FENERBAHÇE ÜNİVERSİTESİ
Ataşehir Kampüsü

"Güvenlik, Donanım ve Lisans Yenilemesi"

T E K N İ K Ş A R T N A M E

1. SATIN ALMANIN KONUSU

İşbu teknik şartname, "Fenerbahçe Üniversitesi, 2020-2021 yılı proje bütçe planında yer aldığı şekliyle "**Bilgisayar, Donanım ve Yazılım Giderleri"** kalemine mahsuben yapılacak olan **"Güvenlik, Donanım ve Lisans Yenilemesi"** işine ilişkin koşulları belirlemektedir. Bu şartname kapsamında tedarik edilecek olan donanım ve yazılım malzemeleri Fenerbahçe Üniversitesinin bilişim alt yapısında ve eklem projeler kapsamında kullanılacaktır.

1.1. Kapsam ve Genel Koşullar

Bu teknik şartname, Fenerbahçe Üniversitesi için satın alınacak "Güvenlik, Donanım ve Lisans Yenilemesi"alımına ilişkin ürünlerin teminini, teknik özelliklerini, teslimini ve garanti sürelerini kapsar. Firmalar teklif mektuplarında teknik şartnameye uygun olan ürünün markasını, fiyatını, teslimat ve garanti süresini ve varsa teknik şartnamede istenmeyen ancak üründe olan ilave özellikleri bildirecektir**.** Ürünlerin şartnamede belirtilen özelliklere ve numunesine uygun olmadığı tespit edildiğinde ayrı bir ücret talep edilmeden istenilen özelliklerdeki ürünle değiştirilecektir.

Bu ihale kapsamındaki işlerde Yüklenici ile İdare arasında "GİZLİLİK" anlaşması yapılacaktır. Kapsam İdare tarafından belirlenecektir.

Yüklenici,projekapsamındaİdaretarafındanbelirlenenstandartprosedürlereveyönergelere uyumlu olacak şekilde hizmet verecek ve kayıtları İdare'nin göstereceği elektronik ortamda saklayacak, istendiğinde İdare' yesunacaktır.

Yüklenici, bu "Şartname" ve eklerinde belirtilsin veya belirtilmesin alacağı ve uygulayacağı kararlarda İdare' nin onayını alacaktır. İdare, yazılı olmak kaydı ile yapılacak işlemler için süreçleri Yüklenici'ye devredebilir.

Yüklenici, çalışmalar sırasında sistemin kesintiye uğramaması için gerekli önlemleri alacak ve müdahaleye başlamadan önce İdare' ye bilgilendirecektir.

İstekli, teklif edeceği ürünlerle ilgili üreticisinden veya yetkili distribütöründen bu ihale için alınmış şartname kapsamında teklif edilen ürünleri satmaya, kurmaya ve teknik desteğini vermeye yetkili olduklarını gösterir. İstekli adına düzenlenmiş yetki belgelerini teklif ile birlikte İdare' ye sunacaktır.

Tüm ürünler (donanım, yazılım, lisans vb.) yeni, kullanılmamış, hasarsız ve eksiksiz olarak, orijinal paketinde işin yapılacağı yere getirilecektir.

Temin ve teslim edilecek her türlü malzemenin nakliye, taşıma, sigortası Yüklenici tarafından karşılanacaktır. Teslim ve kurulum yeri İdare lokasyonudur.

İstekli teklifinde kullanacağı tüm cihazlar, malzemeler ve donanımlara ait marka ve modellerini liste halinde ve yoruma mahal bırakmayacak detayda (isim, ürün kodu, marka, model vb.) sunacağı teklif dokümanında yer verecektir.

Belirtilen tüm ürünler, kurulumu yapıldıktan sonra anahtar teslimi çalışır vaziyette teslim edilecektir.

İstekli, "Şartname" deki tüm maddeleri ayrı ayrı cevaplayacaktır.

1.2. Kısaltmalar

YÜKLENİCİ : Bu teknik şartnameye uygun olarak işi anahtar teslimi yapacak firma.
İDARE : Fenerbahçe Üniversitesi (FBU)
MERKEZ : Fenerbahçe Üniversitesi Ataşehir ana merkez kampüsü

2. Satın Alınacakların Teknik Özellikleri

2020-2021 öğretim yılında, ihtiyaç kapsamında güvenlik ürünü, donanım ve lisans yenilemesi satıl alma işlemi yapılacaktır.

2.1. Veri Sızıntısı Önleme Sistemi (DLP, Endpoint, Discovery)(210)Kullanıcı

2.1.1. Teklif edilecek çözüm; kritik bilgilerin kurum dışına çıkmasını tespit ve önlemek amacıyla, veri sızıntılarını ağ (HTTP, HTTPS, FTP, SMTP), kullanıcı bilgisayarı (LAN,Printer, Uygulama, Web, Email, Taşınabilir Disk) ve mobil telefonlar (Active Sync) seviyesinde tespit edebilmelidir.

2.1.2. Teklif edilecek çözüm, network seviyesinde Web trafiği (HTTP/HTTPS/FTP) üzerinden oluşabilecek veri sızıntılarını kontrol edebilmek için ICAP uyumlu bir Firewall/Proxy ile entegre olarak çalışabilmelidir. ICAP desteği sayesinde bulut tabanlısistemlerle de entegre çalışabilmesi talep edilmektedir.

2.1.3. Teklif edilecek çözüm; web gateway teknolojileriyle doğrudan entegre çalışabilmeli ve ssl tabanlı veri aktarımlarını kontrol edebilmelidir, şayet sağlanamıyorsa yüklenici başka bir üreticiyle entegre olacak şekilde bu özelliği sağlayabilmelidir.

2.1.4. Teklif edilecek çözüm; Web gateway teknolojileri ile entegre olarak hedef bazlı kural tanımlama (örneğin sosyal medya ve genel blog sayfalarında kurumsal veri paylaşımının engellenmesi) yeteneğine sahip olmalıdır, şayet sağlanamıyorsa yüklenici başka bir üreticiyle entegre olacak şekilde bu özelliği sağlayabilmelidir.

2.1.5. Çözüm; Web Security GW ile doğrudan entegre olarak siber tehditlerin ve zararlı uygulamaların neden olacağı veri ihlallerini otomatik olarak algılayabilmeli ve durdurabilmelidir.

2.1.6. Teklif edilecek çözüm, network seviyesinde SMTP trafiği üzerinden olabilecek veri sızıntılarını kontrol edebilmek için gerekli yazılım ve lisansları teklife dâhil etmelidir. MTA olarak çalışacak şekilde entegrasyonu yapılabilmeli, üzerinden geçen SMTP trafiğinde gerekli politikaları çalıştırabilmelidir.

2.1.7. Teklif edilecek çözüm, 210 son kullanıcı ajan lisansına sahip olacaktır. Lisans süresi 1 yıl olacaktır.

2.1.8. Teklif edilen çözüm kritik bilgilerin, kullanıcıbilgisayarları ve ağ seviyesinde tarama yaparak başka hangi sunucu ve kullanıcı bilgisayarlarında bulunduğunu tespit edebilecek keşif modülüne sahip olmalıdır. Keşif modülüne ait lisanslar XXXX kullanıcı için, X yıl olarak teklif edilmelidir.

2.1.9. Keşif modülü; Cloud tabanlı ortamlardan Azure ortamında çalışan Mail sunucular (Office365) ve Share Point online Portal sistemleri gibi cloud tabanlı ortamlar üzerinde de keşif yapabilmelidir.

2.1.10. Tanımlı kritik bilgilerin tespitinde tam bir doğruluk olabilmesi için özel teknolojilere sahip olmalıdır.
2.1.11. Kuruma özel politikalar tanımlayabilmek için; belirli anahtar kelimeler, regular expression'lar, belirli dokuman tipleri kullanılabilmelidir.
2.1.12. Kritik bilgilerin sisteme öğretilebilmesi için, sistem kritik bilgilerin bulunduğu dosyaların ve veri tabanlarının parmak izini alabilmelidir. Dosya sunucusu veya veri tabanlarında parmak izi almak için eğer ayrı bir lisans gerekiyorsa, bu lisanslar çözüm içerisine eklenmelidir.
2.1.13. Parmak izi alınmış veriler, verinin bulunduğu dokümandan (adı, uzantısı) bağımsız olarak, ağ seviyesinde, veri sızıntısı politikaları ile tespit edilebilmelidir. Tespit sistemi orijinal dokümandan bağımsız işleyebilmelidir.
2.1.14. Kritik verilerin tespiti için sıkıştırılmış dosyalar (ZIP, TAR, RAR) en az 12 alt seviyeye kadar açılabilmelidir.
2.1.15. Parmak izi alınacak dosyalara; tip, uzunluk, lokasyon, tabanlı filtreleme politikaları tanımlanabilmelidir.
2.1.16. Parmak izi teknolojisi için erişilen dosyaların orijinal dosya erişim tarihi değiştirilmemelidir.
2.1.17. Sistem şifreli sıkıştırılmış dosyaları otomatik algılayabilmeli ve içeriği analiz edilemeyen bu gibi dosyaları tespit edip engelleyebilecek hazır politikalara sahip olmalıdır.
2.1.18. Farklı dil ve karakter setindeki dosyaların parmak izini alabilmelidir
2.1.19. Sistem ODBC veya JDBC ile veri tabanına düzenli bağlanarak, veri tabanındaki kritik bilgilerin de parmak izini otomatik olarak alabilmelidir. Veri sızıntısı olmaması için, bu yöntem manuel bir iş gerektirmemelidir.
2.1.20. Sistem LDAP, MS Active Directory ile entegre çalışabilmeli, veri sızıntısı politikaları tanımlanırken, LDAP veya AD kullanıcılarına göre politikalar tanımlanabilmelidir. Sistem, birbirinden bağımsız birden fazla Directory Servis tanımlamaya ve entegrasyona izin vermelidir.
2.1.21. Parmak izi alma veya bilgisayarlardaki kritik bilgilerin kopyalarını arama işlemleri için sisteme tanımlanan tüm şifreler, veri tabanı içerisinde şifreli olarak tutulmalı ve tanımlamaların hiçbirisi için şifreler açık bir şekilde konfigürasyon dosyalarına yazılmamalıdır.
2.1.22. Politikalar içerisinde engelleme, izin verme, karantinaya alma, taşınabilir USB diske şifreli kopyalama ve sadece izleme şeklinde aksiyonlar tanımlanabilmelidir.
2.1.23. Anında mesajlaşma, dosya paylaşım programları gibi, şifreli erişime sahip uygulamalar üzerinden gönderilmeye çalışılan kritik verilerin tespiti için, kullanıcı bilgisayarındaki ajanlar kullanılabilmelidir.
2.1.24. Ajanlar en az Windows 7- 8- 8.1- 10, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Mac OS 10.11.x, 10.12.x, 10.13, 10.14) işletim sistemlerini hem 32 bit hemde 64 bit olarak desteklememelidir.
2.1.25. Kullanıcı bilgisayarındaki ajan vasıtasıyla;
2.1.26. Kritik bilgilerin USB depolama aygıtlarına kopyalanması engellenebilmeli veya şifreli kopyalanmalıdır. Sadece tanımlı marka/model USB depolama aygıtlarına izin verilebilmelidir. USB'lere şifreli olarak aktarılan veriler LDAP veya MS AD entegrasyonu ile kullanıcıgruplarınagörefarklışifrelemeimkân sunarak departmanlar arasında veri silintisininönüne de geçişsağlanabilmelidir.
2.1.27. Ajan, bilgisayardan çıkan HTTP/HTTPS ve SMTP trafiğini (Browserlar ve Outlook aracılığıyla) izleyebilmeli ve gerekirse trafiği daha client'dan çıkmadan engelleyebilmelidir (Veri silintisi tespiti için desteklenmesi beklenen kanallar; Web (HTTP,HTTPS,FTP), Email (Outlook , Lotus Notes , Apple Mail vb diğer email

