uniprint

WHITE PAPER

Achieving a Secure Print Infrastructure

Process Fusion

The Challenges

Most IT departments reluctantly consider print as part of their remit. Print has never been considered as either racy or viewed as innovative. It's cumbersome, labor intensive and driven largely by the user, who has neither the inclination nor the responsibility to ensure print security, even when the documents carry the 'confidential' tag. The scenarios that typically lead to breaches form part of our everyday working lives, but they are worth examining.

Unintentional Breach Scenarios

An authorized internal user prints a confidential document to a shared printer. The user rushes to collect it, aware of its sensitivity. But, by the time he reaches the printer, it has been scooped up by mistake as part of a previous print output.

Or, frequently, with a myriad of printing devices available on their network, users send jobs to a different printer before resending to a closer machine, so now multiple copies sit unattended on the out tray of multiple printers in various locations.

Sometimes security breaches are caused by the increased functionality of the printer hardware itself. With today's autostandby green printers, dormant printers render themselves offline, leading users to print a further copy in frustration and several instances of confidential documents start to pile up.

Intentional Breach Scenarios

Disgruntled employees can take advantage of unintentional print errors. Intentional breaches are much harder to legislate for and their consequences are likely to be far reaching. Most firms will take extra precautions around HR and Payroll/Finance assigned printers, but are largely unable to secure the print facility for every member of management and their administrative support team who are also party to confidential information. Disgruntled employees that come into contact with unsecure confidential documents have an immediate weapon in which to progress their case against an organization. Various Data Protection and Freedom of Information acts across the globe mean that individuals have the right to see all data held against them and nothing acts quite like a starting point for a case as piece of indiscriminate print.

*(Tip – Think it won't happen to you? Quocirca Research** shows that 70% of organizations have experienced one or more accidental data breach through printing.)*

Options in Achieving Practical Accountability and a Secure Print Framework

Once you have understood how real the print security threats are within your organization and how they could and do manifest, it is time to go back to the planning stage. Very few IT departments have ever had the luxury, in budget or time, to set out an Optimal Print Infrastructure; printers just tended to proliferate around us. Accurate and ongoing printer mapping used to be a recommended methodology for large companies, but in most enterprises that in itself has become too complex to sustain.

To set out a secure print framework, you should broadly consider three sequential steps:

1. **Decide** – What level of print security you realistically need to achieve and how it can be best achieved.
2. **Document** – Never forget that it is IT's responsibility (not the named department on the printer) to achieve and demonstrate ongoing regulatory compliance when it comes to securing confidential print. Documenting results remains key - from cost savings to regulatory proof points.
3. **Deliver** – A managed, automated, hassle and worry free print service.

We will briefly consider each of these areas in turn:

Decide – Clearly not all print is created equal and therefore it should be treated accordingly. Prioritize the departments where confidential documents proliferate and are vulnerable to breaches. Additionally, identify likely areas of continued misuse for personal print (More than likely, you will already know which printers consume extraordinary resources. Don't be afraid to dig deeper on usage). Both sets of users then become your number one education targets, who need to understand the financial impact of breaches upon a company.
(Tip – Empower and educate users with facts and figures on cost containment.)

Document – Document your findings and analyses, and recommend the appropriate course of action. In a litigation scenario, you will need to prove that your organization has adopted best business practice in order to protect confidential information. Consider also how external influences can alter the mix. Understand how you will incorporate evolving technology and user trends, such as personal and mobile devices due to the BYOD trends, and what your organization's stance is towards printing out Website content - especially social media sites where the user has a freehand in content input. Provide proof that users are assigned printers via IP address, host name or user group membership to allow correct printer mapping to be apportioned at each location.

