PrinterLogic
a VASION solution

Off-Network Printing

How PrinterLogic makes printing easy and secure in today's Zero Trust network-access environments

— Introduction:

Off-Network Printing

MORE THAN EVER, CIOs are committed to secure networks and data. This includes isolating possible attack surfaces (including printers) on highly secure networks with restricted access. Meanwhile, IT departments need to give workers easy access to the resources they need to do their jobs.

PrinterLogic's new Off-network Printing feature bridges this gap by providing convenient access to printers—even when employees, contractors, and partners reside on different networks.

Two important shifts are fueling the demand for Off-network Printing. One is the reliance on more contractors, guest workers, and affiliate partners who are not allowed on company networks, but who need to print. The second is the adoption of cloud-based authentication systems that use an explicit identity-based approach known as Zero Trust network access.[1]

[1] Zero Trust eliminates blanket access for employees with login credentials, and instead provides all workers—regardless of their location—appropriate, measured access from any device. Gartner calls this Zero Trust Network Access (ZTNA). Their Market Guide for Zero Trust Network Access is available here.

Use Case Overview

Here are three common use cases that illustrate how off-network printing serves customer needs:

Organizations adopting Zero Trust

In this scenario, employees are granted access to specific applications and resources, but not the underlying network. IT needs a solution that maintains the security of their new network architecture while meeting their employees' printing needs.

Businesses using onsite contractors

A business regularly employs contractors onsite, but they are not allowed on the corporate network where printers reside. These workers are often allowed on a guest network with limited access. Even still, they need access to the company's printers to complete their work.

Business-affiliate printing

A nurse employed by a hospital's affiliate clinic needs to print a prescription using the hospital's medical records (EMR) software. The clinic is an independent business and is not connected to the hospital's secure network.

Key Benefits

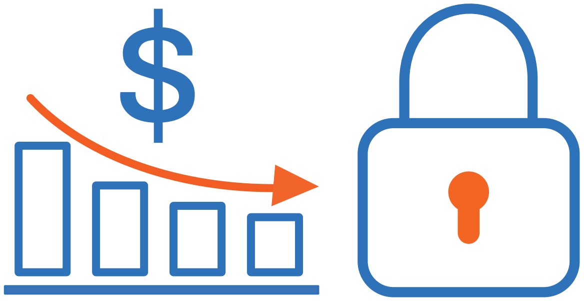
PrinterLogic's Off-network Printing feature allows end users to easily access printers inside an organization's firewall, even if the user is on a different network. The key benefits are outlined below:

Reduced infrastructure costs

PrinterLogic is founded on helping customers eliminate costly print servers. Now, with Off-network Printing, customers can reduce infrastructure even more by eliminating VPNs, hosting services, and external access portals that were used to accommodate the remote printing needs of employees, contractors, partners, and affiliates.

Enhanced security

In its default configuration, PrinterLogic's Off-network Printing feature does not allow confidential data to remain at rest in the cloud. Instead, print jobs are encrypted at their origination point and routed through the PrinterLogic SaaS gateway service to their destination printer. In addition, PrinterLogic conforms to the AWS Security Pillar.



Native, intuitive printing experience.

Because Off-network Printing mimics regular printing, there is no need to train employees on using a new procedure for remote or off-site printing. Users can print from within the document or web page as usual.

High availability and redundancy

As part of the AWS Well-Architected Framework, PrinterLogic inherits several reliability benefits. Gateways scale as needed. If there's a failure, jobs are automatically rerouted to another available gateway. If IT chooses to host the gateway in their data center, redundant gateways can be configured to provide automatic failover if needed.

