Veri Sızıntısı Tespit ve Engelleme Yazılımı (DLP) ve Veri Sınıflandırma Çözümü

Teknik Şartnamesi

Referans No: 2022 /10070131 / 10070517

Veri Sızıntısı Tespit ve Engelleme Yazılımı

1. Veri Sızıntısı Tespit ve Engelleme Sistemi, ağda bulunan kurum bilgilerinin kaybını ve istenmeyen kişiler tarafından sızdırılmasını, kurulu olduğu tüm kullanıcı bilgisayarlarında, sunucularda, bulut ortamında var olan depolama alanlarında, mail sunucularında tespit edip engelleyecektir.

2. Teklif edilecek olan Network DLP bileşenleri sanal cihaz ve/veya yazılım olarak toplamda 800 kullanıcıyı kapsayacak şekilde 3 yıl üreticinin destek paketi dahil tekliflendirilecektir.

3. Teklif edilecek yazılım/yazılımlar için 1 ve 3 yıl bakım ve destek anlaşması tekliflendirilecektir. Hem yurt içi hem yurt dışı bakım ve destek SLA süresi 7x24 olacaktır.

4. Teklif edilecek DLP çözümü 'Gartner Magic Quadrant Data Loss Prevention 'a ait son yayımlanan raporda liderler konumunda yer alan bir üreticinin çözümü olmalıdır.

5. DLP çözümleri İKÜ bünyesindeki bilgisayarlarda yaygın olarak kullanılan Arksigner, ABBY Fine Reader, eToken PKI Client, Microsoft Office ve SAP GUI programlarıyla birlikte çalışabilmelidir.

6. Teklif edilecek çözümün kurum içerisindeki sunucu kurulumları, ajan ve paketlerin dağıtımı, politikaların ve görevlerin kurgulanması teklifi veren yüklenici firma tarafından yapılacak ve kuruma anahtar teslim şekilde sorunsuz teslim edilecektir.

7. Teklif edilecek çözümün kurulum ve diğer tüm konfigürasyon süreçleri tamamlandıktan sonra IKÜ tarafından talep edilen yönetimsel raporlar oluşturulacak ve belirtilen periyotlarda kurum tarafından belirlenecek bir mail hesabı üzerinden ilgili birim yöneticilerine aktarılması sağlanacaktır.

8. Teklif edilecek olan çözüm Microsoft AD yapısı ile tam uyumlu çalışacaktır. İsteğe bağlı olarak grup, kişi, sistem bazlı belirtilen makinelere özel kurallar yazılabilecektir. Sistem,

birbirinden bağımsız birden fazla Directory Servis tanımlamaya ve entegrasyona izin vermelidir.

9. Teklif edilecek çözüm rol tabanlı yönetimi sağlamalıdır. Sistemi kullanacak olan yöneticiler farklı yetki seviyelerinde erişim ve yönetim hakkına sahip olmalıdır.

10. Teklif edilecek ürünün yönetim konsolu üzerinden tüm ajanların ve Add-onların yönetimi yapılabilmeli ve merkezi politikalar uygulanabilmelidir.

11. Teklif edilecek DLP ve Discover çözümleri ya da modülleri en az aşağıdaki işletim sistemlerini desteklemek zorundadır:

a. Microsoft tarafından desteği devam eden Windows client ve server işletim sistemleri.
b. Apple tarafından desteği devam eden MacOS client işletim sistemleri.

12. Teklif edilecek çözümün merkezi yönetim yazılımı en az aşağıdaki işletim sistemlerini desteklemek zorundadır:

a. Windows Server 2016

13. Teklif edilecek çözümün veri tabanı olarak en az aşağıdaki işletim sistemlerinden birini desteklemek zorundadır:

a. Microsoft SQL Server 2016
b. Muadil olarak Oracle database kullanılacak ise veri tabanı lisanslaması yüklenici firma tarafından karşılanacaktır.

14. Cihaz kontrol modülünde Bluetooth, cd/dvd, floopy disk, imaging device, network adapter, pcmci adapter, tape drives, usb drives, wireless ethernet donanımları ön tanımlı olarak gelmeli ve gerekirse el ile yeni donanım tipleri sisteme tanıtılabilmelidir. Bu amaçla donanım GUID leri kullanılabilmelidir.

