



OFISİNİZİ KORUYUN

Canon



OFİSİNİZDEKİ BİLGİLER NE KADAR GÜVENDE?

Günümüzde şirketler yüksek miktarda bilgi kullanıyor ve bağlı teknolojiler, süreçler, kişiler ve kuruluşlardan oluşup ulusal sınırların dışına çıkan karmaşık ağlar oluşturuyor. Ortaya çıkan çevik yeni iş uygulamaları, hem ofisi hem de kişilerin bilgi oluşturma, paylaşma ve tüketme yollarını yeniden şekillendiriyor. Bu karmaşık ortamda verileri güvenceye almak hiç olmadığı kadar zor hale geldi. Çoğu şirket sağlam güvenlik duvarları, güncel antivirüs koruması ve güvenlik yazılımı gibi gelişmiş teknolojilere yatırım yapıyor. Ancak bu korumanın ofis yazıcılarını da kapsamaması gerektiğini sıklıkla unutarak sandıklarından daha büyük bir güvenlik açığı bırakıyorlar.



YAZICILARINIZI DÜŞÜNÜN

Modern çok işlevli yazıcılar (MFP'ler) güçlü araçlar haline geldi. Tıpkı bilgisayarlar ve sunucular gibi onların da işletim sistemleri ve devasa sabit disk sürücülerini var, hem ağa hem de internete bağlanıyorlar ve her gün çok sayıda kritik iş belgesini işlemek üzere ortaklaşa kullanılıyorlar.



RİSKLER NELERDİR?

- Korumasız MFP'lerde depolanan hassas bilgileri yetkisiz kullanıcıların görüntülemesi
- Yanlış kullanım nedeniyle yazdırma altyapınızın kullanılabilirliğinin tehlikeye düşmesi
- Kötü amaçlı yabancıların yazıcı üzerinden ağınıza erişim kazanıp ağınızı başka saldırılar için kullanması
- Yazdırma işleminden sonra çıkış tepsisinde unutulmuş gizli belgelerin açığa çıkması
- Farklı kullanıcılara ait yazdırılmış materyallerin karışması
- Yazım hataları nedeniyle belgelerin faks veya e-posta ile yanlış alıcılara gönderilmesi
- Bilgisayar korsanlarının iletilen yazdırma veya tarama verilerini ele geçirmesi
- Kullanım süresi dolan yazıcıların dikkatsizce bertaraf edilmesi sonucunda veri kaybı yaşanması.

"Yüksek miktarda veri yönettiğiniz ofisinizde bilgi güvenliğinin temel standartlarını benimsemek, karşılığını fazlasıyla alacağınız bir önlemdir. Yazıcılar bugünlerde sıradan makineler olmaktan çıkıp yazdırma işlevi de olan sunucular haline geldi."

(CISO, Publicis Groupe)

ŞİRKETİNİZ İÇİN GÜVENLİ YAZDIRMA ÇÖZÜMLERİ

Tasarımdan gelen güvenlik ve gizlilik

Teknolojileri, ürünleri ve hizmetleri müşterilerimiz için tasarlarken ya da seçerken bunların bilgi güvenliği açısından müşterilerimizin ortamı üzerindeki etkilerini dikkate alıyoruz. Bu yüzden çok işlevli ofis yazıcılarımızda, her büyüklükten şirketin aşağıdakiler için istediği düzeyde korumaya ulaşmasını sağlayan çok çeşitli güvenlik özellikleri hem standart hem opsiyonel olarak bulunuyor:



CİHAZLAR



AĞLAR



BELGELER



KURULUŞUNUZ



**ULUSLARARASI ALANDA
TANINAN STANDARTLAR
VE SERTİFİKALAR**

imageRUNNER ADVANCE çok işlevli yazıcılarımız, Basılı Kopya Cihaz Koruması Profili (HCD_PP) veya IEE P2600.2 Koruma Profili uyarınca Ortak Kriter yöntemi kullanılarak düzenli olarak değerlendirilir ve onaylanır.



