Rekabet Kurumu Başkanlığından,

REKABET KURULU KARARI

Dosya Sayısı : 2025-1-085 **(Devralma)**
Karar Sayısı : **26-03/92-38**
Karar Tarihi : 29.01.2026

A. TOPLANTIYA KATILAN ÜYELER

Başkan : Birol KÜLE
Üyeler : Ahmet ALGAN (İkinci Başkan), Şükran KODALAK, Hasan Hüseyin ÜNLÜ, Ayşe ERGEZEN, Rıdvan DURAN

B. RAPORTÖRLER : Betül AYHAN DEMİRALAY, Kübra Nur KABAR, Zehra Seda KAYNAR

C. BİLDİRİMDE BULUNAN : - Palo Alto Networks, Inc.
Temsilcileri: Av. Dr. Gönenç GÜRKAYNAK, Ebru İNCE, Av. Evgeniya DEVECİ, Petek GÜVEN, Av. Çağla SARIBAY
Yıldız Mahallesi, Çitlenbik Sokak, No:12, Beşiktaş/İstanbul

(1) **D. DOSYA KONUSU: CyberArk Software Ltd.nin tüm hisselerinin ve tek kontrolünün Palo Alto Networks, Inc. tarafından devralınması işlemi.**

(2) **E. DOSYA EVRELERİ:** Rekabet Kurumu (Kurum) kayıtlarına 05.12.2025 tarih ve 77581 sayı ile giren ve eksiklikleri en son 15.01.2026 tarihli ve 79315 sayılı yazı ile tamamlanan bildirim üzerine düzenlenen 28.01.2026 tarihli ve 2025-1-085/Öİ sayılı Devralma Ön İnceleme Raporu görüşülerek karara bağlanmıştır.

(3) **F. RAPORTÖR GÖRÜŞÜ:** İlgili raporda, bildirime konu işleme izin verilmesinde sakınca bulunmadığı ifade edilmiştir.

G. İNCELEME VE DEĞERLENDİRME

G.1. Hissedarlık Yapısı ve İlgili Pazar

(4) Başvuruda; CyberArk Software Ltd.nin (CYBERARK) tüm hisselerinin ve tek kontrolünün Palo Alto Networks, Inc. (PALO ALTO) tarafından devralınması işlemine 4054 sayılı Rekabetin Korunması Hakkında Kanun (4054 sayılı Kanun) ve 2010/4 sayılı Rekabet Kurulundan İzin Alınması Gereken Birleşme ve Devralmalar Hakkında Tebliğ (2010/4 sayılı Tebliğ) çerçevesinde izin verilmesi talep edilmektedir.

(5) İşlemin temelini, taraflar arasında 30.07.2025 tarihinde akdedilen Birleşme Sözleşmesi (SÖZLEŞME) oluşturmaktadır.Aşağıda Tablo 1'de CYBERARK'ın işlem öncesi ve sonrası hissedarlık yapısına yer verilmektedir:

Tablo 1: CYBERARK'ın İşlem Öncesi ve İşlem Sonrası Hissedarlık Yapısı

İşlem Öncesi Hissedarlık Yapısı		İşlem Sonrası Hissedarlık Yapısı	
Hissedarlar	Hisse Oranı (%)	Hissedarlar	Hisse Oranı (%)
(.....)	(.....)	PALO ALTO	(.....)
(.....)[1]	(.....)		
Toplam	100,0	Toplam	100,0
Kaynak: Bildirim Formu			

[1] Bildirim Formu'nda CYBERARK'ın hisselerinin geniş çapta dağılmış olduğu ve "Diğer" olarak ifade edilen hissedarlar arasında (.....) paya sahip olan herhangi bir hissedar bulunmadığı belirtilmektedir.

(6) Devralan ilgili teşebbüs PALO ALTO, merkezi Kaliforniya'da bulunan çok uluslu bir siber güvenlik şirketidir. Teşebbüs, kurumsal siber güvenlik ürünleri ile bu ürünlere ilişkin hizmetlerin geliştirilmesi ve sunulmasına odaklanmaktadır. PALO ALTO'nun sunduğu platform ve hizmetler, yapay zekâ ve otomasyon destekli çözümler aracılığıyla kurumların ağlarını, bulut ortamlarını ve uç noktalarını korumaya yardımcı olmaktadır. Bu kapsamda teşebbüs; (i) ağ güvenliği, (ii) bulut güvenliği, (iii) güvenlik faaliyetleri ve (iv) tehdit istihbaratı olmak üzere dört ana alanda faaliyet göstermektedir. Herhangi bir gerçek kişi veya tüzel kişi tarafından kontrol edilmeyen PALO ALTO'nun sunduğu hizmetlerin detaylarına aşağıda yer verilmektedir:

- Ağ Güvenliği: Makine öğrenimi destekli yeni nesil donanım ve yazılım tabanlı güvenlik duvarları ile bulut üzerinden sunulan güvenli erişim hizmet kenarı (*Secure Access Service Edge*, SASE), güvenlik hizmetleri kenarı (*Security Services Edge*, SSE), SD-WAN[2], güvenli kurumsal tarayıcı ve yapay zekâ tabanlı güvenlik çözümleri dâhil olmak üzere çeşitli bulut tabanlı ağ güvenliği ürünleri, araçları ve hizmetlerini kapsamaktadır. PALO ALTO, güvenli kurumsal tarayıcı (GKT) (*Secure Enterprise Browser*) hizmetleri[3] kapsamında *Prisma Access Browser* adlı bir ürün sunmaktadır. Kötü amaçlı yazılımlara karşı koruma sağlayan *Prisma Access Browser*, bağımsız şekilde sunulabilen bir ürün olmakla birlikte esas olarak *Prisma Secure Access Service Edge* (*Prisma SASE*) kullanan müşteriler tarafından tercih edilmektedir.
- Bulut Güvenliği: Sanal güvenlik duvarları ile uygulamaların geliştirme yaşam döngüsü boyunca; uygulamaların, verilerin ve bulut tabanlı teknoloji altyapısının çoklu ve hibrit bulut ortamlarında güvenliğini sağlamaya yönelik bulut yerel uygulama koruma platformu (*cloud native application protection platform,* CNAPP) sağlamaktadır[4].
- Güvenlik Faaliyetleri: Güvenlik bilgileri ve olay yönetimi araçları, uç nokta güvenliği, güvenlik otomasyonu, saldırı yüzeyi yönetimi ve bunlarla ilişkili diğer güvenlik çözümlerini kapsayan ürünleri içermektedir[5].
- Tehdit İstihbaratı ve Danışmanlık: Müşterilerin siber risklere karşı hazırlıklı olmalarını, bu riskleri etkin şekilde yönetmelerini ve siber saldırılara hızlı biçimde yanıt vermelerini sağlamak amacıyla; olay müdahalesi, tespit ve müdahale, tehdit avcılığı ve uzman güvenlik araştırmacıları tarafından desteklenen siber güvenlik danışmanlığı hizmetlerini kapsayan tehdit istihbaratı ve danışmanlık hizmetleri sunulmaktadır[6].

---

[2] SD-WAN**,** kurumsal ağ trafiğinin yazılım aracılığıyla yönetilmesini ve güvenli şekilde yönlendirilmesini sağlayan, bulut tabanlı ağ güvenliği çözümlerinin bir parçası olan bir teknolojiyi ifade etmektedir. Bkz. https://www.hpe.com/us/en/what-is/sd-wan.html, Erişim Tarihi: 22.12.2025.

