

# Neden Citrix Workspace günümüzde uzaktan çalışma sistemleri için, VPN'den daha iyi bir seçimdir?



Günümüzde çok daha fazla insan uzaktan çalışıyor. VPN, kurumsal sistemlere ve dosyalara güvenli erişim sağlamak için, tercih edilen geleneksel güvenlik çözümüdür. Ancak VPN'lerin yönetimi karmaşıktır ve ağ düzeyinde güvenlik riskleri yaratırlar. Ayrıca kısıtlı bir kullanıcı deneyimi sunarlar, ölçeklenebilirlik ve gizlilik konusunda da, yeterli değildir.

Geleneksel VPN'lerin, eski güvenlik modeli erişimi isteğe göre oluşturan ve Zero Trust çerçevesinde katı şartlara sahiptir. Citrix Workspace, - ağ üzerinden kullanılan, yönetilen veya yönetilmeyen, kendi cihazını getir (BYOD) ş modeli de dahil olmak üzere - tüm intranet web, hizmet olarak yazılım (SaaS), mobil ve sanal uygulamalara erişmek için bulut tabanlı VPN'siz bir çözüm sunuyor. Bu dosyada, uzaktan çalışanlar için güvenlik, performans ve ölçeklenebilirlik gereksinimlerini karşılamak için Citrix Workspace'in neden VPN'den daha iyi bir seçenek olduğunu sizler için, inceledik.

## VPN'ler karmaşık bir yönetime sahiptir

Pozisyonlarına veya erişim iznine sahip oldukları kaynak türlerine bağlı olarak, uzaktan çalışanlara genellikle farklı giriş yöntemleri verilir. Herhangi bir çalışan, yönetici, veya iş ortağı aynı VPN içinde farklı oturum açma noktaları kullanır. Bunun için, genellikle birden çok VPN gerekir ve SaaS uygulamalarına erişim için farklı bir SSO portalı kullanılır. Sistem yöneticileri için bu zaman alıcı bir yöntemdir ve yönetilmesi için ek kaynak gerektirebilir. Acil durum kapasitesi eklemek, bir kapsamlı donanım yükseltmesi veya uzun sürebilecek bir lisans satın alma süreci gerektirir.

VPN'ler genellikle erişim için ikili bir seçenek sunar: Yönetilmeyen bir uç nokta cihazının ağa, kaynaklara ve verilere sınırsız erişime sahip olmasını önlemek için karmaşık ilkelerin yapılandırılması gerekir.

Geleneksel VPN cihazlarını tam olarak yönetilebilen, küresel olarak mevcut bulut tabanlı bir hizmetle değiştirdiğinizde, uygulamalara ve verilere bağlı olan korumalı bir erişim sağladığınız için karmaşık ağ güvenliği ilkelerine gerek kalmaz.

## VPN'ler yüksek hacimli kullanım için tasarlanmamıştır

Uzaktan çalışanlar vlokasyon bağımsız şekilde, şirket ağına sorunsuz bir şekilde erişmeyi beklerler.

Ancak VPN ile tüm kullanıcı trafiği şirket ağı üzerinden iletilir, dolayısıyla trafiği artırır ve performansı düşürür. Ayrıca VPN genellikle merkezi bir konumdan dağıtıldığından, kullanıcılar coğrafi olarak farklı konumlardan dahili web uygulamalarına bağlanırken ekstra bir gecikme yaşarlar ve buna bağlı olarak kullanıcı deneyimi zayıflar.

Uzaktan çalışanlar faturalandırma ve müşteri ilişkileri yönetimi (CRM) tarafından kullanılan uygulamalar gibi iki katmanlı uygulamalara erişirken zorlanabilir. Bu uygulamalar kullanıcıların cihazlarında bir istemciye ihtiyaç duyar ve VPN'lerin ve ağ bağlantılarının hızla aşırı yüklenmesine neden olan kapsamlı bant genişliği gereksinimlerine sahip yerel protokoller kullanırlar.

