berqnet

SD-WAN mı, SASE mi?

WAN bağlantısına ve güvenliğe bütünsel yaklaşım

Giriş

Güvenlik kurumsal düzeydeki tüm teknolojilerin temel koşuludur. Pandemiyle birlikte yaygınlaşan uzaktan çalışmanın hâkim olduğu "yeni normalde" çoklu bulut platformlarının daha fazla kullanılmaya başlanması, bu gelişme beraberinde tehdit ve saldırı sayılarında artışı da beraberinde getirdi. Bu nedenle, şirketlere WAN'larını (Geniş Alan Ağları) ve güvenlik mimarilerini dönüştürmeleri önemle tavsiye ediliyor.

Günümüzde bağlantı ihtiyaçları nedeniyle WAN açısından sağlam çözümlere ihtiyaç duyuluyor. Şirketler de bu nedenle SD-WAN (Yazılım Tabanlı Geniş Alan Ağı) ile yakından entegre güvenlik uygulamalarını devreye almadan önce çok sayıda seçeneği göz önünde bulundurmak zorundadır. Güvenlik bir kuruluşun iş ve yasal yükümlülüklerine göre kurum içi (on-premises) SD-WAN yönlendiricilerinde veya bulutta barındırılan SASE (Güvenli Erişim Hizmeti - Secure Access Service Edge) mimarisi çerçevesinde sağlanabiliyor.

Her işletmenin güvenlik ve ağ kullanım koşullarına uyan "standart beden" bir çözüm asla olmayacaktır. Bununla birlikte, SASE kapsamında WAN için gerçek anlamda dönüştürücü bir yaklaşımı benimsemek mümkün. Sektör uzmanları, SASE'nin SD-WAN ile gelişmiş güvenlik özellikli diğer ağ işlevlerini bir araya getirerek her ölçekte WAN ağ ve güvenlik koşullarını karşılayabileceği konusunda hemfikir.

Gartner, WAN koşullarına ve SASE mimarisinin sağladığı çeşitli faydalara bağlı olarak şu tahminlerde bulunuyor:

%15 >>> %30

2020 >>> 2023

Esnek ve etkin maliyetli ölçeklenebilir bant genişliği sağlayabilmek için kurumsal lokasyonların %30'u 2023 itibarıyla MPLS yerine sadece internet WAN bağlantısı olacak. Bu oran 2020'de yaklaşık %15'di.

%5 >>> %30

2020 >>> 2024

İşletmelerin %30'u 2024 itibarıyla bulutta sunulan SWG, CASB, ZTNA ve şubelerindeki hizmet olarak güvenlik duvarı (FWaaS) yetkinliklerini aynı sağlayıcıdan tedarik edecek. Bu oran 2020'de %5'ten azdı.

%10 >>> %60

2020 >>> 2025

İşletmelerin en az %60'ı 2025 itibarıyla SASE'nin kullanıcı, şube ve edge erişimini kapsayacak şekilde benimsenmesine yönelik net stratejilere ve takvimlere sahip olacak. Bu oran 2020'de %10'du.

Bu rapordan yararlanarak WAN'ın evrim sürecinde SD-WAN'dan SASE'ye nasıl ilerlediğini, iki teknolojinin benzerliklerini ve farklarını, birbirlerini nasıl bütünlediklerini daha iyi anlayabileceksiniz.

