Sentry Print

Technical white paper

Pharos Systems International, Inc.
April, 2021

Table of Contents

SENTRY PRINT OVERVIEW 4

Business Challenges 4

The Cloud Print Revolution 5

A Flexible, Scalable Solution 5

Deployment Topologies 6

Conventional networks with cloud job storage 6

Conventional Networks with Local Job Storage 7

Zero Trust Networks 7

CLOUD CONNECTOR 9

Network configurations 9

Benefits of the Cloud Connector 10

Serverless (Zero Server) configuration 10

Zero Trust network configuration 12

SYSTEM COMPONENTS 14

Print Scout 14

Cloud Connector deployment topology 14

LOCAL CONNECTOR OPTION 17

Network configuration 17

Device Scout 18

Deployment architecture 18

MOBILE RELEASE (QR CODE) OPTION 20

Network configuration 20

Sentry Print mobile app 20

Deployment architecture 20

Configuration 21

Document storage 22

Cloud storage 22

Local storage 22

Document submission via Print Scout 22

Document submission via Mobile 23

Document release 23

AUTHENTICATION OPTIONS 25

Mobile Print (QR Code) – Touchless Print Release 25

Proximity card 25

Control panel (“keypad”) login 26
DATA PROTECTION 27
Document Encryption 27
AWS S3 with KMS encryption 28
Zero Knowledge Encryption 28
Encryption details 28
User Identity Hashing 29
Security is a shared responsibility 29
CUSTOMER READINESS 30
Platform communication 30
Cloud API endpoints 30
Network ports and protocols 30
Cloud Connector / Zero Server configurations 30
Local Connector 32
Mobile Release (QR Code) 35
SR25 Hardware 35
Deployment requirements 36
Print Scout 36
Device Scout 37
Integrating Printers 39
HP Requirements 39
Konica Minolta Requirements 41
Lexmark Requirements 41
Ricoh Requirements 42
Xerox Requirements 42
Sentry Print mobile app 43
Deployment tool 43
NETWORK UTILIZATION 44
Print Scout 44
Print Scout communication patterns 44
Device Scout 45
INTERNET TRAFFIC 49
Monthly Internet Traffic Per User 49
Assumptions 49
Examples 50
REFERENCES 51

SENTRY PRINT OVERVIEW

With Sentry Print, you can easily establish secure printing workflows across your organization without the hassle of setting up and maintaining print servers and queues. Sentry Print is a true cloud (cloud-native) platform built upon Amazon Web Services (AWS).

Sentry Print creates secure print workflows by enforcing user authentication at printers and multi-function devices (MFDs). Employees quickly authenticate themselves at a chosen printer by using their mobile device, their ID badge (proximity card), or by entering their email and PIN or user ID and password into the printer's control panel. Documents are then released only to the document owner, which protects confidentiality.

Because employees must be physically present at a printer to authenticate and collect their document, the solution practically eliminates the problem of abandoned prints—documents that are left in printer trays or tossed into recycle bins. This saves money and prevents waste. This workflow also improves convenience: employees can submit their print jobs from any location, even outside the company network, and then release their documents at any secure printer on the network.

When used along with Beacon Analytics, the solution creates secure and flexible printing workflows and provides the data insights you need to continually optimize your print environment and keep your organization's costs down year after year.

Business Challenges

Our research into business challenges has revealed three broad themes:

1. **Businesses need to transition employee printing into their cloud ecosystem**. Company leaders consistently report that their cloud migration strategy is critical to their business and that print needs to be part of the strategy.

2. **Many businesses must meet strict compliance and security requirements.** These companies are seeking services that meet or exceed their current data compliance and security mandates. Comprehensive data protection and privacy regulations such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) require the appropriate safeguards.

3. **Printing should be a simple, intuitive experience for employees**. How people work has evolved. Employees frequently work outside the office, on their own devices, and at all hours of the day. Print is a utility that must be available and simple to use whenever it's needed.

Sentry Print solves these business challenges while also improving information security, eliminating print infrastructure, and controlling resource costs. Sentry Print provides several configuration options to fit practically any corporate environment and network topology.

The Cloud Print Revolution

Companies are rapidly moving away from a local network infrastructure and toward specialized cloud services. They are decommissioning their data centers, eliminating servers, and relying on service providers to manage their infrastructure and workflows.

Gartner Group predicts that cloud services will grow at nearly three times the growth of all other IT services over the next three years. In a recent technology forecast, the Gartner researchers said, "We know of no vendor or service provider today whose business model offerings and revenue growth are not influenced by the increasing adoption of cloud-first strategies in organizations[1]."

Print has emerged as one of the most critical systems for companies to shift to the cloud, for several reasons, including:

1. **The elimination of print servers delivers a significant and immediate positive return on investment (ROI).** Each server eliminated represents hard savings. Using Microsoft's Total Cost of Ownership (TCO) calculator, a typical enterprise print server costs around $4,000 annually to license and manage.

2. **Cloud-based printing improves flexibility and scalability.** Companies want services that seamlessly grow with their business. They want to avoid the costs and hassle of server planning, setup, and maintenance.

3. **Cloud printing is fast and easy to deploy.** With no server deployments to plan and manage, solution designs are simplified, and consulting services are scaled back.

4. **The solution is always up to date.** IT managers don't have to worry about what product version they are running. Automatic cloud updates ensure that the organization always has the latest features and improvements.

5. **Companies can improve their information security and reduce their risk.** Increasingly, companies are moving IT burdens from in-house services to specialized cloud service providers to shift their risk to companies that are better equipped to manage that risk. Print is no different. Companies like Amazon, Google, and Microsoft provide world-class cloud platforms that are proven to be more secure than conventional corporate networks that rely on perimeter security measures.

A Flexible, Scalable Solution

Every organization is likely to have a different set of requirements to fit their network topology, leverage their preferred identify provider, and establish how print jobs should be stored and delivered. Sentry Print provides several configuration options to fit practically any corporate environment and use case. The choice of these settings will either expand or contract the available feature set of the solution.

These configurations can be used alone or in combination. In this document, we describe these configurations as:

- The “Cloud Connector” option, for Zero Trust networks or for conventional networks with local or cloud storage. This configuration is also relevant to “Zero Server” or “serverless” configurations.

- The “Local Connector” option, which provides multivendor integrated printer support and also supports Active Directory (AD) as the authentication provider. It requires the use of a Device Scout in your network to secure your printers.

- The Mobile Print / QR Code Release option, which leverages the Sentry Print mobile app as a user authentication option for secure document release. Any PCL5-compliant network printer can be enabled for mobile release.

Deployment Topologies

Sentry Print is designed to be flexible to any network topology and customer requirements. Following are a few examples of how it can be deployed.

Conventional networks with cloud job storage

Many companies wanting to take advantage of the benefits of cloud services for their secure printing will have conventional networks in place. These networks focus on perimeter security and allow some level of trust and access to peers on the network.

In this environment, the company network provides workstations and printers access to Internet-based resources and it trusts devices within the network to communicate. Print jobs can be stored in the cloud and pulled (downloaded) by a cloud-aware printer. Or, print jobs can be stored in the cloud and pushed to the printer via the Print Scout.

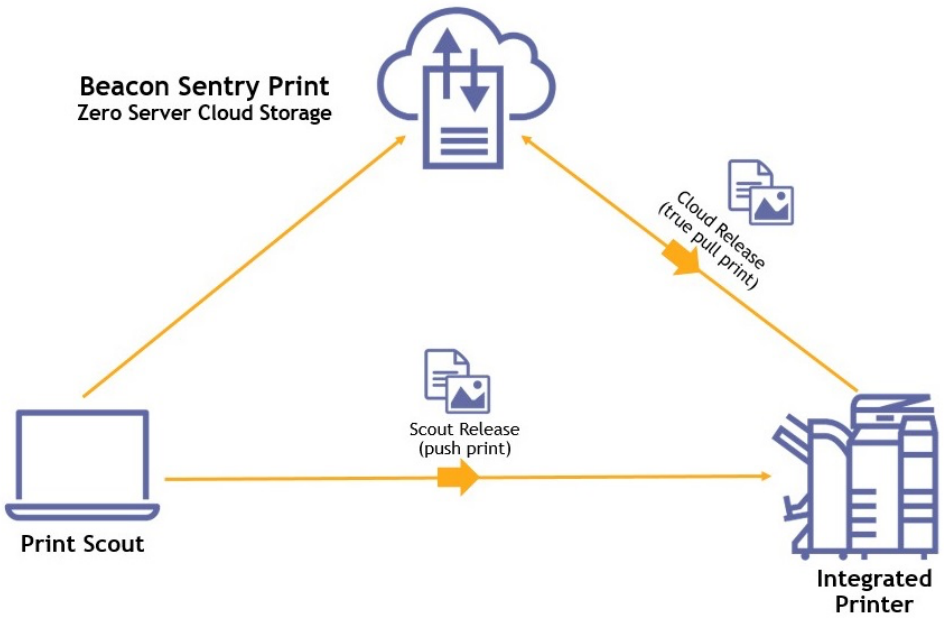

Figure 1: *Sentry Print for conventional networks with cloud storage of print jobs*

Conventional Networks with Local Job Storage

Organizations that do not allow print job data to be stored in the cloud due to security or export restrictions will need their print solution configured for local storage only. In this configuration, the network provides workstations and printers access to Internet-based resources and there's a level of trust and access (line-of-sight) between peers on the network.

Because of these limitations regarding the handling and storage of data, print jobs are stored on-premises and must be pushed to the printer upon successful user authentication. When using the Local Connector configuration or the QR Code option, print jobs are released by the Print Scout and pushed to the printer.

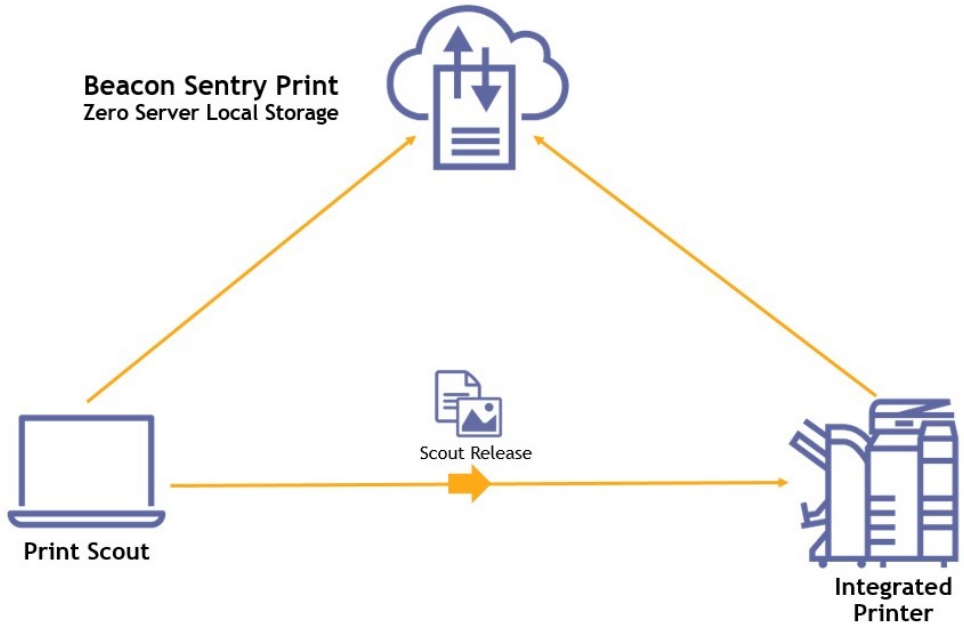

Figure 2: *Sentry Print for conventional networks with local storage of print jobs*

Zero Trust Networks

Large global enterprises are beginning to adopt Internet-only networks that do not allow any lateral communication between peers on the network. This growing trend is in response to increasingly sophisticated attacks and the trend away from centralized data centers and on-site network infrastructures.

These networks provide no way for devices on the network to see each other, let alone communicate. For this reason, these networks are called "Zero Trust networks." User workstations and printers are given access to Internet-based resources but provide zero trust or access to peers on the network. Every device has only its individual connection to the Internet.

The cloud becomes the “broker” which handles the movement of data from workstation to printer. Print jobs stored in the cloud must be pulled (downloaded) from the cloud. Print jobs cannot be stored on the user workstation because the workstation cannot access the printer directly.

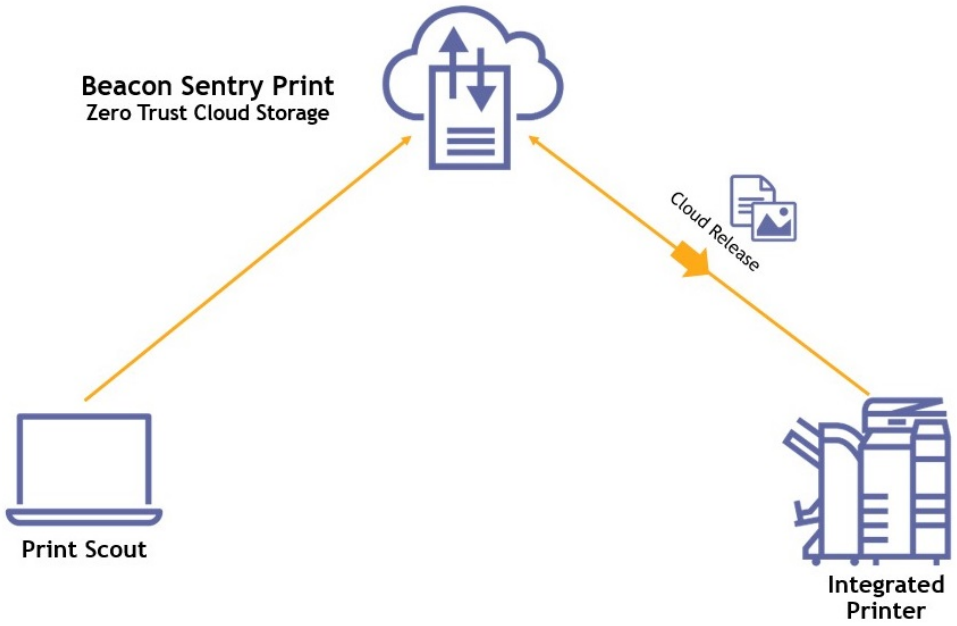

Figure 3: *Sentry Print for Zero Trust networks*

CLOUD CONNECTOR

The Sentry Print system works with the printers and MFDs deployed across your organization. With the Cloud Connector option, the system requires only one software component, the Print Scout. The Cloud Connector is a "site service" that resides in the cloud and is secured for each customer by their site encryption key. The Sentry Print mobile app is an optional component for organizations that want to enable touchless print release workflows for their workforce.