Supports secure release printing

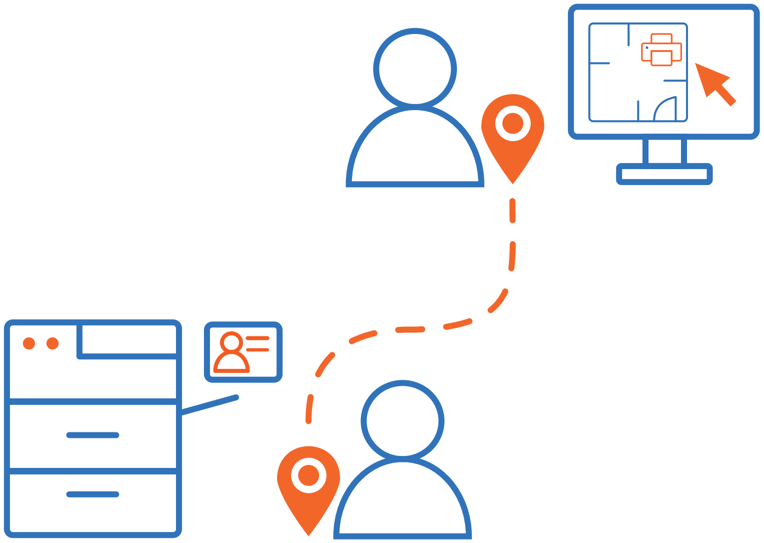
Secure-release printing is especially important with Off-network Printing because the user who initiates the print job may not be near the printer. By holding the print job until the user or a collaborator goes to the printer and authenticates, the confidentiality of sensitive information is maintained.

Mobile worker support

PrinterLogic's solution is great for mobile workers because it lets them print to a corporate network printer from anywhere, at any time. It facilitates collaboration with insider (office-based) staff. Off-network Printing puts every team member on equal footing for document-sharing, even if they reside on different networks.

Eliminate old-school collaboration workarounds

In the past, workers without access to corporate networks used any number of workarounds for collaboration. Some relied on costly personal printers or third-party printing services. Some mailed their documents to an inside collaborator or a client's office. Some emailed content to a helper in the office who could do the printing for them. Either way, these workarounds have been expensive, introduced security risks, and cost time. Off-Network Printing is a "new way to collaborate" when it comes to hard-copy sharing.



— The Infrastructure:

How it works

OFF-NETWORK PRINTING allows users with internet access, from any location, to send print jobs to a printer located behind the company firewall. In addition to the PrinterLogic SaaS or VA instance, there are two other components that 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 and downloads and delivers it to the designated printer.

Three Configuration Options

1. PrinterLogic-hosted model

The preferred (and easiest) 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 their 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.

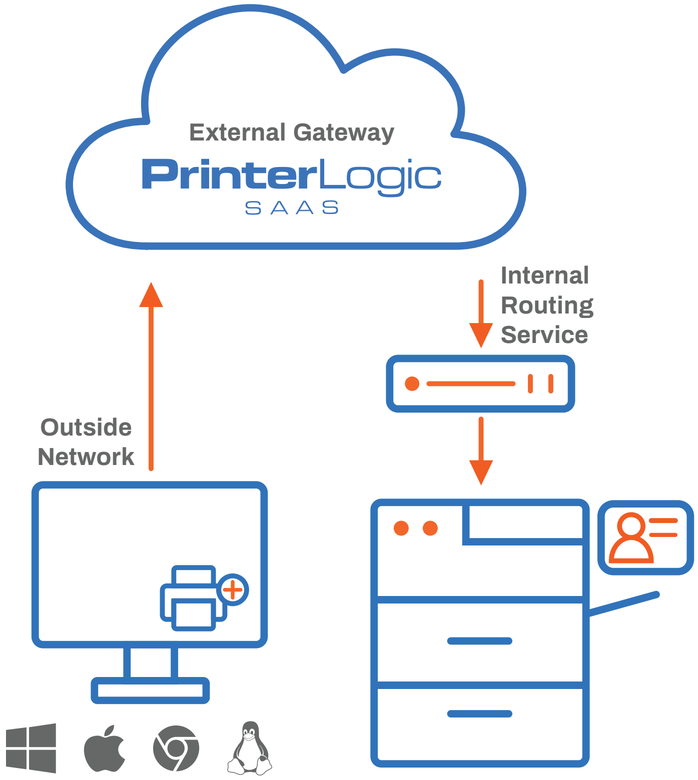


Figure 1. Off-network Printing where the External Gateway is hosted by PrinterLogic in AWS.

2. Customer-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 Public Certificate Authority. Third, port 443 must be open for incoming connections.

