WHITE PAPER

Secure by Design:
UniPrint Infinity's Multi-Layer Approach to Cloud Printing Security

The moving of IT infrastructure up to the cloud usually results in companies being obliged to give up monitoring of their IT, with this being delegated to third-party vendors. Naturally, the thought of losing security controls over sensitive corporate data leads to decision-makers raising concerns surrounding the security of their files in the cloud!

UniPrint Infinity's innovative product empowers users with end-to-end cloud printing security. With its multi-layer approach, UniPrint Infinity secures your cloud printing architecture from all angles. This whitepaper will discuss the four key security features offered by UniPrint's cloud printing solution.

One Virtual Print Queue

In today's IT-driven enterprise world, user-friendliness, cost-savings, and enhanced security protection are paramount to the success of any organization! Enterprises must ensure that all their IT systems and related workflows incorporate all three of these features. Printing, over the course of time, has developed a reputation of being a source of pain for both enterprise employees and administrators.

With complicated user interfaces, poor user experience, issues with driver misconfigurations, printer mapping errors, print data security concerns, and network maintenance costs, enterprise printing has been a nightmare for everyone involved.

The advent of cloud printing has helped to solve some of these issues, with organizations moving their infrastructure to the cloud, effectively lowering costs and eliminating printer mapping and related misconfiguration issues. UniPrint Infinity's Virtual Print Queue (VPQ) adds a whole new level of security to cloud printing!

The implementation of UniPrint's VPQ to your cloud printing environment means users printing from cloud environments such as Microsoft Azure send their print jobs to a single virtual print queue when they print from their workstations or mobile devices. This eliminates the hassle of monitoring issues resulting from multiple print queues, with only one print queue now being used for all enterprise users! After hitting print from their user sessions, the selected print jobs are sent to the VPQ, where they remain until users make their way to enabled corporate printers.

256-Bit End-to-End Data Encryption and Secure Pull Printing

Encrypting corporate print data is of utmost importance to add an additional layer of security to print traffic as it flows to and from the local network. Without encryption of print data, print traffic is highly susceptible to network sniffing, wherein a device or software may be deployed to capture private network data that is being transmitted across the company's network.

Print data is often encrypted using applications which implement the Internet Printing Protocol to develop encrypted text. Adopting the use of secure connections when routing print traffic, such as SSL/TLS, IPsec, or other encryption methods, is another useful way to ensure complete print security.

With state-of-the-art data protection mechanisms, UniPrint's technology ensures that enterprise print traffic always remains secure and confidential. Using the latest 256-bit encryption which provides military grade protection for all print job traffic travelling between networks, enterprise decision-makers can rest assured that their vital corporate information is safe with UniPrint Infinity.

By deploying UniPrint's Infinity Secure Pull Printing solution, enterprise customers can achieve dual print security, as they add user-authenticated pull printing to the existing 256-bit encryption that is offered by UniPrint Infinity.

Secure pull printing significantly reduces the risk of possible security breaches, or corporate intelligence being stolen, as a result of hardcopy output containing sensitive corporate date being left at printers without being picked up or being obtained by unauthorized individuals.

With enabled secure pull printing, users are forced to print consciously, and multi-factor authentication is required to release their print jobs for printing.

For multi-factor authentication, the UniPrint vPad comes with a built-in RFID or HID reader. External card readers are also available for use. Since the vPad is compatible with any printer make and model, standardizing an existing printer fleet is not necessary.

Secure Cloud Printing without VPN

In the past, printers were simple machines where a user would print to one local printer and then go retrieve whatever document they printed. There have always been security issues with legacy printers such as the theft of documentation from the printer before it can be collected. Unfortunately, innovation in software and technology has opened doors to a wide array of new print security threats enterprises must be aware of.