Network configurations

Sentry Print supports any type of corporate network, including conventional networks behind a firewall, minimal infrastructure environments that seek to avoid the use of print servers, and Zero Trust networks.

The Cloud Connector delivers true cloud secure printing workflows that do not require any print servers or other onsite server infrastructure components:

- **Zero Server** is for organizations with a conventional corporate network who want to take full advantage of the features and benefits of a true cloud solution. In this configuration, you can enable cloud storage or local storage of print jobs.
- **Zero Trust** is for organizations that do not have a conventional network infrastructure and want a true cloud solution to enable secure printing capability to employees within a Zero Trust environment.

Both configurations establish a simple and efficient secure printing environment that can be distilled down to "print, park, pull."

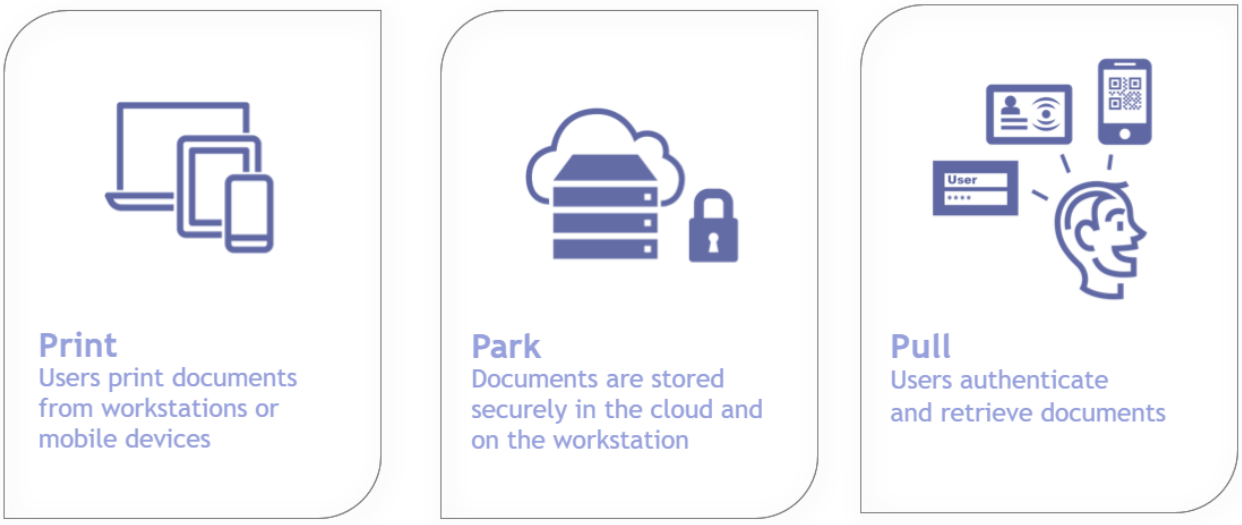

Figure 4: *The Sentry Print workflow: Print, park, pull (with several authentication options)*

Benefits of the Cloud Connector

The Cloud Connector enables companies to take full advantage of the cloud and its many benefits: deep savings in terms of costs and resources, improvements in efficiency and scalability, and the immediate ROI from the elimination of print, application, and database servers.

No servers are needed to enable secure printing workflows on integrated cloud-aware printers. Existing customers can easily migrate from using the local connector and can decommission their Device Scout server.

Sentry Print is a multi-tenant platform built on AWS. It offers high availability, elasticity, and scalability. There is no single point of failure in the system and it can be scaled up to accommodate increased workloads by provisioning resources incrementally. Its elasticity enables the solution to add or reduce services to optimally manage dynamic workloads; this is all handled automatically by AWS.

The Pharos Cloud is designed to expand or contract capacity as needed. It can support organizations with 10 devices or 10,000 devices. It can also support organizations that expand from 500 devices to 5,000 devices. In other words, you will never need to worry about how many printers a server can support or when to add another server to the solution.

Serverless (Zero Server) configuration

There's a growing trend among companies of all sizes to eliminate print servers and reduce IT maintenance tasks in favor of specialized cloud services. The serverless configuration, or "Zero Server" option, provides true cloud print management for companies that do not allow or want print servers within their corporate network and that wish to take full advantage of the features and benefits of a true cloud solution.

This configuration supports conventional networks by using a combination of cloud storage and the employee workstation to "park" jobs until the user is ready to authenticate at a secured device to release (print) the document.

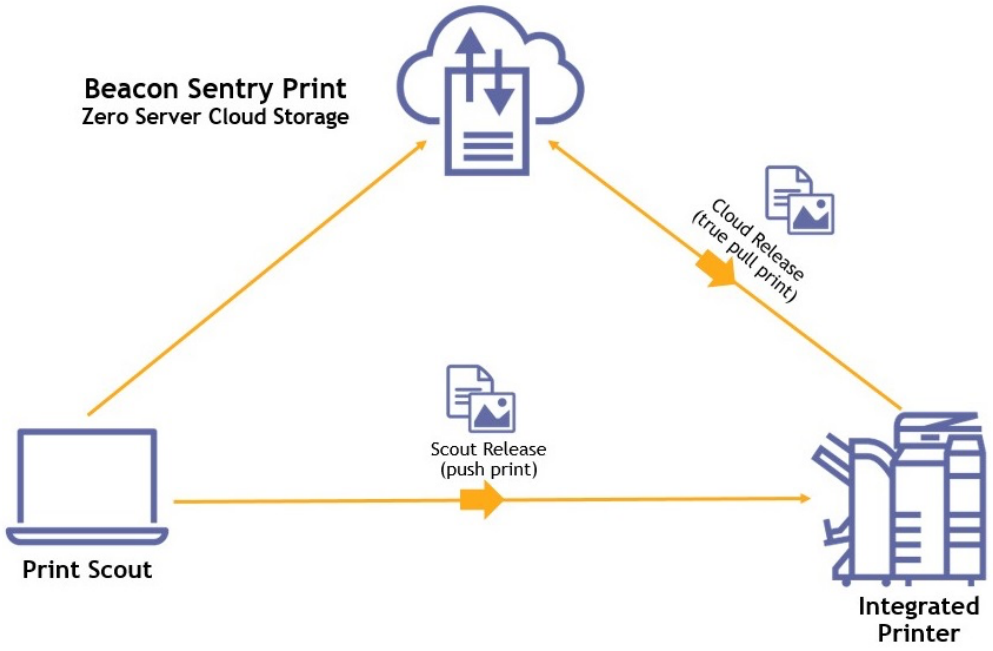

Figure 5: *The serverless (Zero Server) configuration*

Figure 5 shows how the serverless configuration works in a conventional corporate network.

1. Employees print as they normally do, from whatever application they may be using.

2. Depending on the configuration, the print job is parked either in the cloud or on the user workstation, awaiting secure release.

    - If you have cloud storage enabled, the print job is uploaded and stored securely in the cloud. A TLS v1.2 connection is used for data in transit and AES-256 job encryption is used for data at rest.

    - If you have export restrictions or other data policies that restrict cloud storage, the print job is parked by the Print Scout directly on the workstation. AES-256 job encryption is used for data at rest.

3. Employees can now walk up to any secured printer to authenticate and release (print) their documents.

    - If cloud storage is enabled, the cloud-aware printer requests the cloud-stored job and the documents are either printed immediately or the user is presented with a list of jobs to review, select, and print. This is true pull printing because the printer makes the request and downloads the document from the cloud.

    - If cloud storage is not enabled, the Print Scout on the workstation pushes the job to the printer upon successful authentication, and the documents are either printed immediately or the user is presented with a list of jobs to review, select, and print.

Zero Trust network configuration

The Cloud Connector enables organizations to leverage the latest in security technologies and strategies. Specifically, the solution supports Zero Trust networks (sometimes called “Internet-only” networks), in which all devices are connected directly to the cloud with none of the east-west (peer-to-peer) communications that define a conventional corporate network.

This is the next generation network topology used by several large global businesses and in time will become the new security standard employed by organizations. Zero Trust defends against modern cyberthreats by moving beyond perimeter security. It eliminates the threat of lateral movement within a network, also known as east-west communication. The point of infiltration for an attack, such as a printer, is often not the target location. Preventing lateral movement is critical to protect the rest of your network.

In other words, there is no communication between the employee workstation and the printer; there is no channel through which devices can connect. There is no trust or line-of-sight between peers, which reduces many security risks inside the company network.

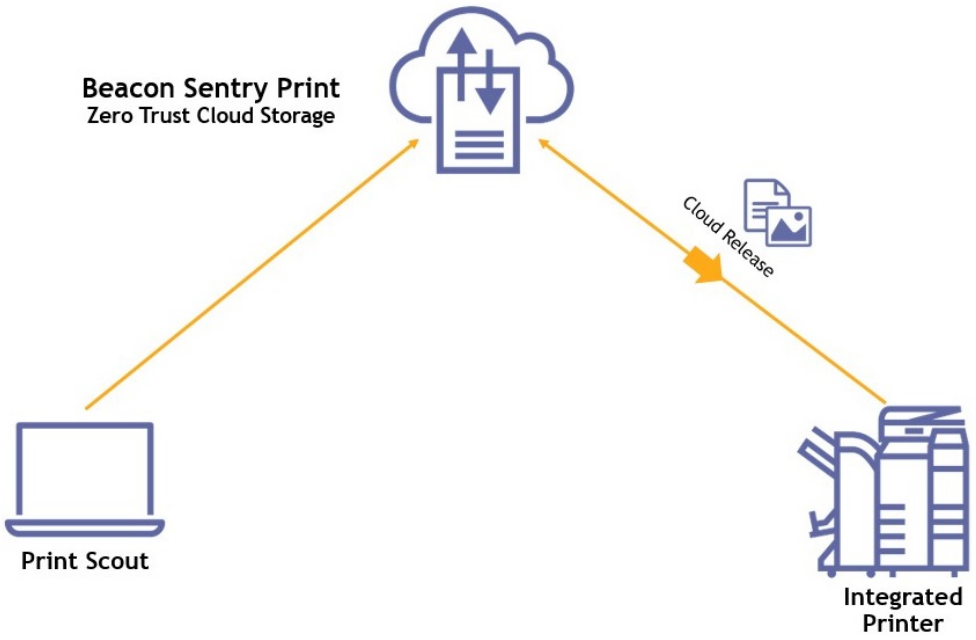

Figure 6: *The Zero Trust network configuration*

The trend toward Zero Trust networks

Companies are increasingly implementing Zero Trust for many reasons. The technologies that support Zero Trust are becoming mainstream amidst growing pressure to protect enterprise systems from increasingly sophisticated attacks. For example, Google's BeyondCorp was one of the first published implementations of a Zero Trust network by a well-known technology enterprise.

The conventional security model (Castle and Moat) entails the outdated assumption that everything on the inside of an organization's network can be trusted. It's no longer a safe assumption that a firewall will protect a network or its data. The moat (firewall) is a deterrent, not a fail-safe. It may be difficult to obtain access from outside the network, but everyone and everything inside the network is trusted by default, which is no longer considered the most secure network model. Once an attacker gains access to the network, they have free reign over everything inside.

The most damaging data breaches happened because hackers were able to move through internal systems without much resistance once they got past the corporate firewalls. Because traditional security models are designed to protect the perimeter, threats that get inside the network are left invisible, uninspected, and free to morph and move wherever they choose to extract valuable business data. Zero Trust defends against these cyberthreats by eliminating the possibility of lateral (east-west) communication within a network.

For those companies looking to transition to this network security model, Sentry Print enables a safe and convenient printing experience within a Zero Trust network.

Micro-segmentation

An important concept of Zero Trust is micro-segmentation, the practice of breaking up security perimeters into small zones to maintain separate access for various parts of the network. Sentry Print implements this segmentation principle. Printers and MFPs can be moved outside the corporate perimeter (externalization) without disrupting employee printing.

The workstation and the printer communicate in a north-south direction with an explicit trusted secure end point within the Pharos Cloud (AWS). Employee printing with Sentry Print does not require implicit trust between the workstation and the printer. It's not constrained to inside the corporate perimeter and it does not require communication over known (insecure) protocols and ports that bad actors commonly prey on.

And as such, if a workstation is compromised, the printer is not exposed. The same applies in the other direction. If the printer is compromised, the workstation is not exposed because there is no peer-to-peer print path (lateral movement).

SYSTEM COMPONENTS

The Sentry Print system works with the printers and multi-function devices deployed across your organization. The system is straightforward and requires only one software component, the Print Scout. Depending on your environment and solution preferences, two optional components may be deployed as part of the system: The Device Scout and the Sentry Print mobile app.

