OFİSİNİZİ KORUYUN

McAfee PROTECTED

COPIER MFP LINE OF THE YEAR 2018 BLI BUYERS LAB LINE OF THE YEAR

BLI BUYERS LAB 2019 PICK
Canon uniFLOW Online
Outstanding Cloud Output-Management Solution

COPIER MFP LINE OF THE YEAR 2020 BLI BUYERS LAB LINE OF THE YEAR
New to the Line

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. Dijital Dönüşüm Çağında 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 kapsaması 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 sürücüleri 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 çıktı tepsisinde unutulan gizli belgelerin açığa çıkması
- Farklı kullanıcılara ait yazdırılmış materyallerin karışması
- Yazım hataları nedeniyle belgelerin faks veya e-posta ile yanlış alıcılara gönderilmesi
- Bilgisayar korsanlarının aktarım durumundaki 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, Ortak Kriter yöntemi kullanılarak ve baskı cihazı güvenliğine yönelik IEEE2600 standartlarının gerekliliklerine uygun olarak rutin bir şekilde değerlendirilip 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 uniFLOW Online Express adlı esnek bir oturum açma çözümü bulunur. Bu çözüm, cihazda oluşturulan bir kullanıcı veri tabanıyla 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.

SABİT DİSK SÜRÜCÜSÜNDEKİ 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.

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 DX cihazlarında 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 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.

TEHLİKELERİ ÖNLEYİCİ GÜVENLİK

imageRUNNER ADVANCE DX ürünleri, yazıcıları saldırılara karşı koruyan çeşitli güvenlik ayarları sunar. Açılışta Sistem Doğrulama işlevi, makine başlatıldığında cihazda güvenilirlik sağlarken McAfee Embedded Control, çalışma sırasında programlar üzerinde değişiklik yapılmasını veya yetkisiz programların başlatılmasını engelleyerek cihazın kullanım ömrü boyunca güvenilirlik sunar. Buna ek olarak Syslog verileri, cihazın gerçek zamanlı güvenlik durumu bilgilerinin yanı sıra izleme özellikleri de sunar (Veriler uygun bir üçüncü taraf SIEM sistemi tarafından okunabilir).

CİHAZLARINIZ NE KADAR GÜVENDE?

1
Cihazlarınız ortak alanlarda bulunuyor ve paylaşılıyor 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?

SABİT DİSK ŞİFRELEME

imageRUNNER ADVANCE DX 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 oluşturulan Şifreleme Modülü Doğrulama Programı (CMVP) ve Japonya Şifreleme Modülü Doğrulama Programı (JCMVP) kapsamında onaylıdır.

SABİT DİSK SİLME

Kopyalanmış veya taranmış görüntü verileri gibi bazı veriler ile bilgisayardan yazdırılan belge verileri, sabit disk sürücüsünde yalnızca geçici bir süre için kayıtlı kalır ve işlem tamamlandıktan sonra silinir. Artık verilerin kalmadığından emin olmak için sabit disk sürücülü cihazlarımız, iş sürecinin parçası olarak artık verileri rutin bir şekilde silme imkanı sunar.

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.

*Belirli modeller için 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 ağınızı 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, ağınızı ve verilerinizi hem iç hem de dış saldırılardan korumak için çeşitli güvenlik çözümleri sunuyor.

IP VE MAC ADRESİ FİLTRELEME

Giden ve gelen iletişim için yalnızca belirli bir IP veya MAC adresine sahip cihazlarla iletişime izin vererek ağınızı üçüncü tarafların yetkisiz erişiminden koruyun.

PROXY SUNUCUSU YAPILANDIRMASI

İletişimi makinenizin yerine üstlenmesi ve ağın dışındaki cihazlara bağlanılırken kullanılması için bir proxy oluşturun.

IEEE 802.1X KİMLİK DOĞRULAMA

Yetkisiz ağ erişimi, yalnızca kimlik doğrulama sunucusunun onayladığı istemci cihazlara erişim önceliği veren bir LAN anahtarı tarafından engellenir.

IPSEC İLETİŞİMİ

IPSec iletişimi, IP ağı üzerinden gönderilen IP paketlerinin üçüncü taraflarca ele geçirilmesini veya değiştirilmesini engeller.

Makine ve bilgisayar gibi diğer cihazlar arasında paylaşılan verilerin dinlenmesini, yanıltılmasını ve kurcalanmasını engellemek için TLS şifreli iletişimi kullanın.

BAĞLANTI NOKTASI KONTROLÜ

Bağlantı noktalarını güvenlik politikası ayarınızın parçası olarak yapılandırın.

OTOMATİK SERTİFİKA KAYDI

Bu özellik, güvenlik sertifikalarını yönetme işini önemli ölçüde kolaylaştırır. Sistem yöneticisi, sektörce tanınan teknolojiyi kullanarak sertifikaları otomatik olarak güncelleyip yayınlayabilir; böylece güvenlik politikalarının her zaman karşılandığından emin olur.

