ÇÖZÜMÜNÜZ,
KASPERSKY ENDPOINT
SECURITY FOR
BUSINESS DEĞİLSE
BİR UÇ NOKTA KORUMA
PLATFORMU DEĞİLDİR

YALNIZCA

ENTEGRE PLATFORMLU GÜVENLİK ÇÖZÜMÜNÜN SUNABİLECEĞİ 10 FAYDA

KASPERSKY lab

Kaspersky Lab'in Küresel BT Güvenlik Riski Raporu, şirketlerin yüzde 94'ünün son 12 ayda dış kaynaklı bir güvenlik olayı biçimine maruz kaldığını ortaya çıkardı[1].

Tehditlerin hacmi ve karmaşıklığı katlanarak artarken, her büyüklükten işletme de genelleştirilmiş bir "kötü amaçlı yazılım" kavramından yola çıkan rastgele, genel bir yaklaşımı benimsemek yerine BT güvenlik risklerini, özellikle de hedef gözeten saldırıları ve kendisini bu saldırılardan nasıl koruyabileceğini daha iyi anlamaya başlıyor.

Ancak maalesef çoğu BT güvenliği satıcısı bu rastgele, geniş yaklaşımı devam ettiriyor: Yeni teknolojileri satın alıp bunları farklı, genellikle uyumsuz kod tabanlarıyla birleştirerek karmaşıklığa yol açıyor ve en az çözdükleri sorunlar kadar yeni sorunlar yaratıyorlar.

Geleneksel uç nokta güvenliği (ayrı kötü amaçlı yazılımdan koruma, şifreleme, cihaz ve ağ kontrolleri) günlerinin sonuna geliyor. BT güvenliği, gelişmiş tehdit koruması ve veri koruması alanlarında sıkı biçimde entegre edilmiş güvenlik teknolojileri vaat eden uç nokta koruma platformları (EPP'ler) trendi gitgide güçleniyor.

Ancak "entegrasyon" ile gerçek bir platform arasında büyük farklılıklar var. Entegrasyon söz konusu olduğundaysa bütünlüğün farklı derecelerinden bahsedilebilir. Çoğu satıcı "entegrasyon" terimini "uyumlu"nun eşanlamlısı olarak kullanıyor.

Bazı satıcılar içinse "uyumlu" ifadesi, 40'a varan alımla satın alınan ürünleri bir araya getirip kendi kod tabanlarında, müşterilerinin kod tabanlarını dikkate almadan çalıştırmayı denemek anlamına geliyor.

Birçok satıcı "entegre" çözümler vaat ediyor ancak biraz yakından incelediğinizde, birlikte "sorun çıkarmadan çalışma" ile bilgiye dayalı ürün yol haritaları ve geliştirme çabalarının ürünü olan gerçek sinerji arasında önemli bir fark olduğunu göreceksiniz. Bazı satıcılar iş alımlarını bütünleştirmede sorun yaşasa bile gerçekten entegre platformlar sunduğunu iddia edebiliyor.

Bir sonraki en iyi çözüm gibi görünen ürünü satın almak, aynı vizyon veya koruma bütünlüğünü sunamaz.

[1] Küresel IT Güvenliği Risk Raporu 2014.

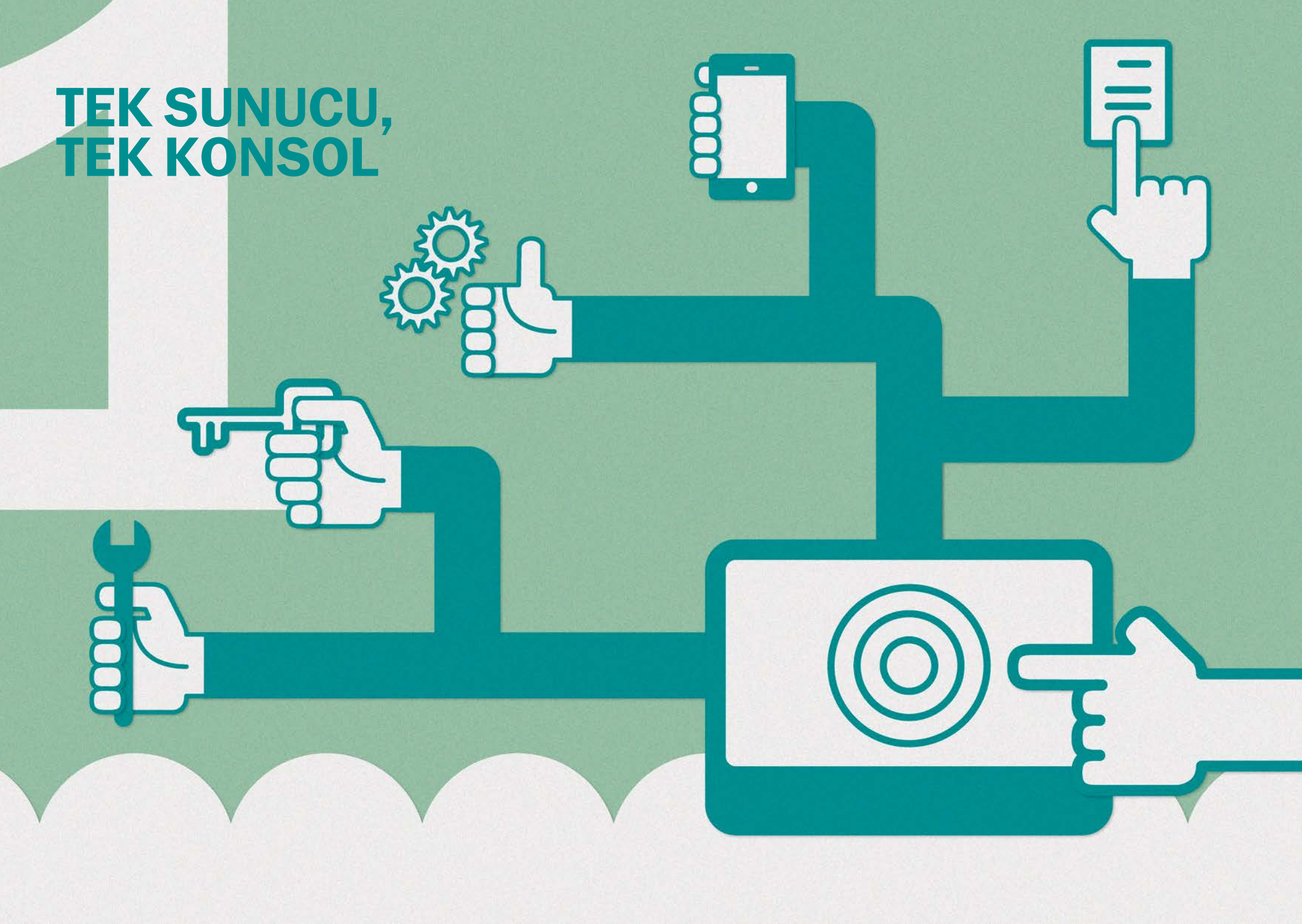
Yalnızca gerçekten derinlemesine entegre bir platform çözümünün sunabileceği bazı avantajlar vardır. Kaspersky Endpoint Security for Business, benzersiz konumuyla BT yöneticilerine şu faydaları sağlar:

