Xerox and Information Security

Your Data, Your Business:
Partnering to Protect What's
Most Important

xerox®

Table of Contents

Overview

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

Nearly every business, and every person in it, is connected to the Internet. Your business—and every organization with which you collaborate—is part of a global system of interconnected computer networks and servers. There are countless users simultaneously performing tasks, accessing and sharing information, shopping for and selling goods and services and communicating via email, instant messaging, Skype™, Twitter and many other services.

The security 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 acquisition or 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.

Today's rising security threats come in various forms and in varying degrees of severity. The explosive proliferation of networked devices means an ever-increasing number of potentially vulnerable points of entry for intruders. And the "hacker" threat is constant, with programs running 24/7 that automatically seek and exploit network security shortcomings.

Security threats vary from relatively harmless spam messages to persistent threats that can take down entire networks.

With such constant Internet activity, you must be sure your company's confidential information stays secure. But the demands change, and change daily.

Networked printers and multifunction printers, or MFPs, which can print, copy, scan to network destinations, send email attachments and handle incoming and outgoing fax transmissions, are particularly vulnerable.

For those in Information Security, it's critical to the security of an organization's network to make sure that security infractions can't happen through network-connected printers and 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.

Printers and multifunction printers are sophisticated, multiple sub-system IT platforms, and meaningful security measures must comprehend every element of the platform.

Today's printers and MFPs are quite different from PCs and servers.

- Printers and MFPs are shared devices with multiple users and multiple administrators.
- Printers and MFPs are embedded devices:
  - There may be a real operating system within the system.
  - The operating system may have a direct external interface.
  - The operating system may be proprietary.
  - The operating system may be Microsoft® Windows®.
- Printers and MFPs have the following, all of which are typically associated with more advanced computing nodes:
  - Network protocol stacks
  - Authentication and authorization functions
  - Encryption
  - Device management
  - Web servers

Overview

Heterogeneity of printer and MFP implementations poses challenges.

- Much more diverse than traditional PCs
- High degree of diversity regarding underlying operating systems among different manufacturers and even within single manufacturer product lines

Traditional PC and server controls are not optimized for printers and MFPs.

- Anti-virus approach
  - May not be available for the operating system type used in the printer and MFP
  - Generally losing the war against malware anyway
  - Complexity of managing data file updates in a distributed environment
- Patching printers and MFPs
  - Software version control of printers and MFPs is inconsistent
  - Configuration management creates operational overhead
- Security Information and Event Management (SIEM)
  - Alerts and awareness from printers and MFPs are uneven
  - Remediation of printers and MFPs is not standardized

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

Just about anyone can launch attacks against a network and a company's information assets if a printer and 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 printer and MFP's output tray to malicious worms pulling sensitive documents off the network.

A printer's and MFP's entire system, along with any device management software on the network, must be evaluated and certified so that Information Security and all the workers of an organization are certain that their documents and network are safe and secure from information predators—or even from internal security breaches.

In that respect, not all printers and 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. 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

- No unauthorized disclosure of data during processing, transmission or storage

INTEGRITY

- No unauthorized alteration of data
- System performs as intended, free from unauthorized manipulation

AVAILABILITY

- System works properly
- No denial of service for authorized users
- Protection against unauthorized use of the system

ACCOUNTABILITY

- Actions of an entity can be traced directly to that entity

NON-REPUDIATION

- Mutual assurance that the authenticity and integrity of network communications are maintained

Security Vulnerabilities: Industry Risks and Costs

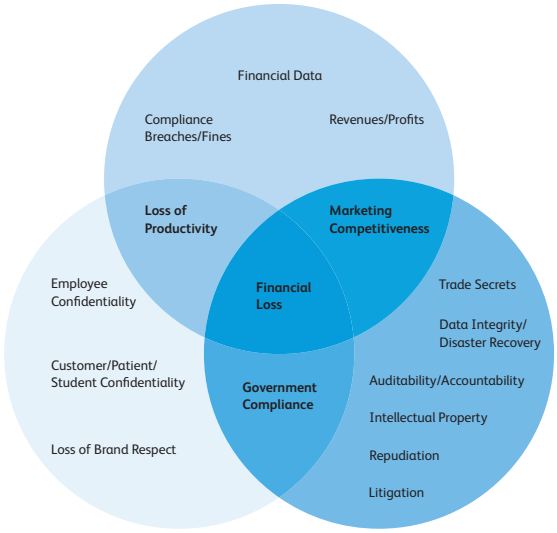
Businesses of all sizes have sensitive information valuable to cybercriminals that must be protected. The threat landscape is changing constantly. With an increase in Bring Your Own Devices (BYOD), wearables for health-tracking data, mobile payment systems, cloud storage and the Internet of Things, the threat is real and continues to grow.