Wherever possible, try and simplify your print associated overhead. *(Tip - If you are working in a* VDI environment*, check out the system stability benefits that* Universal Printer Drivers *can deliver, which seamlessly replaces all native Windows drivers in your infrastructure significantly simplifying printer management.)* For cost justification, empower yourself with a detailed knowledge of your print overhead. Knowing how much it is costing you, (per person, per department, per location) is a powerful tool. Document and manage this ROI cost comparison at the start of the process and at six monthly review intervals. Only then will you fully understand the true cost of print (Staggeringly, Gartner estimates that print as a whole costs the average organization between 1 and 3% of total revenue*) and be able to accurately cross charge the actual costs of print to users and departments. You can

also justify debates about internal print charges by demonstrating likely cost savings that can be enabled by easily automating standard print out policies – such as fast printing in black and white and duplexing. *(Tip - Pull printing is widely noted to reduce paper volume by 20%; duplexing by default saves 30%.)*

Without documented evidence, you have no tool for remediation. Therefore the selection of an archiving tool that allows print data to be archived in a database should be high on your deployment list for security and regulatory compliance. This also allows you a concrete, traceable reference point, if ever required, of who is printing what, where and when.

Deliver – Proof: don't leave it to chance. Whilst education of users is essential, never forget that ultimately it is not their responsibility to provide secure printing. It's yours. Secure pull printing, or sometimes referred to as 'follow me' printing, is a 'must have' in today's litigious world, allowing users to release documents on any network printer in proximity after authenticating themselves.

Empower Sustainable Cost Reduction

In deployment, look for solutions that take the burden of delivery away from you, and that cover all IT platforms and integrate all printers on your existing fleet, regardless of make and model. Look for those solutions that offer sustainable cost reductions. It is worth noting that secure pull printing provides significant knock-on effects in carbon, electricity consumption and resource reductions. This consolidation, or virtualization, has successfully occurred right through data centers worldwide.

The era of printing virtualization is upon us with print appliances and print stream compression now taking the low powered load, high availability providing full redundancy, and centralized print servers dramatically simplifying print management tasks and driving down support costs. *(Tip - Help desks typically log 50% of their calls as being printing related. With the enablement of printing virtualization, typically they receive an immediate 30% reduction in printing related calls.)*

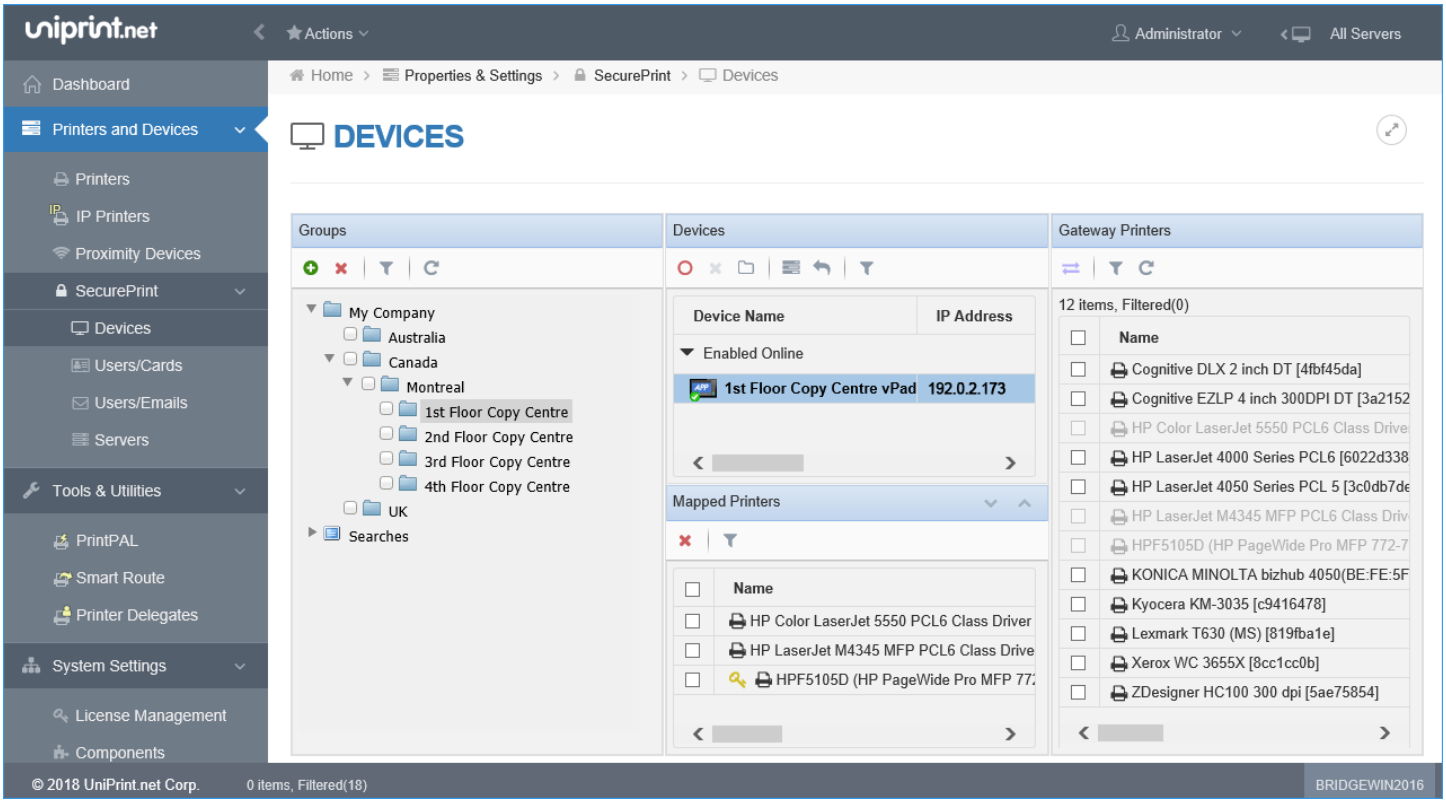
Implementing Secure Printing Process Guidelines