uygulamaları), Uygulama (Google Drive ,File Zilla , Tor , Itunes , DropBox , Skype , Lync vb 3. Parti uygulamalar), Network paylaşımı, Taşınabilir & Flash Disk vb depolama alanları, Printer, CD / DVD yazma işlemleri,)

2.1.28. Ajan, paylaşılan dizinlere yapılan dosya kopyalamalarında (File Share), veriyi analiz edebilmeli ve gerektiğinde bloklayabilmelidir.
2.1.29. Belirli uygulama veya uygulama grupları arasındaki cut, copy, paste, print screen gibi işlemler denetlenebilmeli, istenirse bloklayabilmelidir.
2.1.30. Kullanıcı bilgisayarı ağa bağlı değilken farklı, bağlı iken farklı politikaları icra edebilmelidir.
2.1.31. Sadece kritik verilerin bulunduğu dokümanların yazdırılması engellenebilmelidir
2.1.32. Bilgisayarlar içerisindeki kritik bilgi barındıran dosyalar, keşif yöntemi ile tespit edilebilmeli ve raporlanabilmelidir.
2.1.33. Keşif işlemi bilgisayar kullanılmıyorken veya CPU farklı bir uygulama tarafından meşgul edilmediği sıralarda otomatik olarak yapılabilmelidir.
2.1.34. Ajan; Internet Explorer, Mozilla Firefox , Chrome ve Safari tabanlı browser uygulamalarını desteklemelidir.
2.1.35. Ajan; Office 365 email altyapısını tam olarak desteklemelidir.
2.1.36. Kritik veriler için (dosya ya da veri tabanı) yapılan parmak izi işlemleri sonrasında oluşan parmak izi veri tabanı kullanıcı ajanları üzerinde de taşınabilmeli. Böylece kullanıcı bilgisayarı kurum ağı dışarısına çıktığında, offline olduğunda da parmak izi ile ilgili politikalar çalışabilmelidir. Bahsi gecen parmak izi veritabanı ajan kurulu kullanıcıbilgisayarlarının diskinde tutulmalıdır.
2.1.37. Teklif edilecek çözüm Citrix ve VMWare gibi Sanal Desktop Mimarilerini (VDI) desteklemelidir.
2.1.38. Ajan her türlü kritik veriyi hem ofis içinde hem de ofis dışında herhangi bir VPN bağlantısı olmaksızın korumaya devam edebilmelidir.
2.1.39. Belirli bir kullanıcı bilgisayarındaki ajanı, geçici bir süre ile durdurabilmek ve bunu kayıt altına alabilmek mümkün olabilmelidir.
2.1.40. Ajanlar ve yönetim sunucusu arasındaki iletişim şifreli olmalıdır.
2.1.41. Ajanlar Group Policy Object, SCCM veya SMS ile kullanıcı bilgisayarlarına dağıtılabilmelidir.
2.1.42. Kullanıcıların ajanları stop etmeye çalışması, kapatmaya çalışması durumunda kendini koruyabilmeli ve otomatik olarak tekrar çalışabilmelidir.
2.1.43. Kullanıcı bilgisayarlarında görünen onay/blok ekranları Türkçe olabilmelidir.
2.1.44. Tespit edilen güvenlik ihlalleri için sistem içerisinde bir çağrı kaydı açılabilmeli ve belirli bir kişiye atanabilmelidir.
2.1.45. Açılan her çağrı içerisinde, politika ihlaline neden olan olayın detayları (Source IP, Kullanıcı, Veri sızıntısı tipi, politikası, hedef adres, veri örneği) belirtilmelidir.
2.1.46. Açılan çağrıların içerisinde, adli soruşturmada kullanılabilecek şekilde, ihlale neden olan bilgi saklanabilmelidir.
2.1.47. Çözüm gerektiğinde iç tehdit uygulamaları ile entegre olarak ihlal öncesi ve sonrası için detaylı forensic kaydı (Video Kaydı, Web, Email, File Aktivitesi) tutabilmelidir. Böylece kullanıcı niyetinin tam olarak anlaşılabilmesini sağlamalıdır.
2.1.48. Sisteme rol tabanlı erişim sağlanabilmelidir.
2.1.49. Sistem yöneticilerinin, oluşan çağrılar içerisindeki adli kayıtları görmesi engellenebilmeli, sadece bu çağrılara bakabilecek ve adli kayıtları görebilecek haklara sahip kullanıcılar tanımlanabilmelidir.
2.1.50. Bilgi ihlali durumunda yönetici, bilginin sahibi, bilgiyi gönderene uyarı mesajı eposta ile gönderilebilmelidir.

2.1.51. Farklı kullanıcıların sisteme, sadece yetkili oldukları bilgi ihlali politikalarını görebilecekleri şekilde erişmeleri sağlanabilmelidir.
2.1.52. Ürün içerisinde hazır rapor şablonları olmalıdır. Bu raporların haricinde, kuruma özel raporlar da hazırlanabilmelidir.
2.1.53. Raporlar csv veya pdf formatında çıktı verebilmelidir.
2.1.54. Otomatik raporlar oluşturulabilmeli ve belirlenen periyotlarda sistem yöneticilerine email ile gönderilebilmelidir.
2.1.55. Çözüm oluşan her bir ihlal kaydı için ayrı ayrı SIEM entegrasyonuna sahip olmalıdır.
2.1.56. Çözüm; GDPR ve KVKK gibi yasalara için tam koruma sağlamalıdır. GDPR için tüm Avrupa ülkelerini kapsayacak şekilde hazır politikalara sahip olmalıdır.
2.1.57. Çözüm hali hazırda ek bir veri tanımlamasına ihtiyaç duymaksızın TC kimlik no , Kredi kartı no gibi en az 2000 hazır veri şablonuna sahip olmalıdır.
2.1.58. Belirli bir zaman diliminde, belirli bir sayıda kritik bilginin, zamana yayılarak kurum dışarısına gönderilmesi durumunda (örneğin 1 dakika içerisinde 10 farklı mail içerisinde 1'er adet T.C. kimlik numarasının ayrı mesajlar halinde gönderilmesi ve sonuçta 10 farklı T.C. kimlik numarasının gönderilmesi durumu) sistem bu tarz parçalı veri sızıntılarınızda tespit edebilmelidir.
2.1.59. Ürün içerisinde parmak izi mekanizması dışında kuruma ait kritik verilerin tanımlanması için öğrenme yoluyla çalışan akıllı bir mekanizma (machine learning) olmalıdır.
2.1.60. Teklif edilecek çözüm kritik bilgilerin imaj dosyası olarak kurum dışarısına çıkmasını engellemelidir. Network seviyesinde imaj dosyalarını (PDF, JPEG, BMP, PNG, GIF, TIFF) OCR (Optical Character Recognition) teknolojisi ile tarayabilecek ve veri sızıntısını tespit edebilecek bir çözüme sahip olmalıdır.
2.1.61. Teklif edilecek çözüm güvenlik analiz yeteneklerine sahip olmalı oluşan olay kayıtları üzerinde analizler yaparak en riskli kullanıcıları gösterebilen bir Dashboard ekranına ve gelişmiş analitik rapor yeteneğine sahip olmalıdır.
2.1.62. 3. Parti veri sınıflandırma ürünleri ile birlikte çalışabilmelidir. Bu ürünlerin dosyalara veya E-Postalara eklemiş olduğu meta data bilgilerini tespit edebilmeli ve istendiği durumda bloklayabilmelidir.
2.1.63. Teklif edilecek DLP çözümü, UEBA (User and Entity Behavior Analytics) çözümleri ile entegre edilebilmeli ve bu sayede olası izinsiz girişleri ve zararlı aktiviteleri kullanıcı hareketlerini ve davranışlarını baz alarak tespit edip alarmlar üretebilmeli ve dinamik aksiyonlar alabilmeye (örnek mail karantinaya al, web erişimi engelle, USB kopyalamayışifreleyerek izin ver gibi) veri sızıntılarının dinamik ve proaktif olarakönünegeçmeye olanak sağlayabilmelidir.
2.1.64. Urun içeresindehazır gelen on tanımlı kurallarda bir sihirbaz yardımıylasektörler (örneğin: enerji, finans) ve ülkelerbazında tabi olunan regülasyonlarayönelik (örneğin; KVKK,PCI DSS, GDPR, HIPAA vb.) veri silintisipolitikalarınıhızlıca aktive edebilecek bir özellikolmalıdır.