Print Scout

The Print Scout is lightweight client software that is deployed to employee workstations to enable secure printing and capture printing data. More specifically, the Print Scout:

- Provides a simple setup wizard for each user to register with Sentry Print and begin to print securely
- Submits, holds and releases print jobs
- Collects user printing data for reporting purposes, including:
    - User information from Active Directory (if AD is relevant)
    - Information from the printer that releases the print job (via SNMP)
    - Print job data via print stream analysis (print job name, number of pages, application from which the job was submitted, file format of the print job, and other metadata)

As a system administrator, you can control what data is collected and who can see it. You can configure the Print Scout's collection settings to disable or obfuscate the collection of certain types of data. You can also apply role-based viewing restrictions, giving some system users a limited view of the data. For example, you can enable or disable the collection of the user's name, department, region, building, the document name, and many other user-specific records. Print Scout data collection is covered in the Beacon Analytics technical whitepaper.

Cloud Connector deployment topology

The following illustration depicts the cloud deployment model, service responsibilities, and document submission and release workflows when using the Cloud Connector.

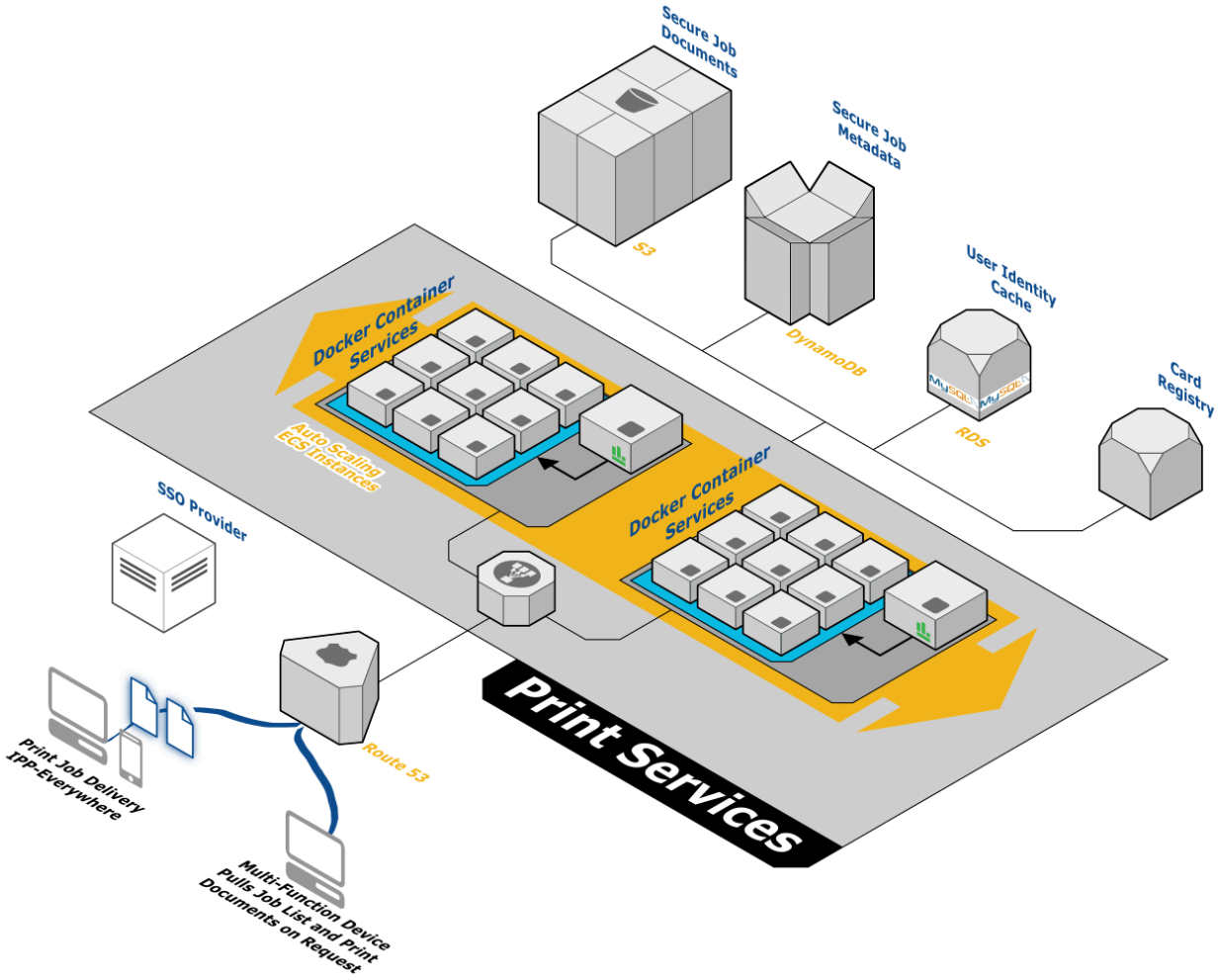

Figure 7: *The Sentry Print deployment topology*

This deployment topology leverages AWS best practices to provide security, scalability, and high availability. This includes using security groups to separate web, app, and data tiers, ELBs for load balancing and scalability, and ECS and EKS clusters for hosting microservice containers.

Services

Print Scout API Service: Provides the API to Print Scouts deployed on workstations, which allows them to retrieve configuration, report their health, auto-update, and submit documents from print queues.

Secured IPP Service: Provides a secure IPP implementation which exposes the IPP v2/IPP-Everywhere API to connected clients such as Linux, Windows, and Mac workstations, in addition to iOS and Android mobile devices. Print documents are submitted from these clients directly to this service in the cloud.

MFP Control Service: Provides control functionality to the applications running directly on MFPs, such as offloading card swipe events, proxying document listing, and reporting copy, fax, and scan transactions. This service will also assist in deploying applications to run on the MFPs.

MFP Data Service: Acts as a bridge between the MFP Control Service and applications running on the MFPs, to the containers directly responsible for managing user documents.

Identity Service: An implementation of the Microsoft Identity Service model, an OAUTH 2 based identity management service. It registers and authenticates users, mobile apps, access cards, and manages related access tokens.

Secure Job Storer: This microservice container is responsible for the storage and retrieval of print documents in the cloud. S3 file storage is used as the backing store for documents, which are encrypted at rest.

Secure Job Indexer: This microservice container is responsible for maintaining the document metadata, serving up the list of user documents and functions such as document expiry. The service is backed by AWS DynamoDB storage.

Secure Job Releaser: This microservice container is responsible for orchestrating the release of print documents to MFPs, maintaining the state of document releases in progress, and providing notifications on the release process to interested parties. The service is backed by AWS DynamoDB storage.

LOCAL CONNECTOR OPTION

The Sentry Print system also supports traditional networks with local services. In this configuration, employees print from their workstations as they normally do. The print job is encrypted and stored on the user's workstation and optionally in the cloud. Employees then walk up to any secured printer on the network. After successful authentication, their documents are released (printed).

The Local Connector option enables you to leverage Active Directory for authentication. Active Directory is not required to use Sentry Print, but if your organization *requires* AD then you must use the Local Connector configuration.

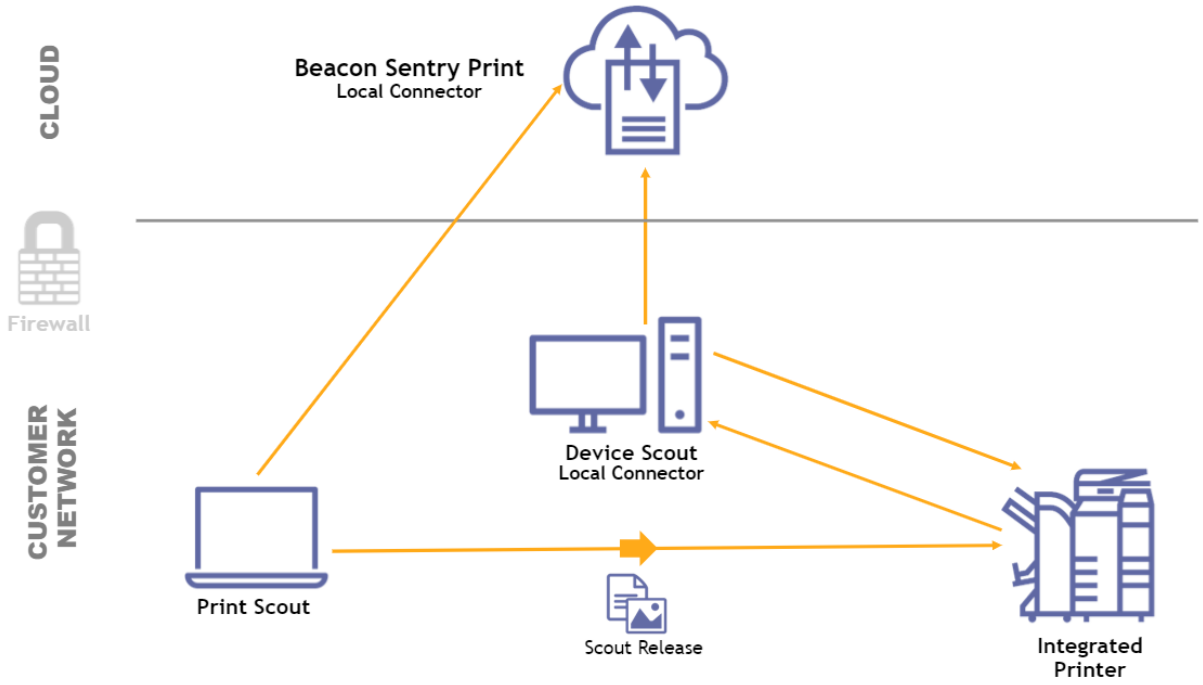

Figure 8: *Sentry Print for conventional networks with local storage of print jobs*

Supported devices

When used with the Local Connector option, Sentry Print works with practically any printer or MFP that you may have in your organization. Support for the user authentication option that involves the printer's control panel will depend on the device in use. All others can be secured via Sentry SR25 hardware or via QR code for print job release using the Sentry Print mobile app.

Network configuration

To deploy Sentry Print in your network using the Local Connector option, you need to install a Device Scout, and then employee workstations will need their own Print Scout installed.

Device Scout

The Local Connector configuration requires an on-premises Device Scout to remotely secure the devices in your environment. In addition to securing your network printers, the Device Scout also collects device data and uploads it to your Sentry Print account. The Device Scout is the server software referred to as the “Local Connector” herein. The Device Scout is not required in Zero Trust network configurations.

Collecting device data

The Device Scout locates all printers within your network and collects data on device status, meters, and consumables for display in Beacon Analytics. The Device Scout collects information from network devices that report themselves via SNMP as output devices:

IP address

Device description

Maintenance kit levels

Device serial number

Non-toner supply levels

Meter reads

Asset number

Monochrome or color

Location

Display reading

MAC address

Device status

Manufacturer

Model number

Error codes

Toner levels

Firmware version/patch level

Deployment architecture

Figure 9 shows the architecture of the solution using the Local Connector option for conventional networks that do not enforce Zero Trust principles.

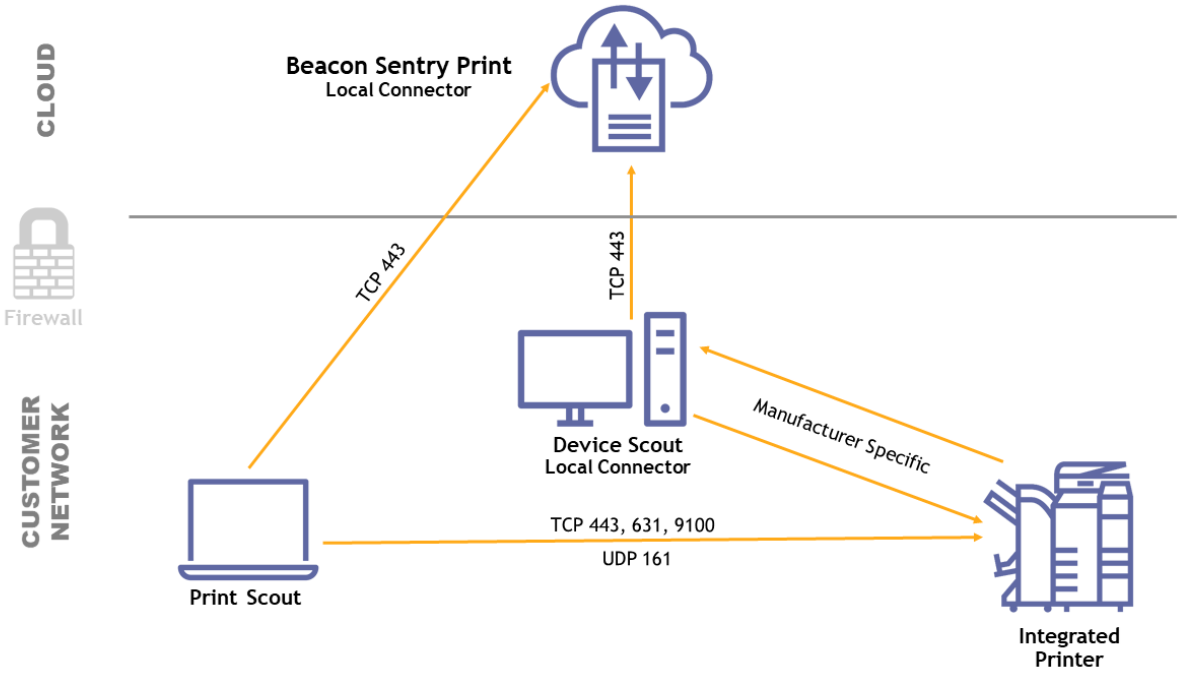

Figure 9: *Deployment architecture (Local Connector)*

- The Print Scout registers itself via an HTTPS (TLS) connection to Sentry Print. The Print Scout maintains a secure connection to the cloud service to enable print job submission and release.

- The Device Scout registers itself via an HTTPS (TLS) connection to Sentry Print. The Device Scout maintains a secure connection to the service to enable device configuration and to secure printers.

