xerox®

Xerox and Information Security

Protecting your data so you can focus on what matters: the success of your business or organization

SECGD-01UB

Table of Contents

1 Overview 1

2 Security Vulnerabilities: Industry Risks and Costs 3

3 The Xerox Security Model 7

- Network Security 9
- Document Security 12
- Data Security 14
- Authentication 17

4 Manufacturing and Supplier Security Practices 21

5 Product Security Evaluation 23

6 Risk Assessment and Mitigation 25

7 Product Returns and Disposals 27

8 Xerox Remote Services 29

9 Regulatory and Policy Compliance 35

10 Summary 37

11 Security Checklist 38

Overview

1

Information is every organization's key asset, and security is essential to the office—for documents and for any devices connected to the network. And in the 21st century, the network is the hub of virtually all business activity.

The threat is very real and the stakes are growing at exponential rates. A breach in the security of an organization's documents can result in unauthorized use of sensitive or proprietary information. It can lead to harmful disclosure, stolen or compromised intellectual property and trade secrets. And for many organizations, these security breaches can end with costly fines and litigation, to the tune of hundreds of thousands to millions of dollars.

When it comes to networked multifunction printers, or MFPs, additional vulnerabilities can be present because these devices can print, copy, scan to network destinations, send email attachments and handle incoming and outgoing fax transmissions. For those in IT, it's critical to the security of an organization's network to make sure that security infractions can't happen through network-connected MFPs—or at the devices themselves.

After all, attacks can originate in unexpected ways:

- The phone line attached to an MFP could be used to access the network
- The web server used to manage the MFPs and printers may be vulnerable to attack
- Unprotected electronic data can be inappropriately accessed while at rest on the hard disk, or in motion to/from the device
- Malicious emails can be sent from an MFP with no audit trail

A multifunction device is a sophisticated, multiple sub-system IT platform, and meaningful security measures must comprehend every element of the platform.

Most MFPs contain:

- One or more operating systems
- Network controller and firmware
- One or more hard disk drives
- Web server
- Page Description Language interpreters (PS & PCL)
- Local user interfaces
- Local hardware ports
- Fax system

This is a very different situation from the copiers of yesterday.

Just about anyone can launch attacks against a network and a company's information assets if an MFP's physical and electronic access isn't securely controlled and protected. Those attacks can be as simple as someone picking up documents left in the MFP's output tray, to malicious worms pulling sensitive documents off the network.

An MFP's entire system, along with any device management software on the network, must be evaluated and certified in order for IT and all the workers of an organization to be certain that their documents and network are safe and secure from information predators—or even from internal security breaches.

In that respect, not all MFPs are equal. Therefore, a comprehensive approach, based on foundational, functional, advanced and usable security, is critical to safeguarding the information assets of today's businesses.

Thankfully, Xerox has the security capabilities to help. For the last 20 years, Xerox has been a leader in providing secure document solutions to a variety of industries across the globe. In fact, every Xerox product and service we offer was designed with security in mind and to seamlessly integrate into existing security frameworks. Plus, security is managed throughout the entire product life cycle from requirements analysis, design, development, manufacturing, deployment, and disposal —giving you and your customers more protection and peace of mind.

At Xerox, we help protect your data at every potential point of vulnerability so you don't have to. We know that by staying focused on what we do best, you can stay focused on what you do best.

Xerox Security Goals

We've identified five key security goals in our quest to provide secure solutions to every one of our customers:

Confidentiality	Integrity	Availability	Accountability	Non-repudiation
• No unauthorized disclosure of data during processing, transmission, or storage	• No unauthorized alteration of data • System performs as intended, free from unauthorized manipulation	• Systems work properly • No denial of service for authorized users • Protection against unauthorized use of the system	• Actions of an entity can be traced directly to that entity	• Mutual assurance that the authenticity and integrity of network communications is maintained

Security Vulnerabilities: Industry Risks and Costs 2

It's amazing the lengths to which some will go to keep their workplaces safe while completely overlooking their multifunction devices. After all, MFPs are networked devices, complete with IP addresses and loaded with company-sensitive information—and potentially vulnerable to attack.

Imagine the costs and damages if your confidential data falls into the wrong hands. A breach in document security could result in unauthorized use or modification, harmful disclosure, or other unwanted outcomes.

According to Forrester's Global IT Budgets, Priorities, And Emerging Technology Tracking Survey, Q2 2010, upgrading the security environment has been a top priority for IT decision-makers for the past four years. In 2010, however, for the first time it is not only a top priority but a critical or high priority for 62% of IT decision-makers.[1]

According to a 2010 benchmark study of 51 U.S. companies about the financial impact, customer turnover and preventive solutions related to breaches of sensitive information, data breaches continue to cost organizations more every year. The average organizational cost of a data breach in 2010 increased to $7.2 million, up 7 percent from $6.8 million in 2009. Total breach costs have grown every year since 2006. Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from 2009.[2]

Security is not optional. Customer privacy concerns and government security regulations are changing the way many industries conduct business today.

Healthcare

Advances in information technology—including the use of handheld computers—have created the need to share important medical data and patient information electronically—and that's where security becomes a major concern.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was put in place by the federal government to force all healthcare organizations to apply uniform data management practices to protect patient information and patient privacy at all times. Under HIPAA, an audit trail is required to track who viewed data, when they viewed it, and if they had the proper authorization to do so.

The Health Information Technology for Economic and Clinical Health (HITECH) Act significantly expanded the U.S. government's efforts to establish a national electronic record keeping system for the healthcare industry. The act was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and meaningful use of health information technology.

Government

Today, local, state, and federal governments have put an emphasis on simplifying processes and improving cross-agency collaboration to provide better outcomes for the citizens they serve. To do so, they're employing various initiatives to take advantage of the latest technologies, while putting strict regulations in place to ensure the information being shared is safe and secure.

The Federal Information Security Management Act of 2002 (FISMA) was established to bolster computer and network security government-wide. It requires that all networked devices—including those used by contractors—meet strict information assurance goals such as integrity, confidentiality, and accountability.

Also, the Department of Defense has adopted additional security measures with the use of Common Access Cards (CAC) and their civilian government counterparts PIV (Personal Identity Verification) cards. Such cards require a PKI infrastructure to ensure a secure authentication and communications environment. Additionally, most Federal government agencies have adopted the FIPS 140-2 standard to certify encryption modules used in MFP products. And finally, most Federal government customers require products be certified to the Common Criteria standard.

Financial Services

Direct deposit, online banking, debit cards, and other advances in information technology are revolutionizing the financial services industry. Though more convenient for both customers and businesses, this heavy use of technology has its own set of security concerns.

The Gramm-Leach Bliley Financial Services Modernization Act of 1999 (GLBA) was instituted to ensure financial institutions that collect or receive private customer data have a security plan in place to protect it. To reach compliance, organizations must complete a risk analysis on their current processes and implement firewalls, restrict user access, monitor printing, and more.

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 further increases the need for accurate collection and reporting of financial data. Through the Office of Financial Research and member agencies, data will be collected and analyzed to identify and monitor emerging risks to the economy and make this information public in periodic reports and annual testimony to Congress.

Education

With today's educational institutions–including K-12, colleges, and universities–transcript requests, financial aid applications, and even class notes can all be found online. Because some schools have their own medical centers, they also have to store and share medical information electronically. This interactive environment enhances the student experience and improves staff productivity, but it also makes schools susceptible to security threats.

Because these institutions manage a variety of information, many state and federal regulations apply, including the Computer Fraud and Abuse Act, USA Patriot Act, HIPAA, and GLBA. However, the most applicable regulation to the education industry is the Family Education Rights and Privacy Act (FERPA).

