CANONIN TIETOTURVARATKAISUT – MONITORI-PALVELU

Canonin Monitori-palvelu huolehtii kaikkien verkkoon liitettyjen Canonin monitoimilaitteiden ja tulostimien hallinnasta sekä varmistaa, että tietoturvakäytäntöjä noudatetaan.

OSA 1: USEIN KYSYTTYJÄ KYSYMYKSIÄ

Tämä dokumentti vastaa tärkeimpiin Monitori-palveluun liittyviin tietoturvakysymyksiin. Lisätietoja Monitori-palvelun sisältämästä tietoturvasta saat paikalliselta Canon-edustajalta.

Kuka omistaa minun tietoni?

Kaikissa tapauksissa omistat tietosi itse, Canon on vain asiakkaiden Monitori-tietojen käsittelijä.

Kuka voi käyttää tietojani?

Tietojen saatavuuden sääntelyyn Canon tarjoaa monitasoisen lähestymistavan, joka käsittää mm. seuraavat:

- Fyysinen käytönvalvonta – Vain valtuutetut henkilöt pääsevät fyysisesti Canonin tiloihin, rakennuksiin tai huoneisiin, joissa henkilötietoja käsitellään.
- Järjestelmään pääsyn valvonta – Henkilötietoja käsitteleviä järjestelmiä voidaan käyttää vain käyttäjärooleihin ja niihin liittyviin käyttöoikeuksiin perustuvalla luvalla.
- Tietojen käytön valvonta – Henkilöt, joilla on oikeus käyttää tietojenkäsittelyjärjestelmiä, pääsevät käsiksi vain niihin henkilötietoihin, joihin heillä on oikeus.
- Tietojensiirron valvonta – Henkilötietoja ei saa lukea, kopioida, muuttaa tai poistaa ilman lupaa siirron yhteydessä, paitsi jos se on tarpeen palvelujen tarjoamiseksi asianomaisen sopimuksen mukaisesti:
- Tietojen syötön valvonta – Canon toteuttaa toimenpiteitä, joiden avulla voidaan jälkikäteen tutkia ja selvittää, onko henkilötietoja syötetty, muutettu tai poistettu Canonin tietojenkäsittelyjärjestelmistä, ja jos on, niin kenen toimesta.
- Töiden valvonta – Kaikki Canonin työntekijät ja sopimussuhteiset alihankkijat tai palveluntarjoajat ovat sopimuksen mukaan velvollisia kunnioittamaan kaikkien arkaluonteisten tietojen luottamuksellisuutta.
- Tietojen erottelun valvonta – Henkilötietoja tallennetaan ja niihin pääsee käsiksi vain kunkin asiakkaan yksittäisen Monitori-järjestelmän tilin kautta.

Tietojen käyttöä valvotaan seuraavin toimenpitein:

- Osana Canonin tietoturvakäytäntöä henkilötiedot edellyttävät vähintään samaa suojaustasoa kuin ”luottamukselliset” tiedot.
- Pääsy henkilötietoihin myönnetään tiedonsaantitarpeen perusteella. Henkilökunnalla on pääsy niihin tietoihin, joita se tarvitsee tehtäviensä hoitamiseksi.
- Henkilötietoja käsitteleviä sovelluksia suojaavat turvatoimet tarkistetaan säännöllisesti. Tätä varten Canon suorittaa IT-järjestelmiensä suhteen sisäisiä ja ulkoisia tietoturvatarkastuksia ja penetraatiotestejä.
- Käsittelyn, käytön ja säilytyksen yhteydessä henkilötietoja ei saa lukea, kopioida, muuttaa tai poistaa ilman lupaa.

Onko tietoni salattu?

AWS-pilvipalveluun tallennetut tiedot on salattu.

Tietojen siirtäminen Canonin ja sen asiakkaiden välillä tapahtuu aina tietoturvallisesti salattujen protokollien avulla.

Henkilökohtaiset tiedot, jotka saatetaan tallentaa valinnaisen laiteasetusten varmuuskopiointipalvelun tai asennustukipalvelun käytön yhteydessä, kuten laitteen osoitekirjan tiedot, salataan AES-256 -salausalgoritmilla.

Miten tietoni erotetaan muiden asiakkaiden tiedoista?

Henkilötietojen käsittelyssä käytetään seuraavia erottelutoimia:

Canon toteuttaa asiakastietojen loogisen erottelun käyttämällä asianmukaisia teknisiä kontrolleja.

