BESCHERM
UW KANTOOR

Canon

HOE VEILIG IS INFORMATIE OP UW KANTOOR?

Hedendaagse organisaties zijn voornamelijk gegrondvest op informatie. Ze creëren complexe internationale netwerken van connected technologieën, processen, mensen en organisaties. Nieuwe flexibele werkmethoden veranderen het kantoor en de manier waarop mensen informatie creëren, delen en gebruiken. Het beveiligen van gegevens in deze complexe omgeving vormt een grotere uitdaging dan ooit. De meeste organisaties investeren in hoogwaardige technologieën, zoals geavanceerde firewalls en de nieuwste antivirus- en beveiligingssoftware. Maar vaak onderkennen ze niet de noodzaak om ook hun kantoorprinters te beveiligen, waardoor ze kwetsbaarder zijn dan ze beseffen.

DENK NA OVER UW PRINTERS

Moderne multifunctionele printers (MFP's) hebben zich ontwikkeld tot krachtige hulpmiddelen, die net als pc's en servers beschikken over besturingssystemen en enorme harde schijven, die verbinding maken met het netwerk en internet, en die door gebruikers worden gedeeld om dagelijks enorme aantallen bedrijfskritische documenten te verwerken.

WAT ZIJN DE RISICO'S?

- Onbevoegde gebruikers kunnen gevoelige informatie bekijken die is opgeslagen op onbeveiligde MFP's
- De beschikbaarheid van uw printinfrastructuur kan in gevaar worden gebracht door verkeerde bediening
- Kwaadwillende buitenstaanders kunnen via de printer toegang krijgen tot uw netwerk, waarna ze verdere aanvallen kunnen uitvoeren
- Onbevoegden kunnen vertrouwelijke documenten onder ogen krijgen die na het printen per abuis in de uitvoerlade blijven liggen
- Geprint materiaal van verschillende gebruikers kan door elkaar raken
- Documenten kunnen per fax of e-mail naar de verkeerde ontvangers worden verzonden als gevolg van typefouten
- Gegevens die onderweg zijn om te worden geprint of gescand kunnen door hackers worden onderschept
- Gegevens kunnen verloren gaan door onzorgvuldige verwijdering van printers aan het einde van de leaseperiode

"Het is de moeite waard om op kantoor, waar u waarschijnlijk enorme hoeveelheden gegevens verwerkt, basisnormen voor informatiebeveiliging te hanteren. Tegenwoordig is een printer geen domme machine meer, maar een server die toevallig papier print."

(CISO, Publicis Groupe)

VEILIGE PRINTOPLOSSINGEN VOOR UW BEDRIJF

Beveiliging en privacy op maat

Bij het ontwerpen of selecteren van technologieën, producten en diensten voor klanten houdt Canon rekening met de waarschijnlijke gevolgen van de informatiebeveiliging voor de omgeving van deze klanten. Daarom zijn Canon's multifunctionele kantoorprinters uitgerust met een groot aantal beveiligingsfuncties, zowel standaard als optioneel, waarmee bedrijven van elke omvang het gewenste beschermingsniveau kunnen realiseren voor:

APPARATEN | NETWERKEN | DOCUMENTEN | UW ORGANISATIE

INTERNATIONAAL ERKENDE NORMEN EN CERTIFICERINGEN

De multifunctionele apparaten van het imageRUNNER ADVANCE-assortiment worden regelmatig geëvalueerd en gecertificeerd volgens de Common Criteria-methodologie en in overeenstemming met het Hard Copy Device Protection Profile (HCD_PP) of IEE P2600.2 Protection Profile.

BEVEILIGINGSTESTS

Canon maakt gebruik van een van de meest rigoureuze testmethoden voor beveiliging in de sector voor kantoorapparatuur. Technologieën die in de productportfolio worden toegepast, moeten aan dezelfde hoge testnormen voldoen als die Canon voor het eigen bedrijf verwacht.

Als marktleider in de ontwikkeling van innovatieve oplossingen voor print- en informatiebeheer voor kantoren en bedrijven werkt Canon samen met klanten aan een allesomvattende benadering van informatiebeveiliging, waarbij rekening wordt gehouden met de beveiligingseffecten van onze kantoortechnologie als onderdeel van hun bredere informatie-ecosysteem.