1. Selecting the Appropriate User Policies for your Enterprise Printing

Securing your print infrastructure is of utmost importance, however, ensuring that there are policies in place to further strengthen your security measures is something that cannot be overlooked. Policies for enterprise print environments may include various customized printing restrictions for individual users, or department-based restrictions, depending on the enterprise's specific requirements. After developing and selecting such policies based on printing requirements and organizational needs, IT departments can move towards implementing these print policies. Automatically enforcing print policies through the use of UniPrint Infinity's centralized management console is a great way to implement print policies across your entire enterprise environment from a single point of administration.

American Red Cross

Case Study: The American Red Cross suffered from cumbersome and high maintenance group policies for client printer mapping, causing delays and extra processing time when users attempted to print. Using UniPrint Infinity's PrintPAL utility, the need for complex group policies to map printers to clients was eliminated, as printer mapping policies were automated, saving users a great amount of time and technical support.



2. Securing Enterprise Print Job Release Mechanisms

In classic printing setups, after users hit print, print jobs are sent immediately to the local printer, and released swiftly upon arrival at the printer. Many of these hardcopy output documents are duplicated or unnecessarily printed, resulting in a large percentage of these papers being recycled or left for possible theft! In industries where printed information is highly sensitive and confidential, this presents a huge security risk. Documents left at printers in hospitals or financial institutions can lead to terrible consequences if stolen or breached. When deploying UniPrint Infinity, users print to a virtual print queue (VPQ), where files remain in a secure, compressed form, until released by user authentication at output management devices known as vPads. This secure end to end mechanism prevents print jobs from being printed and not picked up, as users can only release their jobs when physically present at a printer.

CAROLINA CONTAINER

Case Study: Carolina Container, a packaging company based in the USA, had a critical need for print security given the sensitive nature of customer documents and an increasingly mobile workforce. UniPrint overcame this challenge by offering a vPad user authentication device and encryption control functionality. Print jobs are converted into compressed PDF's and encrypted to increase security. Users must also authenticate themselves before the print jobs are pulled and released to the selected printer, adding an additional layer of security.

