

Print and Imaging Management



Critical for Corporate Security, Cost Control and Social Responsibility

Overview

Organizations of all sizes today use networked printers, scanners and devices that integrate multiple imaging functions—scanning, printing, copying, communicating—in a single unit, known as multifunction printer (MFP) devices. The increasing sophistication of these devices makes sharing documents—even the most sensitive papers—as easy as pressing the ubiquitous “scan-directly-to-email” button. This sophistication, combined with today’s increased requirements for data confidentiality and regulatory compliance, has made it critical for organizations to put in place policies around use of printers, MFPs and other imaging devices.

In addition, security, cost control and environmental awareness are equally important reasons organizations should embrace printing policies.

This white paper describes the security and management issues around use of printers and imaging devices in an office environment and recommends approaches to addressing these, including use of print management software and a print authentication solution integrating smart cards and readers.

Introduction to Managed Print Services

Managed print services (MPS) have been a printing and imaging industry vision for many years. The ultimate goal of MPS is to audit, consolidate and improve the management of an organization’s print and imaging fleet. The potential and influence of a growing MPS market has transformed this vision into a reality. The recent economic downturn presented the opportunity for MPS to re-introduce the benefits of gaining control of costs associated with print solutions that have been difficult to track in the past. With MPS, organizations are now able to identify the number of machines in their network, minimize the quantity of print, scan, and copy hardware, and establish rules and regulations relating to the use of this hardware.

A successful MPS implementation will provide measurable results in three areas. First, it will reduce costs associated with an organization’s print and imaging requirements. Second, it will reduce an organization’s carbon footprint and enable it to meet internal green initiatives. Third, and significantly, it will minimize the potential for data leakage by keeping confidential information and intellectual property out of the public domain meeting the compliance requirements associated with heavily regulated industries.

How to Get Started

There are three main steps to any MPS implementation.

1. **Internal Audit:** This will provide an organization with a complete picture of every device in the organization and the location of each.
2. **Consolidate the Fleet:** This will entail removing seldom-used devices, individual desktop printers and strategically placing MFPs in high traffic areas for multiple individuals to access. Most managed service providers (MSPs), both vendor-centric and vendor-neutral, will maximize use of an organization's existing fleet, if possible, and then add the appropriate number of devices to create a complete network of MFDs for printing, scanning and copying requirements.
3. **Implement Intelligent Print Management:** In this phase, the MSP will implement an intelligent print management solution. This solution will be embedded within the hardware, and will enable the IT team to establish user rules, minimize scanning and copying requirements by moving documents electronically, and authenticate the identity of an employee using the device.

Integral to the solution is a secure document print release system, coupled with a contactless smart card and integrated reader. The secure release system requires employees to present their card to a reader integrated into the printer and be "authenticated" before a document can be printed.

Print Management for Security and Regulatory Compliance

Today's security threats are numerous and widespread. Whether it is the constant barrage of external attacks or internal malicious behavior by employees, organizations around the world are struggling to minimize data leakage to the public domain.

While most organizations spend incredible amounts of time, energy and resources to fend off external attacks, very few spend enough of those resources on establishing an internal security policy that addresses the most inherent risks associated with the removal or transfer of sensitive information. Gartner analyst Richard Hunter indicates that "more than 70 percent of unauthorized access to information systems is committed by employees, as is more than 95 percent of intrusions that result in significant financial losses." Most of these data breaches are not caused by malicious behavior, but rather by employees being unaware of the confidential nature of the data, the lack of an established policy, or the lack of awareness of any established policies.

Many organizations have developed security policies to govern the use and misuse of company computers and laptops. Most of these policies address the use of the internet, instant messaging, email, and the access of confidential files. What's missing from these policies is an entire category of devices that have emerged as high security risks for all organizations: printers, scanners, copiers and all-in-one MFP devices. Because these printing and imaging devices typically are endpoints within an organization's network, they are especially susceptible to misuse. And today's printers and imaging devices are powerful, enabling employees to print or copy documents, and scan images or documents directly to email and other electronic destinations. Significantly, use of these powerful devices is unmonitored and uncontrolled in most enterprises. Therefore, printing and imaging devices have emerged as high security risks for an organization.

One way to minimize these risks is to establish use policies with print management solutions software packages. Print management allows organizations to minimize security risks by establishing rules governing the use of MFP devices, preventing unauthorized employees from using certain functions of the device. A key function of these solutions is the authentication of users for each MFP. Users can be granted or denied certain rights and privileges based on department, hierarchy and position. When an employee prints to a device, the print job is initially delivered to a queue where the request can be checked against the pre-set rules. If the employee has authority to print this document, the document will be released from this queue and delivered to the printer only after the employee presents his or her company identification card to the MFP.

