Improve Information Security

Advanced technology for protecting data and documents

Information security is critical for any organization. If sensitive details about your strategic plans, upcoming offerings or customers wind up in the wrong hands, the risks to profitability — and your image — are unacceptable. Because most of this information exists as a paper or electronic document, that means document security is also a top priority.

Smartplace can help you ensure document security. Smartplace provides a suite of innovative hardware, software and services that make it easy and cost-effective to implement a rigorous document security policy. Our solutions enable organizations to protect critical documents from internal and external threats — without affecting productivity.

What makes a document secure?

Maintaining document security depends on three points: which users have access to documents, what these users can do with documents once access is attained (can they edit, share, distribute or steal them?) and how that access is controlled. Keep in mind, most documents can be accessed many ways by a variety of authorized and unauthorized users. Documents exist as hardcopy output in workspaces and storage. Before they are printed out or copied, documents are transmitted over a local network and often over the Web. After documents are printed out or copied, the file itself may remain in a print queue and information from the file may reside in the output device's memory. Unless all these points of vulnerability are considered, document security can be compromised.

How does Smartplace protect confidential documents?

1. Secure storage and management.

Moving paper documents into electronic storage is a proven way to improve document security, so Smart Technologies offers ways to scan paper directly into enterprise content management (ECM) and enterprise document management (EDM) systems, as well as to secure servers or archives. Smartplace also provides a secure, Web-based storage and management solution that ensures safe access for authorized users. At the device level, user authentication restricts access, while administrative settings can restrict individual users' privileges. Many solutions create audit trails so you can see which user accessed which document at what time.

2. Secure printing.

Smartplace offers print security software solutions that require users to enter an ID and password prior to output, which means sensitive documents are not left sitting in an output tray where unauthorized users can see them or take them. Many printers support encryption of data during transmission from a computer.

3. Network security.

Smartplace solutions help system administrators monitor connected MFPs, printers, faxes, scanners and other devices with ease and efficiency.

This increases the chance that errors, or irregular network activity will be detected before devices or documents are compromised. Smartplace provides simple utilities that allow IT departments to see connected devices at a glance and manage them remotely via the Web.

4. Device security.

Printed documents remain in the memory of output devices, so Smartplace offers ways to prevent hard drive theft, as well as protect confidential information if the hard drive is stolen. Plus, most systems support the industry standard applications and tools administrators use to ensure network security and prevent unauthorized breaches via connected devices such as MFPs and printers.

- Authentication requires users to enter a valid username and password to access device functions. Four methods include Windows (compares login to database of users on Windows network server), LDAP (compares to Lightweight Directory Access Protocol (LDAP) server to protect e-mail address book), basic (compares to login credentials registered in the system's address book) and user code (compares to user codes registered in the system's address book)
- Address Book Encryption encrypts data registered in the MFP's address book to prevent unauthorized viewing

Protect Confidential Documents

Drawing on all the offerings shown here, Smartplace can help your organization establish and maintain exceptional document security.

Hardware

- Secure Socket Layer (SSL) encryption encrypts print data using SSL protocol so the data is undecipherable if unauthorized users try to print it
- Watermarking/overlay adds a layer of visual security
- Unauthorized Copy Control embeds a secure background on documents so they can't be duplicated on other MFPs equipped with this feature
- Data Overwrite Security System (DOSS) overwrites data temporarily stored on the MFP's hard drive with random 1s and 0s, making it virtually impossible to access or reconstruct residual image data (in compliance with ISO 15408 and National Security Agency (NSA) methods)
- Removable Hard Drive (RHD) feature allows organizations to remove the MFP's hard drive with a key lock system and place it in a vault or safe
- Volatile Memory Security System (VMSS) destroys any latent data on the hard drive every time the MFP is turned off; it uses a synchronous dynamic (SD) RAM memory hard drive in place of a traditional magnetic hard drive
- HDD Data Encryption encrypts the data on a device's hard drive, rendering it unavailable to hackers
- Many systems with Scan-to-Email support S/MIME (Secure/Multipurpose Internet Mail Extensions), a standard for public key encryption and e-mail
- Many devices support Kerberos authentication, a network protocol for client/server applications that uses powerful secret-key cryptography
- Some systems support Internet Protocol Security (IPsec) Communications, a suite of protocols designed to secure IP communications via authentication and encryption of each IP packet in a data stream
- Locked Print Password Encryption suspends document printing until the authorized user enters the correct password on the device control panel, preventing unauthorized individuals from viewing or removing a

document from the output tray

- Encrypted PDF Transmission allows users to create PDF files that can only be viewed or forwarded by recipients who enter the correct password; this feature is also available for scanned documents that are converted immediately to secure PDF files

Software

Assessment and Cost Recovery

- Establishes a complete audit trail for every printed document, with detailed metrics for more than 30 job characteristics (user, date, time, printer, file name, application, number of pages, duplex, b/w, color)

Forms Creation/Variable Data & Host Printing

- Automated creation and delivery of direct mail, transactional and trans-promotional documents increase security by reducing or eliminating the need for third-party processing and handling of confidential files

Scan, Capture, Imaging & Document Distribution

- Distributed scanning software use existing authentication processes to control delivery privileges, so the solution can be deployed safely
- Supports LDAP, Microsoft Active Directory and Novell eDirectory authentication, as well as custom authentication, 128-bit encrypted transmission and the erberos protocol

Device Management

- Allows organizations to confirm that network connected devices are validated though the Common Criteria/ISO 15408 Certification

Service

Depend on Smartplace to help with all of the following:

- Network security optimization
- Disaster recovery and business continuity planning
- Intrusion detection and prevention
- Antivirus and spyware detection and remediation
- Managed firewall services
- Security policy development and enforcement
- Mail security and training

*Not all devices have all security features. Ask your local representative for individual system specifications.

Smartplace Business Solutions

www.smartplaceusa.com
info@smartplaceusa.com