BESCHERM UW APPARAAT

Uitgebreide bescherming voor uw fysieke bedrijfsmiddelen

OPLOSSINGEN VOOR GEBRUIKERSVERIFICATIE

Bescherm uw apparaat tegen onbevoegd gebruik door toegangsbeheer voor gebruikers via verificatie te implementeren. Dit biedt bovendien het extra voordeel dat gebruikers sneller toegang hebben tot hun voorkeursinstellingen en printopdrachten, terwijl de controleerbaarheid wordt vergroot. Canon's afdelingsprinters zijn uitgerust met Universal Login Manager, een flexibele aanmeldoplossing die gebruikersverificatie mogelijk maakt via een gebruikersdatabase die op het apparaat is gemaakt, evenals domeinverificatie via Active Directory of uniFLOW-server. Zo kunnen bedrijven de toegang tot apparaten beheren en tegelijkertijd de juiste balans vinden tussen gebruikersgemak en beveiliging.

APPARAATBEHEER

De configuratie van het apparaat, zoals netwerkinstellingen en andere besturingsopties, is alleen toegankelijk voor gebruikers die beheerdersrechten hebben. Zo worden opzettelijke of onbedoelde wijzigingen voorkomen.

PREVENTIEVE BEVEILIGING

ImageRUNNER ADVANCE-apparaten bieden een aantal beveiligingsinstellingen waarmee printers tegen aanvallen kunnen worden beveiligd. De functie Beveiligd opstarten zorgt voor integriteit van het apparaat, terwijl Syslog-gegevens realtime beveiliging van het apparaat bieden (gegevens kunnen worden gelezen door een geschikt SIEM-systeem van derden).

SYSTEEM VOOR TOEGANGSBEHEER

Deze functie biedt nauwkeurige controle over de toegang tot de apparaatfuncties. Beheerders kunnen de standaard beschikbare rollen gebruiken of aangepaste rollen maken met een gewenst toegangsniveau. Zo kan voor bepaalde gebruikers bijvoorbeeld het kopiëren van documenten of het gebruik van de verzendfunctie worden beperkt.

INSTELLING VAN BEVEILIGINGSBELEID

De nieuwste imageRUNNER ADVANCE-apparaten zijn ook uitgerust met een functie voor beveiligingsbeleid, die de beheerder via één menu toegang biedt tot alle beveiligingsinstellingen en waarmee de beheerder deze instellingen kan bewerken voordat ze op het apparaat van kracht worden.

Wanneer het beleid van kracht is, moeten het gebruik van het apparaat en de instellingen voldoen aan dat beleid. Het beveiligingsbeleid kan worden afgeschermd met een apart wachtwoord, zodat de toegang tot dit gedeelte wordt beperkt tot de verantwoordelijke IT-beveiligingsmedewerker. Zo wordt het niveau van controle en garantie extra verhoogd.

BEVEILIGING VAN GEGEVENS OP DE APPARAATOPSLAGMEDIA

De multifunctionele printer bevat voortdurend een grote hoeveelheid gegevens die moet worden beveiligd, van printopdrachten in de wachtrij tot ontvangen faxen, gescande gegevens, adresboeken, activiteitenlogboeken en taakgeschiedenis. Canon's apparaten bieden een aantal maatregelen om uw gegevens in elke fase van de levensduur van het apparaat te beschermen en de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te garanderen.

Afhankelijk van het specifieke apparaatmodel wordt een harde schijf (HDD) of een Solid-State Drive (SSD) gebruikt. Aangezien een harde schijf een fysiek draaiende schijf gebruikt waarop gegevens worden opgenomen, moeten gegevens een aantal keren, meestal drie keer, worden overschreven om ervoor te zorgen dat de gegevens daadwerkelijk zijn gewist. In tegenstelling tot een HDD verplaatst een SSD gegevens door de beschikbare geheugenruimte om ervoor te zorgen dat er zelfs elektrische slijtage van de geheugencellen is. Elke cel heeft slechts een eindig aantal schrijfbewerkingen en dit 'TRIM' -proces maximaliseert de levensduur van de SSD terwijl tegelijkertijd 'logisch verwijderde' gegevens worden overschreven.

