PrinterLogic by VASION

Supporting a Secure, Hybrid Workforce with Off-Network Printing

How Off-Network Printing makes printing accessible and secure in today's Zero Trust network-access (ZTNA) environments

Table of Contents

The Dilemma: Maintaining Network Security while Allowing Open Access 3

The Solution: Off-Network Printing 4

Off-Network Printing: How It Works 5

A Unified Platform that Goes Beyond Printing 8

Conclusion 9

The Dilemma: Maintaining Network Security while Allowing Open Access

More than ever, CIOs are committed to secure networks and data, like isolating possible attack surfaces (including printers) on highly secure networks with restricted access. Meanwhile, your organization relies on contractors and remote employees who aren't on the company network, but need to print, and your IT department must provide them easy access to the resources they need to do their jobs. The dilemma is between those two needs: How do I allow all workers open access to company resources while maintaining strict network security?

Do any of these statements sound like you?

1. **You need to adopt Zero Trust Network Access.** According to Gartner, old security models that assume "inside means trusted" and "outside means untrusted" are quickly becoming obsolete in today's work environment. With increased user mobility and dependence on connected business partners, virtual private networks (VPNs) and demilitarized zones (DMZs) became common. However, these solutions offered too much implicit trust to users and led to abuses by hackers. Today's organizations require anytime, anywhere access to any application, regardless of a user's location. Zero Trust Network Access (ZTNA) addresses this need. It abstracts and centralizes access mechanisms that are managed by specialized security engineers.

   In a Zero Trust environment, even regular (on-site) employees are on a separate network from where data servers and printers reside. Zero Trust levels the playing field for all workers and demands verification from everyone. It begins with a policy of denying access and then grants access based on user identity, the device, and other attributes that provide context to authorize everyone. Zero Trust Network Access appeals to organizations looking for flexible and adaptive ways to serve business ecosystems, including all types of workers and partners.

2. **You're supporting a hybrid organization.** Your organization, as well as most companies today, supports a hybrid model–some employees work from a local office, while some work from home on their home networks, and some utilize a little of both situations. These individuals, regardless of where they're located, need access to the company's printers to complete their work. On top of that, your organization regularly employs contractors on-site who need access to printers just the same. In the past, you may have allowed these workers access to a guest network with limited access. You need a solution that provides everyone printing access, no matter their access level or location.

3. **Your organization's affiliate offices need to print.** Many companies work with and support employees in affiliate offices. For example, a hospital's affiliate clinic nurse must print after-visit summaries using the hospital's medical records (EMR) software. The clinic is an independent business, not connected to the hospital's secure network. In these cases, you must set up a connection that allows those offices to function alongside your main offices easily.

4. **You want to eliminate as much local infrastructure as possible.** Remote printing solutions often require additional local infrastructure, scripting, and/or VPNs to facilitate print jobs securely connecting and traveling to network printers. VPNs, especially to support numerous employees, can quickly become expensive and bog down your network.

The Solution: Off-Network Printing

Remote printing can coexist with a secure Zero Trust Architecture through Vasion's Off-Network Printing. It bridges the gap between a seamless printing experience for your remote and mobile workforce and solidifies security with user identity authentication before printing every time.

As part of our Advanced Security Bundle—add-on functionality to the Vasion Automate Core feature set—this maintains the convenience for end users to print while ensuring that print jobs are routed with secure connections from the workstation to the printer tray. You can ensure all users who should get printing access get printing access, regardless of where they are located, and reap the subsequent advantages:

Reduce Local Infrastructure and Cost
With Off-Network Printing, customers can eliminate additional infrastructure beyond just printer servers, like VPNs, hosting services, and external access portals to accommodate employee, contractor, partner, and affiliate remote printing needs. Off-Network Cloud Printing can even eliminate the need for an Internal Routing Service since it is a fully cloud-hosted solution.

Enable Cloud-Based Printing
With Off-Network Cloud Printing, eliminate local print-routing infrastructure by taking remote printing to the cloud while keeping off-network end users from your organization's internal network.

Encrypt Data End-to-End

In the default Off-Network Printing configuration, print jobs are encrypted at their origination point and routed to their destination printer through the PrinterLogic SaaS gateway service. Jobs through Off-Network Cloud Printing are encrypted while temporarily at rest in the cloud and then downloaded to the printer. Both features ensure that data remains secure while traveling off the network, no matter what.