2.2. Masaüstü Sanallaştırma, Uygulama Sanallaştırma ve Uygulama Kataloğu (210) kullanıcı

2.2.1. Teklif edilen masaüstü sanallaştırma yazılımı masaüstü işletim sistemi olarak Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2 SP1, Windows Server 2012 R2, Windows Server 2016, Ubuntu 12.04-14.04-16.04, RHEL 6.6, 6.7, 6.8, 6.9, 7.2, 7.3, ve 7.4, CentOS 6.6, 6.7, 6.8, 6.9, 7.2, 7.3, ve 7.4, SLED 11 SP3/SP4, SLED 12 SP1/SP2, SLES 12 SP1/SP2 desteklemelidir.
2.2.2. Teklif edilen masaüstü sanallaştırma yazılımı son kullanıcıların sanal masaüstlerine erişmeleri için istemci olarak uyumlu thinclient, zeroclient,

tablet(Windows,iOS,Android), akıllı telefon(iOS,Android), PC(Windows,Linux), Mac(MacOsX) cihazları desteklemelidir.

2.2.3. Teklif edilen masaüstü sanallaştırma yazılımı son kullanıcıların sanal masaüstlerine gerektiğinde hiçbir client yazılımı yüklemeye ihtiyaç olmadan bir HTML5 tarayıcı ile bağlanabilmelerine olanak tanımalıdır. HTML5 üzerinden hem ses hem görüntü iletilebilmelidir.

2.2.4. Teklif edilen masaüstü sanallaştırma yazılımı son kullanıcıların sanal masaüstlerine RDP, PCOIP ve BLAST, BLAST EXTREME protokollerini kullanarak bağlanabilmelerine olanak sağlamalıdır.

2.2.5. Teklif edilen masaüstü sanallaştırma yazılımı son kullanıcıların sanal masaüstlerine bağlanırken kullandıkları band genişliğini ayarlamaya olanak sağlamalıdır.

2.2.6. Teklif edilen masaüstü sanallaştırma yazılımının sunucu modülleri gerektiğinde yedeklilik ve yük dengeleme için birden fazla adet kurulabilmelidir. Bu sunucuların lisansları maksimum adette kurulabilecek şekilde tekliflendirilecektir.

2.2.7. Teklif edilen masaüstü sanallaştırma yazılımı internet üzerinden gelecek kullanıcıların sisteme güvenli bir şekilde kimlik doğrulayıp bağlanmalarını sağlayabilmeli, ssl-vpn gibi bir çözüme ihtiyaç duymadan doğrudan internete açılmaya uygun olmalıdır.

2.2.8. Teklif edilen masaüstü sanallaştırma yazılımı birden fazla ekrana görüntü vermeyi desteklemelidir. Bu ekranlar yüksek çözünürlüklü olabilmelidir.

2.2.9. Teklif edilen masaüstü sanallaştırma yazılımı çift yönlü ses taşınmasına olanak sağlamalıdır. Gerektiğinde ses taşıması için ne kadar band genişliği kullanılacağı ayarlanabilmelidir.

2.2.10. Teklif edilen masaüstü sanallaştırma yazılımı USB üzerinden mikrofon, kulaklık, web kamerası, yazıcı, tarayıcı gibi aygıtların kullanılmasına olanak tanımalıdır.

2.2.11. Teklif edilen masaüstü sanallaştırma yazılımı Active Directory ve Radius kimlik doğrulamasını yöntemlerini desteklemelidir.

2.2.12. Teklif edilen masaüstü sanallaştırma yazılımı RSA Secure ID entegrasyonu sağlayabilmelidir.

2.2.13. Teklif edilen masaüstü sanallaştırma yazılımı 3 boyutlu görüntüleri göstermek adına fiziksel sunucu üzerine takılan uyumlu ekran kartlarını kullanabilmelidir. Bu ekran kartlarının kaynakları gerektiğinde sanal masaüstleri arasında paylaşımlı olarak gerektiğinde ise doğrudan belirli sanal masaüstü bilgisayarlara atanarak kullanılabilmelidir.

2.2.14. Teklif edilen masaüstü sanallaştırma yazılımı storage üzerindeki yükü azaltmak için sanal masaüstlerinin işletim sistemi veya veri disklerinin fiziksel sunucunun belleği üzerine önbelleklenerek kullanılmasına olanak sağlamalıdır.

2.2.15. Teklif edilen masaüstü sanallaştırma yazılımı teklifte belirtilen adette kullanıcı için uygulama sanallaştırma yazılımı da içermelidir. Uygulama sanallaştırma çözümü masaüstü sanallaştırması çözümüne entegre çalışabilmelidir.

2.2.16. Teklif edilen masaüstü sanallaştırma yazılımı istenilen sayıda sanal masaüstlerini tek bir merkezi kopyadan klonlayarak oluşturabilmeli, bu klonlama işlemi sırasında her bir sanal masaüstü bilgisayar için sadece değişen disk alanlarını saklayarak disk alanı kullanımından tasarruf edecek bir teknoloji içermelidir.

2.2.17. Teklif edilen masaüstü sanallaştırma yazılımı, sanal makina imajının, sunucu üzerindeki hafızası içinde (in-memory) klonlanması ile hızlı sanal masaüstü çoklanmasını sağlayabilmelidir.

2.2.18. Teklif edilen masaüstü sanallaştırma yazılımı sanal masaüstlerini klonlarken uyumlu storage üreticilerinin klonlama yöntemlerini kullanabilmelidir.

2.2.19. Teklif edilen masaüstü sanallaştırma yazılımı gerektiğinde istemcilerin arada bir aracı(broker) olmadan doğrudan sanal masaüstü bilgisayarla oturum açabilmelerine izin vermelidir.
2.2.20. Teklif edilen masaüstü sanallaştırma yazılımı son kullanıcı profil verilerini yönetecek bir modül içermelidir.
2.2.21. Teklif edilen uygulama sanallaştırma yazılımı MS terminal server üzerinde çalışan uygulamaları son kullanıcılara verimli bir protokol üzerinden gönderebilmeli ve son kullanıcıların PC, tablet ya da akıllı telefonlarından bağlanıp bu uygulamaları kullanmalarına olanak sağlamalıdır.
2.2.22. Windows uygulamalarını tek bir msi veya exe haline getirebilmelidir.
2.2.23. Bu çözüme uyumlu windows uygulamalarının, farklı versiyonların aynı işletim sistemi içinde eşzamanlı olarak çalışması sağlanmalıdır.
2.2.24. Bu uygulama paketleri çalıştığı işletim sistemi içinde sadece kullanıcı (user) hakları ile çalışabilmelidir.
2.2.25. Active Directory grupları ile entegre çalışabilmelidir.
2.2.26. Sanal masaüstü, uygulama sanallaştırma ve uygulama kataloğu yazılımları ile entegre çalışabilmelidir.
2.2.27. Teklif edilen uygulama kataloğu yazılımının özellikleri aşağıdaki gibi olacaktır.
2.2.28. Teklif edilen uygulama kataloğu yazılımı paylaşılmış uygulamalara pc, akıllı telefon ve tabletlerden erişilmesine olanak sağlamalıdır.
2.2.29. Teklif edilen uygulama kataloğu yazılımı, sanal Windows uygulamaları, SaaS uygulamalar, paketlenmiş windows uygulamaları paylaşılabilmelidir. Teklif edilen uygulama kataloğu yazılımı, Single Sing On (SSO) desteklemelidir
2.2.30. Teklif edilen uygulama kataloğu yazılımı Active Directory ve RSA SecureID kimlik doğrulama desteklemelidir.
2.2.31. Teklif edilen uygulama kataloğu yazılımı masaüstü ve uygulama sanallaştırma yazılımı ile entegre çalışabilmelidir.
2.2.32. Uygulama erişim politikaları (kimlik doğrulama türlerine, uç nokta cihaz platformuna, network aralığına bağlı olarak) yazılabilmeli ve desteklenmelidir.
2.2.33. Teklif edilen yazılımların çalışabilmesi için gereken sanallaştırma yazılımı toplam CPU limiti olmadan masaüstü sanallaştırma yazılımı için oluşturulacak tüm sanal makinaları çalıştırabilecek şekilde lisanslandırılacak ve aşağıdaki özellikleri sağlayacaktır.
2.2.34. Teklif edilen sanallaştırma yazılımı aynı fiziksel sunucu üzerinde oluşturulacak sanal makinaların mevcut sistem kaynaklarının üzerinde kaynak atanmasına (over-commitment) izin vermelidir.
2.2.35. Teklif edilen sanallaştırma yazılımı SMP (Symetric Multi Processing) desteği olmalıdır. Teklif edilen sistemde her bir sanal makinaya istenildiğinde 128 adet sanal CPU atanabilmelidir.
2.2.36. Teklif edilen sanallaştırma yazılımı ile her bir sanal makinaya 6128 GB sanal bellek atanabilmelidir.
2.2.37. Teklif edilen sanallaştırma yazılımı gerektiğinde her bir sanal makine için atanan disk alanın doğrudan disk havuzundan almak yerine, sanal makine diski doldukça büyütebilmelidir. (Thin Provisioning)
2.2.38. Teklif edilen sanallaştırma yazılımı misafir işletim sistemi olarak Windows Xp, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2008R2, Windows Server 2012/2016, Centos, Redhat, Ubuntu, Solaris, MacOSX, FreeBSD desteklemelidir.