Tarvittaessa käytetään monikerroksista käyttöoikeusrakennetta, joka varmistaa että rakenteen ylätason tileillä on pääsy alatason tileihin, mutta alempi taso ei pääse käyttämään muita samalla tai ylemmällä tasolla olevia tilien tietoja.

Mitä tietoja Monitori kerää?

Suurin osa Monitori-palvelun keräämistä ja käyttämistä tiedoista on muita kuin henkilökohtaisesti tunnistettavia laitetietoja, kuten asiakas, laitteen nimi, sarjanumero, sijainti, IP-osoite, tila ja hälytykset.

Monitori-palvelu ei kerää seuraavia tietoja: käyttäjän toimintaan liittyvät tiedot, kuten käyttäjänimi*, päivämäärä/kellonaika, asiakirjan nimi, työn sisältö (kuvatiedot/tulostustiedot) kopioinnin, tulostuksen, skannauksen ja lähetyksen osalta.

Valvooko Canon pilvipalvelunsa tietoturvaa?

Canon suorittaa erilaisia auditointeja varmistaakseen tarjoamiensa pilvipalveluiden tietoturvan. Näin ollen Canon ja sen asiakkaat voivat käyttää kyseisiä palveluita luottavaisin mielin.

Monitori-palvelun tietoturvaan liittyen kolmas osapuoli suorittaa säännöllisesti penetraatiotestejä.

*Käytettäessä valinnaista laiteasetusten varmuuskopiointipalvelua tai asennustukipalvelua voidaan kerätä henkilökohtaisia tietoja, kuten käyttäjänimi ja sähköpostiosoite, jos ne sisältyvät laitteen osoitteistoon, mutta vain jos asiakkaan kanssa on asiasta erikseen sovittu.

Onko Monitori-palvelun pilvi-infrastruktuuri turvallinen?

Monitori-palvelu tarjotaan AWS-alustalla, joka sijaitsee Frankfurtissa, Saksassa.

Onko Monitori-palvelu sertifioitu jonkin merkittävän tietoturvastandardin mukaisesti?

Canon Inc:n Digital Printing Development Centre on sertifioitu kansainvälisen standardin ISO/IEC 27001 mukaisesti. Sertifiointi liittyy Canon Inc:n monitoimilaitteiden ja tulostimien ylläpitopalvelun (mukaan lukien eMaintenance Suite) kehittämiseen.

Saavuttamalla ISO/IEC 27001- ja ISO/IEC 27017 -sertifikaatit Canon Inc. pystyy vahvistamaan, että sen tietoturvaprosessit on sertifioitu kolmannen osapuolen toimesta kansainvälisesti tunnustetun standardin mukaisesti.

Kyseinen standardi osoittaa Canon Inc:n sitoutumisen tietoturvaan niin yrityksessä kuin myös pilvipalvelujen tarjonnassa:

- **Salassapidon turvaaminen** – tietoja voivat käyttää vain valtuutetut henkilöt.
- **Yhtenäisyyden turvaaminen** – tiedot ja prosessit ovat tarkkoja ja täydellisiä.
- **Saatavuuden turvaaminen** – valtuutetut käyttäjät saavat tiedot silloin, kun he niitä tarvitsevat.

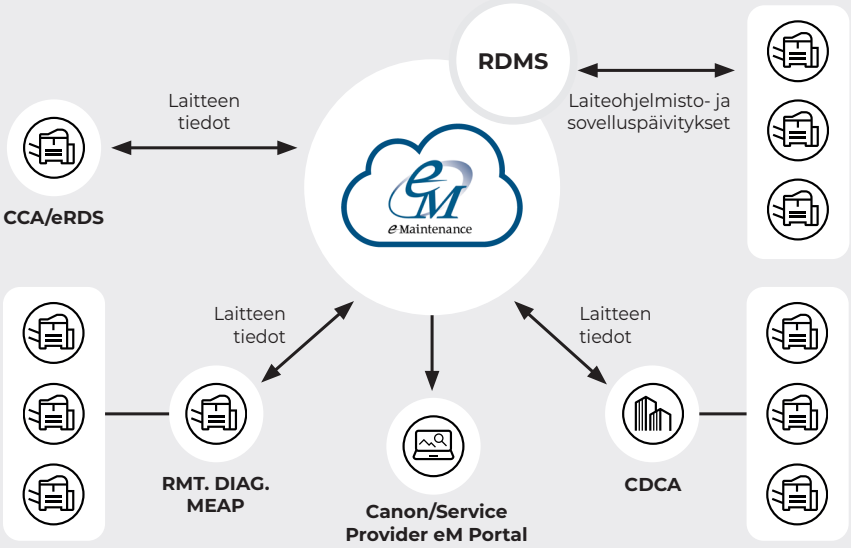
ISO/IEC 27001 edellyttää säännöllistä auditointia ja tarkoittaa, että eMaintenance eli Monitori-palvelun toimintoja kehittää ja toimittaa turvallinen organisaatio, joka on vahvistettu kolmannen osapuolen sertifioinnilla sovittujen kansainvälisten standardien mukaisesti.