İçindekiler

SD-WAN ve SASE Karşılaştırması

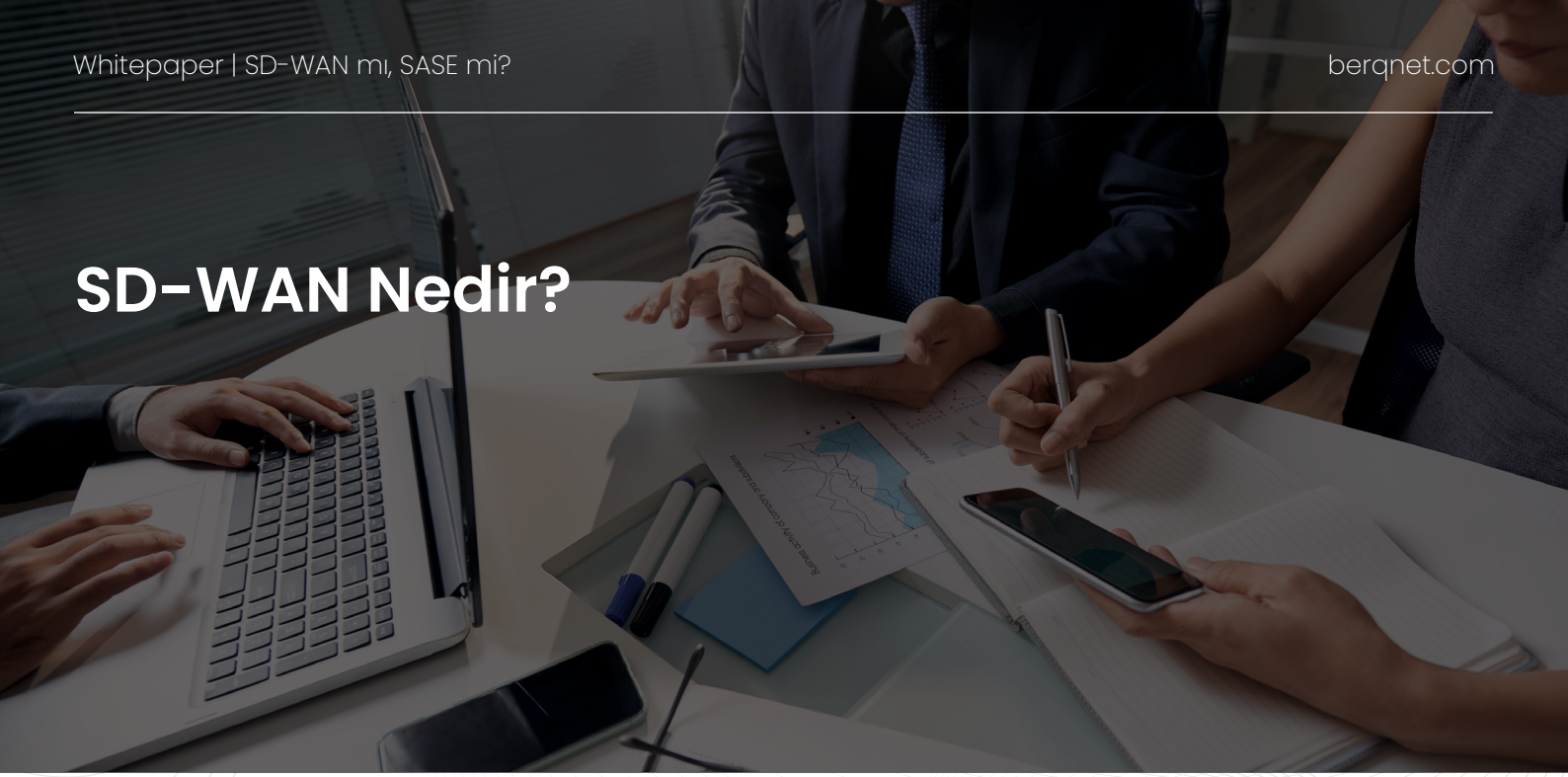
Gartner'in 2019 yılında SASE (Güvenli Erişim Hizmeti - Secure Access Service Edge) olarak bilinen yeni bir ağ ve güvenlik kategorisini tanıtması, sektör için bir kilometre taşı niteliğindeydi. SASE'den önce, SD-WAN özellikle 2010'lu yılların ikinci yarısında sektörün en popüler kelimelerinden biriydi. Ama şimdi SASE dikkatleri kendi üzerine çekiyor!

Bugün hâlâ SD-WAN ve SASE hakkında konuşulurken pek çok farklı yorum yapılıyor. SD-WAN daha ziyade SASE mimarisinin temel ve ayrılmaz bir parçasıdır. SD-WAN cihazları önemli ağ işlevleri sunarken, gelecek nesil SASE daha ileriye giderek SD-WAN ile diğer ağ ve güvenlik hizmetlerini yakınlaştırıp bütünsel bir WAN bağlantı ve güvenlik dokusu oluşturur.

