PHAROS

DATA SECURITY

Pharos Beacon® 1.0

TABLE OF CONTENTS

BEACON OVERVIEW

Beacon is a multi-vendor print management platform in the cloud that gives you a complete view of your organization's print environment, on demand. Beacon gives you clarity and control. It reveals the true cost of your printing and provides the decision support you need to reduce costs and improve end-user convenience.

BEACON FLEET MANAGER

Provides a comprehensive, multi-vendor view of print from all devices and reveals volume, service, and operating cost information to help you build and maintain a more efficient fleet.

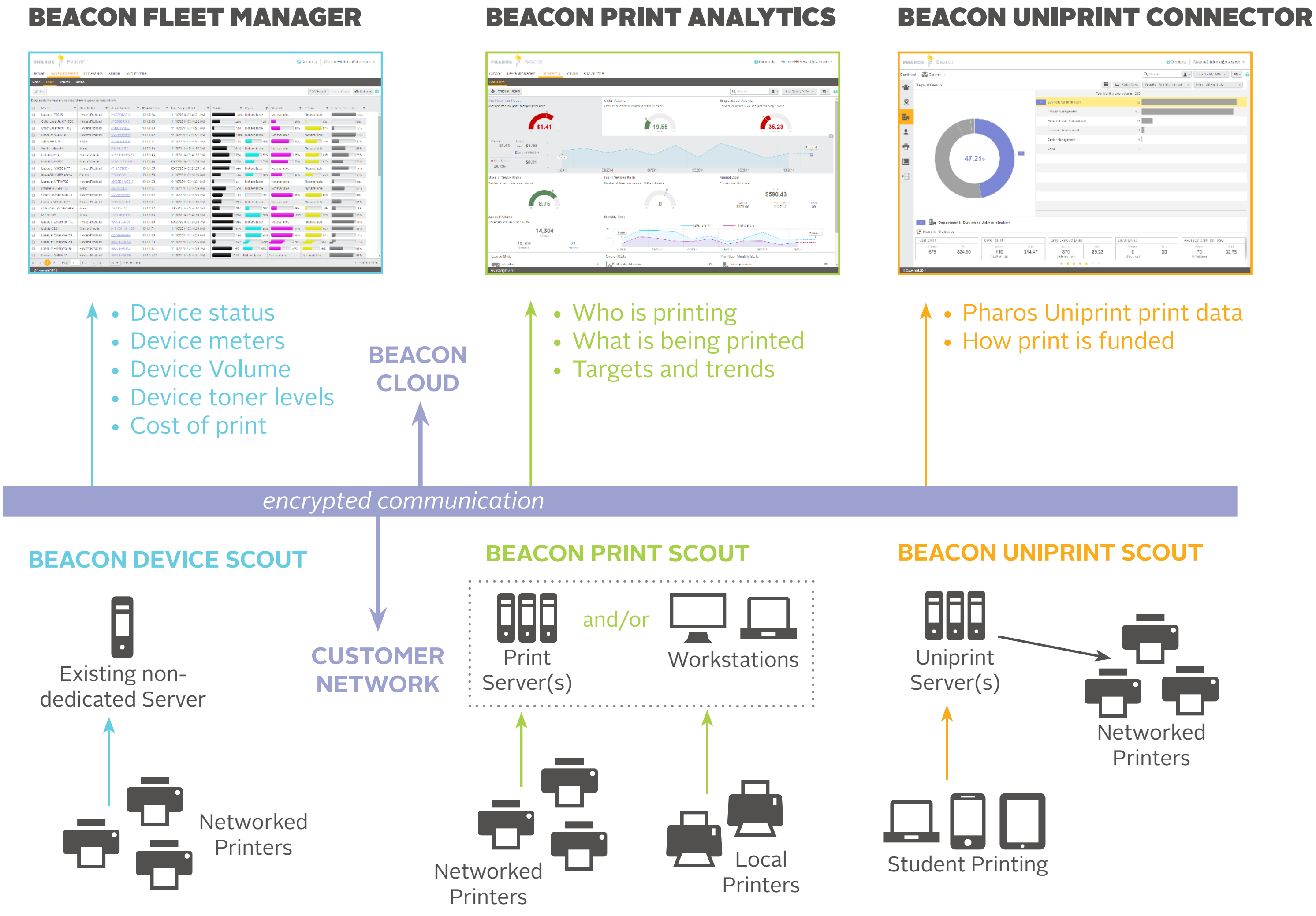
BEACON PRINT ANALYTICS

Reveals how print is created in your environment, including information about the user, the application, the device, and comprehensive output parameters. It reveals opportunities to reduce costs and waste, and it helps you to discover the fleet design that best supports your people.