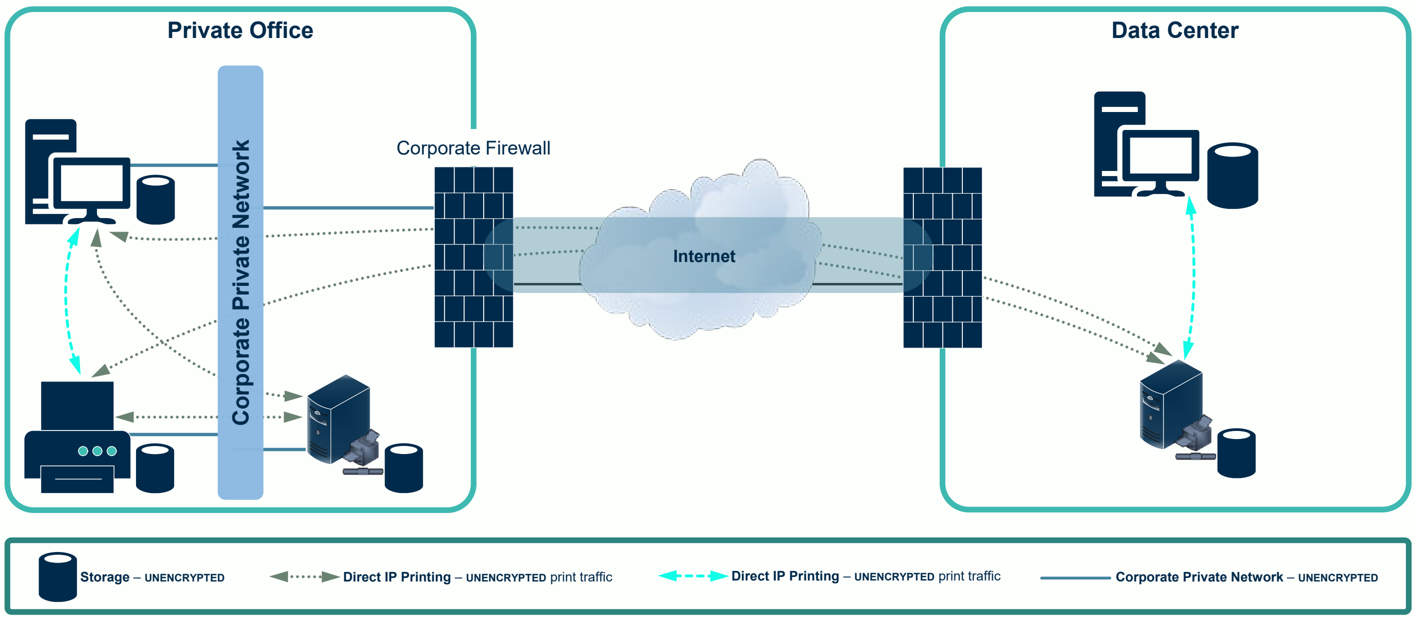
Network printers are often a serious data threat as these machines often handle sensitive information and could provide an access route to other computers on your network. Additionally, advanced multi-function printers are subject to an even larger number of print security threats because they are essentially self-contained computers with their own hard drive, operating system, and direct network connection.

One of the less obvious print security risks is "sniffing" network printer traffic. A network sniffer can be used to illegally capture confidential data being transmitted on a network. It can be a hardware device or a separate software program that examines traffic on the network and takes snapshot copies of the data.

It is not hard for hackers to "sniff" the data being sent back and forth to the printer given how easy it is to obtain software (from the dark web of course) that literally does it for them.

To prevent users on the network from sniffing print jobs as they go to the printer, find out if printers or print servers support encrypted connections to and from the workstations on the network. A great way to mitigate this problem is by using secure virtual private network (VPN) connections when sending print data such as SSL/TLS, IPsec, or other encryption methods.