**GÜVENLİK
TESTİ**

Canon, bu iş için ofis ekipmanı sektöründeki en zorlu güvenlik testi yöntemlerinden birini kullanır. Ürün portföyümüzde kullanılan teknolojiler de kendi çözümlerimizden beklediğimiz aynı yüksek standartlı testlerden geçer.

Ofis ve şirketler için yenilikçi baskı ve bilgi yönetimi çözümleri geliştirmede sektör lideri olan Canon, müşterileriyle birlikte çalışarak ofis teknolojimizin, geniş bilgi ekosistemlerinin parçası olarak güvenlik açısından doğurduğu sonuçları göz önünde bulunduran, kapsamlı bir bilgi güvenliği yaklaşımı benimsemelerine yardımcı oluyor.



CİHAZINIZI KORUYUN

Fiziksel varlıklarınız için kapsamlı koruma



KULLANICI KİMLİK DOĞRULAMASI ÇÖZÜMLERİ

Kimlik doğrulaması aracılığıyla kullanıcı erişim kontrolünü uygulamaya koyarak cihazınızı yetkisiz kullanıma karşı koruyun. Bu çözüm ayrıca kullanıcıların tercih ettikleri ayarlara ve yazdırma işlerine hızla erişmelerini sağlarken hesap verilebilirliği ve kontrolü de geliştirir. Departman yazıcılarımızda Universal Login Manager adlı esnek bir oturum açma çözümü bulunur. Bu çözüm, cihazda oluşturulan bir kullanıcı veri tabanı ile kullanıcı kimlik doğrulaması yapmayı ve Active Directory ya da uniFLOW sunucusu aracılığıyla etki alanı kimlik doğrulaması yapmayı sağlar. Böylece şirketler cihaz erişimini kontrol etme fırsatını yakalarken kullanım rahatlığı ile güvenlik arasında doğru dengeyi kurabilir.



CİHAZ YÖNETİM KONTROLÜ

Ağ ayarları gibi cihaz yapılandırması öğeleri ve diğer kontrol seçeneklerine yalnızca yönetici önceliklerine sahip kullanıcılar erişebilir. Böylece bilinçli ya da istemeden yapılan değişikliklerin önüne geçilmiş olur.



ÖNLEYİCİ GÜVENLİK

imageRUNNER ADVANCE ürünleri, yazıcıları saldırılardan koruyan çeşitli güvenlik ayarları sunar. Güvenli Önyükleme cihaz entegrasyonu sağlarken Syslog verileri, cihazın güvenlik durumu hakkında gerçek zamanlı bilgiler sunar (Veriler uygun bir üçüncü taraf SIEM sistemi tarafından okunabilir).



ERİŞİM YÖNETİM SİSTEMİ

Bu özellik, cihaz işlevlerine erişimin parçalı olarak kontrol edilmesini sağlar. Yöneticiler mevcut standart rolleri kullanabileceği gibi istenen düzeyde erişim önceliklerine sahip özel roller de oluşturabilir. Örneğin, belirli kullanıcıların belge fotokopisi çekmesi ya da gönderme işlevini kullanması engellenebilir.



GÜVENLİK POLİTİKASI AYARI

En yeni imageRUNNER ADVANCE cihazlarda da bir güvenlik politikası işlevi bulunur. Bu işlev, yöneticinin güvenlikle ilgili tüm ayarlara tek menüden erişmesini ve bunları makineye uygulamadan önce düzenlemesini sağlar.

Ayarlar uygulandıktan sonra cihaz kullanımı ve ayar değişiklikleri politikaya uygun olmak zorundadır. Güvenlik politikası ayrı bir parolayla korunabilir; böylece bu alana yalnızca BT güvenliği çalışanlarının erişmesi sağlanarak ek bir kontrol ve güven düzeyi eklenmiş olur.