BEACON UNIPRINT CONNECTOR

Allows you to view how print was funded by sharing information with Uniprint (version 8.4 and higher). It reveals the cost of print for both the back office and all student print environments managed by Uniprint.

BEACON OVERVIEW



BEACON FLEET MANAGER

- Device status
- Device meters
- Device Volume
- Device toner levels
- Cost of print

BEACON PRINT ANALYTICS

- Who is printing
- What is being printed
- Targets and trends

BEACON UNIPRINT CONNECTOR

- Pharos Uniprint print data
- How print is funded

BEACON CLOUD

encrypted communication

CUSTOMER NETWORK

BEACON DEVICE SCOUT

Existing non-dedicated Server

Networked Printers

BEACON PRINT SCOUT

Print Server(s) and/or Workstations

Networked Printers

Local Printers

BEACON UNIPRINT SCOUT

Uniprint Server(s)

Networked Printers

Student Printing

INTENDED USE

Security is essential to everything we do. Pharos is committed to providing software products that are secure for use in all network environments. To perform its intended functions, Beacon will scan, collect, and store information about your print environment, your users, and your print jobs. Beacon also gives you control over what data is collected and who can see it. This document outlines the architecture, polices, and safeguards in place to keep your information secure.

YOUR NETWORK

To take full advantage of the Beacon platform, you will need to install certain components in your local area network. Depending on your requirements and licensing, these components may include:

- Device Scout
- Print Scout
- Uniprint Scout

In some cases, multiple scouts of each type may be installed.

No device or print information can be transmitted to Beacon until one or more scouts are installed and the scouts are activated with a registration key. If your registration key is ever invalidated or deleted from Beacon, no further device or print information will be collected, even if the print/device scouts remain installed.

At any time, you may stop any Pharos scout from collecting information by uninstalling each scout using the Add/Remove Programs feature in the Windows control panel. Instructions on how to uninstall the scouts can be found in the application installation document.

YOUR NETWORK

Beacon Device Scout

The Beacon Device Scout finds all printers within your network and collects data on device status, meters, and consumables for use in Beacon's Fleet Manager views. The Device Scout will attempt to collect the following 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 identification
- Location
- Display reading
- MAC address
- Device status
- Manufacturer
- Model number
- Error codes
- Toner levels
- Firmware Version/ Patch Level

NOT ALL DEVICES WILL REPORT EVERY ATTRIBUTE.

YOUR NETWORK

Beacon Print Scout

The Beacon Print Scout can be deployed to print servers and or workstations (PC and MAC) to collect comprehensive information on how print is being created within the organization.

Print Scouts on print servers collect information on network printers and multi-function devices while Print Scouts deployed to workstations collect data on both network printing and any printing sent to locally attached devices. The Print Scout collects the following types of data:

- Information about the user from Active Directory
- Information from the printing device via SNMP
- Information about the print job via print stream analysis.