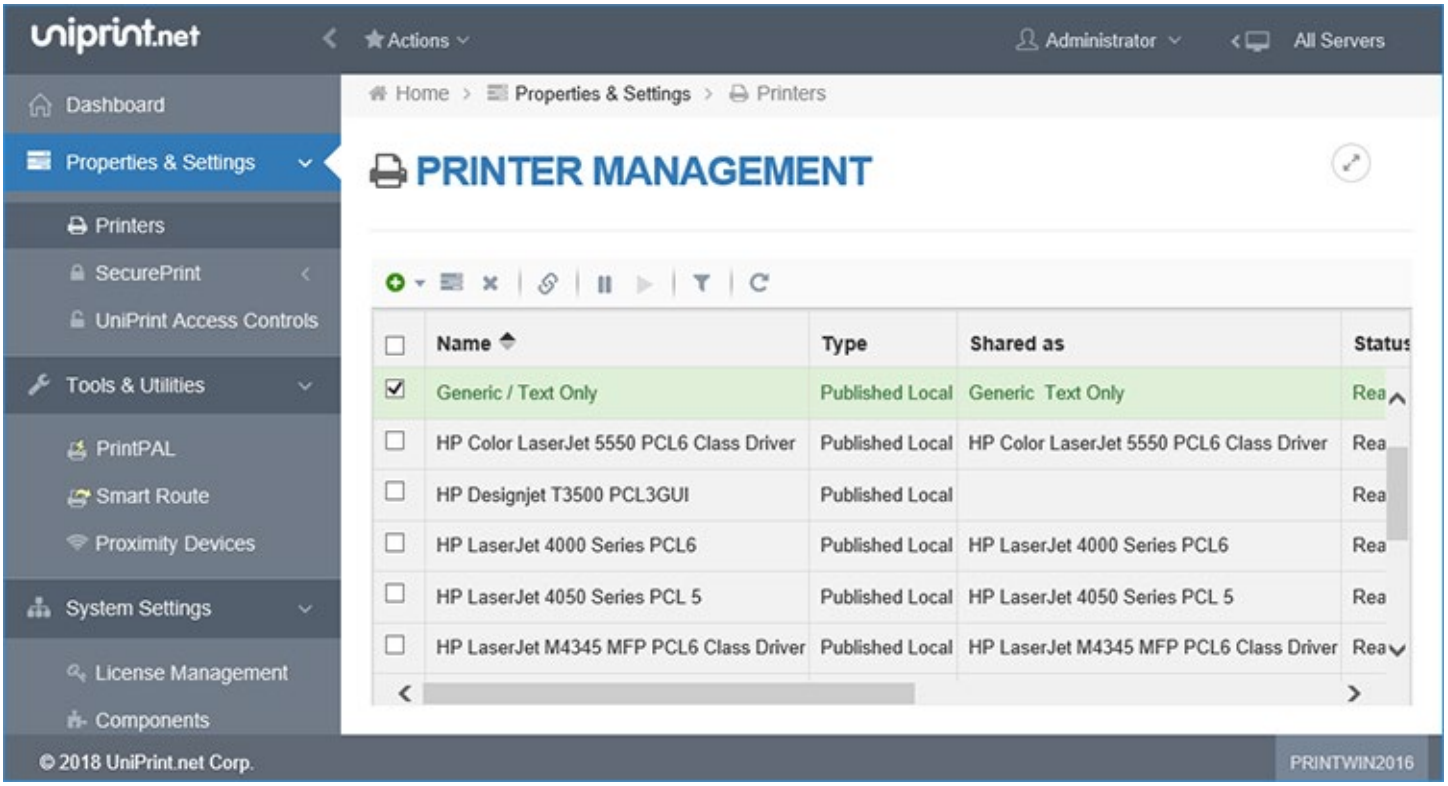
3. Error-free Print Job Routing

Ensuring that print job release mechanisms are completely secure is vital, but so is ensuring that print jobs are sent to functional printers and not printers suffering from downtime. In today's fast-paced enterprise world, where time is of the essence, printer outages are a great inconvenience and may be intolerable in environments such as the healthcare industry. UniPrint Infinity's High Availability module eliminates any single point of failure in the printing system, ensuring that print jobs are always routed to available, functional printers. In a typical printing setup, a failure of any component of the print infrastructure can result in an outage of all printing services. However, with UniPrint Infinity's high availability setup, the bridge and print servers are both duplicated, resulting in automatic redirection of print jobs to the secondary bridge or print servers, in the case of primary server failures. Through this method, users can continue to print seamlessly!

Llywodraeth Cymru
Welsh Government

Case Study: The Welsh Government's scope of operations and nature of sensitive policy matters being worked upon required high levels of security, data protection, and availability of services. With millions of printed output documents produced by a single government department alone each year, it was a vital priority to ensure continuous and maximized uptime with no print outages. Welsh Government extended the UniPrint software to incorporate the High Availability Module to ensure 100% printing uptime of their print infrastructure with a primary to secondary bridge roll over within their Citrix data centers.

The adoption of UniPrint's High Availability module has lead to high availability of print infrastructure with 100% uptime, and made disaster planning and recovery possible.



