

# **Zero Trust and LRS EOM**

How do LRS EOM solutions support your “Zero Trust” strategy?

# Current Approach to Enterprise Security: “Castle and Moat” Defense





What does “Zero Trust” mean?

**“Never Trust, Always Verify”**

Assume the “bad guys” are already inside the network

# According to Wikipedia...

“...**The main concept behind zero trust is that networked devices**, such as laptops, **should not be trusted by default, even if they are connected to a managed corporate network** such as the corporate LAN and even if they were previously verified...”

## According to Microsoft...

“Instead of assuming everything behind the corporate firewall is safe, the **Zero Trust model assumes breach and verifies each request as though it originates from an open network.** Regardless of where the request originates or what resource it accesses, **Zero Trust teaches us to “never trust, always verify.” Every access request is fully authenticated, authorized, and encrypted before granting access.**”



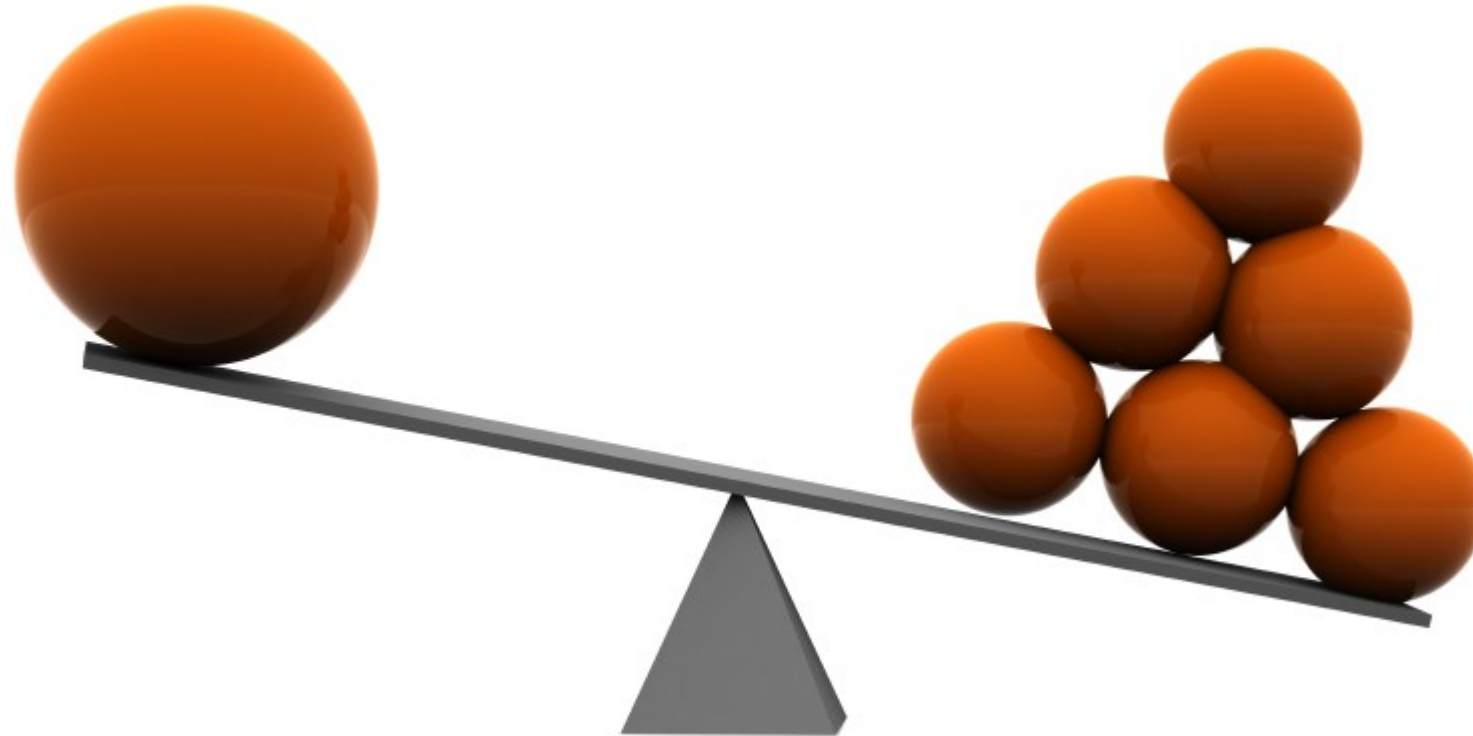
Remember, Zero Trust  
is a security concept,  
**not** a specification

**Goal:** Implement as  
many recommendations  
as possible and practical

# Balance Security and Business Requirements

Only fight battles big enough to matter

Only fight battles small enough to win



# Printing and Security – What’s the Big Deal?



Does the recent “**Microsoft PrintNightmare**” security threat ring any bells?



