berqnet

SASE (Secure Access Service Edge)

Yeni Çalışma Düzeninin Ağ Mimarisi

Giriş

Yeni çalışma düzeninde işgücünün giderek daha geniş alanlara yayılmasıyla iş uygulamalarının büyük çoğunluğu buluta taşınmaya başladı. Artan küreselleşme, işletmeleri uzak kıtalarda ve farklı lokasyonlarda şubeler açmaya yöneltti. Koronavirüs salgını ise şirketleri uzaktan çalışma politikalarını benimsemek zorunda bıraktı. Bu değişiklikler, yer ve zaman fark etmeksizin herhangi bir cihaz kullanılarak veri erişimini güvenli şekilde sağlayacak teknolojileri gerekli kıldı.

Bu ihtiyaçları karşılamak için tasarlanmamış olan geleneksel ağ mimarilerinin, bulut hizmetleri ve dağıtık işgücünün sebep olduğu karmaşıklıkların üstesinden gelmede yetersiz kalması, gelişmiş ağ mimarilerine duyulan ihtiyacı artırdı. SASE (Secure Access Service Edge), güvenli ve bulut hizmetleri için uyarlanmış bir ağ mimarisi sunarak bu ihtiyaçları karşılamayı vaat ediyor.

İçindekiler

SASE Nedir? 3

SASE'ye Duyulan İhtiyaç 3

SASE'nin Amacı 4

SASE'nin Temel Bileşenleri 5

- Sıfır Güven Ağ Erişimi (ZTNA) 5
- Yazılım Tabanlı WAN (SD-WAN) 5
- Hizmet olarak Güvenlik Duvarı (FWaaS) 5
- Güvenli Web Ağ Geçidi (SWG) 5
- Tehdit Koruması 5

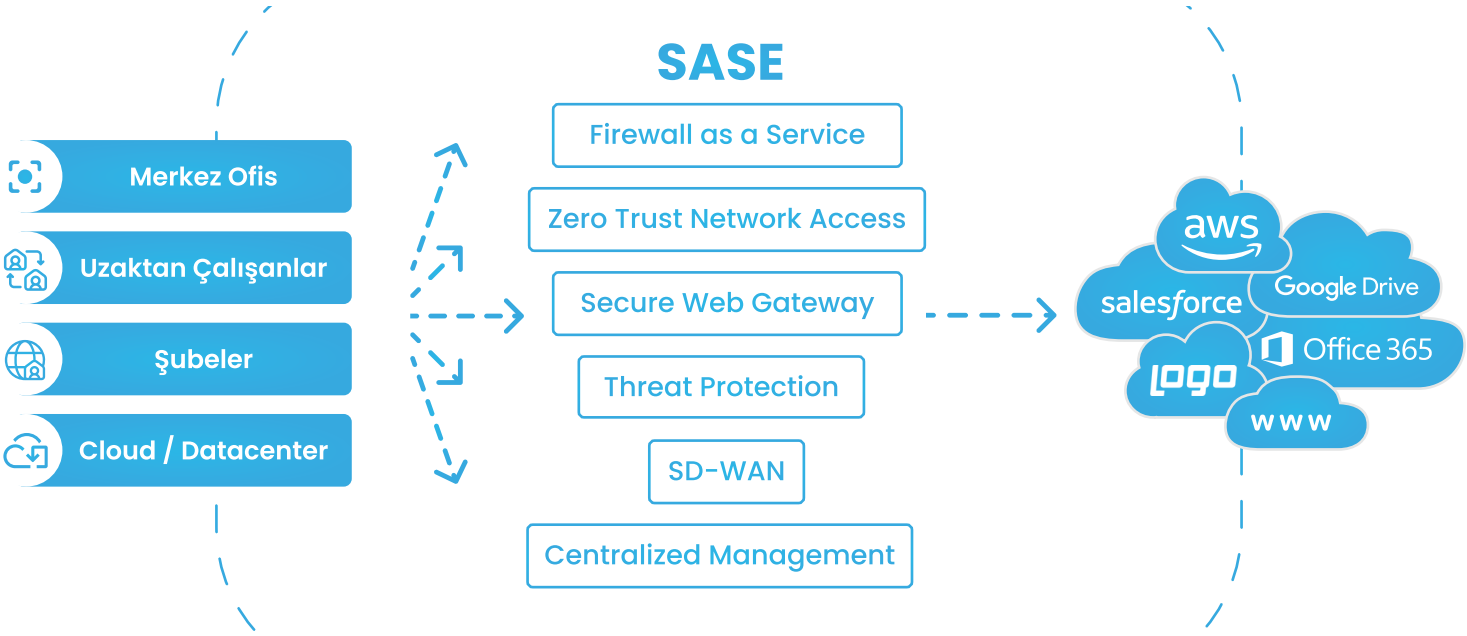
Kullanım Senaryoları 6

- Uzaktan Çalışan Şirketler 6
- +50 Şubeli Şirketler 6

Sonuç 7

SASE Nedir?

