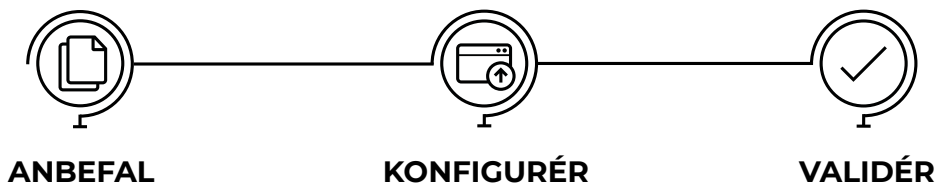


DEVICE HARDENING

Canons Device Hardening forbedrer en printers ydeevne og gør den modstandsdygtig over for sikkerhedsrelaterede problemer. Vores service forbedrer den oprindelige sikkerhed for Canon-printere ved at anvende en sikker profil for ekstra beskyttelse uden ekstra indsats.



FORDELE FOR JERES VIRKSOMHED:

- Reduceret risiko for datatab ved at beskytte data, der er gemt i printere, i hele deres levetid
- Udvid databeskyttelsespolitikker til printere for at opretholde et sikkert miljø
- Reducér risikoen for brud på printerrelateret sikkerhed, og undgå eventuelle lovgivningsmæssige bøder og skader på brandets omdømme



POTENTIELLE TRUSLER MOD JERES VIRKSOMHED

- Jeres printere gemmer og behandler fortrolige data, f.eks. økonomiske rapporter og andre følsomme oplysninger
- Jeres printere er forbundet til netværket, hvilket kan udsætte dem for potentielle angreb
- Jeres enheder betragtes ofte ikke som en sikkerhedsrisiko, hvilket kan gøre dem mere til et enkelt mål

DEVICE HARDENING

DEVICE HARDENING-KONFIGURATION

En sikker profilkonfiguration, der er blevet gennemtestet og inkorporerer anbefalede bedste praksisser for cybersikkerhed og forventninger fra købere af sikkerhedsløsninger.

Canon tilbyder også en skræddersyet service til at imødekomme kundespecifikke krav.

FUNKTION	BESKRIVELSE
Aktivér indstillingen for sikker sletning af data	Data slettes automatisk fra printeren efter hvert job, når alle sider er printet/faxet/scannet/kopieret.
Angiv adgangskode til fjernbrugerinterface	Remote User Interface giver adgang til enhedsindstillinger via webinterface. Adgangskode giver autoriseret adgang til dette interface.
Angiv adgangskode til System Manager	System Manager giver adgang til printere med administratorrettigheder. Adgangskoden er ændret fra fabriksstandard for at give ekstra beskyttelse.
Angiv adgangskode til Remote Management-værktøjet	Remote Operator's Software Kit giver mulighed for fjernadgang til enhedens touchpanel og betjeningsknapper med henblik på service. Adgangskode giver ekstra sikkerhedslag.
Aktivér verificering af systemintegritet ved opstart	Secure Boot er en indbygget printerfunktion, der kontrollerer, om der er pillet ved startkode, firmware og MEAP-applikationer ved opstart af printeren.
Skjul enhedens joblogfiler	Blokerer visning af joblogfiler, der genereres på printeren, da disse kan omfatte filnavne og brugernavne.
Deaktivér ubrugte protokoller og services	Visse aktive protokoller og porte kan øge risikoen for angreb, så de ubrugte indstillinger deaktiveres. Disse omfatter SMB, FTP og IP Fax.
Begræns brug af USB	Printeren kan ikke sluttes til en pc via USB for at kunne bruge print- og scanningsfunktioner. Scannede dokumenter kan ikke gemmes på en USB-nøgle.
Begræns tilslutning til trådløse netværk	Printeren kan ikke tilsluttes virksomhedens netværk via Wi-Fi.
Forbyd adgang til gæstebrugere	Ikke-registrerede brugere kan ikke logge på for at bruge enhedsfunktioner, herunder frigivelse af printjob, der sendes via sikkert print fra printeren.
Gennemtvung automatisk logout	Brugere logges automatisk af, hvis der ikke udføres nogen handlinger i mere end 30 sekunder.
Begræns brug af svage krypteringsalgoritmer	Forbindelse til systemer, der understøtter svag kryptering i forbindelse med IPsec, TLS, Kerberos, S/MIME, trådløst LAN og SNMPv3 deaktiveres.

KONTAKT

Kontakt det lokale Canon-kontor for at få flere oplysninger.

Canon Inc.
canon.com

Canon Europe
canon-europe.com

Danish edition
© Canon Europa N.V. 2023

Canon Danmark
Østmarken 3A
2860 Søborg
Tlf.: 70 15 50 05
canon.dk