



Ağınızı HP'nin en güvenli baskı çözümüyle koruyun¹

%94

fotokopi makinesi/yazıcı güvenliğinin önemli veya çok önemli olduğunu söyleyen finans şirketlerinin oranı²



%61

geçen yıl en az bir kez baskıyla ilişkili veri ihlali yaşadığını bildiren kuruluşların oranı³



%43

uç nokta güvenlik stratejilerinde yazıcıları göz ardı eden şirketlerin oranı⁴





Şirketlerin yalnızca %18'i yazıcıları tehditlere karşı izliyor.⁴ Peki, ya siz?

Görünmeyen risklerden haberdar olun

BT ekipleri sürekli olarak çeşitli aygıtlar ve ortamlarda çalışanların kimlikleri ve müşteri verileri gibi gizli bilgileri korumakla görevlendirilir. Bir çok BT departmanı tekil bilgisayarlara ve ağlara sıkı güvenlik önlemleri uygulasa da, baskı ve görüntüleme aygıtları genellikle göz ardı edilir ve saldırılara karşı korumasız bırakılır. Aygıtlar korumasız olduğunda, tüm ağ siber güvenlik saldırılarına karşı açık hale gelebilir.

Olası maliyetlerden haberdar olun

Tek bir güvenlik ihlali bile oldukça maliyetli olabilir. Güvenli olmayan baskı ve görüntüleme uygulamaları nedeniyle gizli bilgiler tehlikeye atıldığı takdirde kimlik hırsızlığı, rekabet bilgilerinin çalınması, marka imajının ve itibarının zedelenmesi ve hukuki ihtilaf gibi sonuçlarla karşılaşılabilir. Ayrıca, düzenlemelere ve yasalara uygunsuzluk dolayısıyla ağır para cezalarına maruz kalınabilir.

HP yardıma hazır

Ağınızı HP'nin en güvenli baskı çözümüyle koruyun.¹ Her zaman tetikte olan HP yazıcılar, sürekli olarak tehditleri algılar ve durdurur; aynı zamanda da yeni tehditlere adapte olur. HP, kapsamlı çözüm portföyü sayesinde aygıt, veri ve belge koruma süreçlerini otomatikleştirmenize yardımcı olabilir. Baskı güvenliği uzmanlarımız, baştan sona bir görüntüleme ve baskı güvenliği stratejisi oluşturup kullanıma sunmanıza yardım edebilir.

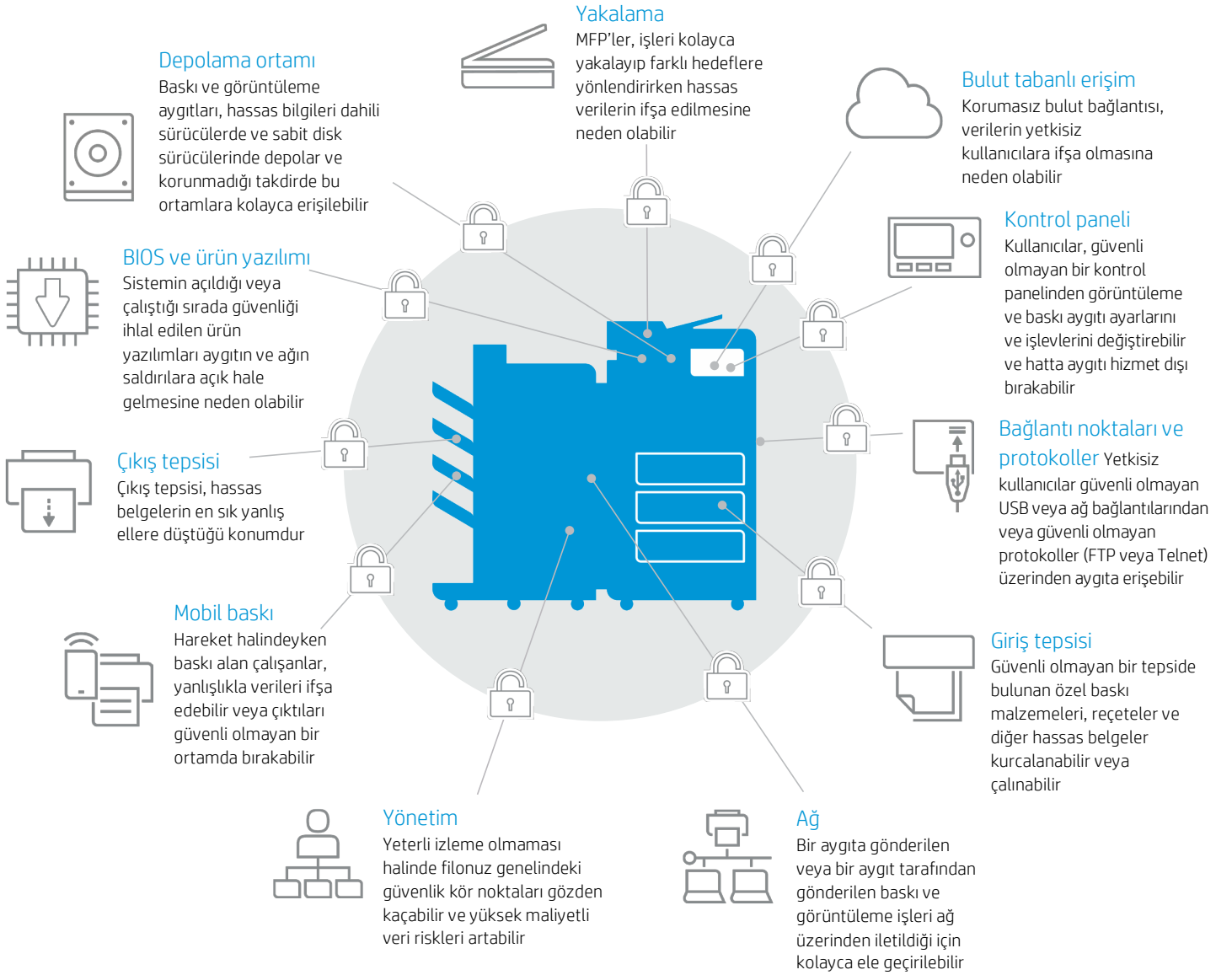
“Baskı güvenliğine uzun süredir yaptığı yatırımın kanıtı olarak HP, pazardaki en geniş ve en derin güvenlik çözümleri ve hizmetleri portföyüne sahiptir.”