[3] GKT ürünleri kullanıcılara ya kurumsal olarak yönetilen bir internet tarayıcısı şeklinde ya da üçüncü taraf bir tarayıcıya entegre edilen ve onun tarafından çalıştırılan bir tarayıcı uzantısı olarak sunulmaktadır. Farklı tedarikçilerin GKT çözümlerinin sunduğu işlevler değişiklik gösterse de GKT'ler genel olarak entegre güvenlik, politika ve kontrol yönetimi, görünürlük, raporlama ve diğer ilgili işlevleri sunmaktadır. GKT ürünlerinin entegre güvenlik özellikleri, örneğin kötü amaçlı internet içeriklerine karşı ve kurumsal verilerin kötüye kullanılması veya kaybına karşı koruma sağlarken, tarayıcı kullanımını da kaydetmektedir. GKT ürünleri aynı zamanda kimlik güvenliği yazılımları ile de entegrasyon sağlamaktadır.

[4] PALO ALTO, Bulut Güvenliği hizmetlerini Cortex Cloud markası ile sunmaktadır. Bkz. https://www.paloaltonetworks.com/cortex/cloud, Erişim Tarihi: 22.12.2025.

[5] PALO ALTO, Güvenlik Faaliyetleri kapsamındaki hizmetlerini Cortex markası ile sunmaktadır. Bkz. https://www.paloaltonetworks.com/cortex, Erişim Tarihi: 22.12.2025.

[6] PALO ALTO, Tehdit İstihbaratı ve Danışmanlık kapsamındaki hizmetlerini Unit 42 markası ile sunmaktadır. Bkz. https://www.paloaltonetworks.com/unit42, Erişim Tarihi: 22.12.2025.

(7) PALO ALTO söz konusu faaliyetleri kapsamında; Cortex XDR, Cloud Delivered Security Services (CDSS), Cortex XSIAM, Cortex Cloud, Cortex XSOAR, Cortex Xpance ve Strata Logging Service adlı ürün ve hizmetlerini sunmaktadır.Şirket satış faaliyetlerini; doğrudan satış ekibinin yanı sıra yeniden satıcılar, küresel ve bölgesel sistem entegratörleri, hizmet sağlayıcılar, yönetilen güvenlik hizmeti sağlayıcıları ve bulut barındırma hizmeti sağlayıcılarından oluşan kanal ortakları aracılığıyla yürütmektedir. PALO ALTO'nun Türkiye'de, İstanbul ve Ankara'da faaliyet gösteren Palo Alto Networks Turkey Siber Güvenlik Destek Hizmetleri Limited Şirketi (PALO TÜRKİYE) adlı bir iştiraki bulunmaktadır. PALO TÜRKİYE, PALO ALTO'nun küresel ölçekte sunduğu siber güvenlik ürünleri ve hizmetlerinin Türkiye'deki satış ve pazarlama faaliyetlerini desteklemektedir.

(8) Devre konu teşebbüs CYBERARK, hem İsrail hem de ABD'de merkezi olan çok uluslu bir şirket olarak faaliyet göstermektedir. CYBERARK kurumsal güvenlik yazılımları ve hizmetlerinin geliştirilmesi ve ticarileştirilmesi alanının "kimlik güvenliği" alt kategorisinde hizmet sunmaktadır. CYBERARK'ın sunduğu üç ana hizmet grubunun detaylarına aşağıda yer verilmektedir:

- Ayrıcalıklı Erişim Yönetimi (*Privileged Access Management*, PAM): Bir kuruluşun bilgi teknolojileri (BT) yöneticileri ya da dış BT hizmet sağlayıcıları tarafından kullanılan ayrıcalıklı hesaplara ve sistem kaynaklarına erişim; şifre rotasyonu, şifre kasası ve oturum gözetimi gibi teknikler aracılığıyla kontrol ve izleme altına alınmaktadır. Bu kapsamda söz konusu çözümler, ayrıcalıklı kullanıcıların BT sistemlerine erişim süreçlerini ve erişim sonrasında gerçekleştirilen işlemleri izlemek suretiyle, olağan kullanıcıların ayrıcalıklı erişim elde etmesini önlemeyi ve ayrıcalıklı erişimlerden kaynaklanan güvenlik risklerini asgariye indirmeyi amaçlamaktadır. CYBERARK ilgili hizmeti kapsamında; ayrıcalıklı erişim yöneticisi, uç nokta ayrıcalıklı erişim yöneticisi, tedarikçi ayrıcalıklı erişim yöneticisi, güvenli bulut erişimi, güvenli altyapı erişimi ve gizli bilgi yönetimi adlı ürünler sunmaktadır.
- Kimlik ve Erişim Yönetimi: Bir kuruluşun çalışanlar ve yükleniciler gibi iç kullanıcılarının ya da müşteriler ve iş ortakları gibi dış kullanıcılarının kimliklerinin güçlü biçimde doğrulanması yoluyla kurumsal veri ve uygulamalara kontrollü erişimini sağlamak için kullanılmaktadır. CYBERARK ilgili hizmeti kapsamında; doğrulama & yetkilendirme, dizin ve kullanıcı yönetimi, tek oturum açma, uyarlanabilir çok faktörlü kimlik doğrulama, uç nokta kimlik doğrulama, uygulama geçidi, kullanıcı davranışı analitiği, güvenli internet oturumları, çalışan parola yönetimi ve güvenli tarayıcı adlı ürünler sunmaktadır.
- Kimlik Yönetimi ve İdaresi: Kimlik yaşam döngüsü yönetimini otomatikleştirmekte, aşırı güvenlik izinlerinin verilmesini en aza indirgemekte ve güvenlik politikalarına uyumun izlenmesini sağlamaktadır. CYBERARK ilgili hizmeti kapsamında; kimlik uyumu, yaşam döngüsü yönetimi, kullanıcı erişim inceleme uyumu, yetkilendirme ve kimlik akışları adlı ürünler sunmaktadır.

(9) CYBERARK mevcut hizmetlerine ek olarak, makineden makineye bağlantı ve iletişimlerin güvenliğini sağlamak amacıyla makine kimliği yönetimi çözümleri de sunmaktadır[7]. Bu kapsamda özellikle; taşıma katmanı güvenliği (*Transport Layer*

[7] CYBERARK'ın ilgili ürün portföyünde, sertifikaların oluşturulması, yenilenmesi ve sona erdirilmesini kapsayan sertifika yaşam döngüsü yönetimi için kullanılan *CyberArk Certificate Manager* yer almaktadır. Buna ek olarak; SSH anahtarlarının yönetimi için *CyberArk SSH Manager*, kod imzalama sertifikaları için *CyberArk Codesign Manager* ve geleneksel PKI altyapılarının bulut tabanlı, güvenli ve kolay yönetilebilir bir yapıyla değiştirilmesini sağlayan CyberArk Zero Touch PKI sunulmaktadır.

Security, TLS), güvenli soket katmanı *(Secure Sockets Layer*, SSL) ve güvenli kabuk (*Secure Shell*, SSH) anahtarları ile kod imzalama sertifikaları başta olmak üzere bulut ortamları, mobil uygulamalar ve nesnelerin interneti uygulamalarında kullanılan kriptografik anahtarlar ve dijital sertifikaların yönetimini sağlanmaktadır. Ayrıca teşebbüs yetkililerince güvenli kurumsal tarayıcı hizmetleri kapsamında da bir ürün sunulduğu, ancak CYBERARK'ın müşteri talebinin yetersizliği nedeni ile GKT ürününü bağımsız olarak sunmadığı ve herhangi bir gelir elde edilmediği belirtilmektedir.