CİHAZ DEPOLAMA MEDYASINDAKİ VERİLERİN KORUNMASI

Çok işlevli yazıcılar, yazdırılmayı bekleyen yazdırma işlerinden alınmış fakslar, taranmış veriler, adres defterleri, aktivite günlükleri ve iş geçmişine kadar çok miktarda veri içerir ve bu verilerin korunması gerekir. Canon cihazları, cihazın kullanım ömrünün her aşamasında verilerinizi koruyup verilerin gizliliğini, doğruluğunu ve uygunluğunu sağlamak için bir dizi önlem sunar.

Cihazın belirli modeline bağlı olarak sabit disk sürücüsü (HDD) veya katı hal sürücüsü (SSD) kullanılır. HDD, verilerin üzerine kaydedildiği fiziki olarak dönen bir tabla kullandığından verilerin etkili şekilde üzerine yazıldığından emin olmak için birden fazla üzerine yazma işlemi (genellikle üç) gerekir. HDD'nin aksine SSD, verileri mevcut bellek alanında taşıyarak bellek hücrelerinde eşit seviyede elektrik aşınması olduğundan emin olur. Her bir hücre üzerine sınırlı sayıda yazma işlemi gerçekleştirilebilir ve bu "KIRPMA" işlemi SSD'nin kullanım ömrünü en üst seviyeye çıkarırken "mantıksal olarak silinen" verilerin de üzerine yazar.

imageRUNNER ADVANCE, üzerine yazma işleminin gerçekleştirilmesini ve üzerine yazma yöntemini ayarlayacak şekilde yapılandırılabilen farklı pek çok yapılandırma seçeneği sunar.



CİHAZLARINIZ NE KADAR GÜVENDE?

1

Cihazlarınız ortak alanlarda bulunuyor ve paylaşıyor mu?

2

Kullanıcılar cihazlara güvensiz erişim elde edebiliyor mu?

3

Cihaz sabit diskinde bulunan bilgileri korumak için almış olduğunuz önlemler var mı?

4

Yetkisiz kullanıcılar cihaz ayarlarını değiştirebiliyor mu?

5

Cihazınızın yaşam döngüsünü ve güvenli bir şekilde nasıl bertaraf edileceğini düşündünüz mü?

DİSK ŞİFRELEME

imageRUNNER ADVANCE cihazlarımız, güvenliği geliştirmek için sabit disk sürücüsündeki tüm verileri şifreler. Veri şifrelemesini gerçekleştiren güvenlik yongası, ABD hükümeti tarafından belirlenen FIPS 140-2 Seviye 2 güvenlik standardıyla uyumludur ve ABD ile Kanada tarafından kurulan Kriptografik Modül Doğrulama Programının (CMVP) yanı sıra Japonya Kriptografik Modül Doğrulama Programı (JCMVP) sertifikasına sahiptir.

VERİ DEPOLAMASINI SİLME

Kopyalanmış veya taranmış görüntü verileri ile bilgisayardan yazdırılan belge verileri gibi bazı veriler, sabit disk sürücüsünde veya katı sürücüsünde yalnızca geçici olarak depolanır ve işlem tamamlandıktan sonra silinir. Atık veri kalmadığından emin olmak için cihazlarımız, işlerin yürütülmesinin bir parçası olarak atık verilerin düzenli olarak silinmesi işlevine sahiptir.

TÜM VERİLERİ VE AYARLARI SIFIRLAMA

Sabit diski değiştirirken veya bertaraf ederken veri kaybını önlemek amacıyla sabit diskteki tüm belgelerin ve verilerin üzerine yazabilir ve makine ayarlarını varsayılanlara geri yükleyebilirsiniz.

SABİT DİSK YANSITMA*

Şirketler ek bir opsiyonel sabit disk kullanarak cihazlarının sabit diskindeki verileri yedekleme imkanına sahiptir. Yansıtma işlemi gerçekleştirilirken iki sabit disk sürücüsündeki veriler tamamen şifrelenir.

*Opsiyonel. Özellikler ve seçeneklerin ofis yazdırma portföyü genelinde kullanılabilirliği hakkında ayrıntılı bilgi almak için lütfen Canon temsilcinizle görüşün.



