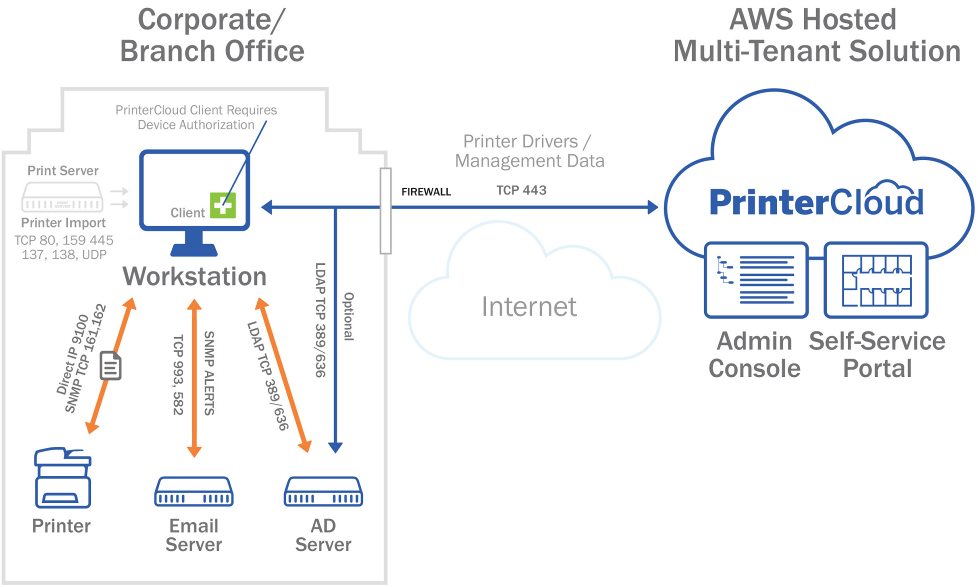
PrinterLogic

PrinterCloud Architectural Overview

PrinterCloud Architectural Overview

PrinterLogic provides PrinterCloud, an enterprise print management solution for IT organizations who want a better, more efficient way to manage printers and drivers throughout the enterprise. PrinterCloud consists of a server component that is hosted in the cloud on Amazon Web Services (AWS) and a client installed on each workstation. This method of print management converts the environment to centrally-managed direct IP printing, eliminating the need for print servers in the environment. Because print jobs go to the printer via direct IP and do not go through the PrinterCloud instance, there is no single point of failure and no additional WAN traffic. Also, there is no need for Group Policy Objects (GPOs) or scripting to deploy and manage printers and printer drivers on end-user workstations.



Amazon Web Services Security

Amazon Web Services (AWS) employs extensive security measures for the data stored in its cloud infrastructure. AWS provides an ISO 27001 certificate for their service infrastructure, which is a widely recognized international security management standard.

PrinterCloud Instance and Client Communications

PrinterCloud is a SaaS-based application that is hosted in the cloud on AWS. The software manages and deploys printers in the organization and is built to use the secure web protocol HTTPS and a security token for communication between the client and the PrinterCloud instance.

PrinterCloud uses a client/server model to manage printer drivers and profiles. The client is a small piece of software installed on individual end-user workstations and is designed to communicate with the PrinterCloud instance using a security token created by the PrinterCloud admin. Upon logging into the workstation and on a scheduled interval, the client sends an HTTPS request to the PrinterCloud instance using its security token to discover if there are any activities assigned to the system or the active logged-in user. If the client does not have a security token, it will be denied communication. Upon receiving a security token that the PrinterCloud admin generates, future client updates and communication to the server are done through HTTPS on port 443, keeping all interactions secure over an encrypted port. It also has the advantage of not needing to open additional ports in the firewall. Expiration lengths can be assigned to any security tokens created by the PrinterCloud admin thus, any tokens not used to authorize a newly installed client within the allotted time frame become invalid, and a new one will need to be generated.

Printer drivers are uploaded into the PrinterCloud instance using either a manual upload or automatic method via a printer import tool. A security token is required for both the workstation and the print server to function properly.

The administrator defines in the interface if a printer driver needs to be installed by the client. When an authorized client checks in, and if a printer needs to be installed, the client will first scan the local workstation for the driver needed. If the driver is not available locally, it will automatically download the driver from the PrinterCloud instance (or optional designated driver cache) and install it using system service privileges on the workstation. The client then configures the driver according to the profile defined in the PrinterCloud Admin Console.

When printer drivers are downloaded from the PrinterCloud instance they are sent over an encrypted port (443) using HTTPS. Optionally the printer drivers can be stored in a local cache on a file server. In this model, the client that is installed on the file server must first receive a security token allowing communication, once a security token has been received the printer drivers are transferred from the PrinterCloud instance over port 443 to a Windows file share on the specified file server. Other clients retrieve the printer driver from the file share using port 445.

Print Job Traffic

Print jobs are sent from the client workstation directly to the printer via direct IP using port 9100 by default and the installed printer driver. Since the print job does not travel to the PrinterCloud instance, it is restricted to the local area network segment created by the IT admin. Metadata from the successful print jobs is sent via HTTPS to the PrinterCloud instance for reporting purposes. Again, a valid security token is required for client to PrinterCloud instance communication.

Optional Active Directory Integration

PrinterCloud employs Active Directory to authenticate and authorize users, groups, and computers for a variety of optional features including AD user account creation, AD login access, pull printing and mobile printing.

With the PrinterCloud instance residing on Amazon Web Services and outside the firewall, IT Admins need to ensure that their firewall rules allow access to their Active Directory port (typically 389 for non-secure or 636 for secure) from the PrinterCloud IP address. The IP address of your PrinterCloud instance can be obtained from PrinterCloud support by sending an email to support@printerlogic.com.

The PrinterCloud instance uses read-only access to the Active Directory server. As a result, PrinterCloud does not write any data to Active Directory. Each time an authentication or Active Directory membership is required, PrinterCloud will request the Active Directory using a BIND service account. The BIND service account information will be encrypted and stored in the PrinterCloud database.

NOTE: For added security, you can use a BIND service account with read-only permissions.

The client installed on the end-user workstation does not connect directly to the PrinterCloud server for authorizing end-users. Instead, the client authenticates directly against Active Directory.

Conclusion

PrinterCloud provides a single integrated platform designed to enable enterprise customers to eliminate print servers. This SaaS solution converts your printing environment to centrally-managed direct IP printing and includes printer driver deployment and management, print job auditing and reporting, and centralized printer management from a single web-based console that has a tangible return on investment from hard-cost print server elimination to saved productivity by eliminating GPOs and scripting and reduced help desk calls.