(10) Bunun yanı sıra CYBERARK'ın, ticari ürünlerinin bazı fonksiyonel unsurlarını bünyesinde barındıran ancak yaygın olarak kullanılmayan iki açık kaynaklı çözüm olan *Conjur*[8] ve *Fuzzy AI*[9] ürünleri bulunmaktadır. İlaveten teşebbüs sunduğu ürünler ile ilgili olarak danışmanlık hizmetleri, eğitim, uygulama hizmetleri ve *red team* hizmetleri (bir kuruluşun sistem ve ağlarına siber saldırıları simüle ederek güvenlik durumlarını değerlendirmek ve güvenlik açıklarını belirlemek) gibi bazı hizmetler de sunmaktadır. Anılan hizmetler, CYBERARK'ın sunduğu temel ürünleri destekleyici ve tamamlayıcı niteliktedir.

(11) CYBERARK, Türkiye'de ürün ve hizmetlerini nihai müşterilere, yalnızca yeniden satıcılar ve distribütörler aracılığıyla tedarik etmektedir. (.....) 2010/4 sayılı Tebliğ uyarınca, bildirim konusu işlemden etkilenme ihtimali olan ve taraflardan iki veya daha fazlasının aynı ürün pazarında faaliyette bulunduğu ya da taraflardan en az bir tanesinin bir diğerinin faaliyet gösterdiği herhangi bir ürün pazarının alt veya üst pazarında ticari faaliyette bulunduğu ilgili ürün pazarları etkilenen pazarları oluşturmaktadır.

(12) Yukarıda yer verildiği üzere, devre konu teşebbüs konumunda olan CYBERARK kurumsal güvenlik yazılımları alanında kimlik güvenliği odaklı çözümler sunmaktadır. Teşebbüs, PAM, kimlik ve erişim yönetimi ile kimlik yönetimi ve idaresi olmak üzere temelde üç ana ürün ve hizmet grubu ile faaliyetlerini yürütmektedir. Bu faaliyetlerine ek olarak CYBERARK; makine kimliği yönetimi, kriptografik anahtar ve dijital sertifika yönetimi alanlarında sunduğu çözümlerle makineden makineye iletişimlerin güvenliğini sağlamakta, güvenli kurumsal tarayıcı hizmetleri sunmakta ve danışmanlık, eğitim ile uygulama hizmetleriyle ürünlerini destekleyici nitelikte faaliyet göstermektedir. Bununla birlikte CYBERARK'ın 2024 yılına ilişkin cirosunun büyük çoğunluğunu oluşturan PAM'ın, CYBERARK'ın temel ürünü olduğu taraflarca beyan edilmektedir.

(13) Devralan konumundaki PALO ALTO ise ağ güvenliği, bulut güvenliği, güvenlik faaliyetleri ve tehdit istihbaratı alanlarını kapsayan geniş bir ürün ve hizmet portföyü aracılığıyla kurumsal siber güvenlik çözümlerinin geliştirilmesi ve sunulması faaliyetlerini yürütmektedir.

(14) Bu kapsamda her ne kadar devralan PALO ALTO ile devre konu varlık CYBERARK'ın faaliyet gösterdikleri ürün ve hizmetlerin birebir aynı kurumsal güvenlik yazılımı ürünleri olmadığı görülse de geniş anlamda her iki teşebbüsün de *kurumsal güvenlik yazılımı* alanında faaliyet gösterdiği değerlendirilmektedir.

(15) *Kurumsal güvenlik yazılım pazarı*, kurumlara siber güvenlik çözümleri sunmak adına geliştirilen özelleştirilmiş bir alan olup bünyesinde farklı işlevler sunan birçok çözüm ve araç barındırmaktadır. Söz konusu yazılım, kurumlarda güvenlik risklerini azaltmak,

---

[8] *Conjur*, yüksek hızda ve geniş ölçekte çalışan bilgi teknolojileri ortamlarında gizli bilgilerin güvenli şekilde saklanması ve güvenli biçimde erişilmesi için kullanılan bir çözümdür.

[9] *Fuzzy AI*, şirketlerin yapay zekâ modeli güvenlik açıklarını tespit etmesine ve bunları gidermesine yardımcı olmaktadır.

siber tehdit ve saldırıları tespit etmek ve önlemek, bilgi teknolojileri altyapısında ortaya çıkabilecek güvenlik olaylarına müdahale etmek için kullanılmaktadır. Bilgi teknolojileri alanında bağımsız bir araştırma şirketi olan Gartner, Inc.'in (GARTNER) 2024 yılı raporuna göre, kurumsal güvenlik yazılımları; (i) erişim yönetimi, (ii) uygulama güvenliği testi, (iii) bulut erişim güvenlik aracısı, (iv) bulut güvenliği duruşu yönetimi, (v) bulut iş yükü koruma platformları, (vi) uç nokta koruma platformları (kurumsal), (vii) kurumsal veri kaybı önleme ürünleri, (viii) kimlik yönetimi ve idaresi, (ix) güvenli e-posta ağ geçidi, (x) güvenli internet ağ geçidi, (xi) güvenlik bilgileri ve olay yönetimi ve (xii) diğer güvenlik yazılımları şeklinde on iki alt kategori altında sınıflandırılmaktadır.

(16) Taraflarca, kurumsal güvenlik yazılımlarının sundukları işlevsellik türlerine göre belirli alt segmentlere ayrılabildiği, bununla birlikte, siber güvenlik alanının dinamik yapısı ve daha önce ayrı şekilde sunulan çeşitli güvenlik işlevlerini içeren daha geniş kapsamlı tekliflere yönelik genel eğilim nedeniyle bu alt kategoriler arasındaki sınırların çoğu zaman belirsiz olduğu ifade edilmektedir.

(17) Avrupa Komisyonunun (Komisyon) *Broadcom/Symantec Enterprise Security Business* kararında[10] kurumsal güvenlik yazılımı *"Kuruluşların verilerine ve bilgi teknolojisi sistemleri yetkisiz erişim riskini azaltmayı amaçlamaktadır. Güvenlik yönetimi, erişim kontrolü, kimlik doğrulama, şifreleme, veri kaybı önleme, saldırı tespiti ve çevresel savunma gibi unsurlar aracılığıyla kurumsal ağ altyapılarının güvenliğini artırmak üzere tasarlanmıştır."* şeklinde tanımlanmıştır[11]. GARTNER segmentlerinden bahsedilmiş[12] ve bu segmentlerin mümkün olan en dar ilgili ürün pazarı tanımını oluşturduğu kabul edilmiştir[13]. Komisyonun *Cisco/Splunk[14]* kararında ilgili pazarın GARTNER segmentlerine göre daha dar tanımlanabileceği tartışılmış ancak bilişim teknolojileri operasyonları analitiği yazılımlarına ilişkin kesin ürün pazarı tanımının açık bırakılabileceği belirtilmiş ve kesin bir pazar tanımı yapılmamıştır[15].

(18) Bu çerçevede mevcut dosya kapsamında tarafların geniş anlamda kurumsal güvenlik yazılımı pazarında faaliyet gösterdiği, bununla birlikte tarafların sundukları ürünlere göre kurumsal güvenlik yazılımı pazarının alt kırımları bakımından ilgili ürün pazarları tanımlanabilecektir.

(19) Ancak İlgili Pazarın Tanımlanmasına İlişkin Kılavuz'un 20. paragrafında inceleme konusu işlemin olası alternatif pazar tanımları çerçevesinde rekabet açısından endişeler yaratmıyor olması halinde pazar tanımı yapılmayabileceği ifade edilmiştir. Bu doğrultuda, ilgili ürün pazarının net bir şekilde belirlenmesi mevcut dosya bakımından ulaşılacak neticeyi değiştirmeyeceğinden işbu dosya kapsamında *kurumsal güvenlik yazılımı* veya alt kırılımlarına dair kesin bir ilgili ürün pazar tanımı yapılmasına gerek olmadığı değerlendirilmektedir.