Beacon Print Scout *(continued...)*

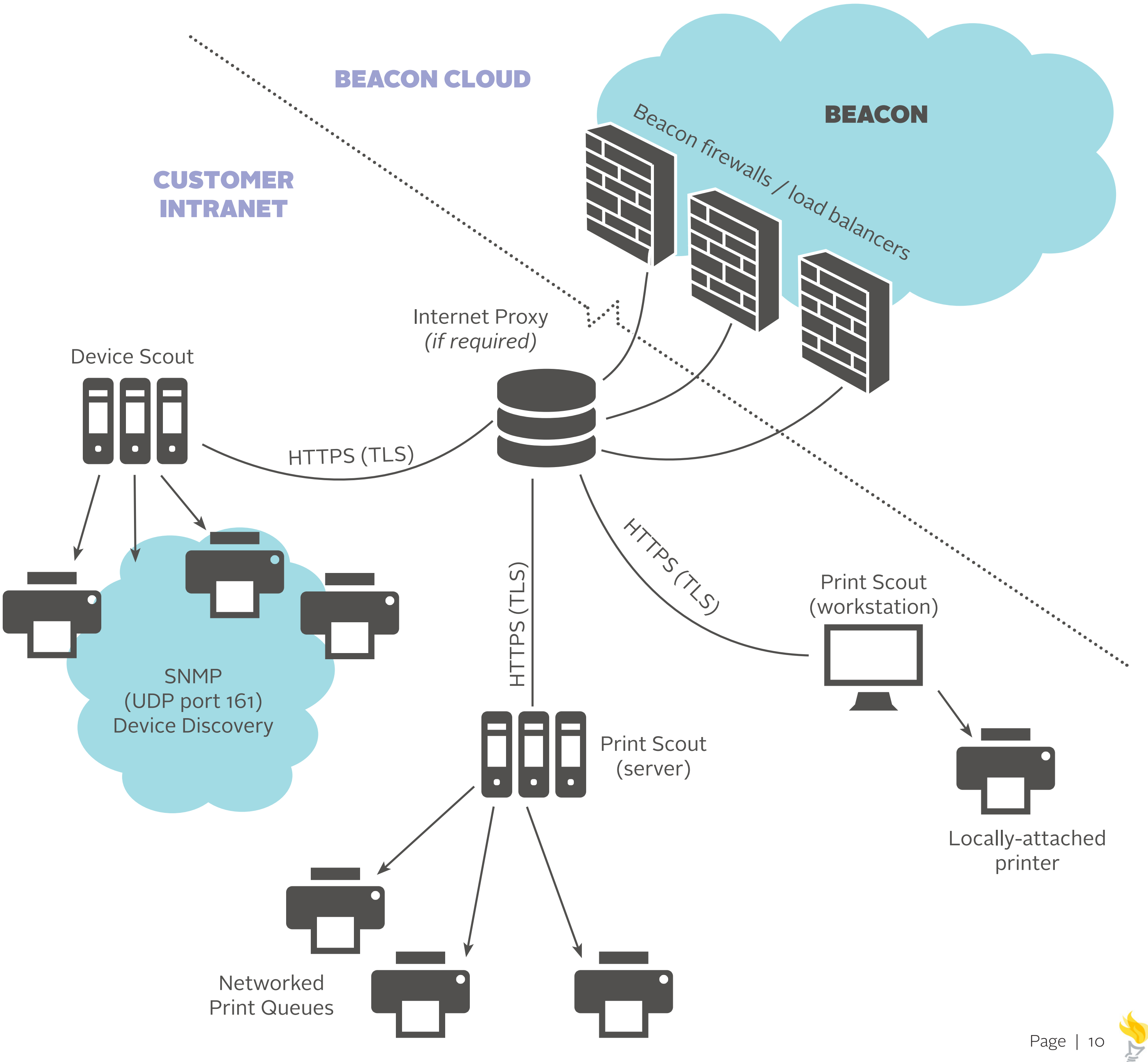
You can control what data is collected and who can see it. You can configure the Print Scout's collection settings to disable the collection of certain types of data and obfuscate certain data if you need to maintain individual privacy. You can also apply role-based viewing restrictions, giving some Beacon users a limited view of the data.

Beacon Uniprint Scout

The Beacon Uniprint Scout can be deployed for Uniprint customers (version 8.4 and higher). The Beacon Uniprint Scout collects data from Uniprint printing activities; this data can be viewed and filtered in a variety of ways within the Beacon Print Analytics dashboards.

BEACON DEPLOYMENT ARCHITECTURE

The Print Scout and the Device Scout may be deployed in the same environment. Depending on your network topology and print environment, you may have multiple print scouts and device scouts. One of each is shown here for simplicity.



