berqnet

Berqnet SASE Adaptive ZTNA (Zero Trust Network Access)

Ürün Broşürü

Sıfır Güven (ZTNA) Yaklaşımı Nedir?

“Kim olursan ol, önce kanıtla” anlayışıyla çalışan modern güvenlik yaklaşımı.

Günümüzde çalışanlar yalnızca ofisten değil; farklı şehirlerden, evden, mobil bağlantılar üzerinden veya seyahat hâlindeyken erişim sağlıyor.

Cihaz çeşitliliği arttı, uygulamalar buluta taşındı ve tehditler her zamankinden daha görünmez bir hâle geldi.

Bu yeni koşullar altında geleneksel güvenlik modeli — yani “ağa bağlandıysan güvendesin” yaklaşımı — modern siber tehditlere karşı yeterli koruma sunmamaktadır.

Sıfır Güven Yaklaşımı (Zero Trust) , modern ağ güvenliğinin temelini oluşturan yeni prensibi tanımlar:
“Hiç kimse, hiçbir cihaz, hiçbir bağlantı kendiliğinden güvenilir değildir.”

Kullanıcı ister ofisten, ister evinden bağlansın; ister şirket cihazını, ister kişisel cihazını kullansın…
Her erişim isteği mutlaka doğrulanır.

Gerekli koşulları sağlamayan hiçbir kullanıcı, hiçbir kaynağa erişemez.
Zero Trust , günümüzün dağınık çalışma modelinin doğal bir ihtiyacıdır.

Geleneksel ZTNA Ne Sunar?

Erişimi giriş anında doğrular, sonrasında aynı izni sürdürür.

Geleneksel ZTNA, Sıfır Güven prensibini uygular ancak bunu tek bir aşamada gerçekleştirir:

1. **Kullanıcının giriş anında kimliği doğrulanır (şifre + MFA)**
2. **Kullanıcının erişeceği uygulamalar belirlenir**
3. **Kullanıcı oturumu açık kaldığı sürece bu izinler değişmez**

Bu model giriş anında güçlü bir kontrol sağlasa da kritik bir varsayıma dayanır:

“Girişte bir kez doğrulandıysa, kullanıcı oturum boyunca güvenilirdir.”

Oysa günümüzde güvenlik riskleri tam da bu noktada ortaya çıkar:

- Kullanıcı başka bir ülkeden bağlanır
- IP aniden değişir
- Cihazın güvenlik durumu bozulur
- Antivirüs kapanır
- Zararlı bir süreç çalışmaya başlar
- Hesap ele geçirilir
- Aynı hesaba farklı coğrafyalardan deneme yapılır

Geleneksel ZTNA bu değişiklikleri fark etmez. Erişim, girişte tanımlandığı şekilde devam eder.
Bu nedenle geleneksel ZTNA, günümüzde yeterli görünse de modern **tehditlere karşı eksik kalır.**

Berqnet SASE Adaptive ZTNA Ne Yapar?

Güveni sadece girişte değil, her erişim anında ve oturum boyunca doğrular.

Berqnet SASE Adaptive ZTNA, Zero Trust modeli üç kritik aşamayı kapsar:

1. **Giriş anı (Giriş Politikaları)** → Kim sisteme giriş yapabilir?
2. **Ağa bağlanma anı (Erişim Politikaları)** → Kullanıcı kurumsal ağlara bağlanabilir mi?
3. **Oturum boyunca izleme (Dedektörler & Yanıtlayıcılar)** → Bağlantı açıkken kullanıcı hâlâ güvenilir mi?