Support Secure Release Printing

Secure Release Printing is vital for off-network users to protect sensitive information and the confidentiality of their documents by holding the print job until the user or a collaborator goes to the printer and authenticates. Off-Network Cloud Printing allows users to release print jobs even when their workstation is offline.

Off-Network Printing: How It Works

Unlike direct IP printing, where your workstation sends print jobs through a direct connection to the printer, Off-Network Printing routes print jobs through the cloud to printers behind your company firewall. Two components make the solution work: the External Gateway and the Internal Routing Service.

The External Gateway

The External Gateway receives off-network print jobs from remote workstations. In the PrinterLogic-hosted model, the External Gateway is hosted as a service in AWS by PrinterLogic. In the customer-hosted model, the External Gateway is hosted by the customer with an SSL (Secure Sockets Layer) certificate. In addition, combined hosting models (known as hybrid models) can be used. The External Gateway uses port 443 to receive print jobs and uses WebSockets to transfer incoming print jobs down to the Internal Routing Service. Print traffic is encrypted using the TLS (Transport Layer Security) cryptographic protocol.

The Internal Routing Service

The Internal Routing Service maintains a constant connection with the External Gateway to watch for print jobs. When the External Gateway receives a print job, the Internal Routing Service opens a new connection for that job, then downloads and delivers it to the designated printer. For organizations that need zero on-prem infrastructure, Off-Network Cloud Printing, described below, eliminates the need for the Internal Routing Service. Instead, this option installs the equivalent functionality as an embedded application on the printer itself that communicates to a storage microservice in the cloud directly to download available jobs.

Four Configuration Options of Off-Network Printing

1. **PrinterLogic-hosted model**

   The preferred method for Off-Network Printing employs an External Gateway hosted by PrinterLogic in AWS. This simplifies configuration because IT only needs to set up the Internal Routing Service inside the organization's network. This service uses WebSockets to maintain a connection with PrinterLogic's cloud-based Gateway. When a print job is received, the Internal Routing service pulls the print job into the customer network.

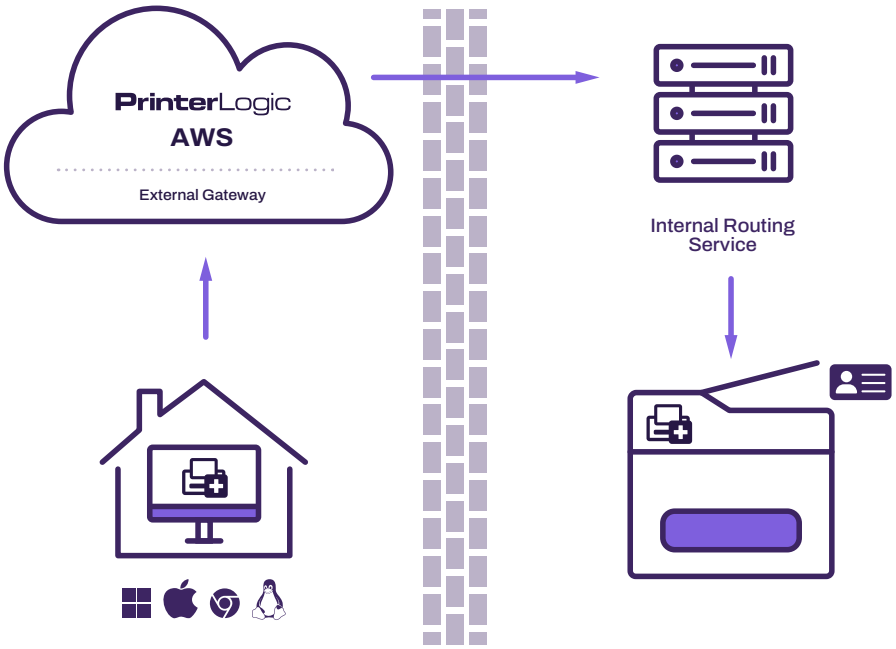

FIGURE 1

2. Self-hosted Model

For various reasons, IT may prefer to host the External Gateway in the organization's data center or private cloud. PrinterLogic supports these scenarios with the following caveats: First, the External Gateway must be accessible to off-network users and have a publicly available IP address and DNS name. Second, it must also have a certificate signed by a Trusted Certificate Authority. Third, port 443 must be open for incoming connections.