This act prohibits the disclosure of personally identifiable education information without the written permission of the student or their guardian.

With so many regulatory and compliance measures to respond to, Xerox has looked to the federal government requirements, among others, as guidelines. By developing solutions that strive to meet the most stringent security standards, we can offer highly secure solutions to all of our customers—regardless of business sector.

1. “The New Threat Landscape: Proceed With Caution.” Forrester Research, Inc., August 2010.
2. “2010 Annual Study: US Cost of a Data Breach.” The Ponemon Institute, LLC, March 2011.

The Xerox Security Model

3

At Xerox, our "Security = Safety" philosophy drives the development of products, services and technologies that are infused with security at every level.

Security is front and center when engineering our "Smart MFPs." As a leader in the development of digital technology, Xerox has demonstrated a commitment to keeping digital information safe and secure by identifying potential vulnerabilities and proactively addressing them to limit risk. Customers have responded by looking to Xerox as a trusted provider of secure solutions that offer a host of standard and optional state-of-the-art security features.

The Xerox Security Development Lifecycle

The development of all Xerox products is guided by the Xerox Security Development Life Cycle process, which builds security into products during the design phase, ensures security through testing and certification, and updates security through ongoing maintenance. The Xerox security strategy consists of three pillars:

State-of-the-art Security Features
Multifunction devices are sophisticated, multiple sub-system network platforms, and Xerox offers the broadest range of security functionality on the market, including encryption, authentication, authorization per user, and auditing.

Certification
ISO 15408 Common Criteria for Information Technology Security Evaluation is the only internationally recognized standard for security certification. Xerox is one of the first manufacturers to seek and obtain certifications for "complete" devices. Because each element of the multifunction platform is a potential point of entry, meaningful security certification must comprehend all elements, including the operating systems, network interface, disk drive(s), web server, PDL interpreter(s), local user interface, local hardware ports, and fax system.

Maintenance
At Xerox, maintaining our multifunction devices' security throughout their lifespan requires ongoing diligence to ensure continuous protection against newly discovered exploits.

- Software updates issued on an ongoing basis
- RSS feed for notification when new security bulletins are released
- Rapid response to identified vulnerabilities
- Patches available at **www.xerox.com/security**
- Security configuration guidance
- Common Criteria information

The Xerox Security Model, in concert with the Xerox Security Development Lifecycle, is a commitment that all features and functions of the system, not just one or two, are safe and secure.

The Xerox Security Model includes four major points of focus:

	Network Security	Document Security
	• IP/MAC Address Filtering • SSL/TLS • Network ports On/Off • IPv6 • Digital Certificate • SNMPv3 • 802.1X (Wire/wireless) • Firewall • Fax/Network separation	• Secure Print • Encrypted PDF • Fax Forwarding to Email and Network • Fax Destination Confirmation • Digital Signatures • Glossmark • Check 21 • Resource Security
	Data Security	**Authentication**
	• HD Overwrite • Data Encryption • Volatile and Non-volatile Memory • Secure Fax • Scan to Mail Box Password Protection • S/MIME for Scan to Email • Job Log Conceal • Hard Disk Removal Program	• Network Authentication • Role Based Access • SMTP Authentication • Microsoft Active Directory Services • Smart Card, including Common Access Card, Personal Identity Verification (PIV) card, .Net, proximity card

Network Security

Many Xerox devices include features to protect the printer or MFP from unauthorized remote access and to protect the confidentiality of “data in motion,” specifically any print job that’s transmitted to the device via the network. These features include:

IP Address Filtering

Internet Protocol (IP) filtering allows for system administrators to create rules to accept or reject information coming to the MFP based on protocols, IP addresses, or ports. This gives the system administrator control over who can and cannot access the device.

Registered IP Addresses:
Available

Non-Registered IP Addresses:
Not available

Secure Socket Layer/Transport Layer Security

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over the Internet. TLS and SSL encrypt the segments of network connections above the Transport Layer, using symmetric cryptography for privacy and a keyed message authentication code for message reliability.

IPsec Encryption

Internet Protocol Security (IPsec) encrypts the connection between clients and printers at a level below standard print protocols such as LPR and Port 9100. IPsec is supported by a variety of PC operating systems including all modern versions of Microsoft Windows. IPsec is designed to provide the following security services:

- Traffic encryption (preventing unintended parties from reading private communications)
- Integrity validation (ensuring traffic has not been modified along its path)
- Peer authentication (ensuring that traffic is from a trusted party)
- Anti-replay (protecting against replay of the secure session)

Network Ports On/Off

With the Network Ports On/Off capability, unnecessary ports and services can be shut off to prevent unauthorized or malicious access. On smaller desktop devices, these options can be adjusted through their control panel or PC-based configuration software. On production devices, tools are provided to set security levels and disable specific ports and services.

IPv6

Internet Protocol version 6 (IPv6) is a protocol for routing network traffic and identifying network-connected devices. IPv6 provides significant security benefits to network users, administrators and application developers. Specifically, IPv6 integrates the IPsec suite of protocols.

Digital Certificates

Digital certificates are electronic documents that use a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

Xerox MFPs support two types of certificates: those from a certificate authority such as VeriSign, or your system administrator can create a self-signed certificate on the device itself. By setting up a certificate on your device, you can enable encryption for specific types of workflows.

The device can be configured for secure access with the SSL protocol, and the enablement of SSL provides encryption for all workflows where the device is used as an HTTPS server.

SNMPv3

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF).

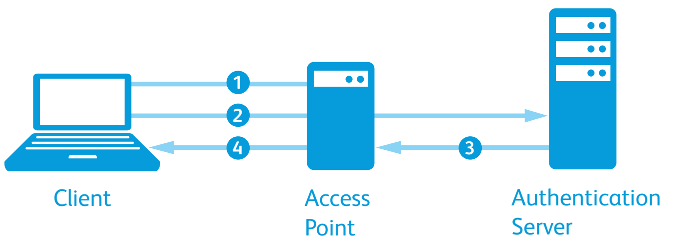
The SNMPv3 protocol provides significantly enhanced security functions including message encryption and authentication.

802.1X Authentication

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a local area network (LAN) or wireless local area network (WLAN).

How it works: 802.1X Authentication

802.1X authentication for wireless LANs provides centralized, server-based authentication of end users.



1. A client sends a "start" message to an access point, which requests the identity of the client.

2. The client replies with a response packet containing an identity, and the access point forwards the packet to an authentication server.

3. The authentication server sends an "accept" packet to the access point.

4. The access point places the client port in authorized state, and traffic is allowed to proceed.

The 802.1X protocol has become more prevalent with the increased popularity of wireless networks. Many organizations lock down port access to their internal networks using this protocol. This prevents any information from passing onto the network until the device is authenticated. From a risk management perspective, this allows for both wireless and wired devices to prove who they are before any information is passed through to the network. If unauthorized access is attempted the port is locked down until unlocked by the system administrator.

The Extensible Authentication Protocol (EAP) is an authentication framework that performs its functions as part of 802.1X authentication. EAP types currently supported by Xerox MFPs:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2

Firewall

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of rules and other criteria.

A built-in firewall manager allows Xerox MFPs to manage all communication access to authorized users, and restrict access via IP filtering, domain filtering, and port blocking.

Fax and Network Separation

Separating the fax interface from the network controller eliminates the security risk of hacking into an office network via the fax line.