– Quocirca, Ocak 2017⁵

Aygıtlarınızı, verilerinizi ve belgelerinizi koruyun

Görüntüleme ve baskı ortamınızda çeşitli noktalarda kritik açıklar bulunabilir. Bu güvenlik açıkları hakkında bilgi sahibi olduğunuzda, riskleri çok daha kolay azaltabilirsiniz.

Görüntüleme ve baskıdaki güvenlik açıkları





Aygıtları koruyun



Daha fazla bilgi

HP Özel Geri Dönüşüm Hizmetleri
hp.com/go/businessrecycling

HP Güvenli Yönetilen Baskı Hizmetleri
hp.com/go/securemps

HP yazıcılar, riskleri azaltmak, uyumluluğu artırmak ve ağınıza baştan sona korumak amacıyla güvenlik izleme ve yönetim çözümleriyle birlikte çalışacak şekilde tasarlanmıştır. (Özellik ve çözümlerin tümü her HP aygıtta bulunmaz.⁶⁾)

Temel güvenlik uygulamaları

Güvenli silmeyle şifrelenmiş depolama

Dahili sürücü veya sabit diskte saklanan hassas bilgiler çalınmaya karşı savunmasız kalma olasılığı taşır. Çoğu HP aygıt verileri korumak için dahili şifreleme özelliğiyle gelir. Saklanan verilere artık ihtiyaç kalmadığında, yerleşik aygıt özelliklerini kullanarak verilerin üzerine güvenli yazabilir ve hassas bilgileri silebilirsiniz.

Güvenli imha

HP Özel Geri Dönüşüm Hizmetleri, eski ürünler çevre bilinciyle geri dönüştürülmeden önce verilerin sabit sürücülerden silinmesini sağlayabilir.

Güvenli yazıcı onarım erişimi

Yazıcı bakım satıcılarının güvenlik uygulamalarının bilinmesi hassas verilerin korunmasına yardımcı olur. Uzman düzeyinde yardım için *HP Güvenli Yönetilen Baskı Hizmetleri (MPS)* veya HP iş ortaklarını tercih edin.

Bağlantı noktaları ve protokolleri devre dışı bırakma

Doğru aygıt yapılandırmasıyla saldırı alanını daraltın. Yetkisiz erişim veya kullanımı önlemek için fiziksel bağlantı noktaları ve güvenli olmayan protokolleri (FTP veya Telnet gibi) devre dışı bırakın.

Aygıt için yönetici erişim denetimi

Aygıt ayarlarını sadece BT personeli veya diğer yetkili personelin ayarlayabilmesi ve yapılandırabilmesi için yönetici parolaları oluşturun.

Beyaz listeye alma veya ürün yazılımı kodu

Beyaz listeye alma uygulamasının filonuzu kötü amaçlı yazılımlara karşı korumanıza nasıl yardımcı olabileceği ile ilgili bilgiler için bir sonraki sayfaya bakın.

