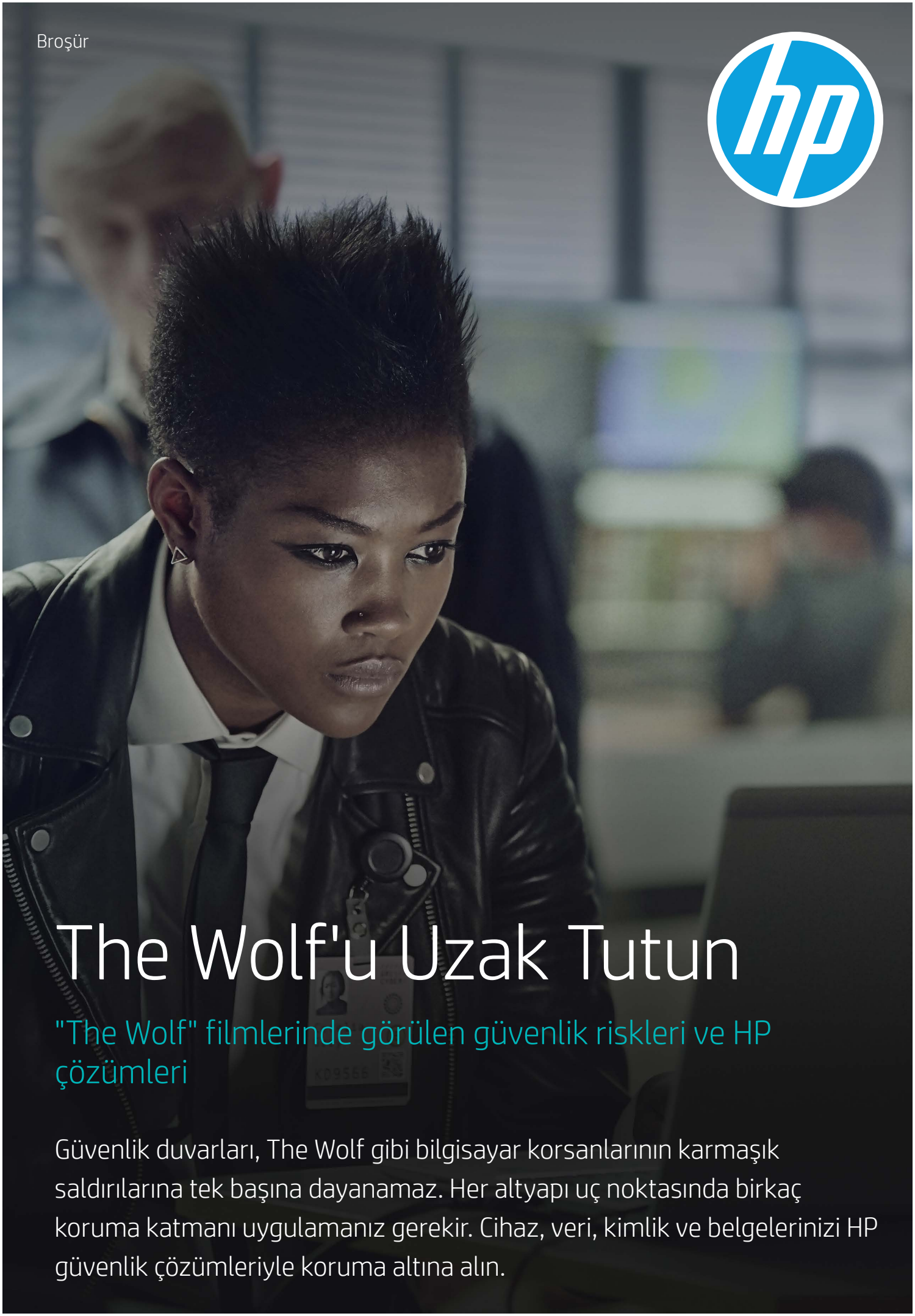
Broşür



The Wolf'u Uzak Tutun

"The Wolf" filmlerinde görülen güvenlik riskleri ve HP çözümleri

Güvenlik duvarları, The Wolf gibi bilgisayar korsanlarının karmaşık saldırılarına tek başına dayanamaz. Her altyapı uç noktasında birkaç koruma katmanı uygulamanız gerekir. Cihaz, veri, kimlik ve belgelerinizi HP güvenlik çözümleriyle koruma altına alın.