# Hey, Wait a Minute...!

- Printers process sensitive/confidential data that is created by critical business applications
- Printers are network-connected, computing devices that support multiple communication protocols
- Multifunction printers also copy, scan and fax
- Printers are often shared by many users
- Printers often have a hard drive




# Print Security - Key Requirements

- Authenticate and authorize users
- Protect printers and multifunction devices
- Protect print data “at the device” while it is printing
- Protect print data “in motion” on the network
- Protect print data “at rest” on print servers
- Audit (track) all print activity



# Zero Trust Makes Sense for Printing

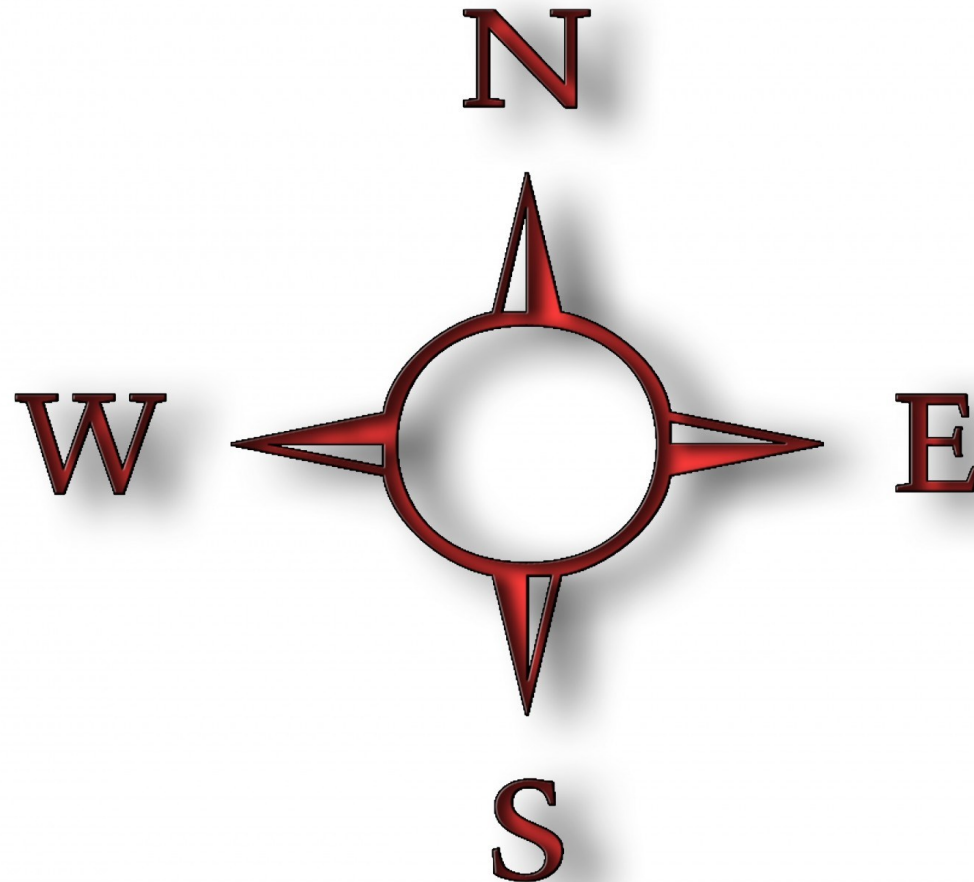




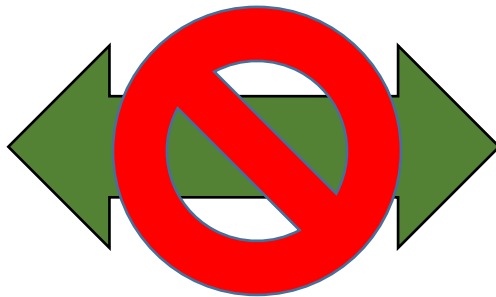
Printing and Zero Trust –  
Is it possible?

Unlikely for all print devices,  
but you can make significant  
progress toward this objective.

