

VPN gerçekte nedir

Seni kimin görebileceğini değiştirir, birinin görüp göremeyeceğini değil.

Açıkça söylemek gerekirse: Bir VPN, internet sağlayıcının veya havaalanı Wi-Fi'nın nereye bağlandığını görmesini engeller. Bu bilgi yok olmaz: artık onu gören VPN şirketine aktarılır. E-posta veya bankacılık gibi zaten şifreli olarak taşınan veriler daha önce de şifreliydi. Birkaç somut amaca hizmet eder ve genellikle çok daha fazlasını çözüyormuş gibi pazarlanır.

Yıllarca VPN hakkında konuştuklarını duydum ve tıpkı antivirüslerde olduğu gibi kulak asmadım: Antivirüs kullanmıyorum ya da neredeyse hiç. Her şeyin gerçek zamanlı kopyalarını üç farklı yerde tutuyorum ve ne indirdiğime, hangi bağlantılara tıkladığıma ve hangi web sitelerini ziyaret ettiğime çok dikkat ediyorum. Bu yüzde yüz bir güvenlik değil ama bende işe yarıyor. Bir gün ayda iki avronun biraz üzerinde bir VPN teklifi gördüm ve meraktan abone oldum. İyi çalışıyor ama çok az işime yaradı: örneğin o zamanlar yalnızca Amerika Birleşik Devletleri'nde açılan bir hizmeti denemek gibi. Kendimi daha güvende hissediyor muyum? Hayır. Bana bu fiyata tekrar teklif ederlerse belki yenilerim; etmezlerse yenilemem. Bu sadece benim deneyimim, hiçbir şeyi kanıtlamaz. Bu yüzden kendime bir VPN'in tam olarak ne yaptığını sordum. İşte benim anladığım şekli.

Bir mektubu, alıcının adresi açıkça görünecek şekilde posta kutusuna attığını hayal et. Postacı, kapalıysa okuyamasa bile kime gönderdiğini görür. O postacı senin internet operatöründür. Bir VPN, mektubunu açıp ileten bir aracıya hitaben yazılmış başka bir zarfın içine koyar. Alışıl gelmiş postacın artık gerçek adresi görmez. Yalnızca o aracıya yazdığını görür.

Bağlandığın ağı kontrol eden kişi – örneğin bir havaalanı Wi-Fi'ı –, artık nereye gittiğini görmez. Ancak aracı, eskiden operatörünün gördüğü şeyi ve bazen daha fazlasını görür, çünkü tüm trafiğin onun üzerinden geçer. Gözetim ortadan kalkmaz: el değiştirir. İsmi de buradan gelir.

Ayrıca bugün yaptığın neredeyse her şey – e-postanı açmak veya bankaya girmek gibi –, tarayıcının asma kilidi sayesinde hedef sunucuya kadar zaten şifreli olarak gider. Bu durum VPN ile de VPN olmadan da gerçekleşir. VPN yalnızca ilk aşamada, kendi sunucusuna kadar koruma ekler. Oradan sonrası her zamanki yoldur.

Bu yüzden bazen böyle satılsa da sana vadedemeyeceği şeyler vardır. E-postana veya bankana giriş yaptıysan, o hizmet VPN olsun veya olmasın senin sen olduğunu bilir. Trafikine hiç kimsenin bakmadığını da garanti etmez: sadece kimin baktığını değiştirir. Şirketin «kayıt tutmuyoruz» demesi bir vaattir; tıpkı büyük bir platformun «mesajlarınız şifrelidir, onları okumuyoruz» demesi gibi. Bir denetim bunu belirli bir anda doğrulayabilir, ancak bu yine de yerine getirileceğine güvendiğin bir şey olarak kalır, tasarımdan ötürü ihlal edilemeyecek bir şey değil.

Ve bir konuşmanın içeriği aynı kalır. Mesajlaşma uygulaman zaten uçtan uca şifreliyorsa, VPN hiçbir şey katmaz. Şifrelemiyorsa, VPN bunu da düzeltmez: mesajın yolunu korur, uygulamanın veya sunucusunun mesaj ulaştığında onunla ne yaptığını değil.

