uniprint

WHITE PAPER

Secure Cloud Printing for Microsoft Office 365 and Azure

Process Fusion

Introduction

Since its release back in 2012, demand for Microsoft Office 365 productivity software has grown exponentially as organizations worldwide enjoy the freedom of transferring responsibility for managing servers and applications to a Cloud based service model. The Microsoft Azure platform takes that one stage further offering an open and scalable Cloud computing platform as a service, providing a highly available Virtual Machine (VM) Cloud service payable on a monthly fee.

For subscribers, critical services and server functions can now be moved with relative ease but what about printing, how realistic is that? Users are struggling with print file sizes and resultant bandwidth issues, not to mention security and compliance concerns. This paper explores the topic further and considers what happens when subscribers elect to migrate everything, including print servers, offsite into the Cloud and pitfalls to avoid.

Some Obvious, But Frequently Understated Facts

Printing and off-premise Cloud adoption, be it provided by Microsoft Azure or IBM Softlayer, literally sit at opposite ends of an organization's infrastructure spectrum. With Cloud adoption, IT admins take advantage of virtualized servers managed elsewhere and that includes print. On the face of it, this should be an overwhelming IT relief, given that print queries represent the second highest volume of inbound IT support desk queries. Yet with printing, the physical to virtual process itself is reversed – users are taking something virtual and making it physical. Printing therefore needs specialized treatment to secure a universal printing infrastructure from any location in the world. Once achieved, Azure based companies can drastically simplify their intra-organizational printing structures and flatten the complexities of coordinating disparate hardware across their widely distributed environments.

Large government departments, financial organizations and healthcare institutions are set to be the big winners from optimized Azure printing. Many of these institutions connect hundreds (if not thousands) of disparate devices and printers, sometimes across multiple locations. As the workplace becomes more mobile, employees need to print from multiple locations in different parts of a building, different offices, or often, from different countries. Struggling with installing different printer drivers each time that an employee needs to print to a new printer is not just annoying, but also time-consuming and a drain on productivity.

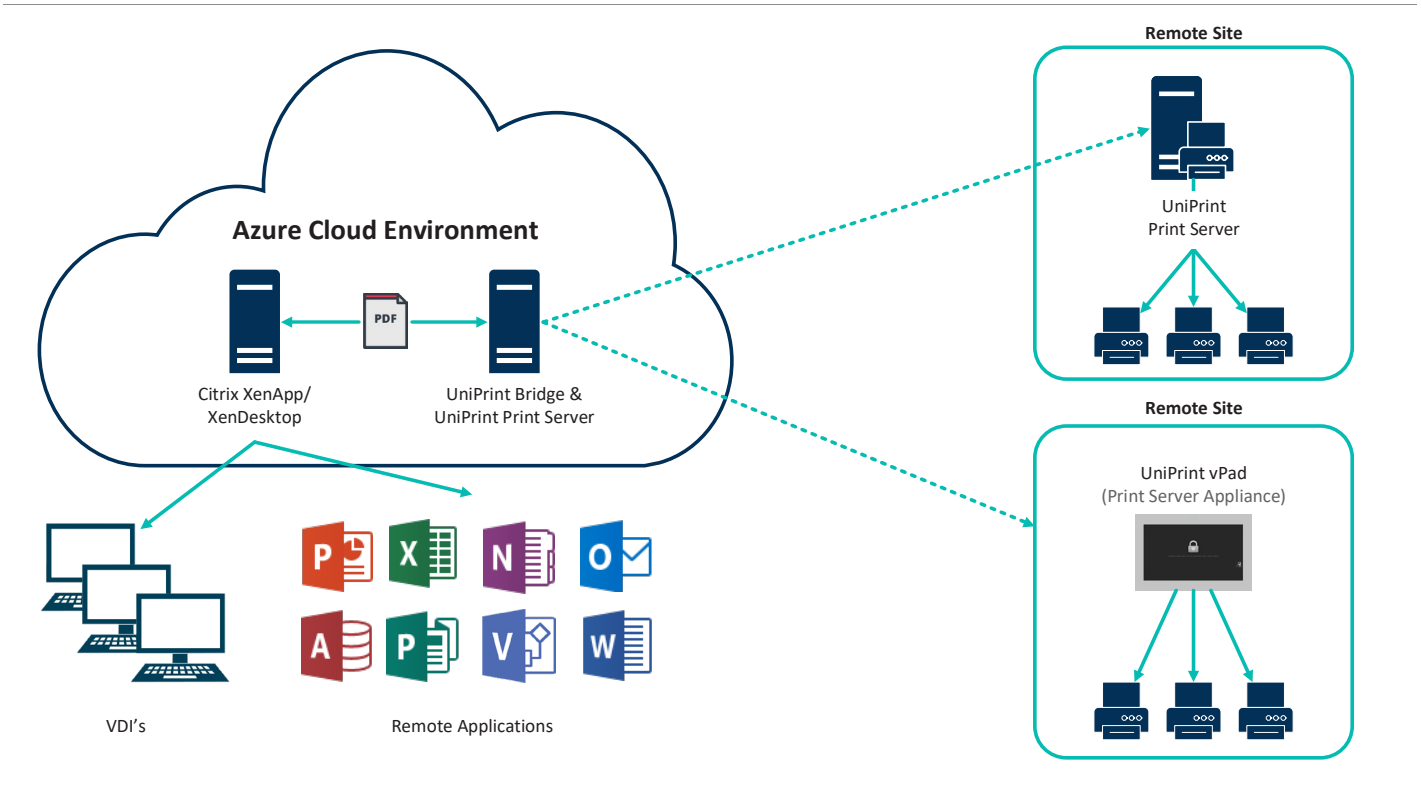
Microsoft Azure on the other hand, connects printers to the web so that they can be accessed from anywhere and at anytime from web-connected devices. Instead of installing unique drivers for every new printer, organizations can print from anywhere, so long as both the printer and the device are linked to the Cloud printing service. Even more, with Cloud printing services, you could print from virtually any device that can connect to the service - including tablets and mobile phones. The BYOD trend now really comes of age.