SASE popüler inanışların aksine, SD-WAN yerine sunulan bir mimari değildir. Nihayetinde ikisi de aynı hedefe ulaşmaya çalışırlar ancak bulutla ilişkileri, araçların yeri ve trafik denetimi gibi konularda ciddi farkları vardır.

Şimdi SD-WAN ile SASE arasındaki benzerlikleri ve başlıca farkları anlamak için bu yönleri tek tek ele alalım.

SASE'den önce sektördeki en popüler kavramlardan biri SD-WAN'dı.



SD-WAN Nedir?

WAN (Geniş Alan Ağı) yönetimine yazılım tabanlı bir yaklaşım getiren SD-WAN, çoklu protokol etiket anahtarlama (MPLS) teknolojilerinin geleneksel WAN'ların yerini alması için tasarlanan bir ağ çözümüdür. Eşleştirilmiş herhangi iki SD-WAN cihazı arasında optimal, güvenli bağlantı için bir çözüm sunar.

WAN bağlantısına daha çevik ve bulut dostu bir yaklaşım getiren SD-WAN, 2010'lu yıllarda ağ altyapısı pazarının en hızlı gelişen segmentleri arasında yer alıyordu. İş yükleri giderek artan hacimlerle buluta taşınırken, SD-WAN işletmelere internet tabanlı VPN'ler (sanal özel ağlar) yerine güvenilir bir seçenek ve MPLS'ye daha dinamik ve etkin maliyetli bir alternatif sunmaktadır.

SD-WAN cihazları, işletmeleri olmaları gereken yere yakınlaştırmakla birlikte, bu tür cihazların büyük kısmı modern kurumların karşı karşıya kaldığı tüm ağ ve güvenlik sorunlarını çözecek şekilde tasarlanmamıştır. Örneğin, SD-WAN cihazlarında global bir omurga olmadığı gibi belirli gelişmiş güvenlik özellikleri de bulunmaz. Esas olarak lokasyonlar arası bağlantı sağlamak amacıyla tasarlandıkları için mobil işgücünü destekleyememektedir.

Başlıca Avantajlar

- MPLS, 4G/5G LTE ve diğer bağlantı türleri genelinde taşıma bağımsızlığı sunarak maliyeti düşürür.
- Uygulama performansını iyileştirir, çevikliği artırır.
- SaaS ve açık bulut uygulamaları için kullanıcı deneyimini ve verimliliği optimize eder.
- Otomasyon ve bulut tabanlı yönetim aracılığıyla operasyonları sadeleştirir.

Faydalar

- Daha iyi uygulama deneyimi sunar.
- Optimal bulut bağlantısı sağlar.
- Sadeleştirilmiş yönetim imkânı verir.
- Etkin maliyet yapısıyla çalışır.
- Bulut dostudur.

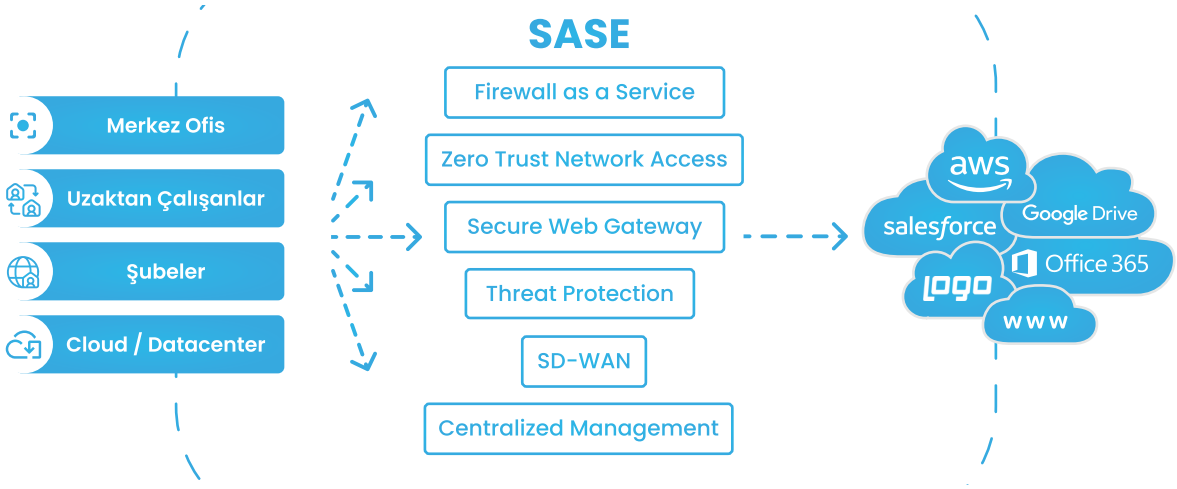
SASE Nedir?