Printing without UniPrint VPN is required for security


Private Office
Corporate Private Network
Corporate Firewall
Internet
Data Center
Storage – UNENCRYPTED
Direct IP Printing – UNENCRYPTED print traffic
Direct IP Printing – UNENCRYPTED print traffic
Corporate Private Network – UNENCRYPTED

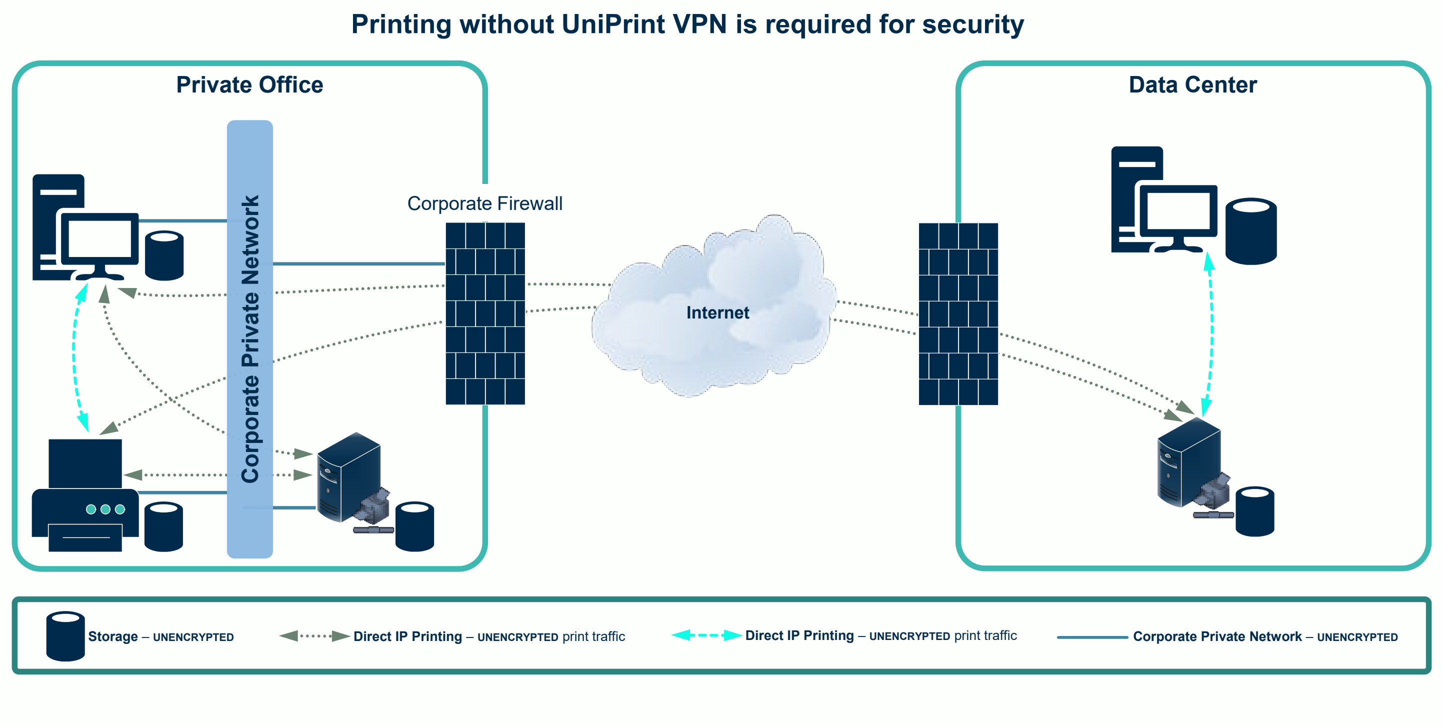
Using a Virtual Private Network

A virtual private network essentially functions as a connection between two points, using the Internet as the connection medium, however, heavily fortified by a firewall at both ends. With VPNs encrypting all communication over the internet, they are essentially a private channel used from one end to another and can be used to setup a secure printing network, so that the risk of third-party access to enterprise print data is non-existent.

Using a Virtual Private Network

A virtual private network essentially functions as a connection between two points, using the Internet as the connection medium, however, heavily fortified by a firewall at both ends. With VPNs encrypting all communication over the internet, they are essentially a private channel used from one end to another and can be used to setup a secure printing network, so that the risk of third-party access to enterprise print data is non-existent.

However, the use of VPNs for printing is not practical for most enterprises. This is mainly due to slower and congested internet speeds from printing image and text rich documents, causing poor performance. Spooled print data can be many times the size of the original document. The bloated print data can wreak havoc on bandwidth availability for critical traffic such as ICA, RDP, and PCoIP. The normal solution is to restrict the bandwidth available for print data. However, this leads to slow printing for users.