(20) İlgili coğrafi pazar belirlenirken, ilgili mal ve hizmetlerin özellikleri ile tüketici tercihleri bakımından giriş engellerinin, ilgili bölge ile komşu bölgeler arasında teşebbüslerin pazar payları veya mal ve hizmetlerin fiyatları bakımından hissedilir bir farklılığın olup olmadığı gibi unsurlar dikkate alınmaktadır.

(21) İlgili coğrafi pazar, rekabet koşullarının homojen olduğu bölge olarak ifade edilebilmektedir. Bu pazarların belirlenmesinde ürün ve faaliyetlerin bölgelere göre

[10] Komisyonun 30.10.2019 tarihli ve M.9538 sayılı kararı.
[11] A.g.k. para. 17.
[12] A.g.k. para. 18.
[13] A.g.k. para. 25.
[14] Komisyonun 13.032024 tarihli ve M.11320 sayılı kararı.
[15] A.g.k. para. 38.

farklılıkları dikkate alınmaktadır. Başvuru konusu devir işlemi kapsamında tarafların Türkiye'deki faaliyetlerinin yalnızca bir bölge ile sınırlı olmaması, ilgili ürünlerin dağıtımı, pazarlanması, fiyatlandırılması ve tüketicilere sunulması tüm ülke çapında genel olarak benzer nitelik arz ettiği hususları göz önünde bulundurularak ilgili coğrafi pazar "Türkiye" olarak belirlenmiştir.

G.2. PALO ALTO ve CYBERARK Müşterilerinin Bildirim Konusu İşleme Yönelik Görüşleri

(22) Bildirim konusu işleme ilişkin olarak bilgi talep edilen teşebbüslerin görüşlerine aşağıda yer verilmektedir:

- (.....) tarafından; söz konusu işlemin teşebbüs açısından olumlu ya da olumsuz bir etki yaratmasının beklenmediği,
- (.....) tarafından; işlem taraflarının işlem neticesinde iş modeline yönelik bir strateji değişikliği gerçekleştirmemesi halinde, şirket ürün ve hizmet alımlarını ihale yönetimi ile gerçekleştirdiğinden, söz konusu ürünler bakımından ihale şartlarını karşılayan, teknik yeterliliğe sahip ve şirket sistemleri ile entegre olabilen teşebbüslerden ürün alımı gerçekleştirebileceği, dolayısıyla işlemin şirketin faaliyetleri üzerinde olası etkilerine ilişkin şu aşamada herhangi bir değerlendirme yapılamadığı ve bunun neticesinde bir görüş sunulmadığı,
- (.....) tarafından; işlemin gerçekleşmesi durumunda PALO ALTO ürünleri ile CYBERARK ürünleri arasındaki entegrasyon miktarının artacağı ve söz konusu entegrasyonun, ürünlerin diğer üçüncü parti yazılımlarla entegrasyon imkanlarını kısıtlamadığı sürece verimlilik artışı sağlayacağı,
- (.....) tarafından; söz konusu işlem ile birlikte tek üreticiye bağımlılığın artmasının, tedarikçi çeşitliliğinin azalması nedeniyle maliyetler ve sözleşmesel/ticari koşullar üzerinde dolaylı etkiler yaratabileceği, ancak mevcut aşamada bu etkilerin net olarak öngörülmediği,
- (.....) tarafından; söz konusu işlemin teşebbüs üzerinde herhangi bir olumsuz etkisinin beklenmediği,
- (.....) tarafından; bildirime konu işlemin gerçekleşmesi halinde teşebbüs nezdinde; lisans modelinin ve fiyatlarının değişmesi, firmanın kendi tesislerindeki altyapı desteğini sürdürmemesi ve bu sebeple bulut bazlı kullanım sunması gibi olası endişelerin oluşabileceği

hususları ifade edilmiştir.

G.3. İşlemin Niteliği ve Bildirim Yükümlülüğü Açısından Değerlendirme

(23) 4054 sayılı Kanun'un 7. maddesi; *"Bir ya da birden fazla teşebbüsün başta hâkim durum yaratılması ya da mevcut bir hâkim durumun güçlendirilmesi olmak üzere ülkenin bütünü yahut bir kısmında herhangi bir mal veya hizmet piyasasındaki etkin rekabetin önemli ölçüde azaltılması sonucunu doğuracak şekilde birleşmeleri veya herhangi bir teşebbüsün ya da kişinin diğer bir teşebbüsün mal varlığını yahut ortaklık paylarının tümünü veya bir kısmını ya da kendisine yönetimde hak sahibi olma yetkisi veren araçları, miras yoluyla iktisap durumu hariç olmak üzere, devralması hukuka aykırı ve yasaktır."* hükmünü haizdir.

(24) Öte yandan, 2010/4 sayılı Tebliğ'in 5. maddesinin birinci fıkrasında, *"Kontrolde kalıcı değişiklik meydana getirecek şekilde; …bir veya daha fazla teşebbüsün tamamının ya da bir kısmının doğrudan veya dolaylı kontrolünün, hisse ya da mal varlığının satın alınmasıyla, sözleşmeyle veya diğer bir yolla bir ya da daha fazla teşebbüs veya hâlihazırda en az bir teşebbüsü kontrol eden bir ya da daha fazla kişi tarafından*

devralınması, Kanunun 7. maddesi kapsamında birleşme veya devralma işlemi sayılır." ifadelerine yer verilmektedir.

(25) Bildirime konu işlem öncesinde CYBERARK, herhangi bir kişi veya teşebbüs tarafından kontrol edilmemektedir. Taraflar arasında akdedilen SÖZLEŞME kapsamında CYBERARK, PALO ALTO tarafından kurulan Athens Strategies Ltd.[16] (ATHENS) ile birleşecektir. Birleşmenin tamamlanmasının ardından ATHENS ayrı bir tüzel kişilik olarak varlığını sona erdirecek; CYBERARK ise varlığını sürdürmeye devam edecektir. Bu noktada ilgili işlemin devralmadan ziyade birleşme niteliğinde olduğu akla gelmekle birlikte, Kurulun geçmiş kararlarında hedef teşebbüsün, devralan teşebbüsün bir iştiraki ile ana teşebbüsün hedef teşebbüsü kontrol edebileceği biçimde birleşmesi ters üçgen veya ters üçlü birleşme (*reverse triangular merger*) olarak adlandırılmakta ve esasında bir devralma işlemi meydana getireceği kabul edilmektedir[17].

(26) Hâlihazırda hiçbir gerçek ya da tüzel kişi teşebbüs tarafından kontrol edilmeyen CYBERARK'ın hisselerinin tamamı ve tek kontrolü işlem sonrasında PALO ALTO tarafından devralınacaktır. Bu doğrultuda, bildirime konu işlem neticesinde CYBERARK'ın tek kontrolünün nihai olarak PALO ALTO'ya geçeceği anlaşılmaktadır.

(27) Bu çerçevede, başvuru konusu işlem ile PALO ALTO, CYBERARK üzerinde tek kontrole sahip olacak ve devre konu teşebbüsün kontrolünde kalıcı bir değişiklik meydana gelecektir. Bu çerçevede, ilgili işlemin 4054 sayılı Kanun'un 7. maddesi ve 2010/4 sayılı Tebliğ'in 5. maddesi kapsamında bir devralma işlemi niteliği taşıdığı sonucuna ulaşılmıştır.