SD-WAN önemli faydalar sağlasa da SD-WAN cihazları tek başına bütünsel bir çözüm sunamamaktadır. SASE de tam olarak burada devreye girmektedir.

SASE, SD-WAN ve ağ güvenlik noktası çözümlerini (FWaaS, CASB, SWG ve ZTNA) birleşik, bulutta yerleşik bir hizmette bir araya getirir. SD-WAN, SASE'nin ayrılmaz bir parçasıdır ama tek bileşeni değildir.

SASE, şubelerde gerekli WAN işlevlerini (SD-WAN, yönlendirme, segmentasyon, bölge temelli güvenlik duvarları ve WAN optimizasyonu gibi) bulutta sunulan ve yönetilen kapsamlı bulut tabanlı güvenlik hizmetleriyle birleştiren bir mimaridir.

SD-WAN esas olarak kurumların çeşitli şubelerini bir veri merkezine bağlamaya, SASE ise uç noktalara ve son kullanıcı cihazlarına odaklanır. SASE'nin trafik denetimi sadece trafiğin SD-WAN gibi bir veri merkezine yönlendirilmesi yerine dünya çapında bulunan çeşitli noktalarda (Point of Presence | PoP) gerçekleşir.



Başlıca Avantajlar

- Bulutta yerleşik mimari
- Global ağ omurgası
- Ağ ve güvenlik bir arada
- Birleşik yönetim sağlar

Faydalar

- İyileştirilmiş performans
- Artırılmış güvenlik
- Optimal kullanım kolaylığı
- Daha düşük maliyetler
- Bütünsel yaklaşım

SASE'nin Temel Bileşenleri

SASE kurumların ağ ve güvenlik işlevlerini uç noktalara daha yakın çalışan ve trafiği geleneksel ağ hizmetlerine kıyasla daha hızlı dağıtan bir bulut hizmeti içinde birleştiren yeni bir mimaridir. Kurumların temel ağ ve güvenlik hizmetlerini tek bir platformda bir araya getirerek yönetimlerini sadeleştirir.

Servis Olarak Güvenlik Duvarı

(Firewall-as-a-Service | FWaaS)

Güvenlik duvarı her ağ güvenlik sisteminin temelidir. SASE içerdiği FWaaS ile gereken ölçekleme kabiliyetini ve esnekliği sağlar ve eksiksiz bir ağ güvenlik sistemini ihtiyaca göre genişletebilir.

Sıfır Güven Ağ Erişimi

(Zero-Trust Network Access | ZTNA)

ZTNA erişim güvenliği için yeni bir yaklaşım sunmaktadır. Uygulamaya erişimi, kullanıcı kimliği, lokasyon, cihaz türü, davranış analizi gibi seçeneklere göre dinamik olarak ayarlayan sıfır güven politikasını benimsemektedir.

SD-WAN

(Software Defined Wide Area Networking)

SD-WAN yaklaşımı internet hatlarının kullanımını optimize etmek için ortaya çıkmıştır. MPLS çözümleri yerine standart internet hatlarını güvenli ve verimli kullanmak üzere tasarlanmış bir ağ çözümüdür. Çok şubeli yapılarda şubelerin birbirleriyle güvenli şekilde bağlanmasını sağlar.

Güvenli Web Ağ Geçidi

(Secure Web Gateway | SWG)

SWG kullanıcıları kötü amaçlı yazılımlar, şifre avcılığı (phishing) ve diğer web kaynaklı tehditlere karşı korur. SASE bütün lokasyonlardaki tüm kullanıcılara SWG koruması sunar ve politikaları çok noktalı çözümlerde tutma ihtiyacını ortadan kaldırır.

Geçiş Neden Gerekli?