Cybercriminals are increasingly focusing their attention on small- and mid-sized businesses (SMBs), because they are easier targets than large enterprises and because SMBs typically lack the resources needed to protect themselves against attacks. Data breaches for large enterprises make news headlines but, unfortunately, we don't hear much in the news about cyber-attacks on SMBs.

The stakes for SMBs are even higher than for large corporations. Customer information maintained within SMBs is becoming a more valuable commodity and the costs of these breaches can devastate an SMB. According to a study conducted in 2015 by IBM and Ponemon Institute, the average total cost of a data breach for the participating companies increased 23% over two years to $3.79 million.[1] The average cost paid for each lost or stolen record containing sensitive and confidential information increased from $145 in 2014 to $154 in 2015.[1]

That doesn't account for possible fines, loss of reputation and business disruption. Security may not always be a top business priority, but keeping information protected is critical for the health of the organization.

What's at Risk



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. HITECH was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and meaningful use of health information technology.

Failure to comply with HIPAA can result in civil and criminal penalties, even if no breach occurs.

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. One example is the Massachusetts state data breach law, which is one of the most aggressive in the nation. Xerox® systems, software and services conform to these strict guidelines, as well as others.

In 2014, the Department of Defense adopted National Institute of Standards and Technology (NIST) 800-53 standards, which is a publication that recommends security controls for federal information systems and organizations, and document security controls for all federal information systems, except those designed for national security.

1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.

Security Vulnerabilities: Industry Risks and Costs

Also, the Department of Defense has adopted additional security measures with the use of Common Access Cards (CAC) and their civilian government counterparts, Personal Identity Verification (PIV) 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 printer and MFP products. And finally, many 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.

A secure exchange of credit card information is vital and compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) helps to alleviate vulnerabilities and protect cardholder data. PCI DSS is a proprietary information security standard for organizations that handle credit cards, including Visa®, Mastercard®, American Express®, Discover® and JCB.

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 the student's guardian.

With so many regulatory and compliance measures requiring a response, 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.

Security Overview

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.

Our Security Strategy

The development of Xerox® products is guided by a Secure Development Life Cycle Process, which takes the Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM) and SANS Institute guidelines into consideration. This involves defining security requirements, assessing risks, analyzing vulnerabilities and penetration testing, as well as information obtained from OWASP and the SANS Institute. This strategy consists of three pillars:

State-of-the-Art Security Features

Printers and 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 was the first manufacturer to seek and obtain certifications for "complete" MFP 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), MFP user interface, local hardware ports and fax system.

Maintenance

At Xerox, maintaining our printer and multifunction devices' security throughout their lifespan requires ongoing diligence to ensure continuous protection against newly discovered exploits. This is accomplished by:

- Ensuring that software updates are issued on an ongoing basis
- Notification of new security bulletins with RSS feeds
- Responding to identified vulnerabilities
- Providing secure installation and operation guidelines
- Providing Common Criteria information
- Making patches available at www.xerox.com/security

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

A Comprehensive Approach to Printer and MFP Security

Xerox long ago recognized and embraced this shift in technology and the evolving needs of the workplace. We offer a comprehensive set of security features to keep your printers/MFPs and your data safe. Xerox secures every part of the data chain, including print, copy, scan, fax, file downloads and system software. **There are four key aspects to our multilayered approach.**

1. Intrusion Prevention

Your first and most obvious vulnerability is the user interface—who has physical access to your printer and its features. User Authentication is the basis for granting access to Xerox® printers and multifunction devices for authorized walkup and network users. Once authenticated, the user can interact with the device or access customer data, which is subject to restrictions based on the user's role. Xerox® printers and MFPs employ a variety of technologies to ensure authorized access to device features and functions by users and other network devices. Then we tackle less obvious points of intrusion—what is sent to the printer and how Xerox® ConnectKey® Technology will intercept attacks from corrupted files and malicious software. Our system software, including DLMs and weblets, is Digitally Signed: any attempts to install infected, non-signed versions will result in the file being automatically rejected. Print files will also get deleted if any part is not recognized as legitimate.