Gelişmiş güvenlik uygulamaları

Ortak Kriter Sertifikaları

HP iş yazıcılarının Common Criteria Certification (CCC) ve FIPS 140 gibi uluslararası geçerliliği olan güvenlik standartlarıyla uyumluluğu onaylanmıştır. Kodun orijinal olduğunu ve bütünlüğünün korunduğunu doğrulamak ve uyumluluk sağlamak için aygıt ürün yazılımı güncellemelerinin kodla imzalandığından emin olun.



Daha fazla bilgi

Yerleşik baskı güvenliği özellikleri:

- HP Sure Start (BIOS bütünlüğü)
- Beyaz listeye alma veya ürün yazılımı kodu
- Çalışma sırasında müdahale algılama
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Saldırıları otomatik olarak algılayıp durdurmak için tasarlanmış baskı güvenliği özellikleri

HP iş yazıcıları, yazıcıların ağındaki saldırılar için giriş noktası olmasını önleyecek güvenlik özellikleri içerir. HP baskı güvenliği, tehditleri en başından durdurmak için gerçek zamanlı algılama, otomatik izleme ve dahili yazılım doğrulama özellikleri sunar.⁷

Pro⁸ sınıfından Enterprise sınıfına kadar her zaman tetikte olan HP iş yazıcıları,⁷ işlemlerin her aşamasında sürekli olarak tehditleri algılar ve durdurur:

- **Başlatma sırasında.** Ön yükleme kodu (Pro aygıtlar) veya BIOS (Enterprise aygıtlar), önemli donanım bileşenlerini yüklemek ve ürün yazılımını başlatmak için kullanılan yönergeler setidir. Kod bütünlüğünün her önyükleme döngüsünde doğrulanması aygıtınızın saldırılardan korunmasını sağlar.
- **Ürün yazılımı yüklenirken.** *Beyaz listeye alma*, sistem başlatıldığı sırada ürün yazılımını denetleyerek orijinal ve geçerli bir kod olup olmadığını, HP tarafından dijital olarak imzalanıp imzalanmadığını belirler. Herhangi bir anormallik tespit edildiğinde cihaz güvenli ve ağ bağlantısı kesik bir halde yeniden başlatılır ve BT ekibine bilgi verilir.
- **Çalışma sırasında.** HP yerleşik özellikleri, aygıtların saldırılara en açık olduğu açılma ve ağa bağlanma sırasında aygıt belleğinin korunmasına yardımcı olur. Bir saldırı olması durumunda aygıt kapanır.

HP Enterprise aygıtlar kendi kendilerini onarabilir

HP Enterprise yazıcılar, tehditleri algılama ve durdurma özelliğinin yanı sıra, saldırılara karşı kendi kendini otomatik olarak onarır; böylece BT ekiplerinin olaya müdahale etmelerine gerek kalmaz.⁷ Bu özellikler, bir saldırı veya anormal bir durum olması halinde yeniden başlatılması için sistemi otomatik olarak tetikler. Yöneticiler ArcSight, Splunk ve SIEMONster gibi Güvenlik Bilgisi ve Olay Yönetimi (SIEM) araçlarıyla durumdan haberdar edilebilir.

- *HP Sure Start*, BIOS'un kendi kendine onarılmasını sağlayan mükemmel bir araçtır.⁷ BIOS riske girerse HP Sure Start, BIOS'un güvenli "altın kopyasıyla" yeniden başlatılır.
- *Çalışma sırasında müdahale algılama*, karmaşık ürün yazılımlarını ve bellek işlemlerini izler ve bir saldırı olması halinde müdahaleyi otomatik olarak durdurarak sistemi yeniden başlatır.
- *HP Connection Inspector* normal etkinlikleri belirlemek, şüpheli istekleri durdurmak ve sistemin yeniden başlatılmasını otomatik olarak tetikleyerek kötü amaçlı yazılımları önlemek için giden ağ bağlantılarını değerlendirir.

Yükseltilebilir HP FutureSmart ürün yazılımının yatırım koruma olanağı sayesinde, beyaz listeye alma, çalışma sırasında müdahale algılama ve HP Connection Inspector özelliklerini mevcut çoğu HP Enterprise yazıcılara ekleyebilirsiniz.⁷

HP JetAdvantage Security Manager denetim döngüsünü tamamlar

Yeniden başlatma tamamlandıktan sonra (veya ağa yeni bir aygıt eklendiğinde), *HP JetAdvantage Security Manager* aygıtın güvenlik ayarlarını otomatik olarak değerlendirir ve gerekiyorsa önceden belirlenmiş şirket politikalarıyla uyumlu hale getirmek için gerekli düzeltmeleri gerçekleştirir.⁹ BT ekiplerinin müdahalesine gerek kalmaz.

Nasıl çalışır?

Yerleşik güvenlik özellikleri, HP aygıtındaki döngüde başlıca dört adım uygular.

