Privia SECURITY

Yönetilen Güvenlik Servisleri (MDR) Hizmeti

Profesyonel Defensive Security Hizmetleri

"Küresel Tehditler için Profesyonel Hizmetler!"

Küçükbakkalköy Mah. Kocasinan Cad.
Privia Plaza No:42 Ataşehir, İstanbul

+90 (216) 514 72 14

www.priviasecurity.com

"Gelişmiş tehdit istihbaratı ve sürekli izleme süreçleriyle, küresel tehdit ortamında organizasyonların siber güvenlik ihtiyaçlarını karşılıyoruz. Küresel tehditlere karşı profesyonel çözümlerimiz, organizasyonların güvenlik stratejilerini en üst düzeye taşır."

MDR (Managed Detection and Response) Hizmeti, organizasyonların siber güvenlik operasyonlarını kesintisiz bir şekilde (7/24) izleyen, analiz eden ve tehditleri etkisiz hale getiren kapsamlı bir güvenlik hizmetidir. Günümüzde siber tehditler giderek daha karmaşık ve yaygın hale gelirken, güvenlik ihtiyaçları da hızla değişmektedir. MDR Hizmeti, karmaşık tehditlere karşı organizasyonların savunma altyapılarını güçlendiren bir hizmet sunar. Siber güvenlik uzmanlarıyla, tehdit tespit sistemleriyle desteklenen hizmet, güvenlik zafiyetlerinin anında tespit edilmesini sağlar. Tehditlerin hızlıca analiz edilmesi, güvenlik olaylarına müdahale sürecini hızlandırarak organizasyonların güvenlik olgunluğunu artırır. MDR hizmeti, SIEM, EDR ve NDR gibi güvenlik teknolojileriyle entegre çalışarak tehditleri tespit etme ve yanıt verme süreçlerini optimize eder.

Siber saldırılar, çeşitli tekniklerle organizasyonların güvenlik zafiyetlerinden faydalanmaya çalışır. Söz konusu durum siber güvenlik ekiplerinin her an hazırlıklı olmasını zorunlu kılar. MDR hizmeti, organizasyonların güvenlik sistemlerini sürekli izleyerek tehditleri önceden fark etmelerine olanak tanır. Gelişmiş tehdit algılama algoritmaları ve yapay zekâ destekli analiz süreçleriyle MDR hizmeti, siber güvenlik ekiplerine gerçek zamanlı bilgi akışı ve yönetim imkânı sağlar.

MDR hizmeti yalnızca tehditlerin tespit edilmesini değil, aynı zamanda etkisiz hale getirilmesini de sağlar. Güvenlik zafiyetleri veya şüpheli aktiviteler tespit edildiğinde hızla harekete geçilir. Tehditlerin büyümeden önlenmesi için geliştirilen hızlı yanıt mekanizmaları, güvenlik zafiyetlerinin kapatılmasını ve dijital varlıkların korunmasını sağlar. MDR hizmeti, organizasyonların güvenlik ekiplerinin iş yükünü azaltarak güvenlik operasyonlarını daha verimli hale getirir.

Hizmete Ait Bileşenler

Tenable Ürün Ailesi MDR Hizmeti ve Ürün Yönetimi

Tenable MDR Hizmeti, güvenlik zafiyetlerini izleyip tespit eden Tenable ürün ailesinin yönetimini ve işletilmesini kapsar. Sistem ve ağ zafiyetlerini sürekli tarayarak organizasyonun güncel küresel tehditlere karşı önlem almasını sağlanır. Tenable'ın sunduğu detaylı raporlar, güvenlik ekiplerine hangi zafiyetlerin öncelikli olarak kapatılması gerektiği konusunda yol göstericidir. MDR ekibimiz, güvenlik açıklarını minimize etmek için Tenable ürünlerini yapılandırıp optimize ederek, teknolojilerin aktif olarak işletilmesine olanak verir.

Picus MDR Hizmeti ve Ürün Yönetimi

Picus MDR Hizmeti, siber güvenlik simülasyonları ile güvenlik sistemlerinin etkinliğini test etmeyi amaçlayan bir hizmettir. Picus'un sürekli saldırı simülasyonları, güvenlik önlemlerinin ve yapılandırılan politikaların ne kadar başarılı olduğunu değerlendirmemizi sağlar. MDR ekibimiz, güvenlik duvarları, IDS/IPS ve diğer güvenlik çözümlerinin mevcut durumunu analiz eder. Organizasyon, güvenlik sistemlerinin eksikliklerini erkenden fark ederek iyileştirme fırsatı elde eder. Picus simülasyonları ile yapılan düzenli testler, güvenlik önlemlerinin etkinliğini ölçüp artırmaya yönelik gerçekleştirilir.