NETWORK AUTHENTICATION

Network authentication allows users to authenticate to the device by validating user names and passwords prior to use. Network authentication authorizes an individual to access one or any combination of the following services: Print, Copy, Fax, Server Fax, Reprint Saved Jobs, Email, Internet Fax and Workflow Scanning Server. Also, users can be authorized to access one or any combination of the following machine pathways: Services, Job Status or Machine Status.

1. Intrusion Prevention

Prevent general access to restricted devices with user access and internal firewall on the printer.

2. Device Detection

Be alerted at startup or on demand if any harmful changes to your printer have been detected.

3. Document and Data Protection

Keep personal and confidential information safe with encrypted hard disk (AES 256-bit, FIPS validated for many products) and image overwrite.

4. External Partnerships

Protect your data and device from malicious intrusions with McAfee whitelisting technology, Cisco® Identity Services Engine (ISE) integration, certification bodies and compliance testing organizations.

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.

LDAP AUTHENTICATION

LDAP authentication (BIND) is supported for authenticating with the LDAP servers for information lookup and access. When an LDAP client connects to the server, the default authentication state of the session is set to anonymous. The BIND operation establishes the authentication state for a session.

SMTP AUTHENTICATION

This feature validates the user's email account and prevents unauthorized users from sending emails from the device. System Administrators can enable TLS for all SMTP send and receive operations.

POP3 AUTHENTICATION BEFORE SMTP

As an additional layer of security, Xerox® MFPs support the ability for System Administrators to enable or disable the POP3 authentication before SMTP feature. POP3 authentication before SMTP forces a successful login to a POP3 server prior to being able to send mail via SMTP.

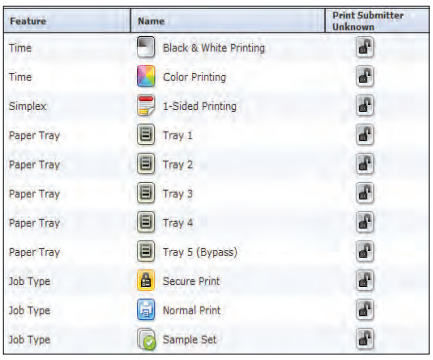
ROLE BASED ACCESS CONTROL (RBAC)

The RBAC feature ensures that authenticated users are assigned to a role of either Non-logged-in User/Logged-in User, System Administrator or Accounting Administrator. Each role has associated privileges with appropriate levels of access to features, jobs and print queue attributes. It enables Administrators to choose precisely which functions are permitted for a given role. Once a user logs into the device with the user's name and password, the device can determine which roles are assigned to that particular user. Restrictions are applied based on the assigned roles. If an entire function is restricted, it can appear locked out to the user after authentication or not appear at all.

Non-logged-in User/Logged-in User | System Administrator | Accounting Administrator

PRINT 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; Microsoft® PowerPoint® presentations automatically print in duplex mode; or Microsoft Outlook® emails always print in black and white.



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

SMART CARD AUTHENTICATION

Also known as Proximity Card or Contactless Smart Card Authentication, Smart Card Authentication protects your printer and MFP from unauthorized walkup access. Xerox® devices support multiple major smart cards (CAC/PIV, .NET, Rijkspas and other smart and proximity cards), around 30 different types of card readers and 65 different proximity cards. 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 device'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 printers/MFPs and the networks that connect them.