15. Donanım tipleri en az bus tipi, donanım adı, seri numarası, instance ID, compatible ID, vendor ID/Product ID parametreleri ile özelleştirilebilmelidir. Tanımlanan donanım tipleri donanım erişim kontrollerinde kullanılabilmelidir.

16. Donanım kontrolleri bloklama, read-only, notify veya monitor aksiyonları ile sonuçlandırılabilmelidir. Oluşan tüm olaylar en geç 5dk içerisinde merkezi yönetim ara yüzünden raporlanabilmeli/izlenebilmelidir.

17. Son kullanıcı gerekçesine (justification) göre bloklama olasılığındaki bir vaka, işleyişin aksamaması için devam edilebilecek özellikte olmalıdır.

18. Kural setlerine bağlı olarak en az aşağıdaki aksiyonlar alınabilmelidir:

a. Monitor
b. Notify User
c. Request Justification
d. Store Evidence
e. Encrypt
f. Block

19. Veri sızıntısı tespit ve engelleme yazılımında yer alacak kurallar kullanıcının online yada offline duruma göre özelleştirilebilmelidir. Bu kapsamda kullanıcı kurum dışında olduğu zaman farklı bir politika ile kısıtlanabilmelidir. Merkez ara yüzünden oluşturulan yeni bir kural güncellemesi durumunda ofis dışındaki bir kullanıcı makinesinde bu süreç aktif olarak çalışabilmelidir.

20. Sistem şifreli sıkıştırılmış dosyaları ve/veya encrypt dosyaları otomatik algılayabilmeli ve içeriği analiz edilemeyen bu gibi dosyaları tespit edip engelleyecek politikalara yazılabilmelidir/desteklemelidir.

21. Harici diskler üzerinde read-only politika kapsamında belirlenen uygulamalar politika harici tutularak çalıştırılması sağlanabilmelidir.

22. Ajan seviyesinde sızıntının izlenmesi/engellenmesi amacıyla bilgilerin şu yollarla özelleştirilmesi mümkün olmalıdır:

a. Uygulamaların bilgi içeren dosyalara ulaşımlarının denetlenmesi. Uygulama tipleri e-mail client, Explorer, IM, P2P, Web browser, Media Burner, MS Office, Scanner, Winrar (Winrar için en az 8 alt seviye sıkıştırılmayı kontrol edebilmelidir) gibi hazır uygulama kalıpları desteklenmeli.Gerekirse bu listeler el ile genişletilip değiştirilebilmelidir. Uygulamalar çalıştığı PC üzerinden gösterilerek listeye dahil edilebilmelidir. Uygulamalar filename, hash, product name, vendor name, working directory parametreleri ile özelleştirilip tanıtılabilmelidir.
b. Discover yaparken dokümanlar; Title, subject, Tags, Categories, Author, Date Created, date modified, Last Saved date gibi parametrelerle özelleştirilebilmelidir.
c. Bilginin gitmesinin sakıncalı olduğu e-mail adresleri ya da domainler hedef olarak tanımlanabilmelidir.
d. Ön tanımlı dosya tipleri dışında el ile yeni tipte dosya uzantıları sisteme tanıtılabilmelidir.
e. Ağ üzerinde çalışan dosya sunucuları sisteme tanımlanabilmelidir.
f. Network IP blokları IP to IP seviyesinde tanımlanabilmelidir.
g. Kurum içerisinde var olan network yazıcılar sisteme tanımlanabilmelidir.
h. Web Uploadlar için hedef URL ler tanımlanabilmelidir. Bu yolla bilgilerin Web upload yolu üzerinde denetlenmesi mümkün olmalıdır.

i. Aynı üreticiye ait dosya, klasör ve usb şifreleme yazılımının kullanılması durumunda kullanıcı tarafından dosyanın harici bir depolama aygıtına çıkarılması durumunda şifreleme yapabilmelidir.

23. Ön tanımlı sözlüklerin dışında, el ile bilginin takibi açısından politikalarda kullanılabilecek özel sözlükler tanımlanabilmelidir. (dictionary,keyword)

24. Kullanıcı bilgisayarlarında görünen mesajlar istenilen dilde olmalıdır.

25. Kredi kartı numarası, T.C. kimlik, mac adres, Ip adres ve tarih gibi yapısı kural konulmaya müsait tanımlar ön tanımlı gelmeli, regex gibi yöntemlerle özel kelime kalıpları hazırlanabilmeli ve kurallarda kullanılabilmelidir.

