which disk security features are included.

If the hard disk for your product is optional, there are two easy ways to find out if your specific model has a hard disk drive. From the printer or MFP's control panel, locate and print the page that lists the device's configuration information. Locate the entry for Hard Disk or Image Disk, as it's sometimes referred to.

An alternative if your device is networked, is to connect to its built-in web server by typing its network IP address into your web browser. Once connected, click on the **Properties** link or tab and review the hardware specs. Look for information on a Hard Disk or Image Disk.



How your customers can protect their data

From the introduction of our first digital products, Xerox recognized the potential security risks of stored data. The robust safeguards built into many of our products like Disk Image Overwrite and Data Encryption, ensure data security from installation and setup, through the productive life of the product, to its eventual recycling or disposition.

Disk Image Overwrite

The Disk Image Overwrite feature “scrubs” the disk drive in accordance with stringent specifications established by the US Department of Defense (DoD). This option became a standard feature on nearly every product in the Office portfolio in 2006.

The Disk Image Overwrite feature can be customized to remove all data from the disk according to customer needs:

- **Immediate**—automatic data overwrite as soon as printing is complete.
- **Scheduled**—automatic, daily data overwrite.
- **On Demand**—executed as needed, prior to disk removal, or for end-of-life device disposition.

Hard Disk Removal Program

Xerox also established a hard disk removal program for any Xerox product at ready for disposition. A Xerox technician will remove the disk and leave it with the customer. This program provides customers physical control of the disk and provides a secure solution for the minority of products without the Disk Image Overwrite feature. Contact Xerox Customer Support for more information on fees and availability in your geography.

Data encryption

In addition, most Xerox products equipped with disk drives also include our data encryption feature. When enabled, it encrypts all stored data with a state-of-the-art AES 128-bit encryption algorithm.

Safeguards for disposition

When a printer, MFP, or copier reaches its end of life, it’s ready to trade-in, recycle, donate, or dispose. But how can your customers be assured any residual intellectual or confidential property on the hard drive isn’t at risk? Here’s a simple process your customers should follow to protect their data for Xerox products:

1. Determine whether the printer, MFP, or copier being retired is equipped with a hard disk.
2. If the Xerox product is equipped with a hard disk, enable the Disk Image Overwrite function and “scrub” the disk.
3. If the product doesn’t include the Disk Image Overwrite function, customers may be able to use a third party software to overwrite the disk. They can also arrange removal of the hard disk by Xerox, enlist your help, or remove it themselves.
4. Xerox provides several venues for the disposition of used equipment including our Trade-In Program, product recycling, and donation referrals for equipment with some remaining usable life. It is in the customer’s best interest to ensure they have overwritten or removed the hard disk prior to the product leaving their facility. While Xerox will make every reasonable effort to safeguard any residual data that remains on a product provided for trade-in or recycling, we can not guarantee its safety. The best practice is for the customer to remove any confidential data prior to disposition.

For more information on product security see www.xerox.com/security

Security safeguards to look for when buying a new printer or MFP

- Hard disk drive image overwrite with a DoD-approved three-pass algorithm
- Hard disk drive data encryption with an AES encryption algorithm
- Hard disk removal option
- Network security support for SSL, IPsec, and SNMPv3
- Device authentication to control, manage, and track device access
- Secure fax
- Secure print feature
- Customer security alert process
- Secure product disposition process

Product/feature availability

A comprehensive list of Xerox products and their available security features is provided in the *Data Protection: Image Overwrite, Encryption and Disk Removal* document. Download the PDF at www.xerox.com/security



Hard disk security risks

Additional Xerox product security features

Beyond hard disk security

In addition to data storage protection, Xerox products provide robust safeguards for data as it's being used.

Network security

Xerox products are compatible with multiple network security protocols. The Secure Sockets Layer (SSL) protocol is used for secure job communication and reporting. The IPsec protocol protects network channels for DNS, DHCP, IPP, lpr, and Port 9100 printing. SNMPv3 is used for encrypted device management.

Securing device use

Firewall—a built-in firewall manages all communication access to authorized users.

Authentication—network authentication validates user names and/or passwords prior to device use. It can also be configured to allow or deny access to specific device functions such as scan, email, or fax functions. For additional security, the device may be configured to require log in by IT staff in order to change access or other configuration settings.

Internal audit log—Xerox MFPs and many of our printers can maintain audit logs to track activity by document, user, and function.

Ports and services—Unused ports and services can be shut off to prevent unauthorized use or malicious access.

Embedded fax

Unprotected fax connections in MFPs can be a back door into the network. Xerox was the first manufacturer to offer Common Criteria-certified products with fax internally separated from other network functions.

Securing the output tray

On a shared device in an office environment the output tray of a printer or MFP can be a security risk. Our Secure Print feature enables a user to send a job to print, where it will wait in the queue, until they enter a password (PIN) at the device to release the job. This feature is ideal for printing confidential documents securely on a workgroup device.

Robust security made easy

It's one thing to provide stringent security features and safeguards for MFPs and printers. But if they aren't easy to set-up and use, company data may continue to be at risk. Xerox makes system administration and device management easy. Our free software, CentreWare®Web, allows IT staff access to device configuration, control, and management over the network through an easy-to-use browser-based interface.

Additional data vulnerability

With all of the attention on digital information security, another critical point of potential security leaks may go unnoticed: paper documents. Paper documents are generally unsecured or locked in file cabinets. Often years worth of proprietary data is kept on file under minimal security in rows of file cabinets.

Xerox offers powerful scanning solutions that can automate the conversion of paper documents into secure, searchable digital archives. Storing your proprietary records digitally is not only more secure than paper documents, it's also more efficient and less expensive. Xerox scanning solutions provide an impressive ROI. They often pay for themselves in as little as six months.

For more information on Scan to PC Desktop®, ScanFlowStore®, and DocuShare® Express visit www.xerox.com/office/software-solutions

Security vigilance and alerts

Xerox is the only printer manufacturer with an active security patch program. We consistently monitor for new vulnerabilities on our MFPs, just as operating system software developers track new viruses that could threaten their software. Xerox security bulletins are posted on www.xerox.com/security. Customers can sign up for the RSS feed to be alerted immediately when a new bulletin or downloadable patch is posted.

For more information on Xerox security or to subscribe to our RSS security feed visit www.xerox.com/security