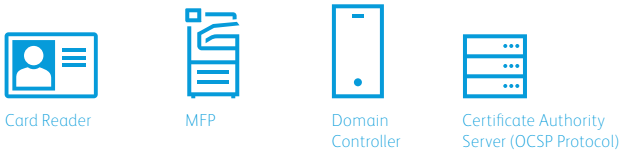
Security Overview

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

The 144k CAC/PIV provides the following benefits:

- Scan to Email S/MIME encryption to self or any recipient in the MFP's local or LDAP global 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 signon to Scan to Home and LDAP

Configuration Diagram for Common Access Card (CAC)/ Personal Identity Verification (PIV)



1. A card is inserted into the reader and the user is prompted to enter a PIN at the MFP.
2. The MFP checks the OCSP server to confirm that the card's certificate has not expired and then verifies the "Chain of Trust" back to a known Certificate Authority.
3. 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.
4. Authorization unlocks Walkup MFP features:
   - Scan to Email
   - Copy
   - Fax
   - Custom Services
   - Workflow Scanning

XEROX® PRINTSAFE SOFTWARE

Xerox® PrintSafe Software provides secure print authentication for printed data on most printers and MFPs, including both Xerox® devices and devices from other vendors. This software is open to work with a variety of industry standard secure readers and cards.

Secure, Convenient and Flexible Print Workflows

The user submits the document.

Simply by pressing "Print", the document is held until authentication.

The user can approach any printer or MFP on their network enabled to accept a PrintSafe job, and authenticate with a simple card swipe or PIN.

Once the user is authenticated, they can select either to release a single job or all secure jobs at the printer or MFP.

Xerox® PrintSafe Software is not limited to Xerox® devices. Any printer or MFP* registered with Xerox® PrintSafe Software can output PrintSafe jobs.

Flexible workflows allow the user to load software on their PC client for direct printing or onto an existing print server, which can easily be configured for Xerox® PrintSafe Software.

*Non-Xerox® devices require a network accessory; see your Xerox Sales Representative for details on the makes/models supported.

DEVICE USER INTERFACE AND REMOTE USER INTERFACE ACCESS

System Administrators can lock out access to device setup screens for unauthorized users from the control panel and Remote User Interface utility in an effort to protect its configuration information.

2. Device Detection

In the unlikely event that your data and network defenses are bypassed, Xerox® ConnectKey® Technology will run a comprehensive Firmware Verification test, either at start-up* or when activated by authorized users. This alerts you if any harmful changes to your printer or MFP have been detected. If any anomalies are detected, the device will display a message advising the user to reload the firmware. Our most advanced built-in solutions use McAfee® Whitelisting** technology that constantly monitors for and automatically prevents any malicious malware from running.

In partnership with Cisco, Xerox has implemented our device profiling in Cisco® Identity Services Engine (ISE). Integration with Cisco Identity Services Engine (ISE) auto-detects Xerox® devices on the network and classifies them as printers for security policy implementation and compliance.

For more information, refer to the following white papers:

McAfee Whitelisting White Paper:
http://www.office.xerox.com/latest/SECWP-03.PDF

Cisco ISE White Paper:
http://www.office.xerox.com/latest/SECWP-04.PDF

*Xerox® VersaLink® Printers and Multifunction Printers
**Xerox® AltaLink® and i-Series Multifunction Printers

3. Document and Data Protection

Document Protection

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.

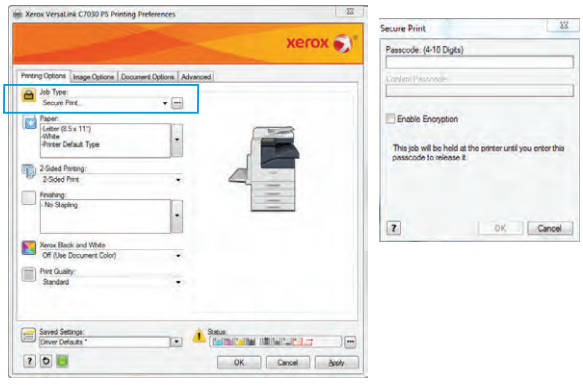
SCAN DATA ENCRYPTION

Users of our Xerox® ConnectKey® Technology-enabled i-Series, VersaLink® and AltaLink® Series Smart MFPs also have the option to encrypt PDF files with a password when using the Scan to Email service.

- Protection outside of firewall
  - Securing data in an unsecure environment
  - Using industry standard protocols such as TLS and Secure PDF

PRINT STREAM ENCRYPTION

The Xerox® Global Print Driver® and some product drivers support document encryption when submitting Secure Print print jobs to ConnectKey Technology-enabled devices. Xerox® AltaLink and i-Series Multifunction Printers also support document encryption for regular print jobs. No additional hardware is required for print driver encryption.