G.4. İşleme İlişkin Bildirim Yükümlülüğü Açısından Yapılan Değerlendirme

(28) 2010/4 sayılı Tebliğ'in 7. maddesinin birinci fıkrası, "*Bu Tebliğin 5 inci maddesinde belirtilen bir birleşme veya devralma işleminde; a) İşlem taraflarının Türkiye ciroları toplamının yedi yüz elli milyon TL'yi ve işlem taraflarından en az ikisinin Türkiye cirolarının ayrı ayrı iki yüz elli milyon TL'yi veya b) Devralma işlemlerinde devre konu varlık ya da faaliyetin, birleşme işlemlerinde ise işlem taraflarından en az birinin Türkiye cirosunun iki yüz elli milyon TL'yi ve diğer işlem taraflarından en az birinin dünya cirosunun üç milyar TL'yi aşması halinde söz konusu işlemin hukuki geçerlilik kazanabilmesi için Kuruldan izin alınması zorunludur.*" düzenlemesini ihtiva etmekte olup hangi tür birleşme ya da devralma işlemlerinin Kurulun iznine tabi olduğunu belirlemektedir. Tarafların ciroları bu kapsamda değerlendirildiğinde; işlem taraflarının Türkiye ciroları toplamının yedi yüz elli milyon TL'yi ve ikisinin Türkiye cirolarının ayrı ayrı iki yüz elli milyon TL'yi aştığı, ayrıca, devre konu teşebbüsün Türkiye cirosunun iki yüz elli milyon TL'yi ve devralan teşebbüsün dünya cirosunun üç milyar TL'yi aştığı anlaşılmaktadır. Dolayısıyla bildirim konusu işlemin, 2010/4 sayılı Tebliğ'in 7. maddesinin birinci fıkrasının hem (a) hem de (b) bendi uyarınca Kurulun iznine tabi olduğu sonucuna ulaşılmıştır.

G.5. Yoğunlaşma Açısından Yapılan Değerlendirme

[16] Taraflarca ATHENS'in bildirim konusu işlemin gerçekleştirilmesi için kurulmuş özel amaçlı bir şirket olduğu belirtilmiştir. Bu çerçevede, anılan teşebbüsler Birleşme ve Devralmalarda İlgili Teşebbüs, Ciro ve Yan Sınırlamalar Hakkında Kılavuz'un 9. paragrafı uyarınca ilgili teşebbüs olarak değerlendirilmemiştir.

[17] Bkz. Kurulun 16.01.2025 tarihli ve 25-02/48-30 sayılı, 28.04.2023 tarihli ve 23-19/354-121 sayılı, 02.03.2023 tarihli ve 23-12/197-66 sayılı, 24.03.2022 tarihli ve 22-14/216-93 sayılı, 24.03.2022 tarihli ve 22-14/215-92 sayılı, 24.02.2022 tarihli ve 22-10/144-59 sayılı, 02.12.2021 tarihli ve 21-58/824-404 sayılı kararları.

(29) 4054 sayılı Kanun'un 7. maddesi *"bir ya da birden fazla teşebbüsün başta hâkim durum yaratılması ya da mevcut bir hâkim durumun güçlendirilmesi olmak üzere ülkenin bütünü yahut bir kısmında herhangi bir mal veya hizmet piyasasındaki etkin rekabetin önemli ölçüde azaltılması sonucunu doğuracak şekilde birleşmeleri veya herhangi bir teşebbüsün ya da kişinin diğer bir teşebbüsün mal varlığını yahut ortaklık paylarının tümünü veya bir kısmını ya da kendisine yönetimde hak sahibi olma yetkisi veren araçları, miras yoluyla iktisap durumu hariç olmak üzere, devralması hukuka aykırı ve yasaktır."* hükmünü amirdir. Hâkim durum kavramı ise 4054 sayılı Kanun'un 3. maddesinde, "*Belirli bir piyasadaki bir veya birden fazla teşebbüsün, rakipleri ve müşterilerinden bağımsız hareket ederek fiyat, arz, üretim ve dağıtım miktarı gibi ekonomik parametreleri belirleyebilme gücü*" olarak tanımlanmaktadır. Hâkim durumun; teşebbüslere fiyatları artırma ve üretim miktarı, ürün çeşitliliği ya da kalitesini azaltma imkânı verdiği ve hâkim durumdaki teşebbüslerin bu davranışlarının tüketici refahını azalttığı kabul edilmektedir.

(30) 4054 sayılı Kanun'un 7. maddesi uyarınca yapılacak bir değerlendirme, işlemden etkilenen pazarlar dikkate alınarak yapılmaktadır. 2010/4 sayılı Tebliğ uyarınca etkilenen pazarlar ise "*Türkiye'de, a) Taraflardan ikisinin veya daha fazlasının aynı ürün pazarında ticari faaliyette bulunduğu (yatay ilişki), b) Taraflardan en az bir tanesinin bir diğerinin faaliyet gösterdiği herhangi bir ilgili pazarın alt veya üst pazarında ticari faaliyette bulunduğu (dikey ilişki), tüm ilgili ürün pazarlarından ve ilgili coğrafi pazarlardan oluşmaktadır*." şeklinde tanımlanmaktadır. Bu noktada işlem taraflarının faaliyetleri arasında yatay ve/veya dikey/ konglomera bir ilişkinin olup olmadığı incelenmiştir.

(31) Devralan PALO ALTO; ağ güvenliği, bulut güvenliği, güvenlik operasyonları ve tehdit istihbaratı alanlarında sunduğu ürün ve hizmetler aracılığıyla kurumsal siber güvenlik çözümleri geliştirmekte ve sunmaktadır. Devre konu CYBERARK ise faaliyetlerini ağırlıklı olarak ayrıcalıklı erişim yönetimi, kimlik ve erişim yönetimi ile kimlik yönetimi ve idaresi alanlarında yürütmekte; buna ek olarak makine kimliği, kriptografik anahtar ve dijital sertifika yönetimi ile güvenli kurumsal tarayıcı çözümleri sunmakta ve danışmanlık, eğitim ile uygulama hizmetleriyle ürünlerini desteklemektedir. Yukarıda yer verildiği üzere pazarın en geniş haliyle kurumsal güvenlik yazılımı şekilde tanımlanması durumunda tarafların faaliyetleri arasında yatay bir örtüşmenin meydana geleceği değerlendirilmektedir.

(32) PALO ALTO ve CYBERARK'ın Türkiye'de kurumsal güvenlik yazılımları pazarındaki pazar paylarına aşağıdaki tabloda yer verilmektedir:

Tablo 2**:** Türkiye'de İşlem Taraflarının ve Rakiplerinin Kurumsal Güvenlik Yazılım Pazarındaki Son Üç Yıla Ait Pazar Payları

Teşebbüsler	Pazar Payı (%)		
	2022	2023	2024
CYBERARK	(.....)	(.....)	(.....)
PALO ALTO[18]	(.....)	(.....)	(.....)
Check Point	(.....)	(.....)	(.....)
Microsoft	(.....)	(.....)	(.....)
ESET	(.....)	(.....)	(.....)
CrowdStrike	(.....)	(.....)	(.....)
Trellix	(.....)	(.....)	(.....)
Diğerleri	(.....)	(.....)	(.....)
Kaynak: Bildirim Formu ve Cevabi Yazı			

(33) Tablodaki verilerden, işlem taraflarının Türkiye'de kurumsal güvenlik yazılım pazarındaki paylarının 2022, 2023 ve 2024 yılları bakımından oldukça düşük seviyede seyrettiği anlaşılmaktadır. Nitekim 2022-2024 döneminde CYBERARK'ın ilgili pazardaki pazar payının sırasıyla %(.....), %(.....) ve %(.....) olarak gerçekleştiği, PALO ALTO'nun ise pazar payının ilgili yıllar bakımından sırasıyla %(.....), %(.....) ve %(.....) olduğu görülmektedir. Ayrıca 2023-2024 dönemi bakımından rakiplerin pazar paylarının oldukça düşük seviyelerde kaldığı ve pazarın parçalı bir yapı sergilediği anlaşılmaktadır. Bu doğrultuda işlem neticesinde tarafların kurumsal güvenlik yazılım pazarında Türkiye'deki birleşik pazar payının %(.....)'dan az olacağı görülmektedir. Bu kapsamda gerek işlem taraflarının kurumsal güvenlik yazılım pazarında görece düşük pazar payına sahip olması gerekse pazarın çok oyunculu, eş deyişle parçalı yapısı dikkate alındığında bildirime konu işlemin, Türkiye'de yatay örtüşme bakımından herhangi bir rekabet karşıtı bir endişeye sebebiyet vermeyeceği değerlendirilmektedir.

