



Canon

CANON eMAINTENANCE İLE BİLGİ GÜVENLİĞİ

Canon'un eMaintenance hizmeti, sıkı güvenlik protokollerine bağlı olarak tüm ağa bağlı Canon MFP ve SFP cihazlarınızın yönetimini ve idaresini üstlenir.

BÖLÜM 1: SIK SORULAN SORULAR

Bu belgeyle, eMaintenance ile ilgili sorabileceğiniz temel güvenlik sorularını yanıtlamak amaçlanmaktadır. eMaintenance'a yerleşik haldeki güvenlik hakkında daha fazla bilgi için lütfen yerel Canon temsilcinizle iletişime geçin.



Verilerimin sahibi kim?

Her durumda verileriniz size aittir; Canon yalnızca müşterilerin eMaintenance verilerinin taraflarca kabul edilmiş veri işleyicisidir.



Verilerime kimler erişebilir?

Canon, verilere erişimi düzenlemek için aşağıdakileri içeren katmanlı bir yaklaşım sunar:

- **Fiziksel erişim kontrolleri:** Kişisel verilerin depolandığı tesislere, binalara veya odalara yalnızca yetkili kişilerin fiziksel olarak erişmesine izin verilir.
- **Sistem erişim kontrolleri:** Kişisel Verileri işleyen sistemlere yalnızca kullanıcı rollerine ve ilgili izinlere dayalı yetki ile erişilebilir.
- **Veri erişimi kontrolleri:** Veri işleme sistemlerini kullanma yetkisine sahip kişiler, yalnızca erişim hakkına sahip oldukları Kişisel Verilere erişebilir.
- **Veri iletim kontrolleri:** İlgili sözleşmeye uygun hizmetlerin sağlanması için gerekli olanlar dışında, Kişisel Veriler aktarım sırasında yetkilendirme olmadan okunmamalı, kopyalanmamalı, değiştirilmemeli veya kaldırılmamalıdır.
- **Veri girişi kontrolleri:** Canon, Canon'un veri işleme sistemlerinde Kişisel Verileri girme, değiştirme veya kaldırma işlemlerinin yapılıp yapılmadığını ve bu işlemler yapıldıysa kim tarafından yapıldığını geriye dönük olarak incelemek ve belirlemek için önlemler uygular.

- **İş kontrolleri:** Tüm Canon çalışanları ve sözleşmeli alt işleyiciler veya diğer hizmet sağlayıcıları, tüm hassas bilgilerin gizliliğinin korunması hususunda sözleşmeyle yükümlülük altındadır.
- **Veri ayırma kontrolleri:** Kişisel Veriler yalnızca her müşterinin kendi eMaintenance kiracısı üzerinde saklanır ve verilere yalnızca buradan erişilebilir.

Veri erişimi aşağıdaki önlemler kullanılarak kontrol edilir:

- Canon'un Güvenlik Politikasının bir parçası olarak, Kişisel Veriler, en az "gizli" bilgiler kadar sıkı bir güvenlikle korunur.
- Kişisel Verilere, bilgi sahibi olması gereken kişilerin erişmesine izin verilir. Görevini yerine getirmek için bilgi sahibi olması gereken personel verilere erişebilir.
- Kişisel Verileri işleyen uygulamaları koruyan güvenlik önlemleri düzenli olarak kontrol edilir. Bu amaçla Canon, kendi BT sistemlerinde dahili ve harici güvenlik kontrolleri ve sızma testleri gerçekleştirir.
- Kişisel Veriler; işleme, kullanım ve saklama sırasında izin alınmadan okunmamalı, kopyalanmamalı, değiştirilmemeli veya kaldırılmamalıdır.



Verilerim şifreleniyor mu?

AWS bulut hizmetinde saklanan veriler şifrelenir.

Canon ve müşterileri arasında veri aktarımı yapılırken bu işlem, her zaman güvenli şifreleme aktarım protokolleri üzerinden gerçekleştirilir.

İsteğe bağlı Veri Yedekleme Hizmeti veya Kurulum Destek Hizmeti kullanılarak depolanabilen cihaz adres defteri verileri gibi kişisel veriler, AES-256 kullanılarak şifrelenir.



