SiteAudit Technical Article

SiteAudit Hosted Security WP

In This Article:

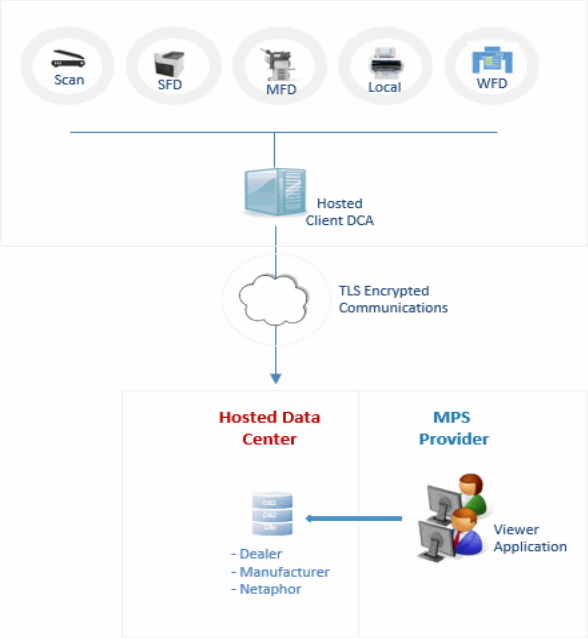
January 2023

Netaphor SiteAudit Hosted™

SiteAudit Hosted is an MPS application for remotely collecting local and networked printer data. It employs a Hosted Client (data collection agent--DCA) that runs at the customer and a viewer(s) that runs at the MPS provider. Data is collected at the customer site and sent via secure transport to a server and stored in a SQL database. It provides a secure and easy way for MPS providers to collect and manage counts, supplies, errors, and printer information.

Security Overview

SiteAudit Hosted Setup



MPS Operations	User Applications
• Discovery Configuration	• Control Panel
• Filtering and Analysis	• Dashboard
• Reporting & Scheduling	• Visualizer
• Alerting Configuration	• Analyzer

Customer Location – Hosted Client (DCA)

Deployment – Data Collection Agent (DCA)

- 64-bit Windows 10/11 or Server 2016, 2019, 2022
- .NET 4.8+ or later
- SiteAudit Hosted Client (DCA)

Discovery and Data Collection

- Discovery SNMP v1/v2c/v3
- Data collection protocols SNMP, HTTP, NPAP, CPCA, WMI; local administrator account for local printers
- Ports scanned: 161, 1650, 9100, 80, 8080, 631, 9300, 47545, 21, 23

Data Transport to Hosted Server

- TCP port 443 – over HTTPS

MPS Provider – SiteAudit Control Panel/Viewer

Deployment – SiteAudit Control Panel

- 32-bit or 64-bit Win10/11 or Server 2016, 2019, 2022
- .NET 4.8+ or later
- SiteAudit Control Panel
- Azure AD Account to access Server

Control Panel Connection to Hosted Server

- TCP port 443 – REST over HTTPS
- SA Hosted Administrator or Viewer license

Security and the Development Process

Netaphor offers, in conjunction with a partner, a FedRAMP authorized (fedramp.gov) service. The version of SiteAudit Hosted that is used in this FedRAMP authorized is the identical to SiteAudit Hosted available to commercial non-governmental users.

To attain this FedRAMP authorization Netaphor is required to follow a Software Development Lifecyle (SDLC) where security is at the core of the SDLC. This includes restricting who has access to see or modify the source code, how design and code changes are reviewed and committed, the testing process, source code analysis, constant vulnerability testing and periodic penetration tests by a 3rd party and review of a Software Bill of Materials to ensure any 3rd party components will not be an issue. Much of the process is automated and run daily to ensure that issues can be caught as and when code changes are made.

Security vulnerabilities are also mitigated per an SLA – 30 days for high, 90 for moderate and 120 for low.

Data Communication

The SiteAudit Hosted Client (DCA) is a data collector. All communication is encrypted prior to transmission to the cloud-based server. Asymmetric encryption is used and is certified with a minimum 4096 Bit SSL Certificate from a trusted Certificate Authority (CA) such as DigiCert™ or VeriSign® (Symantec) for all communication with the Hosted server. Data transmission is via REST.

The MPS Provider uses the SiteAudit Control Panel/Viewer to connect to the data for the customer, stored in a hosted database. They can only do this if they have a properly licensed Control Panel and an Azure AD account with access to the server and the specific end customer's data.

Hosted Client (DCA) Activation

Hosted Client activation is managed by the Netaphor Hosted Server application. Prior to installation a single use installation URL is created and provide to the person performing the installation. This is then used to install the Hosted Client (DCA).

The application uses a REST transport for data communication with the server and all communication to the server is encrypted using TLS 1.2 (or better). If the DCA needs to be reinstalled on a different machine a new DCA installation URL must be requested. The Hosted Client (DCA) does not provide access to the name of the customer database, the username, or the password.