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 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 the user's 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 128-bit or 256-bit AES-encrypted PDFs or password-protected PDFs, which are then securely transmitted over the network, and can be opened, printed or changed 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 the sender's fax was successfully received by the intended recipient.

Security Overview

DIGITAL SIGNATURES

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A digital signature is used to protect the device firmware from undetected modification and to provide data origin authentication. With smart cards, emails can be digitally signed with the sender's certificate. 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

Some Xerox® printers and MFPs have a Secure Watermark feature that helps 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.

USER/TIME/DATE STAMP

Through the Xerox® drivers, a user/time/date 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.

IP ADDRESS FILTERING

Internet Protocol (IP) filtering allows System Administrators to create rules to accept or reject information coming to the MFP device based on specific IP addresses or range of addresses. 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 SOCKETS LAYER (SSL)/TRANSPORT LAYER SECURITY (TLS)

Many organizations are required to comply with security policies that require all transactions between the client and printer or MFP to be secure via secure Web transactions, secure file transfers and secure emails. Data that is transmitted over the network without encryption can be read by anyone that sniffs the network. Xerox mitigates this problem with Secure Sockets Layer/Transport Layer Security for transmissions of data over certain protocols such as HTTPs and IPP.

IPSEC ENCRYPTION

Internet Protocol Security (IPsec) secures all communication at the IP layer and is primarily used to encrypt print submittals to the device. It encrypts all traffic between Point A and Point B in such a way that only trusted users can send and receive the information, the data is not altered during its transmission and only authorized users can receive and read the information.

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 ENABLE/DISABLE

With the Network Ports Enable/Disable capability, unnecessary ports and services can be disabled 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 larger MFPs, tools are provided to set security levels and disable specific ports and services.

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.

MFPs can add digital signatures that verify the source and authenticity of a PDF document. When recipients open a PDF file that has been saved with a digital signature, they can view the document's properties to review the signature's contents including the Certificate Authority, system product name, serial number and the time/date stamp of when it was created. If the signature is a device signature, it will also contain the name of the device that created the document, while a user signature verifies the identity of the authenticated user that sent or saved the document.

Xerox® MFPs can be loaded with a certificate signed by 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.

SNMPV3

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks, which provides greater security by protecting data against tampering, ensuring access is limited to authorized users through authentication and encrypting data sent over a network.

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.

SNMP COMMUNITY NAME STRINGS

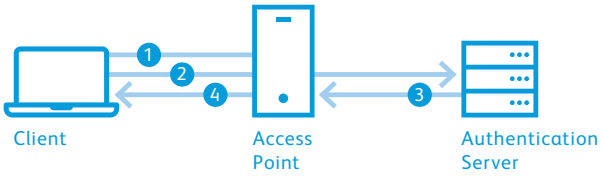
Typical read-only Management Information Base (MIB) data use the "public" string and the read-write community strings that are set to "private." Using the read-write community name strings, an application can change the configurations setting of the device using MIB variables. The read-write community name strings on Xerox® devices can be changed by the System Administrator to increase the security when managing MFPs using SNMP.

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). IEEE 802.1X functionality is supported by many Ethernet switches and can prevent guest, rogue or unmanaged systems that cannot perform a successful authentication from connecting to your network.

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 are:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2
- EAP-TLS (AltaLink® and i-Series products)

FIREWALL

A firewall is a part of a computer system or network that is designed to block the device from external threats and unauthorized access while permitting authorized communications. The device can be configured to permit or deny network transmissions based upon a set of rules and other criteria. Network Administrators can restrict access to network segments, services and the devices' ports to secure the devices.

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.

Data Protection

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 risks. 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.

IMAGE DATA ENCRYPTION

Using 128-bit or 256-bit AES encryption, many Xerox® devices feature data encryption including job, image and customer data, which protects your Xerox® MFP's data at rest from unauthorized access. With data encryption, the disk is partitioned and only the user data partition is encrypted. Operating system partitions are not and cannot be encrypted.

- AES 128-bit or 256-bit encryption, Federal Information Processing Standard (FIPS) 140-2 validated
- All user image data on the hard disk is encrypted

Security Overview

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. Many Xerox® devices can be put into FIPS 140-2 mode, which means that they will utilize only FIPS 140-2 certified encryption algorithms.

