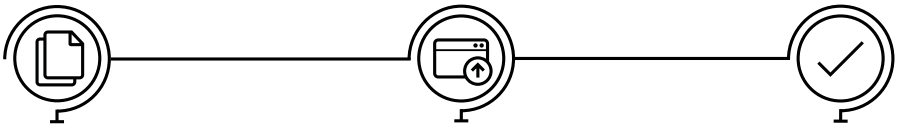
DEVICE HARDENING SERVICE

Device Hardening von Canon Die Leistung eines Drucksystems verbessern und es widerstandsfähiger gegen Sicherheitsprobleme machen. Unser Service verbessert die systemeigene Sicherheit von Canon Geräten durch die Anwendung eines Sicherheitsprofils für mehr Schutz ohne zusätzlichen Aufwand.



EMPFEHLEN **KONFIGURIEREN** **VALIDIEREN**

VORTEILE FÜR IHR UNTERNEHMEN:

- Geringeres Risiko von Datenverlusten durch Schutz der auf den Geräten gespeicherten Daten während ihrer gesamten Lebensdauer
- Erweiterung der Datenschutz-Richtlinien auf Drucksysteme, damit die Arbeitsumgebung sicher bleibt
- Verringerung des Risikos von Sicherheitsverletzungen im Zusammenhang mit Druckern, um mögliche Bußgelder und eine Rufschädigung der Marke zu vermeiden

MÖGLICHE BEDROHUNGEN FÜR IHR UNTERNEHMEN

- Ihre Geräte speichern und verarbeiten vertrauliche Daten, z. B. Finanzberichte und andere sensible Informationen
- Ihre Systeme sind mit dem Netzwerk verbunden und dadurch möglichen Angriffen ausgesetzt
- Ihre Geräte werden häufig nicht als Sicherheitsrisiko gesehen, was sie zu einem größeren Ziel macht.

Canon

DEVICE HARDENING SERVICE

DEVICE HARDENING KONFIGURATION

Eine sichere Profilkonfiguration, die vollständig getestet wurde und die empfohlenen, praxiserprobten Maßnahmen für Cybersicherheit sowie die Erwartungen der Käufer von Sicherheitslösungen berücksichtigt.

Canon bietet auch einen maßgeschneiderten Service an, um kundenspezifische Anforderungen zu erfüllen.

EIGENSCHAFT	BESCHREIBUNG
Aktivierung der Option der sicheren Festplattenlöschung (bei Modellen mit HDD)	Die Daten werden nach jedem Auftrag automatisch aus dem Gerätespeicher gelöscht, wenn alle Seiten gedruckt/gefaxt/gescannt/kopiert worden sind (bei Geräten mit HDD, bei Geräten mit SSDs ist dies technologisch bedingt nicht notwendig).
Festlegung des Kennworts für die Remote-Nutzeroberfläche	Die Fernbedienungsschnittstelle ermöglicht den Zugriff auf die Geräteeinstellungen über eine Webschnittstelle. Der Passwortschutz ermöglicht ausschließlich einen autorisierten Zugriff auf diese Schnittstelle.
Festlegung des Kennworts für den Systemmanager	System Manager ermöglicht den Zugriff auf das Gerät mit Administratorrechten. Das Passwort muss zum zusätzlichen Schutz abweichend von Werkseinstellungen geändert werden.
Festlegung des Kennworts für das Fernverwaltungs-Tool	Das Remote Operator's Software Kit ermöglicht den Fernzugriff auf das Touchpanel und die Bedienelemente des Geräts zu Servicezwecken. Das Passwort bietet eine zusätzliche Sicherheitsebene.
Aktivierung der Überprüfung der Systemintegrität beim Start	Secure Boot ist eine geräteeigene Funktion, die den Code beim Booten, die Firmware und die MEAP-Anwendungen beim Start des Geräts auf Manipulationen überprüft.
Ausblendung von System-Jobprotokollen	Blockierung der Anzeige der am Gerät erzeugten Job-Protokolle, da diese Dateinamen und Benutzernamen enthalten können.
Deaktivierung nicht-verwendeter Protokolle und Dienste	Bestimmte aktive Protokolle und Ports erhöhen das Risiko von Angriffen, deshalb werden nicht deshalb werden nicht genutzte Einstellungen deaktiviert. Einstellungen deaktiviert. Darunter fallen auch SMB, FTP und IP Fax.
Einschränkung der USB-Nutzung	Das Gerät kann nicht über USB an einen PC angeschlossen werden, um die Druck- und Scanfunktionen zu nutzen. Gescannte Dokumente können nicht auf einem USB-Stick gespeichert werden.
Einschränkung der Verbindung zu drahtlosen Netzwerken	Das Gerät kann nicht über WLAN mit dem Unternehmensnetzwerk verbunden werden.
Verbot des Zugriffs von Gastnutzern	Nicht registrierte Benutzer können sich nicht anmelden, um Gerätefunktionen zu nutzen, einschließlich der Freigabe von Druckaufträgen, die über die Gerätefunktion Sicherer Druck gesendet wurden.
Erzwingung der automatischen Abmeldung	Benutzer werden automatisch abgemeldet, wenn mehr als 30 Sekunden lang keine Operationen durchgeführt werden.
Einschränkung der Nutzung schwacher Verschlüsselungsalgorithmen	Die Verbindung zu Systemen, die schwache Verschlüsselung in Bezug auf IPSec, TLS, Kerberos, S/MIME, Wireless LAN und SNMPv3 unterstützen, ist deaktiviert.

KONTAKT

Bei weiteren Fragen wenden Sie sich an Ihre Canon Niederlassung vor Ort.

Canon Inc.
canon.com

Canon Deutschland GmbH
canon-europe.com

German edition

Canon Deutschland GmbH
Europark Fichtenhain A10
D-47807 Krefeld
Canon Helpdesk
Tel.: +49 30 9158 9012
canon.de
canon.at
canon.ch