Osa ISO/IEC 27001 -standardista sisältää ISO/IEC 27017 -standardin, joka määrittelee lisävaatimuksia pilvipalveluja tarjoavien yritysten tietoturvalle. Siinä hahmotellaan tietoturvakehys pilvipalveluja käyttäville organisaatioille.

Canon on päättänyt noudattaa näitä tietoturvavaatimuksia koskevia käytäntöjä, koska näin pilvipalveluasiakkaat voidaan pitää paremmin turvassa tarjoamalla heille johdonmukainen ja kattava lähestymistapa tietoturvaan.

TUNNUS

CCA – Cloud Connection Agent
CDCA – Canon Data Collection Agent
RMT. DIAG. MEAP – Remote Diagnostics MEAP
eRDS – embedded Remote Diagnostic System
RDMS – Remote Distribution & Management Service



OSA 2: eM-INFRASTRUKTUURIVAATIMUKSET

Canonin laitteiden ja eMaintenance eli Monitori-palvelun väliseen viestintään käytetään useita paikallisia ohjelmistoagentteja ja sovelluksia. Kullakin asiakkaalla voi olla käytössä yksi tai useampi näistä sovelluksista riippuen useista tekijöistä, joita ovat mm. laitteen tyyppi, paikallinen infrastruktuuri ja palveluvaatimukset.

Vaihtoehdot ovat seuraavat:

CCA (Cloud Connection Agent)

CCA on uudemman teknologian Monitori-järjestelmän agentti, joka toimii laitteen sisäisesti ilman, että verkkoon tarvitsee asentaa erillistä tiedonkeruuagenttia. Laitetietojen keräämistä varten tarvitaan CCA-yhteys, jotta voidaan hyödyntää kaikkia viimeisimpiä (ja tulevia) Monitori-järjestelmän toimintoja ja palveluita, kuten tekoälyyn perustuvaa ennakoivaa diagnostiikkaa ja korjausta. CCA-yhteys voidaan lisätä laitteisiin, joissa on eRDS.

CDCA (Canon Data Collection Agent)

Tämä on tietokoneeseen asennettava Monitori-palvelun agentti. Kyseinen valvontaohjelmisto asennetaan asiakkaan verkossa sijaitsevaan paikalliseen tietokoneeseen.

RMT. DIAG. MEAP (Remote Diagnostics MEAP)

Tämä on MEAP-alustaa käyttävään laitteeseen upotettu ohjelmisto, jota voidaan käyttää isäntälaitteen ja muiden verkossa olevien Canon-laitteiden valvontaan. Ihanteellinen ratkaisu pieniin verkkoihin, joissa ei tarvita CDCA-palvelinta.

eRDS (embedded Remote Diagnostic Service)

eRDS on laitteeseen upotettu Monitori-palvelun agentti. Tämä valvontaohjelmisto toimii sisäisesti itse laitteessa. eRDS lähettää laitteen hallintatietoja Monitori-palveluun ja se voidaan asettaa vastaanottamaan laiteohjelmisto- ja MEAP-sovelluslisenssipäivityksiä.

RDMS (Remote Distribution & Management Service)

Mahdollistaa valtuutettujen Canon-palveluntarjoajien tuotteiden ja MEAP-sovellusten ja iR-optioiden lisenssien hallinnan sekä laiteohjelmiston ja MEAP-sovelluslisenssien päivityksen.

Laiteasetusten backup-palvelu

Tämä lisäpalvelu luo pilvipalveluun ajastetun varmuuskopion sisäiselle kiintolevylle tallennetuista asetuksista salatussa muodossa. Jos kiinto- tai SSD-levyn ohjain vikaantuu ja vaatii vaihtoa, laitetietojen varmuuskopiointi palauttaa tiedot nopeasti laitteeseen, mikä lyhentää korjausaikaa merkittävästi.

