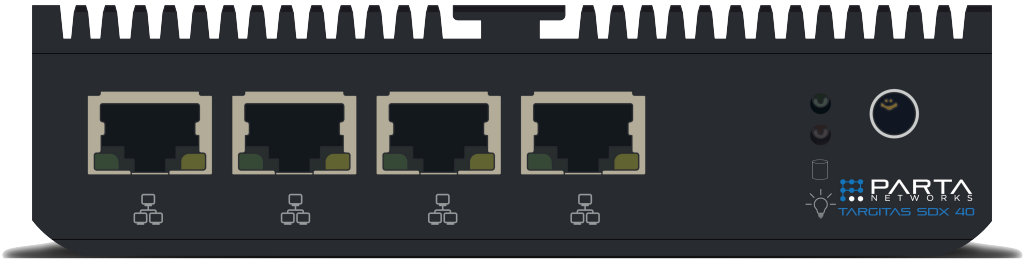
PARTA NETWORKS

TARGITAS® SDX 40



Targitas SDX 40; Yazılım Tanımlı Ağ mimarisine sahip, içinde MPLS Router, Next Generation Firewall, SD-WAN, NAC, NDR, Hotspot ve 5651 loglama bileşenlerini barındıran, Multi-Tenant yapıda çalışan, hepsi bir arada ağ ve ağ güvenliği çözümüdür. Full API desteği sayesinde 3.parti sistemlere kolaylıkla entegre olabilir.

Güvenlik

- Yeni Nesil Güvenlik Duvarı (NGFW) ile geniş alan ağlarında Layer 3 ve Layer 7 seviyesinde filtreleme ve bant genişliği belirleme gerçekleştirilir.
- 7500+ Uygulama ve 650+ Milyon web sitesine tanır. Uygulama ve Web kategorisi bazında filtreleme, bant genişliği düzenleme ve routing gerçekleştirebilir.
- Uçtan uca şifreleme ile tüm ağlarda güvenliği artırır.
- Siber güvenlik kapsamında iki faktörlü kimlik doğrulama özelliğini destekler.
- Targitas, herhangi bir konumda çalışan kullanıcılara uygulama ve servislere kolay erişim imkanı sağlayan esnek ve güvenli bir çözümdür.
- Targitas, sahip olduğu 45+ bin güvenlik imzası sayesinde ağda yer alan cihazları bilinen saldırı yöntemlerine karşı korumaktadır.
- Noktadan noktaya VPN sayesinde iki veya daha fazla nokta arasındaki bölgeye güvenli bir şekilde erişimi sağlamaktadır.
- Network trafiğindeki şifrelenmiş ya da şifrelenmemiş paketlerin, kaynakların ve eklerin kötü amaçlı olması olasılığına karşın etkin koruma sağlar.

Performans

- Dağıtık mikro servis mimarisi sayesinde yüksek performans sağlar.
- Özel olarak geliştirilen algoritmalar sayesinde aynı anda ağ yapısında eşit performans sergiler.
- NAC, Telemetry vb. performans yükleri sanal makineye aktarılarak sahip olunan donanımdan daha yüksek verim alınabilir.

Networking

- Enterprise, data center ve telco teknolojilerini tek bir yapı olarak sunar.
- Ağı bir bütün olarak gören yazılım tanımlı ağ yaklaşımı sayesinde uçtan uca çözümler sunar.
- BGP, MPLS, OSPF, Multicast Routing, PPPoE Server vb. Ağ yapılandırma teknolojilerini destekler.