1. Tek sonucu, tek konsol
2. Tek aracılı mimari*, basit kurulum
3. Tek İlke Avantajı
4. Sinerjinin Etkisi — parçalarının toplamından fazlası
5. Birleştirilmiş yönetici hakları yönetimi — tek konsolla daha fazla denetim ve kontrol özelliği

6. Ortak yapı, görünüm ve his — daha hızlı, daha kolay raporlama
7. Daha net ve derin veri görünümü — entegre panolar ve raporlama
8. Birleştirilmiş lisans yönetimi ve kontrolü — verimliliği artırın, kontrolü ele alın
9. Şirket içinde geliştirilen tek kod tabanlı entegrasyonu derinleştirir
10. Entegre satın alma modeli — ihtiyacınız olan tüm işlevlere tek satın alımla sahip olun

* Platform başına tek aracılı yapı (Windows, Linux, Mac).

TEK SUNUCU, TEK KONSOL



1 TEK SUNUCU, TEK KONSOL

Kötü amaçlı yazılımdan koruma seçeneğinden veri koruması, mobil cihaz yönetimi ve sistem yönetimine uç nokta güvenliğinin her yönünü kapsayan, sıkı biçimde entegre edilmiş, tek yönetim sunucusu ve yönetim konsolu Kaspersky Security Center'ı sunan Kaspersky Lab çözümü, bu açıdan benzersizdir.

Güvenlik ilkeleri ve raporlama, LDAP dizinleri ve Microsoft Exchange gibi harici kaynaklarla entegre edilmiş tek bir konsol aracılığıyla yönetilir. Donanım ve yazılım envanteri veritabanlarının yanı sıra yazılım güvenlik açıkları/güncellemeleri de dahil edilir; böylece aynı veriler farklı işlevlerde kullanılabildiği için entegrasyon ve sinerji olanakları artırılır. Farklı sunucular veya veri kümelerini senkronize etmek gerekmez; her şey tek seferde, aynı sunucuya yüklenir ve aynı konsoldan yönetilir.

Bu derin entegrasyon ve sinerji özellikleri, çoğu Kaspersky'nin platformuyla aynı derinlikte entegrasyon olanağı sunamayan birden fazla, ayrı veritabanlarına sahip alınmış teknolojilerden oluşan rakip çözümlere karşı bariz bir avantaj sunar.

Bu özelliğin faydaları şunlardır:

- **Hızlı, kolay dağıtım:** Tek yönetim sunucusu, konsol kurulumu ve yapılandırma işlemi kullanıma hazır, tamamen entegre işlevsellik sunar.

- **Tek yönetim sunucusu donanımı:** Her ayrı yönetim sunucusu ve konsolu için farklı donanım, sistem veya ek bileşen gereksinimleriyle uğraşmak gerekmez. Kaspersky çoğu dağıtımda sadece TEK sunucu gerektirir.

- **Tek yönetim sunucusu yazılımı:** Küçük işletmeler için altyapı yönetimi kolay olmakla birlikte, daha büyük dağıtımlar için ölçeklenebilir.
  — Bazı ürünler, Kaspersky Lab'e benzer işlevsellik sunmak için ilk kez kullanıma sunulduktan sonra başka paketlerin yüklenmesini gerektirebilir.
  — Daha rahat bir çözüm için Kaspersky platformu, zaman kazandırmak amacıyla kurulum işleminin parçası olarak ek uygulamalar (örn. Microsoft ortamında gerekenler) içerir. Böylece başarıyla çalışır.

TEK ARACILI MİMARİ*, BASİT KURULUM

* Platform başına tek aracılı yapı (Windows, Linux, Mac).

2 TEK ARACILI MİMARİ*, BASİT KURULUM

Donanım ve yazılım yapılandırmalarında eksiksiz, kolayca ulaşılabilir uyumluluk ve sinerji sağlamak için derin kod entegrasyonundan yararlanan bir uç nokta aracısı sunan Kaspersky çözümü, bu açıdan benzersizdir.

Gerçek uç nokta koruma platformları, görevleri yürütmek için minimum sayıda ayrı aracı kullanarak karmaşıklığı azaltan ve entegrasyonu derinleştiren modern bir mimariye sahiptir. Güvenlik açığı taraması, uygulama güncellemeleri ve yama yönetimi gibi birbirleriyle ilişkili işlevler (ve kötü amaçlı yazılımdan koruma ve şifreleme gibi koruma modülleri) tek bir aracı mimarisine sahiptir, böylece performans artırılır ve yönetim hizmet alanı azaltılır.

