berqnet

Berqnet SASE
DPC (Cihaz Durum Kontrolü)

Ürün Broşürü

Kurumsal erişim güvenliği artık yalnızca kullanıcıyı doğrulamakla sağlanamaz.
Yetkili bir kullanıcı, güvenliği zayıf bir cihazla bağlandığında kurum için aynı derecede risk oluşturur.

Berqnet SASE Cihaz Durum Kontrolü (DPC), kurumsal kaynaklara erişen cihazların güvenlik durumunu tanımlar, ölçer ve yönetir.

Erişim kararları, cihazın gerçek güvenlik duruşuna göre verilir ve bu kararlar **Sıfır Güven Politikaları** ile doğrudan aksiyona dönüşür.

Bir cihazın güvenli kabul edilmesi, tek bir kontrolle ya da bağlantı anıyla sınırlı değildir. Cihaz güvenliği; belirlenen kriterlere göre **sürekli doğrulanması gereken bir durumdur.**

Berqnet SASE DPC, kurum tarafından tanımlanan **cihaz durum politikalarını** karşılayıp karşılamadığını kontrol eder. Bu politikalar; cihazın güvenlik yazılımlarının durumu, koruma seviyeleri ve risk göstergeleri gibi kriterlere dayanır.

Sonuç olarak erişim, varsayıma değil ölçülebilir duruma göre yönetilir.

Cihaz Durumunu Sıfır Güven Politikaları ile Yönetin

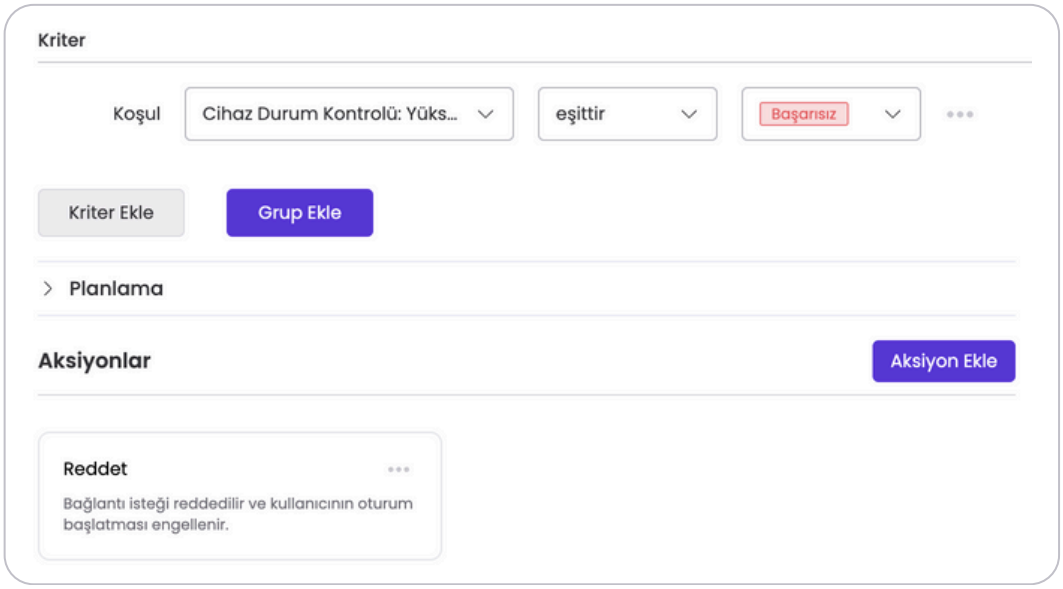
Cihaz Durum Kontrolü özelliği tek başına çalışan bir kontrol mekanizması değildir. Cihaz durum politikaları, Berqnet SASE Sıfır Güven Politikaları (ZTNA) içinde **doğrudan karar girdisi** olarak kullanılır.

Bir cihaz, tanımlı cihaz durum politikasından başarısız olduğunda sistem otomatik olarak aksiyon alır. Bu aksiyonlar, kurumun güvenlik yaklaşımına göre esnek şekilde yapılandırılır.