De imageRUNNER ADVANCE biedt verschillende configuratieopties die kunnen worden geconfigureerd om het moment in te stellen waarop een overschrijving en de overschrijfmethode wordt uitgevoerd.

HOE VEILIG ZIJN UW APPARATEN?

1
Worden uw apparaten gedeeld en bevinden ze zich in openbare ruimten?

2
Kunnen gebruikers onbeveiligde toegang krijgen tot apparaten?

3
Hebt u maatregelen getroffen om informatie op de harde schijf van het apparaat te beschermen?

4
Kunnen onbevoegde gebruikers apparaatinstellingen wijzigen?

5
Hebt u de levenscyclus van uw apparaat en de veilige verwijdering ervan overdacht?

SCHIJFVERSLEUTELING

Canon's imageRUNNER ADVANCE-apparaten coderen alle gegevens op de harde schijf, waardoor de beveiliging wordt verbeterd. De beveiligingschip die verantwoordelijk is voor gegevenscodering voldoet aan de beveiligingsstandaard FIPS 140-2 Level 2 die is vastgesteld door de Amerikaanse overheid, en is gecertificeerd volgens het Cryptographic Module Validation Program (CMVP) dat is vastgesteld door de Verenigde Staten en Canada, evenals volgens het Japanse Cryptographic Module Validation Program (JCMVP).

GEGEVENSOPSLAG VERWIJDEREN

Sommige gegevens, zoals gekopieerde of gescande afbeeldingsgegevens, en documentgegevens die vanaf een computer worden geprint, worden slechts tijdelijk opgeslagen op een harde schijf of een solid-state-apparaat en verwijderd nadat de bewerking is voltooid. Om ervoor te zorgen dat er geen restgegevens worden bewaard, zijn de apparaten van Canon voorzien van mogelijkheden die restgegevens stelselmatig wissen als onderdeel van de taakverwerking.

ALLE GEGEVENS EN INSTELLINGEN INITIALISEREN

Om gegevensverlies te voorkomen bij het vervangen of verwijderen van de harde schijf, kunt u alle documenten en gegevens op de harde schijf overschrijven en de standaardinstellingen van het apparaat herstellen.

SPIEGELEN VAN DE HARDE SCHIJF*

Bedrijven hebben de mogelijkheid om een back-up te maken van de gegevens op de harde schijf van hun apparaat met behulp van een extra optionele harde schijf. Tijdens de spiegeling worden de gegevens op beide harde schijven volledig gecodeerd.

*Optioneel. Neem contact op met uw Canon-vertegenwoordiger voor uitgebreide informatie over de beschikbaarheid van de functies en opties in de printportfolio voor kantoren.

BEVEILIG UW NETWERK

KAN UW PRINTER UW NETWERK IN GEVAAR BRENGEN?

- Laat u netwerkpoorten open en daarmee toegankelijk voor aanvallen?
- Kunnen gasten printen en scannen zonder uw netwerk bloot te stellen aan risico's?
- Is uw beleid voor het gebruik van persoonlijke apparatuur op het werk veilig en ondersteunend?
- Worden printgegevensstromen gecodeerd van de pc naar het uitvoerapparaat?
- Zijn print- en scangegevens beveiligd tijdens de verwerking?

Canon biedt een reeks beveiligingsoplossingen om uw netwerk en gegevens te beschermen tegen aanvallen van binnenuit en van buitenaf.

FILTEREN VAN IP- EN MAC-ADRESSEN

Bescherm uw netwerk tegen onbevoegde toegang door derden door uitsluitend communicatie toe te staan met apparaten die een specifiek IP- of MAC-adres hebben voor zowel uitgaande als inkomende communicatie.

CONFIGURATIE VAN DE PROXYSERVER

Stel een proxy in om communicatie te verwerken in plaats van uw apparaat, en gebruik deze als u verbinding maakt met apparaten buiten het netwerk.

IEEE 802.1X-VERIFICATIE

Netwerktoegang door onbevoegden wordt geblokkeerd door een LAN-switch die alleen toegangsrechten verleent aan clientapparaten die zijn geautoriseerd door de verificatieserver.