BEACON DEPLOYMENT ARCHITECTURE

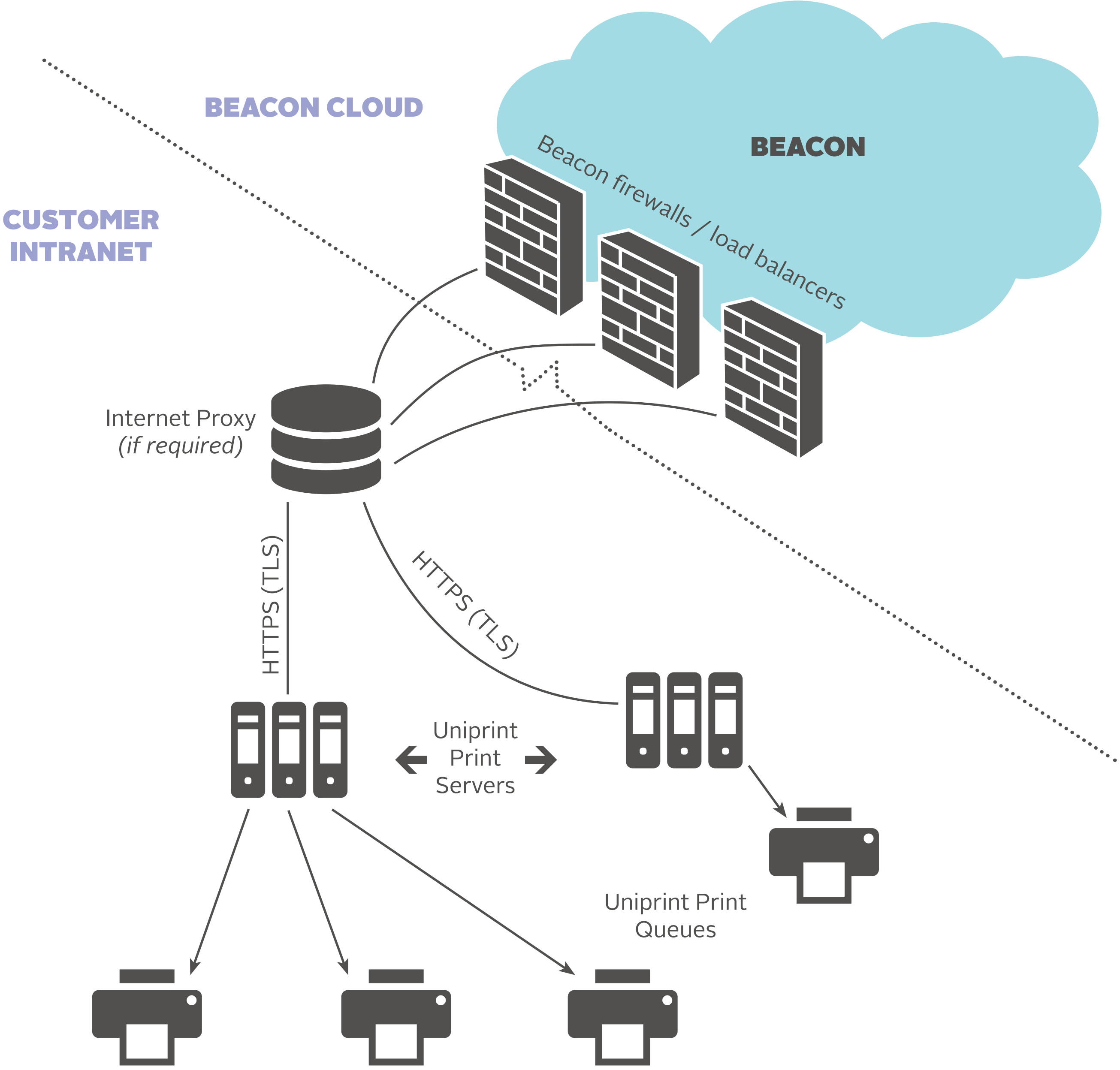
The Device Scout registers itself via an HTTPS(TLS) connection to Beacon. Once the Device Scout has registered and obtained a copy of its configuration, it disconnects from Beacon and operates autonomously until the next configured check-in time.

The Print Scout also registers itself via an HTTPS(TLS) connection to Beacon. The Print Scout behaves slightly differently than the Device Scout in that it will upload job data as it is captured.