Saldırı olursa, HP Enterprise aygıtlar yeniden başlatılarak kendi kendini onarabilir.

HP JetAdvantage Security Manager denetim döngüsünü tamamlar.

Dört. Sürekli izleme

Aygıt çalışırken işlemleri korur ve saldırıları durdurur.

Şüpheli istekleri durdurmak için giden ağ bağlantılarını denetler (sadece Enterprise).

Üç. Ayarları denetleme

Sistem yeniden başlatıldıktan sonra, HP JetAdvantage Security Manager aygıt güvenlik ayarlarını kontrol eder ve etkilenmiş olan tüm ayarları düzeltir.

Bir. BIOS/önyükleme kodunu denetleme

Sadece HP tarafından imzalanmış, orijinal kodun yüklenmesini sağlayarak kötü amaçlı kodun yürütülmesini önler.

İki. Ürün yazılımı denetimi

Sadece orijinal, geçerliliği olan ürün yazılımının (HP tarafından dijital olarak imzalanmış) yüklenmesini sağlar.



Verileri koruma



Daha fazla bilgi

HP Web Jetadmin
hp.com/go/wja

HP Universal Print Driver ile Güvenli Şifrelenmiş Baskı
hp.com/go/upd

HP JetAdvantage İş Akışı Çözümleri
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Sakladığınız veya iletim halindeki tüm verilerin sürekli olarak korunması gerekir. Verilerin güvenli şekilde gelmesi ve kullanılması için birkaç temel adım vardır.⁶

Temel güvenlik uygulamaları

802.1x veya IPsec ağ standartları

Şifrelenmiş ağ standartlarını kullanarak ağ üzerinden aygıt ile *HP Web Jetadmin* veya *HP Embedded Web Server* gibi yönetim araçları arasında gidip gelen verileri koruyun.

İletim halindeki verileri şifreleme

TLS üzerinden İnternet Baskı Protokolü (IPPS) gibi şifreleme yöntemleriyle aygıta gidip gelen baskı işlerini koruyun. Dilerseniz *HP Universal Print Driver Güvenli Şifrelenmiş Baskı* özelliğini kullanarak istemci ile sayfa arasında Microsoft'un FIPS 140 doğrulanmış kriptografik kitaplıklarının yardımıyla oluşturulan kullanıcı tanımlı parolayı temel alan gerçek simetrik AES256 baskı işi şifreleme ve şifre çözme uygulamalarından da yararlanabilirsiniz.

Tarama yapılırken, *HP JetAdvantage İş Akışı Çözümleri* hassas bilgilerin korunmasına ve verimliliğin artırılmasına yardımcı olabilir. Örneğin, HP Capture and Route aracı HP Access Control ile sorunsuz şekilde tümleştirilerek tekli kimlik doğrulama ve bilgi yönetimi için içeriği izleme özelliklerinin getirdiği kolaylıkla üst düzeyde güvenlik sağlar.¹⁰

Yerinde duran verileri şifreleme

Yerleşik şifreleme ile sabit sürücüde saklanan hassas kurumsal bilgileri koruyun. Ekstra güvenlik düzeyi için, aygıta isteğe bağlı HP Güvenilir Platform Modülü (TPM) aksesuarı eklenip aygıt şifreleme anahtarları otomatik olarak TPM'ye sabitlenerek şifreli kimlik bilgileri ve verilerin korunması daha da güçlendirilebilir. TPM, özel sertifika anahtarları oluşturup koruyarak aygıt kimliğinin güvenli şekilde korunmasını sağlar.

Güvenlik duvarı koruması

Yazıcının ağdaki bilgi işlem aygıtlarına erişimini kısıtlayarak ağınıza kötü amaçlı yazılımların ve virüslerin sızmasını önleyin.

Yerel kullanıcı kimlik doğrulama

Kullanıcıların PIN/PIC, LDAP veya Kerberos kimlik doğrulama uygulamaları ile oturum açmasını şart koşarak maliyetleri ve güvenlik risklerini azaltın. Bu uygulamaları Active Directory ile de tümleştirebilirsiniz.

Rol tabanlı erişim denetimleri

HP Access Control Rights Management, yazıcı özelliği kısıtlamaları ile maliyetleri ve güvenlik risklerini azaltmaya yardımcı olur. Rol tabanlı erişim denetimleri farklı kullanıcılara veya ihtiyaçlarına bağlı olarak departmanların tamamına farklı özellikler sağlamanıza izin verir. Örneğin, faks çekecek, e-postaya veya faksa tarayacak kişileri sınırlı tutabilirsiniz.

Gelişmiş güvenlik uygulamaları



Daha fazla bilgi

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

Gelişmiş kimlik doğrulama ve izleme

Gelişmiş kimlik doğrulama (parola, proximity kartları, akıllı kartlar veya biyometrik denetimler gibi) ve izleme çözümleri uygulayarak ekstra güvenlik ve kontrol sağlayın.