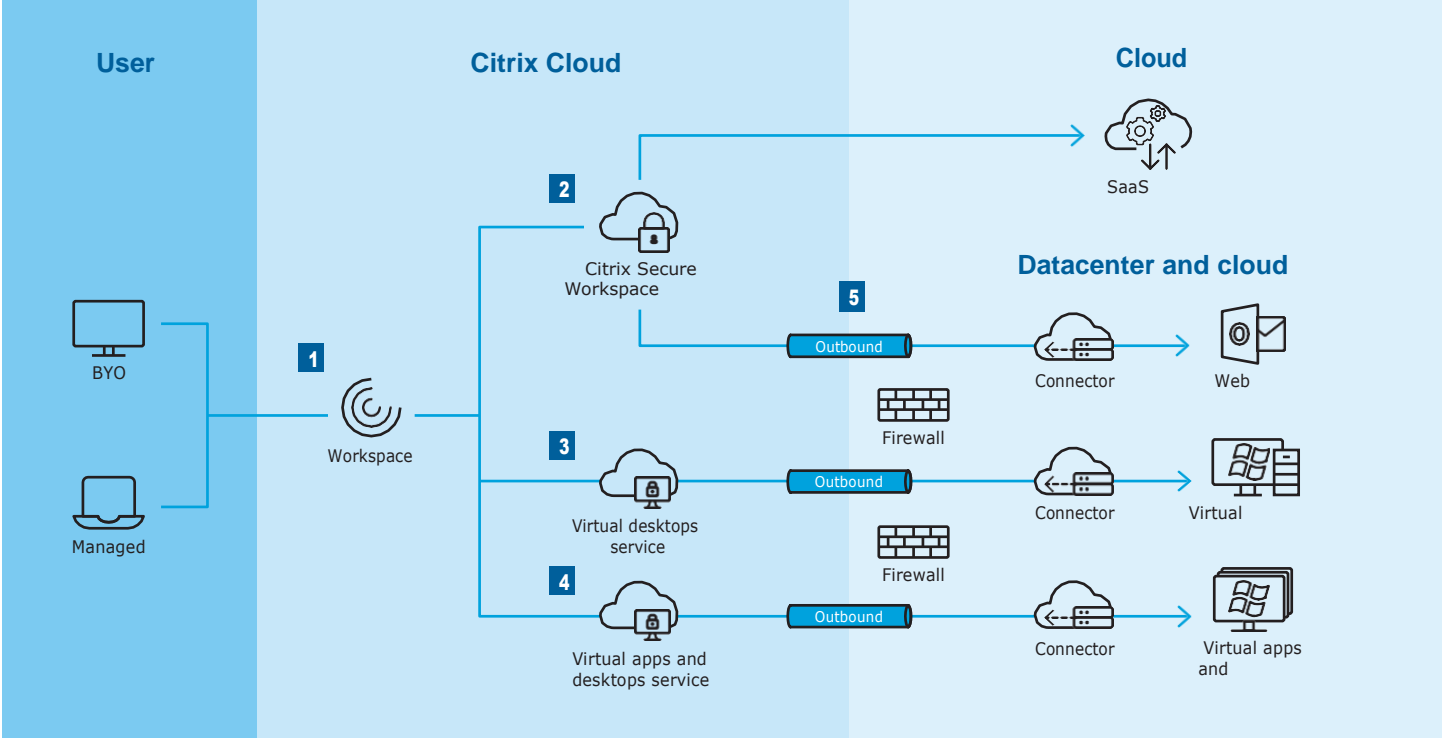
Ağ trafiği ve gecikme süresi arttıkça, uygulamanın yanıt verme hızı düşer, bu da tutarsız ve hatta istenmeyen bir kullanıcı deneyimine yol açar. Kullanıcı tarafındaki yetersiz ağ koşulları da performans ve kullanıcı deneyiminin kontrolden çıkmasına yol açar.

## Citrix, kullanıcılarınıza web uygulamaları için, VPN'siz erişim sağlar

Citrix Workspace'in bir parçası olan Citrix Secure Workspace Access hizmeti, tarayıcı üzerinden erişilebilen uygulamalara VPN'siz erişim sağlar. Böylece modern uygulamalar -tüm bağlamsal güvenlik kontrolleri aktif iken- herhangi bir kullanıcı cihazı tarafından ulaşılabilir ve ağ düzeyinde bir erişim seçeneğine ihtiyaç duymaz.

Citrix Secure Workspace Access küresel olarak erişilebilir olduğundan kullanıcı mümkün olan en yakın noktasya (POP) yönlendirilir. Böylece hem SaaS, hem de web uygulamalarına erişim için üst düzey bir performans ve güvenlik sağlanır.

Geleneksel iki katmanlı uygulamalar için bant genişliği bir sorun kaynağı olabilir. Bu uygulamalara evlerde kullanılan Wi-Fi'ler gibi yüksek gecikmeli ağlardan bağlanıldığında performans düşer. Sanal bir platform üzerinden erişim sağlamak, yalnızca kullanıcı deneyimini geliştirmekle kalmaz; aynı zamanda uygulama katmanında ayrıntılı bir güvenlik sağlar. Citrix Workspace'in bir parçası olan Citrix Virtual Apps and Desktops, bant genişliği gereksinimlerini minimize eder, hem performans hem de güvenlik kontrollerini dinamik olarak ayarlayarak bu uygulamalar için olabilecek en iyi güvenliği ve performansı sağlar.