The Uniprint Scout will also register itself via an HTTPS(TLS) connection to Beacon. The Uniprint Scout behaves similarly to the Print Scout except that it will attach to Uniprint print queues and report job information to Beacon.

Beacon scouts do not listen for incoming connections and do not open any server ports. Once installed and configured, both scouts will initiate network connections in accordance with their configuration settings.

BEACON DEPLOYMENT ARCHITECTURE



The integrity of customer data is critical. Pharos uses a combination of technological and procedural controls to restrict access to customer data.

DATA PROTECTION

Types of Threats We Address

1 MACHINE OR TECHNOLOGICAL FAILURE

Such an event could include power loss, network connectivity loss, or data storage failure. Pharos Beacon uses a cloud-based infrastructure with a minimum of three geographic zones. The Beacon cloud infrastructure can detect a variety of fault conditions and remove or fix defective components on the fly with no interruption of service.

2 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. Pharos Beacon encrypts all external connections using SSL or TLS at the highest level supported by the connecting browser. All application components are isolated by function; only necessary traffic can pass between components.

3 PASSIVE DATA LOSS OR CORRUPTION

These losses could be caused by software defects, incompatibilities between software components, or data storage loss. The Beacon cloud infrastructure mitigates these risks through a formal software quality assurance methodology. In the event of a data corruption problem, Pharos maintains pre-state backups in order to roll back any data-altering changes. Pharos 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.

SECURITY IS A SHARED RESPONSIBILITY

As a Beacon customer, you also share the responsibility to protect your data.

1. Ensure that all scouts are accessible to authorized users only.

2. Ensure that the server is fully patched and meets all other security requirements of your organization.

   a. Ensure that the server is regularly maintained according to the policies of your organization.

   b. Ensure that the minimum necessary credentials are granted to individuals within your organization who require access to the server(s) to perform their job functions.

3. If the Print/Device/Uniprint 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 Pharos technical support before installing.

NETWORK UTILIZATION

Beacon Device Scout

Beacon requires access to your local area network to operate effectively. The following section describes how Beacon will interact with your environment.

The Beacon Device Scout will generate local network traffic when performing the following operations:

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

The Device Scout uses SNMPv1 and SNMPv2 to communicate with local network devices. The Device Scout will also collect the same information from SNMPv3 compatible devices as long as they provide support for SNMPv1 and SNMPv2. 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.

NOTE:
The Device Scout does not record or track SNMP-enabled devices within its scanning range that do not report themselves as output devices.

Beacon Device Scout *(continued)*

The Beacon Device Scout will generate outgoing network traffic when performing the following operations:

- Registering a new scout
- Polling the scout control server for new configuration or instructions
- Uploading discovered device data to Beacon
- Uploading device meter data to Beacon
- Uploading scout health check information to Beacon

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

By default, new device scouts will validate the SSL certificate of the Beacon server endpoint to which they connect. If the validation fails, the device scout will not connect. An administrator can override this setting via the Device Scout Configuration utility if your organization routes outgoing traffic through an SSL proxy or other means of content inspection.

Beacon Device Scout *(continued)*

Here are average payload sizes for the various scout operations:

DEVICE SCOUT NETWORK TRAFFIC SUMMARY		
TASK TYPE	DEVICE TYPE	NETWORK TRAFFIC *(in bytes)*
Discovery	Device	15882
Usage	Non-Device	126
Usage	Device	16621
Status	Device	1960
Integration	Device	3000

Note that 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 IP ranges that are not likely to contain output devices.**

NETWORK UTILIZATION

Scout Communication Patterns

1 REGISTERING A SCOUT

When the scout is first installed, it will include a unique registration code that identifies the scout to Beacon. This registration code is unique to every device scout install; do not re-use or share the registration code. The scout will attempt to open a secure HTTPS connection to Beacon and identify itself using the registration code. If the code is valid, the scout will receive a set of configuration instructions.

2 POLLING THE SCOUT CONTROL SERVER

Upon initial registration, and periodically during normal operation, the 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.

3 UPLOADING DISCOVERED DEVICE DATA

The Device Scout will upload discovered devices once per period, configured within the application. This period can be as frequent as once per hour or once every 48 hours. More frequent uploads will result in newly discovered devices showing up within the application more quickly, but will result in more network traffic.