The MFP does not provide a function to access the network via the fax phone line. The Fax Class 1 protocol used on the MFP only responds to fax commands that allow the exchange of fax data. The data passed from the client PC can only be compressed image data with destination information. Any data other than image information (such as a virus, security code, or a control code that directly accesses the network) is abandoned at this stage, and the MFP immediately ends the call. Thus, there is no mechanism by which to access the network subsystem via the fax line.

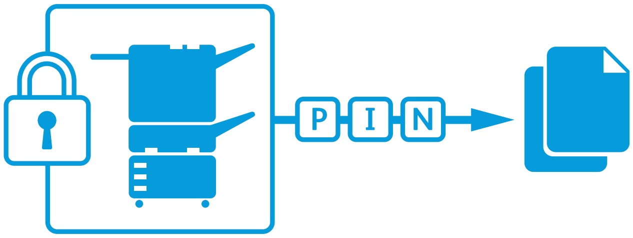
Document Security

Even when all necessary network security measures are in place to effectively protect critical data as it travels between users' computers and office printing devices, security technologies must also ensure that your sensitive hard-copy documents are received and viewed only by their intended recipients.

Xerox employs the latest technologies to safeguard your output, whether printing hard copies or distributing electronic documents.

Secure Print

Sensitive print jobs are held at the printer or MFP until the document owner releases them by entering their unique PIN through the device's front panel user interface. This ensures that a document's intended recipient is physically present when printing sensitive information, and can immediately remove the output from the printer or MFP before exposing it to other device users.



Secure printing based on Common Access Card (CAC)/Personal Identity Verification (PIV) card technologies attaches the print-job sender's identity certificate to their print job. At the device the user must authenticate with their CAC/PIV card before the job will be released.

Encrypted PDF/Password-protected PDF

When scanning a hard copy document for electronic distribution via the Scan to Email feature, Xerox MFPs can create encrypted and password-protected PDFs, which are then securely transmitted over the network, and can be opened only by those who possess the correct password.

Fax Forwarding to Email and Network

Xerox MFPs with fax forwarding capability can route incoming faxes to specific recipients' email in-boxes and/or to a secure network repository, where they can be accessed only by authorized viewers.

Fax Destination Confirmation

A fax sender receives automated confirmation that their fax was successfully received by their intended recipient.

Digital Signatures

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives the recipient confidence to believe that the message was created by a known sender, and that it was not altered in transit.

Secure Watermarks

Xerox printers and MFPs with the Secure Watermark feature help you prevent original printouts with sensitive information from being copied. If a document with a Secure Watermark is copied, the watermark image becomes visible, making it apparent that the document contains sensitive information and has been illegally duplicated.

Check 21

Xerox helps our customers comply with “Check 21” — a government regulation that became mandatory for all financial institutions in October 2004. Xerox is working with financial institutions and other partners to reduce the risk of fraud when legitimate checks are scanned, printed and reused illegitimately as “substitute checks.” This security feature is not limited to checks, but extends to other types of sensitive documents, such as legal contracts.

Resource Security

Allows password control on check-related resources such as fonts, logos and signatures, which are encrypted when not in use. Each supervisor has a unique password and can log in remotely to allow an operator to run a job. Resource Security is available for LCDS/Metacode, PCL or PostScript jobs.

User/Time/Date Stamp

Through the Xerox Global Print Driver®, a user/date/time stamp can be applied to any document printed by any networked device. This provides an audit trail of who printed what, and at what time.

Data Security

Technology has transformed the way employees conduct business. Today, documents take shape in not only the traditional hard copy forms, including handwritten notes and draft versions of paper communications, but also in electronic forms on desktops and in email. Because employees create, store, share and distribute these electronic documents differently than traditional paper documents, this information may be subject to new types of risk. To remain competitive, a company must address these threats by securing the documents and document management systems that contain a company's most valuable asset—knowledge.

Information and document management systems face a wide range of security threats. These threats include intentional espionage acts such as computer hacking, theft, fraud and sabotage, as well as unintentional acts such as human error and natural disasters. Information security is more than protection. It is about ensuring timely access and availability of document content to improve business process and performance. It is also about managing original content and complying with federal regulations.

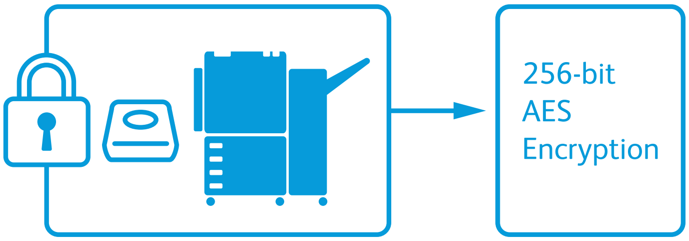
From the introduction of the first digital products Xerox has recognized the risk of retained data being inappropriately recovered from non-volatile storage and built features and countermeasures into our devices to help customers safeguard their data.

Hard Disk Encryption

Using advanced 256-bit AES Encryption, hard disk encryption protects your Xerox MFP's data at rest from unauthorized access.

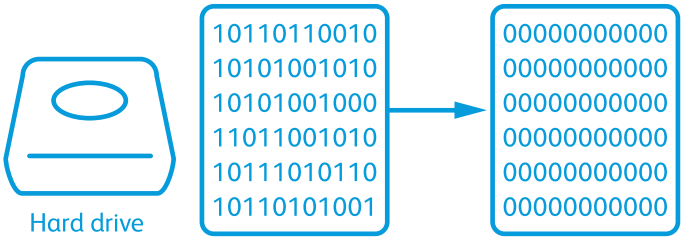
- AES 256 bit encryption, FIPS (Federal Information Processing Standard) 140-2 Validated
- All data is encrypted before it is stored on the hard disk

AES is a small, fast, hard-to crack-encryption standard and is suitable for a wide range of devices or applications. It is the state-of-the-art combination of security, performance, efficiency, ease of implementation and flexibility.



Hard Disk Overwrite

Hard disk overwrite removes data from your Xerox MFP's hard drive once the data is no longer needed. Hard disk overwrite ensures that latent images are removed completely from your MFP's hard drive after each task has been performed. Plus, overwrite software employs a Department of Defense-approved algorithm, per DoDD 5220.22-M



Volatile and Non-volatile Memory

Within every Xerox MFP, the controller includes volatile memory (RAM) and non-volatile memory (hard disk). With volatile memory, all data is lost upon shutdown or system reboot. With non-volatile memory, data typically is stored either in flash or on the MFP's hard drive, and is preserved until it is erased.

As concerns for data security increase, customers want to know how and where data can be compromised. Statements of Volatility are documents created to help identify where customer job data is located in Xerox devices. A Statement of Volatility describes the locations, capacities, and contents of volatile and non-volatile memory devices within in a given Xerox device.

Statements of Volatility have been created for many Xerox devices to help security-conscious customers. These documents may be obtained by contacting your local Xerox support team (for existing customers) or a Xerox sales professional (for new customers).

Secure Fax

Sensitive incoming faxes are held until released by the intended recipient at the device.

Scan to Mailbox Password Protection

When using and MFP's Scan to Mailbox feature, the designated mailbox can be password protected to ensure only those authorized can access the scans stored within. Scan to mailbox security is further enhanced by ensuring that the hard-disk data partition is encrypted.

S/MIME for Scan to Email

Secure/Multipurpose Internet Mail Extensions (S/MIME) provides the following cryptographic security services for the Scan to Email feature: authentication; message integrity and non-repudiation of origin (using digital signatures); and privacy and data security (using encryption).