AĞINIZI GÜVENLİ HALE GETİRİN



YAZICINIZ AĞINIZI TEHLİKEYE ATIYOR OLABİLİR Mİ?

- Ağ bağlantı noktalarını saldırıya açık mı bırakıyorsunuz?
- Misafirler ağınıza riske sokmadan yazdırma ve tarama yapabiliyor mu?
- "İşe kendi cihazını getir" politikalarınız güvenli ve desteklenebilir mi?
- Yazdırma verisi akışları bilgisayardan çıkış cihazına kadar şifreleniyor mu?
- Yazdırma ve tarama verileri iletim sırasında güvende oluyor mu?

Canon, ađınızı ve verilerinizi hem i hem de dıř saldıřılardan korumak iin eřitli gvenlik ozmleri sunuyor.

IP VE MAC ADRESİ FİLTRELEME

Giden ve gelen iletiřim iin yalnızca belirli bir IP veya MAC adresine sahip cihazlarla iletiřime izin vererek ađınızı nc tarafların yetkisiz eriřiminden koruyun.

PROXY SUNUCUSU YAPILANDIRMASI

İletiřimi makinenizin yerine stlenmesi ve ađın dıřındaki cihazlara bađlanılırken kullanılması iin bir proxy oluřturun.

IEEE 802.1X KİMLİK DOĐRULAMA

Yetkisiz ađ eriřimi, yalnızca kimlik dođrulama sunucusunun onayladıđı istemci cihazlara eriřim önceliđi veren bir LAN anahtarı tarafından engellenir.

IPSEC İLETİŐİMİ

IPSec iletiřimi, IP ađı zerinden gnderilen IP paketlerinin nc taraflarca ele geirilmesini veya deđiřtirilmesini engeller. Makine ve bilgisayar gibi diđer cihazlar arasında paylařılan verilerin dinlenmesini, yanıtılmasını ve kurcalanmasını engellemek iin TLS Őifreli iletiřimi kullanın.

BAĐLANTI NOKTASI KONTROL

Bađlantı noktalarını gvenlik politikası ayarınızın parası olarak yapılandırın.

OTOMATİK SERTİFİKA KAYDI

Bu zellik, gvenlik sertifikalarını ynetme iřini nemli lde kolaylařtırır. Sistem yneticisi, sektrce tanınan teknolojiyi kullanarak sertifikaları otomatik olarak gncelleyip yayınlayabilir; bylece gvenlik politikalarının her zaman karřılandıđından emin olur.

KAYIT İZLEME

eřitli kayıtlar, engellenmiř iletiřim istekleri de dahil olmak zere cihazınızın vresindeki aktiviteleri izlemenizi sađlar.

WI-FI DIRECT

Mobil cihazın ađınıza eriřmesine gerek olmadan mobil yazdırma zelliđini kullanabilmek iin eřler arası bađlantıyı etkinleřtirin.

CİHAZA VE CİHAZDAN İLETİLEN VERİLER İİN ŐİFRELEME

Bu seenek, kullanıcı bilgisayarından ok iřlevli yazıcıya iletilen yazdırma iřlerini Őifreler. Evrensel gvenlik zelliđi seti etkinleřtirildiđi zaman PDF formatındaki taranmıř veriler de Őifrelenebilir.

MOBİL MİSAFİR YAZDIRMA

Gvenli ađ yazdırma ve tarama ynetimi yazılımımız, e-posta, web ve mobil uygulama zerinden harici iř gnderme yolları sađlayarak mobil ve misafir yazdırma ile iliřkili yaygın gvenlik risklerini zer. Bu, MFD'yi gvenli bir kaynađa kilitleyerek saldırı vektrlerini en aza indirir.



BELGELERİNİZİ KORUYUN

Tüm şirketler sözleşmeli anlaşmalar, personel bordro bilgileri, müşteri verileri ve araştırma-geliştirme planları gibi birçok hassas belgeyle çalışır. Belgelerin yanlış ellere geçmesi, itibar kaybından ağır para cezaları ve hatta yasal işlemlere kadar birçok sonuç doğurabilir.