2.2.39. Teklif edilen sanallaştırma yazılımı, sanal makinalara verilen disklerin ve sanal makinaların bulunduğu dosya sisteminin sistem çalışırken büyütülmesine izin vermelidir.
2.2.40. Teklif edilen sanallaştırma yazılımı sanal makinalara 62TB boyutunda sanal diskler atanmasına olanak sağlamalıdır.
2.2.41. Teklif edilen sanallaştırma yazılımı 64TB boyutundaki depolama alanlarını yönetebilmelidir
2.2.42. Teklif edilen sanallaştırma yazılımı ile FC, iSCSI ve NFS gibi veri depolama teknolojilerini ve bu teknolojilerle çalışan veri depolama ünitelerini desteklemelidir.
2.2.43. Teklif edilen sanallaştırma yazılımı ile sistemde yetkilendirme yapılabilmeli, belirli operasyonel kişilerin tüm sanal sisteme veya sanal sistemin bir kısmına erişmelerine ve yönetim operasyonlarını gerçekleştirebilmelerine imkan tanımalıdır.
2.2.44. Teklif edilen sanallaştırma yazılımı ile sistem performansı CPU, memory, disk ve network gibi parametreler için anlık veya geçmişe doğru izlenebilmeli, rapor alınabilmelidir.
2.2.45. Teklif edilen sanallaştırma yazılımı tüm sanal sunucuların tek bir merkezden yönetimini sağlayan merkezi yönetim yazılımını içermelidir. (Merkezi yönetim yazılımı lisansları ile teklif edilecektir)
2.2.46. Teklif edilen sanallaştırma yazılımı ile gelen merkezi yönetim yazılımı web arayüzünden bağlanıp yönetmeye olanak sağlamalıdır.
2.2.47. Teklif edilen sanallaştırma yazılımı sanal sunuculara VLAN atanmasına izin vermelidir.
2.2.48. Teklif edilen sanallaştırma yazılımı sanal sunucuların açıkken bir kopyasının çıkarılmasına izin vermelidir.
2.2.49. Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinaları ihtiyaç duyulduğunda paylaşımlı bir disk alanına ihtiyaç duymaksızın sanallaştırma sistemi içindeki başka bir sunucuya aktarabilmeli, bu işlemi aynı anda birden fazla sanal makina için gerçekleştirebilmelidir.
2.2.50. Teklif edilen sanallaştırma yazılımı içerisinde tanımlı sunuculardan birisinde kontrol dışı bir durma olduğunda kapanan sanal makinaların sistemdeki diğer sunucular tarafından otomatik olarak çalıştırılması şeklinde kümeleme hizmeti desteği olmalıdır. Bu hizmet için sanal makinalar arasında önceliklendirme yapılabilmelidir.
2.2.51. Teklif edilen sanallaştırma yazılımı içerisinde çalışan Windows ve Linux sanal makinaların yedeklerini disk ortamına alan bir modülü bulunmalıdır. Bu modül yedeklenmiş verileri tekilleştirme yaparak saklayabilmelidir.
2.2.52. Teklif edilen sanallaştırma yazılımı belirlenen sanal makinaların aynı lokasyondaki veya uzak bir lokasyondaki sanallaştırma sunucuları üzerine replikasyon yapmasına olanak tanımalıdır.
2.2.53. Teklif edilen sanallaştırma yazılımı üçüncü parti antivirus çözümleri ile entegre çalışabilmeli ve ajansız mimari kullanarak sanal makinalar üzerinde virüs taraması yapılmasına olanak sağlamalıdır.
2.2.54. Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinaları diskleri ile birlikte depolama alanları arasında taşıyabilmelidir.
2.2.55. Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinalara CPU, memory, disk ve network kartı eklenmesini desteklemelidir.
2.2.56. Teklif edilen sanallaştırma yazılımı seçilen sanal makinalar için çalıştığı fiziksel sunucuların plansız bir kesinti yaşaması durumunda, kesintisiz olarak diğer fiziksel sunuculardan çalışmasına devam etmesini sağlayabilmelidir.
2.2.57. Teklif edilen sanallaştırma yazılımı fiziksel sunucular üzerindeki memory koruma yöntemleri ile korunmuş memory alanlarını otomatik olarak algılayıp, kritik sistem bilgilerini bu memory alanlarına yazılmasını sağlayacak bir teknoloji içermelidir.

2.2.58. Teklif edilen sanallaştırma yazılımı Hadoop kurulumlarını kolaylaştıracak bir modül içermelidir.
2.2.59. Teklif edilen sanallaştırma yazılımı sanal sunucuların serial port konsoluna network üzerinden bağlanılmasına olanak tanımalıdır.
2.2.60. Teklif edilen sanallaştırma yazılımı sanal makinaların iş yüklerini sürekli izleyip gerek görmesi durumunda fiziksel makinalar üzerindeki iş yükü dağılımını ayarlamak için sanal makinaları otomatik olarak sisteme dahil fiziksel sunucular arasında taşıyabilmelidir. Bu işlemin yapılması istenirse tam otomatik olarak, istenirse de sistem yöneticisine tavsiye şeklinde bilgi vererek gerçekleşebilmelidir.
2.2.61. Teklif edilen sanallaştırma yazılımı fiziksel sunucular üzerinde yük dengelemesi yaparken istenildiğinde yoğun çalışmayan fiziksel makinaların üzerindeki yükü diğerleri üzerine taşıyıp, boşa çıkan fiziksel makinaları elektrik tasarrufu etmek amacıyla kapatılmasına olanak tanımalıdır. Ayrıca ihtiyaç olduğunda kapana fiziksel sunucular tekrar açılabilmelidir.
2.2.62. Teklif edilen sanallaştırma yazılımı depolama ünitesi üzerinde yapılan vm klonlama veya taşıma gibi işlemler sırasında ilgili işlemin iş yükünü depolama ünitesine yükleyerek yapılmasını sağlayabilmelidir.
2.2.63. Teklif edilen sanallaştırma yazılımı üçüncü parti firmaların ürettiği multi-pathing yazılımlarına destek vermelidir.
2.2.64. Teklif edilen sanallaştırma yazılımı depolama alanlarının doluluk oranlarını ve gecikme(latency) değerlerini izleyip, gerektiğinde sanal makinaları daha müsait depolama alanları üzerine otomatik olarak taşıyabilmelidir.
2.2.65. Teklif edilen sanallaştırma yazılımı disk ve network kullanımını sanal makina bazında önceliklendirebilmeli, seçilen sanal makinaların diğer sanal makinalara göre daha fazla disk ve network I/O kaynağı kullanabilmesini sağlayabilmelidir.
2.2.66. Teklif edilen sanallaştırma yazılımı 10Gbit PCI express kartların mantıksal olarak bölünerek, her bir parçasının sanal makinalara doğrudan kullandırılmasına olanak tanımalıdır.
2.2.67. Teklif edilen sanallaştırma yazılımı sanal makinalarda çalışan belirli uygulamalar üzerinde meydana gelebilecek servis kesintilerini tespit edip, gerektiğinde ilgili servisi yada sanal makinayı yeniden başlatarak sorunu düzeltebilecek bir modül içermelidir.
2.2.68. Teklif edilen sanallaştırma yazılımı PVLAN, LACP, Netflow, ERSPAN, Port Mirroring, ACL, CoS Tagging, DSCP Tagging gibi network servislerine destek verebilen ve tek merkezden yönetilebilen bir network çözümü içermelidir.
2.2.69. Teklif edilen sanallaştırma yazılımı fiziksel sanallaştırma sunucuları üzerindeki tüm ayarların merkezi bir şablon olarak hazırlanıp yapıdaki tüm sunuculara tek seferde uygulanmasına olanak sağlamalıdır.
2.2.70. Teklif edilen sanallaştırma yazılımı gerektiğinde fiziksel sunucular üzerine sabit disk takılmasına gerek kalmadan, networkten boot edip çalışabilmelidir.
2.2.71. Teklif edilen sanallaştırma yazılımı fiziksel sunucular üzerindeki SSD diskleri istenilen sanal makinalar için okuma önbelleği (read-cache) olarak kullanabilmelidir.
2.2.72. Teklif edilen yazılımlarla birlikte sanal depolama yazılımı lisansları da verilmelidir.
2.2.73. Sanal veri depolama yazılımı, herhangi bir ek bileşen kullanmadan sanallaştırma katmanının yetenekleri ile dağıtık veri depolama sistemi kurabilme özelliğine sahip olmalıdır.
2.2.74. Sanal veri depolama yazılımı, fiziksel sunucuların lokal disklerini istenirse hibrit (SSD ve SAS), istenirse de tamamını SSD diskler kullanarak olmak üzere kullanabilmelidir.
2.2.75. Sanal veri depolama yazılımı, tüm kurulum yönetimini sunucu sanallaştırma yönetim yazılımı üzerinden yapabilmelidir.