IPSEC-COMMUNICATIE

IPSec-communicatie voorkomt dat externe IP-pakketten die via het IP-netwerk worden verzonden, onderscheppen of manipuleren. Gebruik met TLS gecodeerde communicatie om te voorkomen dat gegevens die tussen de het apparaat en andere apparaten, zoals computers, worden uitgewisseld, worden opgespoord, vervalst en gesaboteerd.

POORTBEHEER

Poorten configureren als onderdeel van uw beveiligingsbeleid.

AUTOMATISCHE INSCHRIJVING CERTIFICEREN

Met deze functie wordt het lastige onderhoud van beveiligingscertificaten drastisch verminderd. Met behulp van erkende technologie kan een systeembeheerder certificaten automatisch bijwerken en vrijgeven, zodat er altijd aan het beveiligingsbeleid wordt voldaan.

LOGBOEKBEWAKING

Met verschillende logboeken kunt u de activiteit rondom uw apparaat controleren, met inbegrip van geblokkeerde communicatieverzoeken.

WI-FI DIRECT

Schakel peer-to-peer-verbinding in voor mobiel printen, zonder dat het mobiele apparaat toegang tot uw netwerk nodig heeft.

CODERING VAN GEGEVENS DIE WORDEN VERZONDEN NAAR EN VAN HET APPARAAT

Met deze optie worden printopdrachten gecodeerd die worden verzonden van de pc van de gebruiker naar de multifunctionele printer. Door de universele beveiligingsfunctieset in te schakelen, kunnen gescande gegevens in PDF-indeling ook worden gecodeerd.

MOBIEL PRINTEN DOOR GASTEN

Canon's veilige software voor print- en scanbeheer in het netwerk pakt algemene beveiligingsrisico's voor mobiel printen en printen door gasten aan door via e-mail, internet en mobiele applicaties externe banen voor het indienen van opdrachten aan te bieden. Hierdoor worden aanvalsvectoren tot een minimum beperkt door het MFD te vergrendelen tot een veilige bron.

BESCHERM UW DOCUMENTEN

Alle bedrijven hebben te maken met gevoelige documenten, zoals contractuele overeenkomsten, salarisgegevens van het personeel, klantgegevens, onderzoeks- en ontwikkelingsplannen en meer. Als documenten in verkeerde handen vallen, kunnen de gevolgen variëren van een beschadigde reputatie tot hoge boetes of zelfs juridische stappen.

Canon biedt een reeks beveiligingsoplossingen om uw gevoelige documenten gedurende de gehele levenscyclus te beschermen.

VERTROUWELIJKHEID VAN HET GEPRINTE DOCUMENT

Beveiligd printen
De gebruiker kan een pincode instellen om te printen, zodat het document pas kan worden geprint nadat de juiste pincode is ingevoerd op het apparaat. Zo kunnen gebruikers de documenten beveiligen die ze als vertrouwelijk beschouwen.

Alle printopdrachten blokkeren
Op imageRUNNER ADVANCE-apparaten kan de beheerder alle ingediende printopdrachten blokkeren, zodat gebruikers zich eerst moeten aanmelden voordat opdrachten kunnen worden geprint. Zo kan de vertrouwelijkheid van alle geprinte documenten worden gewaarborgd.

Postvakken
Printopdrachten of gescande documenten kunnen in een postvak worden opgeslagen voor toegang op een later tijdstip. Postvakken kunnen worden beveiligd met een pincode om ervoor te zorgen dat alleen de toegewezen eigenaar de inhoud kan bekijken die erin is opgeslagen. Deze beveiligde ruimte op het apparaat is geschikt voor het bewaren van documenten die vaak moeten worden uitgevoerd (zoals formulieren), maar waarmee zorgvuldig moet worden omgegaan.

Beveiligd printen met uniFLOW*
Met uniFLOW MyPrintAnywhere kunnen gebruikers veilig printopdrachten verzenden via het universele stuurprogramma en ophalen bij elke printer in het netwerk.

BELEMMEREN OF VOORKOMEN DAT DOCUMENTEN DUBBEL WORDEN GEMAAKT

Printen met zichtbare watermerken
Stuurprogramma's kunnen zichtbare markeringen op de pagina printen, over de inhoud van het document heen of erachter. Dit ontmoedigt het kopiëren van het document door de gebruiker bewust te maken van de vertrouwelijkheid van het document.