Discovery and Data Collection

SiteAudit performs a discovery using SNMP. The discovery allows both inclusion and exclusion of IP addresses. Discovery over SNMP v1/v2c/v3

- each included network, range, static IP on the list determines the addresses in that list
- each excluded network, range, static IP determine if any of these addresses are excluded
- IPv4 and IPv6 addresses are supported

SiteAudit scans the following ports to find printers:

- 161 SNMP to see if SNMP is enabled.
- SNMP is used to collect data
- 80 & 8080 HTTP to see if there is an embedded web server. HTTP is used to collect data
- 9100 Print protocol for printers, used to collect data
- 1650 Same as 9100
- 631 IPP print protocol, used to collect data.
- 135 RPC, used to detect a Windows host for local printers
- 47545 (CPCA) and 9300 (NPAP) may also be used if the printer supports those protocols
- Ports 21 (FTP) and 23 (Telnet) to identify potential security vulnerability

To minimize network traffic data is collected by type and in configurable intervals. Read more about discovery and data collection at https://support.netaphor.com/index.php?/article/AA-00594
Read about DNS discovery https://support.netaphor.com/index.php?/article/AA-00391/0/

Network Traffic

SiteAudit data collection can be characterized as a *slow, steady receipt of packets*. This results in a smaller percent of the network bandwidth being used. Network traffic is dependent on the number of devices that SiteAudit is monitoring. Below are examples of the amount of network traffic is used by three different fleet sizes: 250, 1,000 and 10,000 printers.

Traffic estimates are based on a typical environment, but results may vary depending on mix of local and networked printers, number of counters, address spacing, number of IP addresses and other factors.

Number of Printers	% Usage in 100 MB Network	% Usage in GB Network
250	0.003	0.000293
1000	0.001	0.000977
10000	0.103	0.010058594

Read more about network traffic at https://support.netaphor.com/index.php?/article/AA-00594

Data Collected

Data collected consists of printer asset information, counters, supplies and error information. A sample of the collected data is listed below.

Asset Information	**Supplies**	**Counters**
Manufacturer	Supplies Remaining Level %	Total Pages
Model	Original Supply Level	B/W All
IP Address	Percentage of Supplies Used	B/W Print
Printer Name	Date Toner Detected	B/W Copy
Product Number	Replaced On Date	B/W Large
Serial Number	Supplies Description	Color All
Asset Tag	Supplies Type	Color Print
Location	Supplies Part Number	Color Copy
Printer MAC Address	Supplies Serial Number	Color Large
Host MAC Address	Supplies Installation Date	Large
		Small
Errors	**Errors (continued)**	Copied
Alert Code	Service Level Agreement Name	Print
Severity Level	Contact	Fax
Training Level	Total Errors	Scanned
State	Uptime %	
Resolution Status	Last Successful Communication	
Incident Description	Last Notified	
Incident Duration	Device Status (Ready/Error/Warning)	
Incident Start & End	Response Time	

There is no credit card or personal data stored. Job data may be collected if SiteAudit is configured to collect this information. By default, this feature is disabled. Local administrator credentials with access to the target workstations is required to configure this feature. For a complete list of data see https://support.netaphor.com/index.php?/article/AA-00779/104/

Credentials

SiteAudit requires credentials in the following instances:

- For logging into the SiteAudit Control Panel – an Azure AD account will be required to access the Control Panel and the Hosted data. Policies of the AD to which the account belongs are enforced during the login process (e.g., MFA)
- For directly connected printer discovery, Windows administrator credentials for the hosts with attached printers (required by DCA and entered on machine where DCA is installed)
- Direct printer discovery using WMI requires an account that has full permissions for the ROOT WMI namespace (required by DCA and entered on machine where DCA is installed)
- For SNMPv3 discovery (required by DCA and entered on machine where DCA is installed)

SiteAudit stores all passwords in Windows Protected Storage and can only be decrypted on the machine where they were entered. If the DCA is moved to a new machine, these passwords must be

Common Questions about Data Collection

- Device Data Collection: Only device data is collected. User information is not collected from a device. Information, such as user accounts on the device for Follow Me Printing or secure print or the list of jobs on devices, is not collected

- No Personally Identifiable Information (PII) such as user passwords, credit card information, SSN etc. are collected or stored by SiteAudit

- Job Data collection is optional. This data is collected from the Windows Spooler but must be enabled by the user to allow this. It is disabled by default.

- External Communication – outside the firewall: This is under control of the customer. The only external communication is via notification email or scheduled reports. The customer can control which notifications are sent and to whom. The same is true for scheduled reports

Summary

By using TLS1.2 transport mechanisms and secure hosted servers certified by trusted CAs the appropriate security mechanism are used by the SiteAudit Hosted architecture to ensure printer data is protected.

Netaphor Software Inc.

SiteAudit Hosted was launched in October 2011 and is sold to customers in over 50 countries.

Founded in 1997 and headquartered in Irvine, Calif., Netaphor Software, Inc. (www.netaphor.com) develops and sells asset management tools that help companies control printer costs and improve service. The company's flagship product, SiteAudit, is the leading software solution in the Mid-Market & Enterprise spaces to identify and manage costs and service saving organizations up to 30 percent during the printer asset lifecycle. Netaphor SiteAudit 5.0, 6.0 and 7.0 are the winners of the Buyers Lab (BLI) "Pick" award as Outstanding Fleet Management Solution by the editors at BLI analysts.