ThreatMon MDR Hizmeti ve Ürün Yönetimi

ThreatMon MDR Hizmeti, gerçek zamanlı tehdit algılama ve izleme süreçleriyle organizasyonların güvenliğini korur. MDR ekibimiz, ThreatMon platformunu kullanarak siber tehdit istihbaratı sağlar. Zararlı ağlar sürekli izlenerek, organizasyonla ilgili istihbarat verileri sağlanır. ThreatMon'un sunduğu analizlerle tehditlerin kaynağını ve tehdit organizatörleri erkenden tespit edilir.

Trellix (McAfee ve FireEye) Ürün Ailesi MDR Hizmeti ve Ürün Yönetimi

Trellix MDR Hizmeti, McAfee ve FireEye çözümlerinin entegrasyonu ile tehdit tespiti ve yanıt sürecini hızlandırır. MDR ekibimiz, uç nokta güvenliği, ağ güvenliği ve tehdit avcılığı gibi tüm Trellix ailesine ait ürünlerini işletir. FireEye'ın gelişmiş tehdit istihbaratı ve McAfee (Trellix)'nin uç nokta güvenliği özellikleri bir araya getirilerek kapsamlı bir koruma sağlanır. Organizasyonlar, Trellix MDR çözümleri ile organizasyonun tüm güvenlik operasyonlarını yönetme şansına sahip olur.

Wazuh MDR Hizmeti ve Ürün Yönetimi

Wazuh MDR Hizmeti, açık kaynaklı güvenlik izleme ve tehdit algılama çözümlerini içerir. MDR ekibimiz, Wazuh'un SIEM ve HIDS özelliklerini kullanarak güvenlik olaylarını analiz eder. Wazuh, ağ aktivitelerinin ve güvenlik olaylarının detaylı bir şekilde izlenmesini sağlar. Güvenlik zafiyetleri anında tespit edilir ve bu zafiyetlere yönelik anında müdahale sağlanır. Wazuh'un sunduğu veri analitiği ve raporlama özellikleri ile güvenlik politikaları olgunlaştırılır.

DarkTrace MDR Hizmeti ve Ürün Yönetimi

DarkTrace MDR Hizmeti, yapay zekâ destekli siber güvenlik çözümleri ile ağ tabanlı anomalileri tespit eder. MDR ekibimiz, DarkTrace'in gelişmiş anomali tespiti özelliklerini kullanarak güvenlik zafiyetlerini analiz eder. DarkTrace, makine öğrenimi ile desteklenen bir çözüm olduğundan, organizasyonun normal ağ aktivitelerini öğrenir ve olağan dışı hareketleri tespit eder. MDR ekibimiz, bu anormal aktiviteleri izleyerek tehditlere anında müdahale eder. DarkTrace'in gelişmiş analitik özellikleri, tehditlerin kaynağını ve etkisini hızlıca anlamamıza yardımcı olur.

Netsparker MDR Hizmeti ve Ürün Yönetimi

Netsparker MDR Hizmeti, web güvenlik tarama çözümleri ile organizasyonun web uygulamalarını analiz etmeye olanak verir. MDR ekibimiz, Netsparker'ın tarama araçlarını kullanarak web uygulamalarında zafiyet taramaları gerçekleştirir. Web uygulamalarında bulunan güvenlik zafiyetleri hızlıca tespit edilip, giderilmesi için güvenlik ekiplerine raporlar sunulur. MDR ekibimiz, güvenlik açıklarını düzenli olarak test ederek web uygulamalarının korunmasını sağlar.

Acunetix MDR Hizmeti ve Ürün Yönetimi

Acunetix MDR Hizmeti, web güvenlik zafiyetlerini tespit eden Acunetix çözümlerinin yönetimini sağlar. MDR ekibimiz, Acunetix ile düzenli olarak uygulama güvenlik testleri yaparak güvenlik zafiyetlerini kapatma süreçlerini yürütür. Web uygulamalarında en çok karşılaşılan zafiyetleri önleyerek organizasyonun güvenlik düzeyini artırır. Acunetix'in sunduğu detaylı raporlar, güvenlik ekiplerinin riskleri öncelik sırasına göre ele almasını sağlar.