- 1 Kimlik sağlayıcı seçimi (AD, AAD, Okta, Google, Radius ve diğerleri)
- 2 Gelişmiş güvenlik ile hizmet olarak yazılım (SaaS) ve web uygulamalarına VPN'siz erişim
- 3 Windows 10 PC'lere VPN'siz erişim
- 4 Gelişmiş güvenlik ile Windows ve Linux uygulamalarına ve masaüstü bilgisayarlara VPN'siz erişim
- 5 Yalnızca giden yönündeki denetim kanalı, kaynağa özel erişim sağlar

Citrix Virtual Apps and Desktops, uzaktan çalışanlar için daha iyi bir deneyim sunar. Ağ ve bilgisayarı yoran uygulamalar veri merkezinde sanallaştırılır ve optimize edilir. Uygulama istemcisi de sanallaştırılır ve veri kaynağının yakınında çalışır. Uzaktan çalışanlar yoğun ağlarda bile iyi performans gösteren internet bağlantısı için optimize edilmiş bir protokol kullanır.

### VPN'ler çalışan gizliliğini tehlikeye atar

Güvenlik ilkeleri ağ izlemeyi gerektirir. VPN bölünmüş tünellemeyi devre dışı bırakacak şekilde yapılandırıldığında kişisel ve özel uygulamalara ait tüm trafik bile kurumsal ağ üzerinden taşınır. Dolayısıyla işle ilgili olmayan trafik de gözlemlenebilir, bu da cihazı kendi kişisel amaçları için kullanan uzaktan çalışanların gizlilik açısından bazı endişeler duymasına yol açar. Uzaktan çalışanlar, başka birinin internet bağlantılarını izleme, bilgisayarlarına ve ev ağlarına erişim veya ziyaret ettikleri web sitelerinden veri toplama olasılığından rahatsızlık duyarlar.

Ancak erişim uygulama katmanında süreç sona erdiğinde çalışanlar gizliliklerinin güvencede olduğunu hisseder. Kullanıcı izlemeye tabi değildir ve kişisel ağ trafiği gizli kalır.

### VPN'ler BYOD (Kendi Cihazını Getir) metodunda BT ekiplerinin ve altyapısının zorlanmasına neden olabilir

Çalışanların kendi seçtikleri cihazı kullanmalarına izin vermenin avantajlarının farkında olan birçok kuruluş BYOD yöntemlerini benimsiyor. Ancak, uzaktan çalışanlar VPN aracılığıyla ağa bağlandığında kullandıkları cihazların güvenlik güncelleme ve uyumluluk durumunu sürekli olarak sağlamak BT kaynaklarını zorlayabilir. İşte bu noktada BYOD metodunun uç nokta ve erişim maliyetlerini azaltan etkisi biter ve BT altyapısının zorlanmasına neden olur.

Çoğu VPN BYOD ve yönetilmeyen cihazları desteklemek için bağlamsal ve ayrıntılı güvenlik ilkeleri sunamaz. Uzaktan çalışanların şirket tarafından verilen ve yönetilen bir cihaza sahip olması gerekir.

Üstelik kurumlar maaş ödemeleri, sosyal haklar gibi işlemleri, dış firmalardan hizmet olarak alır. Sözkonusu, dış hizmet firmaların cihazlarının uç noktasını kontrol etmek ve güvenliğini sağlamak imkansız hale gelir.

Diğer taraftan Citrix Workspace web tarayıcısı veya Citrix Workspace uygulaması üzerinden tüm cihazlarda iyi bir kullanıcı deneyimi sunar

Uzaktan çalışanlar BYOD veya kişisel cihazlardan fiziksel masaüstlerine erişime ihtiyaç duyabilir. Citrix Remote PC Access, kullanıcıların ofisteki fiziksel Windows bilgisayarlarına herhangi bir yerden erişmelerini sağlar. Mobil cihazlarda her uygulama için ayrı Micro-VPN özelliği tüm cihazlarda VPN bağlantısı ihtiyacını azaltır. Böylece VPN istemcisini yapılandırma ve başlatma gereksinimi ortadan kalktığından kullanıcı memnuniyeti artar, kurumsal verilere sorunsuz ve güvenli bir erişim sağlanır.

## VPN'ler ağınıza erişim bağlantısı açar

VPN'ler erişimin ya hep ya hiç olduğu eski bir güvenlik modeline sahiptir. Kimin neye eriştiğini göremez veya kontrol edemezsiniz. Bu durum içeriden gelen tehditleri ve çalışanların kimlik bilgilerini korumayı zorlaştırır.