- *HP Access Control Secure Authentication*, kontrolü tekrar ele almanızı, güvenliği güçlendirmenizi ve maliyetleri düşürmenizi sağlar. NFC özellikli mobil aygıtlarla dokunarak kimlik doğrulama gibi çeşitli gelişmiş denetim ve seçeneklerden yararlanın.
- *HP Access Control Job Accounting*, verileri doğru biçimde izleyip toplamanıza, sonuçları analiz etmenize ve rapor oluşturup göndermenize yardımcı olur. Veri madenciliğiyle elde edilen verileri kullanarak baskı maliyetlerini bölüştürün, çalışanları daha akılcı şekilde baskı almaya yönlendirin ve BT ekibine filo çapında öngörülerini iyileştirmeleri için gereken bilgileri sağlayın.

Ağ erişimine dahil edilen mobil aygıtlar

Yazıcı erişim denetimi için genel baskı güvenliği politikanızın bir parçası olarak mobil aygıtlarınızdan faydalanın. HP, güvenli kimlik doğrulamalı baskı ve gelişmiş yönetim ve raporlama özellikleri sağlayan sunucu tabanlı çözümler sunar.

- *HP JetAdvantage Connect** şirketler için tasarlanmış pratik ve güvenilir bir mobil baskı deneyimi sunar. Mobil baskıları yönetmek için mevcut BT ağ araçları ve politikalarından en iyi şekilde yararlanarak zamandan kazanın ve tasarruf edin.¹¹ Kullanıcılar, tıpkı bilgisayardaki kadar kolay bir şekilde çeşitli akıllı telefonlar ve tabletlerden ihtiyaç duydukları zaman ve yerde güvenli baskı alabilirler.
- *HP Access Control*, mobil baskıları yönetme özellikleri içerir. Mevcut e-posta altyapısından faydalanarak mobil kullanıcıların bir baskı işini e-postayla baskı kuyruğuna göndermelerini, ardından çözümün çalıştığı bir yazıcı veya MFP'den işi almalarını sağlar. Ağ baskı aygıtlarını Mobile Release gibi güvenli kimlik doğrulama özellikleriyle koruyun.

Veri sızıntılarını gerçekleşmeden önce durdurun

HP çözümleri, veri kayıplarına karşı koruma sağlayan özellikler sunar. *HP Capture and Route Veri Kaybı Önleme* çözümü sayesinde hassas bilgilerin taranmasını ya da faksla gönderilmesini önleyebilirsiniz. *HP Erişim Denetimi Baskı Verisi Kaybı Önleme* çözümü, hassas bilgilerin yazdırılmasına önlemenize olanak verir. En önemli verilerinizi izleyin ve ihlalleri iş akışlarında yavaşlamaya neden olmadan caydırıp önleyin. Tercih ettiğiniz sürelerle göre akıllı güvenlik uyarıları alın.

Yazıcılara dijital sertifikalar uygulama

Ağ yazıcıları ve MFP'lere dijital sertifikalar uygulayarak baskı ortamınızın güvenliğini artırın. Sertifikaları otomatik olarak yüklemek ve yenilemek için HP JetAdvantage Security Manager aracını kullanarak zamandan kazanın.⁹



Belgeleri koruma



Daha fazla bilgi

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

HP ve TROY belge koruması
hp.com/go/HPandTROY

Geniş BT güvenlik planınıza akıllı donanım ve yazılım çözümleri ekleyerek basılı belgelerinizdeki hassas bilgileri koruyun.⁶

Temel güvenlik uygulamaları

Önceden basılan formlara erişimi denetleme

Yazıcılarınıza ve MFP'lerinize kilitli giriş tepsileri takarak çekler, reçeteler veya diğer hassas belgelerin basılmasında kullanılan özel kağıtların çalınmasını önleyin.

İsteğe bağlı PIN ile veya kimlik doğrulamalı baskı kullanarak hassas belgeleri koruma

Kullanıcılar PIN ile veya Kimlik doğrulamalı baskıyı tercih ederek kişisel yazıcılara bağımlılığı ortadan kaldıracak ve baskı işlerinin yanlış ellere düşmesini engelleyebilir. Bu güvenlik önemleri, aygıttan alınmayan çıktıların önüne geçerek maliyetlerin ve atık miktarının azaltılmasını da sağlar.

PIN ile baskı uygulamalarında, kullanıcılar gizli baskı işleri gönderirken işin alınabilmesi için aygıtı girilmesi gereken bir PIN atayabilir.