Yönetim

- Ağ ve ağın erişilebilirliğini kontrol etmeyi sağlar.
- Aktif olarak tek bir arayüz üzerinden tüm ağ etkinliklerinin görüntülenmesini, filtrelenmesini ve yönetilmesini sağlar.
- Genişleyebilir, izlenebilir, uygulama seviyesinde performans ölçümünün yapıldığı ve özel politikaların oluşturulduğu, uygulamaların servis bazında kontrol altında tutulduğu, yazılım ile programlanabilen bir altyapıya sahiptir.
- Cihazların birbirleri ile haberleşmesi için ortak bir dil ile ağdaki cihazlar, donanım bağımsız merkezi bir yönetime sahip olmaktadır.
- Zero Touch Provisioning (ZTP) methodu kullanılarak uç cihazların ilk kurulumda kendileri için hazırlanan konfigürasyonu merkezden alması ve template yapısı kullanılarak birden fazla uç cihazdaki güvenlik özelliklerinin merkezden tek bir değişiklik ile yönetilmesi sağlanır.

Attributes	SDX 40
Layer-3 Firewall	
Layer 3 Statefull Firewall	✓
NAT Support	✓
Port Forwarding	✓
IPS	✓
DoS Protection	✓
Layer 3 QoS	✓
Layer 7 QoS	✓
Layer 7 Filtering	✓
Policy Based Routing	✓
Active Directory Support	✓
Binat Support	✓
Firewall flow forwarding support to the specified IP address	✓
ToS (Tyoe of Service) and priority modify	✓
FTP Proxy Support	✓
Layer-7 Next Generation Firewall	
OSI Layer 7 level analysis and filtering	✓
7.500+ Application identification	✓
650M+ categorized web sites identification	✓
Internal 5651/GPDR Logging	✓
NDR support	✓
Destination Aware Detection	✓
SSL Inspection	✓
Layer 7 Traffic Shaping and Bandwith Control	✓
Scheduled L7 filtering	✓
MAC Logging	✓
IP Accounting	✓
Attached SD-WAN Rules	✓
MAC based L7 filtering rules	✓
Cyber Thred Intelligence	✓
Application Aware Routing	✓
Application Aware QoS (Guarantee/Max)	✓
Application Aware Filtering	✓

SLA (Latency, Jitter, Packet Loss, Quota)	✓
Cost Based SLA Selection	✓
Backup Interface	✓
Best Path Selection	✓
Dynamic Path Selection and Dynamic Multipath Optimization	✓
Ability to utilize multiple links simultaneously	✓
Application aware WAN Bonding	✓
Built-in link load balancing and failover	✓
Encryption and secure communication between branches	✓
Local Breakout / Direct Internet Access	✓
Real-time visibility into network traffic, applications, protocol, web categories threats and users	✓
Application performance monitoring and reporting	✓
Real-time visibility into network performance and application usage	✓
Traffic analytics and reporting	✓
Proactive alerts and notifications	✓
Historical data and trend analysis	✓
Multiple Serving IP Adddress	✓
Strong Authentication and Encryption Algorithm	✓
ESP and AH Encapsulation Method Support	✓
Tunnel and Transport Encapsulation Mode Support	✓
Detailed logging and telemetry	✓
NAC	
IEEE 802.1X Support	✓
Local RADIUS Server	✓
Integration with Active Directory	✓
Dynamic Vlan Assignment	✓
Internal 5651 Logging	✓
MAC Auth. possibility	✓
Hotspot	
Support AD, Local User, TC Credentials and SMS Authentication Method	✓
Support L2 and L3 Hotspot	✓
Customizable Captive Portal	✓
Internal 5651 Logging	✓

Management users can block specifis users Hotspot connection.	✓
Detailed Hotspot Auhtentication and Accounting logging	✓
ZTNA	
Client Authentication Control	✓
Client Device Posture Control	
Client Accounting Control	✓
Secure and simple access to applications and services, regardless where they are located	✓

License Type	License Content
BASE	Layer 3 Statefull Firewall
DPI	Deep Packet Inspection Module
HOTSPOT	Hotspot Module
SSL VPN	SSL VPN Module
NGIPS	Next Generation Intrusion Prevention System Module
NAC	Network Access Control Module
BGP	Border Gateway Protocol Configuration Module
MPLS	Multi Protocol Label Switching Configuration Module
WAF	Web Application Firewall Module
VM	Running Targitas Targitas in a Virtual Machine