1. Sezon The Wolf

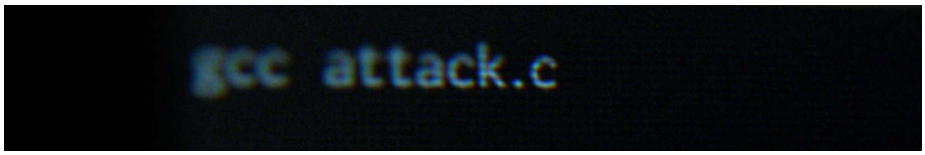
The Wolf, global bir finans kuruluşunu güvenlik açığı olan uç noktalarına saldırarak çökertir. Bir mobil cihaz kullanarak yazıcılardan birine erişir ve verileri yakalayıp okumak için kötü amaçlı bir yazılım yerleştirir. Ardından The Wolf, kullanıcılardan birini bir "kimlik avı" e-postasıyla gönderdiği ve bir PDF'e gizlenen kötü amaçlı kodu yazıcıya göndermek üzere kandırır.

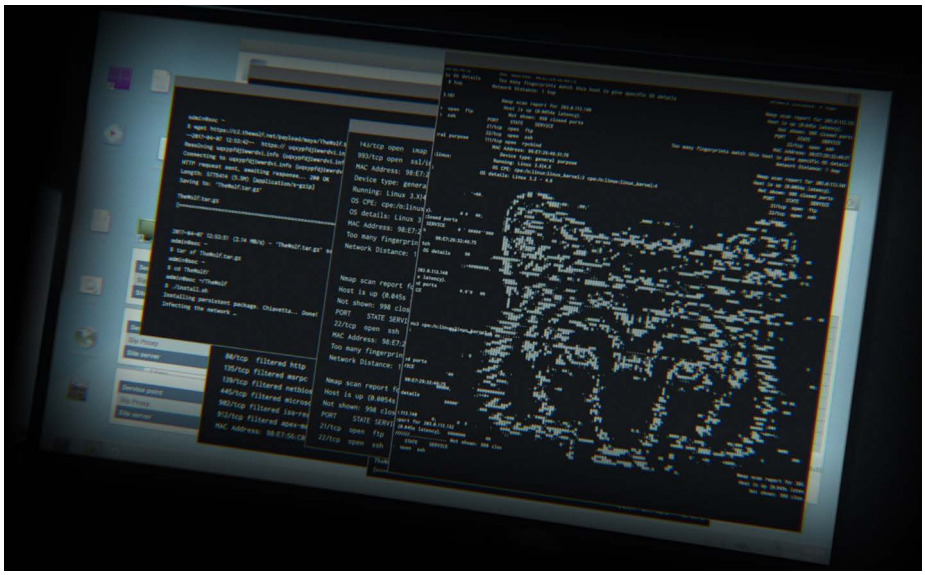
Yazıcıdaki kötü amaçlı yazılım, güvenlik duvarını aşıp şirketteki bilgisayarların BIOS düzeyine ulaşır ve böylece veri toplayabilir ve ağ savunmaları devreye girdiğinde bile kendi kendini yeniden kurabilir.

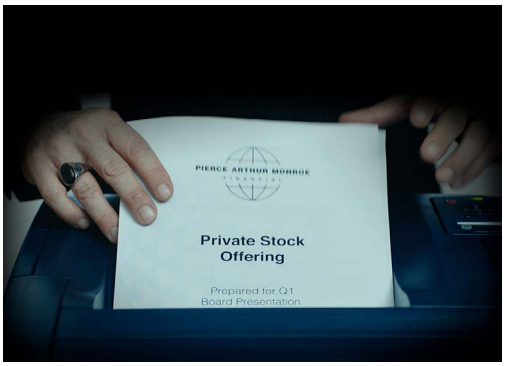
The Wolf, bir yazıcının çıkış tepsisinde bırakılmış bir baskıyı alır ve firmanın bir sonraki borsa işlemini sabote ederek hisse sahiplerinin güvenini sarsar.