NETWORK UTILIZATION

Scout Communication Patterns *(continued)*

4 UPLOADING DEVICE METER DATA

The Device Scout will upload meter reads to the scout control server on a scheduled basis, which can be as frequent as once per hour or once every 48 hours. This setting is configurable within the Beacon application. More frequent uploading of meter reads will result in more up-to-date information available within the Beacon application, but will result in more network traffic.

5 UPLOADING SCOUT HEALTH CHECK INFORMATION

The Device Scout Monitor runs as a scheduled Windows task to check the health of the scout and its ability to communicate with Beacon. It tracks the successful completion of scout activities such as discoveries, status collections, and configuration updates. It uploads information about the health of the scout on a configured basis (as frequently as once every 12 hours or as infrequently as once every 48 hours). More frequent updates will allow problems with the scout to be detected earlier, while less frequent updates will result in less network activity.

NETWORK UTILIZATION

SNMP Device Discovery

The Beacon Device Scout uses SNMP scanning to discover new printing devices on a configured network segment. Some network monitoring tools may treat SNMP scans as sources of network congestion. Pharos recommends registering the Beacon Device Scout with your network security office so that they know to expect certain traffic from the scout.

The scout can be configured to exclude certain subnets or IP addresses, restrict its discovery activities to certain times of the day, or reduce network utilization to a specified level.

SNMP Device Discovery *(continued)*

SCOUT BEHAVIOR

The Beacon Device Scout retrieves its configuration data by initiating an outgoing secured 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.

Additionally, the Device Scout will only communicate with output devices when configured to do so, and does not hold open continuous data connections. The Beacon Device Scout also does not open server ports while operating.

AUTOMATIC SCOUT UPDATES

From time to time, a new version of the Beacon Device Scout will be released containing updated functionality and any bug fixes. You can configure the scout to update automatically. When this feature is enabled, 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 download the newer version and install it. Based on customer preferences, this setting can be easily enabled or disabled.

NETWORK UTILIZATION

Beacon Print Scout

The Beacon Print Scout uploads print job information as it occurs. The Print Scout does not perform network-wide discoveries; it will only know about the printers connected to the local machine or printers having print queues on the local machine.

PRINT SCOUT NETWORK TRAFFIC SUMMARY		
TASK TYPE	**FREQUENCY**	**NETWORK TRAFFIC** *(in bytes)*
AD lookups	once per day, per print user	Depends on size of average AD record
Status	1x24hrs	2kB
Print Job Uploads	On print	3kB
Device SNMP lookup	On print	2.5kB

1 PRINT SCOUT STATUS CHECKS

The Print Scout checks in with Beacon once per day to upload its health report and check for new settings. This check is under 2kB and in most cases will return an empty response if there have been no configuration changes. The Print Scout will also check for configuration changes when each job is uploaded.

NETWORK UTILIZATION

Beacon Print Scout *(continued)*

2 ACTIVE DIRECTORY LOOKUPS

When a user prints, the Print Scout will lookup Active Directory (AD) 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. However, the maximum traffic AD lookups can generate would be the total number of unique AD users times the average AD record size. The Mac Print Scout does not lookup user information in Active Directory.

3 DEVICE SNMP LOOKUP

The Print Scout will attempt to verify output device information via SNMP when a job is processed. The SNMP lookup will occur only once per day. It is a small subset of data that the Device Scout collects, and averages 2.5kB per device.

4 PRINT JOB UPLOADS

The bulk of network traffic will be job data sent to the Beacon server. This data is highly variable because of the strings involved (printer name, driver name, user details, SNMP details, etc.). A good approximation is 2.5-3kB per job.