In S/MIME communication, when sending data to the network, a signature is added to each mail message based on the certificate information retained in the device. Encryption is performed when sending data based on the certificate corresponding to each mail message's designated address. The certificate is verified when data transmission is designated as well as when the data is to be sent. S/MIME communication is conducted only when the certificate's validity is confirmed.

Scan to Email Encryption

Email encryption via Smart Card Authentication allows users to send up to 100 encrypted emails to multiple recipients in an organization's LDAP directory using the recipients' public keys. Users may view certificates of potential recipients prior to sending email. The MFP disallows sending to users without an encryption certificate. Also, the MFP logs all records of email sent with an option for the administrator to receive confirmation reports.

Job Log Conceal

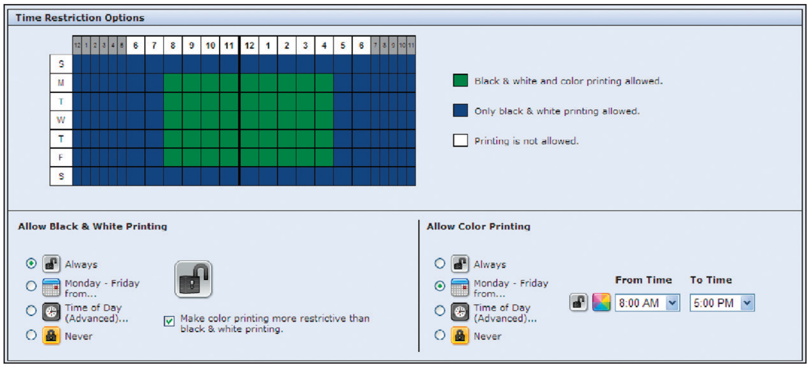
Hides job details when non-authorized users view job queue.

Hard Disk Removal Program

Xerox has developed a disk removal program so that prior to a device being returned a Xerox technician will remove the disks and leave them with the customer. This program charges a flat fee per machine for the service.

Print Restrictions

The User Permissions for Printing feature allows an administrator, using local device users and groups, to restrict printing based on specific criteria.



Time Restriction Options

	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
S	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
M	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦
W	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦
T	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦
F	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦
S	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

🟩 Black & white and color printing allowed.

🟦 Only black & white printing allowed.

□ Printing is not allowed.

Allow Black & White Printing

● Always
○ Monday - Friday from...
○ Time of Day (Advanced)...
○ Never

☑ Make color printing more restrictive than black & white printing.

Allow Color Printing

○ Always
● Monday - Friday from...
○ Time of Day (Advanced)...
○ Never

From Time: 8:00 AM
To Time: 5:00 PM

System administrators can set user restrictions by user and group.
The above interface shows where time-based restrictions are configured.

PostScript Passwords

Another printing-related area of risk is when printing with the PostScript page description language (PDL). PostScript includes commands that allow print jobs to change the printer's default behaviors, which could expose the device. Because, the PostScript language includes very powerful utilities that could be used to compromise an MFP's security, administrators can configure the device so that PostScript jobs are required to include a password to change the printer's default behaviors. The basic privileges of the PostScript interpreter within the controller are limited by design, but administrators have some capability to manage the operation of the PostScript subsystem.

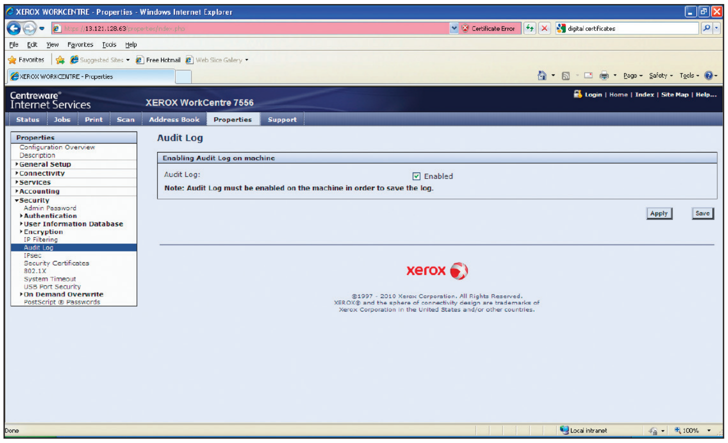
Audit Log

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

The audit log can be enabled or disabled by the system administrator, and can track access and attempted access to the device.

An example of an audit log entry:

"User xx logged into the Xerox WorkCentre MFP at 12:48 AM and faxed 10 pages to 888.123.1234."



Audit Log

Enabling Audit Log on machine

Audit Log: ☑ Enabled

Note: Audit Log must be enabled on the machine in order to save the log.

©1997 - 2010 Xerox Corporation. All Rights Reserved.
XEROX® and the sphere of connectivity design are trademarks of Xerox Corporation in the United States and/or other countries.

The Audit Log interface is accessed from a system administrator's workstation using any standard web browser.

Authentication

Authentication is the basis for granting access to Xerox multifunction devices for authorized users. Once authenticated, the user can interact with the MFP or access customer data, subject to restrictions based on the user's role.

Xerox MFPs employ a variety of authentication technologies to ensure authorized access to device features and functions by users and other network devices.

Network Authentication

By validating user names and passwords prior to use, network authentication restricts workers' access to scan, email and fax features as needed.

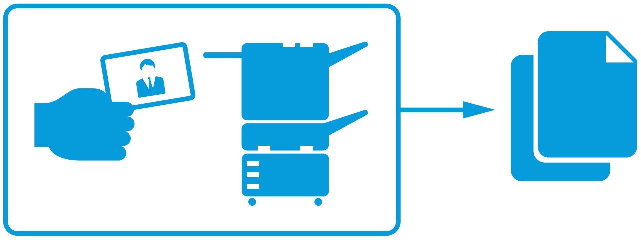
Role Based Access Control (RBAC)

The RBAC feature ensures that authenticated users are assigned to a role of User, Operator, or Administrator. Each role has associated privileges with appropriate levels of access to features, jobs and print queue attributes.

User **Operator** **Administrator**

Smart Card Authentication

Also known as Proximity Card or Contactless Smart Card Authentication, Xerox Smart Card Authentication protects your MFP from unauthorized walk-up access. With Smart Card Authentication, users can be authenticated using a two-factor identification system—possession of the card and a personal identification number entered at the MFP's user interface—to gain access to the walkup features at the device and on the network.



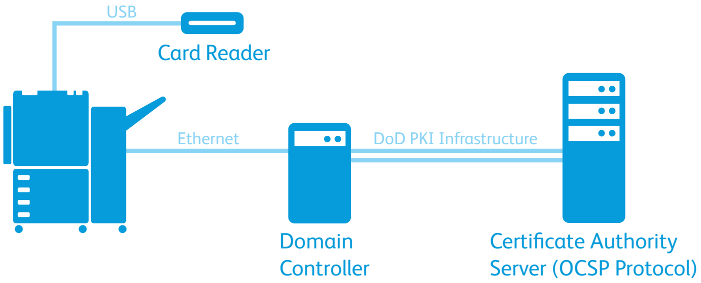
The Common Access Card/Personal Identity Verification (CAC/PIV) is a U.S. Department of Defense smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-government employees, and eligible contractor personnel. The CAC/PIV can be used for general identification, controlled building access and for authentication of personal computers, in addition to MFPs and the networks that connect them.

The Xerox 144k CAC/PIV is a version of the smart card. Users can be authenticated using two-factor identification to gain access to walk-up services at the device.