# East-West vs. North-South



# “Preferred Model” for Zero Trust Printing



# “Preferred Model” for Zero Trust Printing

Print Submission via HTTPS (encrypted)

Print Management Software

Print Delivery via HTTPS (encrypted)

Com

DMZ

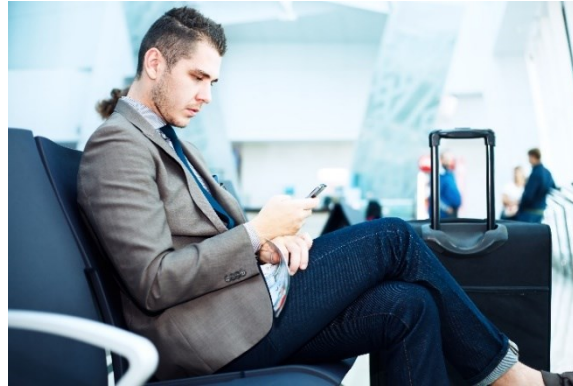


# The Evolving Work Environment

**Home Office  
(Intranet or Internet)**



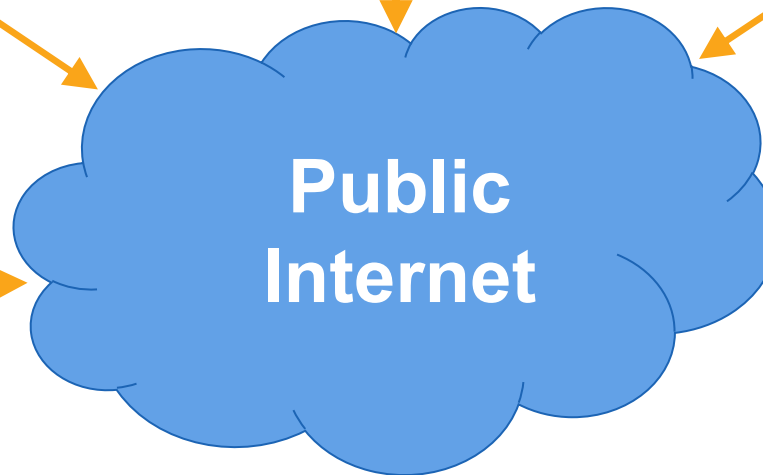
**Roaming Worker  
(Intranet or Internet)**



**Remote Offices  
(Intranet or Internet)**



**Major Corporate Locations  
and Data Centers (Intranet)**



**Printers and MFPs  
(Intranet, Internet, USB)**



**Applications Running Everywhere!**



# Builds on Three “Pillars” of Zero Trust




# Authentication vs. Authorization



## 1. Authentication

- Verifies you are who you say you are
- Methods:
  - a. Login form
  - b. HTTP authentication
  - c. HTTP digest
  - d. X.509 certificates
  - e. Custom authentication method



## 2. Authorization

- Decides if you have permission to access a resource
- Methods:
  - a. Access controls for URLs
  - b. Secure objects and methods
  - c. Access control lists (ACLs)

# Examples of LRS User Authentication

- User access of Personal Print Manager (PPM)
- User access of VPSX Print app on mobile devices
- User access a print device (e.g., swipe their badge)
- User access of VPSX admin console and associated apps
- Validate print device using a trusted (CA) certificate
- Guest Printing (associate unique code with email address)



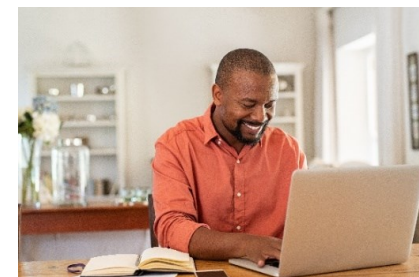
# User Authentication Methods

- Active Directory (AD)
- LDAP
- Azure Active Directory, including support for MFA
- OpenID Connect for other cloud-based identity providers such as PingID, Okta, etc.
- SQL Server for MFPsecure badge/code authentication
  - Identifies which badge/code belongs to which user