2.2.76. Sanal veri depolama yazılımı, yeni tip DIMM based SSD ve NVMe SSD diskleri desteklemelidir.
2.2.77. Sanal veri depolama yazılımı, tekilleştirme, sıkıştırma, RAID5/6 özelliklerine sahip olmalıdır.
2.2.78. Sanal veri depolama yazılımı, IPv4 ve IPv6 desteğine sahip olmalıdır.
2.2.79. Sanal veri depolama yazılımı, sunucu sanallaştırma katmanında yapılan replikasyon özelliğini desteklemelidir.
2.2.80. Sanal veri depolama yazılımı, tüm sağlık, hata ve performans bilgisini sunucu sanallaştırma yönetim yazılımı üzerinden gösterebilme özelliğine sahip olmalıdır.
2.2.81. Teklif edilen masaüstü sanallaştırması yazılımının kapasite ve performans değerlerini izleyip analiz edecek, aşağıdaki özelliklerde bir modülü bulunmalıdır.
2.2.82. Performans izleme yazılımı disk, bellek, cpu ve network kaynaklarına göre performans izlemesi yapabilmelidir.
2.2.83. Performans izleme yazılımı sistem kaynak kullanım eğrisini öğrenerek otomatik olarak kaynak kullanımı için adaptif eşik tanımlamaları yapabilmeli ve kaynak kullanımını bu alt eşiğin altına veya üst eşiğin üstüne çıktığında alarm verebilmelidir.
2.2.84. Performans izleme yazılımı gerektiğinde sistemdeki alarm, hata veya uyarıları kaynak kullanım grafikleri ile ilişkilendirerek performans sorununa neden olabilecek olayları tespit edebilmelidir.
2.2.85. Performans izleme yazılımı kendi veritabanına sahip olmalı, üçüncü parti bir veritabanına ihtiyaç duymamalıdır.
2.2.86. Performans izleme yazılımı sistemdeki tüm sanal makinaları izleyerek sanal makinalara atanan kaynak miktarlarının doğru olup olmadığını kontrol edebilmeli, bu konuda iyileştirmeler yapabilmek için tavsiyelerde bulanabilmelidir.
2.2.87. Performans izleme yazılımı masaüstü sanallaştırma ürününe entegre olarak, sanal masaüstü, hypervisor, ağ, depolama cihazları ve iletişim protokolü dahil tüm katmanlarda izleme ve analiz yapabilmelidir ve masaüstü sanallaştırma ürünene özel hazır dashboard'lar sunabilmelidir.
2.2.88. Teklif edilen masaüstü sanallaştırması çözümü beraberinde sanal masaüstlerine anında uygulama dağıtmayı destekleyecek bir uygulama sanallaştırma ve dağıtım çözümü bulunmalıdır.
2.2.89. Anında uygulama dağıtım çözümü Windows uygulamalarının teker teker yada gruplar halinde oluşturularak, son kullanıcı masaüstlerine Active Directory'deki kullanıcı hesabı, bilgisayar hesabı, OU ya da gruop bilgisine göre atanmasına izin vermelidir.
2.2.90. Uygulama dağıtırken, uygulama dosyalarını ağ üzerinden taşımak yerine disk altyapısını kullanmalı, büyüklüğünden bağımsız olarak uygulamaları saniyeler içinde kurabilmelidir.
2.2.91. Kendi sanal bilgisayarında oturum açmış kullanıcıların, oturumlarını kapatıp açmadan yeni gelecek uygulamaları kullanmalarına imkân sağlamalıdır.
2.2.92. Kullanıcıların havuzdan herhangi bir bilgisayarı seçip kullandığı (stateless vdi) senaryoda bile kullanıcıların kurdukları uygulamaları ve oluşturdukları dosyaları algılayarak, bundan sonra login olacakları bilgisayarlara taşıyabilmelidir.
2.2.93. Teklif edilen masaüstü sanallaştırma yazılımı son kullanıcı profillerini ve kurumsal politikaları yönetecek bir modül içermelidir. Bu modül, aşağıdaki özellikleri desteklemelidir:
2.2.94. Kullanıcı bazlı olarak uygulama ayarlarının önceden tanımlanmış ayarlar olarak gönderilmesini merkezi bir yönetim arayüzü ile desteklemelidir.
2.2.95. Değişen uygulama ayarlarını kullanıcı bazlı olarak tutabilecek, istenildiğinde daha önce belirlenen uygulama ayarları zorlanabilmelidir.

2.2.96. Yazılan politikalar, son kullanıcı IP'sine, uç nokta cihazının ismine, platform bilgisine, group üyeliğine vb faktörlere bağlanabilmelidir.

2.2.97. Kullanıcı bazlı olarak, istenilen Windows kullanıcı policy'ler (User ADMX) yönetilebilmelidir.

2.2.98. Kullanıcı bazlı olarak sanal uygulamaların çalıştığı işletim sistemi içinde istenilen uygulamaların bloklanmasını desteklemelidir.

2.2.99. Registry ayarlarının yapılması, Ağ sürücüsü (network drive) bağlanması, dosya tipini belirleme (file type association=, dosya yönlendirme (folder rediction), logon/logoff task'ları oluşturma, yazıcı tanımlarının dinamik olarak yapılması özelliklerini desteklemelidir.

2.2.100. Standard kullanıcının "yönetici" (runas admin) hakları ile istenilen uygulamaları çalıştırmasını desteklemelidir.

2.2.101. Yönetilen ayarların, kullanıcının mevcut oturumu kesmesi veya tekrar oturuma bağlanması koşullarında yenilenmesini desteklemelidir.

2.2.102. Bağlantı ayarlarının dinamik olarak kullanıcı bazlı olarak ayarlanmasını, belirtilen şartlara göre (AD site ismi, son kullanıcı cihazının IP'si, uc nokta cihazın ismi, platformu, zaman aralığı vb) usb, yazıcı, clipboard, sürücü yönlendirme (drive redirection), html erişim ve bandwidth ayarlarının dinamik olarak yönetilmesini sağlamalıdır.

2.2.103. Teklif edilen çözüme ait lisanslar ile birlikte en az 1 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 1 yıl boyunca 5 gün 9 saat (hafta içi mesai saatleri içinde) destek hizmeti verilmelidir.

2.2.104. Sistem yönetim personeli ilgili yazılımın üreticisine herhangi bir aracıya ihtiyaç duymadan doğrudan çağrı açabilmeli ve doğrudan destek alabilmelidir.

2.3. Sunucu (1) Adet

2.3.1. **SUNUCU SİSTEMLERİ (1 Adet)**

İşlemci

2.3.2. Her bir işlemci 64-bit komut setini desteklemelidir.

2.3.3. Sunucu üzerinde en az 2 adet, en az 2.6 GHz çalışma hızında fiziksel işlemci olmalıdır.

2.3.4. Her bir işlemci en az 16 çekirdekli olmalıdır. Sunucuda toplam olarak en az 40 çekirdek olmalıdır.

2.3.5. Her bir işlemci üzerinde en az 22 MB L3 önbellek bulunmalıdır.

Ana Bellek

2.3.6. Sunucu üzerinde kullanılan her bir bellek PC4, DDR4 olacaktır.

2.3.7. Sunucu üzerinde her biri 2666MT/s, en az 32 GB kapasitesinde olan, toplamda en az 768 GB bellek bulunacaktır.

2.3.8. Sunucu üzerinde en az 24 adet bellek yuvası bulunacaktır.

2.3.9. Teklif edilecek sunucu RDIMM, LRDIMM ve NVDIMM bellek tipini desteklemelidir ve sunucu üzerinde en az 24 adet bellek yuvası bulunmalıdır. Sunucunun 1.5TB'a kadar toplam bellek desteği bulunmalıdır. Bellek modülleri ECC (Error Check Correction) özelliğinde olacaktır.

Disk Birimleri

2.3.10. Sunucu için en az 2 adet, her biri en az 240 GB kapasiteli, SATA SSD teknolojisinde diskler verilmelidir. Diskler çalışma esnasında sökülüp takılabilmelidir.

2.3.11. Teklif edilecek sunucu üzerinde elektrik kesilmesine karşı pil korumalı korumalı üzerinde en az 2 GB uçucu olmayan bellek bulunan RAID denetleyicisi bulunmalıdır.

RAID kartı donanımsal olarak RAID 0/1/5/10/50/60 yapabilme yeteneğine sahip olmalıdır.

2.3.12. Sunucu üzerinde en az 8 adet 2.5 inch disk yuvası bulunacaktır.

Ağ Kartı (Ethernet Kartı)

2.3.13. Her bir sunucu üzerinde en az 1 adet 10/100/1000Mbps hızında uzaktan erişim ve yönetim sağlayacak arabirimi olmalıdır.

2.3.14. Her bir sunucu üzerinde en az 1 adet Dual port 10Gb SFP+ Ethernet port bulunmalıdır. Portlar ile birlikte 2 adet 10Gb SR modüller takılı olarak gelecektir. Modüller üretici marka ile aynı olmalıdır.

2.3.15. Her bir sunucu üzerinde en az 2 adet Single port 16Gb FC HBA kart bulunmalıdır. Portlar ile birlikte 2 adet FC modül takılı olarak gelecektir. Modüller üretici marka ile aynı olmalıdır.

Diğer Özellikler

2.3.16. Sunucu için gerekli PDU ve kabloları ile birlikte daha önce kullanılmamış olarak teslim edilecektir.

2.3.17. Her bir sunucu üzerinde çalışma esnasında sökülüp takılabilen; en az 2 adet, herbiri 750W gücünde yedekli güç kaynağı bulunmalıdır. Sunucu üzerine gerektiğinde en az 2 adet, herbiri 2400W gücünde yedekli güç kaynağı takılabilmelidir.

2.3.18. Her bir sunucu için, çalışma esnasında sökülüp takılabilen en az 6 adet yedekli ve teklif edilen sistemin tüm fan yuvaları dolu olacak şekilde fanlar takılı bulunmalıdır.

2.3.19. Sunucuda Trusted Platform Module 2.0 (TPM 2.0) desteği bulunmalı ve gerekli lisanslar ile teklif edilmelidir.

2.3.20. Teklif edilecek sunucu üzerinde 2 adet VGA portu, en az bir adet DB9 RS232 portu, 2 adeti arka tarafta, 2 adeti ön tarafta ve 1 adedi dahili olmak üzere toplam 5 adet USB portu bulunmalıdır.

2.3.21. Teklif edilecek sunucu üzerinde en az 1 adeti PCIe Gen3 x16 stekleyen en az 4 adet PCIe slotu bulunmalıdır.

2.3.22. Sunucular üzerine, Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi işletim sistemleri kurulabilecektir.

2.3.23. Teklif edilecek sunucu üzerinde embedded olarak en az 16MB belleğe sahip ve en az 1920*1200 çözünürlüğü destekleyen grafik kartı bulunmalıdır.