The Xerox 144k CAC/PIV provides the following benefits:

- Scan to Email S/MIME encryption to self or any recipient in the MFP's LDAP address book
- Digital signing using the Email Signing Certificate from the user's card
- Automatic population of the 'To:' field when using the MFP's Scan to Email function
- Up to 2048-bit certificate key
- Restrict outgoing transmissions to recipients with valid certificates
- Receive email confirmation reports and maintain audit logs
- Single sign-on to Scan to Home and LDAP
- 256-bit hard disk encryption
- Support for both IPv4 and IPv6 networks

Configuration Diagram for Common Access Card authentication



1.	2.	3.	4.
A card is inserted into reader and the user is prompted to enter their PIN at the MFP.	The MFP validates with the Validation Authority the "Chain of Trust" of the Domain Controller and the OCSP certificate by ensuring they were created by the Root Directory.	The MFP initiates an encrypted challenge/response dialog between the Domain Controller and the Common Access Card. If successful the Domain Controller issues a 'Ticket Granting Ticket' and authorization is complete.	Authorization unlocks Walkup MFP features: • Scan to Email • Copy • Fax • Custom Services • Network Scanning

LDAP Authentication

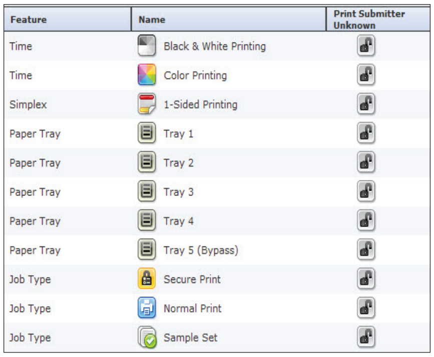
LDAP authentication requires the LDAP client to first tell the LDAP server who is going to be accessing the data so the server can decide what the client is allowed to see and do. If the client authenticates successfully to the LDAP server, then when the server subsequently receives a request from the client, it will check whether the client is allowed to perform the request.

Microsoft Active Directory Services

The Microsoft Active Directory Services (ADS) feature enables the device to authenticate user accounts against a centralized user account database, instead of exclusively using the user account database that is managed locally at the device.

User Permissions

Xerox user permissions provide the ability to restrict access to print features by user, by group, by time of day, and by application. Users and groups can be set up with varying levels of access to print features. For example, limits can be set that allow color print jobs only during certain hours of the day; PowerPoint presentations automatically print in duplex mode; or Outlook e-mails always print in black-and- white.



Feature	Name	Print Submitter Unknown
Time	Black & White Printing	🔓
Time	Color Printing	🔓
Simplex	1-Sided Printing	🔓
Paper Tray	Tray 1	🔓
Paper Tray	Tray 2	🔓
Paper Tray	Tray 3	🔓
Paper Tray	Tray 4	🔓
Paper Tray	Tray 5 (Bypass)	🔓
Job Type	Secure Print	🔓
Job Type	Normal Print	🔓
Job Type	Sample Set	🔓

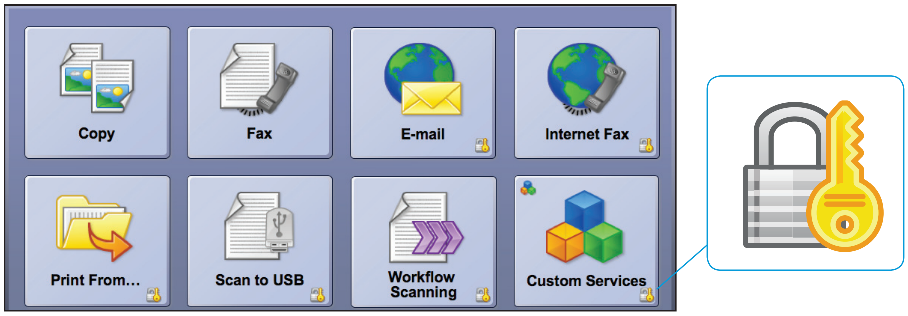
Set color user permissions and other print restrictions with intuitive graphical interfaces.

Secure Access

Secure access is an authentication mechanism that leverages your existing building access cards to unlock a Xerox MFP. This optional authentication system is considered “convenience authentication,” because the feature enables the convenient swiping of an end user’s existing ID badge. The system verifies the user’s authentication and then unlocks the device for use. This is more convenient to the end user versus typing in their username and password at the device.

A server is located between the device and the LDAP/AD server, and passes authentication information back and forth between it and the MFP. The feature also allows the added security of two-factor authentication, which requires the end user to swipe their card and then enter a PIN before the device is unlocked.

As a side benefit, this capability enables the Follow-You-Printing feature. Follow-You-Printing allows a user to submit their print job to the network and then retrieve that document from any networked MFP, anywhere in the world, that includes the same convenience-authentication swipe card capability.



A touch-screen user interface from a Xerox WorkCentre MFP shows how IT administrators can choose to require authentication for specific walk-up features and functions.

Manufacturing and Supplier Security Practices

4

Xerox and our major manufacturing partners are members of the Electronic Industry Citizenship Coalition (**http://www.eicc.info**). By subscribing to the EICC Code of Conduct, Xerox and other companies demonstrate that they maintain stringent oversight of their manufacturing processes.

Also, Xerox has contractual relationships with its primary and secondary suppliers that allow Xerox to conduct on-site audits to ensure the integrity of the process down to the component level.

Xerox also is a member of the US Customer Agency Trade Partnership Against Terrorism (**http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat**). This initiative is focused on supply-chain security. Examples of practices adopted by Xerox under this program are those put in place to counter theft or hijacking. Within North America, all trailers moving between the factory and the product distribution centers (PDCs), and between the PDCs and Carrier Logistics Centers (CLCs), are sealed at the point of origin. All trucks have GPS locators installed and are continuously monitored.

Product Security Evaluation

5

Document security means peace of mind. One of the hallmarks of the Xerox multifunction product line is a commitment to information security. Our systems, software and services comprehend and conform to recognized industry standards and the latest governmental security regulations.

Common Criteria Certification

Common Criteria Certification provides independent, objective validation of the reliability, quality, and trustworthiness of IT products. It is a standard that customers can rely on to help them make informed decisions about their IT purchases. Common Criteria sets specific information assurance goals including strict levels of integrity, confidentiality, and availability for systems and data, accountability at the individual level, and assurance that all goals are met. Common Criteria Certification is a requirement of hardware and software devices used by federal government on national security systems.

Achieving Common Criteria Certification

Common Criteria Certification is a rigorous process that includes product testing by a third-party laboratory that has been accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform evaluation of products against security requirements. Products are tested against functional security requirements based on predefined Evaluations Assurance Levels (EALs).

For healthcare, financial services and other industries, the need for security is no less important. Whether they are protecting their customers' privacy, or intellectual and financial assets, assurance that networks, hard drives and phone lines are safe and secure from hackers, viruses and other malicious activities is critical. Common Criteria Certification, while not a requirement outside the federal government, can provide independent validation.

With approximately 150 devices having completed the certification process, Xerox has the most Common Criteria Certified MFPs of any manufacturer. Plus, Xerox is the only vendor to receive certification for each device's entire system, rather than a kit or specific feature.

Visit **www.xerox.com/information-security/common-criteria-certified/** to see which Xerox MFPs have achieved Common Criteria Certification.