Uygulama Alanları

Yeni Nesil Güvenlik Duvarı (NGFW)

- Ipv4 ve Ipv6 desteklenmektedir.
- L3/L7 seviyesinde güvenli ağ geçidi olarak çalışır.
- Port Yönlendirme gerçekleştirir.
- Deep Packet Inspection ile SSL trafiğini yönetir.
- 7500+ Uygulama ve 650+ Milyon web sitesine tanır. Uygulama ve Web kategorisi bazında filtreleme, bant genişliği düzenleme ve routing gerçekleştirebilir.
- MAC adresine özel Layer 7 filtreleme ve bant genişliği düzenleme gerçekleştirebilir.
- Deep Packet Inspection NDR modunda hizmet verebilir ve sanal ağlarda mikro segmentasyon sağlar.
- SSL Inspection gerçekleştirebilir.
- RFC uyumlu Full NAT, NAPT ve BINAT özelliklerini sağlar.
- IPSEC VPN/ IPSEC NAT Traversal ile sanal özel ağ kurabilir.
- Policy based Routing ile gelişmiş yönlendirme politikaları kullanılabilir.
- Coğrafi bölgelere göre güvenlik politikaları uygulanabilir.
- Kullanıcı dostu arayüzü sayesinde, QoS, DDoS, DPI, Hotspot, PBR, IPS, MS-AD ve NAT dahil tüm politikalar tek bir ekrandan yapılandırılabilmektedir.
- 5651 Yasalı kanuna tam uyumluluk ile izleme ve loglama yapmaktadır.
- Active Directory kullanıcılarının Web Filtreleme, Güvenlik Duvarı, Kimlik Doğrulama vb. modüllerinde kullanılabilmesini sağlar.

SD-Branch

- Şubelerdeki ağ ve internet trafiğine ait güvenlik politikalarının, ilgili trafiğin daha merkeze ulaşmadan şubede uygulanmasını sağlar. Bunu Zero Touch Provisining methodu aracılığı ile SD-WAN Controller üzerinden gerçekleştirir ve merkezi orkestrasyonun bir parçası olarak çalışır.
- Tek merkezden şubelerdeki güvenlik politikaları yönetilebilir ve şube üzerinden geçen trafiğe ait analizler incelenebilir.
- Şubeler arasında haberleşmeyi hızlı, etkin ve güvenli şekilde sağlar.
- Geliştirilen karar algoritmaları sayesinde yapılandırılması kolaydır.
- Her WAN bağlantısının stabilitesini kontrol eder. WAN bağlantılarının performans değerlerine göre (Latency, Jitter ve Packet Loss) yönlendirme politikaları oluşturulabilir. İstenilen Uygulama ve Web kategori trafiğinin belirlenen kritere göre en iyi performans gösteren WAN bağlantısından yönlendirilmesi veya belirli stabilite şartlarını sağlayan WAN bağlantılarından trafiğin dengeli bir şekilde aktarılması vb. Politikalar uç cihazlarda uygulanır.
- Kritik uygulamaların sağlıklı çalışabilmesi için en iyi bağlantının seçileceği şekilde uygulama veya kullanıcı trafiği arasında ayrım yapar.

SD-WAN

- Ağ trafik yönetimi, güvenliği ve izleme şeklini donanım bağımsız yazılım tabanlı hale getiren, farklı tipte kurumsal ağları (MPLS, LTE, PPPoE, enterprise internet vb.) uzak hedeflere bağlamak için kullanılan, merkezi olarak yönetilen WAN sanallaştırması ile optimum performansı elde etmeye çalışan, bütünleşik yazılım tanımlı, geniş alan ağıdır.
- Dağıtık ağ mimarilerini birbirine güvenle bağlar.
- Optimizasyon için çoklu bulut ortamıyla entegredir.
- Basit bir kullanıcı arayüzüne sahiptir.
- Gerçek zamanlı tehdit algılama ve önleme özelliğine sahiptir.
- Ağı görünür kılar.