Printen/kopiëren met onzichtbare watermerken
Als deze optie is ingeschakeld, kunnen documenten worden geprint of gekopieerd met ingesloten verborgen tekst op de achtergrond. Bij dupliceren wordt de tekst op het document weergegeven en fungeert zo als afschrikmiddel.

HOE VEILIG ZIJN UW DOCUMENTEN?

1
Kunnen onbevoegde gebruikers geen toegang krijgen tot gevoelige documenten op de printer?

2
Kunt u de vertrouwelijkheid garanderen van alle documenten van gebruikers die het gedeelde apparaat passeren?

3
Kan iemand met gevoelige documenten uit uw printer weglopen?

4
Kunt u veelvoorkomende vergissingen voorkomen bij het verzenden van documenten vanaf het apparaat?

CONTROLE UITOEFENEN OP HET VERZENDEN EN FAXEN VAN DOCUMENTEN

Bestemmingen voor verzenden beperken
Om het risico op informatielekken te beperken, kunnen beheerders de beschikbare verzendbestemmingen beperken tot alleen de bestemmingen in het adresboek of op de LDAP-server, het adres van de aangemelde gebruiker of bepaalde domeinen.

Automatisch aanvullen van adressen uitschakelen
Voorkom het verzenden van documenten naar verkeerde bestemmingen door het automatisch invullen van e-mailadressen uit te schakelen.

Bescherming van het adresboek
Stel een pincode in om het adresboek van het apparaat te beschermen tegen ongeoorloofde bewerking door gebruikers.

Bevestiging van faxnummer
Voorkom dat documenten naar onbedoelde ontvangers worden verzonden door gebruikers te vragen het faxnummer tweemaal in te voeren ter bevestiging, alvorens de fax te verzenden.

Vertrouwelijkheid voor ontvangen fax
Stel het apparaat in om documenten in het geheugen op te slaan zonder te printen. U kunt de vertrouwelijkheid van ontvangen faxdocumenten ook beschermen door voorwaarden in te stellen om de opslaglocatie te bepalen voor een vertrouwelijk postvak IN. U kunt ook pincodes instellen.

DE OORSPRONG EN AUTHENTICITEIT VAN DOCUMENTEN CONTROLEREN VIA DIGITALE HANDTEKENINGEN

Handtekening van het apparaat
Er kan een handtekening van het apparaat worden toegepast op gescande documenten in PDF- of XPS-indeling, met behulp van een sleutel- en certificaatmechanisme, zodat de ontvanger zowel de oorsprong van het document als de authenticiteit kan controleren.

Handtekening van de gebruiker*
Met deze optie kunnen gebruikers een PDF- of XPS-bestand verzenden met een unieke digitale gebruikershandtekening die is verkregen van een certificeringsinstantie. Op deze manier kan de ontvanger controleren welke gebruiker het bestand heeft ondertekend.

*Optioneel. Neem contact op met uw Canon-vertegenwoordiger voor uitgebreide informatie over de beschikbaarheid van de functies en opties in de printportfolio voor kantoren.

BEVEILIGING VAN BEDRIJFSGEGEVENS

Canon kan helpen bij de algehele bescherming van informatie in uw organisatie.

COMPLETE CONTROLE VOOR UW VOLLEDIGE BEHOEFTEN OP HET GEBIED VAN VASTLEGGEN EN UITVOEREN

Met Canon's modulaire software voor uitvoerbeheer kunnen bedrijven netwerkapparaten veilig delen, zodat ze opdrachten zorgeloos kunnen printen op elke printer die is verbonden met de server voor uitvoerbeheer. Mobiele gebruikers worden ondersteund door een centraal beheerde service, waarbij zowel interne als gastgebruikers veilig kunnen printen vanaf mobiele apparaten. De scanmodule biedt de mogelijkheid om documenten vast te leggen, te comprimeren, te converteren en te distribueren van het multifunctionele apparaat naar een groot aantal bestemmingen, waaronder cloudgebaseerde systemen. U kunt printopdrachten ook veilig omleiden naar de meest geschikte printer, waardoor de printkosten voor elk document worden geoptimaliseerd.
Canon's oplossing verbetert de beveiliging van documenten in uw hele bedrijf, in combinatie met volledige documentadministratie voor een volledig overzicht van de activiteiten per gebruiker, per apparaat en per afdeling.