Members of the Common Criteria Recognition Agreement

- Australia (CA)
- Austria
- Canada (CA)
- Czech Republic
- Denmark
- Finland
- France (CA)
- Germany (CA)
- Greece
- Hungary
- India
- Israel
- Italy (CA)
- Japan (CA)
- Korea (CA)
- Malaysia
- Netherlands (CA)
- New Zealand (CA)
- Norway (CA)
- Pakistan
- Singapore
- Spain (CA)
- Sweden (CA)
- Turkey
- United Kingdom (CA)
- United States (CA)

CA = Certificate Authoring

Risk Assessment and Mitigation

6

Proactive Security for Emergent Threats

Offering you the market's most secure products and solutions today is just part of our story. Our scientists and engineers are hard at work developing the next generation of innovative security technologies to combat tomorrow's threats and keep your documents safe. DataGlyph® technology, micro-printing, fluorescence and infrared print security, Glossmark®, Correlation Marks print mark technology, and erasable paper, just to name a few. Other things Xerox does:

Keep a close eye on the latest risks
We closely monitor vulnerability clearinghouses to keep up to date on the latest information—so you don't have to.

Issue security bulletins
We're proactive in providing you with security patches when necessary, keeping your equipment up to date and your data safe.

Distribute RSS feeds
Up-to-the-minute updates are automatically distributed to customers' RSS feed readers.

Provide you with a wealth of information
If you want to learn more on your own, we offer an ever-expanding library of security articles, white papers and guides.

Visit **www.xerox.com/security** to access our full breadth of security resources.

Xerox manages security problems through identification, analysis, prioritization, coding, and testing. In addition to our own extensive internal testing, Xerox regularly monitors vulnerability clearinghouses made available by such entities and resources as US-CERT, CVE, and Oracle Critical Patch Updates report; Microsoft Security Bulletins, for various software and operating system vulnerabilities; and bugtraq, SANS.org and secunia.com for open source vulnerabilities. A robust internal security testing program is also engaged that involves vulnerability analysis and penetration testing to provide fully tested patches. Visit **www.xerox.com/security** to read the Xerox Vulnerability Management and Disclosure Policy from the Xerox Security web site.

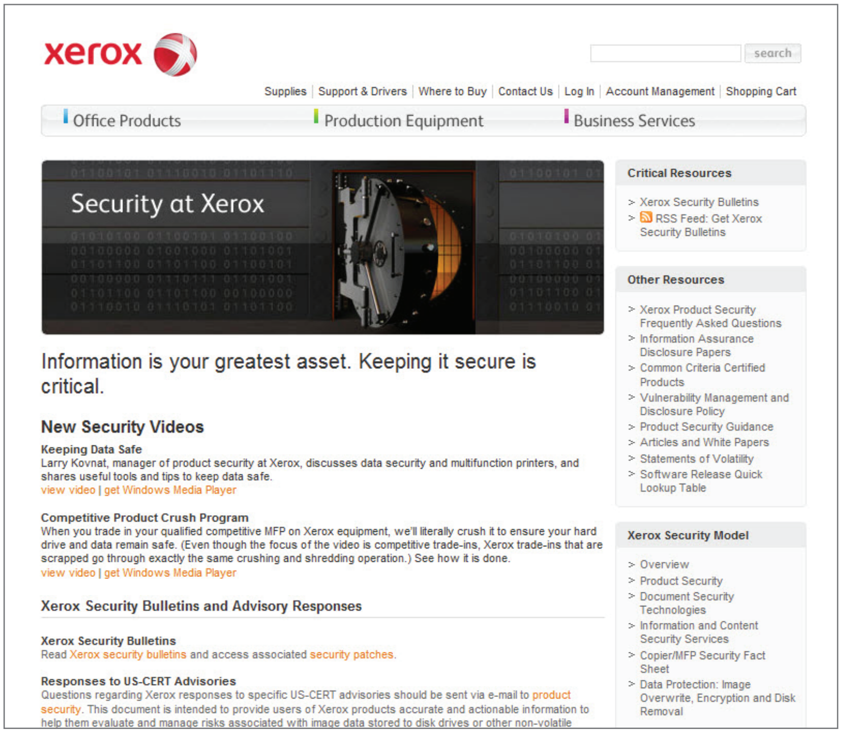
Xerox Security Bulletins and Patch Deployment

Xerox developers follow a formal security development life cycle that manages security problems through identification, analysis, prioritization, coding, and testing. We strive to provide patches as expediently as possible based on the nature, origin and severity of the vulnerability. Depending on the severity of the vulnerability, the size of the patch, and the product, the patch may be deployed separately or take the form of a new release of software for that product.

Depending on which Xerox product requires a patch, customers can download security patches from the Xerox web site at **www.xerox.com/security**. For other Xerox products, the security patch will be made available as part of a new release version of system software. You can register to receive bulletins regularly. In the US, customers should sign up for the Xerox security RSS feed. Outside the US, contact your local Xerox support center.

From the Xerox.com/security website, you have access to timely information updates and important resources:

- Xerox Security Bulletins
- RSS Feed: Get Xerox Security Bulletins
- Xerox Product Security Frequently Asked Questions
- Information Assurance Disclosure Papers
- Common Criteria Certified Products
- Vulnerability Management and Disclosure Policy
- Product Security Guidance
- Articles and White Papers
- Statements of Volatility
- Software Release Quick Lookup Table
- FTC Guide for digital Copiers and MFPs


xerox
search
Supplies | Support & Drivers | Where to Buy | Contact Us | Log In | Account Management | Shopping Cart
Office Products
Production Equipment
Business Services
Security at Xerox

Information is your greatest asset. Keeping it secure is critical.

New Security Videos

Keeping Data Safe
Larry Kovnat, manager of product security at Xerox, discusses data security and multifunction printers, and shares useful tools and tips to keep data safe.
view video | get Windows Media Player

Competitive Product Crush Program
When you trade in your qualified competitive MFP on Xerox equipment, we'll literally crush it to ensure your hard drive and data remain safe. (Even though the focus of the video is competitive trade-ins, Xerox trade-ins that are scrapped go through exactly the same crushing and shredding operation.) See how it is done.
view video | get Windows Media Player

Xerox Security Bulletins and Advisory Responses

Xerox Security Bulletins
Read Xerox security bulletins and access associated security patches.

Responses to US-CERT Advisories
Questions regarding Xerox responses to specific US-CERT advisories should be sent via e-mail to product security. This document is intended to provide users of Xerox products accurate and actionable information to help them evaluate and manage risks associated with image data stored to disk drives or other non-volatile

Critical Resources
> Xerox Security Bulletins
> RSS Feed: Get Xerox Security Bulletins

Other Resources
> Xerox Product Security Frequently Asked Questions
> Information Assurance Disclosure Papers
> Common Criteria Certified Products
> Vulnerability Management and Disclosure Policy
> Product Security Guidance
> Articles and White Papers
> Statements of Volatility
> Software Release Quick Lookup Table

Xerox Security Model
> Overview
> Product Security
> Document Security Technologies
> Information and Content Security Services
> Copier/MFP Security Fact Sheet
> Data Protection: Image Overwrite, Encryption and Disk Removal

The Security section of Xerox.com is your portal to a diverse breadth of security-related information and updates, including bulletins, white papers, patches and much more.