Verilerim diğer müşterilerin verilerinden nasıl ayrılıyor?

Kişisel Veriler, aşağıdaki ayırma kontrolleri kullanılarak işlenir:

Canon, müşteri verilerinin mantıksal olarak ayrılmasını sağlamak için uygun teknik kontrollerden faydalanır.

Uygulanabildiği durumlarda, çok katmanlı ağaç yapısı, bir üst kiracının kendi alt kiracılarına erişebilmesini sağlar ancak alt kiracılar aynı düzeydeki veya daha üst düzeydeki (örneğin üst kiracılar) kiracılara erişemez.



eMaintenance tarafından hangi veriler toplanır?

eMaintenance tarafından toplanan ve kullanılan verilerin çoğunluğu müşteri, cihaz adı, seri numarası, konum, IP adresi, durum ve uyarılar gibi kimliği açıkça çıkarmayacak cihaz verileridir.

Şu bilgiler eMaintenance tarafından toplanmaz: Kullanıcı adı*, tarih/saat, belge adı, KOPYALAMA, YAZDIRMA, TARAMA ve GÖNDERME işlemlerinin yapıldığı iş içerikleri (görüntü verileri/yazdırma verileri) gibi kullanıcının operasyonlarıyla ilgili bilgiler.



Canon kendi bulut güvenliğini denetliyor mu?

Canon, kendisinin ve müşterilerinin bulut hizmetlerini güvenle kullanabilmesini sağlamak amacıyla, sunduğu bulut hizmetlerinin bilgi güvenliği uygulama durumunun göstergeleriyle ilgili çeşitli denetimler gerçekleştirir.

eMaintenance güvenlik önlemlerini doğrulamak için üçüncü bir tarafça düzenli olarak sızma testleri gerçekleştirilir.

*İsteğe bağlı Veri Yedekleme Hizmeti veya Kurulum Destek Hizmetinin kullanıldığı durumlarda, yalnızca müşteriyle özel anlaşma yapılması koşuluyla, cihaz adres defterinde bulunan kullanıcı adı ve e-posta adresi gibi kişisel veriler toplanabilir.





eMaintenance bulut altyapısı güvenli mi?

eMaintenance hizmeti, Almanya'nın Frankfurt şehrinde bulunan AWS platformunda barındırılmaktadır.



eMaintenance'ın başlıca güvenlik standartlarından herhangi birine uygun bir sertifikası var mı?

Canon Inc. Dijital Baskı Geliştirme Merkezi, uluslararası ISO/IEC 27001 standardı sertifikasına sahiptir. Alınan sertifika, Canon Inc.'nin Çok İşlevli Cihazlar (MFD) ve Yazıcılar için İzleme Hizmeti (eMaintenance Paketi dahil) geliştirmesiyle ilgilidir.

ISO/IEC 27001 ve ISO/IEC 27017 sertifikalarıyla Canon Inc., kendi güvenlik süreçlerinin uluslararası düzeyde kabul gören bir standarda göre üçüncü taraflarca sertifikalandığını teyit edebilmektedir.

Bu standart, Canon Inc.'nin şirket içinde ve sunduğumuz çevrimiçi hizmetlerde bilgi güvenliğine bağlılığını göstermektedir:

- **Gizlilik:** Bilgilere yalnızca erişim yetkisi olan kişilerin erişebilmesini sağlama.
- **Bütünlük:** Bilgilerin ve işleme yöntemlerinin doğruluğunu ve eksiksizliğini korumaya alma.
- **Ulaşılabilirlik:** Yetkili kullanıcıların gerektiğinde bilgilere erişebilmesini sağlama.



ISO/IEC 27001 düzenli incelemeyi zorunlu kılmaktadır ve bu zorunluluk, İzleme Hizmeti işlevlerinin, kabul edilen uluslararası standartlara göre üçüncü taraf sertifikasyonu ile onaylanmış güvenli bir kuruluş tarafından geliştirilip sunulduğu anlamına gelir.

ISO/IEC 27001'in bir kısmı, özellikle bulut hizmeti sağlayıcıları için ek güvenlik kontrollerini tanımlayan ISO/IEC 27017'yi içerir. Bulut hizmetlerini kullanan kuruluşlar için bilgi güvenliği çerçevesini ana hatlarıyla ortaya koyar.