- The Device Scout communicates with the local Active Directory server using LDAP (TLS) to authenticate user credentials (if the authentication provider is Active Directory).

- The secure printer communicates via an HTTPS (TLS) connection to Sentry Print to release documents.

- The Print Scout delivers documents to the printer via an IPPS (TLS) connection. If the printer is not enabled for IPPS, the solution will fall back to using IPP. If IPP is also not supported, the solution will fall back to the RAW protocol. Neither IPP nor RAW are encrypted. To ensure that encryption is used to deliver documents, enable IPPS printing on your printers.

- The communication between the Integrated Printer and the Device Scout will vary based on the printer manufacturer. For details on OEM-specific ports, please see page 32.

MOBILE RELEASE (QR CODE) OPTION

You can configure Sentry Print to enable secure print submission and release using a mobile device. This solution option involves the use of the Sentry Print app for iOS and Android devices. This workflow option provides the following benefits:

- **Convenience and flexibility:** Employees can submit print jobs from their own mobile device, from any location or network, and then securely release their documents at any printer on your network.
- **Simple, touchless document release:** Employees walk up to a secure network printer with their mobile device and use the Sentry Print app to scan the QR code affixed to the printer. All documents held in their queue are released immediately after scanning. There is no need to touch the device control panel.
- Companies can enable secure print workflows without having to embed software on a printer; no installation or configuration is required for printers.
- Any PCL5-compliant network printer can be enabled for mobile release.

Network configuration

To deploy Sentry Print using the QR Code option in your network, you need to install one Device Scout to perform device discovery across the IP range(s) you specify, and Print Scouts must be installed on employee workstations. Users will also need to download and configure the Sentry Print mobile app for iOS and Android devices.

Sentry Print mobile app

The Sentry Print mobile app enables employees to release the documents parked in their secure queue by quickly scanning a QR code affixed to a printer on your network. To submit or release print jobs, employees must first download the Sentry Print mobile app from the App Store (iOS) or Google Play store (Android). Submitting documents from the app requires cloud storage of the print job.

Deployment architecture

Figure 10 shows the architecture of the Mobile Print option, including document submission and the document release workflow via QR code.

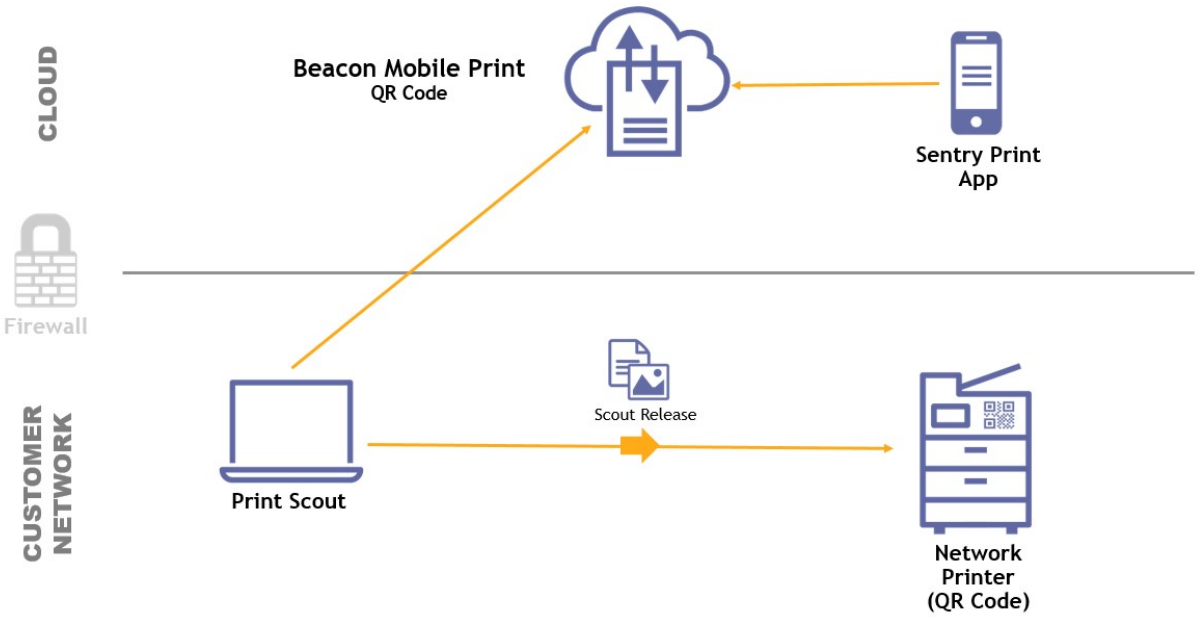

Figure 10: *Deployment architecture (QR Code)*

- The Print Scout registers itself via an HTTPS (TLS) connection to Sentry Print. The Print Scout maintains a secure connection to the cloud service to enable print job submission and release.
- The Secure Print mobile app registers itself via an HTTPS (TLS) connection to Sentry Print. The Secure Print mobile app establishes a secure connection to the cloud service to release documents when a network printer QR code is scanned with the mobile app using the phone's camera.
- The Device Scout is used for device discovery and is not required as part of the secure release system thereafter.

Configuration

Configuring QR Code release is a simple two-step process:

- **Secure your printers:** The system enables the administrator to quickly create QR code labels for each printer. A standard label template makes it easy to print these QR code labels and affix them to each printer. Each code contains a unique GUID that identifies the device for secure print release.
- **Activate mobile devices:** The Setup Guide (a click-through wizard) steps the user through the activation process. During this process, the user is directed to download the Sentry Print app on their mobile device. The Setup Guide generates a one-time QR code;

the user then activates their app by scanning this onscreen code. This binds the user to their mobile device to enable secure print release.

Document storage

How a document is submitted and released depends on whether print jobs are stored in the cloud or locally.

Cloud storage

When print jobs are stored in the cloud:

- In the case of an IPP-Everywhere submission, the document is sent directly to the Secured IPP Service in the cloud. This service interacts with both the Secure Job Indexer and Secure Job Storer services to "park" the document for later release and store its metadata for analysis and reporting via Beacon Analytics print analytics web dashboards.
- For print jobs submitted via Windows queue, the workstation interacts with the Print Scout API Service to send the document to the cloud, from which point the interaction is the same as those coming via the Secured IPP Service.

Local storage

With the local storage option, print jobs are parked on the user workstation. After the user successfully authenticates at the device, pressing **Print** or **Print All** instructs the MFP to communicate with Sentry Print to release the documents, which are then pushed from the workstation to the printer via the Print Scout.

When enabled in the Local Connector configuration, an encrypted copy of the print job is stored in the cloud. This allows jobs to be released even when the submitting workstation (Print Scout) is unavailable. When the submitting workstation is not available (in sleep mode, offline, etc.) the job may be routed through any available Print Scout on the network. Therefore, an active Print Scout must always be available in the system.

Document submission via Print Scout

To submit a document to print, users select the Print command in whatever application they are using. On Windows or Mac workstations, this opens a standard Print dialog box that shows the Sentry Print queue selected by default.

The user is redirected to complete the Print Scout user registration (if the user has not already completed the process). Upon successful user registration, the print submission will proceed, either via IPP-Everywhere or Windows print queue.

Document submission via Mobile

With the optional Sentry Print mobile app, employees can submit print jobs from their mobile device using IPP-Everywhere technology. After a simple configuration, users can print from any location or any external wireless network.

The app creates a connection between the user and the Sentry Print system. It quickly establishes the user identity and provides the profile required for printing. Users can then submit print jobs by using the native Print command on their phone.

Submitting documents from the Sentry Print app requires cloud storage of the print job. Users can print from any location or any external wireless network. They can also securely release their documents at any secured printer in the system by using the app to scan a QR code affixed to the printer. (See the “Touchless printing” section on page 25.)

Document release

After print submission, the user may release (print) their documents at any enabled printer or MFP. Users are required to authenticate before they can access their print queue (see the next page for more details). Upon successful user authentication, the job list is displayed on the MFP control panel. As shown in Figure 11, the user is first presented with a simple screen that provides a one-touch method to **Print All** jobs in their queue.

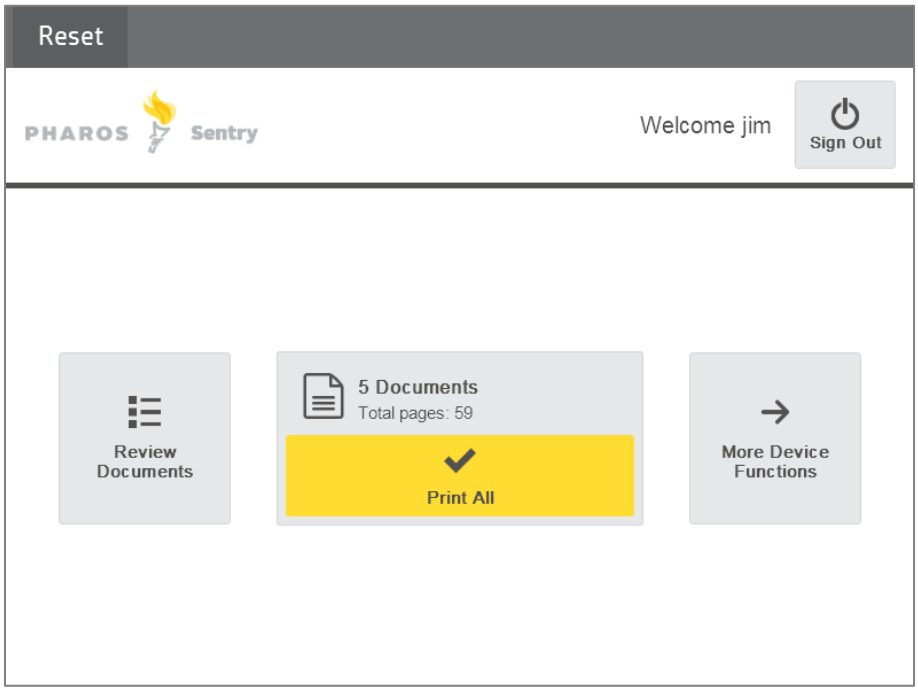

Figure 11: *After authenticating, the user can easily print all documents or access other options*

Or, the user can press **Review Documents** to view all job(s) in the queue. The job list displays the document name, submission time, and page count. as shown in Figure 12 below. Finally, the user can press **More Device Functions** to access copy, scan, or email functions.

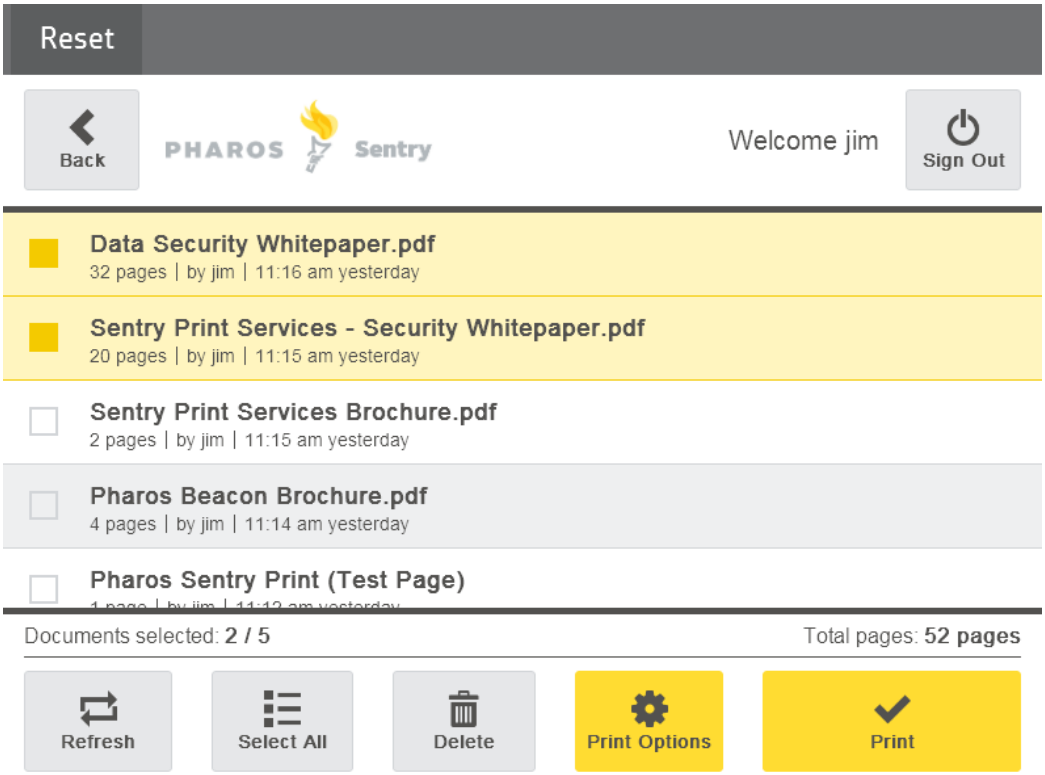

Figure 12: *Documents held in the Sentry Print queue (on the device control panel)*

If **Review Documents** is selected, the user can select one or more documents in the list and then press **Print**. This action (or the **Print All** command shown in Figure 12) instructs the MFP to pull the document from the cloud or push it from the workstation.

Upon successful print output, the MFP notifies the MFP Data Service which in turn tells the Secure Job Releaser to update the release state and orchestrate the cleanup of the document metadata and contents.

AUTHENTICATION OPTIONS

Sentry Print supports authentication at the printer by scanning a QR code with a mobile device, swiping an ID badge (proximity card), or entering an email and PIN into the printer's control panel. With the Local Connector configuration, username and password is another authentication option when Active Directory is in use.