2.3.24. Sunucu üzerinde fiziksel müdahaleleri engelleyebilmek için kilitlenebilir ön kapak bulunmalıdır.

2.3.25. Teklif edilen sunucu üzerinde sistem kurulumu için gerekli dosyalar embedded olmalıdır ve herhangi bir disk, sürücü'ye ihtiyaç olmadan embeded sistem üzerinden sistem kurulabilmelidir.

2.3.26. Sunucu üzerinde HTTPS ve SSLv2 sertifika ile erişim sağlayacak kendine ait 1 Gb hızında fiziksel bağlantı noktasına sahip uzaktan yönetim modülü bulunmalıdır.

2.3.27. Sunucu ön panelinde bulunan USB portlardan bir adeti uzaktan yönetim portu tarafından erişilebilmeli, sunucu kapalı olduğu esnada bu port üzerinden takılabilecek USB bellek ile firmware güncellemesi veya provizyonlama yapılabilmeli ve uzaktan yönetim networkünün kurulu olmadığı veya çalışmadığı esnada USB kablo ile bir bilgisayara bağlayarak uzaktan yönetim web ara yüzüne erişilebilmelidir.

2.3.28. Uzaktan yönetim modülünün HTML5 desteği olmalı ve herhangi ajan, eklenti yüklenmeden modern web sunucuları yönetilmeli, uzaktan KVM erişimi yapılabilmeli, uzaktan medya bağlantısı yapılarak işletim sistemi kurulabilmeli ve güncellemeler yapılabilmelidir.

2.3.29. Sunucular sanal medya özelliğini desteklemelidir, uzaktaki bir bilgisayara bağlı USB bellek, CD, DVD, vb. medyaları kullanabilmelidir.

2.3.30. Uzaktan yönetim modülü sunucu RAID kartının yönetimini gerçekleştirebilmeli, sunucuya sonradan eklenecek disklerin RAID yapılandırmasını yapabilmeli ve mevcut RAID guruplarına disk eklemesi yaparak kapasitesini artırılmasını sağlayabilmelidir.

2.3.31. Sunucu, üzerine yüklenecek BIOS, firmware vb dosyalarının sertifika vasıtası ile güvenliğini ve orijinalliğini kontrol edebilmeli, sunucu üzerinde, güvenlik sertifikalarının saldırılara karşı korunmasını sağlayan, uçucu olmayan güvenli bir bellek alanı bulunmalıdır.

2.3.32. Teklif edilecek sunucun kabinete konumlandırılması için gerekli ekipmanlar ile teklif edilmelidir.

2.3.33. Teklif edilecek sunucunun istenildiğinde cep telefonu veya tablet üzerinden erişim ve yönetim desteği olmalıdır.

2.3.34. Sunucu ile beraber verilen bütün komponentler sunucu üreticisi tarafından üretilmiş veya sunucu üreticisi tarafından onaylanarak tedariki sunucu üreticisi tarafından yapılmış olmalı ve üreticiye ait bir portal üzerinden sunucunun güncel konfigürasyonu sorgulanabilmeli, sunucu garantisi, sunucu üzerinde gelen bütün komponentleri kapsamalıdır.

2.3.35. 220 V AC ve 50 Hz tek veya üç faz enerji beslemesi ile şehir şebekesinde çalışacaktır. Enerji girişi için besleme kablo fişleri mevcut kabinler içerisindeki güç dağıtım ünitelerine uygun tipte olacaktır.

2.3.36. Sunucular en az 3 yıl boyunca ertesi iş günü üretici garantisine sahip olacaktır.

2.4. Yedekleme Yazılımı (8 Cpu Yenileme + 2 Cpu Yeni Lisans) (1) Yıl

2.4.1. Yazılım Vmware vSphere (4.1, 5.x ve 6.x) ve Microsoft Hyper-V (2008R2, 2012, 2012R2, 2016) sanallaştırma platformlarında çalışan sanal makinaların yedeklemesini, replikasyonunu, proaktif olarak izlenmesini ve raporlanmasını herhangi bir ajan kurulumu gerektirmeden, imaj seviyesinde ve uygulama tutarlı olarak yapabilmelidir.

2.4.2. Yazılım, yedekleri saklamak için Windows, Linux, CIFS/SMB dosya paylaşımlarını ve üzerinde dahili tekilleştirme sunan cihazları kullanabilmelidir.

2.4.3. Yazılım HPe ve DellEMC tekilleştirme ünitelerinin lisanslı (Boost ve Catalyst) eklentileri ile entegre çalışabilmeli ve tekilleştirmenin bir kısmını kaynakta yaparak ağ üzerinden geçen trafiği ve diskteki yükü azaltmalı ve yedekleme sürelerini kısaltmalıdır.

2.4.4. Yazılım tanımlanmış 3 farklı yedekleme deposunu tek bir 'büyütülebilen yedek deposu' olarak kullanarak disk alanı yönetimini basitleştirmelidir.

2.4.5. Yazılım bir yedekleme görevi içindeki her sanal makina için ayrı ayrı tam ve artımlı dosya zincirleri oluşturabilmelidir.

2.4.6. Yazılım herhangi bir ajan kurulumu gerektirmeden kullanıcı tarafından özelleştirilebilen veya devre dışı bırakılabilen dahili sıkıştırma ve tekilleştirme sunmalıdır.

2.4.7. Yazılım artımlı yedekler için hipervizörlerin sunduğu Değişen Blok Takibi (CBT) özelliğini kullanmalıdır.

2.4.8. Yazılım yedeklerin saklandığı diskte bulunan tam ve artımlı yedekleri kullanarak yeni tam yedekler oluşturabilmelidir.

2.4.9. Yazılım ile yedeklenmesi istenmeyen sanal diskler ile NTFS dosya sistemlerindeki dosya ve klasörler seçilerek; geçici dosyalar ve silinmiş öğelere ait disk blokları tespit edilerek yedekleme ve replikasyon işlemi dışında bırakılabilmelidir.

2.4.10. Yazılım yedekleme ve replikasyon için sanal makina verisini doğrudan Veri Depolama ağı üzerinden, Ağ üzerinden veya Hipervizör I/O platformu üzerinden aktarma seçenekleri sunmalıdır.
2.4.11. Yazılım saklanan yedekleri ve ağ trafiğini uçtan uca (kaynakta, aktarırken ve depolarken) AES256bit şifreleyebilmeli ve kayıp şifre koruması sunmalıdır.
2.4.12. Yazılım diskte bulunan yedekleri replikasyon kaynağı olarak kullanarak geri dönüş noktalarını yedeklerden oluşturabilmelidir.
2.4.13. Yazılım görevlerin kullanabileceği network bant genişliğini, eş zamanlı çalışacak görev sayısını, yedek diskine aynı anda yazılabilecek kanal sayısı ve veri oranını yöneticinin istediği değerlerde limitleyebilmelidir.
2.4.14. Yazılım kaynak Sanal Makinaların bulunduğu disk alanlılarındaki I/O gecikmelerini izleyebilmeli ve kullanıcı tarafından belirtilen değer aşıldığında o disk alanı üzerinde bir yedekleme veya replikasyon görevi başlatmamalı ve çalışan ortam performansının olumsuz etkilenmesi engellenmelidir.
2.4.15. Yazılım bir disk alanına alınmış yedeklerin tamamını veya sadece içerisinden seçilen belirli Sanal Makinaların yedeklerini ikincil bir disk alanına; yedeğin kopyalanması veya uzun dönem arşivlenmesi (GFS) amacı ile otomatik olarak kopyalayabilmeli, periyodik doğrulama ve hata giderme yapabilmelidir.
2.4.16. Yazılım bir disk alanına alınmış yedekleri ve Windows veya Linux sunucular içerisinden dosyaları teyp ünitelerine, teyp kütüphanelerine ve Sanal Teyp Kütüphanelerine arşivleyebilmeli, teyp üzerindeki dosya ve yedek dönüş noktalarının takibini yapabilmelidir.
2.4.17. Yazılım teyp medya havuzlarının birden fazla teyp kütüphanesi üzerinde oluşturulabilmesini, teypleri paralel kullanabilmeyi ve teyp havuzları üzerinde GFS arşivlemeyi desteklemelidir.
2.4.18. Yazılım teybe yedeklenmiş bir sanal makinanın doğrudan ana sunucu üzerine geri yüklenmesini desteklemelidir.
2.4.19. Yazılım üretici onaylı bir bulut servis sağlayıcı tarafından sunulan Bulut üzerinde disk hizmetini, yedeklerin saklanacağı bir yedek deposu olarak tanımlayabilmeli, yedeklerini veya yedek kopyalarını bu alana gönderebilmelidir.
2.4.20. Yazılım üretici onaylı bir bulut servis sağlayıcı tarafından sunulan Bulut üzerinde Sanal Ana Sunucu hizmetini, replikasyon hedef ana sunucusu olarak tanımlayabilmeli ve sanal makina replikasyonu yapabilmelidir.
2.4.21. Yazılım daha az ağ bant genişliği kullanarak yedekleri üretici onaylı bir bulut yapısındaki ikinci bir disk alanına kopyalamak veya replikasyonu yapabilmek için dahili WAN Hızlandırıcı sunmalıdır.
2.4.22. Yazılım Microsoft SQL ve Oracle sunucuların içerisinden ajan kullanmadan belirtilen disk alanına ve yedekleme görevinin zamanlama ayarlarından bağımsız frekanslarda 'Transaction Log' yedeği alabilmelidir.
2.4.23. Yazılım diske alınan her yedeği otomatik olarak doğrudan yedek dosyasından izole bir ortamda çalışır hale getirerek, işletim sistemi, hipervizör servisi ve uygulama seviyesinde test ederek bunu rapor olarak ilgili kullanıcılara gönderebilmelidir.
2.4.24. Yazılım bir veya birden fazla Sanal Makinayı doğrudan yedek dosyasından noktasından, izole bir ortamda kullanıcının belirleyeceği sıra ve kaynak ile çalışır hale getirerek test, hata tespiti veya eğitim amaçlı kullanılmasını sağlamalıdır.
2.4.25. Yazılım replike edilmiş bir Sanal Makinayı istenilen geri dönüş noktasından, önceden tanımlanmış Sanal Ağ ayarları ile çalışır duruma getirebilmelidir.
2.4.26. Yazılım replike edilmiş Microsoft Windows işletim sistemine sahip bir Sanal Makinayı istenilen geri dönüş noktasından, önceden tanımlanmış IP ayarları ile çalışır duruma getirebilmelidir.