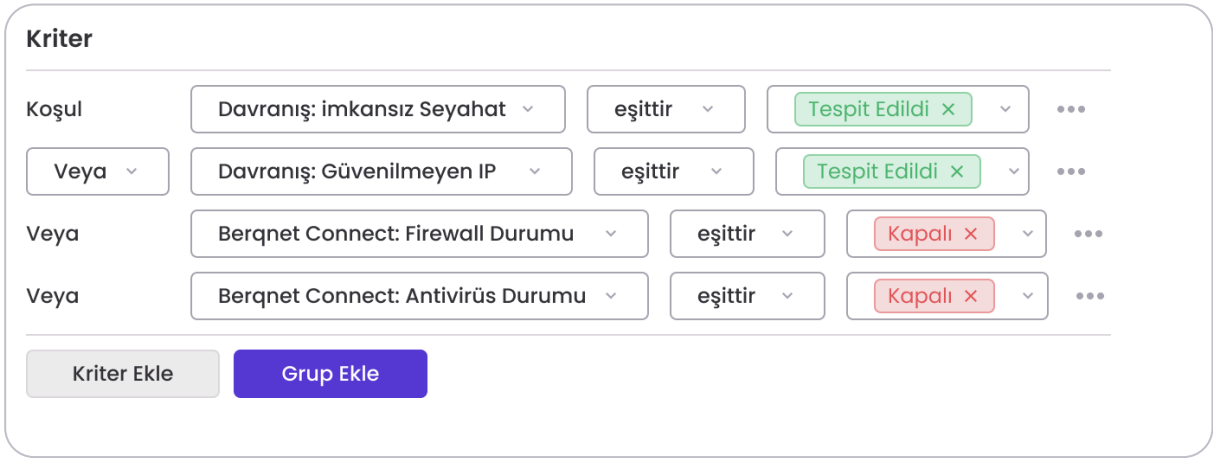
Adaptive ZTNA , bu üç aşamada topladığı kullanıcı davranışı, konum, risk ve cihaz güvenliğiyle ilgili sinyallerle dinamik, esnek ve her an güncel bir güvenlik modeli sunar.

Adaptive ZTNA Sistemi Nasıl Çalışır?

Üç aşamalı, sürekli yaşayan bir güvenlik mimarisi

Berqnet SASE Adaptive ZTNA, Sıfır Güven yaklaşımını bir adım ileri taşıyarak erişimi yalnızca giriş anında değil, tüm oturum boyunca değerlendirir.
Her aşamada toplanan davranış, risk ve cihaz verileri analiz edilir ve kurumunuzun yapılandırdığı politikalar doğrultusunda erişim kontrolü uygulanır.

Adaptive ZTNA erişimi üç kritik aşamada değerlendirir.



1. Giriş Aşaması – Giriş Politikaları

Sisteme kimin giriş yapabileceği davranış ve risk verileriyle belirlenir
Kullanıcı veya yönetici sisteme giriş yapmak istediğinde Adaptive ZTNA yalnızca şifreyi doğrulamaz; kişinin genel güvenilirliğini de analiz eder:

- IP adresi riskli bir bölgeden mi geliyor?
- Konum beklenenden farklı mı?
- Arka arkaya başarısız giriş denemeleri var mı?
- Yeni bir ülke/şehir mi?
- Hesap ele geçirilmiş olabileceğine dair işaret var mı?
- Hesabın son aktiviteleri olağan dışı mı?

Bu sinyaller **Berqnet Risk Motoru** tarafından değerlendirilir ve her giriş isteğine bir risk seviyesi atanır. Giriş aşamasında uygulanan izin, MFA veya erişim reddi gibi kararlar, tanımlı giriş politikalarına göre yürütülür.

Bu sayede sisteme yalnızca kimliği doğrulanmış değil, aynı zamanda davranış açısından güvenilir kullanıcılar giriş yapar.

2. Erişim Aşaması

Adaptive ZTNA'nın ikinci değerlendirme noktası, kullanıcı Berqnet Connect üzerinden ağlarınıza erişim sağlamak istediği andır.
"Bu kullanıcı şu anda kurumsal ağa bağlanmaya uygun mu?"
Erişim Politikaları bu aşamada cihazdan ve kullanıcıdan gelen güvenlik sinyallerini analiz eder:

Cihaz güvenliği:

- Antivirüs aktif mi ve güncel mi?
- Firewall açık mı?

- Zararlı veya şüpheli bir süreç çalışıyor mu?
- Kritik servisler kapatılmış mı?
- Bilinmeyen uygulamalar devrede mi?
- Sistem güvenlik ayarları değiştirilmiş mi?

Kullanıcı davranışı:

Yeni bir ülkeden mi bağlanıyor?
Beklenmeyen bir IP üzerinden mi geliyor?
Risk seviyesi yüksek mi?
Son aktiviteleri olağan dışı mı?