SASE olarak kısaltılan Secure Access Service Edge, ağ ve güvenliği birleştiren bulut tabanlı bir mimaridir. Bu model, özellikle günümüzün modern kuruluşlarının güvenli erişim ihtiyaçlarını karşılamak için tasarlandı. SASE'nin ana bileşenleri Sıfır Güven Ağ Erişimi (ZTNA), Servis Olarak Güvenlik Duvarı (FWaaS), Güvenli Web Ağ Geçidi (SWG), Tehdit Koruması ve Yazılım Tabanlı WAN'dır (SD-WAN). Bir başka deyişle SASE, dijital dönüşümünün ve dağıtık işgücünün zorluklarını ele alan bir teknolojiler bütünüdür.



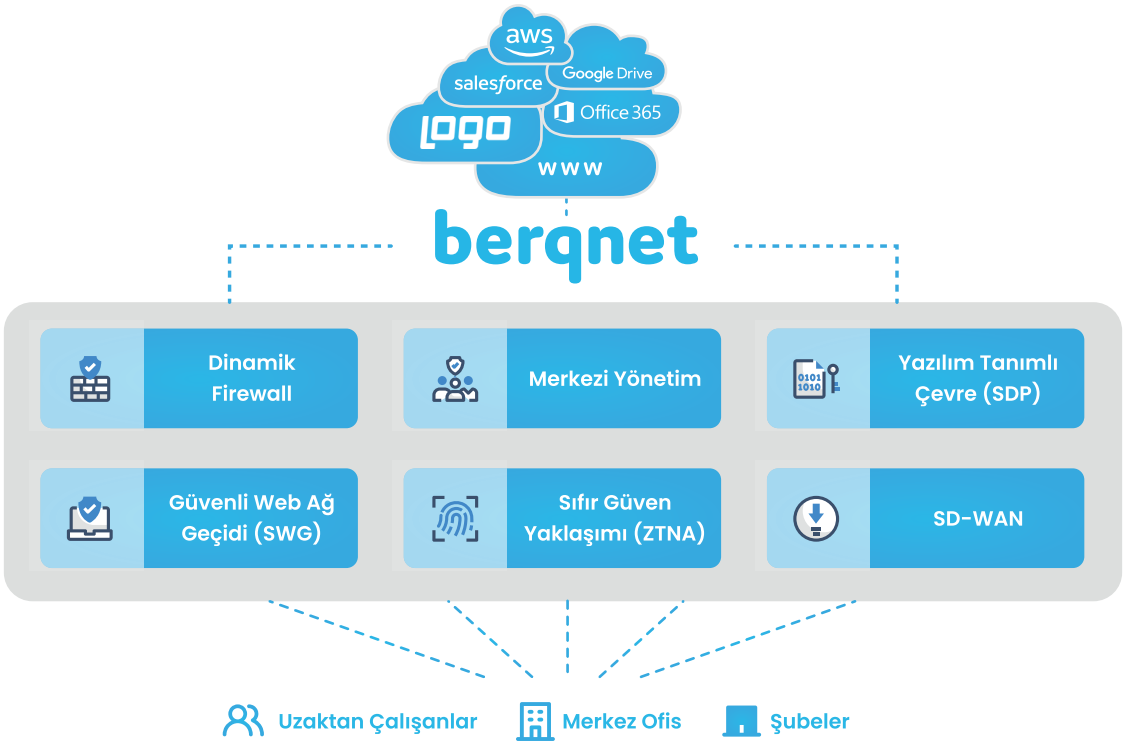
Daha Verimli Uzaktan Erişim İhtiyacı

Uzaktan çalışma yöntemini uygulayan şirketlerin katlanmaları gereken en önemli zorluklardan biri düşük ağ performansıdır. Bu şirketlerin büyük bir çoğunluğu, uzaktan çalışanların şirket ağına bağlanmalarını sağlamak için VPN'lerden, yani sanal özel ağlardan yararlanmak zorunda kalır. VPN aracılığıyla ağa bağlanan uzaktan çalışanlar, genellikle trafik taşıyıcıları sebebiyle ortaya çıkan yığılma noktalarına maruz kalır. Bu da gecikme sorunlarına ve internet bağlantısında doygunluğa neden olur. Geleneksel ağlara gereğinden fazla yükleme yapmak da son derece maliyetli olabilir. Bu nedenle birçok şirket uzaktan çalışanlar için tek bağlantı hattı kullanır. Bu hatlarda kesinti olduğunda tüm uzaktan çalışanlar iş yapamaz hale gelir. Kullanıcıya ait cihazları yönetmek de başlı başına bir zorluktur. Yeni çalışanları sisteme tanıtmak için BT ekiplerinin yeni çalışanlara VPN konfigürasyonları göndermesi gerekir. Bu süreç sancılı olabilir. VPN kullanımı ayrıca güvenlik endişelerine de yol açabilir. VPN aracılığıyla ağa bağlanan çalışanların erişimini mikro düzeyde denetlemek oldukça zordur. SASE, uzaktan çalışanların şirket kaynaklarına kolayca ve güvenli bir şekilde bağlanmasına olanak sağlayarak bu zorlukların üstesinden gelir.

SASE'nin Amacı

SASE'nin üç temel amacı vardır: Üretkenliği artırmak, ağ güvenliğini desteklemek ve internet bağlantısının maliyetini azaltmak.
SaaS uygulamalarını kullanan işletmelerde SaaS akışını ofisteki veri merkezine yeniden yönlendirmek, kullanıcı deneyimini kötü yönde etkileyen ve üretkenliği azaltan yığılmalara neden olur. SASE, bulut tabanlı uygulamalara ve verilere hızlı, güvenilir ve güvenli bir bağlantı sunarak performansı artırır.