Canon, hassas belgelerinizi yaşam döngüleri boyunca koruyacak çeşitli güvenlik çözümleri sunar.



YAZDIRILMIŞ BELGELER İÇİN GİZLİLİK

Güvenli yazdırma

Kullanıcı, yazdırma işi için bir PIN kodu belirleyebilir; bu sayede doğru PIN kodu makineye girilmeden belge yazdırılmaz. Bu, kullanıcıların gizli kabul ettikleri belgeleri güvenceye almasını sağlar.

Tüm yazdırma işlerini tutma

imageRUNNER ADVANCE'de yönetici tüm gönderilmiş yazdırma işlerinin tutulmasını sağlayabilir; bu durumda yazdırılan tüm materyallerin gizliliğini korumak için işler yazdırılmadan önce kullanıcıların oturum açması gerekir.

Posta kutuları

Yazdırma işleri veya taranmış belgeler, daha sonraki bir aşamada erişilmek üzere posta kutusunda depolanabilir. Posta kutularının içindeki içeriği yalnızca kendilerine atanmış kullanıcıların görüntüleyebilmesi için posta kutuları PIN koduyla korunabilir. Makinedeki bu güvenli alan, sık sık yazdırılması (ör. formlar) fakat dikkatlice yönetilmesi gereken belgeleri saklamaya uygundur.

uniFLOW güvenli yazdırma*

uniFLOW MyPrintAnywhere güvenli yazdırma sayesinde kullanıcılar yazdırma işlerini evrensel sürücü üzerinden gönderip ağ üzerindeki herhangi bir yazıcıdan alabilir.



BELGELERİN KOPYALANMASINA KARŞI CAYDIRICI VEYA ENGELLEYİCİ ÖNLEMLER

Görünür filigranlarla yazdırma

Sürücüler, sayfada belge içeriğinin yukarısına veya arkasına görünür işaretler yazdırma özelliğine sahiptir. Bu, kullanıcılar arasında belgenin gizliliği hakkında farkındalık oluşturarak kopyalamaktan caydırır.

Görünmez filigranlarla yazdırma/kopyalama

Bu seçenek etkinleştirildiğinde belgeler arka plana gömülmüş gizli metinlerle yazdırılabilir veya kopyalanabilir; belge kopyalandığı zaman görünür hale gelen yazı, caydırıcı işlev görür.

BELGELERİNİZ NE KADAR GÜVENDE?

1

Yetkisiz kullanıcıların yazıcıdaki hassas belgelere erişmesi engelleniyor mu?

2

Paylaşılan cihazdan geçen kullanıcı belgelerinin hepsinin gizliliğinin korunduğundan emin misiniz?

3

Birileri hassas belgeleri yazıcınızdan alabilir mi?

4

Cihazdan belge gönderirken yapılan yaygın hataları önleyebiliyor musunuz?



BELGE GÖNDERME VE FAKSLAMA İŞLEMLERİNİN KONTROLÜNÜ SAĞLAYIN

Gönderme hedeflerini sınırlandırma

Bilgi sızıntısı riskini azaltmak için yöneticiler, kullanılabilir gönderme hedeflerini adres defteri veya LDAP sunucusundaki adreslerle, oturum açan kullanıcının adresiyle veya belirli etki alanlarıyla sınırlandırabilir.

Otomatik adres tamamlamayı devre dışı bırakma

E-posta adreslerinin otomatik olarak tamamlanmasını devre dışı bırakarak belgelerin yanlış hedeflere gönderilmesini önleyin.

Adres defteri koruması

Cihazın adres defterini kullanıcıların yetkisiz olarak düzenlemesine karşı korumak için bir PIN kodu belirleyin.

Faks numarası onayı

Kullanıcıların faks göndermeden önce faks numarasını iki kez girmelerini şart koşarak belgelerin yanlış alıcılara gönderilmesini önleyin.