Cihaz durumuna bağlı olarak:

- Ek kimlik doğrulama talep edilebilir
- Kurumsal kaynaklara erişim engellenebilir
- Aktif bağlantı sonlandırılabilir
- Kullanıcı erişimi geçici veya kalıcı olarak kısıtlanabilir

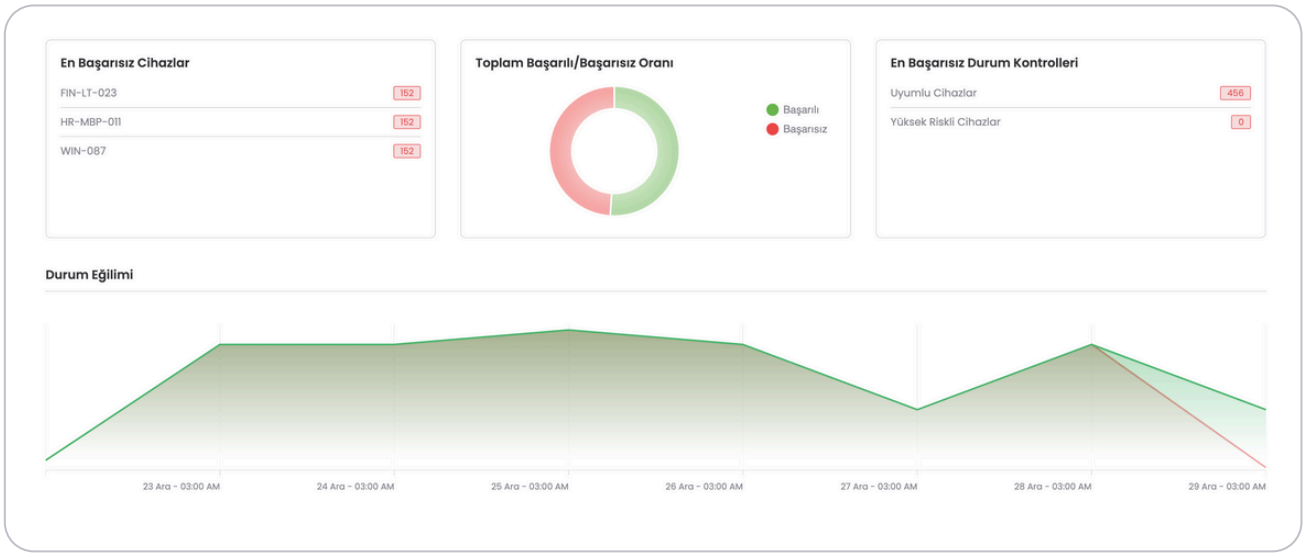
Tüm bu süreçler manuel müdahale olmadan, **politika bazlı** olarak yürütülür.



Sürekli Değerlendirme, Anlık Müdahale

Cihaz güvenliği sabit değildir. Bağlantı kurulduktan sonra da değişebilir. Cihaz Durum Kontrolleri, cihazın güvenlik durumunu yalnızca erişim öncesinde değil, **oturum boyunca** izler.

Cihaz durumu değiştiğinde ilgili Sıfır Güven Politikası otomatik olarak yeniden değerlendirilir ve gerekli aksiyon anında uygulanır.
Bu sayede güvenlik, gecikmeli uyarılarla değil, **anlık kararlarla** sağlanır.



Otomatik ve Denetlenebilir Raporlama

Berqnet SASE, cihaz güvenliğini yalnızca uygulatmaz; **kanıtlar.** Cihaz durum politikaları üzerinden:

- Hangi cihazların kontrollerden geçtiği
- Hangi cihazların başarısız olduğu
- Bu durumların hangi zaman aralıklarında gerçekleştiği

otomatik olarak raporlanır.

Bu raporlar sayesinde cihaz güvenliği görünür hale gelir, denetlenebilir olur ve iç denetim süreçlerini destekler. Güvenlik ekipleri, cihaz güvenliğini geçmişe dönük olarak **veriye dayalı** şekilde izleyebilir.

Merkezi Yönetim, Tutarlı Güvenlik

Tüm cihaz durum politikaları, aksiyonlar ve raporlar tek bir merkezden yönetilir.
Politikalar kullanıcıya, cihaza veya erişim senaryosuna göre tutarlı şekilde uygulanır.

Operasyonel yük azalırken, güvenlik kararları **kurum genelinde standart** hale gelir.

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