CloudFlare MDR Hizmeti ve Ürün Yönetimi

CloudFlare MDR Hizmeti, güvenlik ve ağ koruma çözümlerini yöneterek organizasyonların dijital altyapısını korur. MDR ekibimiz, CloudFlare'in DDoS koruması, web uygulama güvenlik duvarı (WAF) ve içerik dağıtım ağı (CDN) özelliklerini işletir. CloudFlare, web trafiğini analiz ederek zararlı aktiviteleri anında engeller ve web sitelerinin güvenliğini sağlar. Hizmet, organizasyonların çevrimiçi varlıklarını korurken hız ve performansı da artırır. MDR ekibimiz, CloudFlare'in tüm güvenlik özelliklerini organizasyonun güvenlik stratejisi ile uyumlu hale getirir.

Rapid7 MDR Hizmeti ve Ürün Yönetimi

Rapid7 MDR Hizmeti, güvenlik zafiyetlerini ve saldırı tehditlerini izleyen Rapid7 çözümlerini yönetir ve işletir. MDR ekibimiz, güvenlik zafiyetlerini anında tespit eden InsightVM gibi Rapid7 ürünlerini optimize eder. InsightIDR ile tehdit algılama süreçleri güçlendirilerek güvenlik ekiplerinin hızlı müdahale etmesi sağlanır. Rapid7, tehdit istihbaratına dayalı analizlerle riskleri önceliklendirir ve zayıf noktaların tespit edilerek ortadan kaldırılmasını sağlar. MDR hizmetimiz, zafiyet yönetimi ve tehdit tespiti süreçlerini sürekli izleyerek güncel güvenlik zafiyetlerinin giderilmesine katkıda bulunur.

Elasticsearch MDR Hizmeti ve Ürün Yönetimi

Elasticsearch MDR Hizmeti, veri analitiği ve olay izleme çözümlerinin işletilmesini kapsar. MDR ekibimiz, Elasticsearch, Logstash ve Kibana gibi bileşenlerini kullanarak güvenlik olaylarını analiz eder. Hizmet, büyük miktarda veriyi anlamlı hale getirerek güvenlik zafiyetlerinin ve tehditlerin hızlıca tespit edilmesini sağlar. Elasticsearch'ün veri görselleştirme araçları, güvenlik ekiplerinin olayların kökenini anlamasına yardımcı olur. MDR ekibimiz, Elasticsearch çözümlerini organizasyonun güvenlik ihtiyaçlarına göre yapılandırır. Güvenlik olaylarına ilişkin detaylı analizler, tehditleri minimize etmek için düzenli raporlama sağlar.

Qualys MDR Hizmeti ve Ürün Yönetimi

Qualys MDR Hizmeti, güvenlik zafiyeti yönetimi ve uyumluluk süreçlerini destekler. MDR ekibimiz, Qualys'in güvenlik zafiyetlerini tarayan ve analiz eden çözümlerini kullanarak işletilmesini sağlar. Güvenlik zafiyetlerinin hızlıca tespit edilmesi ve giderilmesi için Qualys çözümleri, güvenlik ekiplerinin işini kolaylaştırır. Qualys'in sunduğu düzenli raporlar ve uyarılar, güvenlik operasyonlarının etkinliğini artırır. MDR hizmeti, güvenlik ve uyumluluk gereksinimlerini karşılayarak organizasyonların tehditlere karşı hazırlıklı olmasını sağlar.

Fortify MDR Hizmeti ve Ürün Yönetimi

Fortify MDR Hizmeti, uygulama güvenliği çözümlerini yöneterek işletilmesini sağlar. MDR ekibimiz, Fortify'ın güvenlik açıklarını analiz eden çözümlerini yapılandırarak yazılım geliştirme süreçlerinde güvenlik önlemleri alınmasını sağlar. Fortify, yazılım kaynak kodlarını tarayarak güvenlik zafiyetlerini kodlama seviyesinde eder ve giderilmesini sağlar. MDR hizmetimiz, yazılım geliştirme süreçlerinin güvenli bir şekilde ilerlemesini sağlar.