Mobile Print (QR Code) – Touchless Print Release

With the mobile QR code authentication option, employees can use the Sentry Print app on their mobile devices (iOS and Android) to quickly scan a QR code affixed to a secure printer in the system. This option immediately releases all print jobs in the user's queue. Each QR code contains a unique GUID that identifies the device for secure print release. No information about the device is contained in the QR code.

Touchless printing

Enabling secure release using the Sentry Print app provides users with a simple, fast, and efficient print workflow option that does not require any interaction with the printer control panel. Whether you call it touchless print, touch-free print, contactless print, or even zero-touch print, the intent is the same: making it easier for employees to avoid touching shared surfaces whenever possible.

Users can even submit print jobs from home using their workstation or Sentry Print app on their mobile phone, and then coordinate the release of the document when a trusted colleague is present at a network device to collect the document.

Proximity card

With this configuration, employees use their access cards (proximity cards) to quickly authenticate at a chosen device to release their print jobs. Proximity cards are hashed using a one-way, non-reversible hash before being sent to the cloud for authentication. Proximity cards are securely stored in the cloud as a one-way, non-reversible hash.

Device communication

When using the **Local Connector** configuration, the Device Scout generates 2048-bit RSA certificates that secure the channel between the printer and the four services hosted on premises: authentication, authorization, accessories, and statistics. All communications to these four services are sent over port 4321. If a port other than 4321 is required, a configuration file must be changed post-install but pre-deployment, and the service must be restarted. Additionally, the deployment service pushes a public certificate to the printer so that the printer can securely access Sentry Print using TLS v1.2 over port 443.

When using the **Cloud Connector** configuration, communication is encrypted via TLS v1.2 over TCP port 443 using certificates that have been signed by industry-trusted authorities.

Control panel (“keypad”) login

With this configuration, employees enter their username and password, email and PIN, or passcode into the printer’s control panel to quickly authenticate at the chosen device to release their print jobs.

Username and password

When Active Directory is set as the authentication provider, employees can authenticate using their AD credentials (username and password). User credentials are kept within the company’s network and are never sent to the cloud. The authentication attempt is requested by the Local Connector to the company’s Active Directory domain controller.

Email and PIN

When email is set as the authentication provider, employees can authenticate using their email address and PIN from the workstation Setup Guide. The email and PIN are hashed using a one-way, non-reversible hash before being sent to the cloud for authentication. The email and PIN are securely stored in the cloud as a one-way, non-reversible hash.

Passcode

When OpenID is set as the authentication provider, employees can authenticate using their system-generated passcode from the workstation Setup Guide. The passcodes are hashed using a one-way, non-reversible hash before being sent to the cloud for authentication. The passcodes are securely stored in the cloud as a one-way, non-reversible hash.

Device communication

When using the **Local Connector** configuration, the Device Scout generates 2048-bit RSA certificates that secure the channel between the printer and the four services hosted on premises: authentication, authorization, accessories, and statistics. All communications to these four services are sent over port 4321. If a port other than 4321 is required, a configuration file must be changed post-install but pre-deployment, and the service must be restarted. Additionally, the deployment service pushes a public certificate to the printer so that the printer can securely access Sentry Print using TLS v1.2 over port 443.

When using the **Cloud Connector** configuration, communication is encrypted via TLS v1.2 over TCP port 443 using certificates that have been signed by industry-trusted authorities.

DATA PROTECTION

The integrity of your data is critical. Sentry Print uses both technological and procedural controls to restrict access to data. The system gives you control over what data is collected and who can see it. No device or printing information can be transmitted to the cloud service until scouts are installed and activated. At any time, you may stop a scout from collecting information by uninstalling it.

In today's high-risk security climate, every organization must continually refine its security strategy to address evolving threats. Your print environment should be part of your organization's security strategy and a standard part of your processes and procedures. Here, we describe various types of attacks that exist within a printing context, and how Sentry Print addresses these threats.

- **General malicious attack:** Such an event could include an attempt to intercept data in transmission, denial of service, or the attempted altering or disabling of established security measures such as logins or encrypted communication. Sentry Print encrypts all external connections using TLS at the highest level supported by the connecting browser or service. All application components are isolated by function; only necessary traffic can pass between components.
- **Malicious attack of print data:** Such an event could include an attempt by a third party to intercept company print data. To prevent this, Sentry Print employs one of two kinds of encryption, based on where the document is stored at rest. Configurations in which the document is held at rest on the client side will use a Zero Knowledge Encryption scheme. Documents stored in the cloud are protected by Amazon S3 KMS encryption.
- **Machine or technological failure:** Such an event could include power loss, network connectivity loss, or data storage failure. Sentry Print uses a cloud infrastructure with a minimum of three geographic zones. This cloud infrastructure can detect a variety of fault conditions and remove or fix defective components with no interruption of service.
- **Passive data loss or corruption:** Such losses could be caused by software defects, incompatibilities between software components, or data storage loss. The Sentry Print infrastructure mitigates these risks through a formal software quality assurance methodology. In the event of a data corruption problem, the system maintains pre-state backups to roll back any data-altering changes. The system also uses segregation of duties and least privilege principles to restrict the level of access employees have, to include only that which is required to perform their job function. Access levels are periodically reviewed and adjusted as business needs or job roles change.

Document Encryption

The Sentry Print system leverages the latest encryption standards to ensure that documents are secure. There are two kinds of file encryption used in the system, based on the configuration in use. When a document is stored in the cloud, it is encrypted at rest using AWS S3 KMS encryption. When it's stored on the client, it leverages zero knowledge encryption.

AWS S3 with KMS encryption

For documents stored in the cloud, Sentry Print leverages Amazon Simple Storage Service (S3) with Key Management Service (KMS) encryption. This provides access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of websites.

Print jobs are secured with S3 KMS encryption. The document is sent to the cloud protected in transit by HTTPS and then encrypted at rest. The following links provide more information on Amazon S3 and KMS encryption:

https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

Zero Knowledge Encryption

In addition to full encryption of transport, the system also employs zero knowledge encryption for documents at rest whenever the document is stored on the client side (by the Print Scout) or in the cloud whenever push print is being used; in other words, in the hybrid configuration that leverages local print job storage. The Print Scout sends print jobs directly to a printer in the system, hence “push print.”

The cloud storage configurations of Sentry Print do not use zero knowledge encryption because the printers and MFPs pull the documents directly from the cloud themselves.

During installation, you are provided a system-generated site encryption password. The system does not retain a copy of this password; you must securely backup the password to enable future scout installation and maintain the security of the print data.

The site encryption password is used to generate a 256-bit AES key, using the derivation function PBKDF2 with 1,000 iterations. This key is used to encrypt documents before they leave your local network, and to decrypt them prior to print release. In addition, a PKI 2048-bit RSA key pair is generated for communication security with both the private key and AES key above being installed on the scouts in your local network.

When documents are released (printed), they are decrypted when they arrive back on your network. Therefore, even in the unlikely event that an attacker breaches the cloud security measures in Sentry Print, the attacker would be unable to access any document data.

Encryption details

ITEM	ENCRYPTION USED
ENCRYPTION OF DATA TRANSPORT	TLS Version: 1.2
DOCUMENT ENCRYPTION	AES 256-bit
MFP CERTIFICATES	2048-bit RSA

User Identity Hashing

When the user taps a proximity card or enters an email + PIN, or passcode, the values are hashed using a one-way, non-reversible SHA-256 key and sent to the cloud for validation. The system looks at the hash value and authenticates the user accordingly.

Security is a shared responsibility

As a Sentry Print customer, you share the responsibility to protect your data. As your organization continually refines its security strategy to address evolving threats, make certain that securing your print environment is a priority. Add these security items to your standard processes to help you address the diverse and ever-evolving threats out there.

1. Ensure that all scouts are accessible to authorized users only.
2. Ensure that servers and/or workstations hosting scouts are fully patched and meet all other security requirements of your organization.
    a. Ensure that servers and/or workstations are regularly maintained according to the policies of your organization.
    b. Ensure that the minimum necessary credentials are granted to individuals within your organization.
3. If the Print/Device Scout will be installed on a shared server, (i.e. a server that performs multiple functions or that will be running software from another vendor), ensure that you have verified compatibility with technical support before installing.
4. Ensure that all printers are fully patched and meet all other security requirements of your organization.
5. If using the Sentry Print mobile app, ensure that all mobile devices are fully patched and meet all other security requirements of your organization.

CUSTOMER READINESS

This section details the environmental requirements and recommendations necessary to successfully deploy Sentry Print. It also records the ports and protocols used in each network configuration.

Platform communication

Your email security software must be set to trust the following email address from Sentry Print to help prevent your organization from quarantining or blocking the message or sending the email communication to the Junk or Spam folder:

Beacon Admin <no-reply@beacon.pharos.com>

Cloud API endpoints

Sentry Print cloud API endpoints process collected data and print jobs, push application updates and configuration settings, and broker communication between systems components.

The software components, such as the Print Scout and cloud-aware printer, must be able to securely communicate to the cloud API endpoints. If permitted by your organization, Pharos recommends whitelisting the domain ***.beacon.pharos.com** to ensure that communication with current and future cloud API endpoints is permitted. Below is a list of cloud API endpoints if your organization requires the list of permitted URLs.

- https://api.beacon.pharos.com
- https://devicescout.beacon.pharos.com
- https://files.beacon.pharos.com
- https://login.beacon.pharos.com
- https://mfp-api.beacon.pharos.com
- https://printscout.beacon.pharos.com
- https://www.beacon.pharos.com

Network ports and protocols

The following diagrams show the ports and protocols used in the various configuration and user authentication options.

Cloud Connector / Zero Server configurations

Figures 13 and 14 show the basic structure and ports required to deploy Sentry Print using the Cloud Connector / Zero Server configuration, first with secure document release from the cloud, and then with Scout-based document release.

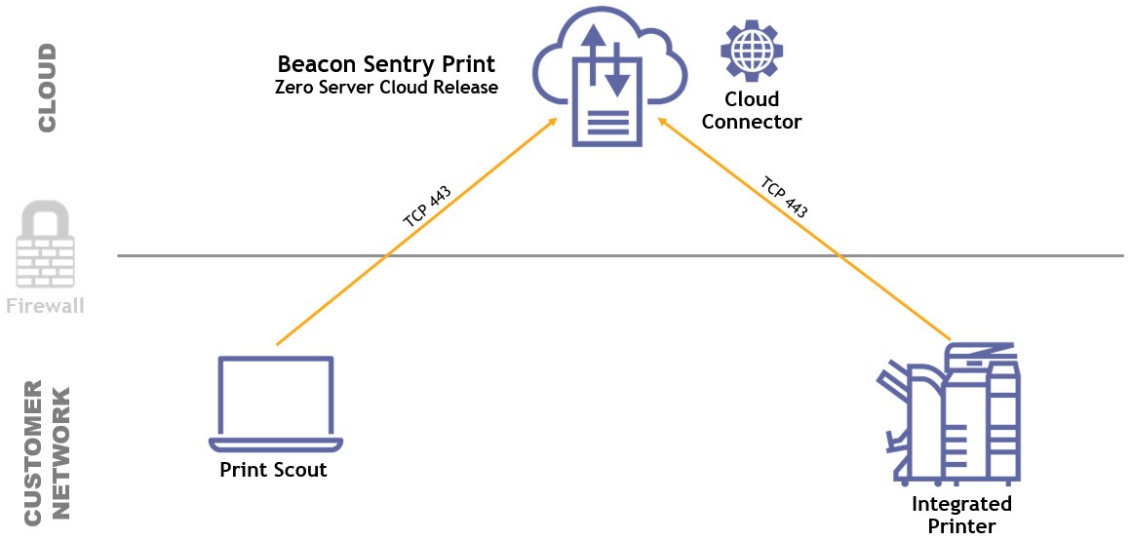

Figure 13: *Ports required for the Cloud Connector / Zero Server configuration (cloud release)*

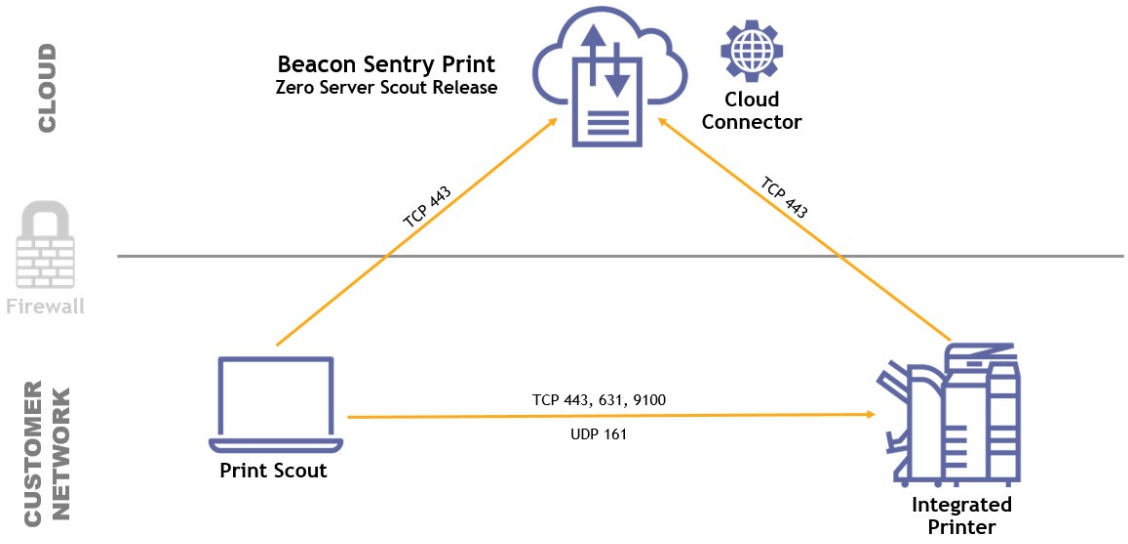

Figure 14: *Ports required for the Cloud Connector / Zero Server configuration (Scout release)*

Figure 15 shows the basic structure and ports required to deploy Sentry Print in a Zero Trust network environment.