SASE, ağ güvenliğini garanti altına almak için birden fazla yaklaşımdan yararlanır. Bu yöntemlerden biri sıfır güven ağ erişimidir. Sıfır Güven Ağ Erişimi (Zero Trust Network Access | ZTNA), kullanıcıların kimliğini sürekli olarak doğrulayan gelişmiş bir kimlik denetimi ve erişim kontrolü mekanizmasıdır. Kullanıcılar yalnızca yetkileri olan kaynaklara erişebilir. Bu paradigma, bir saldırı durumunda güvenlik ihlalinin kapsamını sınırlamak açısından hayati önem taşır. Güvenli Web Ağ Geçidi (Secure Web Gateway | SWG) ve tehdit koruması, SASE ağı güvenliğinin diğer temel taşlarıdır.
İnternet akışını MPLS (çoklu protokol etiket anahtarlama) devreleri aracılığıyla veri merkezlerine geri yönlendirmek oldukça pahalıdır. Bu akışı geleneksel MPLS'den SASE SD-WAN'a geçirmek, maliyet verimliliği açısından önemli bir faktördür. SD-WAN, internet bağlantısı maliyetini %65'ten daha fazla oranda azaltabilir.



SASE'nin Temel Bileşenleri

SASE, modern ağların tüm yönlerini desteklemek amacıyla farklı işlevleri olan çeşitli teknolojilerden oluşur. SASE'yi oluşturan temel teknolojilerden bazıları şunlardır: Sıfır Güven Ağ Erişimi (ZTNA), Servis Olarak Güvenlik Duvarı (FWaaS), Güvenli Web Ağ Geçidi (SWG), Tehdit Koruması ve Yazılım Tabanlı WAN (SD-WAN).

Sıfır Güven Ağ Erişimi (ZTNA)

ZTNA, ağa erişen her şeyin güvenilmez olduğu varsayımına dayanarak birlikte çalışan teknolojiler bütünüdür. ZTNA'nın birincil işlevi, kullanıcıları doğrulamak ve yalnızca yetkili oldukları kaynaklara erişim izni vermektir.

Yazılım Tabanlı WAN (SD-WAN)

SD-WAN, geniş alan ağlarının düşük maliyetli bir şekilde optimum performans göstermelerine olanak tanır. SD-WAN'ın temel işlevlerinden bazıları bant genişliği birleştirmek, güvenli şube bağlantısı ve gecikme optimizasyonu sağlamaktır.

Tehdit Koruması

Tehdit Koruması Sistemi, iş ağına yapılan iç ve dış siber saldırıları anında tespit ederek önler.

Servis Olarak Güvenlik Duvarı (FWaaS)

FWaaS, işletmelerin şirket içi UTM ve güvenlik duvarı sistemlerinin güvenlik ve ölçeklemeyle ilgili zorlukların üstesinden gelmelerini sağlayan bulut tabanlı bir güvenlik duvarı hizmetidir.