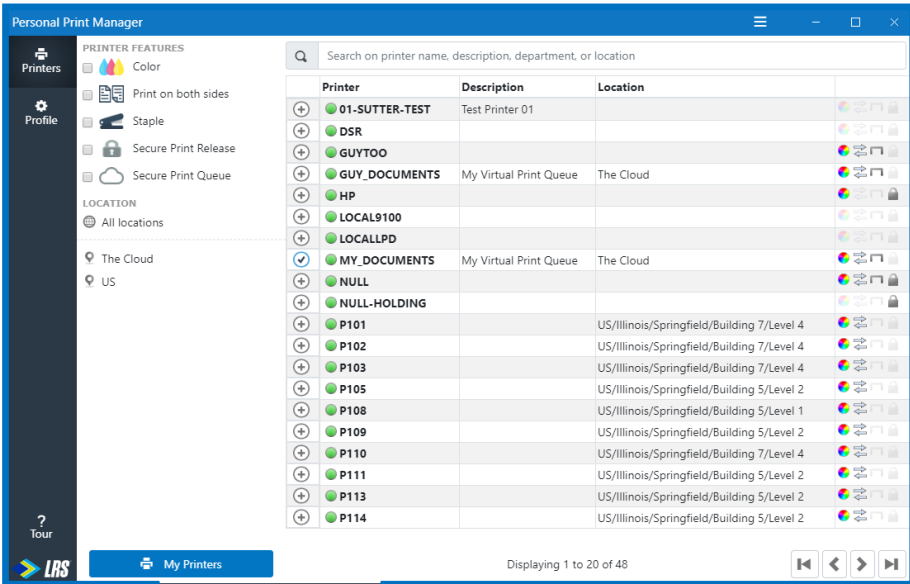
# Examples of LRS User Authorization

- Administrator security rights in VPSX admin console and associated applications
- User access to print devices/queues (real or virtual)
- User login at printers and multifunction devices to access secure print and secure scan apps
- Pull printing release restrictions
- Delegation to retrieve (pull) print jobs
- Authorize guests to print



# Mobile/Desktop (Front-End) Printing





# “Direct-IP” Push Printing

X.509 certificate is installed on the print device. PPM can positively **validate** that the destination device is truly the expected device. Peer verification validates the certificate presented by the device to confirm its credentials and authenticity.

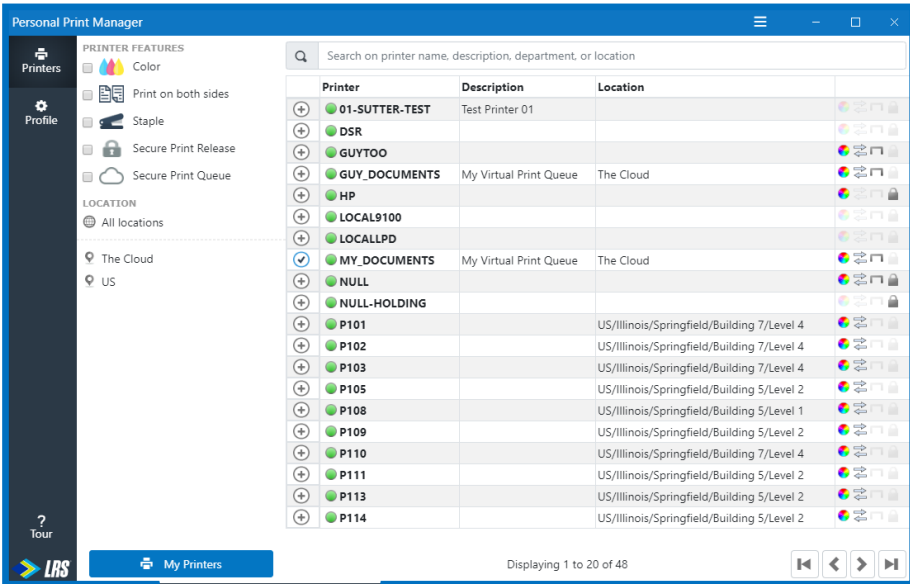
With PPM, users are **authenticated**, and they can **only** select the printers that they are **authorized** for. PPM tracks **all** print activity from desktops.



All print data is sent **encrypted** using IPPS (IPP over TLS).



# “Direct-IP” Pull Printing (Direct Secure Release)



With PPM, users are **authenticated**, and they can **only** select the virtual printers (PPQs) that they are **authorized** for. Print Jobs are held securely on the user’s desktop until they are released at the print device. Print job metadata is sent securely to the central VPSX system.



