

DEVICE HARDENING SERVICE

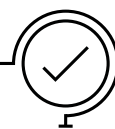
Device Hardening de Canon mejora el rendimiento de los dispositivos de impresión para protegerlos de problemas relacionados con la seguridad. Nuestro servicio mejora la seguridad nativa de los dispositivos Canon mediante la aplicación de un perfil seguro que le confiere una mayor protección sin esfuerzo adicional.



RECOMENDACIÓN



CONFIGURACIÓN



VALIDACIÓN



BENEFICIOS PARA TU EMPRESA:

- Reduce el riesgo de pérdida de datos al proteger los datos almacenados en los dispositivos durante toda su vida útil
- Amplía las políticas de protección de datos para dispositivos de impresión con el fin de mantener un entorno seguro
- Reduce el riesgo de filtraciones de seguridad relacionadas con las impresoras para evitar posibles sanciones reglamentarias y daños a la reputación de la marca



POSIBLES AMENAZAS PARA TU EMPRESA:

- Tus dispositivos almacenan y procesan datos confidenciales, como informes financieros y otra información confidencial
- Tus dispositivos están conectados a la red, lo que los expone a posibles ataques
- A menudo se pasan por alto los riesgos de seguridad de tus dispositivos, lo que los hace más susceptibles a ataques

DEVICE HARDENING SERVICE

CONFIGURACIÓN DE DEVICE HARDENING

La configuración de un perfil seguro que se ha puesto a prueba por completo e incorpora las prácticas recomendadas y las expectativas en materia de ciberseguridad de los compradores de soluciones de seguridad.

Canon también ofrece un servicio personalizado para satisfacer los requisitos específicos del cliente.

CARACTERÍSTICA	DESCRIPCIÓN
Activar la opción de borrado seguro de datos	Los datos se borran automáticamente del almacenamiento del dispositivo después de cada trabajo cuando todas las páginas se han impreso, enviado por fax, escaneado o copiado.
Establecer una contraseña de la interfaz de usuario remoto	La interfaz de usuario remoto permite acceder a la configuración del dispositivo a través de la interfaz web. La contraseña permite el acceso autorizado a esta interfaz.
Establecer una contraseña del administrador del sistema	El administrador del sistema permite acceder al dispositivo con privilegios de administrador. La contraseña predeterminada se cambia para una mayor protección.
Establecer una contraseña de la herramienta de gestión remota	El kit de software de operador remoto permite acceder de forma remota al panel táctil y los controles del dispositivo para realizar tareas de mantenimiento. La contraseña proporciona una capa de seguridad adicional.
Activar la verificación de la integridad del sistema al inicio	El arranque seguro es una función nativa del dispositivo que comprueba si se ha manipulado el código de arranque, el firmware y las aplicaciones MEAP al iniciar el dispositivo.
Ocultar los registros de trabajos del dispositivo	Bloquea la visualización de los registros de trabajos generados en el dispositivo, ya que pueden incluir nombres de archivo y nombres de usuario.
Desactivar los protocolos y servicios no utilizados	Ciertos protocolos y puertos activos podrían aumentar el riesgo de ataques, por lo que se desactivan los ajustes que no se utilicen. Entre ellos se incluyen SMB, FTP y fax IP.
Restringir el uso de USB	El dispositivo no se puede conectar a un PC a través de USB para utilizar las funciones de impresión y escaneo. Los documentos escaneados no se pueden guardar en un dispositivo de memoria USB.
Restringir la conectividad a redes inalámbricas	El dispositivo no se puede conectar a la red de la empresa mediante Wi-Fi.
Prohibir el acceso a usuarios invitados	Los usuarios no registrados no pueden iniciar sesión para utilizar las funciones del dispositivo, incluida la liberación de trabajos de impresión enviados a través de la función de impresión segura del dispositivo.
Forzar el cierre de sesión automático	La sesión de los usuarios se cierra automáticamente si no se realiza ninguna operación durante más de 30 segundos.
Restringir el uso de algoritmos de encriptación débiles	Se impide la conexión a sistemas que admiten protocolos de cifrado débil, como IPSec, TLS, Kerberos, S/MIME, LAN inalámbrica y SNMPv3.



CONTACTO

Para obtener más información, contacta con tu oficina local de Canon.

Canon Inc.
canon.com

Canon Europe
canon.es

Spanish edition
© Canon Europa N.V. 2023

Canon España, S.A.
Avda. de Europa, 6
28108 Alcobendas (Madrid)
Tel.: 91 538 45 00
Fax: 91 564 01 17
canon.es