Product Returns and Disposals

7

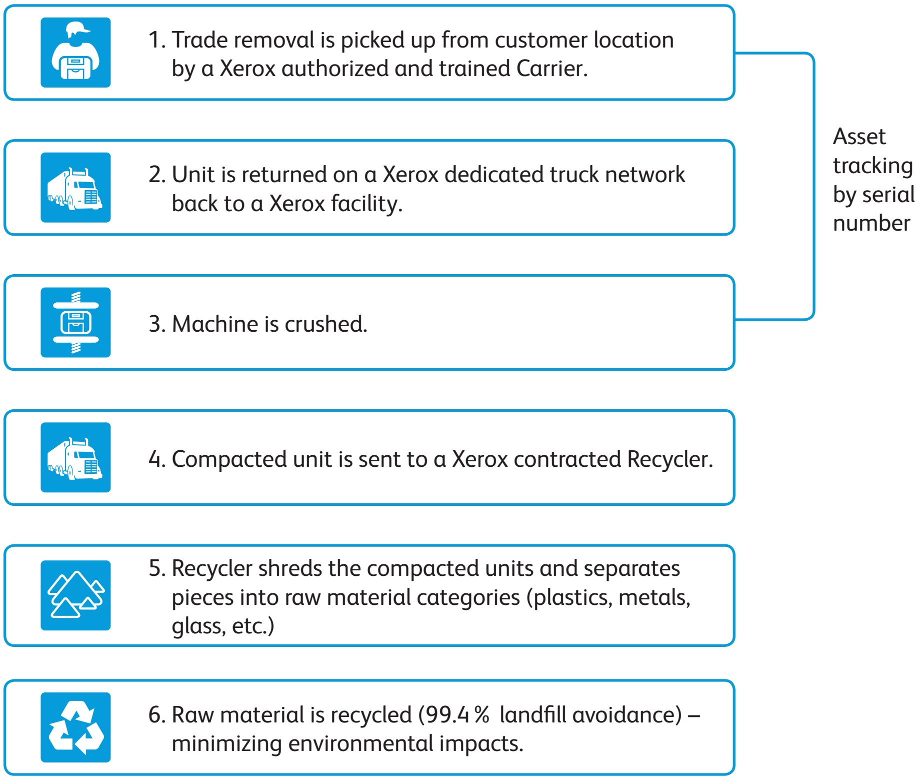
A Competitive Trade-in Option to Address MFP Security Concerns

If a customer trades their Xerox or competitive equipment with us as part of a new MFP implementation, we will make any residual customer data inaccessible. The Xerox process includes picking-up the competitive equipment from the customer's site and maintaining possession of it until drop-off at the destruction facility. Xerox tracks the equipment while it's in our possession to ensure the integrity of the process until the entire unit is crushed, including the hard drive.

This end-to-end process gives our customers peace of mind that their data is protected when trading-in their current non-Xerox equipment for new Xerox equipment. In order to reduce program costs and to continue to offer this service free-of-charge, Xerox does not provide a written guarantee that customers' data has been destroyed. However, we manage this comprehensive program to ensure the highest-possible level of confidence that all left-over data has been rendered inaccessible without adding expensive tracking/auditing/sampling processes. We are reviewing additional cost options should a customer have the need for both a high level of confidence in the destruction process and official documentation for auditing purposes.

Additionally, virtually all new Xerox MFPs come standard with 256-bit AES disk encryption as well as 3-pass disk overwrite features to ensure our customer's data is protected from day one on their new equipment.

Equipment Trade — Xerox Reverse Logistics and Asset Disposal



1. Trade removal is picked up from customer location by a Xerox authorized and trained Carrier.
2. Unit is returned on a Xerox dedicated truck network back to a Xerox facility.
3. Machine is crushed.
4. Compacted unit is sent to a Xerox contracted Recycler.
5. Recycler shreds the compacted units and separates pieces into raw material categories (plastics, metals, glass, etc.)
6. Raw material is recycled (99.4 % landfill avoidance) – minimizing environmental impacts.

Asset tracking by serial number

Xerox Remote Services

8

Xerox is responsive to your security concerns. Xerox Remote Services are designed to avoid making networks more susceptible to viruses. Remote Services transactions always originate from the device, based on authorizations made by you. Remote Services can only communicate with a secure server at Xerox that conforms to the stringent requirements of the internal Xerox Corporation information management infrastructure. You do not need to make any changes to Internet firewalls, proxy servers, or other security infrastructure.

Xerox systems are designed to integrate within your workflows. They connect to the network and push machine data to Xerox Communication servers where the information can be reviewed and analyzed to be used to evaluate service issues as well as to automate billing and supplies replenishment. This built-in knowledge-sharing feature of Xerox systems is what makes Xerox Remote Services viable and its approach unique.

Xerox Remote Services helps differentiate Xerox machine performance and support from other equipment suppliers. While other vendors may remotely monitor some of their machines, Xerox has developed integrated systems and remote tools, and coupled them with highly skilled Xerox support teams who are tasked with working to make you more productive and satisfied. This combination creates a high-value Remote Services capability that provides proactive problem resolution, and a robust underlying knowledge of your needs.

A key enabler for creating these support processes is the ability to transmit machine performance data back to the Xerox infrastructure.

The Results Are Tangible

- Transmitting machine data translates to faster preventative maintenance, predicts machine failure and reduces the cycle time to fix problems.
- A multitude of engineering tools leverage data to monitor your machine's health and performance, diagnose problems and recommend corrective actions to your service and support team.
- Active remote monitoring enhances customer experience by using your machine's data to understand your environment and set thresholds and action plans to accommodate your production needs.
- Automated Meter Reading can save you time as well as ensure accuracy over manually retrieving billing information.
- Automated Supplies Replenishment can allow for ordering of supplies when needed without customer interaction.
- On certain models, automatic downloading of software patches is supported to fix problems and add features.
- The expertise of hundreds of Xerox engineers is available.

Xerox Remote Services include capabilities designed to address the following security-related concerns:

Identification and Authentication
The process of uniquely and reliably identifying a device.

Authorization
The process of granting the device remote access services based on our customer's security needs and product acquisition decisions.

Data Integrity
The ability to verify that data has not been subjected to unauthorized modification.

Audit Capabilities
The ability to track all communication between a machine and Xerox.

Customer Confidentiality
The prevention of access by unauthorized parties by making use of encryption techniques (i.e., https).

Within the end-to-end Remote Services system, the system design goals respond to network security concerns in two main categories.

Your Network

The first category is security concerns related to the connection of the client software to your network and to the transmission of data across the Internet to Xerox. Xerox Remote Services incorporate the following controls:

- You must authorize communications between the device and Xerox.
- Communications from the device shall not include Personally Identifiable Information (PII) unless authorized by you.
- The transmission of job data is not possible without express independent permission and initiation by you (approval to send diagnostic, supplies usage, and billing data is separate from approval to send job data).
- Job data is separately encrypted and is not generally available to the back-end systems or personnel which are not specifically designated.
- The Remote Services Client Software allows a secure connection from the device to Xerox. It is not possible to use this connection to access your network or data beyond what is pushed to Xerox by the customer.
- The integrity and authentication of any information (data or code) downloaded from the Communications Server to the device by the Remote Services Client is verified prior to installation.

Transaction Security

The second category is the network security concerns related to the exchange of information between you and Xerox in executing transactions. The following controls have been established:

- The Xerox Communication Server and the Remote Services Clients mutually identify and authenticate themselves to each other.
- All transactions uploaded by the Remote Services Client to the Xerox Communication Server is able to be audited through the device transaction history log by both you and Xerox. A transaction log can be viewed which gives service personnel and privileged users the ability to audit the information shared with Xerox.

Xerox Managed Information Security Services

Application Security
The software application itself imposes a very complex security program based on “access control lists” that control user rights and privileges to all objects in the hosted repository. The design and implementation of this application security is customized for each customer and is driven by business requirements. Each and every user has a unique user ID and a password compliant with Xerox security rules. Each user is authenticated against Xerox’s authentication server to gain access to the individual application.