SentinelOne MDR Hizmeti ve Ürün Yönetimi

SentinelOne MDR Hizmeti, uç nokta güvenliği çözümlerini (EDR) yöneterek siber tehditlere karşı koruma sağlar. MDR ekibimiz, SentinelOne'ın gelişmiş tehdit algılama ve yanıt özelliklerini kullanarak güvenlik olaylarını analiz eder. SentinelOne, cihazları gerçek zamanlı olarak izleyerek tehditleri anında tespit eder. MDR ekibimiz, uç noktalarda tespit edilen tehditleri hızlıca izleyip analiz ederek müdahale süreçlerini başlatır.

Checkmarx MDR Hizmeti ve Ürün Yönetimi

Checkmarx MDR Hizmeti, kod güvenliği çözümlerini yöneterek yazılım geliştirme süreçlerinde güvenliği artırır. MDR ekibimiz, Checkmarx'ın kaynak kod analizi yaparak güvenlik zafiyetlerini tespit eden çözümünün işletilmesini sağlar. Kaynak kod güvenliği taramaları sayesinde olası riskler erkenden tespit edilir ve giderilir. Checkmarx, yazılım geliştiricilere güvenli kod yazmaları için de ayrıca rehberlik sunar. MDR hizmeti, yazılım altyapısının güvenliğini sağlamak için kod tarama süreçlerini düzenli hale getirir.

Thales MDR Hizmeti ve Ürün Yönetimi

Thales MDR Hizmeti, veri koruma ve şifreleme çözümlerini yöneterek hassas bilgilerin güvenliğini sağlar. MDR ekibimiz, Thales ürün ailesini kullanarak veri güvenliğini sağlama ve şifreleme süreçlerinin işletilmesini temin eder. Thales, hassas verileri şifreleyerek yetkisiz erişimleri önler ve veri ihlallerine karşı koruma sağlar.

Swimlane MDR Hizmeti ve Ürün Yönetimi

Swimlane MDR Hizmeti, güvenlik orkestrasyonu ve otomasyon çözümlerini yöneterek güvenlik operasyonlarını hızlandırır. MDR ekibimiz, Swimlane çözümlerini işleterek otomatik müdahale süreçlerini devreye alır. Swimlane, güvenlik olaylarının otomatik olarak analiz edilmesini ve müdahale edilmesini sağlar. MDR ekibimiz, tekrarlanan tehditlere karşı otomatik yanıt süreçleri ile operasyonları hızlandırır. Hizmet, insan hatalarını minimize ederek güvenlik operasyonlarını daha verimli hale getirir.

Cobaltstrike MDR Hizmeti ve Ürün Yönetimi

Cobaltstrike MDR Hizmeti, penetrasyon testleri ve güvenlik değerlendirmelerini yöneterek organizasyonun güvenlik durumunu analiz eder. MDR ekibimiz, Cobaltstrike'ın düzenli penetrasyon testleri ile güvenlik zafiyetlerini erkenden belirler. Cobaltstrike çözümü, güvenlik ekiplerine güvenlik açıklarının kaynaklarını ve önceliklerini gösterir. MDR hizmeti, düzenli olarak testler yaparak organizasyonun küresel tehditlere karşı hazırlıklı kalmasını sağlar.

Sık Sorulan Sorular

MDR hizmeti nedir ve kurumlara nasıl fayda sağlar?

MDR (Managed Detection and Response), organizasyonların siber tehditleri tespit etme, izleme ve bunlara yanıt verme süreçlerini işletmeye yarayan bir yönetilebilir siber güvenlik hizmettir. MDR Hizmeti, gelişmiş siber güvenlik teknolojileri ve siber güvenlik konusunda uzmanlaşmış ekiplerin birleşimiyle, siber saldırılara karşı etkin bir savunma mekanizması oluşturur. MDR, organizasyonların güvenlik operasyonlarını sürekli işleterek, olası tehditleri anında tespit eder ve müdahale eder. Gerçekleştirilen çalışmalarla güvenlik zafiyetlerinin minimize edilmesi ve iş sürekliliğinin sağlanması hedeflenir. Ayrıca, MDR hizmeti, organizasyonların mevcut güvenlik altyapılarını değerlendirerek, gerekli iyileştirmeleri önererek işletilmesini sağlar. Süreç boyunca, organizasyonların ihtiyaçlarına özel siber güvenlik çözümleri sunulur ve güvenlik stratejileri sürekli güncellenir.

