marco
Technology Made Clear.

PRINT AWARE

Security and Vendor Onboarding

- MANAGED SERVICES
- BUSINESS IT SERVICES
- CYBERSECURITY
- COPIERS & PRINTERS

800.847.3098
MARCONET.COM

Security and Vendor Onboarding

This document provides comprehensive technical, security, and compliance information for IT and vendor onboarding reviews — prepared proactively so your team has answers before the questions are asked.

Product Overview

Marco Print Aware is a managed print services monitoring platform. Print Aware installs a lightweight Data Collection Agent (DCA) on servers, workstations, or on a dedicated hardware appliance within the customer network to silently collect printer meter data, toner levels, and device health, without capturing any printed content.

How It Works

1. Install Agent — The agent is installed on 1 or more Windows, Mac OS, or Linux systems installed inside the customer network – no inbound ports are required through a company firewall.
2. Devices discovered via SNMP — Agent uses SNMP (port 161) to discover all printers on configured internal network segments.
3. Meter data collected — ~10 KB per device per collection cycle. Fully configurable frequency.
4. Encrypted upload to cloud — All data encrypted in-transit (TLS 1.2+) and at-rest in U.S.-based hyperscaler datacenters.
5. Alerts & reports generated — Proactive toner alerts, meter reports, and billing data available via web dashboard.

Data Classification Summary

Data Collected	Never Collected
✓ Page counts (print / copy / scan / fax)	× Printed, scanned, copied, or faxed document content
✓ Toner & supply levels	× Patient health information (PHI) of any kind
✓ Device model, serial number, MAC address	× Protected Health Information (HIPAA-covered data)
✓ Device firmware version	× Personally identifiable information (PII)
✓ Internal IP address (for device identification)	× Payment card information (PCI)
✓ Device service alerts	× Financial reports or transaction data (SOX scope)
✓ Encrypted metadata	× User credentials, passwords, or access tokens
	× Files or documents stored on the host machine
	× Email content or communication data
	× Browser history or web activity

Architecture and Hosting

Marco Print Aware is a SaaS platform securely hosted in the cloud. The Data Collection Agent (DCA) is installed within the customer's network and communicates outbound only, no inbound ports or firewall exceptions are required on the customer side.

Component	Details
Hosting provider	Hosting is localized to the geography of the client – Example: US clients connect to US hyperscale datacenter locations (ex. AWS, Azure, and GCP)
Data residency	Data is localized to the geography of the client – Example: United States clients data stays in the US
Deployment model	Multi-tenant SaaS — managed, owned, and operated by Marco Technologies LLC
Inbound ports required	None — all traffic is outbound from the agent installed in the customer network
Outbound port	443 (HTTPS), 7000 (TCP)
Web dashboard access	Browser-based (ex. Chrome) — available at https://portal.marconet.com
Authentication	SSO via Microsoft EntraID | Validated email / password + MFA
Data encryption	TLS 1.2+ in transit, AES-256 at rest

Network Requirements

> **✓ No inbound ports or firewall rules required. All traffic is outbound from the customer network only.**

The following domains should be whitelisted to ensure full platform functionality. The recommended approach is to allow the entire *.printaware.marconet.com domain.

Domain	Protocol	Port	Purpose
dcam.printaware.marconet.com	gRPC / HTTP/2	443	Agent jobs, meter uploads, alerts
csr.printaware.marconet.com	gRPC / HTTP/2	443	Agent authentication and registration
hc.printaware.marconet.com	HTTPS	443	Agent health status reporting
cdn.printaware.marconet.com	HTTPS	443	Agent self-update / auto-upgrade
remotetechnician.printaware.marconet.com	Proprietary	7000	Remote Technician (enabled by default; opt-out available — see note below)

Notes:

✓ Internal SNMP traffic: The agent uses SNMP v1/v2/v3 on UDP port 161 to communicate with printers on the local network.

✓ Internal HTTP traffic: The agent uses HTTP/HTTPS to communicate with printers on the local network for services like remote panel or local web services.

✓ Remote Technician is enabled by default. Clients may opt out; opting out impacts remote support capabilities and associated SLA terms. Consult your Marco account representative if you have any questions.

Security and Compliance

HIPAA
Compliant
No PHI collected. Meter data only.

SOX
Compliant
No financial records accessed.

FISMA
Compliant
No increased risk to gov systems.

Security Control	Detail
Encryption in transit	All communication between the DCA and cloud uses TLS 1.2+ over HTTPS/gRPC. No unencrypted channels are used.
Encryption at rest	All data stored in the cloud platform is encrypted at-rest using AES-256 whole volume encryption.
Antivirus compatibility	Each Print Aware release is submitted to major AV vendors prior to public release. The DCA directory may need to be whitelisted in strict default-deny environments.
Admin rights (runtime)	No elevated permissions required for daily operations. Admin rights are required at installation only. Service runs as Local System account.
Virus scan support	Real-time and scheduled AV scans are fully supported. No conflicts with standard AV tooling. Exclusions may be required for the DCA directory.
Penetration testing	Conducted at minimum annually by a third party. Summary available under NDA upon request.
SOC 2 Type II	Marco Technologies SOC 2 Type II report is available under NDA upon request. Contact your Marco account representative.