Kurumsal ağlar hızla değişim geçirirken, kurumlar da bulut tabanlı altyapıdan giderek daha fazla yararlanmakta olup uzaktan çalışan ekiplerini desteklemektedir. Bu değişiklikler bir yandan da kurumların WAN altyapılarını güncellemelerini gerektirmektedir.

Bulut güvenlik hizmetlerinin ortaya çıkmasıyla SD-WAN SASE diye nitelenen bir hizmet haline evrildi. Bu evrimle kurumların değişen güvenlik ihtiyaçlarının karşılanması ve SD-WAN'ın kısıtlarının aşılması amaçlanmaktadır.

SD-WAN'ın sadece bir ağ çözümü olarak tasarlanması bu durumun en önemli nedenlerinden biridir. SD-WAN'dan önce internete ve bulut uygulamalarına yönlendirilen trafik bir MPLS devresi aracılığıyla kurumsal bir veri merkezine çekilmekte ve güvenliği de kurumsal bir güvenlik duvarıyla sağlanmakta idi. SD-WAN ile optimal ağ yolunun kurumsal güvenlik sistemlerini atlayıp doğrudan internete gitmesi sağlanmaktadır.

SASE, bulutta bir hizmet olarak devreye alınan güvenliği SD-WAN ağ optimizasyonu ile bir araya getirerek SD-WAN'ın kısıtlamalarını çözebiliyor. Ağ ve güvenlik hizmetlerinin yakınlaşması, içerik denetimi ve tek bulut hizmeti olarak sunulan güvenlik politikasının uygulanması ile trafiği genel merkezin ağı aracılığıyla yönlendirme ihtiyacının ortadan kalması anlamına geliyor. Buluttaki SASE çözümleri hemen her yerde uygulanabilmeleri sayesinde uzaktan çalışanlar ve bulut tabanlı altyapı için uygun hale geliyor ve ağ gecikme sürelerini minimuma indiriyor.

Bulut güvenlik hizmetlerinin ortaya çıkmasıyla SD-WAN SASE'ye evrildi

Benzerlikler

SD-WAN ile SASE çözümleri arasında seçim yapılırken SASE'nin, SD-WAN'ın gelecek neslini ve üst kümesini temsil ettiği göz önünde bulundurulmalıdır. Bir SD-WAN cihazının yapabildiği her şeyi SASE de yapabilir. Ancak, SASE ayrıca kurumların sıfır güven modelini bulutta etkin bir şekilde uygulamasını sağlayan entegre bir güvenlik paketi de sunar.

SASE ve SD-WAN benzer amaçlara hizmet etmelerine rağmen mimari açıdan fazla ortak noktaları bulunmamaktadır. Bununla birlikte, öne çıkan benzerlikleri arasında geniş alan ağları ve sanallaştırılmış altyapı sayılabilir.

- İkisi de coğrafi olarak uzak uç noktaları birbirine ve kurumların ağ kaynaklarına bağlarken özellikle altyapıları noktasında farklılık göstermektedir.
    - SASE altyapısı özel veri merkezlerini, ortak lokasyonlardaki tesisleri veya uç nokta işlevi gören bir bulutu kapsar. Networking, optimizasyon ve güvenlik işlevleri bu konumlarda çalışır.
    - Aksine, SD-WAN'da bu işlevler bir şubede ve genel merkezde bölmelere ayrılmıştır.
- İkisi de her yerden kumanda edilebilir.
- Temelde farklı formatlara sahip olmalarına karşın ikisi de sanallaştırılmıştır. İkisi de sanallaştırılmamış WAN gibi sabit işlevli özel kutulara bağlı değildir.
    - SASE güvenlik ve networking işlevlerini bir bulutta veya bir veri merkezinde ve bir güvenlik aracısında yürütür.
    - SD-WAN'da ise işlevler yazılım olarak çalışır. SASE güvenlik ve networking işlevlerini bir bulutta veya bir veri merkezinde ve bir güvenlik aracısında yürütür.
- İkisi de benzer amaçlara hizmet etmelerine rağmen bağlantı, mimari ve güvenlik gibi faktörler açısından farklıdır.

Bir SD-WAN cihazının yapabileceği her şeyi SASE de yapabiliyor!