26. Daha önceden çeşitli kriterlerle (Dosya tipi, uzantı, dosya detay özellikleri vs.) belirlenen bilgiler ağ ortamında olmaması gereken kaynaklarda bulunması durumunda(discover) otomatik olarak bu dosyalar karantinaya alınabilmeli, dosyalar bulunduktan sonra fingerprint taskı ayrıca yazılabilmeli, delil amaçlı kayıtlanması ya da sadece monitör yöntemi ile olay kayıt bilgisi oluşturulabilmelidir. Bu işlem scriptler ile yapılacaksa, scriptler yüklenici tarafından yazılacaktır.

27. Bilgilerin dışarı çıkması amacıyla isminin değiştirilmesi, sadece bir kısmının yollanması, paragrafların yerlerinin değiştirilmesi gibi bilgi manipülasyonları fark edilebilmeli ve engellenebilmelidir.

28. Bilgiler; dosyalara ulaşım (file access), geçici hafızaya alma(clipboard), E-posta ile yollanması, Web upload ile gönderilmesi, screen capture, uygulamaların bilgiye ulaşması, yazıcıdan yollanması, harici disklere yazılması, bulut uygulamaların ajanları ile dosyaların gönderimi, pdf/image writer ve belirlenen network ve portlar üzerindeki hareketleri sırasında takip edilebilmeli ve gerektiğinden kesilebilmelidir.

29. Son kullanıcı ajanı en az aşağıdaki bulut sistemleri üzerinde koruma tekniklerini desteklemelidir. Bu uygulamalar üzerinde Cut, Copy, Paste ve File Access işlemleri takip edilebilmelidir.

a. Box
b. Dropbox
c. GoogleDrive
d. iCloud
e. Office 365
f. OneDrive
g. Syncplicity
h. P2P Uygulamalar
i. WhatsApp

30. Politikaların genelinde monitör modunda olmaları için özel kullanıcı grupları tanımlanabilmelidir.

31. Yönetim arayüz üzerinden tüm kayıtlar takip edilebilmeli, kayıtlar için filtreler yazılıp istenilen olay kayıtlarına hızlı ulaşım sağlanabilmelidir.

32. Ya yönetim yazılımı üzerinden sistemlere yetkili bir hesap tanımı girilerek ajan basılabilmeli ve yönetilebilmeli, ya da SSCM vb. uygulama ile dağıtım yapılabilmelidir. Dağıtım paketi firma tarafından oluşturulacak ve teslim edilecektir.

33. MS Sharepoint Portal gibi doküman yönetim uygulamalarını destekleyecek, bunlarda bulunan bilgileri otomatik olarak tarayabilme yeteneğine sahip olmalıdır.

34. DLP çözümünün keşif (discover) modülü en az aşağıdaki bilgi depolama alanlarını desteklemelidir:

a. NFS
b. File Server
c. Sharepoint
d. MS-SQL Veri tabanları
e. Oracle Veri tabanları
f. MySql commercial versiyonları
g. Microsoft Exchange

35. Discovery işlemi en az aşağıdaki amaçlarda kullanılabilmelidir:

a. Sunulan çözüm ile tarihe ve tarih aralığına göre, dosya adına göre, dosya türüne göre, dosya içeriğindeki belirli kelime veya kelime gruplarına göre, dosya etiketine, kategorisine ve dosya büyüklüğüne göre veri aramayı desteklemelidir.

36. Keşif taramalarında bandwidth limitasyonu ayarı yapılabilmelidir.

37. Keşif taramalarının geçmiş sonuç bilgileri takip edilebiliyor olmalıdır.

38. Keşif taramaları sonucunda GUI üzerinde analitik raporlar üretilebilmelidir.

39. Keşif taramalarında en az aşağıdaki filtreler kullanılabilmelidir:

a. File Extension: El ile tanımlamaya imkân sağlamalı ve hazır gruplara sahip olmalıdır. Örn.Database files, executable files, Audio files, Source code, Script File vb.
b. File Information: File size, File name,File Extension, File Owner, Date created, Date modified, Date Accessed vb.

40. E-posta üzerinden yapılabilecek bir ihlal için tam kontrol sağlanmalıdır. Teklif edilecek çözüm MS Outlook 2013 ve üzeri versiyonları desteklemelidir.