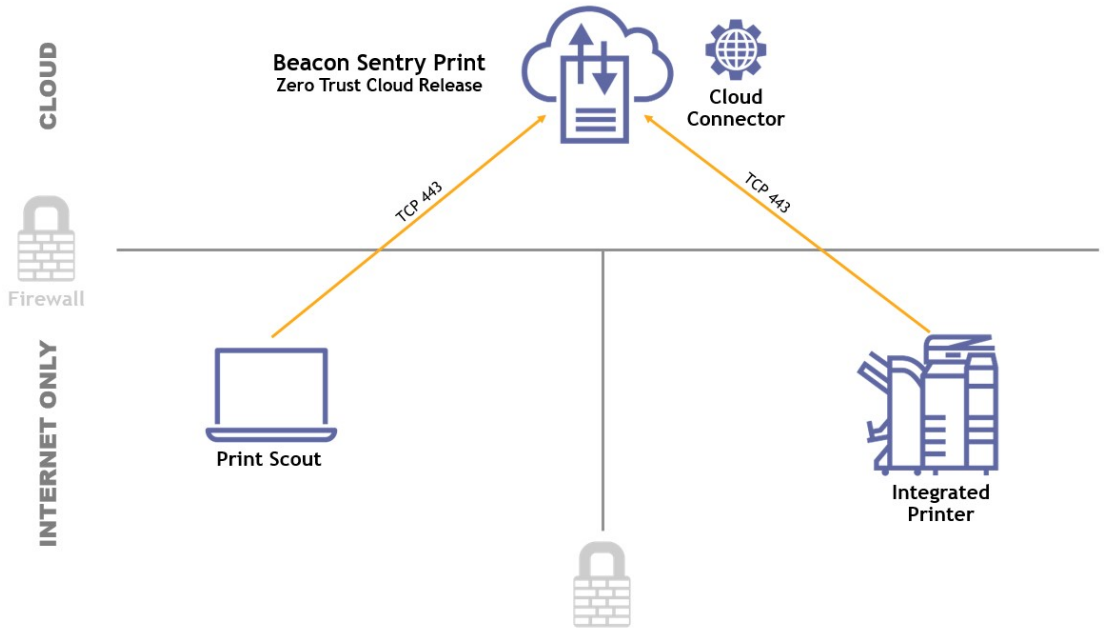

Figure 15: *Ports required for Sentry Print in a Zero Trust network environment*

Local Connector

In a Local Connector environment, the ports required to enable communication between the site service (Device Scout) and the printer will vary based on the printer manufacturer. Figure 16 shows the structure and ports required in the Local Connector configuration with HP devices.

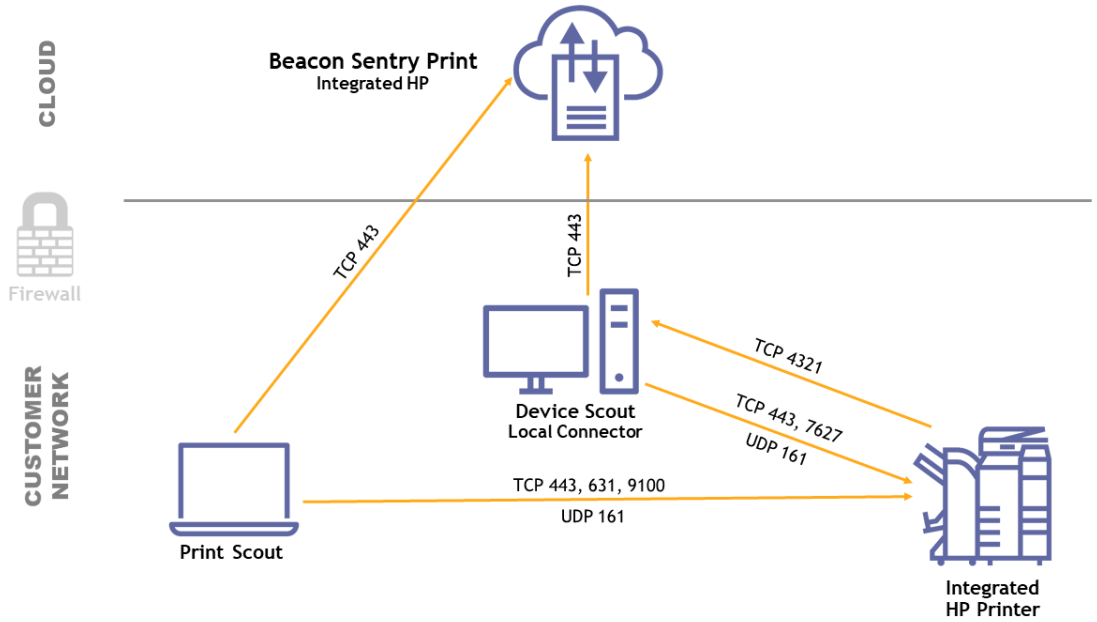

Figure 16: *Structure and ports required for deployment of Local Connector (HP devices)*

Figure 17 shows the structure and ports required in the Local Connector configuration with Konica Minolta (KM) devices.

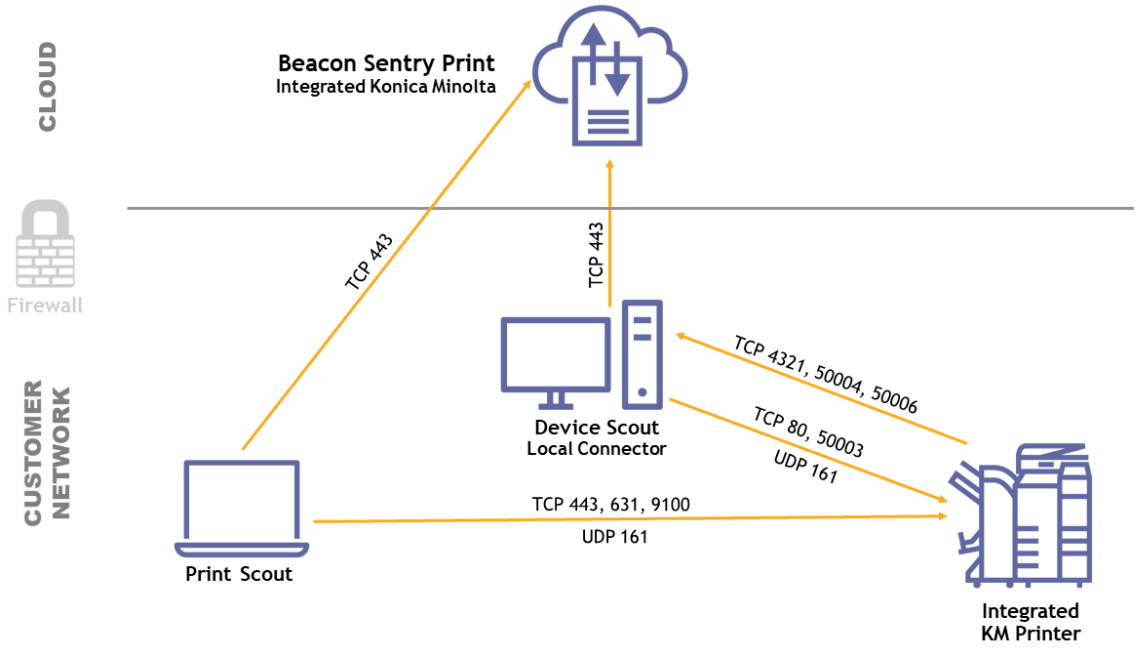

Figure 17: *Structure and ports required for deployment of Local Connector (KM devices)*

Figure 18 shows the structure and ports required in the Local Connector configuration with Lexmark devices.

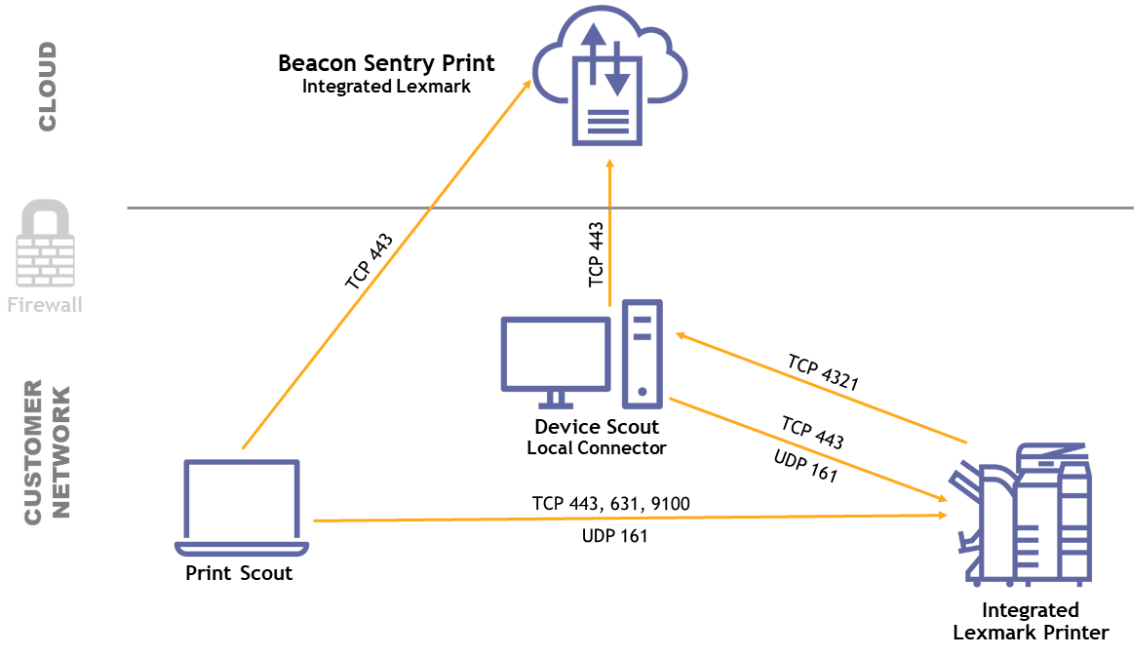

Figure 18: *Structure and ports required for deployment of Local Connector (Lexmark devices)*

Figure 19 shows the structure and ports required in the Local Connector configuration with Ricoh devices.

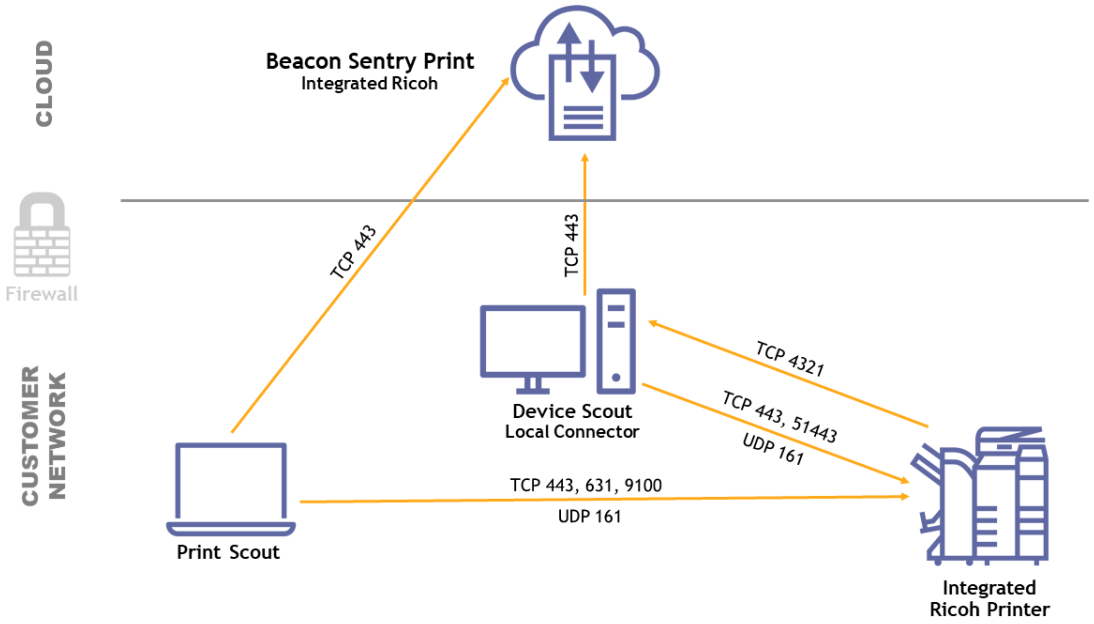

Figure 19: *Structure and ports required for deployment of Local Connector (Ricoh devices)*

Figure 20 shows the structure and ports required in the Local Connector configuration with Xerox devices.