NAC

- Belirlenmiş politikalar sayesinde erişimi kontrollü olarak sağlar.
- Sadece güvenlik ilkelerine uyan ve giriş izni verilmiş kullanıcıların ağa dahil olmasını sağlamaktadır.
- Yerel ağ ve BYOD kaynaklı Zero Day saldırılarının etkisini minimuma indirir.
- Ağ güvenlik denetlemesi yapar.
- Ağa erişim esnasında, önce veya sonra izinsiz erişim, yetkisiz giriş, cihaz uyumu ve davranışlarını denetler.
- Aracısız erişim kontrolüne sahip Targitas SDX 40, kullanıcıların ağa erişmeden önce uçtan uca güvenliğe göre yetkilendirmeye izin verir.
- 2FA ile yüksek seviyede güvenlik sağlar.
- Dynamic Vlan ataması sayesinde esneklik sağlar.
- Ağ erişimlerinin telemetrik olarak izlenmesini sağlar.

Uygulama Alanları

Hotspot

- Targitas Hotspot; lokal kullanıcı, Sms, Active Directory, Kimlik bilgileri, Elektra,Sedna ve Opera otelcilik yazılımı entegrasyonları aracılığıyla, kullanıcıların internet erişiminden önce kimlik doğrulama mekanizmasından geçmesini sağlar.
- Kullanıcıların yönetilmesi için güçlü bir platformdur.
- 5651 sayılı kanuna uygun loglama modülüne entegredir.
- Çalışmakta olduğunuz SMS operatörünün API desteği olması durumunda sisteme en kısa sürede entegre edilmektedir.

Secure Web Gateway (SWG)

- Web filtreleme yaparken kaynak olarak MS-AD, Hotspot ve NAC gibi Targitas modüllerinde yer alan tüm kullanıcılar tanımlanabilir.
- Aynı zamanda 5651 Sayılı kanuna uygun loglama yapmaktadır.
- 97 farklı kategoride 650 Milyon domain/url kategorize edilmiştir.
- Zero Day desteği sayesinde web'den gelen tehditleri önler.
- TLS Inspection özelliği sayesinde SSL-Offloading'e gerek kalmadan (kullanıcıya sertifika yüklettirmeden) web filtreleme politikalarını işletir.
- Yönetilebilir DoS politikaları ile olası servis dışı bırakma saldırılarının önüne geçer.
- Oldukça esnek bir web filtreleme olanağı sağlar. URL'ye göre, kullanıcıya göre, zamana göre politikalar oluşturarak internet erişiminin efektif olarak kontrol edilmesini ve sınırlandırılmasını sağlar.

BRAS

- Targitas geniş bant uzaktan erişim sunucusu olarak da kullanılabilir.
- Targitas üzerinde yer alan tüm AAA modülleriyle entegredir.
- COA desteği vardır.
- PPP Over Ethernet Server özelliği RFC 2516 uyumludur.
- Layer Two Tunneling Protocol desteği RFC 2661 uyumludur.

Telemetri

- Sistemin ve ağın, güvenlik bileşenlerini de içerecek şekilde düzenli olarak fotoğrafını çeker ve olası sorunlarda network yöneticilerine alarm gönderip, sorun kaynağının analiz edilmesinde kolaylık sağlar.
- Anlık olarak ve geçmişe dönük gelişmiş bir raporlama altyapısı sunar.
- Günlük, haftalık, aylık olarak web erişim istatistikleri hazırlar. Bu istatistikler; kullanıcıya, URL'ye, tarihe, saate, download/upload miktarına ve diğer birçok kritere göre filtrelenebilir.
- Her gün, günlük olarak erişim bilgilerinin bulunduğu, günlük olarak ağdaki hareketlere ilişkin genel ve detaylı bilgileri barından bir raporu PDF olarak hazırlar.
- Her günün sonunda, günlük erişim loglarını 5651 kanununa uygun olarak imzalar ve depolar.
- Anlık olarak; ağdaki aktif cihazlar ve kullanıcılar görüntülenebilir, kullanıcıların kullandığı bant genişliği miktarı, kullanıcıya ilişkin IP, Port, Mac Adresi bilgileri, erişim sağlanan URL'ler görüntülenebilir.