41. Keşif kuralları ile hassas bilgilerin istemciler üzerinde tespit edilmesi ve tespit sonrası bu dosyaların monitör edilmesi, karantinaya alınması, kullanıcı erişim yönetimi politikası uygulaması mümkün olmalıdır.

42. Keşif modülü OCR tekniği ile resim dosyalarında yer alan hedef veriyi tespit edebilmelidir. Teklif edilecek çözüm içerisinde OCR desteği ile veri tespiti zorunlu bir özellik olarak yer almalıdır. OCR içinde Türkçe desteği olmalıdır.

43. DLP sisteminin ağ modülü switchler üzerinde verilen span port (veya tap cihazı ile) vasıtasıyla trafiği dinleyebilmeli ve trafik karakteristiğini çıkarabilmelidir. Monitör modülü en az aşağıdaki protokolleri desteklemelidir:

a. SMTP
b. IMAP
c. POP3
d. HTTP
e. LDAP
f. TELNET
g. FTP
h. IRC
i. SMB
j. HTTPS (Web Gateway span mode veya TAP cihazı ile)

44. Monitör modülü yük dağılımı yapacak şekilde kümele tekniği ile çalışabilmelidir.

45. Veri sızıntısı tespiti ve engelleme yazılımı, ağ seviyesinde çalışan koruma-aksiyon (prevent) modülü hedeflenen Email ve Web trafiğini belirlenen kurallar ile engelleye bilmelidir. Olası proxy sistemleri ile ICAP protokolu üzerinden entegre olabilmelidir. E-Mail trafiği için ise MTA modda çalışmalı ve X-header eklentileri yapabilmelidir. Prevent modülü yük dağılımı yapacak şekilde kümeleme modunda çalışabilmelidir.

46. Teklif edilecek çözümün içerisinde yer alabilecek Koruma-Aksiyon (Prevent) modülü, Microsoft Exchange ActiveSync ve Microsoft Office 365 ActiveSync ile entegre çalışabilmelidir.

47. Teklif edilecek DLP çözümü, en az kendi ile aynı CASB çözümü ile entegre çalışabilmelidir.

48. Kurum içeresinde hali hazırda kullanılmakta olan log yönetim veya bilgi olay yönetim platformuna (SIEM) syslog veya farklı bir metod vasıtası ile logları iletebilme özelliğine sahip olmalıdır.

49. Hedef veriyi tanımlayacak sistemde var olan parametreler için en az aşağıdaki teknikler desteklenmelidir:

a. Sözlükler: Hazır gelen şablonlar dışında el ile tanımlamalara imkân sağlamalıdır. Sözlük içeriklerinin tanımlamalarında kelime başlangıçları, sonları ve harf duyarlılığı gibi özellikler ile denetlenebilir olmalıdır.
b. Advanced Pattern: Hazır gelene şablonlar dışında (T.C. kimlik numarası, IBAN, Kredi kart numaraları vb.) el ile tanımlamaya imkân sağlamalıdır. Bu amaçla Regex kullanılabilmelidir.
c. Doküman özellikleri: Title, author, keyword, subject vb. filtrelerle tanımlanabilmelidir.
d. File extension: Hazır gelen şablonlar dışında el ile tanımlamaya imkân sağlamalıdır.
e. True File Type Grupları (html dosyaları, grafik dosyaları vb.): Hazır olarak gelen şablonlar kullanılabilmelidir.
f. Application Templates: Hazır gelen uygulama şablonlarına (Installers, Firefox, Java compiler vb.) ek olarak elle tanımlamaya imkân sağlamalıdır. Bu amaçla command line, executable directory, file hash, file name, vendor name vb. kriterler kullanılabilmelidir.
g. Son kullanıcı tanımlamaları.
h. Ağ paylaşımları.
i. URL listeleri.

50. DLP sisteminde Data-in-Use, Data-in-Motion ve Data-in-Rest olayları için hazır dashboardlar sağlanmalı ve ekranlar yoluyla ilgili bilgi sızıntılarının detaylarına inmek mümkün olmalıdır.