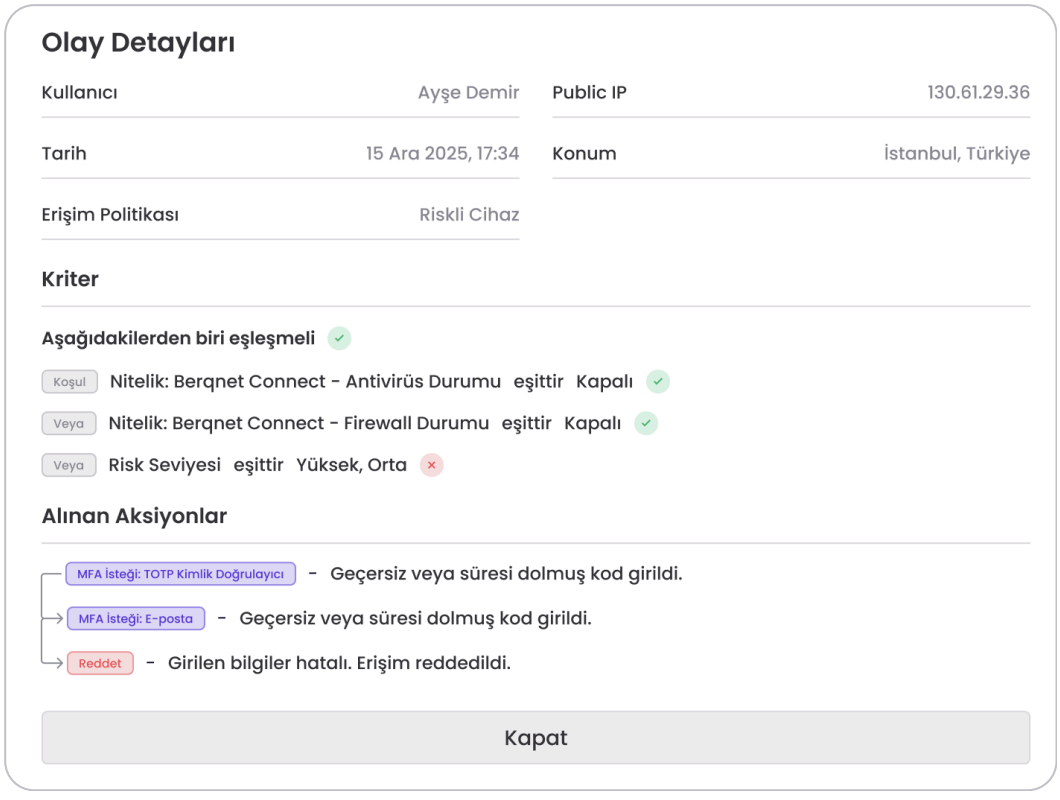
Bu sinyaller **Berqnet Risk Motoru** tarafından değerlendirilir ve her ağa erişim isteğine bir risk seviyesi atanır.

Bu analiz sonucunda otomatik aksiyonlar alınır:

- Ağa erişime izin verilebilir
- Erişim reddedilebilir
- Ek kimlik doğrulama istenebilir
- Kullanıcı veya IP engellenebilir
- Sistem uyarısı veya webhook üretilebilir
- E-posta bildirimi gönderilebilir

✓ **Tüm erişim olayları Berqnet Manager'da kayıt altına alınır.**

Yöneticiler, ağa erişim isteğinin hangi kritere takıldığını, hangi politikanın devreye girdiğini ve hangi aksiyonun uygulandığını detaylı olarak görünür.
Bu aşama, çalışanların yalnızca girişte değil, **bağlantı kurdukları anda** da güvenli olduklarından emin olmayı sağlar.



3. Oturum Boyunca – Dedektörler ve Yanıtlayıcılar

Bağlantı açık olsa bile: "Bu kullanıcı hâlâ güvenilir mi?" kontrolü sürer

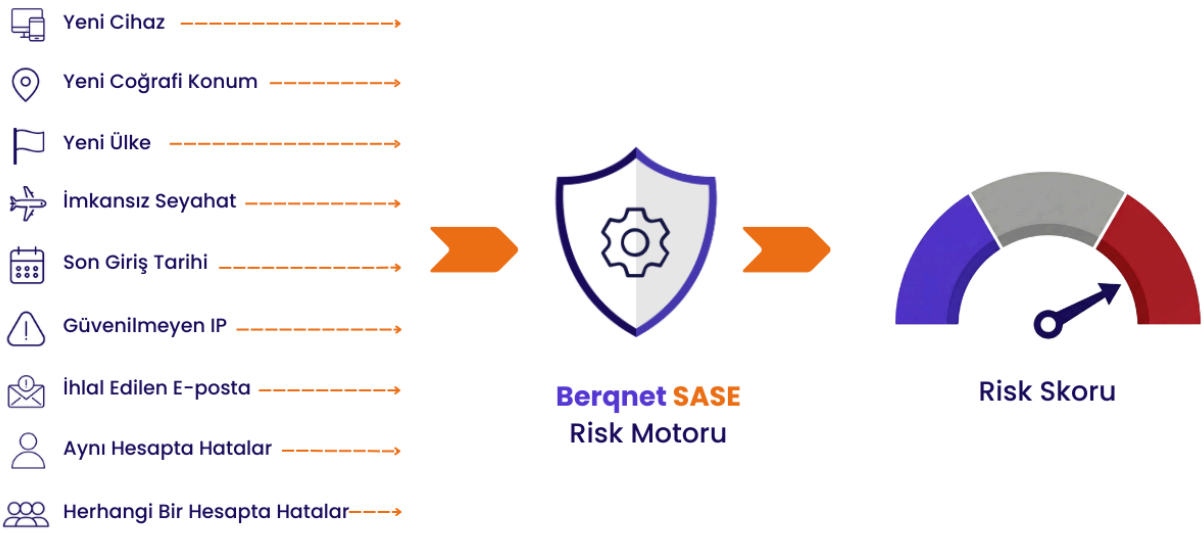
Adaptive ZTNA erişim verildikten sonra bile güvenliği bırakmaz.