MPLS Router

- Targitas MPLS Router; gre, egre, mgre, eoip gibi kurumsal tünelleme protokolleri ile vxlan, nvgre gibi veri merkezi tünelleme protokollerini tek cihazda destekler.
- Multi VRF desteği vardır.
- RIP, OSPF ve BGP desteği vardır.
- Omurga bir yönlendiricide desteklenmesi gereken tüm BGP özellikleri mevcuttur.
- Telco operatörlerinin ihtiyaç duyacağı tüm MPLS fonksiyonlarını içerecek şekilde MPLS desteği vardır.
- MPLS tünelleme protokolü olarak LDP kullanılmaktadır.
- L2VPN ve L3VPN desteği vardır.
- Multicast routing desteği vardır.
- Tüm bu özellikleri Ipv4 ve Ipv6 için destekler.

NFV

- Ağ fonksiyonlarının sanallaştırılması capex ve opex maliyetlerini azaltır.
- Multi-queue SR-IOV teknolojisi üzerine inşa edilmiştir.
- Eski nesil ASIC'lere göre üstün performans sağlar.
- Sanallaştırma hipervizörü üzerinde çalışır.
- Vmware ve KVM desteği vardır.

Uygulama Alanları

NDR (Network Detection Response)

- Mikro Segmentasyon çözümü olarak NDR, Firewall bulunamadığı ortamda gerekli güvenliği sağlar. Aynı IP ağında yer alan sanal sunucuların kendi aralarında gerçekleşen doğu-batı trafiğini uygulama (DPI) ve tehdit (IDS) seviyesinde görünür kılar.
- 5651 Sayılı kanuna uygun loglama, alarm üretme yeteneği, makine öğrenmesi tabanlı anomali tespiti özellikleri sayesinde güvenlikte görünürlüğü artırır.
- NDR modunda bir ağ topolojisine kolaylıkla entegre olur. İlk kurulum anında herhangi bir sistem kesintisine neden olmaz.

Yeni Nesil Saldırı Engelleme Sistemi (NGIPS)

- Targitas NGIPS, sahip olduğu 45+ bin güvenlik imzası kullanılarak IPS (Saldırı Engelleme Sistemi) ve IDS (Saldırı Tespit Sistemi) rollerinde görev alır.
- 61 farklı kategoride 38 farklı etki sınıfına ait IPS imzasına sahiptir. Bu özelleştirme sayesinde farklı tür işletim sistemi ve sunucular için farklı saldırı tür ve risk seviyeleri için imzaları barındıran IPS Politikaları oluşturulur.
- NDR modunda görev alabilir.