51. Oluşan DLP olayları ile ilgili detaylı izleme ara yüzü sağlanmalı bu vaka izleme ekranında en az aşağıdaki bilgiler sunulmalıdır:

a. Oluşma zamanı
b. Incident Type
c. Severity
d. Destination
e. Actual Action
f. Son kullanıcı bilgisi
g. Computer name
h. IP bilgisi
i. Eşleşen politika

j. Audit log (Bu vakayı kimin incelediği)

52. Vaka ekranlarında (Incident Response / Management vs.) delil bilgileri izlenebilir olmalıdır.

53. Oluşan vakalar karşılığında hedeflenen sistem yöneticilerine uyarı mailleri oluşturulabilmelidir. (Alarm mekanizması)

54. Oluşan vakalarla ilgili ara yüzden Case açılabilmeli ve ilgililere atanabilmelidir. Açılan her çağrı içerisinde, politika ihlaline neden olan olayın detayları (Source IP, zaman bilgisi, Kullanıcı bilgisi, Veri sızıntısı tipi, politikası, hedef adres, veri örneği, vb.) belirtilmelidir.

55. Help Desk alt yapısı ile merkezi olarak son kullanıcıların karantinaya alınmış olayları üst yöneticisi ya da tanımlanan kişi tarafından serbest bırakılmalıdır. Açılan çağrıların içerisinde, adli soruşturmada kullanılabilecek şekilde, ihlale neden olan bilgi saklanabilmelidir.

56. Ajanlar ve yönetim sunucusu arasındaki iletişim şifreli olmalıdır.

57. Kullanıcıların ajanları stop etmeye çalışması, kapatmaya çalışması durumunda kendini koruyabilmeli ve otomatik olarak tekrar çalışabilmelidir.

58. Teklif edilecek çözüm, vaka analizlerinde hassas verilerin sistem kullanıcısı tarafından görüntülenmesini engelleyecek teknikleri içerisinde barındırmalıdır.

59. Belirli uygulama veya uygulama grupları arasındaki cut, copy, paste, print screen gibi işlemler denetlenebilmeli, istenirse engellenebilmelidir.

60. Kural ihlali durumunda bilgiyi göndermek isteyene uyarı mesajı e-posta veya pop-up ile gönderilebilmelidir.

61. Teklif edilecek çözüm güvenlik analiz yeteneklerine sahip olmalı, oluşan olay kayıtları üzerinde analizler yaparak en riskli kullanıcıları gösterebilen bir dashboard ekranına sahip olmalıdır.

62. Sadece kritik verilerin bulunduğu belgelerin baskıya gönderilmesi engellenebilmelidir.

Veri Sınıflandırma Çözümü

1. Teklif edilecek çözüm, İŞVEREN personelinin mevcut otomasyon ürünleriyle, doküman ve diğer dijital dosyalarının sınıflandırılması ve kişisel verilerin sınıflandırılması işlemlerini gerçekleştirecektir.

2. Teklif edilecek çözüm, en az 800 kullanıcı için, en son sürümü destekleyecek şekilde lisanslı olacaktır.

3. Teklif edilecek çözüm, Microsoft Office 2010, 2013, 2016, 2019, Microsoft Outlook 2010, 2013, 2016 üzerinde çalışabilen paketlerden oluşmalı, Microsoft Windows 7, Windows 8, Windows 8.1 ve Windows 10 ve teklif verildiği tarih itibari ile destek süreci devam eden Windows Server versiyonları üzerindeki bütün dosya biçimlerini sınıflandırmayı desteklemelidir.

4. Teklif edilecek çözüm web tabanlı bir ara yüz üzerinden yönetime sahip olmalı, tek bir merkezi ara yüz üzerinden yönetilebilmelidir.

5. Teklif edilecek çözüm Active Directory, LDAP ile entegre olabilmelidir.

6. Teklif edilecek çözüm, sınıflandırma yöntemi olarak; kullanıcı bazlı sınıflandırma, otomatik sınıflandırma ve önerilen sınıflandırma seçeneklerini destekler nitelikte olmalıdır. Sınıflandırma yöntem seçenekleri iş birimlerinin ihtiyaçlarına göre yapılandırılabilmelidir.

7. Teklif edilecek çözüm, GDPR ve KVKK kanunlarına uygun veri setlerini içinde barındıracak ya da başka bir sistemle entegre edilip atayabilecektir ve veri sınıflandırması ile ilgili bu kural şablonlarının güncellenmesine izin verecektir.