4. Timed Automatic Document Destruction

While the most common source of data breaches in printing involve hardcopy theft or misplacement, there is another way that thieves can gain access to documents during their print lifecycle. As outlined previously, files are stored in a virtual print queue (VPQ) before being released by users at the vPad. However, what if users forget to authenticate and release their documents? Although there will be no possibility of hardcopy theft, hackers can quite possibly breach the server and view the forgotten print jobs. UniPrint Infinity offers system administrators the ability to set a pre-determined time, based on their organization's requirements, after which all inactive print jobs in a print queue will be destroyed and deleted with no possibility of recovery, ensuring maximum security for unreleased print jobs!

Ensuring Complete Security of Hardcopy Documents

1. Print Activity Statistics and Reporting

After constructing guidelines for a secure printing process and ensuring a secure workflow, it is essential to safeguard printed output as well, as hardcopies happen to be the component of printing that are most prone to theft and breach. A great way for enterprises to start their journey towards safeguarding hardcopy output would be to maintain and store detailed statistics of all user, and system specific activities, along with the ability to automatically or manually create reports to assist administrators in managing the print environment. Print job statistics and reporting should include information such as the name of users who printed specific documents, document names, devices used to create and send print jobs, print job release device details, and the timing and date of released print jobs.

These capabilities make users feel more accountable and reinforce high-integrity driven printing decisions, knowing that their printing activity can be traced, and automated reports are checked regularly by administrators to ensure no counter-productive printing behaviours. UniPrint Infinity's Statistics module enables the tracking of print statistics including the monitoring of who, what, where, and when, as it pertains to printed output, along with subsequent creation of reports based on these findings, outlining printing trends across your enterprise and for individual users. Through these features, UniPrint Infinity allows for enhanced user tracking and security monitoring.

2. Archival of all Print Jobs

Data and document retention is a cumbersome task for any organization, however in certain industries such as the healthcare industry, there are regulations requiring healthcare providers to archive patient data for a certain amount of time, before discarding it. Having to store hardcopy documents can make this even more tedious, and more prone to a possible data breach. Automated archival of all print jobs is an ideal solution for organizations required to retain information. With the ability to view the exact contents of any individual print job, administrators can view exactly what any specific user printed. This is an extremely useful tool for internal print auditing and tracking users who print illicit or unacceptable material from enterprise devices. UniPrint Infinity's Archiving feature stores actual PDF copies of print jobs in an archives database, allowing administrators anytime access to monitor what exactly users are printing, and ensure security and regulatory compliance.