Kimlik doğrulamalı baskı, baskı işlerinin bulut ortamında veya kullanıcının bilgisayarında saklanmasını sağlar. Kullanıcılar işlerini kimlik doğrulamalı baskı yoluyla basmak için istedikleri baskı konumunda kimliklerini doğrular. HP, iki adet bulut tabanlı kimlik doğrulamalı baskı çözümü sunar:*

- *HP JetAdvantage Secure Print*, baskı işlerini bulut ortamında veya kullanıcının masaüstünde saklayan KOBİ'ler için tasarlanmış ekonomik bir çözümdür. Kolaylıkla kurulabilen ve kullanılabilen bu çözüm, kullanıcıların işleri bir mobil aygıttan almalarını sağlar ve çok tedarikçili aygıtları destekler.¹²
- *HP JetAdvantage Private Print*, HP'nin karmaşıklığa neden olmadan kimlik doğrulamalı baskı avantajları sunan bulut tabanlı ücretsiz çözümüdür. Kolaylıkla kurulabilen bu çözüm için sunucu, montaj ya da bakım gerekli değildir.¹³

Gelişmiş güvenlik uygulamaları

Tüm baskı işleri için zorunlu kimlik doğrulamalı baskı

HP Access Control Secure Pull Printing, gizli bilgilerin korunmasını, aygıt güvenliğinin güçlendirilmesini ve verimliliğin artırılmasını sağlar. Sunucu tabanlı bu güçlü çözüm, yaka kartıyla başlatma gibi çeşitli kimlik doğrulama biçimleri, kurumsal düzeyde güvenlik ve yönetim özellikleri sunar.

Belgelerin kopyalanmasını ve üzerinde değişiklik yapılmasını önlemek için MICR, filigran ve diğer özellikleri kullanma

HP ve TROY sahteciliği önleme çözümlerinde,* kimyasal kurcalamaya maruz kaldığında kağıt üzerinde lekeler bırakan güvenlik toneri kullanılır, basılı sayfalara değişken veri filigranları ve belgeleri tek tek izleyip denetleyen makine tarafından okunabilir kodlar eklenir. MFP'ler reçete, doğum belgesi veya transkript gibi basılı hassas belgelere özel imzalar, şirket logoları ve güvenlik fontları gibi sahteciliği önleme özellikleri yerleştirebilir.



Baskı ortamınızı izleme ve yönetme



Daha fazla bilgi

HP JetAdvantage Güvenlik Yöneticisi
hp.com/go/securitymanager

Güvenlik izleme ve yönetim çözümleriyle, güvenlik açıklarını tespit edip birleşik, politika tabanlı bir yaklaşım oluşturarak verileri koruyabilir, riskleri azaltabilir ve uyumluluk sağlayabilirsiniz.⁶ Koruma açıklarını ortadan kaldırın ve maliyetli cezaları önleyin.

Temel güvenlik uygulamaları

Aygıtları en son ürün yazılımları/işletim sistemleri ile güncelleştirme

HP Web Jetadmin¹⁴ ile ürün yazılımı güncelleştirmelerinin tüm filoya dağıtılmasını sağlayarak aygıtları en güncel aygıt koruma ve güvenlik özellikleriyle donatın.

Yazıcı güvenliği olay günlüklerini inceleme

HP aygıtları, gerektiğinde BT ekibinin sorunları düzeltebilmesi için sistem günlüğü sunucusuna yazıcı etkinliklerini/bildirimlerini gönderir.

Aygıt ayarlarına erişme ve düzeltme

Microsoft System Center Configuration Manager (SCCM) için bir eklenti olan *HP Print Manageability Integration Kit* (MIK) ile tüm filoda temel yazıcı güvenlik ayarlarını yönetin. Microsoft SCCM, uç noktaları uzaktan planlamak, dağıtmak, yapılandırmak ve yönetmek için geniş ölçüde kullanılan bir yönetim çözümüdür. HP Print MIK, en çok kullanılan 15 güvenlik ayarını bulup eriştikten sonra düzelterek sonuçlar hakkında rapor düzenler.

Tüm filoda kapsamlı güvenlik yönetimi için *HP JetAdvantage Security Manager*¹ ı tercih edin.⁹ Bu çözüm, maliyetleri düşürüp daha az kaynak kullanarak filo genelinde bir güvenlik politikası oluşturmanıza, aygıt ayarlarını düzeltme işlemlerini otomatikleştirmenize, benzersiz sertifikalar yükleyip yenilemenize ve uyumluluğu kanıtlamak için gereken raporları almanıza yardımcı olur.

Gelişmiş güvenlik uygulamaları

Tehditleri algılamak ve belgelemek için SIEM yazılımı dağıtma

HP FutureSmart aygıtlarından alınan etkinlik verileri ArcSight, Splunk ve SIEMONster gibi olay algılama araçlarına gönderilerek gerçek zamanlı olarak izlenebilir. BT güvenlik ekibi, geniş BT ekosisteminin bir parçası olarak yazıcı uç noktalarını kolayca görüntüleyebilir ve yazıcı güvenlik uyarılarını algılayarak çözümleyebilir.