Canon, bilgi güvenliğine ilişkin tutarlı ve kapsamlı bir yaklaşım getirerek bulut hizmeti müşterilerini daha güvende tutması nedeniyle bilgi güvenliği kontrollerine yönelik bu uygulama kurallarına uymayı tercih etmiştir.

ÖNEMLİ

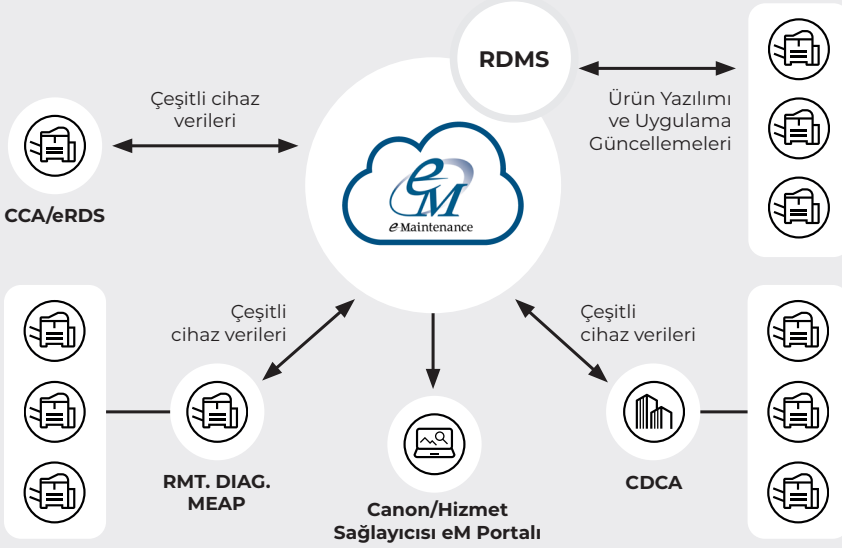
CCA: Bulut Bağlantı Aracısı

CDCA: Canon Veri Toplama Aracısı

RMT, DIAG, MEAP: Uzaktan Tanılama MEAP

eRDS: Gömülü Uzaktan Tanılama Sistemi

RDMS: Uzaktan Dağıtım ve Yönetim Hizmeti



BÖLÜM 2: eM ALTYAPISI GEREKLİLİKLERİ

eM, Canon cihazları ile eM hizmeti arasında sağlanan iletişim için çeşitli yerel araçlar ve yazılım uygulamaları kullanır. Cihaz türü, yerel altyapı kurulumu ve hizmet gerekliliği gibi çeşitli faktörlere bağlı olarak, her müşteri bunlardan birini veya daha fazlasını etkinleştirmiş olabilir.

Seenekler ařađıdaki gibidir:

CCA (Bulut Bađlantı Aracısı)

CCA, eMaintenance'a ait en g¼ncel cihaza g¼m¼l¼ aracıdır ve ađınızda ayrı bir veri toplama aracısı y¼klemeye gerek kalmadan cihazda dahili olarak alıřır. Farklı t¼rlerde cihaz verilerini toplayabilmesi nedeniyle CCA bađlantısı, yapay zeka tabanlı Tahmine Dayalı Tanılama ve Onarım dahil olmak ¼zere en g¼ncel (ve gelecekteki) eMaintenance iřlevleri ile hizmetlerinden yararlanmak aısından gereklidir. CCA, eRDS alıřtıran mevcut cihazlara eklenebilir.

CDCA (Canon Veri Toplama Aracısı)

eMaintenance'a y¼nelik, bilgisayara y¼klenen bir aracıdır. Bu izleme yazılımı, m¼řterinin ađındaki yerel bir bilgisayara y¼klenir.

RMT. DIAG. MEAP (Uzaktan Tanılama MEAP)

eMaintenance'a y¼nelik bu cihaza g¼m¼l¼ aracı yazılımı, ana cihazı ve ađdaki diđer Canon cihazlarını izleme iřlevine sahip MEAP platformunu kullanır. CDCA sunucusu gerektirmeyen k¼¼k ađlar iin idealdir.

eRDS (G¼m¼l¼ Uzaktan Tanılama Hizmeti)

eRDS, eMaintenance'a y¼nelik eski bir cihaza g¼m¼l¼ aracıdır. Bu izleme yazılımı, cihaz ¼zerinde dahili olarak alıřır. Cihaz y¼netimi bilgilerini eMaintenance hizmetine g¼nderen eRDS, ¼r¼n yazılımı ve MEAP uygulama lisansı g¼ncellemelerini alacak řekilde ayarlanabilir.