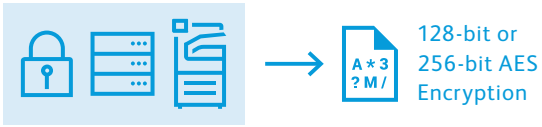


IMAGE OVERWRITE

Image overwrite erases image data from your Xerox® device's hard drive once the data is no longer needed. This can be performed automatically after completion of processing each job, scheduled on a periodic basis, as well as at the request of the System Administrator. Xerox® devices feature both Immediate and On Demand Image Overwrite.

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 image data is lost upon shutdown or system reboot. With non-volatile memory, image 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 image data is located in Xerox® devices. A Statement of Volatility describes the locations, capacities and contents of volatile and non-volatile memory devices within 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), a Xerox sales professional (for new customers) or may be accessed at www.xerox.com/security.

SECURE FAX

Sensitive incoming faxes are held until released by the System Administrator.

SCAN TO MAILBOX PASSWORD PROTECTION

When using an MFP's Scan to Mailbox feature, the designated mailbox can be password protected to ensure only those authorized can access the scans stored within it. Scan to Mailbox security is further enhanced by encryption of the hard disk image data partition.

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 information is entered, 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. Most Xerox® MFPs using Smart Card Authentication also provide the ability to digitally sign emails. 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

The standard Job Log Conceal function ensures that jobs processed through the device are not visible to a walkup user or through the Remote User Interface. The Job Log information, although concealed, is still accessible by the System Administrator, who can print the Job Log to show copy, fax, print and scan usage on the device.

HARD DRIVE RETENTION OFFERING

Xerox provides a Hard Drive Retention Offering for Xerox® devices to those customers who are concerned that the image data on their hard drive is more sensitive or even classified. This service allows a customer, for a fee, to retain their hard drive(s) and sanitize or destroy them in a manner that they feel will keep their image data secure.

REMOTE SERVICES DATA VALIDATION

Many Xerox® devices obtain customer buy-in prior to transmitting Personal Identifiable Information (PII) and Customer Identifiable Information (CII) via Remote Services to Xerox.

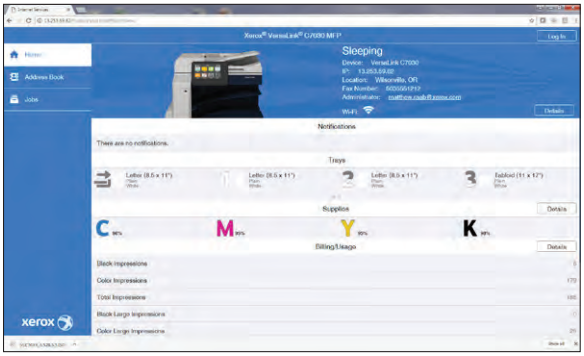
POSTSCRIPT PASSWORDS

Another printing-related area of risk is when printing with the Adobe® PostScript® page description language (PDL). PostScript includes commands that allow print jobs to change the device's default behaviors, which could expose the device. Because the PostScript language includes very powerful utilities that could be used to compromise a device's security, administrators can configure the device so that PostScript jobs are required to include a password to change the device'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.

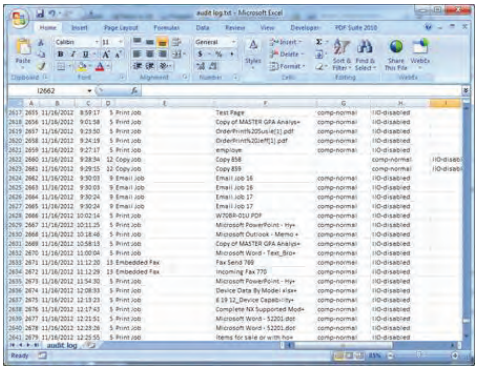
AUDIT LOG

Xerox® MFPs and many of our printers can maintain Audit Logs to track activity by document, user and function. The Audit Log is enabled by default on newer devices and can be enabled or disabled by the System Administrator. It can track access and attempted access to the device and transmit audit logs to a SIEM system or audit log server. An example of an Audit Log entry: "User xx logged into the Xerox® AltaLink® MFP at 12:48 AM and faxed 10 pages to 888.123.1234."