NETWORK UTILIZATION

Beacon Uniprint Scout

The Uniprint Scout will upload Uniprint job data as it passes through a Uniprint print queue. The network activity pattern is very similar to the Print Scout:

UNIPRINT SCOUT NETWORK TRAFFIC SUMMARY		
TASK TYPE	**FREQUENCY**	**NETWORK TRAFFIC** *(in bytes)*
Uniprint user lookup	On print	Depends on average user record size in the Uniprint database
Scout Status	1x24hrs	2kB
Uniprint Job Uploads	On print	3kB
Device SNMP lookup	Once per day, per device	2.5kB

NETWORK UTILIZATION

Beacon Uniprint Scout *(continued)*

1 UNIPRINT SCOUT STATUS CHECKS

The Uniprint Scout will check in with Beacon once per day to upload its health report and check for any new settings. This check is under 2kB and in most cases will return an empty response if there have been no configuration changes. The Uniprint Scout will also check for configuration changes when each job is uploaded.

2 DEVICE SNMP LOOKUP

The Uniprint Scout will attempt to verify output device information via SNMP when a job is processed. The SNMP lookup will occur only once per day. It is a small subset of data that the Device Scout collects, and averages 2.5kB per device.

3 UNIPRINT JOB UPLOADS

The bulk of network traffic is the Uniprint job data being sent to the Beacon server. This data is highly variable because of the strings involved (printer name, user details, etc.). A good approximation is 2.5-3kB per job.

CLOUD ARCHITECTURE

Beacon runs in the Pharos cloud to deliver a safe and scalable application experience. Pharos exclusively uses Infrastructure-as-a-Service (IaaS) providers that have achieved a SSAE 16 audit and ISO 27001 security certification covering all IaaS infrastructure and facilities. Additionally, Beacon uses a tiered application structure to isolate data within the cloud.

CLOUD ARCHITECTURE

Infrastructure Security

Pharos conducts periodic vulnerability assessments in all production environments. Access to production environments is restricted based on business need. Access roles are configured using Segregation of Duties (SOD) principles. System access levels are periodically reviewed and adjusted when necessary.

All production operating system and framework components are patched during predetermined maintenance windows. Pharos uses generally accepted guidelines for deploying new operating system and framework updates in a test environment before promoting to production.

Pharos monitors all vendor service bulletins for zero-day vulnerabilities and has processes in place for emergency patching should the need arise.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

Federal Information Security Management Act (FISMA) compliance is not affected by the use of Beacon. Pharos Beacon is not intended to be part of an internal control system for FISMA, and will not interfere with these controls.

The use of Pharos Beacon will not have an impact on compliance with the Federal Information Security Management Act (FISMA) for covered entities. Beacon does not collect, house, or transmit any information regarding the content of print jobs, thus has no way of accessing, housing, or transmitting high risk information, even if this information is printed or otherwise sent to print devices monitored by Pharos Beacon.

For more information about the Federal Information Security Management Act, visit http://csrc.nist.gov/groups/SMA/fisma/index.html

GRAMM-LEACH-BLILEY ACT (GLBA)

The use of Pharos Beacon will not have an impact on compliance with the Gramm-Leach-Bliley Act (GLBA) for covered entities. This is because Pharos Beacon does not collect, house, or transmit any information regarding the content of print jobs, and thus has no way of accessing, housing, or transmitting customers' personal financial information, even if this information is printed or otherwise sent to print devices monitored by Pharos Beacon.

For more information about the Gramm-Leach-Bliley Act, visit http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)

The use of Pharos Beacon will not have an impact on compliance with the Health Insurance Portability & Accountability Act (HIPAA) for covered entities. This is because Pharos Beacon does not collect, house, or transmit any information regarding the content of print jobs, and thus has no way of accessing, housing, or transmitting electronic protected health information (ePHI) as defined by HIPAA.

For more information about HIPAA, visit http://www.hhs.gov/ocr/hipaa/

SARBANES-OXLEY

Pharos Beacon is not intended to be used as part of an internal control structure as outlined in Section 404: Management Assessment of Internal Controls, and will not interfere with these controls.

Information Technology controls are an important part of compliance with Sarbanes-Oxley. Under this Act, corporate executives become responsible for establishing, evaluating, and monitoring the effectiveness of internal control over financial reporting. There are IT systems in the market that are designed specifically for meeting these objectives. Pharos Beacon is not designed as an IT control system, and will not interfere or put at risk other systems that are intended for that purpose.

For more information about Sarbanes-Oxley, visit
http://thecaq.aicpa.org/Resources/Sarbanes+Oxley