Çoğu rakip teklif yama yönetimi, uygulama kontrolü veya şifreleme gibi işlevler ve özellikler için aynı makinede birden fazla aracı gerektirir. Bu, aracı uyumluluğuyla ilgili olası sorunlara yol açar ve ek testlerin yapılmasını gerektirir.

* Platform başına tek aracılı yapı (Windows, Linux, Mac).

Bu özelliğin faydaları şunlardır:

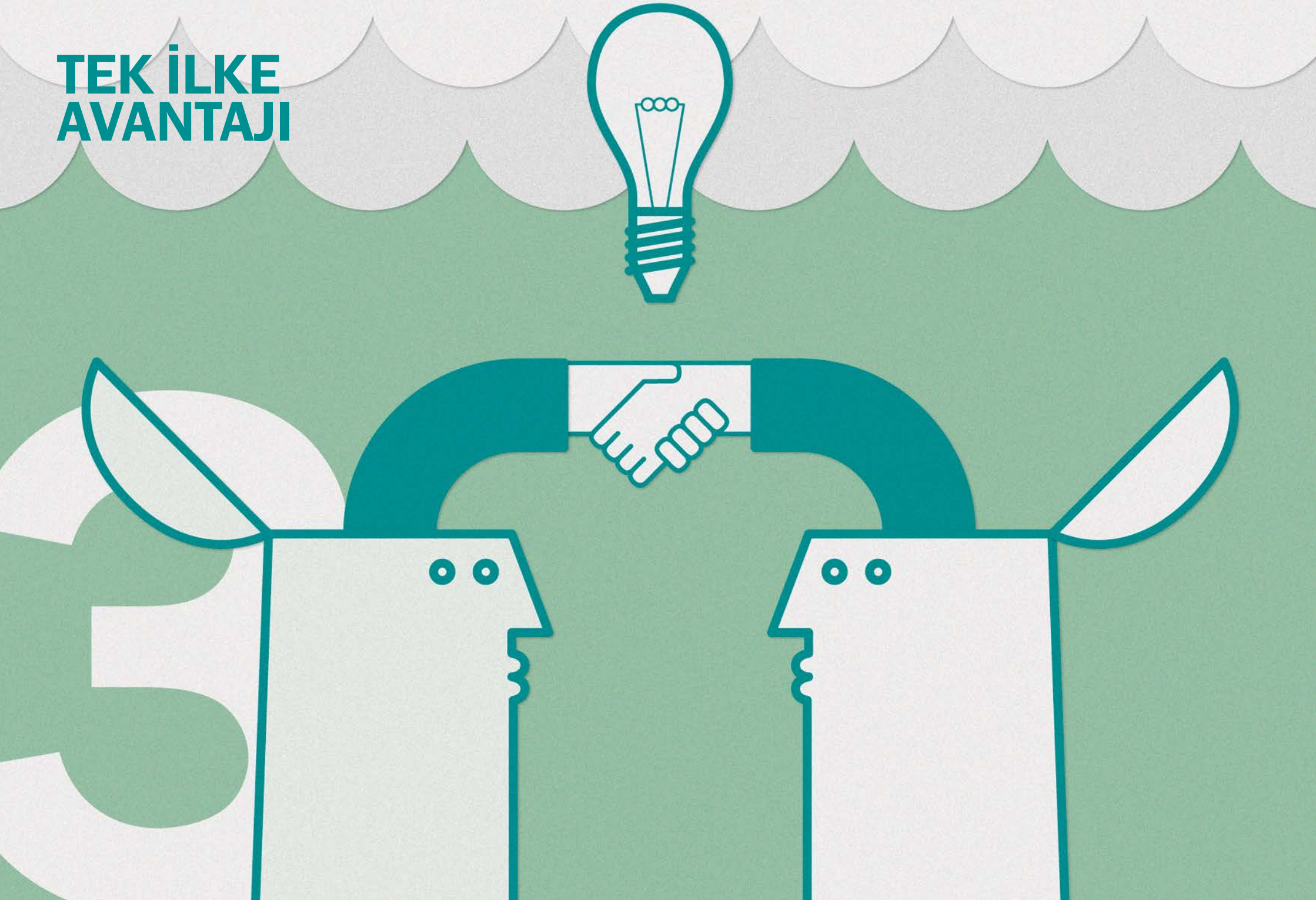
- **İlk dağıtım ve güncellemelerde zaman kazandırır:** Kontrol edilecek tek bir kurulum görevi vardır; sistemi yeniden başlatma gereksinimleri yoktur.

- **Farklı sistem gereksinimleriyle uğraşmak gerekmez:** Alım yoluyla büyümenin yazılım uyumluluğu zorlukları oluşturduğu sır değildir. Satın alınarak eklenen işlevler, birlikte geldikleri yazılıma ek olarak yeni, ayrı destek gereksinimleri oluşturabilir. Bunu dağıtıma başlarken fark etmeniz pek de iyi sonuçlar doğurmaz… Yönetilen uç nokta platformları/cihazları için farklı yazılım bileşenleri arasında kusursuz uyumluluğu sadece organik, entegre edilmiş bir gelişim yaklaşımı garanti edebilir. Bu aynı zamanda istemci tarafındaki uyumluluk testlerinin sayısını azaltır.

- Sistem performansı ve yönetim hizmet alanında **daha az etki.**

- **Sinerji senaryolarının geliştirilmesi için temel:** Derin entegrasyon esnekliğe ve daha iyi işlevselliğe olanak tanır. Kaynak hizmet alanını artırmadan özellikleri genişletin.

TEK İLKE AVANTAJI



3 TEK İLKE AVANTAJI

Karmaşıklık güvenliğin düşmanıdır ancak bir kuruluşta bilgi güvenliğini her yönüyle yönetmek için genellikle birbirinden farklı birçok çözümü bir arada kullanmak gerekir. Yönetim işlemlerini ne kadar basitleştirebilirseniz o kadar netliğe sahip olur ve riski azaltırsınız.