2.4.27. Yazılım veri kaybı olmadan veri merkezi taşımasını organize edecek Planlı Taşıma özelliği sunmalıdır.
2.4.28. Yazılım bir veri merkezi kesintisi sırasında tek tuşla tüm sanal makinaları tanımlanan sırayla çalışır hale getirebilecek bir Kurtarma Planı hazırlama özelliği sunmalıdır.
2.4.29. Yazılım bir sanal makinayı doğrudan diskte bulunan tam veya artımlı yedek dosyasından ilave bir kopyalama veya müdahaleye gerek kalmadan çalışır duruma getirebilmelidir.
2.4.30. Yazılım bir sanal makinayı tam veya artımlı yedek dosyasından orijinal yerine veya başka bir ana sunucu üzerine geri yükleyebilmelidir.
2.4.31. Yazılım bir sanal makinanın sadece ana sunucu üzerindeki dosyalarını geri yükleyebilmelidir.
2.4.32. Yazılım bir sanal makinanın sadece seçilen sanal disklerini geri yükleyebilmelidir.
2.4.33. Yazılım geçerli bulut hizmetleri abonelik bilgileri sağlandığında, bir sanal makinayı doğrudan Microsoft Azure ortamına geri yükleyebilmelidir.
2.4.34. Yazılım sanal makinaya herhangi bir ajan/servis kurulumu gerektirmeden, sanallaştırma platformunun desteklediği tüm işletim sistemlerinden, sunucunun tamamını geri yüklemeye gerek kalmadan sadece istenilen klasör veya dosyaları arama, bulma, dışa aktarma ve geri yüklemesini yapabilmelidir.
2.4.35. Yazılım sunucuya bir ajan/servis kurulumu gerektirmeden, Microsoft Active Directory, Microsoft Exchange, Microsoft SQL, Microsoft Sharepoint ve Oracle yedekleri içerisinden uygulama öğelerini ve veri tabanlarını orijinal yerine geri yükleyebilmeli veya dışarı aktarabilmeli, bu işlemi yedeklerden, replikalardan ve yedek kopyalarından gerçekleştirebilmelidir.
2.4.36. Yazılım PostgreSQL, MySQL dahil her türlü sanallaştırılmış uygulamadan uygulamaların yönetim araçlarını kullanarak obje bazlı kurtarma yapabilmek için sanal makinayı doğrudan yedek dosyasından izole bir ortamda açarak kullanıcı erişimine sunabilmelidir.
2.4.37. Yazılımın Web uygulaması kullanılarak yedekler içerisinden Sanal Makinaların ve Dosyaların geri yüklemesi yapılabilmelidir.
2.4.38. Yazılımın Web uygulaması kullanılarak yedekler içerisinden Microsoft Exchange 2010, 2013, 2016 posta kutuları ve SQL Veritabanları geri yüklenebilmelidir.
2.4.39. Yazılım sanal makinaları ana sunucu ve disk alanları üzerinde taşıma özelliği sunmalıdır.
2.4.40. Yazılım kendi konfigürasyon yedeğini herhangi bir kullanıcı müdahalesi gerekmeden tanımlı disk alanına alabilmeli ve tüm ayarları ve tanımlamaları içerecek şekilde geri yüklenebilmelidir.
2.4.41. Uzak ofislerde ve uç noktalarda yedekleme ve kurtarma işlemleri için uzak nokta etkileşim proksi sunucusu ve yükleme sunucuları kullanılabilmelidir.
2.4.42. Yazılım dahili komut satırı (PowerShell) Desteği sunmalıdır.
2.4.43. Yazılımın yönetim konsolu 64 bit bir Microsoft Windows işletim sistemine sahip herhangi bir fiziksel veya sanal, sunucu veya kişisel bilgisayar üzerinde, çoklu kullanıcı ve sunucu/istemci modeli ile çalışmalıdır.
2.4.44. Yazılımın tüm bileşenleri Microsoft Windows Server 2016 üzerine kurulabilmeli ve tüm özellikleriyle desteklenmelidir.
2.4.45. Yazılım yeni versiyon ve güncellemeleri yayınlandığında konsolda uyarıda bulunmalı ve yöneticiyi ilgili indirme sayfasına yönlendirmelidir.
2.4.46. Yazılım ile Vmware vSphere ve Microsoft Hyper-V sanal platformlarındaki ana makine, sanal makine ve veri depoları için 7x24 gerçek zamanlı ve geçmişe dönük izleme, raporlama, kapasite planlama ve uyarı sistemi sunmalıdır.

2.4.47. Yazılım, geçmişe dönük performans ve alarm verilerinin saklanması için gerekli veritabanını kurulum esnasında otomatik olarak yüklemelidir.
2.4.48. Yazılım, istenildiği takdirde harici bir Microsoft SQL veri tabanını da kullanabilmelidir. SQL 2008, 2008 R2, 2012, 2014 ve 2016 versiyonları ve MS SQL Always-on mimarisi desteklenmelidir.
2.4.49. Yazılımın konsol, veritabanı ve web sunucusu bileşenleri aynı sunucu üzerine veya yapının büyüklüğüne göre farklı sunucular üzerine kurulabilmelidir.
2.4.50. Yazılım vmware ortamlarında vcenter üzerinde tanımlanmış kullanıcı erişimlerine göre kullanıcılara sadece yetkileri olan bölümlerde izleme ve raporlama sunabilmelidir.
2.4.51. Yazılım, Microsoft Windows tabanlı sanal makinaların işletim sistemlerine ayrı bir araç ile ulaşmaya gerek kalmadan yürüttüğü işlemleri görüntülemeli, yönetmeli ve konsol erişim sağlamalıdır.
2.4.52. Yazılım, Sanal altyapı ağacındaki her nesne için, nesnenin yapısına uygun olarak tasarlanmış özet bir kontrol paneli sağlamalıdır. Yazılım ile her nesne için en kullanışlı bilgilere hızlıca göz atılabilmeli ve istenirse daha detaylı verilere de aynı ekrandan ulaşılmalıdır.
2.4.53. Yazılım, disk hacmi, disk sorunları, disk alanı kullanımı, veri deposu görüntüleme de dahil tam bir veri depolama görüntülemesi sağlamalıdır.
2.4.54. Yazılım sanallaştırma altyapı bileşenleri ile ilgili önceden tanımlanmış, kategorize edilmiş ve kurulum tamamlandığında kullanıcı müdahalesi gerektirmeden çalışmaya başlanan hazır alarmlar sunmalıdır.
2.4.55. Yazılım, sanallaştırma sunucusu, sanal makinalar ve veri depolarında oluşabilecek sorun ve darboğazları tespit edip alarmlar üretmeli, önceden tanımlanmış kişi ve gruplara e-posta olarak iletebilmeli ve tanımlanmış programları çalıştırmalıdır.
2.4.56. Yazılım, tespit ettiği sorun ve darboğazların tanımını, nedenlerini ve çözümü için önerilen yöntemleri görüntülemeli, ayrıca vmware ve microsoft'un internet kaynaklarında sorun ile ilgili makaleye doğrudan link vererek yönlendirme yapmalıdır.
2.4.57. Yazılım içerisindeki tüm alarmların tanımları, eşik değerleri, etkin oldukları altyapı alanı, etkin olacağı zaman aralığı ve alarm durumunda alınacak aksiyonlar özelleştirilebilmelidir.
2.4.58. Yazılım içerisindeki tüm alarmların eşik değerlerinin doğru belirlenebilmesi için geçmiş performans değerlerini kullanarak alarm modelleme özelliği sunulmalıdır
2.4.59. Yazılım, yedekleme, snapshot, vmotion gibi sanal sunucu, ana sunucu veya disk üniteleri üzerinde ilave yük oluşturan sistem faaliyetleri sırasında alarmları devre dışı bırakabilme özelliği sunmalıdır.
2.4.60. Yazılım kapasite planlama özelliği sayesinde sunucu, işlemci, bellek, disk, ağ gibi kritik sistem kaynaklarının geleceğe dönük kullanım ömrü hakkında ayrıntılı raporlar verebilmelidir.
2.4.61. Yazılım içerisinde sık kullanılan ve tecrübelere dayalı olarak önceden tanımlanmış ve her biri özelleştirilebilen raporlar ve rapor şablonları bulunmalıdır.
2.4.62. Yazılım içerisindeki tüm raporlar istenilen sıklıkta zamanlanarak ilgili kişi veya gruplara, paylaşım ve portallere otomatik olarak gönderilebilmelidir.
2.4.63. Yazılım içerisindeki her bir raporun kapsamı ortamdaki en küçük objeden başlayarak disk alanlarına, sunuculara, kümelere, gruplara, veri merkezlerine ve sanal ortamın tamamına kadar büyütülebilmeli ve her rapor için bağımsız olarak bu kapsam tanımlanabilmelidir.
2.4.64. Yazılım içerisinde sık kullanılan ve tecrübelere dayalı olarak önceden tanımlanmış ve her birinin içeriği ve formatı özelleştirilebilen özel konsollar (Dashboard'lar) bulunmalıdır.