MDR hizmeti ile geleneksel güvenlik hizmetleri arasındaki farklar nelerdir?

Geleneksel güvenlik hizmetleri genellikle güvenlik duvarları, antivirüs yazılımları ve IDS/IPS gibi pasif savunma mekanizmalarına dayanır. Geleneksel yaklaşımlar, bilinen tehditlere karşı koruma sağlarken, gelişmiş ve yeni ortaya çıkan saldırı tekniklerine karşı yetersiz kalabilir. MDR hizmeti ise, sürekli izleme, tehdit istihbaratı ve hızlı olay müdahalesi gibi özelliklerle siber güvenlik savunmasını güçlendirir. Ayrıca MDR hizmeti, alanında uzman güvenlik analistlerimiz tarafından yönetilir ve organizasyonların güvenlik operasyonlarını 7/24 izleyerek, olağandışı aktiviteleri tespit eder ve müdahale eder. MDR hizmeti, geleneksel güvenlik yaklaşımlarının ötesine geçerek, dinamik ve sürekli gelişen tehdit ortamına uyum sağlar.

MDR hizmeti alırken nelere dikkat edilmelidir?

MDR hizmeti alırken, hizmet sağlayıcının deneyimi ve uzmanlığı öncelikli olarak değerlendirilmelidir. Hizmet sağlayıcının, organizasyonun sektörüne ve ihtiyaçlarına uygun çözümler sunabilme kapasitesi önemlidir. Ayrıca kullanılan teknolojilerin güncel ve gelişmiş olması, tehdit tespiti ve müdahale süreçlerinin etkinliği açısından kritik önem taşır. Hizmetin 7/24 izleme ve hızlı müdahale yetenekleri, siber saldırılara karşı etkin bir savunma için gereklidir. Raporlama ve şeffaflık, organizasyonun güvenlik durumu hakkında düzenli bilgi sahibi olmasını sağlar. Maliyet ve hizmet kapsamı dengesi de göz önünde bulundurulmalıdır.

MDR hizmeti hangi sektörler için uygundur?

MDR hizmeti finans, sağlık, enerji, üretim, perakende ve kamu gibi siber güvenlik tehditlerine maruz kalan tüm sektörler için uygundur. Özellikle hassas verilerin işlendiği ve saklandığı sektörlerde, MDR hizmeti kritik bir öneme sahiptir. Finans sektöründe, müşteri bilgileri ve finansal verilerin korunması için MDR hizmeti kullanılır. Sağlık sektöründe, hasta bilgileri ve tıbbi verilerin güvenliği için MDR hizmeti tercih

edilir. Enerji sektöründe altyapı güvenliği ve operasyonel süreklilik için MDR hizmeti önemlidir.

MDR hizmetinin maliyeti nedir ve bütçelendirme nasıl yapılmalıdır?

MDR hizmetinin maliyeti, organizasyonun büyüklüğü, ihtiyaçları, hizmet kapsamı ve seçilen teknolojilere göre değişiklik gösterir. Genellikle hizmetin kapsamı genişledikçe maliyet de artabilir. Bütçelendirme yaparken organizasyonun mevcut güvenlik durumu, risk profili ve korunması gereken varlıkların değeri göz önünde bulundurulmalıdır. Ayrıca MDR hizmetinin sağlayacağı faydalar ve olası siber saldırıların maliyetleri karşılaştırılmalıdır. Maliyetlerin yanı sıra, hizmetin kalitesi ve etkinliği de değerlendirilmelidir.

MDR hizmeti ile SOC (Security Operations Center) arasındaki farklar nelerdir?

SOC (Security Operations Center) organizasyonların siber güvenlik operasyonlarını yöneten ve izleyen birimdir. SOC, genellikle organizasyon bünyesinde kurulur ve iç ya da dış kaynaklarla yönetilir. MDR hizmeti ise, dış kaynaklı bir hizmet olup, güvenlik teknolojilerinin işletilmesini konu edinir. MDR, SOC'un fonksiyonlarını yerine getirirken, ek olarak tehdit istihbaratı, gelişmiş analiz yetenekleri ve otomatik yanıt süreçlerini de içerebilmektedir. MDR hizmeti, güvenlik olaylarına müdahale ve yanıt süreçlerinde dışarıdan destek sağlayarak operasyonel yükü azaltır. MDR hizmeti, organizasyonlara esnek ve dış kaynak destekli çözümler sunar. MDR'nin sağladığı otomatik müdahale ve tehdit izleme yetenekleri, SOC işlevlerini güçlendirir. MDR, SOC yapısını destekleyici ve tamamlayıcı bir çözüm olarak da düşünülebilir.