Gerçek bir Uç Nokta Koruma Platformu, kurumsal altyapıdaki uç noktaların keşfedilmesini, dağıtılmasını, ilke yapılandırmasını ve güncellenmesini kontrol eder. Kaspersky Endpoint Security'nin platform başına tek aracılı yapısı, yöneticilerin yönetilen grup için tek etkin ilke ayarlayarak birden fazla ilke incelemesi ya da korelasyonuna gerek olmadan tüm gerekli bileşenleri kapsamasını sağlar.

"Ağ Aracısı" uç noktayı yönetici sunucusuna bağlayarak sistem yönetim görevlerini gerçekleştirir (örn. yazılım ve donanım envanteri, güvenlik açığı taraması ve yama yönetimi) ve işlevler arasında gerçek esneklik ve sinerjiye olanak tanır.

Bu özelliğin faydaları şunlardır:

- **Basitleştirilmiş ilke ve görev yönetimi:** Tek bir paylaşılan parametre ve ön gereksinim dizisi sayesinde yönetilen gruplar, sunum ayarları, bildirimler, ilk uygulaması optimize edilerek BT yöneticisi için fazlalık olan işlemler ve görevler ortadan kaldırılır.

- **İlke ve görev uygulama üzerinde kolay kontrol:** Tek pano ile dağıtım ve yürütme raporlaması, ilke durumu ve uyumluluğunun tüm ağda bir bakışta kapsamlı biçimde görülmesini sağlar.

- **Modernleştirilmiş ilke ve görev değişiklikleri:** Değişiklikler tek adımda yapılır. Otomatik ilke atama, çeşitli koruma ayarlarından uygulama, cihaz ve web kontrolleri ile şifreleme ilkelerine kadar çeşitli güvenlik parametrelerini aynı anda kapsayabilir.

SİNERJİNİN ETKİSİ — PARÇALARININ TOPLAMINDAN FAZLASI

4 SİNERJİNİN ETKİSİ — PARÇALARININ TOPLAMINDAN FAZLASI

Kaspersky'nin güvenli platformunun temelini oluşturan entegre uç nokta koruma özellikleri, daha karmaşık, gelişmiş güvenlik yönetim senaryolarının bile uygulanmasını kolaylaştırır. Gerçek entegrasyonun sunduğu güvenlik, her bir özelliği oluşturan parçaların ötesine geçer, örneğin:

Bir işletme, İnternet tabanlı tehditlere karşı kapsamlı korumanın yanında ilke tabanlı web trafiği ve indirilen dosyaları tarama işlevlerini uygulamak için Kaspersky'nin uygulama kontrolü özelliğini kullanarak sadece BT'nin onayladığı tarayıcının kullanılmasını zorunlu kılabilir. Daha sonra bu tarayıcı, yüksek öncelikli güvenlik açığı yamalarının otomatik olarak uygulanmasıyla daha güvenli bir hale getirilebilir ve Otomatik Güvenlik Açıklarını Önleme ile sıfır gün saldırılarına karşı korunabilir. Bu şekilde Kaspersky'nin entegre özellikleri, çok geniş bir saldırı vektörüne karşı güvenlik şemsiyesi sağlar. Sinerjinin Etkisi ile kastettiğimiz şey budur.

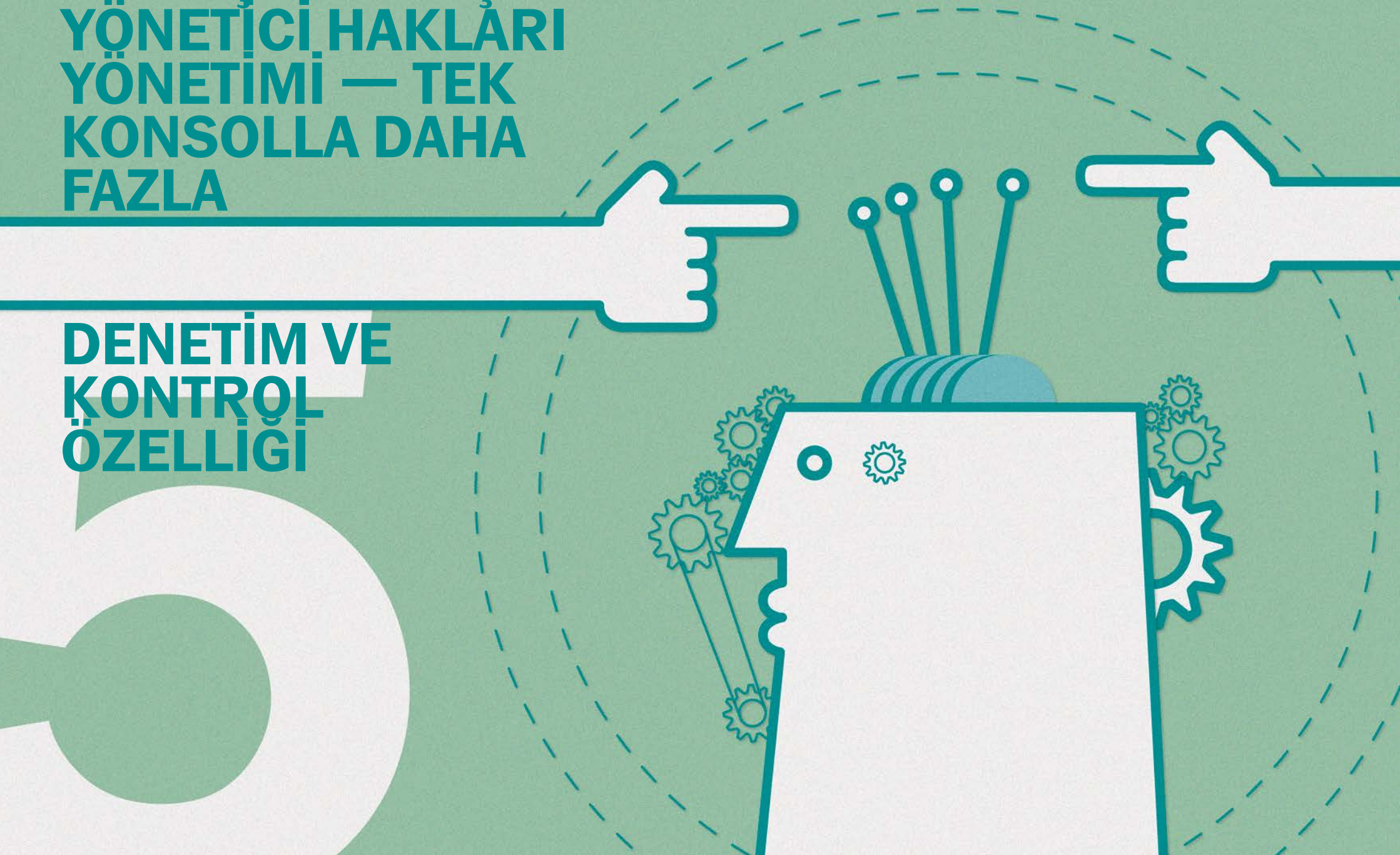
Bu özelliğin faydaları şunlardır:

- **Güvenlik yönetimi uygulamaları ve farklı işlevlerden toplanan bilgilerin çapraz paylaşımı, örneğin:**
  - — Çıkarılabilir cihazlar hakkında toplanan bilgiler cihazları kontrol etmek ve şifrelemek için kullanılır;
  - — Uygulamalar hakkındaki bilgilerin uygulama kontrolü ve şifreleme ilkelerine katkısı olur;
  - — Cihazlarda veri güvenliğine entegre edilen mobil cihaz yönetimi (MDM);
  - — Yama yönetimi kararları güvenlik açığı değerlendirmelerine göre verilebilir.

Sinerjinin Etkisi yukarıda açıklanan senaryolarla sınırlı değildir. Kaspersky'nin derin kod entegrasyonu, donanım ve yazılım yapılandırmaları arasında eksiksiz, kolayca ulaşılabilen uyumluluk ve sinerji sağlar. Kaspersky platformuyla güvenlik, her bir özelliği oluşturan parçaların ötesine geçer.

BİRLEŞTİRİLMİŞ YÖNETİCİ HAKLARI YÖNETİMİ — TEK KONSOLLA DAHA FAZLA

DENETİM VE KONTROL ÖZELLİĞİ



5 BİRLEŞTİRİLMİŞ YÖNETİCİ HAKLARI YÖNETİMİ — TEK KONSOLLA DAHA FAZLA DENETİM VE KONTROL ÖZELLİĞİ

BT departmanlarında personel sayısının yetersiz olması, çoğu KOBİ ve kuruluşta görülen bir sorundur. Ekonomik kesintiler ve BT karmaşıklığın artması, BT yöneticilerinin görevleri artarken bunlara ayırabilecekleri zamanın azalması anlamına gelir.

Kaspersky'nin Uç Nokta Koruma Platformu, günlük güvenlik görevleri için birleştirilmiş yönetim araçları sağlayarak bu sorunu çözer. Derin entegrasyon ayrıcalık kontrolü ve günlükleri tek bir konsoldan yönetmeye olanak tanır. Tüm işlemler tek bir günlüğe kaydedilir; rakip ürünlerinse ayrı konsollar ve sunuculardan veri çekmesi gerekir.

Birleştirilmiş hak yönetimi ve günlük kaydı, personel eylemlerinin daha etkili biçimde kontrol edilmesine olanak tanıyıp bu eylemler hakkında bilgi sunarak izinlerin daha etkili biçimde yönetilmesini destekler. Bunun sonucunda güvenlik artar ve BT işlemleri ve yönetimi üzerinde denetim kontrolü sağlanır. Üstelik tüm bunlar tek bir konsolla gerçekleşir.

Bu özelliğin faydaları şunlardır:

- **Kolay tanımlanan ve kontrol edilen izinler:** "BT'cinin" her şeyden sorumlu olduğu tipik bir KOBİ'de, okuma/değiştirme, erişim vs. izinlerini ayarlama gibi güvenlik ile ilgili tüm görevleri gerçekleştirmek kolay olur.

- **Olaya hızlı müdahale ve birleştirilmiş olay günlüğü:** BT yöneticileri de insandır; hata yapabilirler ve bir güvenlik olayı durumunda hızla müdahale edebilmek çok önemlidir. İzinlerin hızla değiştirilmesine veya engellenmesine olanak tanıyan işlev ve bu değişiklikleri takip edebilme özelliği, önemli unsurlardır. Ayrı çözümlerde karmaşık olaylar için birden fazla analiz işlemi oluşturmak gerekebilir. Karmaşıklığı ortadan kaldıran Kaspersky; uç nokta güvenliği, ilke ve yönetim etkinliği değişikliklerini tek bir günlük dosyasında toplar ve tek bir yönetim konsolu arabiriminden sağlar.

ORTAK YAPI, GÖRÜNÜM VE HİS — DAHA HIZLI, DAHA KOLAY RAPORLAMA

6 ORTAK YAPI, GÖRÜNÜM VE HİS — DAHA HIZLI, DAHA KOLAY RAPORLAMA

Yöneticiler baskı altındayken kendilerine zaman kazandıracak veya bir görevi gerçekleştirmeyi kolaylaştıracak her fırsattan yararlanmak ister. Birleştirilmiş, entegre özelliklere ve ortak arabirime sahip Uç Nokta Koruma Platformları raporlama, analiz ve olay yönetimini kolaylaştırır. Kaspersky Security Center da ortak görünüme ve hisse sahip benzer bir rapor yapısı üretir.