Güvenlik Açıkları

- Yazıcının Wi-Fi veya Bluetooth® özelliğinin kullanıcıdan kimliğini doğrulaması istenmeden açılması
- Yazıcı veri dosyalarının şifrelenmemesi
- Kullanıcıların şüpheli e-posta veya baskı dosyalarını tanımaması
- Yazıcılarda ve bilgisayarlarda BIOS düzeyinde kötü amaçlı yazılımlara karşı koruma olmaması
- Hassas belgelerin çıkış tepsilerinde açıkta bulunması







2. Sezon The Hunt Continues

The Wolf dünya sağlık sektörünün en büyük kayıt yönetimi şirketlerinden biri tarafından depolanan hasta kayıtlarını hedef alır. Önce bir bilgisayara sızar, ardından güvenlik açığı oluşturulacak bağlantılı cihazları aramak için bir yazıcının USB bağlantı noktasını kullanarak güvenlik duvarını aşar ve kötü amaçlı yazılım yükler.

Yazıcı bölümlere ayrılmamış bir ağ üzerinde olduğundan The Wolf, hassas bilgilerle dolu veritabanlarına bağlı sunuculara kolayca erişebilir. Milyonlarca gizli hasta kaydını çalar ve bu kayıtlar şifreli olmadığı için okunabilir.

Hastane ve yazılım şirketi bu durumdan sorumlu tutulur ve itibarlarının zedelenmesinin yanı sıra büyük para cezalarına çarptırılırlar.

Güvenlik Açıkları

- Yazıcı USB bağlantı noktasının kimlik doğrulama gerektirmemesi
- Veri dosyalarının şifrelenmemesi
- Yazıcılarda kötü amaçlı yazılımlara karşı koruma olmaması
- Yazıcıların güvenlik olaylarına karşı izlenmemesi

3. Sezon True Alpha

The Wolf, dünyanın en büyük kargo şirketlerinden birinde ve uluslararası bir havaalanındaki faaliyetlerin aksamasını sağlar.

Zararsız görünen bir PDF'i e-posta üzerinden göndererek kargo şirketindeki bir ofis memurunun saldırı amaçlı bir Postscript dosyasını bir yazıcıya göndermesini sağlar. Dosya yazıcıya gönderildiğinde gizlenmiş kötü amaçlı yazılım tüm ağa yayılır ve açığa çıkmaz. The Wolf kısa süre içinde CEO'nun gündem konusu olan konferans sunumuna, bir limanda kargo yükleyen vinçlere ve denizdeki gemilerin otomatik pilot yazılımına erişir.

Daha sonra The Wolf, büyük bir havaalanına odaklanarak havaalanındaki ışıkları ve potansiyel olarak ağdaki birden fazla sistemi kontrol etme konusunda becerilerini sergiler. HP yazıcıları BT personelinin araştırma yapmasına ve saldırıyı durdurmasına yardımcı olur.

Güvenlik Açıkları

- Geçici konumlardaki yazıcıların güvenlik için yeterli yapılandırma olmadan ağa eklenmesi
- Bilgisayarlarda yanlışlıkla indirme işlemlerine karşı web tarama koruması olmaması
- IoT cihazlarının izlenmemesi ve kötü amaçlı yazılım algılama özelliklerine sahip olmaması
- Yazıcı sistem günlüklerinin tehdit izleme araçlarına bağlı olmaması

Benzer saldırılara karşı nasıl korunabilirsiniz?