(34) Diğer taraftan, işlem taraflarınca sunulan cevabi yazılarda, kurumsal güvenlik yazılımı alanında sunulan farklı çözümlerin, müşteriler tarafından tercih edilen kurulum modeli ve kullanım senaryosuna bağlı olarak ilgili oldukları ölçüde birbirini tamamlayıcı nitelik taşıyabildiği belirtilmektedir. Bu doğrultuda PALO ALTO ve CYBERARK'ın en beş büyük müşterisi arasında yer alan teşebbüslerden, taraflardan almakta oldukları ürün ve hizmetler arasındaki tamamlayıcılık ilişkisine yönelik değerlendirmeleri talep edilmiş olup gelen cevaplarda;

- (.....) tarafından; (.....), ağ güvenliği çözümleri ile kimlik ve anahtar güvenliği çözümlerinin birbirini tamamlayıcı nitelikte olduğu, ancak söz konusu ürünlerin birbirlerine bağımlı olmadığı, farklı üreticilerin çözümleriyle de entegre şekilde çalışabildiği,
- (.....) tarafından; (.....) söz konusu üç ürün grubunun birbirinden bağımsız olarak çalışabildiği; ürünler bağımsız nitelikte olmakla birlikte sadece bu üç uygulama özelinde değil, tüm güvenlik ürünleri birbirini tamamlayıcı ürünler olduğunu,
- (.....) tarafından; (.....), söz konusu ürünlerin tedarik süreçlerinin birbirinden farklı olduğu ve birlikte satın alınmadığı, PALO ALTO'nun ağ, uzaktan erişim ve bulut güvenliği çözümleri (örneğin; VPN erişim bileşeni, Prisma Access ve Prisma Cloud ile XSOAR'ın yönetim arayüzleri) kapsamında, kullanıcıların ve yetkili personelin sistemlere erişimi sırasında CYBERARK Identity çözümü aracılığıyla kimlik doğrulama, Tek Oturum Açma (*Single Sign-On*, SSO) ve Çok Faktörlü

[18] İşlem taraflarınca sunulan cevabi yazıda; GARTNER raporlarının, PALO ALTO'ya ilişkin Türkiye özelinde bir tahmin sunmadığı, söz konusu pazar payı tahminlerinin PALO ALTO'nun Türkiye'deki kurumsal güvenlik yazılımına ilişkin cirosunun, 2024, 2023 ve 2022 yılları için sırasıyla 2024 GARTNER raporu ve 2022 GARTNER raporunda yer alan ilgili toplam pazar büyüklüklerine bölünmesi suretiyle hesaplandığı ifade edilmiştir.

Kimlik Doğrulama *(Multi-Factor Authentication,* MFA) ile güvence altına alındığı; bu suretle CYBERARK'ın kimlik güvenliği katmanının, PALO ALTO ürünlerinin kullanımında erişimlerin güvenli şekilde tesis edilmesini sağlayan tamamlayıcı bir unsur olarak konumlandığı, bu çerçevede ürünler arasında entegre kullanım ve birbirini güçlendiren güvenlik katmanları çerçevesinde bir tamamlayıcılık ilişkisinin mevcut olduğu**,**

- (.....) tarafından; (.....), (.....), Prisma Cloud uygulaması ile Cyberark uygulaması şifre yönetimi konusunda entegre bir şekilde çalışabildiği, bu sayede güvenli şekilde şifrelerin saklanması, yönetilmesi işlemlerinin gerçekleştirilebildiği

hususları ifade edilmiştir.

(35) Gelen bilgiler çerçevesinde, PALO ALTO ve CYBERARK ürünlerinin birbirlerinden bağımsız olarak temin edilip kullanılabildiği, bununla birlikte söz konusu ürünlerin bazı kullanım senaryolarında entegre biçimde çalışarak güvenlik çözümlerini destekleyen ve güçlendiren tamamlayıcı nitelik taşıdığı, bunun yanı sıra, esasen tüm güvenlik ürünlerinin birbirlerini tamamlayıcı ürünler olduğu anlaşılmaktadır.

(36) Bu kapsamda devralan PALO ALTO ile devre konu CYBERARK'ın kimlik güvenliği ürün ve hizmetleri arasında bir tamamlayıcılık ilişkisi bulunduğu değerlendirilmiştir. Bu sebeple, kurumsal güvenlik yazılımları hizmetleri pazarında rekabeti kısıtlayıcı bir konglomera etki doğma olasılığı incelenmiştir. Ortaya çıkabilecek ilk endişe, birleşik teşebbüsün müşterilere, kurumsal güvenlik yazılımları bakımından entegre (uçtan uca) çözümler sunarak rakip ürünlerin birlikte işlerliğini azaltma ve/veya engellemesine ilişkindir. Ayrıca birleşik teşebbüsün PALO ALTO ve CYBERARK bünyesinde bulunan ürün ve hizmetlerin paket satış veya bağlama uygulamaları ile müşterilere sunma ihtimali mevcut dosya kapsamında değerlendirilmesi gereken bir diğer endişedir.

(37) Tarafların sunduğu ürünlerin kurumsal güvenlik yazılımı pazarının alt segmentlerinde yer aldığı dikkate alındığında, işlem taraflarının bu pazarlardaki payları önem arz etmektedir. Aşağıdaki tabloda Türkiye'de CYBERARK'ın kurumsal güvenlik yazılımın alt kırılımları bazında pazar paylarına yer verilmektedir:

Tablo 3: CYBERARK'ın Türkiye'de GARTNER Segmentleri Bazında Kurumsal Güvenlik Yazılım Pazarındaki Son Üç Yıla Ait Pazar Payları

Teşebbüs	GARTNER Segmenti	Pazar Payları		
		2022	2023	2024
CYBERARK	Kimlik Yönetimi ve İdaresi	(.....)	(.....)	(.....)
	Erişim Yönetimi	(.....)	(.....)	(.....)
	Diğer Güvenlik Yazılımları	(.....)	(.....)	(.....)
Kaynak: Cevabi Yazı				

(38) CYBERARK'ın Türkiye pazarında 2022, 2023 ve 2024 yıllarına ilişkin GARTNER segmentleri bazında pazar payları incelendiğinde, erişim yönetimi segmenti bakımından pazar paylarının sırasıyla %(.....), %(.....) ve %(.....) olarak gerçekleştiği, diğer güvenlik yazılımları segmentine ilişkin olarak ise %(.....), %(.....) ve %(.....) olduğu görülmektedir. Bununla birlikte işlem taraflarınca sunulan cevabi yazıda; PALO ALTO'nun Türkiye'de kurumsal güvenlik yazılım pazarını oluşturan GARTNER segmentleri bazında ciro verilerinin sınıflandırılmadığı, dolayısıyla segment bazında pazar payı bilgisinin sağlanamadığı belirtilmektedir. Bununla birlikte söz konusu segmentler bazında Türkiye'deki pazar paylarının küresel ölçekte sunulan pazar paylarından yüksek olmayacağı ifade edilmektedir. Bu doğrultuda aşağıda yer verilen tabloda PALO ALTO'nun GARTNER segmentleri bazında küresel ölçekteki pazar paylarına yer verilmektedir:

Tablo 4: Küresel Ölçekte Tarafların GARTNER Segmentleri Bazında Kurumsal Güvenlik Yazılım Pazarındaki Son Üç Yıla Ait Pazar Payları

Teşebbüs	GARTNER Segmenti	Pazar Payları		
		2022	2023	2024
PALO ALTO	Uç Nokta Koruma Platformu	(.....)	(.....)	(.....)
	Güvenli İnternet Ağ Geçidi	(.....)	(.....)	(.....)
	Güvenlik Bilgileri ve Olay Yönetimi	(.....)	(.....)	(.....)
	Bulut İş Yükü Koruma Platformları	(.....)	(.....)	(.....)
	Bulut Erişim Güvenliği Aracıları	(.....)	(.....)	(.....)
	Bulut Güvenliği Durum Yönetimi	(.....)	(.....)	(.....)
	Diğer Güvenlik Yazılımları	(.....)	(.....)	(.....)
Kaynak: Cevabi Yazı				

(39) Tablo 4'de yer alan verilerden, PALO ALTO'nun küresel ölçekte GARTNER segmentleri bakımından pazar paylarının %(.....) ila %(.....) oranları ile düşük seviyelerde kaldığı anlaşılmaktadır.

(40) Diğer taraftan işlem taraflarınca sunulan cevabi yazıda; CYBERARK'ın cirosunun büyük çoğunluğunu PAM ürününün oluşturduğu ve PAM'ın CYBERARK'ın temel ürünü olduğu, GARTNER raporlarında, PAM kimlik güvenlik yazılımının ayrı bir alt segmenti olarak tanımlanmadığı, diğer alt segmentlerde sınıflandırılmayan kurumsal güvenlik yazılımı türleri ile birlikte "Diğer Güvenlik Yazılımları" alt kategorisi altında ele alındığı, öte yandan 2024 yılı itibarıyla PAM alanındaki küresel pazar payının yaklaşık %(.....) civarında olduğunu tahmin edildiği, bununla birlikte CYBERARK'ın, Türkiye'deki pazar payının yukarıda belirtilen küresel pazar payından önemli ölçüde farklılaşmasında herhangi bir gerekçe bulunmadığı belirtilmektedir. Ayrıca CYBERARK'ın rakipleri olan Delinea ve Beyond Trust'un her birinin yaklaşık %(.....), Saviynt, One Identity, Wallix, SenhaSegura, Arcon, ManageEngine, ve Netwrix'in her birinin ise en fazla %(.....) pazar payına sahip olduğunun, kalan pazar payının ise daha küçük ölçekli rakipler arasında dağıldığı dile getirilmektedir. Bu kapsamda CYBERARK'ın cirosunun büyük kısmını oluşturan PAM ürünü bakımından pazarda lider konumda olduğu anlaşılmaktadır.

(41) CYBERARK'ın PAM çözümünün odağının bir şirketin bilgi teknolojileri (BT) sistemine, BT yöneticileri ile sistemin diğer "ayrıcalıklı" kullanıcıları tarafından erişimin kontrolü ve izlemesi olduğu, söz konusu kullanıcıların, şirketin BT sistemindeki ayrıcalıklı olmayan kullanıcılara kıyasen BT sistemi üzerinde daha geniş işlem yapma yetkilerine sahip olmaları nedeniyle "ayrıcalıklı" olarak tanımlandığı, bir PAM çözümünün bu türden ayrıcalıklı kullanıcıların BT sistemine erişim biçimlerini kontrol etmek ve aynı zamanda erişim verilmesi akabinde sistemde ne yaptıklarını izlemek suretiyle, ayrıcalıklı olmayan kullanıcıların ayrıcalıklı erişim elde etmesini önlemeyi ve güvenlik risklerini asgariye indirmek amacıyla ayrıcalıklı kullanıcıların erişimini çeşitli şekillerde sınırlandırmayı hedeflediği belirtilmektedir. Bu doğrultuda örneğin, bir şirket bir PAM çözümünü ve aynı zamanda PALO ALTO'nun, Cortex XSIAM ürününü kullanmayı tercih edebilecektir. Bu senaryoda PAM çözümünün, Cortex XSIAM'ın yönetim altyapısına PAM erişim kontrollerinin, erişimi kontrol etmek ve yönetmek üzere kullanılabileceği, bu sayede ise yalnızca yetkili BT yöneticileri ve diğer ayrıcalıklı kullanıcıların Cortex XSIAM ürün ortamındaki yapılandırmalarda değişiklik yapabilmesi kontrol edilerek güvence altına alınabildiği ifade edilmektedir. Dolayısıyla CYBERARK'ın PAM ürünün çeşitli senaryolar altında PALO ALTO tarafından sunulan güvenlik ürünlerle ile birlikte çalışmasının söz konusu olabileceği anlaşılmaktadır. Bununla birlikte işlem taraflarınca sunulan cevabi yazıda, ürünlerin birlikte çalışılabilirliğinin ve çoklu tedarikçi kullanımının sektörde yaygın bir uygulama olduğu belirtilmektedir.

(42) Bu kapsamda CYBERARK ve PALO ALTO'nun müşterilerinden, işlem taraflarından sağlamış oldukları ürünlerin tedariki sürecinde birden fazla tedarikçiyle çalışılıp çalışılmadığı, söz konusu süreçte tek bir tedarikçiyle veya birden fazla tedarikçiyle çalışmanın avantaj veya dezavantajlarına yönelik görüşleri talep edilmiştir. Bu çerçevede;

- (.....) tarafından; her iki üreticinin çözümlerinin tedarikinde tek bir tedarikçiye bağlı kalınmadığı, birden fazla tedarikçiyle paralel alım süreçleri yürütüldüğü, aynı üreticiye ait farklı ürün gruplarının farklı tedarikçiler üzerinden satın alınabildiği,
- (.....) tarafından; kurumsal güvenlik yazılım pazarında, büyük teşebbüslerin küçük teşebbüsleri devralmak suretiyle ürün gamlarını genişlettiği; Microsoft, Check Point ve PALO ALTO gibi büyük oyuncuların yanı sıra irili ufaklı çok sayıda teşebbüsün pazarda faaliyet gösterdiği, ilgili ürünlerin tedariki amacıyla Türkiye'de yerleşik üç firmadan destek alındığı, ürünler birbirinden bağımsız olduğu için işleme onay verilmesi durumunda edinim ve destek anlamında herhangi bir endişelerinin bulunmadığı,
- (.....) tarafından; PALO ALTO ve CYBERARK ürünlerinin farklı tedarikçilerden de temin edilmekte olduğu, birden fazla tedarikçiyle çalışmanın avantajları arasında tedarikçi bağımlılığının önlenmesi, fiyat ve ticari koşullarda rekabetin sağlanabilmesi ve ihtiyaçlara uygun çözümlerin seçilebilmesinin yer aldığı, tek tedarikçiyle çalışmanın olası avantajlarının ise satın alma, sözleşme ve destek süreçlerinin tek muhatap üzerinden yürütülmesinden kaynaklanabilecek kolaylıkları kapsadığı,
- (.....) tarafından; *Cyberark* ve *Conjur* uygulama lisanları için tek tedarikçi olarak CYBERARK ile çalışıldığı, tek bir tedarikçi ile çalışılmasının destek süreçlerinin daha etkin yönetilmesi, ürünlerin tek bir çatı altında toplanması sayesinde uyumluluğun ve yönetim kolaylığının artması ile lisanslama maliyetlerinin optimize edilmesi açısından avantaj sağladığı, *Prisma Cloud* uygulama lisansı bakımından hâlihazırda tek tedarikçi olarak Quasys Dijital Teknoloji Çözümleri AŞ ile çalışıldığı, tek tedarikçi ile çalışılmasının; firma tarafından alınan destek süreçlerinin etkin şekilde yönetilmesi, ürünlerin tek bir çatı altında toplanması sayesinde uyumluluk ve yönetim kolaylığı sağlanması ile lisanslama maliyetlerinin optimize edilmesi açısından avantajlarının bulunduğu, bununla birlikte herhangi bir zamanda alternatif bir tedarikçi ile sözleşme imzalanarak çalışmaya başlanmasının mümkün olduğu, bu nedenle söz konusu durumun herhangi bir dezavantaj oluşturmadığı

hususları belirtilmiştir.