This is just one example of the many ways print management solutions and secure print authentication can minimize the risk of internal data leakage.

Print Management for Cost Control

With the average company spending three percent of their revenues on print associated costs¹, it is no wonder that organizations everywhere are evaluating how to consolidate and optimize their printer fleets. While these organizations will find added value in the improved security, regulatory compliance and successful internal green initiatives, the most important goal for many organizations is a reduction in costs.

Companies are increasingly turning to print management software that provides the ability to associate printer usage and costs by individual, department, location and many other variables. Some of the features include:

- Tracking printer usage
- Detailed usage reports
- Ability to establish quotas
- Accounting and department charge-back
- Ability to establish rules-based printing
- Client and project billing

By using a print management solution, organizations can reduce the amount of paper used, and on average, save \$150 to \$200 a year per employee. While this number may or may not be significant to the bottom line there are myriad factors that are difficult to quantify. Some of these factors include:

- Consumables such as toner, ink, ribbon, spare parts
- Power consumption, which will be reduced as the printer will only run when an employee is present to pick up their print job. The device will not run print jobs without authentication by an employee.
- Shredding services, which typically charge by the pound or by the hour. Either way, with less waste there is less to shred, reducing the associated costs.
- Maintenance fees, which could be reduced as the device is not utilized unnecessarily thereby preventing degradation and lengthening the life of the product
- Device downtime: is a variable cost that is difficult to assess but relates to employee productivity. Go take a look at the MFP between finance and sales that is not working.

How does this effect our employees productivity when they are consistently dealing with a down printer. Device downtime is a wildcard within the additional hidden costs.

When an organization implements a print management solution and only prints documents when an employee provides authentication at the printer, it can realize immediate cost reduction in paper and also reduce soft costs associated with the reduction in printer use.

Going Green with Managed Printing

Corporate America has entered an age when Corporate Social Responsibility is more than just an altruistic pursuit. Companies of all sizes, in all industries, are feeling pressure to save money and simultaneously meet the growing demand for environmental responsibility and accountability. Controlling document printing is one key initiative that allows organizations to focus on being “green” while achieving cost savings.

A recent study established the following information:

- The average employee prints 10,000 pages/year, of which 17 percent are considered waste. Print management saves 1,700 pages/year/employee, equating to a cost savings between \$102-\$221/year/employee.
- Those same 10,000 printed pages consumed 51.5 kWh of electricity in the print process. Almost 9 kWh hours of electricity were spent on printing the 1,700 pages that the user didn't really want.
- Manufacturing those 10,000 pieces of paper produced 284.5 pounds of greenhouse gases, which is the equivalent of just over one week of car exhaust.

Controlled document printing is achieved by enabling networked printers or MFP devices with third-party software and a contactless card reader. Print jobs are released only when an authorized user presents their contactless card to the reader on the device.

In addition, a secure print management system can enable the following:

- Eliminates wasted paper by deleting print jobs that are not released in pre-set timeframes
- Reduces the use of toner and the wear-and-tear on the device by printing fewer documents
- Saves electricity by allowing the device to be in a low power mode until a card presentation takes place
- Enhances accountability by giving administrators the ability to track MFP usage by user or department
- Offers users convenience by using the same contactless card that is used to enter the building

By going green with managed printing, organizations are reducing print waste, minimizing their carbon footprint and meeting their corporate social responsibility.

HID Global Solutions for Secure, Managed Printing

HID Global is partnering with the leading MFP manufacturers and their application solution partners to develop robust authentication solutions for securely printing documents, minimizing costs associated with printing, and reducing the carbon footprint of organizations around the world.

Using the HID Global physical access cards—which are already the standard for secure ID and access at Fortune 1000 corporations worldwide—will minimize capital investment while maximizing cost control and security. By printing documents only when an employee has presented his or her HID card to the print device, companies can reduce the amount of paper, toner and electricity used on a daily basis, saving money and helping reduce environmental waste. And by reducing the ability for sensitive data to be accessed and mishandled, organizations can enforce security policies and meet industry specific compliance requirements such as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act and Payment Card Industry (PCI) Data Security Standard (DSS).

If you're already using HID cards and readers for secure access at your company, chances are you will be able to integrate these into a secure printing solution. Many current MFP devices work with HID Prox and iCLASS® cards, as well as HID keyfobs and tags.

Companies today are looking for opportunities to maximize their investment of any capital expenditures. By using the HID cards that are already an integral part of an employee's daily business process, companies can seamlessly add other solutions such as secure print authentication that continue to enhance the value of the physical access system. HID has focused on building an ecosystem of partners that bring a variety of products and solutions and we have worked closely to ensure those applications will work with the HID card already being carried.

ⁱ "Assessing & Benchmarking Document Costs: Developing a Future Document Strategy," InfoTrends & ALL Associates Group, March 2006