Printing without UniPrint VPN is required for security
Private Office
Corporate Private Network
Corporate Firewall
Internet
Data Center
Storage – UNENCRYPTED
Direct IP Printing – UNENCRYPTED print traffic
Direct IP Printing – UNENCRYPTED print traffic
Corporate Private Network – UNENCRYPTED

VPN connections also tend to have high monthly costs and ongoing maintenance expenses. In addition to this, VPN-based print networks do not allow for users to print from remote locations or when away from the office, as static IP addresses are necessary to assign printers to users in VPN settings.

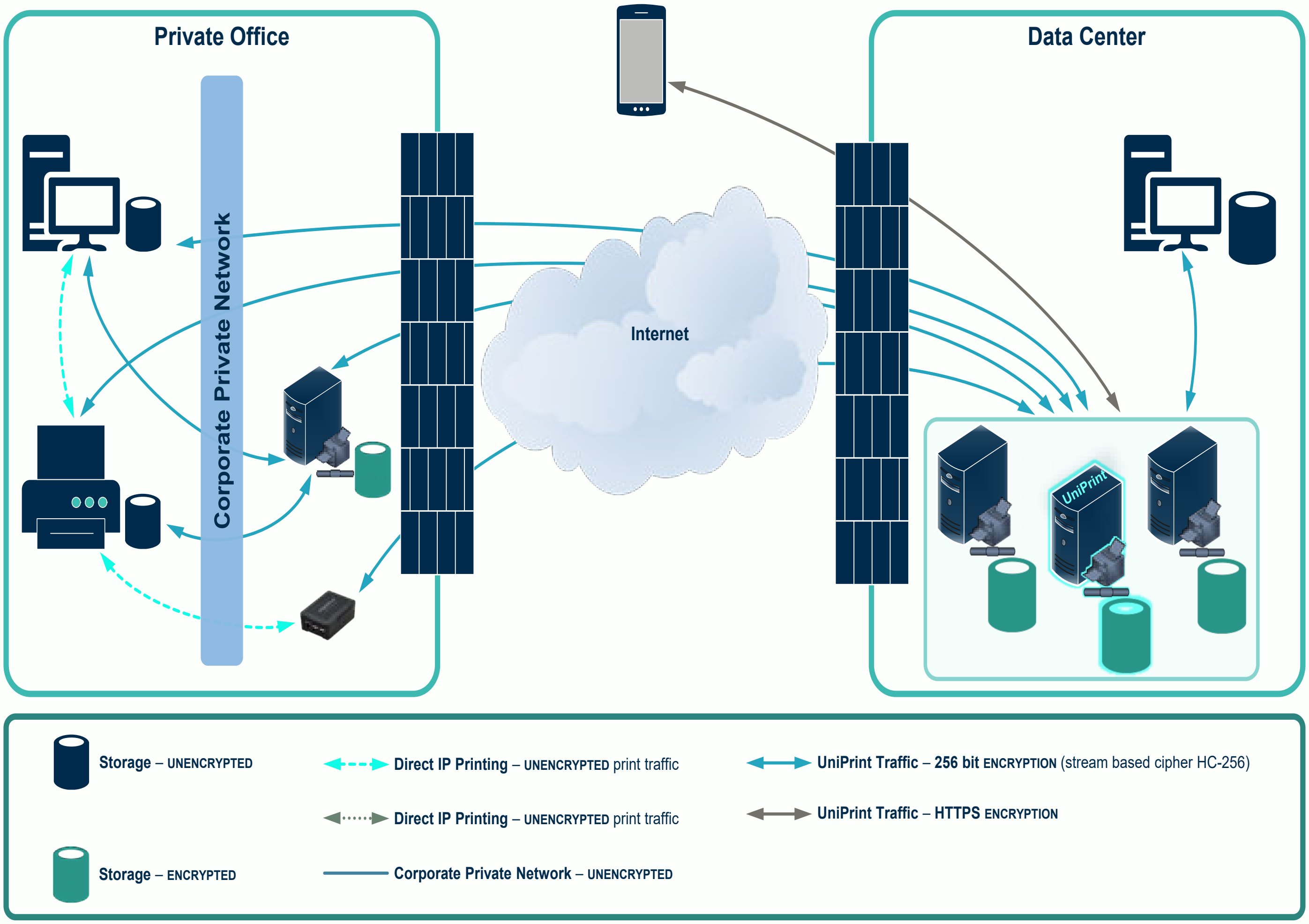
Entire networking reworking must also be carried out when adopting VPN-based enterprise printing, as IP addresses must be unique within a particular VPN network. Assigning dynamic IP addresses is extremely costly to implement and is therefore simply unaffordable for most companies.