MDR hizmeti hangi güvenlik tehditlerine karşı koruma sağlar?

MDR hizmeti, zararlı yazılımlar, arka kapılar, fidye yazılımları, kimlik avı saldırıları, gelişmiş kalıcı tehditler (APT), DDoS saldırıları ve veri ihlalleri gibi çeşitli tehditlere karşı koruma sağlar. Güvenlik teknolojilerini 7/24 izleyerek, şüpheli aktiviteleri ve olağandışı davranışları erkenden tespit eder. MDR hizmeti, tehditlerin kaynağını ve etki alanını belirleyerek anında müdahale sürecini başlatır. Tehdit istihbaratı sayesinde, organizasyonun karşılaşabileceği en güncel tehdit türlerine yönelik önlemler alınır. Otomatik yanıt süreçleri ile zararlı aktiviteler hızlıca etkisiz hale getirilir. MDR hizmeti hem iç hem de dış tehditlere karşı organizasyonun güvenlik altyapısını güçlendirir.

Siber Güvenlikte Doğru Çözüm Ortağınız

2018 yılında siber güvenliğin geleceği için yola çıkan Privia Security, kuruluşundan bu yana, müşterilerine yüksek kaliteli hizmet sunmayı amaçlamaktadır. Güçlü ve yetenekli ekibimiz, siber güvenliğin her alanında hizmet verdiğimiz organizasyonlara en güvenilir ve kapsamlı çözümleri sunarak, organizasyonların dijital dünyadaki güvenlik ihtiyaçlarını karşılamaktadır.

Günümüzde hızla gelişen ve karmaşık hale gelen siber tehditlerle mücadele etmek giderek zorlaşıyor. Bu noktada Privia Security olarak, müşterilerimize ihtiyaç duydukları hem defansif hem de ofansif siber güvenlik stratejilerini en ileri teknolojiyle sunuyoruz. İnovatif AR-GE ürünlerimiz ve stratejik danışmanlığımız sayesinde organizasyonların siber güvenlik olgunluğunu artırmayı ve onlara proaktif çözümler sunmayı hedefliyoruz. Şu anda 300'den fazla büyük kuruluşun güvenliğini sağlamaktan gurur duyuyoruz.

Uluslararası ve Yerel Siber Güvenlik Çözümleri

Privia Security olarak, Avrupa, Asya, Ortadoğu ve Amerika dahil olmak üzere geniş bir coğrafyaya siber güvenlik hizmetleri sunmaktayız. Offensive, Defensive ve Forensic alanlarında uzmanlaşmış ekiplerimiz, kritik altyapılar, aviyonik sistemler, kurumsal ağlar ve askeri alanlar gibi farklı sektörlerde faaliyet gösteren organizasyonlara özel çözümler geliştirmektedir.

Ayrıca savunma kapasitelerini güçlendirmek isteyen ülkelere yönelik geliştirdiğimiz PriviaHub siber savaş simülasyonu ile siber savaş stratejilerinin test edilmesi, tatbikatların yürütülmesi ve uzmanların niteliklerinin ölçülmesi için kapsamlı çözümler sunuyoruz. Bu inovatif platform özel sektör, akademi ve askeri alanlarda tatbikat ihtiyaçlarını karşılamak üzere tasarlanmıştır.

İleri Teknoloji ile Güvenli Gelecek

İstanbul, Ankara, Londra ve Cumhuriyet Teknopark'taki Ar-Ge merkezimizde, müşterilerimize değer katan projeler geliştiriyoruz. Penetrasyon testleri, Red Team operasyonları, siber güvenlik eğitimleri ve kurumlara özel siber güvenlik çözümlerimizle sektörde fark yaratmaya devam ediyoruz. "Privacy For You" sloganımızla, güvenlik ve gizliliğe yenilikçi bir bakış açısı getiriyor ve müşterilerimizin dijital geleceğini güvence altına alıyoruz.

Privia
SECURITY