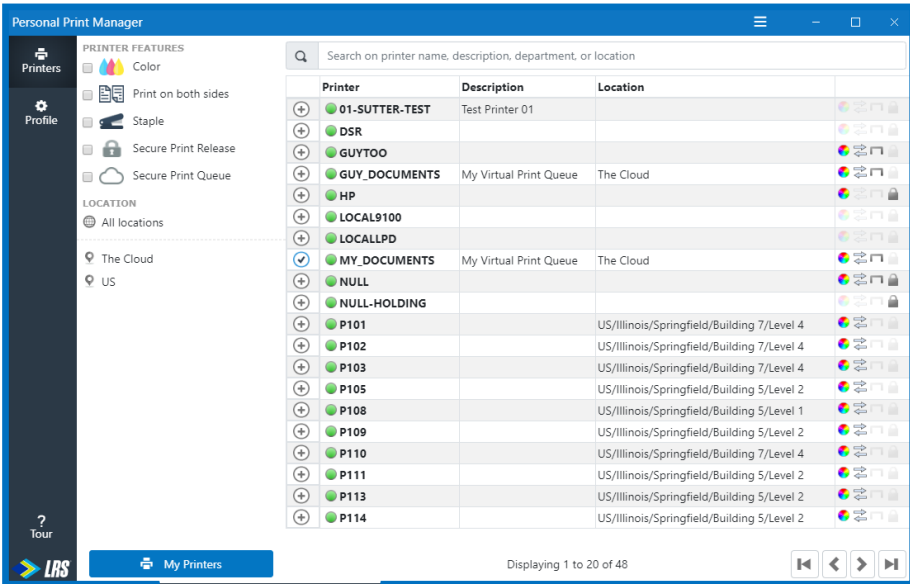
X.509 certificate is installed on the print device. PPM can positively **validate** that the destination device is truly the expected device. Peer verification validates the certificate presented by the device to confirm its credentials and authenticity. Users **must authenticate** at the print device to retrieve their print jobs.



All print data is sent **encrypted** using IPPS (IPP over TLS). The central VPSX system tracks **all** pull print activity from the desktops.







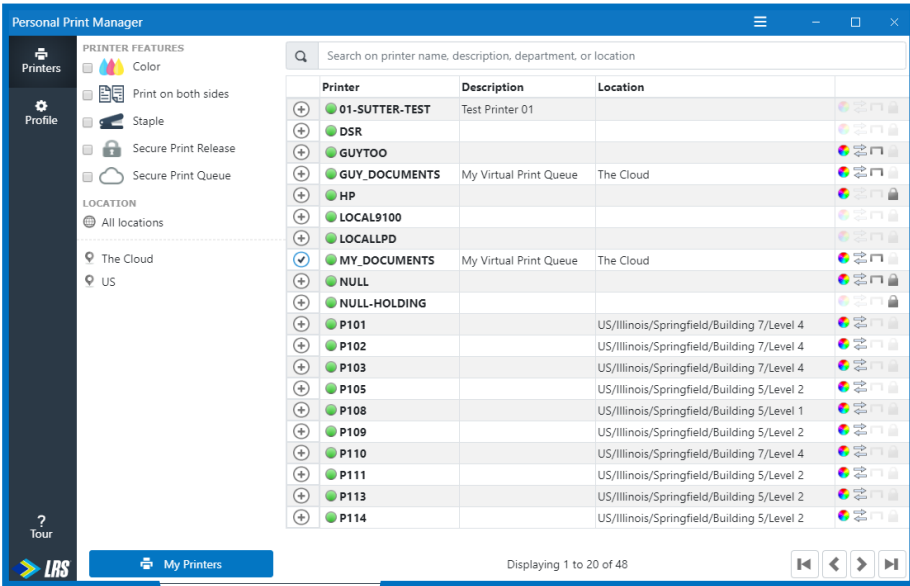
# Server-Based Push Printing

With PPM, users are **authenticated**, and they can **only** select the printers that they are **authorized** for.

X.509 certificate is installed on the print server and print device. PPM can positively **validate** that the VPSX server is the expected server, and VPSX can positively **validate** that the destination printer is the expected device. Peer verification validates the certificate presented by the device to confirm its credentials and authenticity.



All print data is sent **encrypted** using IPPS (IPP over TLS). VPSX tracks **all** print activity from desktops.



# Server-Based Pull Printing

X.509 certificate is installed on the print device. PPM can positively **validate** that the destination device is truly the expected device. Peer verification validates the certificate presented by the device to confirm its credentials and authenticity. Users **must authenticate** at the print device to retrieve their print jobs.

With PPM, users are **authenticated**, and they can **only** select the virtual printers (PPQs) that they are **authorized** for.