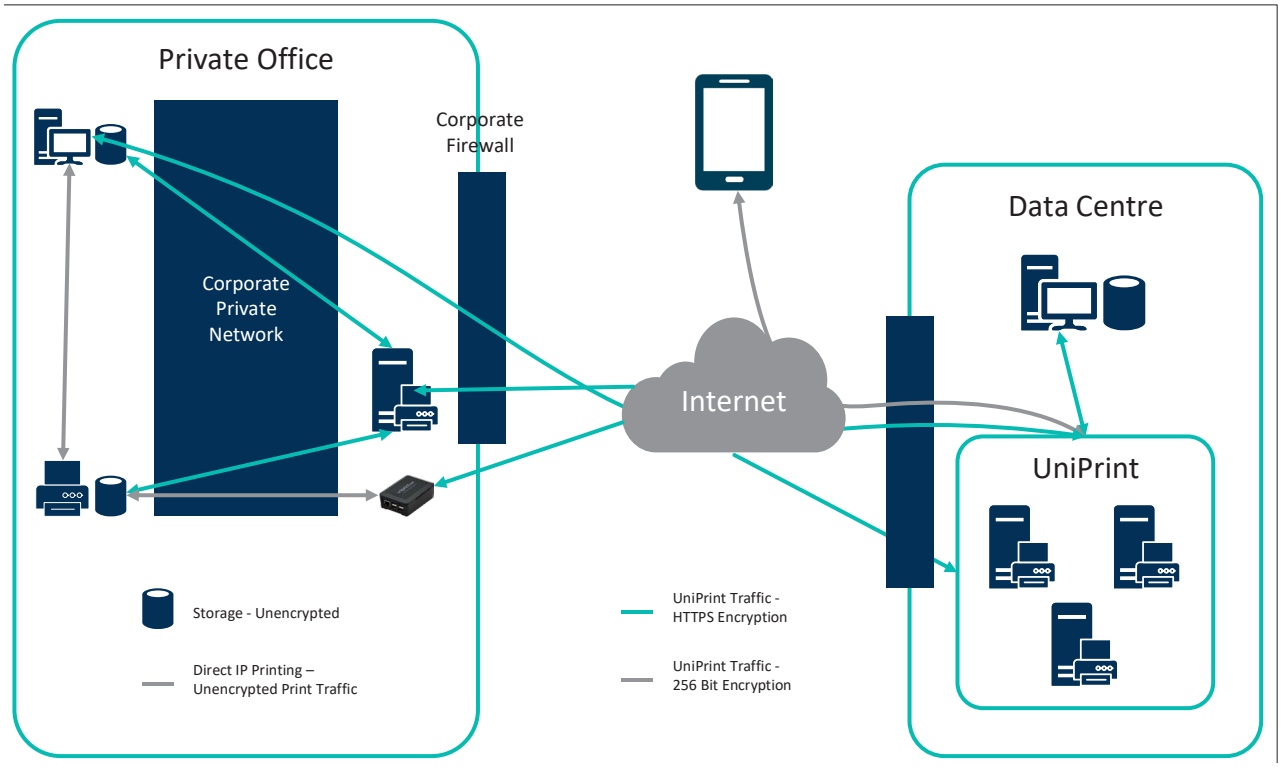
Print Data Network Security

Sniffing presents a significant security risk to enterprise print infrastructures. A network sniffing device or program can be used to illegally capture private data that is transmitted across a network. The sniffer may be a hardware device or a software program that examines traffic on the network and captures snapshots of the data. To prevent sniffing of network print data and further strengthen enterprise print security, organizations should encrypt both the outgoing and incoming print data between the office and data center. This results in data being protected from the moment it leaves the user workstation until the print document is released at the vPad.

Secure by Design: Ultra-Secure End-to-End Encryption

Encrypting enterprise print data may be achieved using third-party print software applications which use the Internet Printing Protocol to create encrypted text. Using secure encryption connections when sending print data such as SSL/TLS, IPsec, or other encryption methods, is a great way to ensure end-to-end print infrastructure security.

With enhanced security and data protection mechanisms in place, UniPrint ensures that enterprise print communication always remains private! UniPrint deploys the latest 64-bit and 256-bit encryption, providing military grade protection for all print job traffic between the corporate network and data center. UniPrint's Secure Print mechanism and vPad devices both enable secure release of documents through the use of randomized authentication codes which are to be entered at the print station, immediately prior to receiving pending print jobs. Subsequently, hardcopy output is protected, and unauthorized users are prevented from obtaining confidential information.