Ağa eklenen yeni baskı aygıtlarını otomatik yapılandırma

HP JetAdvantage Security Manager'daki Anında Açılma Güvenlik özelliği, ağa eklendiklerinde veya sistem yeniden başlatıldıktan sonra yeni aygıtları otomatik olarak yapılandırır.

Baskı filosu güvenliği uyumluluk denetim raporları

HP JetAdvantage Security Manager'ı kullanarak güvenlik politikalarının yazıcılara uygulandığını ve müşteri verilerinin korunduğunu gösteren uyumluluk kanıtı raporları oluşturur.



Daha fazla bilgi

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Uyumluluk ihlalleri işinize zarar verebilir

Hiç korunmayan veya yeterli düzeyde korunmayan uç noktalar siber suçlar için daha büyük fırsatlar oluşturur. Büyüyen bu tehdide karşı koymak için devlet makamları dünya genelinde katı düzenlemeler uygulayarak kuruluşların müşteri bilgilerini daha iyi korumalarını şart koşuyor.

Uyumluluk konusunda yetersiz kalan kuruluşlar ise cezalar, iş kaybı

itibarın zedelenmesi ve toplu davalar gibi ağır bedellerle karşılaşabilir.

Uyumluluk gerekliliklerini karşılamaya ve kurumsal bilgileri güvenlik tehditlerine karşı korumanıza yardımcı olan HP Enterprise yazıcılar ve HP JetAdvantage Security Manager gibi aygıt ve çözümleri kullanmak son derece önemlidir.



İhtiyaç duyduğunuz yardımı alın

Kendi başınıza korunmak ve güvenliği sağlamak zorunda değilsiniz. Danışmanlardan oluşan bir destek ekibi size veri, cihaz ve belge güvenliğini nasıl daha iyi koruyabileceğinizi gösterebilir.

Baskı güvenliği uzmanlarıyla birlikte çalışarak şu anki baskı güvenliği açıklarını değerlendirin. Kurumsal gereksinimler ve en iyi uygulamalara göre kapsamlı bir baskı güvenliği politikası oluşturmanıza ve benzersiz iş ortamınızda en yüksek düzeyde güvenlik sağlamanız için bir plan hazırlamanıza yardımcı olabiliriz.

Endüstrinin lideri olarak kabul edilmiştir

HP, ilk IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment raporunda birinci sırada yer almıştır. (Raporu [burada](#) bulabilirsiniz.) Rapora göre “HP Inc.’nin tüm baskı ve belge altyapısını göz önüne alan güvenlik yaklaşımı, aygıtın kilitlenmesinden başlayarak aygıt kullanımının ve içerik korumasının tüm boyutlarına uzanır.” Burada gösterilen grafik IDC 2017 Vendor Assessment raporundandır.¹⁵

IDC MarketScape satıcı analizi modeli, belirli bir pazardaki ICT tedarikçilerinin rekabetçi uygunluğuna genel bir bakış sunmak üzere tasarlanmıştır. Araştırma yönteminde, her bir satıcının belirli bir pazardaki konumunun grafik bir gösterimini sunacak şekilde niteliksel ve niceliksel kriterleri esas alan titiz bir puanlama yöntemi kullanılmaktadır. Beceri puanı, satıcının kısa vadede ürün, pazara çıkış ve iş yürütme uygulamalarını ölçer. Strateji puanı, 3 ila 5 yıllık bir zaman dilimi için satıcının stratejileriyle müşteri gereksinimlerinin uyumunu ölçer. Satıcının pazar payı simgelerin büyüklüğüyle ifade edilmiştir.¹⁵

Başlangıç

Daha yüksek düzeyde koruma ile güvenle yola devam etmenizi sağlayacak HP güvenlik özellikleri, çözümleri ve hizmetleri hakkında kapsamlı bilgi için satış temsilcinizle görüşün.

Daha fazla bilgi

hp.com/go/printsecurity

¹ "En güvenli baskı deneyimi" beyanı aynı sınıf yazıcıların yayınlanmış güvenlik özelliklerine ilişkin 2017 tarihli HP incelemesine dayanmaktadır. HP, saldırıları izleyip algılayarak otomatik olarak durdurabilen ve ardından önyükleme sırasında yazılım bütünlüğünü otomatik olarak kendi kendine doğrulayabilen güvenlik özelliklerinin bir birleşimini sunar. Ürün listesi için bkz. hp.com/go/LJCompatibility.

² InfoTrends, "Designing Hardware & Solutions," Brendan Morse, Ekim 2016.

³ Quocirca, "Managed Print Services Landscape, 2016," quocirca.com/content/managed-print-services-landscape-2016, Temmuz 2016.