Kullanıcı bağlıyken risk seviyesi değişebilir, cihaz güvenlik durumu bozulabilir veya olağan dışı bir davranış ortaya çıkar.

Dedektörler neleri izler?

- Yeni ülke/şehir
- İmkânsız seyahat
- Güvenilmeyen IP'den gelen trafik
- Cihazdaki güvenlik durumunun aniden değişmesi
- Antivirüs veya firewall'un kapanması
- Şüpheli süreç veya servislerin devreye girmesi
- Potansiyel zararlı davranışlar

Bu sinyaller Berqnet Risk Motoru tarafından değerlendirilir ve kullanıcının oturum süresince davranışlarına göre bir risk seviyesi atanır.



Yanıtlayıcılar ne yapar?

Dedektörlerin tespit ettiği riskli davranışlara karşı, tanımlı politikalar doğrultusunda aşağıdaki aksiyonlar alınır:

- Kullanıcının bağlantısını sonlandırma
- Oturumu kapatıp yeniden doğrulama isteme
- Kullanıcı ve IP'yi engelleme
- Sistem uyarısı oluşturma
- Yöneticilere e-posta gönderme
- Harici sistemlere webhook gönderme

✓ **Tüm dedektör olayları Berqnet Manager'da kayıt altına alınır.**
Yönetici, oturum sırasında:

- Hangi davranışın tetiklendiğini
- Risk seviyesinin nasıl değiştiğini
- Hangi yanıtlayıcı aksiyonunun uygulandığını

anlık olarak görülür ve geçmiş kayıtlardan raporlanır.

Bu yapı sayesinde güvenlik, kullanıcı bağlandıktan sonra bile aktif şekilde çalışmaya devam eder ve riskli durumlar anında kontrol altına alınır.

Berqnet Adaptive ZTNA ile Güvenlik Artık Kesintisiz Bir Süreç

Bugünün çalışma düzeni, modern tehditler ve dağınık erişim modelleri; güvenliği yalnızca giriş anına sıkıştıran eski çözümleri geride bırakıyor. Berqnet Adaptive ZTNA, erişimi her aşamada değerlendiren yapısıyla işletmelere statik bir güvenlik değil, sürekli yaşayan ve güncel kalan bir koruma sağlar.

Davranış, risk ve cihaz verilerini tek bir merkezde birleştirerek;
kimin ne zaman, nasıl ve hangi koşullarda erişim sağlayabileceğini detaylı şekilde kontrol etmenize olanak tanır.

Her tetiklenen olayın Berqnet Manager'da görünür olması, güvenliği yalnızca otomatik bir mekanizma olmaktan çıkarıp, tamamen yönetilebilir ve denetlenebilir bir yapıya dönüştürür.

berqnet

Hakkımızda

Logo Siber Güvenlik ve Ağ Teknolojileri A.Ş. ünvanıyla 2013 yılında , KOBİ ölçeğinde işletmelerin siber güvenlik ihtiyaçlarına yönelik çözüm üretme amacıyla kurulduk. 2015 yılında Berqnet markalı ilk ürünümüzün satışına başladık. 2022 yılı itibari ile ünvanımız Berqnet Siber Güvenlik Teknolojileri A.Ş. olarak değişti. %100 yerli AR-GE ekibimiz tarafından geliştirilen firewall (güvenlik duvarı) ve sıfır güven yaklaşımı (zero trust) ile güvenli uzaktan erişimi sağlayan ağ güvenliği platformu ürün gruplarını sunmaktayız. Çözümlerimizi aktif olarak kullanan binlerce işletmenin siber güvenlik, yasalara uyumluluk ve internet yönetimi ihtiyaçlarını karşılamaktayız.

berqnet.com

0850 577 23 77

LinkedIn/berqnetsiberguvenlik