Security Concerns Still Mean Private Or Hybrid Cloud Adoption

However many times, organizations cite high levels of security concerns that make them hesitant from total adoption of Microsoft Cloud and elect to maintain their own private Cloud or hybrid Cloud that still maintains their own security and access over sensitive data. But implementing private and hybrid Clouds for printing isn't without its own set of complications.

Consider the infrastructure of government departments as just one example. Every department has its own structure for printing, each with Active Directories, and thousands of users dispersed over wide geographic areas. Consolidating printing in this situation requires aligning all the printers, drivers, devices, and users within the system - something that can't be done easily or efficiently. Even more, this system is routinely bogged down with driver updates creating a giant logistical headache. Every device needs to be updated for every driver update for every printer when the updates crop up. And for the devices that don't have printer drivers - those will never be able to print at all.

The only option is to deploy a universal printer driver solution like UniPrint InfinityClou's UPD, that can seamlessly connect and manage all printers within complex enterprise environments and ensures that users can identify the right printer without extraneous hassle. The structure should require as little effort on the user's part as possible, so this particular iteration of Cloud services must keep the location in mind. Printers should automatically connect to whatever network makes the most sense (like the library in a university or the particular building a printer is attached to) so that only a few printers out of all the printers in the Cloud get exposed to each user based on localities.



Creation Of A Virtual Print Queue (VPQ) For Secure Microsoft Azure Printing

With these concerns in mind, those enterprises that have adopted Microsoft Azure have sought to take extra steps for enhanced security, compatibility and authentication of their print estate. Some have simplified intra-organizational printing structures to align the printers, drivers, devices and users within the system through adoption of UniPrint InfinityCloud, an encompassing, effective and efficient enterprise cloud printing solution. The software suite comes with user-authenticated pull printing that improves document security, and enables a high availability setup with load balancing capabilities that allows full redundancy to maximize printing uptime, all of which are key to driving enterprise Cloud success. Today, large organisations are gaining essential 'Secure Pull Printing' through the Cloud through creation of a Virtual Print Queue that allows them to release the print job only when users authenticate their credentials on an attached low cost print appliance such as a vPad user authentication device.

This authentication releases the documents only to the intended recipients so that print output never falls into the wrong hands or lies, unforsaken, at the side of the wrong printer. With this secure printing to the Cloud, Microsoft Azure users are also assured of a reliable print trail for auditing and compliance. This is an increasingly important point in Europe where organisations will shortly have only 24 hours to accurately report and detail data breaches to the Information Commissioners Office or face massive fines. This includes loss or breach of their print data. UniPrint InfinityCloud is the only solution to identify and plug the gap on data breaches of print from Microsoft Azure environments.

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