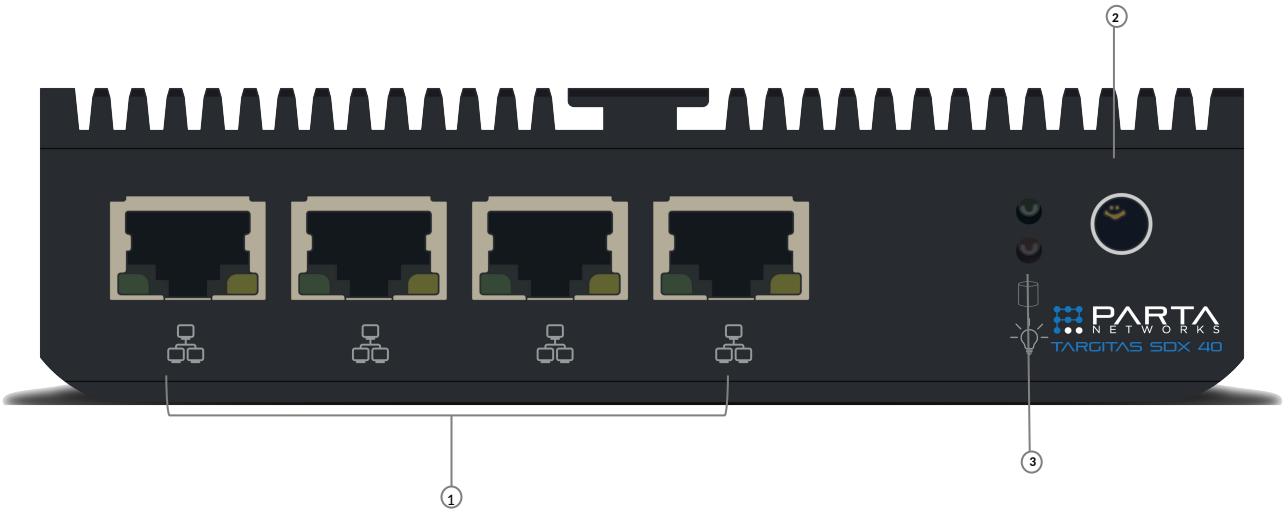
Zero Trust Network Access (ZTNA)

- Targitas ZTNA, herhangi bir konumda çalışan kullanıcılara uygulama ve servislere güvenli ve kolay erişim imkanı sağlayan esnej, güvenli ve kapsamlı bir çözümdür.
- Kimlik, gereksinim ve erişim temelli doğrulama gerçekleştirir. Kullanıcı doğrulamasına ek olarak bağlanan cihazın durumu kapsamlı bir şekilde değerlendirilir. Kullanıcı ve cihaz değerlendirmesi ardından doğrulanan bağlantının iç ağda erişim yetkisi sınırları içerisindeki uygulama ve servislere ulaşabilir.
- Targitas ZTNA, kullanıcıların doğrulama ardından iç ağda IP adresine sahip olmadan uygulama ve servislere erişmesini sağlar. IP adresi kullanıcıda bulunmadığı için ZTNA, saldırı yüzeyini küçültmeye yardımcı olarak siber riskleri azaltır.