GECENTRALISEERD PRINTERPARKBEHEER

Met onze software voor apparaatbeheer IW MC kunnen apparaatinstellingen, beveiligingsbeleid, wachtwoorden en certificaten, evenals firmware worden bijgewerkt en via het netwerk naar uw Canon-apparaten worden verzonden. Zo bespaart u uw IT-team kostbare tijd en blijft de beveiliging van uw printinfrastructuur up-to-date.

BEHEERDE PRINTDIENSTEN

Canon MPS combineert innovatieve technologie en software met de juiste diensten om u de gewenste print- en documentervaringen te bieden, zonder het bijbehorende gedoe voor uw IT-teams. Door proactief beheer en voortdurende optimalisatie van uw printinfrastructuur en documentworkflows kan Canon u helpen uw beveiligingsdoelstellingen te bereiken, terwijl u de kosten optimaliseert en de productiviteit in uw hele bedrijf verhoogt.

ONTWIKKELING OP MAAT

Canon beschikt over een team interne ontwikkelaars die een oplossing op maat kunnen voorstellen en ontwikkelen - een oplossing die geschikt is voor uw specifieke situatie of voldoet aan uw unieke vereisten.

HOE ALLESOMVATTEND IS UW AANPAK VAN DE BEVEILIGING VAN UW BEDRIJF?

- Geldt uw beveiligingsbeleid ook voor uw park van multifunctionele apparaten?
- Hoe zorgt u ervoor dat uw printinfrastructuur up-to-date is en dat verbeteringen en foutoplossingen tijdig en efficiënt worden geïmplementeerd?
- Kunnen gasten printen en scannen zonder uw netwerk bloot te stellen aan risico's?
- Is uw beleid voor het gebruik van persoonlijke apparaten op het werk veilig en te handhaven in uw hele printerpark?
- Heeft uw IT-team voldoende tijd om beveiligingsproblemen te onderzoeken?
- Is de balans tussen beveiliging en gebruikersgemak in orde?

WAAROM CANON?

Canon maakt het verschil. Canon gebruikt haar kennis en jarenlange ervaring om verandering mogelijk te maken.

Verandering bij Canon's klanten, bij een digitale transformatie en werken op nieuwe manieren. Bredere maatschappelijke veranderingen met voortdurende aandacht voor duurzaamheid als onderdeel van Canon's impact en cultuur.

Tenslotte veranderingen bij Canon zelf, met de investering in nieuwe markten, producten en technologieën. Canon staat voor iedereen klaar: klanten, medewerkers en de samenleving in het algemeen.

Canon is gebouwd op vier kernwaarden:

BEVEILIGING

Canon's oplossingen en diensten helpen alle documenten en gevoelige gegevens te beveiligen, zowel op papier als digitaal, gedurende de hele documentlevenscyclus. Oplossingen en diensten ontworpen met het oog op beveiliging.

DUURZAAMHEID

Canon's duurzaamheidsbeleid ligt op één lijn met de Duurzame Ontwikkelingsdoelstellingen van de VN, waaronder toezeggingen voor verlaging van de CO2-uitstoot tijdens de gehele levenscyclus van het product, door minder verpakking en consolidatie van distributiecentra.

Al deze eigenschappen samen maken Canon tot de juiste partner.

ONDERSTEUNING

Een divers dienstenpakket om de hoogste kwaliteit te garanderen, voor optimale klanttevredenheid. Experts in huis die werken aan het verbeteren van efficiëntie en zich inzetten om Canon's klanten optimaal te ondersteunen.

INNOVATIE

Meer dan 80 jaar innovatie op het gebied van fotografie met geavanceerde technologie al resultaat. Pionierswerk in de industrie en een sterke betrokkenheid bij toekomstige technologische ontwikkelingen.

New to the Line

Canon uniFLOW Online
Outstanding Cloud Output Management Solution

Canon Belgium NV
Berkenlaan 3
1831 Diegem
Telefoon: 02 722 04 11
canon.be
contact@canon.be

Canon Nederland N.V.
Brabantlaan 2
5216 TV 's-Hertogenbosch
Telefoon: (073) 6 815 815
canon.nl
b2b@canon.nl

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Dutch edition 1.0
© Canon Europa N.V., 2021