⁴ Spiceworks tarafından HP adına Kuzey Amerika, EMEA ve APAC bölgelerinde 309 BT karar vericiyle gerçekleştirilen anket, Kasım 2016.

⁵ Quocirca, "Print security: An imperative in the IoT era," quocirca.com/content/print-security-imperative-iot-era, Ocak 2017.

⁶ Çözümler her HP aygıtta desteklenmeyebilir; çözümlerin ek olarak satın alınması gerekebilir.

⁷ HP'nin en güvenli yerleşik güvenlik özellikleri, FutureSmart ürün yazılımının 4.5 veya üzeri bir sürümü yüklü olan Enterprise sınıfı HP aygıtlar için geçerlidir ve aynı sınıftaki HP yazıcıların yerleşik güvenlik özellikleri hakkında yayınlanan 2017 tarihli HP incelemesine dayanmaktadır. HP, BIOS'a kadar bütünlük denetimi ve kendi kendini onarma kapasitesi içeren güvenlik özelliklerinin bir birleşimini sunar.

⁸ Belirli HP LaserJet Pro ve PageWide Pro aygıtlarda saldırıları algılayarak durdurabilen yerleşik özellikler bulunur. Daha fazla bilgi için lütfen hp.com/go/LJCompatibility adresini ziyaret edin.

⁹ HP JetAdvantage Security Manager ayrı satın alınmalıdır. Daha fazla bilgi için bkz. hp.com/go/securitymanager.

¹⁰ Parolayla korunan uç havuza bilgi gönderirken ek bir parola gerekir.

¹¹ HP JetAdvantage Connect önde gelen mobil aygıtlarla çalışır. Android™, Google Chrome™ ve Microsoft işletim sistemleri kullanılan aygıtlara bir seferliğine bir eklenti yüklenmesi gerekir. Ayrıntılar ve desteklenen işletim sistemlerinin listesi için bkz. hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: Kimlik doğrulamalı baskı tüm ağ bağlantılı yazıcı veya MFP'lerle çalışır. Aygıt üzerinde kimlik doğrulama çoğu HP LaserJet, PageWide ve OfficeJet Pro aygıtlarında ve bazı HP olmayan aygıtlarda sunulur. Bazı aygıtlar için bir ürün yazılımı yükseltmesi gerekebilir. Bulut depolama ve baskı işlerinin alınması için internet bağlantısı gerekir. Bir mobil aygıttan baskı işi başlatmak için ağ bağlantısı ve QR kodu gerekir. Daha fazla bilgi ve desteklenen yazıcıların ve MFP'lerin bir listesi için bkz. hp.com/go/JetAdvantageSecurePrint.

¹³ HP JetAdvantage Private Print ücretsiz olarak sunulur ve web hizmetleri etkinleştirilmiş yazıcının internete bağlı olmasını gerektirir. Bazı ülkelerde sunulmaz. Daha fazla bilgi için bkz. hp.com/go/JetAdvantagePrivatePrint.

¹⁴ HP Web Jetadmin hp.com/go/webjetadmin adresinden ücretsiz olarak indirilebilir.

¹⁵ IDC tarafından yapılan basılı kopya satıcıları incelemesine ve HP'nin liderliği konusunda bildirilen görüşlere dayanmaktadır: "HP, sunduğu güçlü BT hizmetleri ve becerileriyle avantajlı konumdadır ...ve tüm BT altyapısı genelinde kapsamlı ve tümleşik bir güvenlik stratejisi sunar." KAYNAK: [IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment](http://www.idc.com/analysis/hp-worldwide-security-solutions-and-services-hardcopy-2017-vendor-assessment), yazarlar Allison Correia ve Robert Palmer, Ekim 2017, IDC Doc #US41988517.

*Baskı Çözümlerinin kullanılabilirliği ülkeye göre değişebilir.

Güncelleştirmeler için kaydolun

hp.com/go/getupdated



İş arkadaşlarınızla paylaşın

© Copyright 2014-2018 HP Development Company, L.P. Bu belgede yer alan bilgiler önceden bildirilmeden değiştirilebilir. HP ürün ve hizmetlerine ilişkin yegane garantiler, bu ürün ve hizmetlerle birlikte verilen açık garanti bildirimlerinde belirtilmiştir. Buradaki hiçbir ifade ek bir garanti verilmesi olarak yorumlanmamalıdır. HP, bu belgedeki teknik hatalardan veya yazım hatalarından ya da eksikliklerden sorumlu tutulamaz.

Android ve Google Chrome, Google Inc.'nin tescilli ticari markalarıdır. Microsoft, Microsoft şirketler grubunun ABD'de tescilli ticari markasıdır.

4AA3-1295TRE, Ocak 2018, Rev. 11