2.4.65. Yazılım içerisindeki her bir konsola bağımsız olarak ağ üzerinden veya portal sunucularından erişmekiçin direkt URL Link vermelidir.
2.4.66. Yazılım içerisindeki her bir konsolun (dashboard) her bir öğesinin (widget) kapsamı ortamdaki en küçük objeden başlayarak disk alanlarına, sunuculara, kümelere, gruplara, veri merkezlerine ve sanal ortamın tamamına kadar büyütülebilmeli ve her rapor için bağımsız olarak bu kapsam tanımlanabilmelidir.
2.4.67. Yazılım tüm nesneleri ister fiziksel altyapı odaklı ister kategori odaklı görüntüleyebilmelidir. Tüm raporlar ve konsollar ister fiziksel ister iş odaklı objeler üzerinden düzenlenebilmelidir.
2.4.68. Yazılım kategorilerinin ve alt kriterlerinin kullanıcı tarafından herhangi bir sayı sınırlaması olmadan düzenlenmesine olanak sağlamalıdır.
2.4.69. Yazılım veri tabanında sakladığı geçmiş performans verilerini kullanarak sanal altyapı üzerindeki tüm nesneler için trend analizi yapmalıdır.
2.4.70. Yazılım veri tabanında sakladığı geçmiş performans verilerini kullanarak, koşul/aksiyon analizi yapmalıdır. Örneğin sanal ortamdaki bir fiziksel ana sunucuda sorun oluşması durumunda sistemin geri kalanının nasıl çalışacağını veya bu durumda ne kadar ilave kaynak sağlanması gerektiğini raporlamalıdır.
2.4.71. Yazılım sanallaştırma sunucusu ve sanal makinaların kaynak kullanımını tanımlanan gruplara göre raporlama ve ücretlendirme yapmalıdır.
2.4.72. Yazılım, Yedekleme altyapısının bileşenleri için gerçek zamanlı izleme sunmalıdır.
2.4.73. Yazılım, Yedekleme altyapısının bileşenleri için kullanım ve kapasite planlama raporları sunmalıdır.
2.4.74. Yazılım, sanal altyapıda bulunan tüm sanal makinalar için, bu sunucuların ilk ve son yedeklenme ve replikasyon tarihlerini, geri dönüş nokta sayılarını, hangi görev içinde korunduklarını içeren kapsamlı bir korunma raporu sunabilmelidir.
2.4.75. Yazılım konsolu üzerinden sanal makinaları işletim sistemi içinden kapatma, açma ve direkt kapama işlemleri yapılabilmelidir.
2.4.76. Sanal Altyapı içerisindeki her öğe ile ilgili tüm raporlara ayrı bir arayüzü gerek olmaksızın doğrudan konsol içerisinden erişim sağlanabilmelidir.
2.4.77. Yazılım yedekleme ücretlendirmesi özelliği sunabilmelidir.
2.4.78. Yazılım sanal altyapı içerisindeki sanal makinaları, sağlıklı yedeklemeyi engelleyecek (disk boyutu, açık snapshot, vmware veya hyperv araçlarının güncelliği vb) faktörleri denetleyerek uygun olmayanları raporlayabilmelidir.
2.4.79. Yazılım, sanal sunucularda günlük değişen veri miktarını hesaplayarak yedekleme alanı hesaplarında kullanılmak üzere raporlayabilmelidir.
2.4.80. Yazılımın lisanslaması korunmakta (yedeklenmekte ve/veya replike edilmekte) ve izlenip raporlanmakta olan sanal makinaları çalıştıran ana sunucuların fiziksel işlemcisi bazında olmalıdır. Yapısal bileşenlerin sayısı (proksi, konsol, disk vb), işlemci çekirdeği, Sanal Makina sayısı, disk kapasiteleri ve uygulama ajanlarına göre bir lisanslama modeli olmamalıdır.
2.4.81. Lisanslama modelinde bir üst limit bulunmamalı, ilave lisans alınarak yapı istenildiği kadar sunucuyu kapsayacak şekilde büyütülebilmelidir.

2.5. Güvenlik Duvarı ve Güvenlik Duvarı Analiz Programı Lisans Yenilemesi (1) Yıl

2.5.1. Kurumumuzda çalışan 1 Adet FortiGate-600E Güvenlik Sistemleri ve Analyzer Log Yazılımı için güncelleme servisleri satın alınacaktır.
2.5.2. Kurum bünyesinde bulunan 1 (bir) adet Fortigate 600E ağ güvenlik sisteminin ve Analyzer Log Yazılımının garanti süresinin bitiminden itibaren en az 1 YIL yazılım üretici güncelleme paketi teklife dahil edilmelidir.

2.5.3. 1 Adet FG-600E Güvenlik sistemi için alınacak güncelleme servislerinin aşağıdakileri içermesi gerekmektedir:
2.5.4. 1 Yıl Süreli Firmware/Yazılım güncelleme
2.5.5. 1 Yıl Süreli Üretici firmadan 24x7 e-mail destek
2.5.6. 1 Yıl Süreli sınırsız kullanıcı için AntiVirus güncellemesi
2.5.7. 1 Yıl Süreli sınırsız kullanıcı için Uygulama Kontrol güncellemesi
2.5.8. 1 Yıl Süreli sınırsız kullanıcı için IPS güncellemesi
2.5.9. 1 Yıl Süreli sınırsız kullanıcı için URL Kategori Filtreleme güncellemesi
2.5.10. 1 Yıl Süreli sınırsız kullanıcı için AntiSpam güncellemesi
2.5.11. 1 Yıl Süreli sınırsız kullanıcı için Sandbox Cloud güncellemesi
2.5.12. 1 Yıl Süreli Donanım Garantisi.

2.6. İŞLETİM SİSTEMİ LİSANSLARI

2.6.1. Satın Alınacak Ürünler ve Miktarları

Nitelik		Adet
İşletim Sistemi	WINVDAPerDvc ALNG SubsVL OLV E 1Mth Acdmc AP PerDvc	210
İşletim Sistemi	CoreCAL ALNG LicSAPk OLV E 1Y Acdmc Ent UsrCAL	5

2.6.2. İşletim Sistemi lisansı FENERBAHÇE ÜNİVERSİTESİ REKTÖRLÜĞÜ adına, Kurumsal Open Lisanslama yöntemi ile satın alınacaktır.
2.6.3. Kurumun, satın alınacak olan İşletim Sisteminin mevcut alt sürümlerini kullanma hakkı olacaktır.
2.6.4. FENERBAHÇE ÜNİVERSİTESİ REKTÖRLÜĞÜ adına satın alınan İşletim Sistemi Lisansı web üzerinden (https://www.microsoft.com) görülecektir.
2.6.5. Satın alınan İşletim sistemi lisansı bilgisayarlara hem 32 bit hem de 64 bit kurulumunu desteklemeli ve aynı zamanda dil tercihi olmalıdır (Türkçe-İngilizce).
2.6.6. Satın alma süreci sonucunda İşletim Sistemi lisansının satın alındığı şirket, FENERBAHÇE ÜNİVERSİTESİ REKTÖRLÜĞÜ adına düzenlenmiş olana Microsoft Akademik Open Lisans anlaşması sözleşmesini, FENERBAHÇE ÜNİVERSİTESİ REKTÖRLÜĞÜ Bilgi Teknolojileri bölümüne teslim etmek zorundadır.

3. SERVİS, BAKIM, GARANTİ TESLİM KOŞULLARI

3.1. Tüm cihazların teslim yeri FBÜ Ataşehir Merkez Kampüs Binasıdır.
3.2. Yüklenici en geç 4-6 hafta içinde cihazları çalışır durumda teslim edecektir.
3.3. Alınacak tüm cihazlar İstanbul'da servisi olan tescilli bir markanın ürünü olmalıdır.
3.4. Garanti kapsamında bakım, onarım, parça değişimi ve nakliye de dahil olmak üzere tüm Masraflar yüklenici firma tarafından sağlanır. Garanti süresince cihaza müdahale yapılması gerektiğinde mümkün ise cihazın kullanım yerinde yapılacaktır.
3.5. Garanti süresince (müşteri kaynaklı hatalar dışında üründe çıkacak sorunlardan hiçbir ücret talep edilemez.
3.6. Ürünle birlikte kolay kullanımı ve işlevi için gerekli dokümanlar beraber verilmelidir.
3.7. Teklif süresi ……. Tarihleri arası geçerlidir. İletim tarihini geçen teklifler geçersiz sayılacaktır.

3.8. Şartname itiraz durumunda sartname@fbu.edu.tr mail adresine mail atılması ve itirazın gerçekleştiği maddeler belirtilmesi gerekecektir.

3.9. Hizmet için verilen teklifler Dolar (USD) cinsinden verilmelidir.

3.10. 3 yıllık tek alım server, diğerlerinde 1 yıllık yenileme yapılacaktır.

3.11. Satın alınan ürünlerin lisansları "FENERBAHÇE ÜNİVERSİTESİ" adına lisanslanmalı ve İdare' nin vermiş olduğu "fbu.edu.tr" uzantılı mail adresine kayıt edilmesi gerekmektedir.

4. KABUL ŞARTLARI

4.1. Proje, tüm bileşenleri ile bitirildiği zaman İdare tarafından kabul işlemi yapılacaktır. Projenin kabulü yapılmadan bitmiş sayılmayacaktır. Kabul şartları aşağıdaki gibidir.

4.1.1. Teklifteki tüm cihazlar eksiksiz bir şekilde kurulmuş çalışıyor olmalı

4.1.2. Tüm sanal makineler yeni yapıya taşınmış olmalı

4.1.3. Tüm danışmanlıklar verilmiş olmalı

4.1.4. Tüm yedekleme ve iş sürekliliği sistemlerinde tam fonksiyonel testler yapılmış olmalı

4.1.5. Tüm sistemler, sorunsuz 30 gün boyunca çalışıyor olmalı

4.1.6. Tüm eğitimler verilmiş olmalı

4.1.7. Projeye ait tüm dokümanların İdare' ye teslim edilmiş olması


FENERBAHÇE ÜNİVERSİTESİ
2016
FBÜ
FENERBAHÇE ÜNİVERSİTESİ