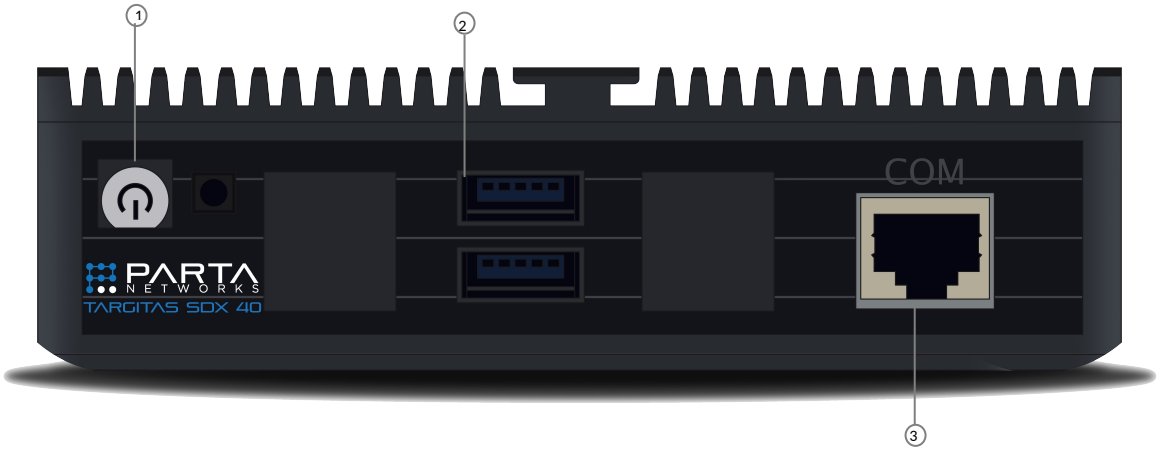
VPN Gateway

- IPSec protokolü ile site-to-site (noktadan noktaya) güvenli bağlantı sağlar. IPSec destekleyen tüm cihazlarla uyumludur.
- SSL VPN ile kullanıcıların ağa yüksek şifreleme ile dahil olmasını sağlar. Targitas AAA modüllerinde yer alan tüm nesneler kimlik doğrulama aracı olarak kullanılabilir.
- Clientless SSL VPN destekler.

Donanım Özellikleri



No	Açıklama
1	4 x 2.5GbE RJ45
2	Güç Desteği
3	Led Sinyalleri



No	Açıklama
1	Power Tuşu
2	2x USB Girişi
3	Console Portu

Teknik Özellikler

Donanım Özellikleri	
İşlemci	4 Cores
Bellek	8 GB DDR4
Maksimum 2.5 GbE RJ45 Bakır Port	4
Maksimum 10 GbE SFP+ Fiber Port	0
Maksimum 40 GbE QSFP+ Fiber Port	0
USB Port	2
Konsol Port	1
Dahili Depolama	128GB SSD
Desteklenen SFP Modülleri	
Performans	
Router Throughput	2.5 Gbps
Firewall Throughput	2.5 Gbps
NDR Throughput	2.5 Gbps
DPI Throughput MTU 1500	850 Mbps
DPI Throughput MTU 9000	2.4 Gbps
Eşzamanlı oturum (TCP)	2.000.000

Boyutlar	
(WxDxH)	130 x 135 x 40 mm
Ağırlık	0.550 Kg
Güç	
AC Güç Kaynağı	60W Power Adapter
Giriş	12V 5A DC
Çevresel Parametreler	
Sıcaklık	0~40ºC
Nem (RH)	5~90%
Onaylar ve Uyumluluk	
Sertifikalar	CE/FCC Class A, UL, RoHS

Targitas Destek Merkezleri

Parta Networks
Teknik Destek Merkezleri

Targitas Ankara, İstanbul, İzmir Destek Merkezleri müşterilerimiz için stratejik olarak konumlandırılmıştır. Destek mühendisleri aracılığıyla müşterilerimizin ihtiyaç duyduğu desteği hızlı şekilde sağlamaktadır.

Olası bir güvenlik riskinde hızlı müdahaleye de olanak sağlayan Destek Merkezleri kullanıcıların zorluk yaşamamasını, yaşanan olası bir zorluğun da kısa sürede aşılmasını sağlar. Targitas Destek Merkezleri, tüm teknik sorunları olabildiğince verimli bir şekilde çözmek için aşağıdaki önem tanımlarını ve hedef yanıt sürelerini destekler.

Seviye 1 : 1 Saat içinde müdahale,
Targitas yazılım veya donanım koşulları, ticari faaliyetlerin yürütülmesini tamamen yada kısmen engelliyor. Cihaz açılmıyor veya trafik geçmiyor.

Seviye 2 : 4 Saat içinde müdahale,
Kritik olmayan sorunların giderilmesi veya Targitas ürün ailesi dışında kalan ürünler ile entegrasyon talepleri.

Seviye 3 : Ertesi iş günü içinde müdahale,
Targitas ürünlerinin konfigürasyon (“nasıl yapılır”) destekleri.

Tasarlanan bu metotlar sayesinde kullanıcıları birçok prosedür, maliyet ve zaman kaybından hariç tutmaktadır. Ortaya koyulan hizmetin devamlılığını, kullanıcıya yönelik sağlar.