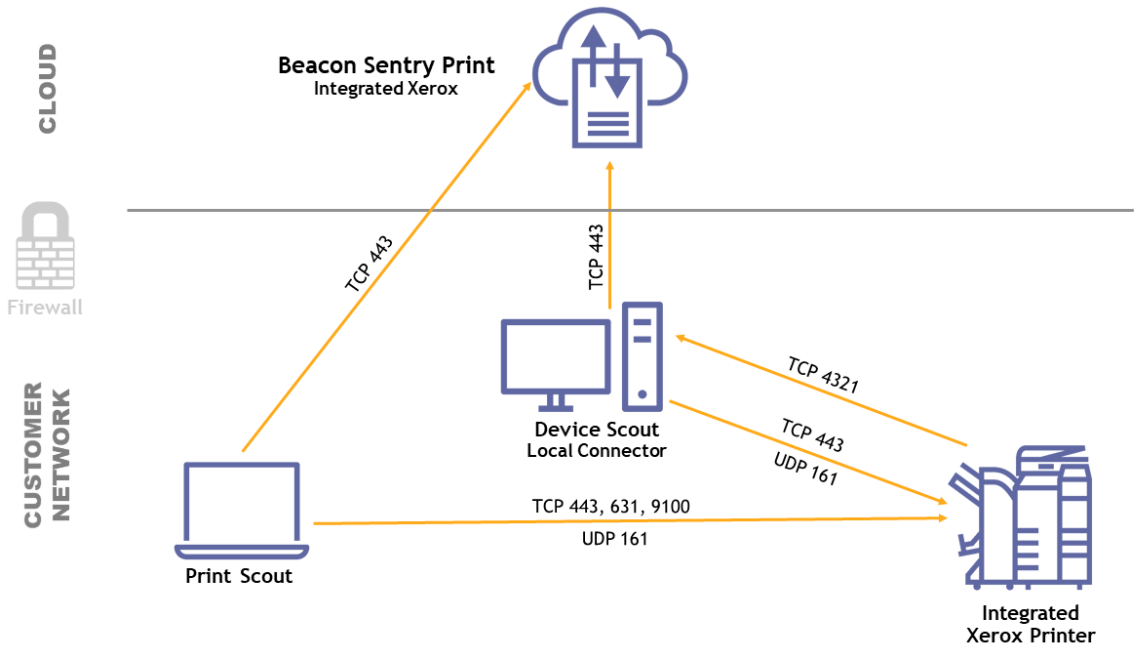

Figure 20: *Structure and ports required for deployment of Local Connector (Xerox devices)*

Mobile Release (QR Code)

Figure 21 shows the basic structure and ports required in the Mobile Print (QR Code) release workflow.

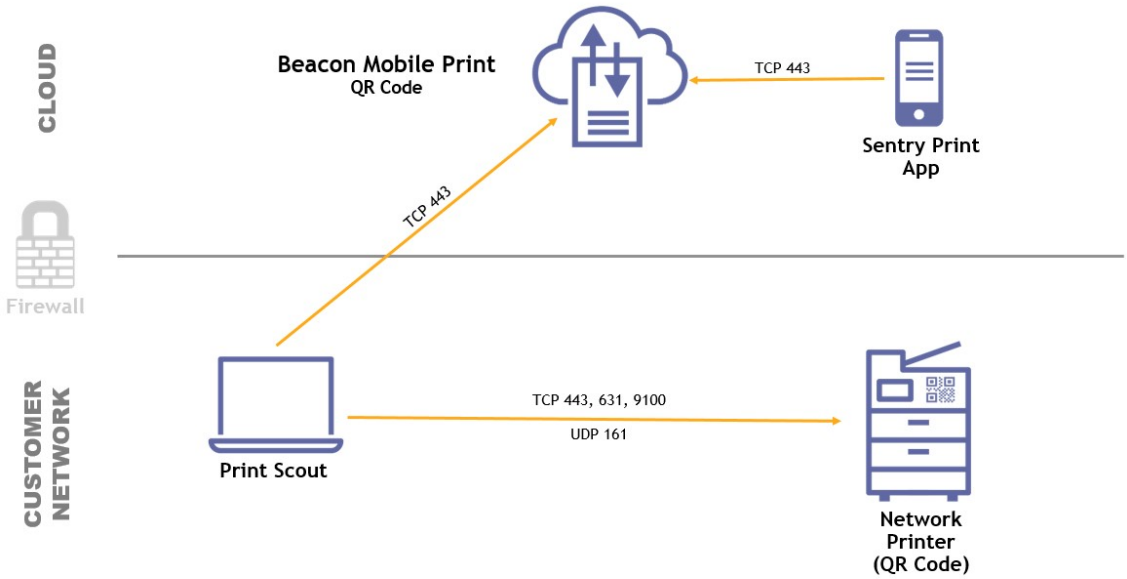

Figure 21: *Structure and ports required for Beacon Mobile Print option*

SR25 Hardware

The Sentry SR25 is a small piece of hardware that attaches to a printer to enable secure print authentication. These are used when a printer model does not support integrated software to control access.

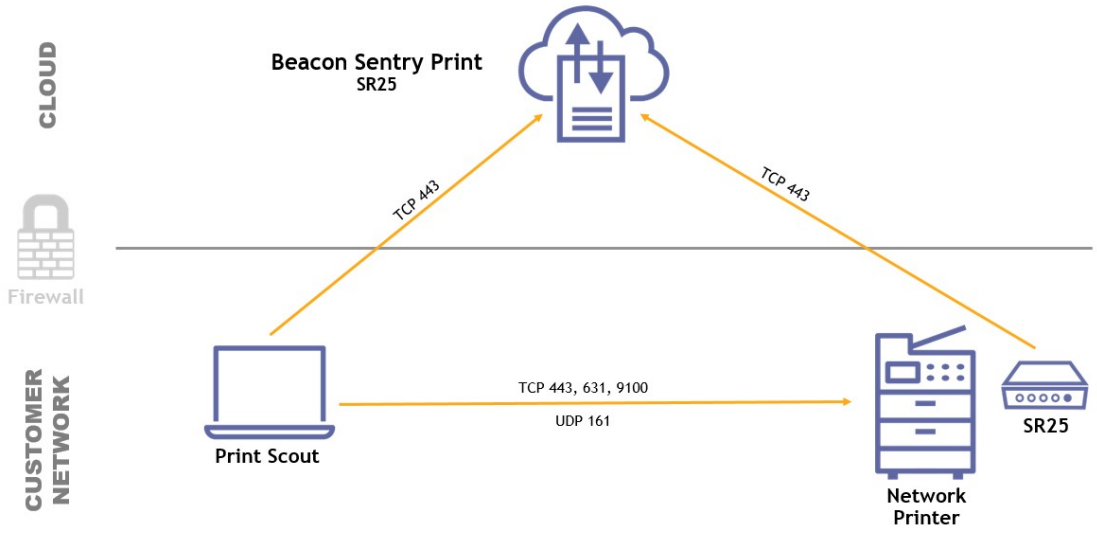

Figure 22 shows the basic structure and ports required in the SR25 release workflow.

Deployment requirements

Print Scout

The Print Scout is lightweight client software that is deployed to employee workstations to enable secure printing and capture printing data. The Print Scout encrypts and stores secure print jobs, uploads a copy to the cloud (when cloud storage is enabled), and decrypts and delivers secure print jobs to network printers (when local storage is enabled).

Requirements

1. Supported operating systems:
    - Windows: 8.1 and 10
    - macOS: 10.14, 10.15, and 11
    - Ubuntu: 18.04 and 20.04 (when OpenID is enabled)
    - Red Hat: 8
    - Windows Server®: 2012 R2, 2016, and 2019
2. TLS v1.2 must be enabled.
3. For Windows systems, Microsoft .NET Framework 4.6.1 (or newer) must be installed.

4. The Print Scout must be installed on print user workstations to (1) submit, store, manage and release a secure print job and (2) enable the Secure Print mobile app.
5. The Print Scout must be able to communicate with network printers to (1) collect device data and (2) release a secure print job when local storage is enabled.
6. The Print Scout must be able to communicate with the cloud APIs to (1) upload collected print job, device data, and print user information, (2) upload encrypted secure print job, and (3) download application updates and configuration settings.
7. The Web proxy server configuration (server, port, user credentials) is known, if required to access the Internet (cloud).
8. For Windows systems, end point protection (antivirus) software must trust the Print Scout executable (exe) files and dynamic link library (dll) files within this directory path and all its subfolders:

   C:\Program Files (x86)\PharosSystems\PrintScout

9. End point protection (antivirus) software must trust the Windows services for the Print Scout:

   Pharos Systems Print Scout Service

   Pharos Systems Print Scout Spooler Service

10. When using OpenID Connect (OIDC) to authenticate, the Print Scout must be able to communicate with the OIDC identity provider to authenticate the print user.
11. When using the Local Connector configuration and Active Directory is the authentication provider, the Print Scout must be joined (1) to an on-premises Microsoft Active Directory domain and (2) to the same domain as the Device Scout.
12. When using email and PIN for authentication, the print user must be able to verify that the email address is valid.
13. The following network ports must be open:
    - Outbound (Print Scout connecting to the cloud API endpoint):
      - 443 TCP (TLS v1.2)
    - Outbound (Print Scout connecting to the network printer):
      - 161 UDP (SNMP v1/v2 or SNMP v3)
      - 631 TCP (IPP)
      - 443 TCP (IPPS)
      - 9100 TCP (RAW)

Device Scout

The Device Scout remotely secures the network devices in your environment, authenticates users to Active Directory, and collects device data and uploads it to your Sentry Print account. The Device Scout is not required when using the Cloud Connector configuration.

Requirements

1. Supported operating systems:
    - Windows Server: 2012 R2, 2016, and 2019
    - Windows: 8.1 and 10
2. TLS v1.2 must be enabled.
3. Microsoft .NET Framework 4.6.1 (or newer) must be installed.
4. The Device Scout must be able to communicate with the cloud APIs to (1) upload collected device data and (2) download application updates and configuration settings.
5. The Web proxy server configuration (server, port, user credentials) is known, if required to access the Internet (cloud).
6. For Windows systems, end point protection (antivirus) software must trust the Device Scout and Local Connector executable (exe) files and dynamic link library (dll) files within this directory path and all its subfolders:

    C:\Program Files (x86)\PharosSystems\DeviceScout

    C:\Program Files (x86)\PharosSystems\Sentry Print Service
7. End point protection (antivirus) software must trust the Windows services for the Device Scout and Local Connector:

    Pharos Device Scout Service

    Pharos Systems Sentry Print Service
8. The Device Scout must be able to communicate with network printers to collect device data.
9. When using the Local Connector configuration, the Device Scout must be able to communicate with network printers to (1) secure integrated printers and (2) authenticate users. If Active Directory is the authentication provider, the Device Scout must be (1) joined to an on-premises Microsoft Active Directory domain and (2) joined to the same domain as Print Scouts (print user workstations).
10. The following network ports must be open:
    - Outbound (Device Scout connecting to the cloud API endpoint):
        - 443 TCP (TLS v1.2)
    - Outbound (Device Scout connecting to the HP integrated printer):
        - 443 TCP (TLS v1.2)
        - 7627 TCP (TLS v1.2)
        - 161 UDP (SNMP)
    - Inbound (HP integrated printer connecting to the Device Scout):
        - 4321 TCP (TLS v1.2)
    - Outbound (Device Scout connecting to the KM integrated printer):

    - 80 TCP (HTTP)
    - 50003 TCP (TLS v1.2)
    - 161 UDP (SNMP)
- Inbound (KM integrated printer connecting to the Device Scout):
    - 4321 TCP (TLSv1.2)
    - 50004 TCP (TLSv1.2)
    - 50006 TCP (TLSv1.2)
- Outbound (Device Scout connecting to the Lexmark integrated printer):
    - 443 TCP (HTTP)
    - 161 UDP (SNMP)
- Inbound (Lexmark integrated printer connecting to the Device Scout):
    - 4321 TCP (TLSv1.2)
- Outbound (Device Scout connecting to the Ricoh integrated printer):
    - 443 TCP (TLS v1.2)
    - 51443 TCP (TLS v1.2)
    - 161 UDP (SNMP)
- Inbound (Ricoh integrated printer connecting to the Device Scout):
    - 4321 TCP (TLSv1.2)
- Outbound (Device Scout connecting to the Xerox integrated printer):
    - 443 TCP (HTTP)
    - 161 UDP (SNMP)
- Inbound (Xerox integrated printer connecting to the Device Scout):
    - 4321 TCP (TLSv1.2)

Integrating Printers

Printers can be integrated into the Sentry Print system for user authentication via proximity card or keyboard control panel login. Upon successful login, the user may choose to print all documents in the queue, review and select documents to print, or access other device functions such as copy, scan to email, and fax. Integrated printers track all secure print, copy, scan to email, and fax activity.