Alınan faksların gizliliği

Makineyi belgeleri yazdırmadan, bellekte depolayacak şekilde ayarlayın. Dilerseniz bir gizli gelen kutusunu depolama konumu olarak ayarlamak ve PIN kodları belirlemek için koşullar uygulayarak alınan faks belgelerinin gizliliğini de koruyabilirsiniz.



BELGE KAYNAĞINI VE ORJİNALLİĞİNİ DİJİTAL İMZALARLA DOĞRULAYIN

Cihaz imzası

PDF veya XPS formatında taranmış belgelere, anahtar veya sertifika mekanizması kullanarak cihaz imzası uygulanabilir; bu sayede alıcı belgenin hem kaynağını hem de orijinalliğini doğrulayabilir.

Kullanıcı imzası*

Bu seçenek, kullanıcıların bir PDF veya XPS dosyasını sertifika yetkilisinden alınan özel dijital kullanıcı imzasıyla göndermesini sağlar. Bu sayede alıcı, belgeyi hangi kullanıcının imzaladığını doğrulayabilir.

*Opsiyonel. Özellikler ve seçeneklerin ofis yazdırma portföyü genelinde kullanılabilirliği hakkında ayrıntılı bilgi almak için lütfen Canon temsilcinizle görüşün.



KURUMSAL BİLGİ GÜVENLİĞİ

Canon, kuruluşunuzun genel bilgi korumasına katkıda bulunabilir.



UÇTAN UCA YAKALAMA VE ÇIKTI İHTİYAÇLARINIZ İÇİN TAM KONTROL

Modüler çıktı yönetimi yazılımımızla şirketler, ağ cihazlarını güvenli bir şekilde paylaşarak yazdırma işlerini çıktı yönetimi sunucusuna bağlı olan herhangi bir yazıcıda güvenli bir şekilde gerçekleştirebilir. Mobil kullanıcılar da merkezi olarak kontrol edilen bir sunucu tarafından desteklenir. Bu sunucuda hem şirket içi hem de misafir kullanıcılar, mobil cihazlardan yazdırma işlemine güvenli bir şekilde erişebilir. Kurumsal yakalama ihtiyaçları için tarama modülü, belgelerin yakalanmasını, sıkıştırılmasını, dönüştürülmesini ve çok işlevli cihazdan bulut tabanlı sistemler de dahil olmak üzere çok çeşitli hedeflere dağıtılmasını sağlar. Ayrıca yazdırma işlerini güvenli bir şekilde en uygun yazıcıya yönlendirerek her bir belge için yazdırma maliyetini optimize edebilirsiniz. Çözümümüz, şirketiniz genelinde belge güvenliğini geliştirirken belgelerin eksiksiz bir şekilde hesabını tutarak kullanıcı, cihaz ve departman aktivitelerinin tamamen şeffaf olmasını sağlar.



MERKEZİ FİLO YÖNETİMİ

Cihaz yönetimi yazılımımız IW MC; cihaz ayarları, güvenlik politikaları, parolalar, sertifikalar ve ürün yazılımlarının ağdaki Canon cihazları filonuza gönderilip bu cihazların güncellenmesini sağlayarak BT ekibinize zaman kazandırır ve yazdırma altyapınızın güvenliğinin güncel kalmasını sağlar.



YAZDIRMA HİZMETLERİ YÖNETİMİ

Canon MPS, yenilikçi teknoloji ve yazılımı doğru hizmetlerle birleştirerek istediğiniz yazdırma ve belge deneyimini, BT ekiplerinize zahmet yaratmadan sağlayabilir. Proaktif yönetim ve yazdırma altyapınız ile belge iş akışlarınızın sürekli optimizasyonu aracılığıyla güvenlik hedeflerinize ulaşırken maliyet optimizasyonu sağlayıp üretkenliği şirket genelinde artırmanıza yardımcı olabiliriz.