KAYIT İZLEME

Çeşitli kayıtlar, engellenmiş iletişim istekleri de dahil olmak üzere cihazınızın çevresindeki aktiviteleri izlemenizi sağlar.

Wİ-Fİ DIRECT

Mobil cihazın ağınıza erişmesine gerek olmadan mobil yazdırma özelliğini kullanabilmek için eşler arası bağlantıyı etkinleştirin.

CİHAZA VE CİHAZDAN İLETİLEN VERİLER İÇİN ŞİFRELEME

Bu seçenek, kullanıcı bilgisayarından çok işlevli yazıcıya iletilen yazdırma işlerini şifreler. Evrensel güvenlik özelliği seti etkinleştirildiği zaman PDF formatındaki taranmış veriler de şifrelenebilir.

MOBİL MİSAFİR YAZDIRMA

Güvenli ağ yazdırma ve tarama yönetimi yazılımımız, e-posta, web ve mobil uygulama üzerinden harici iş gönderme yolları sağlayarak mobil ve misafir yazdırma ile ilişkili yaygın güvenlik risklerini çözer. Bu, MFD'yi güvenli bir kaynağa kilitleyerek saldırı vektörlerini en aza indirir.

ÇİFT AĞ

En yeni teknoloji artık çift ağ özelliği sunuyor. Ağlar arasında daha sıkı ve güvenli bir ayrımın sağlanması için birincil ağ her zaman kablolu olurken, ikincil hat artık kablosuz veya kablolu kullanılabiliyor.

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 yazdırılamaz. Bu, kullanıcıların gizli kabul ettikleri belgeleri güvenceye almasını sağlar.

Tüm yazdırma işlerini tutma
imageRUNNER ADVANCE DX'te 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.

Kurumsal düzeyde veri kaybını önleme
Temel veri kaybı önleme özelliklerini uniFLOW ile birlikte iW SAM Express'e yükseltin. Bu sunucu tabanlı çözüm, güvenlik tehditlerini önlemek için yazıcıya ve yazıcıdan gönderilen belgeleri kaydedip arşivlemenizi ve metin ya da öznitelikleri kullanarak bu belgeleri analiz edip yorumlamanızı sağlar.

Belge kaynağını takip etme*
Gömülü kod aracılığıyla belgenin kaynağı bulunabilir.

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
Yazdırılan belgelerin kaynağını bulabiliyor musunuz?

4
Birileri hassas belgeleri yazıcınızdan alabilir mi?

5
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 ORİJİNALLİĞİNİ 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.

POLİTİKALARI ADOBE LIFECYCLE MANAGEMENT ES ENTEGRASYONUYLA UYGULAYIN

Kullanıcılar, hassas ve çok değerli bilgileri istenmedik veya kötü amaçlı ifşalara karşı korumak amacıyla PDF dosyalarını güvenceye alıp erişimi ve kullanıcı haklarını kontrol edecek sürekli ve dinamik politikalar uygulayabilir.

Güvenlik politikaları sunucu düzeyinde yönetilir, bu sayede bir dosya dağıtıldıktan sonra bile haklar değiştirilebilir. imageRUNNER ADVANCE DX serisi, Adobe® ES entegrasyonu için yapılandırılabilir.

*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.

KAPSAMLI BELGE DENETİMLERİ

Ofis belge hizmetleri mimarimiz, imageRUNNER ADVANCE DX cihazlarında işlenen tüm belgelerin eksiksiz kaydını (yani tarama ve iş meta verileri) tutmak için müşteriye özel seçeneklerle geliştirilebilir.

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 ağınızı 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?

UZMANLIK

Donanım ve yazılım entegrasyonu, sistem ihlallerinin ihtimalini azaltır.

ORTAKLIK

Müşterilerimizin daha iyi çalışmasına yardımcı olur ve **veri güvenliği tehditlerini proaktif şekilde ele alacağımızı** biliriz.

HİZMET

Müşterilere hizmet veren **bilgi güvenliği ekibi**, aynı zamanda kendi şirket içi BT güvenliğimizi de yönetir.

Kurumsal güvenlik duvarının içindeki ve dışındaki potansiyel tehditlerin hepsini dikkate alırız.

YENİLİK

Ürünlerimiz ve hizmetlerimiz, **kullandıkları akıllı yöntemlerle** bilgi güvenliği risklerinin ihtimalini en aza indirir.

SCAwards 2017 EUROPE

Siber güvenlik uzmanlığını ödüllendiren **2017 SCA Awards Europe**'ta, en iyi güvenlik ekibi kategorisinde**"yüksek övgü"**.

Canon ABD iki **BLI PaceSetter Awards 2017** ödülünü kazandı (Belge Görüntüleme Güvenliği ve Mobil Yazdırma).

Canon Inc.
Canon.com

Canon Avrupa
canon.com.tr

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
Fax: +90 (216) 571 68 99
canon.com.tr

Turkish edition
© Canon Europa N.V., 2019

Canon

McAfee PROTECTED