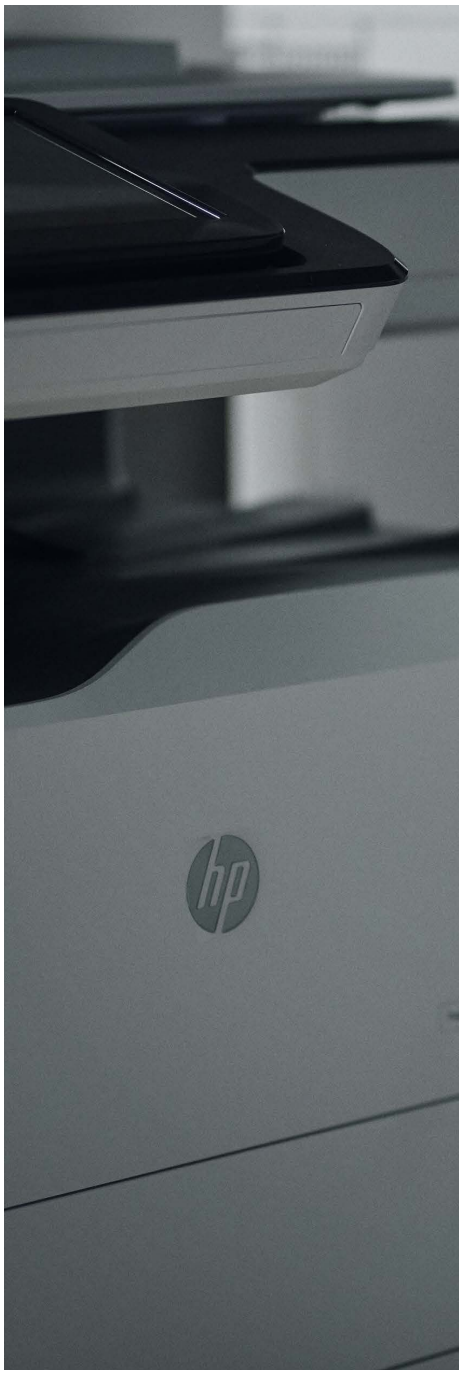
Kimlikleri koruyun: HP Elite bilgisayarlarda güçlendirilmiş çok faktörlü kimlik doğrulamasıyla oturum açma güvenliğini artırın.

Cihazları koruyun: Saldırıları otomatik olarak algılamak, durdurmak ve cihazı kurtarmak için altyapınızı kötü amaçlı yazılım koruması bulunan HP Elite bilgisayarlar ve HP Enterprise yazıcılar ile MFP'lere yükseltin. Gerekmeyen USB bağlantı noktalarını kapatın veya kullanıcı denetimleriyle erişimi kontrol altına alın. Web tabanlı kötü amaçlı yazılımların yayılmasını önlemek için tarayıcı sekmelerini HP Sure Click ile fiziksel olarak yalıtın.[1]

Verileri koruyun: HP Access Control gibi bir yazıcı kimlik doğrulama ve şifreleme çözümü uygulayın.[2] Wi-Fi ve Bluetooth yazıcı özelliklerini kullanmak için kullanıcı kimlik doğrulaması isteyin ve verileri şifreleyin. PrinterOn Enterprise gibi bir mobil kimlik doğrulama ve şifreleme çözümü dağıtın. Bekleyen ve aktarılan verileri şifreleyin.

Belgeleri koruyun: HP Access Control gibi bir kimlik doğrulamalı baskı çözümü kullanın.[2]

İzleme ve yönetim özelliklerini geliştirin: Filo güvenlik politikalarını, yazıcılar için HP JetAdvantage Security Manager[3] veya Microsoft SCCM için HP Printer Security Eklentisi ile veya bilgisayarlar için HP Manageability Integration Kit (MIK)[4] ile otomatik olarak yapılandırın. Sistem günlüklerinin güvenlik olaylarını takip etmesini sağlayın ve gerçek zamanlı uyarılar için cihazları Güvenlik Bilgileri ve Olay Yönetimi (SIEM) araçlarına bağlayın. Yazıcıları güvenlik için yapılandırması amacıyla HP güvenlik eğitimine sahip bir MPS sağlayıcısından yardım alın.



HP'nin kapsamlı güvenlik özellikleriyle şirketinizi koruyun

Dünyanın en güvenilir baskı deneyimi[5]

Çalışma sırasındaki müdahaleleri algılama ve HP Sure Start ve HP Connection Inspector gibi özelliklere sahip HP Enterprise yazıcılar ve MFP'ler BT ekibinin müdahalesine gerek kalmadan saldırıları otomatik olarak algılar, durdurur ve cihazı kurtarır. Diğer korumalar arasında şifrelenmiş sabit sürücüler, yükseltilebilir ürün yazılımları ve SIEM araçlarına güvenlik uyarıları gönderme özellikleri yer alır.

hp.com/go/PrintersThatProtect

Dünyanın en güvenli ve yönetilebilir bilgisayarları[6]