Using UniPrint Infinity

By deploying UniPrint Infinity's secure cloud printing solution, administrators can solve all these issues that come with VPN-based printing networks, while enterprise executives can save costs and focus on other areas of corporate need. All print traffic is encrypted, and administrators can setup remote print servers, while managing printer mapping through the PrintPAL utility, without having to set up site-to-site VPNs.

Along with high-level security enabled through secure pull printing and the latest print data encryption, UniPrint Infinity provides cloud users with the benefit of premium print security, while saving on costly VPN setups.

Printing with UniPrint VPN is not required


Private Office
Corporate Private Network
Internet
Data Center
UniPrint
Storage – UNENCRYPTED
Storage – ENCRYPTED
Direct IP Printing – UNENCRYPTED print traffic
Direct IP Printing – UNENCRYPTED print traffic
Corporate Private Network – UNENCRYPTED
UniPrint Traffic – 256 bit ENCRYPTION (stream based cipher HC-256)
UniPrint Traffic – HTTPS ENCRYPTION

The setup also enables direct IP printing from workstations to network printers, which removes the complicated setup of having a dedicated print server for printing purposes, while keeping unencrypted print data safe within the corporate network.

UniPrint Infinity and the vPad also eliminates both slow printing and bandwidth issues by compressing the data transmitted from the printer server in the data center, and the decompressing it at the remote location. This reduces the amount of bandwidth consumed, enabling fast, trouble-free printing.

By integrating serverless printing with secure cloud printing, it is possible to manage your Windows printing, VMWare VDI, Citrix XA/XD, or cloud environment under one management platform without remote print servers.

Our Multi-Layer Security Approach

Take the example of UniPrint Infinity operating in an Azure environment. While Microsoft does establish a secure Azure cloud operating environment, it does not guarantee protection against possible print data breaches between the cloud and the network. This is where UniPrint Infinity proves its benefit for any cloud environment. UniPrint Infinity is presented as a pre-configured virtual machine (VM) within the Azure cloud environment, enabling secure pull printing and mobile printing from the cloud.

Initially, UniPrint Infinity converts and encrypts all print jobs to secure, 256-bit encrypted PDF print jobs, to build the first line of defense to print data breaches, even before the document is physically printed. With most enterprise print data breaches often occurring at the print stations and being associated with unauthorized hardcopy obtainment, UniPrint Infinity goes on to significantly reduce this risk through its virtual print queue and secure pull printing.

Users often mistakenly leave their printed documents at the printer, out of forgetfulness, leaving sensitive information open to anyone. UniPrint's SecurePrint and pull printing mechanisms prevent this situation altogether. UniPrint's SecurePrint forces users to password-protect their desired print jobs before they initially hit Print. Pending print jobs are then delivered to and remain on the SecurePrint server, waiting to be released, rather than automatically going through print servers and printing, as takes place in traditional printing environments. After arriving at the print release station and authenticating, users simply enter their secure password before their pending documents are finally released to the printer for retrieval.

For further security, UniPrint Infinity also provides multifactor authentication, consisting of the user being required to authenticate via RFID or HID technology, along with entering the SecurePrint password before their print job is released for printing. 2019

Try UniPrint InfinityCloud for a FREE
30-day trial and see how easy cloud printing can be

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