For Xerox® ConnectKey® Technology-enabled multifunction printers, the Audit Log can be automatically and securely sent to a SIEM system to provide for continual monitoring of the MFP.



The Audit Log interface is accessed from a System Administrator's workstation using any standard Web browser.



The log can then be exported into a .txt file, and opened in Microsoft® Excel®.

4. External Partnerships

Xerox works with compliance testing organizations and security industry leaders such as McAfee to wrap their overarching standards and know-how around ours. The following malware protection features are available on Xerox® ConnectKey® Technology-enabled MFPs (Xerox® AltaLink® and i-Series Multifunction Printers).

MCAFEE® EMBEDDED CONTROL—ENHANCED SECURITY

Xerox® MFPs built on Xerox® ConnectKey® Technology include McAfee Embedded Control integration powered by Intel® Security, resulting in the industry's first lineup of multifunction printers that protect themselves from potential outside threats. McAfee's whitelisting technology detects unauthorized attempts to read, write or add to protected files and directories and sends alerts if they occur. Also, seamless integration with Xerox® CentreWare® Web Software, the Xerox® MPS toolset and McAfee ePolicy Orchestrator® (McAfee ePO™) allows for monitoring from the preferred console.

MCAFEE EMBEDDED CONTROL—INTEGRITY CONTROL

Integrity Control builds on the Enhanced Security capabilities and adds prevention of new files from being executed from any location by untrusted means. Only approved software is allowed to run, which prevents both general and targeted attacks. Useful especially for enterprise-wide security implementations, Xerox and Intel Security offer whitelisting technology that ensures the only function those devices are doing are the services you want to deliver. This same technology is used to protect servers, ATMs, point-of-sale terminals and embedded devices such as mobile devices.

MCAFEE'S EPOLICY ORCHESTRATOR (EPO)

McAfee's ePolicy Orchestrator (ePO) is a security management software tool that makes risk and compliance management easier for organizations of all sizes. It presents the users with drag-and-drop dashboards that provide security intelligence across endpoints—data, mobile and networks—for immediate insight and faster response times. ePolicy leverages existing IT infrastructures by connecting management of both McAfee and third-party security solutions to LDAP, IT operations and configuration management tools.

For third-party independent proof that we achieve top levels of compliance, certification bodies like Common Criteria (ISO/IEC 15408) and FIPS 140-2 measure our performance against international standards. They recognize us for our comprehensive approach to printer security.

CISCO® IDENTITY SERVICES ENGINE (ISE) INTEGRATION

Centrally manage and deploy printer security policies. Our partnership with Cisco provides greater Xerox® print device detection capabilities, resulting in finer-grain security policy enforcement. Xerox® devices are automatically recognized and classified by Cisco ISE, permitting network access control and reduction of overhead by eliminating manual entry of printer attributes. Our profiling of printers with Cisco ISE thwarts spoofing attempts by saboteurs to gain unfettered access to sensitive systems. Xerox® print device integration with Cisco ISE provides an operationally efficient approach to meeting security policy objectives.

Regulatory and Policy Compliance

Modern printers and MFPs are a focus for compliance due to the personal and sensitive data they access, store and communicate. Non-compliance can lead to lost business opportunities, losing existing customers or even legal action. Levels of required compliance vary by country and vertical market.

The Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the Data Protection Act in the UK are examples of standards that may need to be met to continue business legally.

Common Criteria Certification is an internationally recognized security standard that meets U.S. Department of Defense specifications.

With industry-leading security features and a flexible approach to configuration and deployment, Xerox® devices can conform to any standard and have the controls available to match any need.

Xerox® systems, software and services conform to recognized industry standards and the latest governmental security regulations. Our products offer features that enable our customers to meet those standards. The following standards are examples:

- Payment Card Industry (PCI) Data Security Standards Version 3.0
- 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 Common Criteria for Information Technology Security Evaluation
- ISO-27001 Information Security Management System Standards
- Control Objectives for Information and Related Technology
- Statement on Auditing Standards No. 70
- NIST 800-53, adopted by Federal Government and DOD in 2014
- Federal Risk and Authorization Program (FedRAMP)

Product Security Evaluation

Document security means peace of mind. One of the hallmarks of the Xerox® 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 third-party 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, 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 the 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 security functional requirements based on predefined Evaluation Assurance Levels (EALs) or specialized assurance requirements.