Bir BT yöneticisinin iş günü genellikle rutin ama önemli sayısız görev içerir. Bu görevlerin tamamı izlenmeli ve raporlanmalıdır. Karışık çözümlü bir ortamda bu iş için çok sayıda pano kullanılır ve bu panolar raporları PDF'den HTML ve doğrudan e-postaya kadar farklı biçimlerde üretir. Tüm bunlara bakmaya VE her şeyin yolunda gittiğinden emin olmaya kimin zamanı vardır?

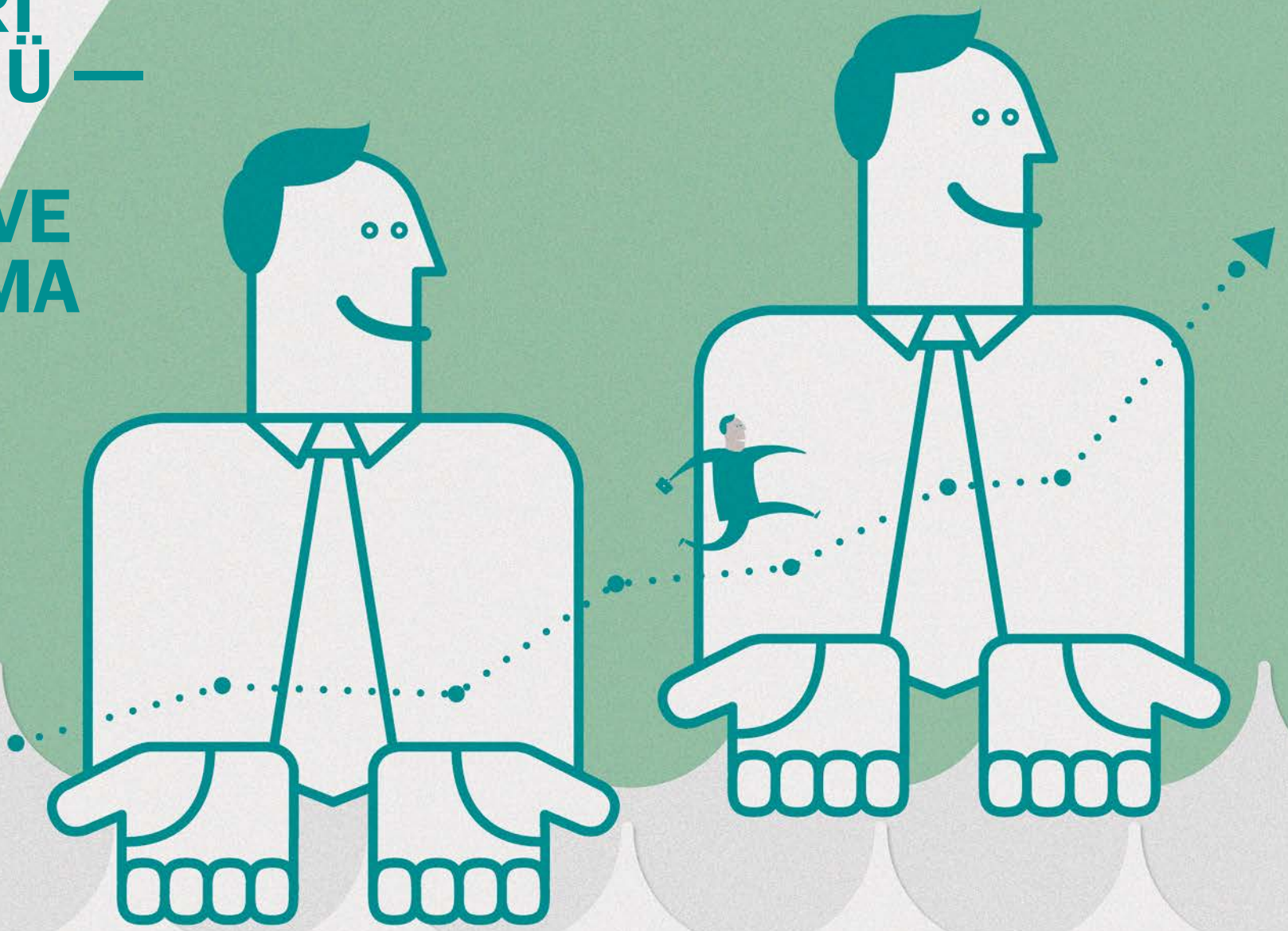
Böyle bir ortamda, kullanılabilirlik veya verimlilikte elde edilecek en küçük gelişme bile oldukça zaman kazandırabilir ve zaten işi başından aşkın olan BT güvenliği yöneticilerinin iş yükünü (ve tabii ki stresini) azaltabilir. Görünümü ve hissi değişmeyen ortak raporlama analiz ve değerlendirmeyi kolaylaştırır, olay yöntemini geliştirir ve BT güvenliğine proaktif şekilde yaklaşmayı destekler.

Bu özelliğin faydaları şunlardır:

- **Daha kolay ve hızlı rapor analizi:** Rapor şablonlarında aynı terminoloji ve yapı kullanılır. "Bilgisayar, PC, düğüm, makine", yönetilen uç nokta için kullanılan eşanlamlı terimlerdir. Bu terimlerin hepsi ürünlerde ve satıcı literatüründe birbirinin yerine kullanılır; işin içine yeterince ürün girdiğinde bu durum kafa karışıklığı yaratabilir. Karışık çözümlü ortamınızdaki güvenlik bileşenlerinin her biri benzer bir dil sorununa sahip olursa ne olur? Bu bileşenlerinin her birinin her parametresi "aynı ama farklı" adlara sahip olursa neyle karşı karşıya kalırsınız? Böylesine karmaşık bir ortamda, tehditleri veya diğer olayları araştırmak, kuruluma aşina olan yöneticiler için bile göründüğünden çok daha karmaşık bir hal alır. Yöneticiler bu karmaşıklığı kabul edebilir ancak denetçiler veya düzenleyiciler gibi şirket dışı müfettişlerin de dahil olduğu bir durumda ne olur? Onlara altyapınızın karmakarışık bir görünümünü sunduğunuzda, yanlış bir izlenim bırakabilirsiniz.