RDMS (Uzaktan Dađıtım ve Y¼netim Hizmeti)

Yetkili Canon Hizmet sađlayıcılarının, MEAP uygulamaları ile iR seeneklerinin ¼r¼n ve lisanslarını y¼netmenin yanı sıra ¼r¼n yazılımı ve MEAP uygulama lisanslarını g¼ncellemesine imkan tanır.

Veri Yedekleme Hizmeti

Bu isteđe bađlı hizmet, dahili depolama cihazında saklanan ayarları řifrelenmiř bir biimde d¼zenli olarak buluta yedekler. Deđiřtirmeyi gerektiren HDD/SSD/ Denetleyici arızası durumunda, Veri Yedekleme Hizmeti, verileri cihaza geri y¼kleyerek onarım s¼resini b¼y¼k ¼l¼de kısaltabilir.

Gerekli Ađ Eriřimi

eMaintenance'ın iřlevlerinin alıřması iin m¼řterilerden Canon cihazlarının bulunduđu kendi ađları ¼zerinden ilgili URL'lere eriřim izni vermesi istenir. L¼tfen ortamınız iin gereken belirli URL'lerin listesini Canon temsilcinizden ¼đrenin.

ÇEŞİTLİ eMAINTENANCE BAĞLANTI URL'LERİ

Canon, Güvenlik Duvarı istisnalarında
aşağıdakiler gibi joker karakterlerin
kullanılmasını önerir:

*.srv.ygles.com *amazonaws.com
*c-cdsknn.net *.ugwdevice.net

CCA	
hbp-ec1.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
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com - Port 443 veya Port 8883	hbpm-ec1.srv.ygles.com - Port 443
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX ve üstü (standart Mod)	CDCA v2.XX ve üstü (CCA Modu)
rgt.srv.ygles.com	hbp-ec1.srv.ygles.com
hbpm-ec1.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	a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com
camapi.srv.ygles.com	rgt.srv.ygles.com
camapis.srv.ygles.com	hbpm-ec1.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 için (CCA modu v4.0 ve üstü)	RMT, DIAG, MEAP (HTTP Modu)
hbp-ec1.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	
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srv.ygles.com	
hbpm-ec1.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-anls.srv.ygles.com Port 443, yalnızca eRDS bulunan mevcut cihazlarda CCA'nın uzaktan etkinleştirilmesi için gereklidir	
RDMS için	
device.c-cdsknn.net - Port 443	a02.c-cdsknn.net - Port 443
device02.c-cdsknn.net - Port 443	
Veri Yedekleme Hizmeti için	
hbp-ec1.srv.ygles.com - Port 443	b01.ugwdevice.net - Port 443
kinesis.eu-central-1.amazonaws.com - Port 443	cnvextdata-anls.srv.ygles.com - Port 443
cognito-identity.eu-central-1.amazonaws.com - Port 443	camapi-ec1.srv.ygles.com - Port 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com - Port 443 ali 8883	camapis-ec1.srv.ygles.com - Port 443
rgt.srv.ygles.com - Port 443	camapi.srv.ygles.com - Port 443
hbpm-ec1.srv.ygles.com - Port 443	camapis.srv.ygles.com - Port 443
a01.ugwdevice.net - Port 443	dcf-ec1.srv.ygles.com - Port 443

Şubat 2025 - V.01

Canon Inc.
canon.com

Canon Avrupa
canon-europe.com

Turkish edition
© Canon Europa N.V. 2025

Canon Eurasia

Istanbul
Görüntüleme ve Ofis Sistemleri A.S.
Degirmen Sokak Nida Kule İş Merkezi No:18/10
K:1 Kozyatağı 34742 Kadıköy/Istanbul
Tel: +90 (216) 571 68 00
+90 (216) 706 73 76

Canon