Tarvittava verkkoyhteys

eMaintenance eli Monitori-palvelun toiminta edellyttää, että asiakkaita pyydetään antamaan Canon-laitteille pääsy verkon kautta tarvittaviin URL-osoitteisiin. Canon-edustajaltasi saat luettelon niistä URL-osoitteista, joita oma ympäristösi edellyttää.

YKSITTÄISET MONITORI-YHTEYDEN URL-OSOITTEET

Palomuurin rajoituselementtien suhteen Canon suosittelee yleismerkkien käyttöä. Esimerkkejä:
*.srv.ygles.com *.amazonaws.com
*.c-cdsknn.net *.ugwdevice.net

CCA	
hbp-ec1l.srv.ygles.com - Port 443	rgt.srv.ygles.com - Port 443
kinesis.eu-central-1.amazonaws.com - Port 443	camapi.srv.ygles.com - Port 443
cognito-identity.eu-central-1.amazonaws.com - Port 443	camapi-ec1.srv.ygles.com - Port 443
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com - Port 443 or Port 8883	hbpm-ec1l.srv.ygles.com - Port 443
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX ja uudemmat (vakiotila)	**CDCA v2.XX ja uudemmat (CCA-tila)**
rgt.srv.ygles.com	hbp-ec1l.srv.ygles.com
hbpm-ec1l.srv.ygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ec1.srv.ygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ec1.srv.ygles.com	a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com
camapi.srv.ygles.com	rgt.srv.ygles.com
camapis.srv.ygles.com	hbpm-ec1l.srv.ygles.com
mds-ec1.srv.ygles.com	camapi-ec1.srv.ygles.com
gdlp01.c-wss.com	camapis-ec1.srv.ygles.com
www-ec1.srv.ygles.com	camapi.srv.ygles.com
cam-ec1.srv.ygles.com	camapis.srv.ygles.com
	mds-ec1.srv.ygles.com
	gdlp01.c-wss.com
	www-ec1.srv.ygles.com
	cam-ec1.srv.ygles.com
RMT. DIAG. MEAP (CCA-tila v4.0 ja uudemmat)	**RMT. DIAG. MEAP (HTTP-tila)**
hbp-ec1l.srv.ygles.com	a01.ugwdevice.net - Port 443
kinesis.eu-central-1.amazonaws.com	b01.ugwdevice.net - Port 443
cognito-identity.eu-central-1.amazonaws.com	
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srv.ygles.com	
hbpm-ec1l.srv.ygles.com	
camapis-ec1.srv.ygles.com	
camapis.srv.ygles.com	
camapi-ec1.srv.ygles.com	
camapi.srv.ygles.com	
mds-ec1.srv.ygles.com	
eRDS	
a01.ugwdevice.net - Port 443	
b01.ugwdevice.net - Port 443	
cnvextdata-an1s.srv.ygles.com – portti 443 tarvitaan vain CCA-etäaktivointiin laitteissa, joissa on eRDS.	
RDMS	
device.c-cdsknn.net - Port 443	a02.c-cdsknn.net - Port 443
device02.c-cdsknn.net - Port 443	
Laitetietojen backup-palvelu	
hbp-ec1l.srv.ygles.com - Port 443	b01.ugwdevice.net - Port 443
kinesis.eu-central-1.amazonaws.com - Port 443	cnvextdata-an1s.srv.ygles.com - Port 443
cognito-identity.eu-central-1.amazonaws.com - Port 443	camapi-ec1.srv.ygles.com - Port 443
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com - Port 443 or Port 8883	camapis-ec1.srv.ygles.com - Port 443
rgt.srv.ygles.com - Port 443	camapi.srv.ygles.com - Port 443
hbpm-ec1l.srv.ygles.com - Port 443	camapis.srv.ygles.com - Port 443
a01.ugwdevice.net - Port 443	dcf-ec1.srv.ygles.com - Port 443

Helmikuu 2025 – versio 01

Canon Inc.
canon.com / canon.fi

Canon Europe
canon-europe.com / canon.fi

Finnish edition

Canon Oy
Huopalahdentie 24, PL 1
00351 Helsinki
puhelin 010 544 20
canon.fi