- **Basitleştirilmiş olay yönetimi:** Farklı BT altyapısı düğümlerinde kötü amaçlı yazılım veya ilke ihlalleri gibi benzer olayları kolayca tanıyın.

DAHA NET VE DERİN VERİ GÖRÜNÜMÜ — ENTEGRE PANOLAR VE RAPORLAMA



7

DAHA NET VE DERİN VERİ GÖRÜNÜMÜ — ENTEGRE PANOLAR VE RAPORLAMA

Uç Nokta Koruma Platformları panolar ve raporlamaya bütünsel bir yaklaşım sağlamalıdır. Gerçek entegrasyon arabirim görünümü ve hissinin ötesine geçer. Örneğin, yönetim konsolunda tek bir "uç nokta özellikleri" sekmesi tıklandığında uygulanan ilkeler, durum güncellemeleri ve olaylar gibi yönetilen istemcinin güvenliğiyle ilgili tüm bilgiler sunulmalıdır.

Panolar ve raporlarda araştırma sürecini kolaylaştırmalı ve uç noktanın daha görünür olmasını sağlamalıdır. Entegrasyon farklı bileşenlerden bilgi toplamaya olanak tanıyarak bunu önemli ölçüde kolaylaştırır.

Bu özelliğin faydaları şunlardır:

- **Tüm uç nokta güvenliği bileşenleri için tek pencereli bölme:** "Kahve içerken" bakabileceğiniz, tüm sabahınızı almayan bir pano; yönetilen uç noktaların durumu, dağıtım görevlerinin yürütülmesi ve lisans kontrolünün yanı sıra ana güvenlik olaylarını içerir.

- **Modernleştirilmiş kapsamlı inceleme ve analiz:** Uç nokta yönetimi, güvenlik açığı değerlendirmesi ve yama yönetimi, donanım ve uygulama envanteri ve oluşturulan kullanıcı hesapları gibi çeşitli açılardan analiz yapmak ve veri toplamak için birbirine bağımlı raporları kapsamlı biçimde inceleyin. Kötü amaçlı yazılım algılama ve veri şifreleme durumu gibi koruma durumu ve olaylar için kolay görünürlük. Bu, güvenlik analizi ve araştırmayı modern, kolay bir işlem haline getirir.

- **Kullanıma hazır idari raporlama:** İdari raporlama, BT güvenliği yöneticisinin sorumluluklarının temel bir bileşenidir. Farklı konsollar ve veri kümelerinden kapsamlı raporlar oluşturmak, zaman alan ve başınızı ağrıtan bir iştir. Bu yüzden Kaspersky'nin Uç Nokta Güvenlik Platformu idare raporlama işlevini kullanıma hazır olarak sunar. Üçüncü taraf araçları kullanarak özel raporlar oluşturmak gerekmez. Diğer projelere odaklanmak için daha fazla zamanınız olur.

BİRLEŞTİRİLMİŞ LİSANS YÖNETİMİ VE KONTROLÜ — VERİMLİLİĞİ ARTIRIN, KONTROLÜ ELE ALIN

8 BİRLEŞTİRİLMİŞ LİSANS YÖNETİMİ VE KONTROLÜ — VERİMLİLİĞİ ARTIRIN, KONTROLÜ ELE ALIN

Kurumsal ağın tamamındaki tüm güvenlik çözümlerinin lisanslarını yönetmek artık her zamankinden kolay. Kaspersky Labs sayesinde TÜM işlevler tek bir lisans kullanarak etkinleştirilir: uç nokta güvenliği, veri koruması, mobil cihaz yönetimi ve sistem yönetimi.

Bu tek lisans durum veya konum, ağdaki fiziksel veya sanal makineler ve sabit veya mobil cihazlardan bağımsız olarak kurumsal uç nokta altyapısı genelinde kolayca dağıtılabilir. Kaspersky'nin entegre lisans yönetimi işlevi, lisans doğruluğunu daha sıkı biçimde kontrol ederken ödediğiniz paranın karşılığını daha etkili şekilde kullanmanıza olanak tanır.

Bu özelliğin faydaları şunlardır:

- **Lisans denetimi için tek pencereli bölme:** Durumu izlemek ve kontrol etmek için farklı lisans kontrol araçlarına başvurmak gerekmez.
- **Verimli lisans kullanımı:** Değişen BT ortamında esnek dağıtımla maliyetleri azaltın. Buna örnek olarak geleneksel PC'ler ve dizüstü bilgisayarlardan aynı işlevlere sahip mobil cihazlara geçiş yapmak verilebilir.
- **Güvenlik çözümünüzü kolayca yükseltme imkanı:** Kaspersky'nin Uç Nokta Koruma Platformu ile güvenlik işlevini ihtiyaçlarınıza göre artırabilirsiniz. Uç nokta güvenliğiyle işe başlayın ve yeni bir lisans ekleyerek şifreleme veya sistem yönetimi gibi özellikleri kolayca etkinleştirin.

ŞİRKET İÇİNDE GELİŞTİRİLEN TEK KOD TABANLI ENTEGRASYONU DERİNLEŞTİRİR

9 ŞİRKET İÇİNDE GELİŞTİRİLEN TEK KOD TABANLI ENTEGRASYONU DERİNLEŞTİRİR

Entegre Uç Nokta Koruma Platformumuzun kalbinde Kaspersky'nin kendi bünyesinde oluşturduğu ve sürdürdüğü tek kod tabanı bulunur.