8. Teklif edilecek çözüm, kendi kolektörünü kullanarak Merkezi Raporlama yeteneğine ve raporlama ara yüzüne sahip olmalıdır. Raporlama ara yüzünden kurum aktif kullanıcı sayısını, sınıflandırma eğilimlerini, hata eğilimlerini ve alarm üreten girişimleri raporlanabilmelidir.

18. Teklif edilecek çözüm üzerinde bulunan ara yüz ve/veya raporlama modülünde, hangi kullanıcıların hangi kural tablolarını aldığı, kullanıcıların bilgisayarlarında bulunan ajan veya Add-on versiyon bilgilerinin detaylarını görmek mümkün olmalıdır.

19. Teklif edilecek çözüm, herhangi bir tasarım, ses, video veya resim dosyasının nesne menüsü yardımıyla sınıflandırılmasına izin vermelidir.

20. Teklif edilecek çözüm; olay, koşul, aksiyon (IF & ANY) değişkenlerini kullanarak İŞVEREN ihtiyaçlarına göre esnek sınıflandırma, etiketleme oluşturulmasına imkân sağlamalıdır.

21. Teklif edilecek çözüm; kullanıcıların Office, Outlook üzerinde kolaylıkla sınıflandırma yapabilmelerini ve düzenlenebilir sınıflandırma ekranlarını içermelidir.

22. Teklif edilecek çözüm en az aşağıdaki veri tiplerini sınıflandırabilmelidir;

a. Adobe Portable Document Format: .pdf
b. Microsoft Visio: .vsdx, .vsdm, .vssx, .vssm, .vsd, .vdw, .vst
c. Microsoft Project: .mpp, .mpt
d. Microsoft Publisher: .pub
e. Microsoft Office 2010, 2013, 2016, 2019, Office 365: .xls, .xlt, .doc, docx .dot,
f. .ppt, .pps, .pot, .pptx

g. Microsoft XPS: .xps .oxps
h. Images: .jpg, .jpe, .jpeg, .jif, .jfif, .jfi.png, .tif, .tiff
i. Autodesk Design Review 2013, 2016, 2019: .dwfx
j. Adobe Photoshop: .psd
k. Digital Negative: .dng
l. Txt, csv

23. Teklif edilecek çözüm, kullanıcıların Office dokümanında sınıflandırma değerlerini değiştirmek istemeleri durumunda, hassas içeriği bulan bir yetenek sağlamalıdır.

24. Teklif edilecek çözüm yüksek data boyutuna sahip (2 GB üstü) Microsoft PowerPoint dosyalarını da sınıflandırabilmelidir.

25. Teklif edilecek çözüm, sınıflandırılacak dosyalar açılmadan, tek tık veya çoklu seçim ile sınıflandırma yapabilme kabiliyetinde olmalıdır.

26. Teklif edilecek çözüm, işbu şartname gereğince teklif edilecek DLP programlarının yararlanabileceği Office dokümanının meta bilgisine, sınıflandırma bilgisi ekleme yeteneğini sağlamalıdır.

27. Teklif edilecek çözüm, dokümanı kayıt yapma veya yazıcıya gönderme anında sınıflandırmaya zorlama yeteneğini desteklemelidir.

29. Teklif edilecek çözümün, İŞVEREN personel bilgisayarları üzerinde geçmişe yönelik (Hali hazırda var olan dokümanlar) veri sınıflandırma keşfi yapabilmelidir.

30. Teklif edilecek çözümün ajan vay Add-on kurulumları aynı çözümün merkezi ara yüzü üzerinden veya SCCM üzerinden sorunsuz yüklenebilmelidir. SCCM paketleri yüklenici tarafından hazırlanacaktır.

31. Teklif edilecek çözümün ajanları, uygulanan politikaları merkezi sunucuları üzerinden HTTPS servisi veya SMB protokolü olarak kolaylıkla çekebilmelidir.

32. Teklif edilecek çözüm üzerinde farklı kullanıcı guruplarına farklı politikalar uygulanabilmelidir.

33. YÜKLENİCİ teklif edeceği ürünün şartnamede yer alan bir veya birden fazla maddeyi karşılayamadığı durumda, ürün ile entegre çalışan yazılım, donanım ya da lisans eklemesi ile maddelerin talep ettiği teknik özellikleri sağlayabilmesi halinde, teklifine gerekli yazılım, donanım ve lisans bileşenlerini de ekleyecektir.

İDARE **YÜKLENİCİ**