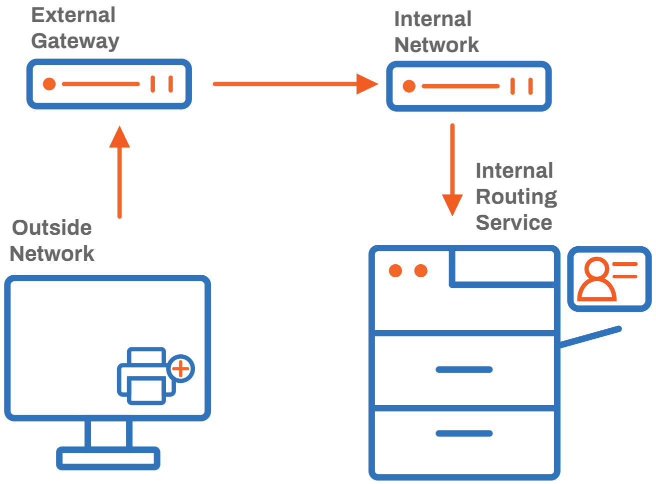


Figure 2. Off-network Printing where the External Gateway is hosted by the customer.

3. Hybrid Model

PrinterLogic-hosted and customer-hosted scenarios can be used together to provide flexibility and redundancy in configurations. These scenarios are illustrated in Figure 3.

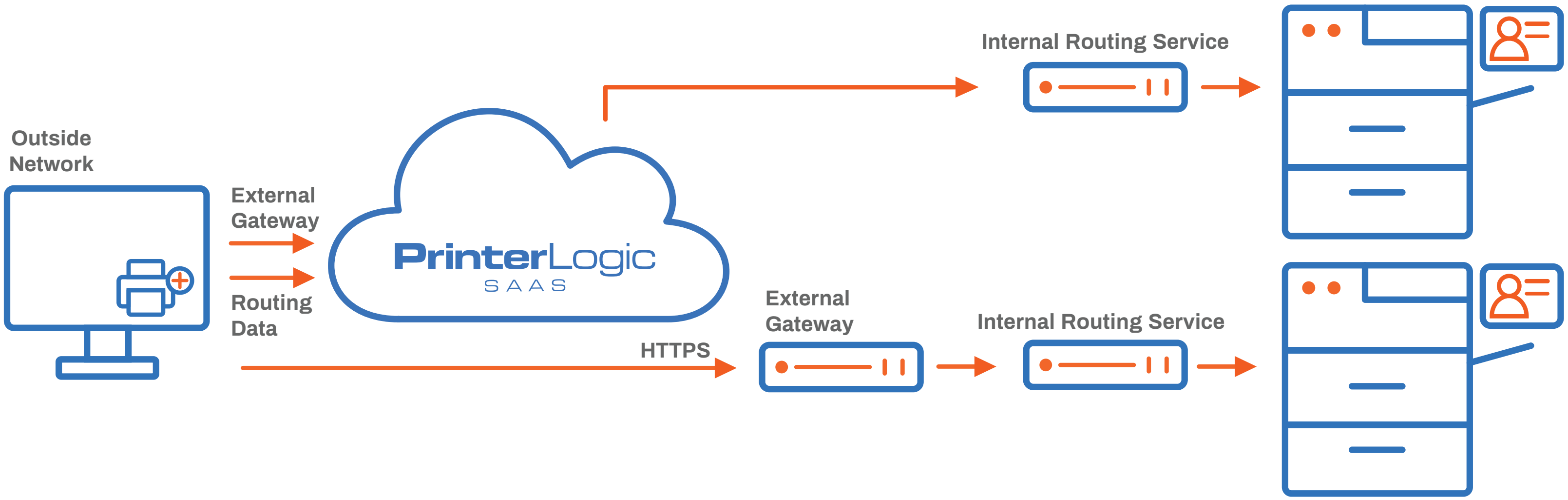


Figure 3. Off-network Printing using a hybrid model. Both PrinterLogic-hosted and customer-hosted External Gateway are used for redundancy.

More about Zero Trust

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 increased dependence on connected business partners, virtual private networks (VPNs) and demilitarized zones (DMZs) became common. But 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 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.

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]

Two PrinterLogic Platform Options

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-premises use that has equivalent functionality.

PrinterLogic’s Off-network Printing feature is included in the SaaS and Virtual Appliance platforms.

[2] Gartner, Inc., *Market Guide for Zero Trust Network Access*, June 8, 2020.

Conclusion

PRINTERLOGIC'S NEW OFF-NETWORK PRINTING FEATURE lets 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 network architecture, and how to provide easy, intuitive printing access to contractors, guests, and affiliate partners without VPNs or web portals.

Off-network Printing bridges the gap between the demands for better network security and the disconnects that occur for any worker or partner who is trying to print from outside the organization's firewall.