Diğer satıcılar hızla değişen tehdit ortamında ürün tekliflerini artırmak için alım stratejisini izlerken, tüm çözümlerini kendi bünyesinde geliştiren ve sürdüren Kaspersky bu açıdan benzersizdir. Diğer satıcıların aksine, bu yaklaşım kod tabanı seviyesinde derin entegrasyonu destekleyerek bu belgede daha önce açıklanan faydaları sunmamıza olanak tanır.

Bu özelliğin faydaları şunlardır:

- Tek yönetim sunucusu ve yönetim konsolu;
- Tek uç nokta istemci mimarisi;
- Tek ilkeler ve birleştirilmiş görevler;
- Entegre işlevsellik için sinerji etkisi;
- Entegre panolar ve raporlama.

Kod tabanı ve geliştirme sürecinin aynı olması güncelleme ve yama yönetimini hızlandırmaya da yardımcı olur: Çoğu rakip üründe iki veya daha fazla uygulamayı (ve bunlara eşlik eden bileşenleri) güncellemek zorunda kalan kullanıcılar, Kaspersky ile yalnızca tek bir uygulamayı günceller.

ENTEGRE SATIN ALMA MODELİ — İHTİYACINIZ OLAN TÜM İŞLEVLERE TEK SATIN ALIMLA SAHİP OLUN

10

10 ENTEGRE SATIN ALMA MODELİ — İHTİYACINIZ OLAN TÜM İŞLEVLERE TEK SATIN ALIMLA SAHİP OLUN

Tek bir sipariş tüm güvenlik ihtiyaçlarınızı ve işlevleri kapsar; tek bir lisans her şeyi etkinleştirir.

Bu özelliğin faydaları şunlardır:

- **Tek paketle farklı ihtiyaçları karşılayın:** Kaspersky kullanıcıları, farklı müşteri ihtiyaçlarını karşılayan farklı seviyelerdeki çeşitli işlevleri tek bir lisans paketiyle alabilir. Bu, benzersiz bir avantajdır.

SON OLARAK...

Kaspersky Lab ile kullanıcılar başından sonuna aynı kod tabanı ve Ar-Ge kullanılarak geliştirilen gerçek bir Uç Nokta Koruma Platformuna sahip olur. Entegre kötü amaçlı yazılımdan koruma ve yazılım güvenlik açığı teknolojilerimiz tamamen kendi bünyemizde, daha etkili korumayı geliştirmek için modern tehditlerin sistemlere nasıl sızdığını düzenli olarak araştıran özel araştırma grubumuz tarafından geliştirilmiştir.

Kaspersky Lab'in kendi uygulama beyaz listesi ve güvenlik açığı araştırma grubu, iş ortaklarımız ve satıcılarımızdan oluşan ekosistemimizi yöneterek sürekli olarak güncellenen bir yasal yazılım veritabanı sunarken mevcut yamalar hakkında en güncel bilgileri sağlar.

Uç nokta güvenliği ve istemci/sistem yönetimi teknolojisinin birleştirilmesi büyüyen bir trenddir. Tamamen kendi bünyesinde oluşturduğu kod tabanlı ve geliştirme süreciyle güvenlik işlevleri ve geleneksel olarak sistem yönetiminin bileşenleri olarak görülen işlevler arasındaki açık sinerjiden yararlanan Kaspersky Lab, bu yönüyle benzersizdir.

Kaspersky Lab entegrasyonu gerçek bir Uç Nokta Koruma Platformu sunuyor. İsteğe bağlı değil, optimum korumaya sahip olun.

Daha fazla bilgi için: **www.kaspersky.com/business**

ŞİMDİ BAŞLAYIN: 30 GÜNLÜK ÜCRETSİZ DENEME

Hiçbir zorunluluk içermeyen deneme sürümüyle üstün güvenlik platformumuzun işletmenizi kötü amaçlı yazılım ve siber suça karşı nasıl koruduğunu keşfedin.

Ürünlerin tam sürümlerini indirmek için bugün kaydolun ve ürünlerimizin BT altyapınızı, uç noktalarınızı ve gizli işletme verilerinizi ne kadar başarılı koruduğunu değerlendirin.

KASPERSKY LAB HAKKINDA

Kaspersky Lab, bugün uç nokta koruma çözümleri alanında dünyanın en büyük özel tedarikçisidir. Şirket uç nokta kullanıcılarına yönelik güvenlik çözümleri üreten tedarikçiler arasında dünyada ilk dört arasında yer alır*. 17 yıldan daha uzun bir geçmişiyle BT güvenliği konusunda birçok yeniliğe imza atan Kaspersky Lab, büyük kuruluşlar, KOBİ'ler ve tüketicilere yönelik verimli dijital güvenlik çözümleri sunar. İngiltere'de tescilli bir holding şirketine sahip olan Kaspersky Lab, bugün dünya çapında 200'ün üzerinde ülke ve bölgede faaliyet göstermekte, dünyanın dört bir köşesindeki 300 milyonun üzerinde kullanıcıya koruma sağlamaktadır.
Daha fazla bilgi için **www.kaspersky.com** adresini ziyaret edin.

* Şirket, 2012 IDC Dünya Çapında Uç Nokta Güvenliği Gelirleri değerlendirmesinde Tedarikçi kategorisinde dördüncü sırada yer almıştır. Bu değerlendirme, Worldwide Endpoint Security 2013-2017 Forecast and 2012 Vendor Shares (Dünya Çapında Uç Nokta Güvenliği 2013–2018 Tahminleri ve 2013 Tedarikçi Pazar Payları) (IDC No. 242618, Ağustos 2014) başlıklı IDC raporunda yayınlanmıştır. Raporda yazılım tedarikçileri, 2012 yılındaki uç nokta güvenliği çözümlerinin satışından elde edilen kazanca göre sıralanmıştır.

İLETİŞİME KATILIN

#securebiz

Bizi YouTube'da izleyin


Bizi Slideshare'de görüntüleyin


Bizi Facebook'ta beğenin


Blogumuzu inceleyin


Bizi Twitter'da takip edin

LinkedIn'de bize katılın

KASPERSKY lab