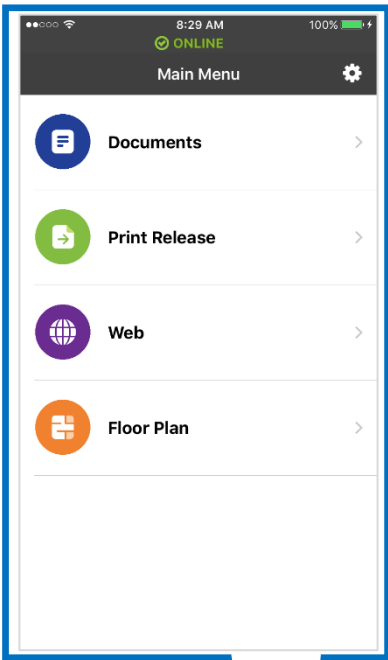
# Mobile Push Printing

With the VPSX Print app, users are **authenticated**, and they can **only** select the printers that they are **authorized** for.

X.509 certificate is installed on the print server and print device. PPM can positively **validate** that the VPSX server is the expected server, and VPSX can positively **validate** that the destination printer is the expected device. Peer verification validates the certificate presented by the device to confirm its credentials and authenticity.



All print data is sent **encrypted** using IPPS (IPP over TLS). VPSX tracks **all** print activity from desktops.



With the VPSX Print app, users are **authenticated**, they can **only** select the virtual printers (PPQs) that they are **authorized** for.

# Mobile Pull Printing

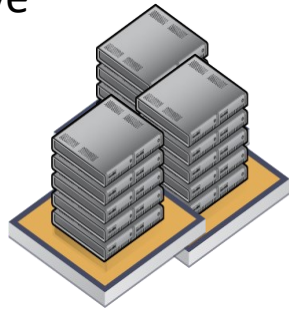
X.509 certificate is installed on the print server and print device. PPM can positively **validate** that the VPSX server is the expected server, and VPSX can positively **validate** that the destination printer is the expected device. Peer verification validates the certificate presented by the device to confirm its credentials and authenticity. Users **must authenticate** at the print device to retrieve their print jobs.



All print data is sent **encrypted** using IPPS (IPP over TLS). VPSX tracks **all** print activity from desktops.

# Scan Workflows from MFP

- Google Drive
- SharePoint
- OneDrive
- Teams
- Box
- Folder
- Fax
- Email
- PageCenterX
- Business Applications
- Document Management Systems



X.509 certificate is installed on the MFP for HTTPS communication with the MFPsecure server. Users **must authenticate** at the MFP, and they will only see the scan workflows that they are **authorized** for.

“Send to” storage/application destinations support various **secure communication protocols**.

All scan data and metadata is sent **encrypted** using HTTPS.

# Application (Back-End) Printing



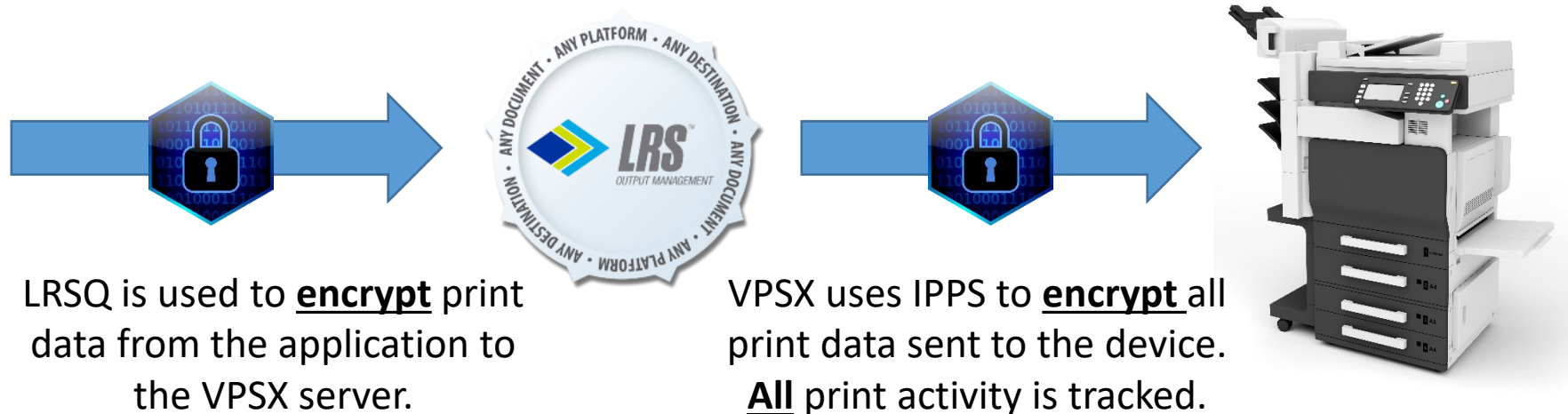
# Application Push Printing

Business applications **authenticate** users and **authorize** (enable) printing to defined printers.