Bunların hiçbirisi onu işe yaramaz kılmaz. Nereye bağlandığını halka açık bir Wi-Fi'dan, bu geçmişini satmak isteyen bir operatörden veya bir hizmeti engelleyen bir ülkeden gizlemek gerçek bir iştir ve bunu iyi yapar. Yine de pazarlama genellikle bu katmanın verebileceğinden fazlasını vadeder.

Bir VPN veya seni korumayı vadeden herhangi bir hizmet karşısında kendine sorman gereken soru «şifreli mi?» değildir. Muhtemelen evet, en azından bir bölümde. Soru şudur: Birinden aldığım güveni kime emanet ediyorum? Ve eğer bu güven yersiz çıkarsa elimde ne kalır?

Bir VPN, işini iyi yaptığında yalnızca bağlantının aracısının kim olduğunu değiştirir. Mesajları hiçbir sunucudan geçmeyen Solo2 gibi bir uygulama ise aracıyı konuşmadan tamamen çıkarır. Birbirleriyle yarışmazlar: farklı sorunları çözerler.

Bunları birbirine karıştırmak, insanın kendini gerçekte olduğundan daha güvende sanmasının çok yaygın bir yoludur.

Editörün Notu: Bu Cuadernos'lar şirket veya ürün isimlerinden bahsettiğinde, bu suçlama amacı taşımaz. Bunları inşa edenler, milyonlarca insanın kullandığı ve takdir ettiği işler yapıyorlar. Bizim işaret ettiğimiz şey yapısaldır — marka değil, modeldir. Markalar, okuyucunun tanıdığı markalar olduğu için örnek olarak yer almaktadır.

Kaynaklar ve ek okumalar

- HTTPS protokolü ve aktarım şifrelemesi, IETF tarafından kamuya açık şekilde belgelenmiş açık standartlardır.
- Aynı derlemede: «Arada kimse olmadığında» ve «Anonim değilsin», yapı ile vaat arasındaki aynı ayrımı başka açılardan ele alır.

[← ÖncekiAnonim değilsin](#)

Son okumalar

- [Düşünce · 29 Haziran 2026 Anonim değilsin](#)
- [Düşünce · 27 Mayıs 2026 Bir imzanın düzeltmeyeceği şeyler](#)
- [Analiz · 26 Mayıs 2026 Gerçek vs. görünür gizlilik: kendinize sormanız gereken sorular](#)

Bu makaleyi ihtiyacınız olan her yere yanınızda götürün.

[↓ Markdown](#) [↓ Düz metin](#) [↓ PDF](#)

Dosya cihazına indirilecektir. Oradan kaydedebilir, Solo2'ye aktarabilir veya istediğin yerde paylaşabilirsin. Cuadernos hedef noktaya senin yerine karar vermez.

Mühür mumu · SHA-256 6dae093e4c88dc911b61400c03faa4af58ca72a3c36c6a8a36d46844bcabb3f9

[Özellikler](#) [Fiyatlar](#) [Yükle](#) [Yenilikler](#) [Blog](#) [Pro](#) [Yardım](#) [Hakkımızda](#) [İletişim](#)
[Şeffaflık](#) [Doğrulama](#) [Gizlilik](#) [Koşullar](#) [Çerezler](#)

Cuadernos Lacre · [Menzuri Gestión S.L.](#) yayını ·

R.Eugenio tarafından yazıldı · [Solo2](#) ekibi tarafından düzenlendi.

Bu web sitesi çerez kullanmaz. Tarayıcınızın yüklediği her şey tarafımızca yazılmış ya da denetlenmiştir ve Avrupa sunucularımızda barındırılır: anonim ziyaret sayacı (Umami, kendi sunucumuzda barındırılan) ve dil seçici ile açık/koyu tema tercihiniz için gereken minimum JavaScript; bu tercih kendi cihazınızda saklanır. Üçüncü taraf kaynak yok, izleyici yok, profillemeye yok, veri paylaşımı yok. Bizi takip etmek isterseniz: [RSS](#).