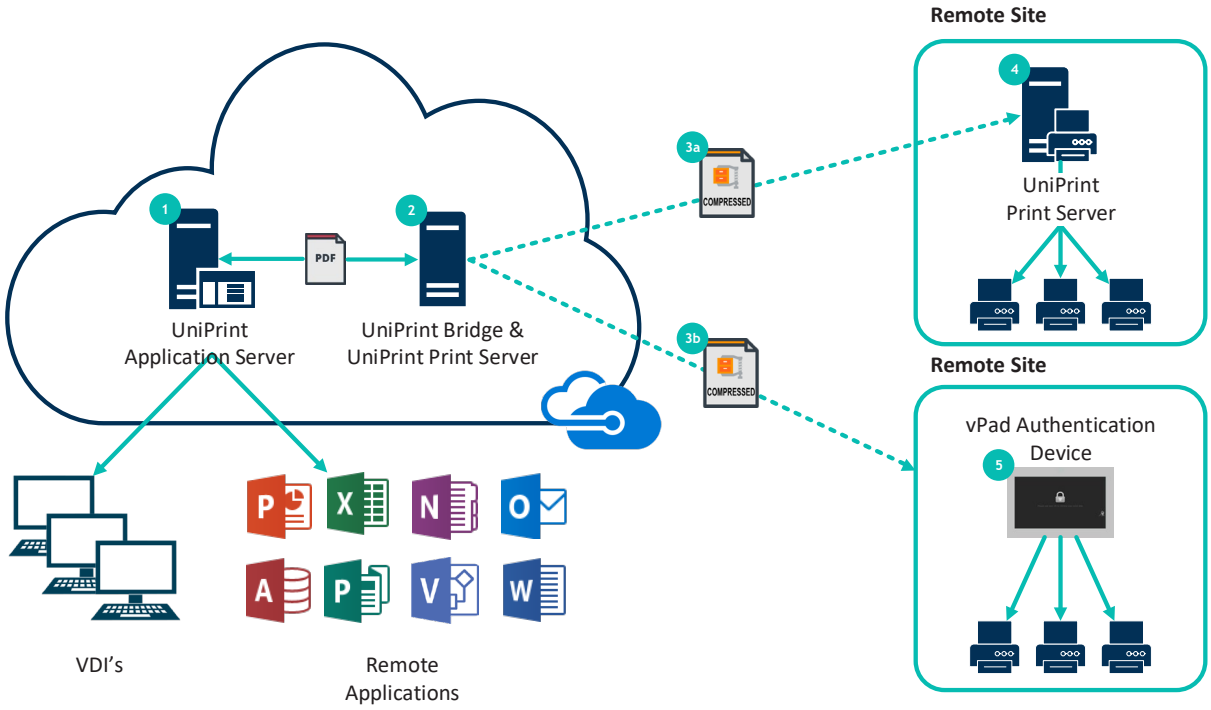


Cloud Printing Security

Adopting cloud services comes with organizations having to give up direct control over their printing infrastructure as it is moved to the cloud, naturally leading to concerns about security. UniPrint Infinity's secure solution ensures complete cloud printing security. Consider the example of cloud printing from a Microsoft Azure cloud environment.

While Microsoft ensures security within the Azure cloud environment, it doesn't secure against print data breaches between the Azure virtual network and the on-premise network, nor within the on-premise network. This is where UniPrint Infinity assist Azure users. UniPrint Infinity is deployed as a pre-configured virtual machine (VM) within Microsoft Azure. This deployment enables mobile printing, secure pull printing and network printing from anywhere in the cloud.

UniPrint Infinity also goes a step further by helping to avoid print data breaches on-premise. On-premise data breaches most often occur at the printer itself. This is where users tend to leave or forget to pick up their sensitive documents that may be inadvertently taken or viewed by unauthorized personnel. UniPrint SecurePrint and pull printing prevents this from occurring. With SecurePrint, the user must initially password protect the print job with a SecurePrint password before they click Print. Their print job is then sent to and stored on the SecurePrint server, awaiting release, not automatically going through to the print server and subsequently printing. After arriving at the printer, the user authenticates using the vPad appliance and enters the SecurePrint password before the print job is released to the printer for printing. For additional security, SecurePrint and the vPad series support multifactor authentication whereby the user is required to tap their RFID or HID card and also enter a SecurePrint password before their print job is released for printing.



Printing Securely Through the Cloud from any Device in the Hybrid Office

UniPrint Vault is a mobile app that works in conjunction with UniPrint Infinity, and SecurePrint, to provide a universal printing experience for users wanting to release print jobs at their on-site or remote home locations. UniPrint Vault provides smartpphone users the flexibility to authenticate and release their print jobs through the cloud in several secure ways (NFC, QR Code, iBeacon) ensuring print jobs securely follow users anywhere.

As the UniPrint Vault requires users to authenticate only when in front of the print station, documents containing sensitive information are released with minimal delay, significantly reducing the risk of a hard-copy theft or misplacement. Trying to maintain consistency and keeping your print environment secure can be a huge challenge. By adopting UniPrint Vault, it gives users the ease of managing their print jobs from a single platform, whether it be documents they'd like to print while at the office or directly from their home printers.

About Process Fusion

Process Fusion is a software company and a cloud solution provider. We help organizations transform inefficient, paper (labor) intensive business processes into a secure, automated, mobile ready Digital First experience for all participants.

Contact:

3250 Bloor Street West
Suite 1000, East Tower
Toronto, Ontario, Canada
M8X 2X9

uniprint.net
processfusion.com

Universal. Unified. Unique.

Process Fusion