ÖZEL GELİŞTİRME

Şirket içi geliştirici ekibimiz, durumunuza veya özel gereksinimlerinize uygun özel bir çözüm sunup geliştirebilir.

KURUMSAL GÜVENLİK YAKLAŞIMINIZ NE KADAR KAPSAMLI?

- Güvenlik politikanız çok işlevli cihaz filonuzu da kapsıyor mu?
- Yazdırma altyapınızın güncel kalmasını ve geliştirmeler ile hata düzeltmelerinin zamanında ve etkili bir şekilde uygulanmasını nasıl sağlıyorsunuz?
- Misafirler ağınıza riske sokmadan yazdırma ve tarama yapabiliyor mu?
- "İşe kendi cihazını getir" politikaları yazdırma filonuz genelinde güvenli ve desteklenebilir mi?
- BT ekibiniz güvenlik endişelerini araştırmak için yeterli zamana sahip mi?
- Güvenliğin sağlanması ile kullanım rahatlığı arasında doğru dengeye sahip misiniz?



NEDEN CANON?

Canon, görüntüleme demektir. Bu görüntülemeyi bir fark yaratmak ve değişime yön vermek için kullanıyoruz.

Dijital dönüşümden geçen ve yeni yöntemlerle çalışan müşterilerimizi düşünüyoruz. Kurumsal mirasımızın ve kültürümüzün bir parçası olarak devam eden sürdürülebilirlik odağımız ile daha kapsamlı bir toplumsal değişim sağlamayı hedefliyoruz.

Son olarak yeni pazarlara, ürünlere ve teknolojilere yatırım yaptığımızdan müşterilerimize, çalışanlarımıza ve toplumun daha geniş bir kesimine uzun vadede fayda sağlamak için buradayız.

Canon, 4 temel unsuru esas alır:



GÜVENLİK

Canon çözümleri ve hizmetleri, belge yaşam döngüsü boyunca basılı veya dijital formatta olması fark etmeksizin tüm belgelerin ve hassas bilgilerin güvende tutulmasına yardımcı olur. Çözümlerimizi ve hizmetlerimizi, tasarımdan gelen güvenlik ilkesi ışığında güvenliği düşünerek geliştirdik.



SÜRDÜRÜLEBİLİRLİK

Canon, ambalajların boyutunu küçültüp dağıtım merkezlerini birleştirerek ürün yaşam döngüsü boyunca CO2 emisyonlarını azaltma konusunda verdiği taahhütler gibi sürdürülebilirlik uygulamalarını Birleşmiş Milletler Sürdürülebilir Gelişim Hedefleri (SDG'ler) ile uyumlu hale getirdi.

Tüm bu unsurları bir araya getiren Canon, sizin için doğru iş ortağıdır.



DESTEK

Müşteri memnuniyetiyle sonuçlanan ve en yüksek kaliteyi sağlayan çok çeşitli bir hizmet portföyü sunuyoruz. Verimliliği artırmayı hedefleyen ve müşterilerimiz için yeni olanakları açığa çıkarmaya kararlı şirket içi uzmanlığa sahibiz.



YENİLİK

80 yılı aşkın süredir üstün teknoloji sunan, görüntü odaklı yenilikte uzun bir geçmişe sahibiz. Sektörde ilklere imza atıyoruz ve gelecekte teknoloji alanında yaşanacak gelişmelere katkıda bulunmakta son derece kararlıyız.



New to the Line



Canon uniFLOW Online
Outstanding Cloud Output Management Solution

Canon Eurasia Görüntüleme ve Ofis Sistemleri A.Ş.
Değirmen Sokak Nida Kule İş Merkezi No: 18/10
K: 2 Kozyatağı 34742 Kadıköy
İstanbul, Türkiye
Tel: +90 (216) 571 68 00
Faks: +90 (216) 571 68 99

Canon Inc.
Canon.com

Canon Eurasia
canon.com.tr

Türkçe versiyon 1.0
© Canon Europa
N.V., 2021

Canon