Güvenli Web Ağ Geçidi (SWG)

SWG, nerede çalıştıkları fark etmeksizin kullanıcıları internet kaynaklı tehditlerden korumak için tasarlanmıştır. Bu teknoloji, kötü amaçlı ve istenmeyen yazılım gibi tehditleri tespit eder ve engeller. SWG'nin standart işlevlerinden bazıları uygulama tanımlamak ve kontrol etmek, kötü niyetli internet akışını filtrelemek ve internet güvenliği ve uyumluluk politikalarını uygulamaktır.

Kullanım Senaryoları

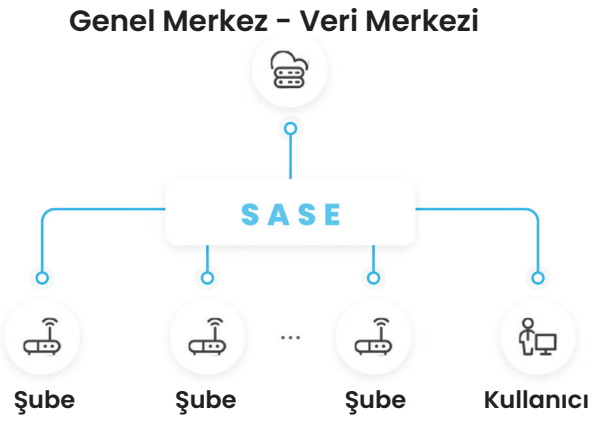
SASE BT dünyasını kasıp kavuruyor. Bazı uzmanlar bu hızlı adaptasyonu Covid-19 pandemisine bağlasa da, temel sebep bu teknolojinin modern dünyadaki birçok kullanım alanına hitap etmesidir. SASE'nin kayda değer bazı kullanım senaryoları şunlardır:

Uzaktan Çalışan Şirketler

SASE'nin popüler olmasındaki en önemli nedenlerden biri, uzaktan çalışanların sayısındaki hızlı artıştır. BT departmanları, geleneksel VPN sistemlerinin uzaktan çalışanların taleplerini ve şirketlerin güvenlik ihtiyaçlarını karşılamada yetersiz kaldıklarının farkına vardı. Bu durum onları SASE ve ZTNA teknolojilerini benimsemeye yöneltti. Uzaktan çalışanlara geniş ölçekte hizmet verme olanağı, SASE'yi uzaktan çalışanları bulunan şirketler için en iyi teknolojilerden biri haline getiriyor.

+50 Şubeli Şirketler

SASE teknolojilerinin iş dünyasında yer almaya başlamasından önce bazı şirketler SD-WAN çözümlerini kullanıyordu. Bu teknolojiler çeşitli yönlerden faydalı olsalar da BT ekiplerinin yeni zorluklarla karşılaşmasına yol açtı. Örneğin BT ekipleri her şubede güvenlik duvarları, izinsiz girişleri önleme ve URL filtreleme gibi hizmetleri sağlamakla yükümlüydü. Bu da teknolojiye yoğun işgücü tahsis edilmesinin yanı sıra, ağ performansında darboğazlara neden olma riskini de doğurdu. SASE teknolojisi tüm bu zorlukları giderebilir. Bu teknoloji, şubelerin en yakın bulut ağ geçitlerine bağlanmasına olanak tanır. Ayrıca güvenlik ekiplerinin buluttaki merkezi bir yönetim uygulamasından planlarını yürütmesini sağlar.



Sonuç

SASE, devrim niteliğinde bir ağ mimarisidir. Ancak SASE'nin uygulanmasına, mimari gerekliliklerle başlanmamalıdır. Bu teknolojiyi benimsemek isteyen şirketler, işleri için en anlamlı kullanım senaryolarını değerlendirmekle işe başlayarak daha sağduyulu davranmış olur. Berqnet, SASE çözümleri sunan sektör lideri markalardan biridir. Berqnet olarak size yalnızca SASE ürünleri sunmakla kalmıyor, işinize uygun kullanım senaryolarını değerlendirerek ihtiyaçlarınızı en iyi şekilde karşılayan çözümleri sunuyoruz. Bizimle bugün iletişime geçin ve iş ağınızın dönüşümünü birlikte gerçekleştirelim.

berqnet

berqnet.com

Berqnet Hakkında

Berqnet, Logo Siber Güvenlik ve Ağ Teknolojileri firmasının tescilli markasıdır. İşletmelerin siber güvenlik ihtiyaçlarına yönelik çözüm üretmek amacıyla 2013 yılında kurulan Logo Siber Güvenlik, %100 yerli AR-GE ekibi tarafından geliştirilen SASE ve Firewall ürün aileleri ile pazarın ihtiyaçlarını yakından takip ederek çevik ve kararlı ilerleyişine devam etmektedir.