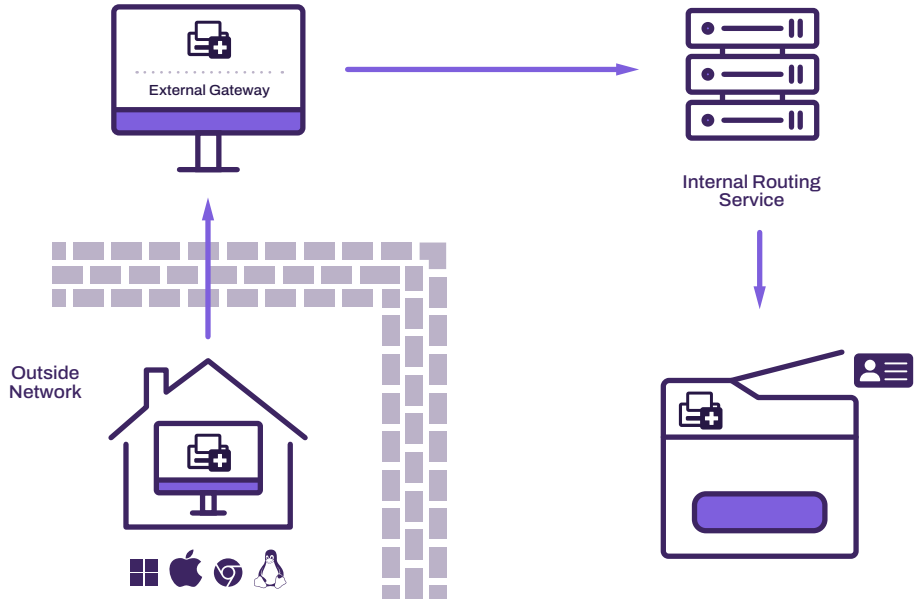

FIGURE 2

3. Hybrid Model

PrinterLogic-hosted and self-hosted scenarios can be used together to provide flexibility and redundancy in configurations. This scenario is illustrated in Figure 3.

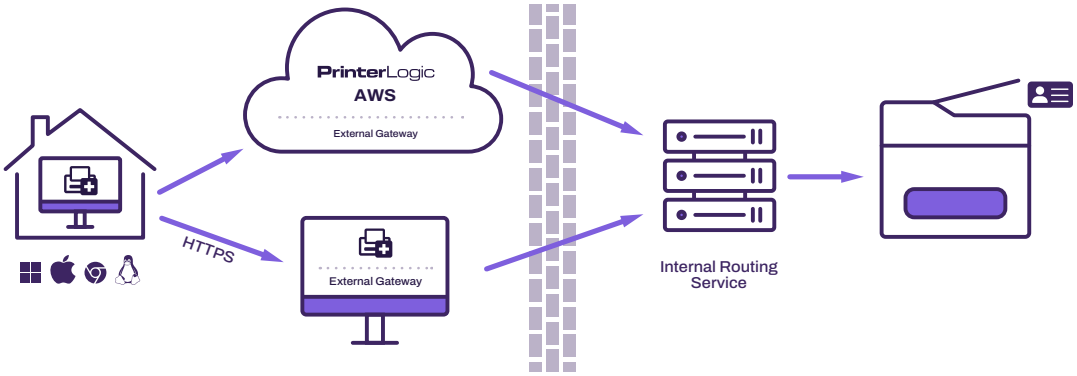

FIGURE 3

4. **Off-Network Cloud Printing**

Off-Network Printing has proved to be a key solution for IT administrators to enable their remote and mobile workforce to print and eliminate the support of local infrastructure like the Internal Routing Service. Off-Network Cloud Printing eliminates the print routing infrastructure hosted on a workstation and instead temporarily holds print jobs at rest in a cloud storage microservice and communicates with a small app on the designated printer.