(43) Yukarıda yer verilen teşebbüs görüşleri incelendiğinde; kurumsal güvenlik çözümlerinin tedarikinde uygulamada ağırlıklı olarak birden fazla tedarikçiyle çalışıldığı ve müşterilerin birden fazla tedarikçi ile çalışmasının önünde herhangi bir engel bulunmadığı anlaşılmaktadır.

(44) Ayrıca CYBERARK ve PALO ALTO'nun müşterilerinden, birlikte çalışılabilirliğin sektörde yaygın bir uygulama olup olmadığının anlaşılması ve bildirime konu işlemin birlikte çalışılabilirlik üzerindeki etkisine yönelik bilgi talep edilmiştir. Bu kapsamda;

- (.....) tarafından; güvenlik çözümlerinin birlikte çalışabilir olması durumunun sektörde yaygın kullanılan bir uygulama olduğu, anılan birlikteliğin aynı üreticinin çözümleri altında ya da farklı üreticilerin çözümlerinin entegrasyonları ile de sağlanabildiği, aynı üretici çözümlerinin entegrasyonun daha kolay ve birlikte işlerliği test edilmiş çözümler olması nedeniyle uygulama kolaylığı

açısından avantaj sağlayabileceği, bu nedenle bildirim konusu işlemin gerçekleşmesi durumunda söz konusu pazardaki ürünlerin birlikte işlerliği üzerindeki etkilerinin kullanıcı deneyimi açısından olumlu olabileceği,

- (.....) tarafından; güvenlik alanındaki risklerin farklı katmanlarda ve farklı nedenlerle ortaya çıktığı; bu nedenle kritik altyapı kurumlarında gerçek anlamda güvenliğin, farklı üreticilere ait nitelikli ürünlerin birlikte kullanılmasıyla sağlanabildiği,
- (.....) tarafından; güvenli ağ alanında ürünler sunmakta olan PALO ALTO ile kimlik güvenliği alanında hizmet sunan CYBERARK birlikteliğinin tek ekran ve merkezi yönetim gibi faydalar getirebileceği ve ürün satın alımlarında tercih sebebi haline gelebileceği, bununla birlikte tek bir sistem altında birleşen güvenlik yönetiminin güvenlik açığı yaratma ihtimali olabileceğinin de değerlendirildiği,
- (.....) tarafından; kurumsal güvenlik yazılımı pazarında, ağ güvenliği, bulut güvenliği ve kimlik/erişim güvenliği çözümlerinin farklı tedarikçiler tarafından sağlanması ve müşterilerin ihtiyaçlarına göre entegrasyon yoluyla birlikte çalışacak şekilde kurgulanmasının sektörde yaygın bir uygulama olduğu, kurumsal ölçekte güvenlik mimarilerinin çoğunlukla "çoklu tedarikçi" yaklaşımıyla kurulduğu; ürünler arası entegrasyonların da standart arayüzler ve uygulama/kimlik doğrulama mekanizmaları üzerinden sağlandığı, (.....)'un söz konusu ürünlerin mevcut kullanımı da, farklı güvenlik katmanlarında kullanılan ürünlerin birlikte çalışabilirlik temeline dayandığı, söz konusu devralma işleminin PALO ALTO ve CYBERARK ürünlerinin birlikte işlerliğini doğrudan artırması veya azaltmasının beklenmediği, ancak birleşik teşebbüslerin entegrasyonlara ilişkin ticari politikalarının potansiyel etki yaratma riski taşıdığı,
- (.....) tarafından; kurumsal güvenlik yazılımı pazarındaki kurumsal güvenlik uygulamalarında birlikte işlerliğin/birlikte çalışabilirliğin sektörde yaygın bir uygulama olduğu, söz konusu devralma işleminin pazardaki ürünlerin birlikte işlerliği/birlikte çalışabilirliği üzerinde olumsuz bir etki yaratmasının beklenmediği,
- (.....) tarafından; söz konusu işlemin birlikte çalışabilirlik üzerinde herhangi bir etkisinin bulunmadığı, kurumsal güvenlik yazılım pazarında PALO ALTO ve CYBERARK ürünleri kapsamında hizmet veren çok sayıda üreticinin bulunduğu, CYBERARK tarafından ilgili ürünlerin sadece PALO ALTO ürünleriyle çalışacağına ilişkin herhangi bir bildirim alınmadığı

hususları ifade edilmektedir.

(45) Yukarıda yer verilen teşebbüs görüşlerinden özetle; kurumsal güvenlik yazılımı pazarında birlikte çalışabilirliğin müşteri ihtiyaçları doğrultusunda şekillenen ve farklı üreticilerin çözümlerinin entegrasyonuna dayanan yaygın bir uygulama olduğu, bunun yanı sıra tek bir sistem altında birleşen güvenlik sisteminin güvenlik açığı yaratma riskini doğurduğu, bildirim konusu işlemin işlem tarafları ile rakip ürünlerin birlikte çalışabilirliği üzerinde doğrudan olumsuz bir etki yaratmasının beklenmediğini anlaşılmaktadır.

(46) Tüm bu değerlendirmeler ışığında, mevcut dosya kapsamında yapılan olası konglomera etkilere ilişkin değerlendirmeler sonucunda; PALO ALTO ile CYBERARK'ın faaliyetleri arasında Türkiye'de tamamlayıcılık ilişkisinin bulunduğu, ancak pazarın çok oyunculu yapısı, pazarda farklı oyuncular tarafından sağlanan ürünlerin birlikte çalışabilir şekilde kurgulanmasının yaygın bir uygulama olduğu ve müşterilerin çok sayıda tedarikçi ile çalışmasının önünde herhangi bir engel bulunmadığı hususları dikkate alınarak, işlem neticesinde birleşik teşebbüsün

paketleme/bağlama stratejisi aracılığıyla veya ürünlerin birlikte çalışabilirliği azaltmak ve/veya engellemek suretiyle rekabet karşıtı bir etkiye neden olmayacağı değerlendirilmektedir.

(47) Yapılan inceleme ve değerlendirmeler neticesinde, bildirime konu işlem ile 4054 sayılı Kanun'un 7. maddesi çerçevesinde başta hâkim durum yaratılması ya da mevcut bir hâkim durumun güçlendirilmesi olmak üzere etkin rekabetin önemli ölçüde azaltılması sonucunun ortaya çıkmayacağı kanaatine ulaşılmaktadır.

H. SONUÇ

(48) Düzenlenen rapora ve incelenen dosya kapsamına göre, bildirim konusu işlemin 4054 sayılı Kanun'un 7. maddesi ve bu maddeye dayanılarak çıkarılan 2010/4 sayılı Rekabet Kurulundan İzin Alınması Gereken Birleşme ve Devralmalar Hakkında Tebliğ kapsamında izne tabi olduğuna; işlem sonucunda etkin rekabetin önemli ölçüde azaltılmasının söz konusu olmaması nedeniyle işleme izin verilmesine, gerekçeli kararın tebliğinden itibaren 60 gün içinde Ankara İdare Mahkemelerinde yargı yolu açık olmak üzere OYBİRLİĞİ ile karar verilmiştir.