Authentication and Access Control

Capability	Supported?	Detail
Single Sign-On (SSO)	✓ Yes	Supported via native Microsoft EntraID integration.
EntraID Directory Integration	✓ Yes	Native integration with Microsoft EntraID for authentication
Multi-Factor Authentication	✓ Yes	MFA enforced through the customer's Microsoft EntraID / identity provider. If leveraging local authentication, MFA is required by Marco.
Role-Based Access Control	✓ Yes	Platform supports role-based, discretionary, and mandatory access controls with separation of duties.
Account Lockout	✓ Yes	Handled by Microsoft EntraID / SSO provider; inherits customer's lockout policies. If leveraging local authentication, Lockout is done by Marco.
Password Management	Via SSO	Credentials managed entirely by Microsoft EntraID. No platform-side password storage. Local authentication is encrypted in platform.
Audit Log	✓ Yes	Platform logs change history including what changed, by whom, and when.
IP Filtering	✓ Yes	Platform supports IP-based allowlisting to restrict access to approved IP ranges.
Session Timeout	✓ Yes	Inactive sessions enforced per customer's identity provider configuration.
Admin Rights at Runtime	✗ No	No elevated permissions required for normal daily operations. Installation requires admin.

Data Classification

The table below provides the complete classification of data collected and transmitted by the Marco Print Aware agent versus data that is explicitly out of scope and never accessed.

Data Element	Collected / Transmitted	Classification
Printer metadata	Device make, model, location, and firmware	Operational — printer identity only
Serial number	Device-level hardware identifier	Operational — device tracking
Printer networking metadata	IP address, MAC address, and hostnames	Operational — local network identifiers only
Page/copy/scan/fax counts	Meter counter values only	Billing/operational data
Toner/supply levels	Percentage remaining per cartridge	Operational — proactive alerts

DATA THAT IS NEVER COLLECTED OR TRANSMITTED
✕ Printed, scanned, copied, or faxed document content
✕ Patient health information (PHI) of any kind
✕ Protected Health Information (HIPAA-covered data)
✕ Personally identifiable information (PII)
✕ Payment card information (PCI)
✕ Financial reports or transaction data (SOX scope)
✕ User credentials, passwords, or access tokens
✕ Files, documents, or data stored on the host machine
✕ Email content or communication data
✕ Browser history or web activity

System Requirements

Component	Minimum	Recommended (100+ devices)
Operating System	Windows (all active/supported versions), macOS, or Linux	Windows Server 2016 or newer
CPU	1 GHz × 2 Cores	3 GHz × 4 Cores
Memory (RAM)	2 GB	4 GB or more
Disk Space	2 GB HDD	10 GB SSD
Network	Outbound internet (see Section 3)	Outbound internet (see Section 3)
Java / .NET	Not required	Not required — fully self-contained
3rd Party Software	None required	None required
Browser (webadmin)	Chrome or Firefox (latest)	Chrome or Firefox (latest)

Deployment Notes:
✓ Silent / unattended installation supported
✓ Runs as a Windows service (Local System account) — no admin rights required after installation
✓ Does not require ActiveX, Java, .NET, Adobe Flash, or any other 3rd party runtime
✓ Not recommended on laptops or machines that frequently shut down (reliability impact)

Disaster Recovery and High Availability

RTO	RPO	DR Testing	DR Technology
12 hours Time to restore after full site loss	**1 hour** Maximum data loss window under DR scenario	**Annual** Full DR plan tested once per year	**Azure ASR** Azure Site Recovery — active/passive

High Availability Architecture
The SaaS platform uses redundant hardware and software within the cloud environment. Agent clustering is supported and requested for all environments.

Data Backup & Retention
Customer data is backed up on a rolling basis. Operational data is deleted upon customer request. A formal data retention policy governs backup/DR data lifecycle. No customer-side backup configuration is required.

No Customer DR Config Required
Print Aware does not require the customer to configure or maintain any DR infrastructure. All DR is managed at the platform and hosting layer by the platform.

Support and Operations

Marco Print Aware Support

Category	Details
Phone Support	800.847.3070
Hours	8:00 AM – 5:00 PM CT, Monday–Friday (excluding federal holidays)
Primary Contact	
Escalation Path	
Client SLA	Defined in the customer contract. Contact your Marco account representative.
Support Remote Access	Support teams use on-demand controlled remote access; no persistent inbound connection
SOC 2 Type II	Available under NDA upon request. Contact your Marco account representative.
Ticketing Integration	ServiceNow integration available through Marco Insights Platform

Change Control and Patch Management

Category	Details
Update mechanism	Self-updating agent. Updates pushed automatically when available.
Release schedule	No fixed schedule for point releases. Updates deployed when ready.
Customer notification	Agents auto-upgrade when a new version is available. Version updates and release notes are posted in the Print Aware portal.
Disabling auto-update	Auto-update can be disabled for controlled environments, but agents will not connect
Intune / SCCM deployment	Staged/at-will deployment via SCCM or Intune is supported.
3rd party patching	Vendor monitors and patches 3rd party dependencies.
Version history	Release notes are available in the Print Aware portal alongside each version update notification.

AI Tool Usage (Development): AI is used internally in the software development lifecycle. No customer data or PHI is used in AI tools. Customer data will not be used for model training or unsupervised learning.