PrinterLogic can be hosted in AWS or Azure public cloud, which receives incoming print jobs from remote workstations over port 443. Customer data is logically separated into Amazon Elastic File System (EFS) folders within the cloud. Jobs are sent to the PrinterLogic ONCP External Gateway via an encrypted tunnel, where they are given a universally unique identifier to ensure that the job will route to the correct place. The print jobs are held in an encrypted state, temporarily at rest in the cloud storage microservice, until the destination printer is ready to receive the job.

The ONCP application, installed on a designated off-network printer's Control Panel Application (CPA), calls to the storage, then downloads the job over port 443, and the document is printed. If the print job was originally held for Secure Release, this communication is triggered by the user releasing the job from the Control Panel Application installed on the printer.

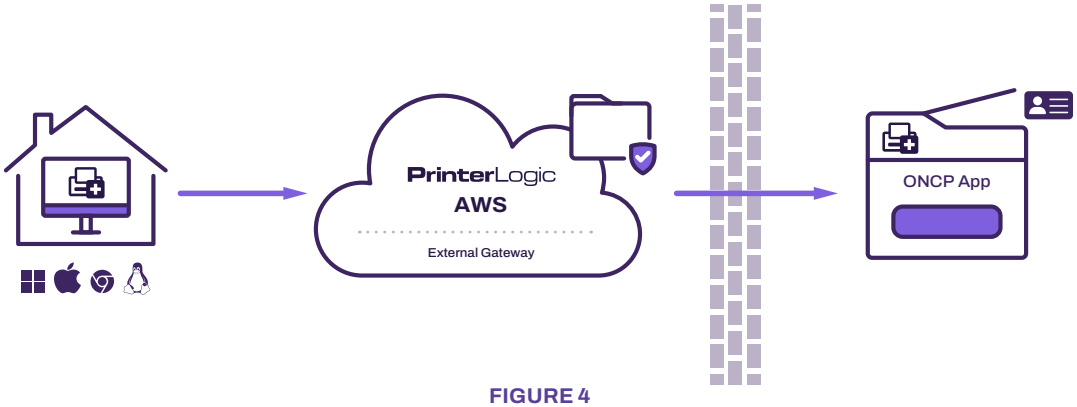

FIGURE 4

A Unified Platform that Goes Beyond Printing

PrinterLogic earned its reputation by providing a serverless printing infrastructure that is feature-rich, secure, and easy to use. There is no need for Group Policy Objects (GPOs) or time-consuming scripting to deploy and manage printers and drivers. There are two versions of PrinterLogic. One is a true SaaS implementation that eliminates the need for print servers, hardware resources, licensing, or maintenance. The other

is an easily updated Virtual Appliance for on-premise use with equivalent functionality. Any configuration model of Off-Network Printing can be supported on a SaaS or Virtual Appliance instance. Off-Network Cloud Printing is available for SaaS instances only.

When you're ready to go beyond printing and bridge the gap between your print environment and the digital work critical to a modern organization, look for a solution to unify the entire organization. The leaders who can see beyond the current state to one where the most critical business processes and systems are orchestrated and automated while still offering a Zero Trust-enabled SaaS print environment that allows on-the-ground work to get done will be the leaders who unlock true operational efficiency and scale. Visit us at Vasion.com to learn where your future of work can go.

Conclusion

PrinterLogic's Off-Network Printing features let you keep printers on your most secure networks while allowing all workers to print—no matter what network they're on. It solves two key IT challenges: how to manage printing in a Zero Trust environment and how to provide easy, intuitive printing access to contractors, remote workers, and affiliate partners without VPNs or web portals. Off-Network Printing bridges the gap between the demands for better network security and the disconnects for any employee or partner trying to print from outside the organization's firewall.

Vasion Automate, including PrinterLogic, builds upon the company's best-in-class enterprise print management technology with an intuitive content management and business process cloud platform. With Vasion's unified digital platform, businesses can capture analog and digital content, automate workflows, create agreements with e-signatures, and securely manage content wherever it is stored.

Additionally, the PrinterLogic solution pioneered digital transformation in the print management space by helping IT professionals eliminate all print servers and deliver a highly available serverless printing infrastructure. Whether your organization is paperless, still dependent on paper-based processes, or somewhere in between, Vasion has the solutions to help drive compliance, scalability, and accountability throughout your digital transformation. Schedule a demo to start your journey today.