Farklar

	SD-WAN	SASE
Odak	Ofisleri genel merkeze ve veri merkezine, ayrıca kullanıcıları doğrudan buluta bağlar.	Bulutta yerleşik güvenlik araçları sunar; ağın kalbinde bulut yer alır.
Uygulama	Esas olarak fiziksel, yazılım veya bulut bağlantıları aracılığıyla uygulanır. Kurumlar yönetilen, özelleştirilmiş veya hibrit SD-WAN arasından seçim yapabilir.	Hem şirket içi hem de bulut tabanlı ağları korur. Bulut işlevi, kurumlar için daha özelleştirilebilir olmasını sağlar.
Mimari	Tüm ağ altyapısının bir kurumun veri merkezi etrafında oluşturulduğu geleneksel networking konseptini izler.	Şirket içinde ya da bulut tabanlıdır; veri merkezi sadece bir başka güvenli erişim noktasıdır.
Güvenlik	Kapsamlı güvenlik için üçüncü taraf bileşenleri gerektirir.	Entegre güvenlik içerir.
Güvenlik ve bağlantı	Şubeleri ağlara bağlar ve trafiği yönlendirmek için yapılandırılmış ağ politikalarını izler.	Uç noktaları güvenli erişim noktalarına bağlar ve trafiği veri merkezlerine geri yüklemeden dünya çapında dağıtılmış POP'ler aracılığıyla gönderir.
Uzaktan erişim	Entegre uzaktan erişim yetkinliğine sahip olmadığı için üçüncü taraf bileşenleri gerektirir.	Entegre uzaktan erişim içerir.

Sonuç

Uzaktan çalışma koşulları ve ihtiyaçları zaman içinde ve dağıtılmış lokasyonlar bazında değişirken kesin olan bir şey var: Geleneksel teknolojiler artık yeterli değildir.

Ancak bu durum bir yandan da WAN'ın hızlı bir şekilde SD-WAN'a (yazılım tabanlı WAN) evrilmesine yardımcı oldu. Dağıtılmış lokasyonlar için trafik yönetimi açısından geleneksel WAN bağlantısının yarattığı pek çok soruna çözüm sunsa bile, temel yaşam döngüsü konularını çözmesi gerektiren bir noktaya ulaştı. Kurumlar bu konuları akılda bulundurarak özellikle uzaktan çalışan ekiplerini desteklemek için tasarlanmış yeni bir mimari türü olan SASE'ye geçmeyi düşünmelidir. SASE ve SD-WAN pek çok açıdan benzer olsa dahi, kurumlar iki teknoloji arasında seçim yaparken öncelikle tüm ihtiyaçlarını dikkatle değerlendirmelidir.

Dağıtılmış ağların geleceği

SD-WAN pek çok açıdan benzer olsa dahi, kurumlar iki teknoloji arasında seçim yaparken öncelikle tüm ihtiyaçlarını dikkatle değerlendirmelidir.

SASE hâlâ gelişmekte olan bir teknolojidir. Birçok ürün ve hizmet sağlayıcı da bu nedenle SD-WAN çözümlerine ek olarak artık SASE de teklif ediyor. Hibrit çalışma modellerinin giderek arttığı da dikkate alındığında bu trendin devam edeceği söylenebilir. Bununla birlikte, sektör uzmanları SASE çözümlerinin kademeli olarak SD-WAN'ları devre dışı bırakacağı konusunda hemfikir.

Gartner'ın Öngördüğü Stratejik Yol Haritası

Gartner'ın SASE için öngördüğü stratejik planlama varsayımları şöyle:

• 2023'e kadar esnek, uygun maliyetli ölçeklenebilir bant genişliği sağlamak için kurumsal lokasyonların %30'u (2020'de yaklaşık %15) MPLS yerine sadeceinternet WAN bağlantısına sahip olacak.

• 2024'e kadar işletmelerin %30'u (2020'de %5'ten daha az) aynı hizmet sağlayıcının bulutta sunacağı SWG, CASB, ZTNA ve şube ofis FWaaS özelliklerini benimseyecek.

• 2025 yılına kadar işletmelerin en az %60'ı (2020'de %10) SASE'nin benimsenmesi için kullanıcı, şube ve uç erişimini kapsayan açık strateji ve zaman çizelgelerine sahip olacak.

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.