HP Requirements

1. The printer must be a supported model as certified by HP.

2. The printer readiness requirements must have been completed:
    - Firmware must be version 4.8 or later.
    - Local administrator password must be known.
    - DNS settings must resolve the (1) Beacon cloud API endpoints (when using the cloud connector) or (2) Device Scout server (when using the local connector).
    - Date and time settings must be accurate to allow TLS secure communication.
    - Web proxy settings must be configured if required to access the public Internet.
    - Cross-Origin Resource Sharing (CORS) must be enabled.
    - If trusted sites are enabled in CORS, the trusted sites list must include *.beacon.pharos.com (when using the Cloud Connector) and the Device Scout server (when using the Local Connector).
    - Color print must be enabled to provide color printing capability for non-domain, macOS, Linux, iOS and Android users.
    - The TCP Idle Timeout may be increased to prevent truncating lengthy or complex print jobs
    - Sleep after inactivity may be turned off and sleep schedule may be enabled to improve proximity card reader performance during business hours.
3. When using the Cloud Connector configuration, cloud API endpoints also launch the Secure Print app, authenticate users, and enable display of the user's print job list.
4. When using the Local Connector configuration, the HP printer must be able to access the Device Scout fully qualified domain name (FQDN) to launch the Secure Print app, authenticate users, and display the user's print job list.
5. The Web proxy server configuration (server, port, user credentials) must be known if required to access the Internet (cloud).
6. The following network ports must be open:
    - Outbound (HP printer connecting to the cloud API endpoint, in Cloud Connector configurations)
        - 443 TCP (TLS v1.2)
    - Outbound (HP printer connecting to the Device Scout, in Local Connector configurations)
        - 4321 TCP (TLSv1.2)
    - Inbound (Deployment tool (for Cloud Connector option) or Device Scout (for Local Connector option) connecting to the HP printer):
        - 443 TCP (TLS v1.2)
        - 7627 TCP (TLS v1.2)

Konica Minolta Requirements

1. The printer must be a supported model as certified by Konica Minolta (KM).
2. The printer readiness requirements must have been completed:
    - Local administrator password must be known.
    - DNS settings must resolve the (1) Beacon cloud API endpoints and (2) Device Scout server.
    - Date and time settings must be accurate to allow TLS secure communication.
    - Web proxy settings must be configured if required to access the public Internet.
    - Web Browser is licensed and enabled on the printer.
    - Web browser cache is disabled.
    - SSL and PKI protocol settings are enabled and configured.
    - OpenAPI and TCP Socket settings are enabled and configured.
3. The Web proxy server configuration (server, port, user credentials) must be known if required to access the Internet (cloud).
4. The following network ports must be open:
    - Outbound (KM printer connecting to the Device Scout)
        - 4321 TCP (TLSv1.2)
        - 50004 TCP (TLSv1.2)
        - 50006 TCP (TLSv1.2)
    - Inbound (Device Scout connecting to the KM printer):
        - 80 TCP (HTTP)
        - 50003 TCP (TLS v1.2)
        - 161 UDP (SNMP)

Lexmark Requirements

1. The printer must be a supported model as certified by Lexmark.
2. The printer readiness requirements must have been completed:
    - Local administrator password must be known.
    - DNS settings must resolve the Device Scout server.
    - Date and time settings must be accurate to allow TLS secure communication.
3. The Web proxy server configuration (server, port, user credentials) must be known if required to access the Internet (cloud).
4. The following network ports must be open:

- Outbound (Lexmark printer connecting to the Device Scout)
    - 4321 TCP (TLSv1.2)
- Inbound (Device Scout connecting to the Lexmark printer):
    - 443 TCP (TLS v1.2)
    - 161 UDP (SNMP)

Ricoh Requirements

1. The printer must be a supported model as certified by Ricoh.
2. The printer readiness requirements must have been completed:
    - Local administrator password must be known.
    - DNS settings must resolve the Device Scout server.
    - Date and time settings must be accurate to allow TLS secure communication.
3. The Web proxy server configuration (server, port, user credentials) must be known if required to access the Internet (cloud).
4. The following network ports must be open:
    - Outbound (Ricoh printer connecting to the Device Scout)
        - 4321 TCP (TLSv1.2)
    - Inbound (Device Scout connecting to the Ricoh printer):
        - 443 TCP (TLS v1.2)
        - 51443 TCP (TLS v1.2)
        - 161 UDP (SNMP)

Xerox Requirements

1. The printer must be a supported model as certified by Xerox.
2. The printer readiness requirements must have been completed:
    - Local administrator password must be known.
    - DNS settings must resolve the Device Scout server.
    - Date and time settings must be accurate to allow TLS secure communication.
3. The Web proxy server configuration (server, port, user credentials) must be known if required to access the Internet (cloud).
4. The following network ports must be open:
    - Outbound (Xerox printer connecting to the Device Scout)
        - 4321 TCP (TLSv1.2)

- Inbound (Device Scout connecting to the Xerox printer):
    - 443 TCP (TLS v1.2)
    - 161 UDP (SNMP)

Sentry Print mobile app

Employees can use the Sentry Print mobile app to submit print jobs and release documents at a secure printer by scanning the QR code affixed to the printer in the system. All documents in the user's queue are immediately printed.

Requirements:

1. Supported operating systems:
    - Android 7 or newer
    - iOS 8 or newer
2. The Sentry Print mobile app is free and must be downloaded using a supported mobile device from the (1) Google Play Store or (2) Apple App Store.
3. The Sentry Print mobile app must be able to communicate with the cloud API endpoints to release a user's print jobs.
4. The following network ports must be open:
    - Outbound (Secure Print mobile app connecting to the cloud API endpoint):
        - 443 TCP (TLS v1.2)

Deployment tool

This command line utility secures and unsecures an integrated printer via the Cloud Connector. For the Deployment tool to work, the following network ports must be open:

- Outbound (Deployment tool connecting to the cloud API endpoint):
    - 443 TCP (TLS v1.2)
- Outbound (Deployment tool connecting to the HP integrated printer):
    - 443 TCP (TLS v1.2)
    - 7627 TCP (TLSv1.2)

NETWORK UTILIZATION

Print Scout

The Print Scout securely uploads print job information as it happens. The following table details the network traffic created by the Print Scout.

TASK TYPE	FREQUENCY	NETWORK TRAFFIC (IN BYTES)
Status	1x24hrs	2K
AD lookups	Once per day, per user	Depends on size of average AD record
Cloud connection keep-alive	Every minute	< 0.1K
Print job metadata uploads	On print submission	3K
Print job content uploads	On print submission	Variable based on the size and complexity of the print job. This is off by default and conditional on customer setting.
Incoming release requests and notifications	On print release	< 1K
Incoming job contents	On print release	Variable based on the size and complexity of the print job. This is used only when a user's workstation is offline and cloud holds a copy of their job contents.
Job delivery to printer	On print release	Variable based on the size and complexity of the job.
Device SNMP lookup	On print release	2.5K

Print Scout communication patterns

- **Print Scout status checks:** Each Print Scout checks in once per day to upload its health report and check for new settings. This check is under 2 KB and will usually return an empty response if there have been no configuration changes. The Print Scout will also check for configuration changes when a print job is submitted.

- **Active Directory lookups:** When an employee submits a print job, the Print Scout will look up Active Directory information about that user. The AD lookup will occur only once per day. AD traffic is difficult to estimate because the amount of data stored in AD is highly variable from one organization to the next. However, the maximum traffic equates to the total number of unique AD users multiplied by the average AD record size.
- **Cloud connection:** The communication channel between Print Scouts and the cloud is kept alive by means of a server-initiated ping. This request occurs approximately once per minute and consists of a small packet of bytes.
- **Print job metadata uploads:** Data describing each print job is sent to the cloud service. This data is variable because of the strings involved (document name), but a fair approximation is 1 KB per print job.
- **Print job content uploads:** The contents of the print job can be optionally uploaded to the server when configured to do so. This copy is used as a backup in case the user's workstation is unavailable at the time they choose to release their job at a printer. The size of this content is based on the size and complexity of the source document, but it is compressed prior to transfer. Typical one-page text documents are less than 100 KB.
- **Incoming release requests and notifications:** The server will issue requests to Print Scouts when a user selects their jobs to release at a printer. Notifications on the success or failure of the request are sent from the Print Scout back to the server. These requests and notifications comprise a small amount of text data, less than 1 KB in size.
- **Incoming print job content:** When necessary, and if configured to do so, a copy of the user's job contents may be delivered from the cloud service to the Print Scout. This can happen when the user's workstation becomes unavailable (goes into sleep mode, goes offline, etc.). In such an event, the server will select another Print Scout to perform the print release.
- **Job delivery to printer:** The user's job contents are ultimately delivered from a Print Scout to their chosen printer. The data at this point is uncompressed but would equal the amount that would be delivered to a printer if the user were direct printing from Windows, without the Print Scout.
- **Automatic scout updates:** From time to time, a new version of the Print Scout will be released, with updated functionality and any bug fixes. The scout will check for new versions of itself whenever it checks for new configuration information. If a new version is available, the scout will automatically download and install the new version silently.

Device Scout

Sentry Print requires access to your local area network to operate effectively. The Device Scout will generate **local network traffic** when performing these operations:

- Scanning configured network ranges for printing devices
- Collecting meter data from discovered devices
- Collecting service alerts from discovered devices

- Configuring integrated printers
- Logging into a secure device

The Device Scout uses SNMP to communicate with local network devices and supports SNMPv1/v2 and/or SNMP v3. In some cases, the Device Scout will also try to connect to a device using HTTP port 80, if the device is a known model that cannot report serial number or meter reads via SNMP.

The Device Scout will generate **Internet traffic** when performing these operations:

- Registration
- Polling the Device Scout control server for new configuration or instructions
- Uploading discovered device data
- Uploading device meter data
- Uploading Device Scout health check information
- Configuring integrated printers
- Logging into a secure device
- Interacting with a secure device (user activity)

The Device Scout uses secure HTTPS communication when connecting to Sentry Print. Additionally, all end-user access to the application is encrypted using TLS. Unencrypted SNMP traffic is restricted to the local subnets that the Device Scout is configured to monitor.

Device Scout network traffic

Here are the average payload sizes for the various Device Scout operations:

TASK TYPE	NETWORK TRAFFIC (IN BYTES)
Device discovery	15.8 K
Non-device usage	< 0.1K
Device status	16.6 K
Securing a device	2K
Printing from a secure device	< 100K

Excluding IP ranges

Non-printing SNMP-configured devices respond with a 126-byte payload, which tells the Device Scout that the device is **not** a printing device. While not harmful, this overhead may add up over large IP ranges. Therefore, we recommend using "Exclude Ranges" in the Device Scout configuration to skip over any IP ranges that are not likely to contain output devices.

Device Scout communication patterns

- **Registering a Device Scout:** Customers create and configure a Device Scout record in the web application. To download the installation package, you must enter the site encryption key. A unique installation package per Device Scout record is created. During the installation of this package, the Device Scout will open a secure connection to Sentry Print and identify itself using the registration information contained in the package. Once a package has been installed and registered, it cannot be used again.
- **Polling the scout control server:** Upon initial registration, and periodically during normal operation, the Device Scout will poll the control server for updates to its configuration state. Updates might include new IP ranges to scan, a new version to download, or a new schedule for discovering or reading devices.
- **Uploading discovered device data:** The Device Scout will upload discovered devices once per period, configured within the application. Discovery scans can be configured daily or weekly. More frequent uploads will result in more network traffic, but newly discovered devices will be displayed in the application more quickly.
- **Uploading device meter data:** The Device Scout will upload meter reads to the scout control server on a scheduled basis. Usage (meter) data can only be scheduled for a daily scan and upload. You configure this setting within the application.
- **Uploading toner data:** Toner information will be collected along with meter data by default. Or, you can configure it to be collected as frequently as 15-minute intervals.
- **Uploading scout health check information:** The Device Scout Monitor runs as a scheduled Windows task to check the health of the Device Scout and its ability to communicate. It tracks the successful completion of scout activities such as discoveries, status collections, and configuration updates. It uploads this information on a configured basis, once per day.
- **Cloud connection:** The communication channel between the Device Scout and the cloud is kept alive by means of a server-initiated ping. This request occurs approximately once per minute and consists of a small packet of bytes.
- **Logging into a secure printer via username/password entry:** The Device Scout controls the configuration settings on integrated printers. When a user logs into a secure printer via username/password entry, the solution will attempt to authenticate locally with Active Directory. The printer then retrieves and decrypts a document list from the cloud. Documents are then delivered to the device by a Print Scout.
- **SNMP device discovery:** The Device Scout performs SNMP scans to discover new printing devices on a configured network segment. Some network monitoring tools may treat SNMP scans as sources of network congestion. We recommend registering the

Device Scout with your network security office so that they know to expect this network traffic.

- You can configure the Device Scout to exclude certain subnets or IP addresses, restrict its scans to certain times of the day, and reduce network utilization to a specific level.
- **Scout configuration data:** The Device Scout retrieves its configuration data by initiating an outgoing secure HTTPS connection to the scout control server. When the configuration has been received, the Device Scout terminates the connection and operates without any outgoing connections until the next scheduled configuration check.
- **Automatic scout updates:** From time to time, a new version of the Device Scout will be released with updated functionality and any bug fixes. By default, the Device Scout will check for new versions of itself daily. If a new version is available, the scout will automatically download and install the new version. Based on your organization's preferences, you can easily control this setting; you can set it to Notify, Off, or Automatic (the default).

INTERNET TRAFFIC

The following table provides details and guidance on the Internet traffic required by Sentry Print. The number of documents per user per month is intended as an example only. Data consumption can be tailored depending on whether cloud-based document storage is required.

Monthly Internet Traffic Per User

Scenario	Cloud Storage? No	Yes	
Number of secure documents[1]	5/day	5/day	
Average document size[2]	0.5 MB	0.5 MB	
Cloud document storage	No	Yes	
Print Document information			
Transmission per document			
Document metadata	0.002 MB	0.002 MB	
Document contents[3]	0.000 MB	0.550 MB	
Job metadata for reporting	0.003 MB	0.003 MB	
Transmission per document	0.005 MB	0.555 MB	
Documents per user (example only)	152/month	152/month	
Data transmitted per month	**0.760 MB**	**84.406 MB**	
Workstation connection			
Keep-alive packet per minute	0.0001 MB	0.0001 MB	
Connection data month	**3.241 MB**	**3.241 MB**	
Other data transmission			
Print Scout daily status, AD look-ups	0.004 MB	0.004 MB	
Device Scout daily device meters	0.005 MB	0.005 MB	
Other data transmission daily total	0.009 MB	0.009 MB	
Other data transmission / month	**0.274 MB**	**0.274 MB**	
Total Internet bandwidth	**4.28 MB**	**87.92 MB**	**per user, per month**

Assumptions

The guidance on traffic volume is based on the following:

1. An average of 5 secure documents printed per day, per user.
2. Document size can vary based on the nature of the documents printed. Calculations are based on an average document size of 500KB.
3. For cloud document storage, the solution will first attempt to retrieve the document from the user's workstation. We assume that 10% of the time, the user's workstation may not be available (e.g. in sleep mode or offline). In this case, documents are retrieved from the cloud.

Examples

Scenario 1:
Organization with 500 users storing documents in the cloud

Traffic per user: 87.92 MB per month

Total traffic: 500 x 87.92MB = **43.96 GB per month**

Scenario 2:
Organization with 1000 users not storing documents in the cloud

Traffic per user: 4.28 MB per month

Total traffic: 1,000 x 4.28MB = **4.28 GB per month**

REFERENCES

[1] "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019," https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g