X.509 certificate is installed on the print server and print device. VPSX can positively **validate** that the destination printer is the expected device. Peer verification validates the certificate presented by the device to confirm its credentials and authenticity.



**Business Applications**



# Application Pull Printing

Business applications **authenticate** users and **authorize** (enable) printing to virtual printers (PPQs).



LRSQ is used to **encrypt** print data from the application to the VPSX server.



VPSX uses IPPS to **encrypt** all print data sent to the device. **All** print activity is tracked.



X.509 certificate is installed on the print server and print device. VPSX can positively **validate** that the destination printer is the expected device.

Peer verification validates the certificate presented by the device to confirm its credentials and authenticity. Users **must authenticate** at the print device to retrieve their print jobs.



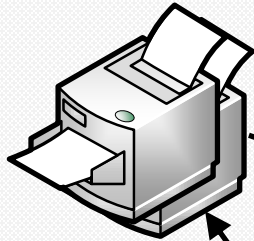
# Internet Pull Printing and Scanning



# Internet Pull Printing: Logic Flow (Direct Secure Release)

## Internet-Only Offices

Network printer(s) at Internet-only location with MFPsecure/Print

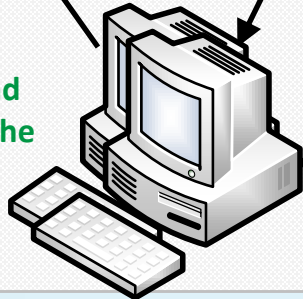


3. User authenticates at print device and selects print job for release

5. PPM client on user's desktop sends job to network printer using IPPS

1. Authenticated and authorized user submits print job to PPQ, and the print job is held securely on the user's desktop

Desktop(s) with PPM



LRS Notification Service (Maintained by LRS)

Note: All communication with the Gateway and LRS Notification Service uses HTTPS to ensure all information is encrypted.

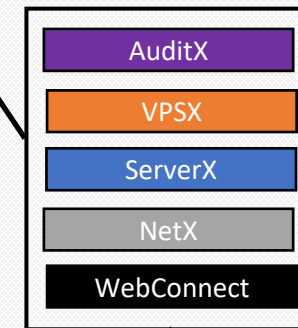
2. PPM client sends print job metadata

6. PPM client updates status of job

## Data Center/Private Cloud

7. VPSX tracks print activity

4. VPSX notifies PPM client on user's desktop to release print job



Gateway

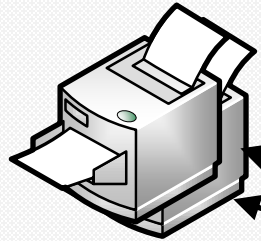
MFPsecure

Publish connection URL to the Gateway

# Internet Pull Printing: Logic Flow (Print Jobs on the VPSX Server)

## Internet-Only Offices

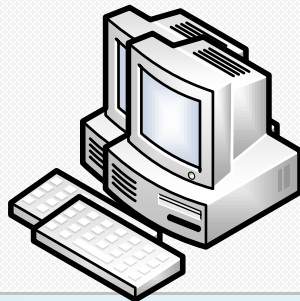
Network printer(s) at Internet-only location with MFPsecure/Print



2. User authenticates at device and selects print job(s) for release

3. Secure Print app (running on print device) retrieves print job(s) from VPSX via Gateway

Desktop(s) with PPM



**Note:** All communication with the Gateway uses HTTPS to ensure all information is encrypted.

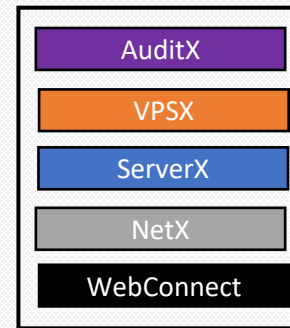
## Data Center/Private Cloud

Application (e.g., SAP, EMR)



