



## **CloudPrinting Monitor (CPM): Captura de datos de los equipos de impresión**

### **Versatilidad, seguridad, rendimiento y transparencia**

CloudPrinting Suite permite recibir los datos de los equipos de varias formas:

- a) **TRAPS:** Si los dispositivos disponen de esta opción y está activada, Nubepriint recibirá y gestionará con esta información.
- b) **Otros sistemas de monitorización:** para facilitar la migración de clientes que están utilizando actualmente cualquier herramienta de monitorización. Nubepriint puede recibir los datos capturados e incorporarlos a su sistema para su gestión, igual que si los recibiera de su propio CPM.
- c) **CloudPrinting Monitor (CPM):** Software de captura de datos de Nubepriint:
  - o **Características de CPM:**
    - Se ejecuta en el cliente y no requiere instalación
    - Configurable y controlable por el cliente
    - Captura inteligente de los datos de los equipos
    - Configurable para cualquier tipo de red y tamaño
    - Se pueden generar ilimitado número de CPMs
    - Ilimitado número de equipos
    - Transparente en la red del cliente: está diseñado con la prioridad de no ser invasivo
    - Multiplataforma nativa (Microsoft Windows, GNU Linux, Apple OS X)
    - Si necesidad de software/licenciamiento de terceros (máquinas virtuales, base de datos, frameworks, etc)
    - Soporta varios protocolos de comunicaciones (HTTP, SMTP) y autenticación (Proxy, etc)
    - Minimización del ancho de banda consumido
    - Sistema de descubrimiento de Impresoras automático: permite realizar una monitorización paralela: lecturas sobre IPs fijas y a la vez, con otra periodicidad, descubrimiento de nuevos equipos en las redes.
  - o **Seguridad del CPM:**
    - Totalmente respetuoso con la red y sus equipos, cumpliendo los criterios de comunicaciones y seguridad más exigentes y las más importantes regulaciones internacionales:
      - a. RFCs de comunicaciones y seguridad
      - b. HIPAA: Health Insurance Portability and Accountability Act
      - c. Sarbanes-Oxley Act
      - d. Gramm-Leach-Bliley Act
      - e. Federal Information Security Management Act
      - f. ENISA Advising Directives
      - g. Otros
    - No captura ningún dato confidencial (jobs, nombres, etc.). Solamente los datos necesarios para la gestión de MPS
    - Admite capas de cifrado y comunicaciones sobre SSL (1024-bit HTTPS).
    - No necesita acceso al Servidor de impresión. Los datos que se transmiten desde el cliente al servidor CPS son totalmente auditables por el cliente y el proveedor del servicio.