VPN'ler, kullanıcıların sadece uygulama erişimine ihtiyaç duyduğu durumlarda ağ düzeyinde bir güvenlik saldırısı olasılığını artırır. Güvenliği ihlal edilmiş uç noktalar bile ağa dahil olabilir ve böylece kötü amaçlı yazılımlar ağda kolayca yayılabilir.

## Citrix Workspace, uzaktan çalışanlar için güvenli, VPN'siz bir çözümdür

Citrix, kurumunuzun güvenlik, yönetim ve ölçeklenebilirlik ihtiyaçlarının üstesinden gelen kullanımı kolay bir uzaktan çalışma ortamı sunar. Citrix Workspace tüm kaynakları herhangi bir cihazdan erişilebilen kişiselleştirilmiş tek bir kullanıcı arayüzünde toplar.

Seçilen yöntem ve cihazdan bağımsız olarak, uzaktan çalışanlar uygulamalarınıza, dosyalarınıza ve verilerinize VPN olmadan tekil oturum açma (SSO) kolaylığı ile erişir.

Uygulamalara ve verilere korumalı erişim sağlanır ve karmaşık ağ güvenlik ilkelerine gereksinim duyulmaz.

Çalışanlarınız ister sanal, web veya (SaaS) uygulamaları kullansın, Citrix Workspace yetkilendirme düzeylerini kullanıcı ve cihaz tabanlı olan durumsal veya bağlamsal bilgilere göre belirler. Bağlamsal güvenlik ilkeleri, yalnızca bir kullanıcıyı tanımlamanıza ve kimliğini doğrulamanıza değil, aynı zamanda kullanıcı ve cihaz durumu, konum ve IP adresi gibi parametrelere dayalı olarak bir uygulama içinde hangi kullanıcı eylemlerinin izinli olduğunu yönetmenizi sağlar.

Üstelik Citrix Workspace kuruluşların farklı düzeylerde uygulama veya kaynak erişimi belirlemesine izin verir. Dosyalarda değişiklik ( kes ve yapıştır yapma, dosya yazdırma ve yerel kopya alma gibi) belirli işlemleri yalnızca belirlenen kişilerin ve cihazlarda yapmasına izin verir.

Citrix Secure Workspace Access hizmeti SaaS ve web uygulamalarına güvenli erişim kontrolleri ve görünürlük özelliklerini ekleyebilirsiniz. Uygulama koruma fonksiyonları tuş kaydediciler ve ekran görüntüsü alan kötü amaçlı yazılımları engeller. Güvenilmeyen bir cihazdan bağlanan çalışanın erişimini reddetmek yerine kullanıcıların erişebileceği işlevler kısıtlanabilir.

Citrix Workspace güvenlik yöneticilerine kullanıcı risk değerlendirmesi ve risk puanlaması yapma imkanı vererek sürekli izleme ve kontrol yapmayı kolaylaştırır. İlk oturum açma doğrulamasından sonra işletmeyi koruyan önlemler uygulanır.

### Citrix Secure Workspace Erişiminin Avantajları:

- Basit dağıtım ve yapılandırma
- Kolay yönetim ve bakım
- Temel ağ koruması
- Kullanıcı gizliliği koruması
- Bağlamsal veya koşullu erişim
- Zenginleştirilmiş kullanıcı deneyimi
- Hızlı ölçeklenebilirlik
- Uzaktan çalışanlar için yüksek performans
- Kullanıcının cihaz seçme esnekliği (BYOD)
- Sürekli güvenlik ve izleme

## Özet:

Her kuruluş, lokasyon ve cihazdan bağımsız olarak tüm uzaktan çalışanlarının, şirket içi çalışanlar kadar güvenli bir şekilde bağlantı kurduğundan emin olmak ister. Geleneksel VPN'lerin aksine Citrix Workspace ihtiyacınız olan güvenlik ve kontrolü sağlar.

Citrix Workspace'in özellikleri ve avantajları hakkında daha fazla bilgi edinmek için, satış ekibimiz ile iletişime geçebilirsiniz.

[CitrixSales\\_TR@exclusive-networks.com](mailto:CitrixSales_TR@exclusive-networks.com)



©2020 Citrix Systems, Inc. Her hakkı saklıdır. Citrix, Citrix logosu ve burada yer alan diğer markalar Citrix Systems, Inc. ve/veya bir veya daha fazla yan kuruluşun mülkiyetindedir ve ABD Patent ve Ticari Marka Bürosu'nda ve diğer ülkelerde tescilli olabilir. Diğer tüm markalar ilgili sahiplerinin mülkiyetindedir.  
RES160 10/20