4. VPSX tracks print activity

1. Authenticated and Authorized User submits print job(s) to PPQ (data is encrypted)



Gateway

Publish connection URL to the Gateway

MFPsecure

# Internet Scanning: Logic Flow

## Internet-Only Offices

Network MFP at Internet-only location with MFPsecure/Scan

1. User authenticates at MFP and sees the scan workflows that they are authorized for



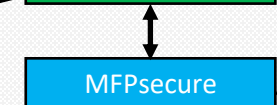
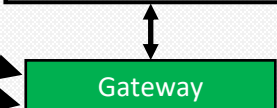
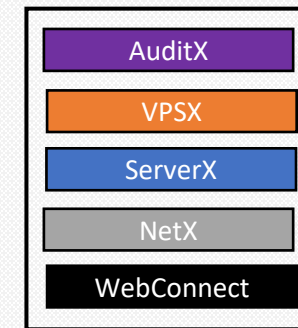
2. Secure Scan app performs workflow and sends file and metadata securely to the MFPsecure/Scan server

**Note:** All communication with the Gateway uses HTTPS to ensure all information is encrypted.

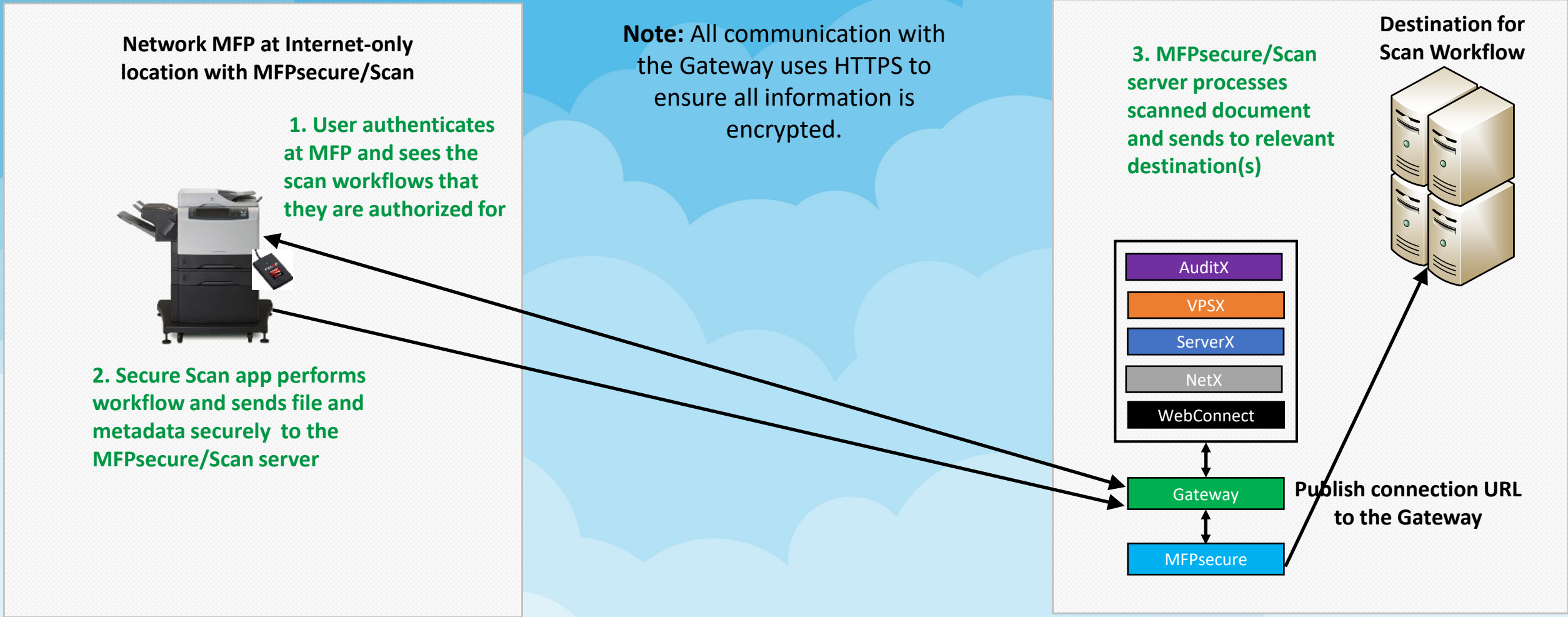
## Data Center/Private Cloud

3. MFPsecure/Scan server processes scanned document and sends to relevant destination(s)

Destination for Scan Workflow



Publish connection URL to the Gateway



# Closing Thoughts



Only fight battles big enough to matter

Only fight battles small enough to win

# Questions