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 one of the largest numbers of Common Criteria Certified MFPs. In addition, Xerox was the first manufacturer to certify the entire device and Xerox is the only manufacturer to always certify the entire device.

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

Risk Assessment and Mitigation

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: micro-printing, fluorescence and infrared print security, Xerox® Glossmark® and Correlation Marks print mark technology, just to name a few. For more information about these technologies, visit www.xerox.com/security.

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 and updates 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.

In addition to our own extensive internal testing, Xerox regularly monitors vulnerability clearinghouses made available by such entities and resources as US-CERT 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 Vulnerability Management and Disclosure Policy.

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 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 U.S., customers should sign up for the security RSS feed. Outside the U.S., contact your local Xerox support center.

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

- Security Bulletins
- RSS Feed: Get 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

www.xerox.com/security is your portal to a diverse breadth of security-related information and updates, including bulletins, white papers, patches and much more.

Manufacturing and Supplier Security Practices

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 U.S. Customs Agency Trade Partnership Against Terrorism. 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 Returns and Disposals

Hard Drive Retention Offering for Xerox® Products

Xerox provides a Hard Drive Retention Offering to allow customers in the United States, for a fee, to retain the hard drive on leased Xerox® products. This service may be required for customers with very sensitive data, perhaps classified, or with internal policies or regulatory standards that mandate specific disposition processes for hard drives.

Upon request for this service offering, a Xerox service technician will travel to the customer location, remove the hard drive and provide it 'as is' to a customer representative. At this time, Xerox does not provide hard drive sanitization, cleansing or destruction services on site at customer locations. Customers will need to make arrangements for final disposition of the physical hard drive received from the technician.

To determine if your Xerox® product contains a hard drive or review security features available to secure data on hard drives, please visit www.xerox.com/harddrive.

For more details about this program, contact your Xerox sales representative or visit www.xerox.com/security under Security Resources in the Articles and White Papers section.

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

Summary

Network and data security are among the many challenges that businesses face on a daily basis. And because today's printers and 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 so that Information Security and all the workers of an organization are 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 www.xerox.com/security.

Security Checklist

IT security managers are already overwhelmed with managing security demands. Small businesses must rely on effective systems and security software to do much of the work for them. The last thing you and your staff need is more high-touch activity or manual interventions to monitor and keep updated every device and data stream in your environment, including your MFPs and printers.

A comprehensive network security plan should include three points of emphasis, with a strategy in place for each to ensure you have a plan that works.

1. "Hands-off, self-protecting" devices that are resilient to new attacks
2. Compliance with the most up-to-date security standards and regulations
3. Complete visibility on the network

The New Security Standard for a New Age

- Security cannot be an afterthought.
- Information is an increasingly valuable intellectual property.
- Firewalls aren't enough; security policies must be holistic and ubiquitous.
- Protection for embedded devices is now an integral part of today's security imperative.

Xerox offers comprehensive, multi-layer security that is easy to deploy and manage, and helps keep your business compliant with industry and government standards. Xerox® technology is tested and validated to protect against unauthorized access, data and identity.

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.

		Competitor		
	Xerox	1	2	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	✓			
Image Overwrite	✓			
Secure Fax	✓			
Port Blocking	✓			
Scan to Mailbox Password Protection	✓			
Hard Drive Retention Offering	✓			
Print Restrictions	✓			
Audit Log	✓			
Role Based Access Control	✓			
Smart Card Authentication	✓			
Common Access Card/ Personal Identity Verification	✓			
User Permissions	✓			
"Full System" Common Criteria Certification	✓			
Integration with Standard Network Management Tools	✓			
Security Updates Via RSS Feeds	✓			
Embedded McAfee Protection Powered by Intel® Security	✓			
McAfee® Integrity Control	✓			
McAfee® ePolicy Orchestrator® Integration	✓			
Cisco® Identity Services Engine (ISE) Integration	✓			

To learn more, visit **www.xerox.com**.