HP Elite bilgisayarlar işletim sisteminin alt, iç ve üst katmanlarını koruma altına alarak en sık karşılaşılan tehditlere karşı koruma sağlar. Çok faktörlü kimlik doğrulama daha güçlü kimlik koruması sağlar, HP Manageability Integration Kit[4] tüm bilgisayar filosunda güvenliğin daha kolay yönetilmesine yardımcı olur. Diğer korumalar arasında sabit sürücü şifrelemesi, HP Sure Recover,[7] HP Sure Click[1] ve HP Sure View yer alır.

hp.com/go/ComputerSecurity

PrinterOn Enterprise

Kuruluşlar için güvenilir, güvenli ağ içi mobil baskı elde edin. Neredeyse tüm masaüstü ve mobil cihazları, birden fazla satıcının güvenilir ağ üzerinde olan ve olmayan yazıcılarına bağlayın.

hp.com/go/businessmobileprinting

HP Access Control[2]

Tüm kuruluşunuzda rol tabanlı baskı kimlik doğrulaması, yetkilendirme ve kimlik doğrulamalı güvenli baskı özellikleri sunarak kontrolü geri kazanın, güvenliği güçlendirin ve maliyetleri düşürün.

hp.com/go/hpac

HP JetAdvantage Security Manager[3]

Kapsamlı bir politika tabanlı baskı güvenliği uyumluluk aracı ile filo güvenliğinizi korumak için gereken maliyet ve kaynakları azaltın. Filonun tamamını kapsayan bir güvenlik politikası oluşturun, cihaz ayarlarını düzeltme işlemlerini otomatikleştirin, benzersiz sertifikalar yükleyip yenileyin ve filo çapında uyumluluk raporları oluşturun.

hp.com/go/securitymanager

Daha fazla bilgi için bkz.
hp.com/go/hpsecure

[1] HP Sure Click, çoğu HP bilgisayarda sunulur ve Internet Explorer ile Chromium™ tarayıcıları destekler. Office ve Adobe Acrobat yüklü olduğunda desteklenen ekler, salt okunur moddaki Office (Word, Excel, PowerPoint) ve PDF dosyalarını içerir.

[2] HP Access Control ayrı satın alınmalıdır. Daha fazla bilgi için lütfen bkz. hp.com/go/hpac.

[3] HP JetAdvantage Security Manager ayrı satın alınmalıdır. Ayrıntılar için bkz. hp.com/go/securitymanager.

[4] HP Manageability Integration Kit önceden yüklü değildir ve hp.com/go/clientmanagement adresinden indirilebilir.

[5] Aynı sınıf rakip yazıcıların yayımlanan güvenlik özelliklerine ilişkin 2018 tarihli HP incelemesine dayanmaktadır. Yalnızca HP, saldırıları izleyip algılayarak otomatik durdurabilen ve önyükleme sırasında yazılım bütünlüğünü kendi kendine otomatik doğrulayabilen güvenlik özelliklerinin bir birleşimini sunar. Yazıcıların listesi için: hp.com/go/PrintersThatProtect. Daha fazla bilgi için: hp.com/go/printersecurityclaims.

[6] 7. Nesil veya üzeri Intel® Core® İşlemciler, Intel® tümleşik grafik kartları ve Intel® WLAN özelliklerine sahip HP Elite Bilgisayarlar için Kasım 2016 itibarıyla yıllık satış hacmi 1 milyon birimin üzerinde olan satıcılar arasından HP'nin herhangi bir ek ücret olmadan sunulan eşsiz ve kapsamlı güvenlik özelliklerine ve HP Manageability Integration Kit tarafından Microsoft System Center Configuration Manager kullanılarak donanım, BIOS ve yazılım yönetimi dahil bir kişisel bilgisayarın her yönüyle yönetimine dayanmaktadır.

[7] HP Sure Recover, 8. nesil Intel® veya AMD işlemcilere sahip HP Elite bilgisayarlarda sunulur ve açık, kablolu ağ bağlantısı gerektirir. Birden fazla dahili depolama sürücüsüne sahip olan Intel® Optane™ platformlarında sunulmaz. Veri kaybını önlemek için önemli dosyalarınızı, verilerinizi, fotoğraflarınızı, videolarınızı vb. yedeklemeniz gerekir.

Güncelleştirmeler için kaydolun
hp.com/go/getupdated

İş arkadaşlarınızla paylaşın

4AA7-0231TRE, Ağustos 2018, Rev. 1