Network Security

Platform Services employs many different security tools and techniques to ensure that our network for the hosted repository is secure. First of all, each customer application has a unique URL and port, so there is no overlap on any customer interface. All traffic, whether over the Internet or through a private line, is 128 bit SSL encrypted with a certificate from a trusted third-party. For additional security for some clients, all traffic is routed through a 3DES encrypted VPN. Furthermore, some clients will have additional security through limiting the IPs to which our firewalls will respond.

All Internet-facing applications have a web server located in an isolated DMZ, with an actively monitored intrusion detection appliance on the Internet connection. All application software is operated on separate servers in a secure zone on the network, which does not have any direct access to clients, the Internet, or any other private external connection. All of your data is stored on a storage area network, which is accessible only from the Secure Zone.

Physical Security

All production equipment for the hosted repository service is located in Class 9 data centers, with appropriate physical security features in place. This includes live security personnel, identity authentication, fire suppression, redundant power, and physical man-barriers. Platform services maintains a geographically disparate second site for disaster recovery.

Logical Security

Because Platform Services operates multiple clients on the same physical hardware and network, there is a need for proper local separation of customer data. This is achieved through running a separate instance of software [web server, application server, database] for each customer with a unique “owner account” for each instance, and storing data on a dedicated volume on the storage area network for each customer.

Policies and Procedures

Platform services follow all pertinent Xerox security policies in terms of personnel screening, confidentiality contracts, and right down to the clean desk policy. In addition to this, Platform Services has policies specific to the Hosted Repository, for example, we have defined authorities from each customer to authorize user accounts and password resets and monthly reports of user activities for customer review to ensure normal activity

Remote Services Architecture

A high-level view of the end-to-end Remote Services architecture would involve communication flow between the Remote Services Client (direct-device and/or proxy-host) and the Xerox Communication Server. Remote Services Clients are embedded either in Xerox devices or in a hosted application (e.g. CentreWare® Web). The clients are configured to connect with and send messages specifically to the Xerox Communication Server.

Xerox Remote Services use industry-standard web services protocols for all communications between Remote Services Clients and the Xerox Communication Server. Web services are accessed via the secured-socket HTTP (HTTPS/SSL) that is common to web browsers and web servers. Use of web services as the underlying mechanism for all Remote Services transactions ensures both interoperability and compatibility with firewalls.

By using HTTP, web services can also take advantage of the Secure Socket Layer (SSL) protocol for security and HTTPS connection management capabilities in order to prevent customer data from being broadcast over the open Internet.

A proxy server is commonly used in network environments to provide a firewall system between the end-user network and the Internet. Most firewalls/proxies are configured to block requests on all but a few network ports. Firewalls, however, usually allow traffic on port 80 for HTTP and 443 (secured HTTP or HTTPS) so browsers can access the Internet. By using HTTP or HTTPS over standard ports, Remote Services Clients are able to communicate through firewalls. The Remote Services Clients act like any web browser (over standard ports) requiring no "holes in the customer firewall" or changes to other equipment at the customer site. Remote Services Clients support the 128 bit SSL encryption.

Customers initiate all interactions between their environment and the Xerox Communication Server. Remote Services Client Software may initiate an interaction with the Xerox Communication Server upon the occurrence of an event (e.g. a customer presses a button on the machine UI, a timer triggers an alarm, etc).

To achieve the effect of two-way connectivity the Remote Services Client Software periodically "checks-in" with the Xerox Communication Server to receive any "instructions" for them. This check is infrequent and very lightweight, avoiding congestion of the customer intranet.

Xerox digitally signs all packages downloaded by the Remote Services Client. The customer benefits from this software integrity because it addresses the following issues:

- Content Source: This feature certifies that the packages really come from Xerox.
- Content Integrity: This feature confirms that the packages have not been altered or corrupted since they were signed.

Xerox Print Services

Xerox Print Services helps you streamline management, control costs and maximize your results across the office. As a market leader in managed print services, Xerox has the tools, resources and experience to drive efficiencies throughout your organization, while helping safeguard against potential security vulnerabilities. We protect documents from inappropriate distribution by controlling access at the device through user authentication. We also continually monitor your device and your network port, recommending actions to maximize your information security. Our Extensible Interface Platform® (EIP) technology, a software platform that is embedded in our multifunction devices, enables an easy transition from paper to digital and facilitates direct links to back office systems. We help you track your assets and highlight any nonconformance of unauthorized devices added to your network. We also manage move/add/change requests and provide an audit trail for a secure document infrastructure.

Miscellaneous Services

Document Integrity
DigiFinish Book Integrity ensures that the proper book cover is applied to a book block. This validation process prevents both cover/book block mismatch and mis-orientation of covers due to improper loading by the operator.

Stock and Page Verification
Stock verification validates that each piece of paper on which an image is printed is the stock actually intended for that image, so a mismatch is recognized as soon as it occurs. Page verification ensures that the actual sequence of printed pages [impression sequence] corresponds with the intended page sequence for the job. This capability can be implemented with either of two symbologies [barcodes or dataglyphs] based on user needs.

Regulatory and Policy Compliance 9

Xerox systems, software and services conform to recognized industry standards and the latest governmental security regulations. For example, Xerox products support the standards set forth in:

- Payment Card Industry (PCI) Data Security Standards (2006)
- Sarbanes-Oxley
- Basel II Framework
- The Health Insurance Portability and Accountability Act (HIPAA)
- E-Privacy Directive (2002/58/EC)
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act
- The Health Information Technology for Economic and Clinical Health Act
- Dodd-Frank Wall Street Reform and Consumer Protection Act
- ISO-15408
- ISO-27001
- Control Objectives for Information and related Technology
- Statement on Auditing Standards No. 70

Summary 10

Network and data security are one of the many challenges that businesses face on a daily basis. And because today's MFPs serve as business-critical network devices that receive and send important data through a variety of functions, ensuring comprehensive security is paramount.

An MFP's entire system, along with any device management software on the network, must be evaluated and certified in order for IT and all the workers of an organization to be certain that their documents and network are safe and secure from information predators—or even from internal security breaches. In that respect, Xerox MFPs lead the industry. Our comprehensive approach, based on foundational, functional, advanced and usable security, is critical to safeguarding our customers' information assets.

Recognizing this, Xerox continues to engineer and design all of its products to ensure the highest-possible level of security at all potential points of vulnerability. We're committed to safeguarding your data so you can focus on the pursuits and activities that make your business or organization as successful as possible.

For more information about the many security advantages offered by Xerox, visit our security website, **www.xerox.com/security**.

Security Checklist

11

When comparing Xerox MFPs with other manufacturers' products, use the following checklist to determine whether the competitors' devices provide the same level of end-to-end security as delivered by Xerox.

	Xerox	Competitor 1	Competitor 2	Competitor 3
IP/MAC Address Filtering	✓			
IPsec Encryption	✓			
IPv6	✓			
802.1X Authentication	✓			
Secure Print	✓			
Scan to Email Encryption	✓			
Encrypted PDF/Password-protected PDF	✓			
Digital Signatures	✓			
"256-bit AES" Hard Disk Encryption	✓			
Hard Disk Overwrite	✓			
Secure Fax	✓			
Port Blocking	✓			
Scan to Mailbox Password Protection	✓			
Hard Disk Removal Program	✓			
Print Restrictions	✓			
Audit Log	✓			
Role Based Access Control	✓			
Smart Card Authentication	✓			
Common Access Card / Personal Identity Verification	✓			
User Permissions	✓			
Secure Access	✓			
"Full System" Common Criteria Certification	✓			
Integration with Standard Network Management Tools	✓			
Security updates via RSS feeds	✓			