T.C
BARTIN İL ÖZEL İDARESİ
PLAN VE PROJE MÜDÜRLÜĞÜ

TEKLİF MEKTUBU

TEKLİF SAHİBİNİN	
Adı Soyadı/Ticaret Ünvanı	.....
Tebligat Adresi	.....
Bağlı Olduğu Vergi Dairesi	.....
Vergi Numarası	.....
T.C.Kimlik Numarası	.....
Telefon No	.....
Faks No	.....
E-Mail	.....

İdaremiz ihtiyacı olan aşağıda cinsi, miktarı ve özellikleri yazılı mal alım / hizmet alım / yapım işi 4734 Sayılı Kamu İhale Kanunu'nun ilgili maddeleri gereği doğrudan temin yoluyla yapılacaktır. Söz Konusu işi KDV. hariç Kaç TL'na verebileceğiniz/yapabileceğinizi **03/03/2025 Pazartesi günü Saat 16:30**'a kadar kapalı zarf ile İdaremiz Plan ve Proje Müdürlüğüne veya taranmış halinin bilgiislem@bartinozelidare.gov.tr e-posta adresine gönderilmesi rica olunur.

İlker SARIKAYA
Plan ve Proje Müdürü

S.NO	CİNSİ , PLAKASI, MODELİ	MİKTAR	BİRİM FİYATI	TOPLAM TUTARI
1	Kurumsal Anti-Virüs Programı Lisansı (140 Kullanıcılı - 1 Yıllık)	1 Adet		
	EK: Teknik Şartname			
			GENEL TOPLAM	

Teklif konusu işin tamamını KDV.hariç (Rakamla).....-
TL'na (Yazıyla), ...-
TL.'na bedel karşılığında, teklifin teyidine müteakip, belirtilen iş günü içerisinde teslim etmeye / yapmayı,

22.11.2016 tarihli ve 29896 sayılı resmi gazetede yayımlanarak yürürlüğe giren 678 sayılı KHK'nin 30. maddesinde belirtilen hükümlere göre yapılacak araştırma sonucu talep ve ödemenin yapılacağı, aksi durumda herhangi bir hak iddia etmeyeceğimi, idaremizin çıkarına aykırı bir eylem ve oluşum içerisinde olmayacağımı,

- İdarenizin çıkarlarına aykırı bir eylem ve oluşum içerisinde olmayacağımı,
- İdare teklifde belirtilen miktarın tamamanı alıp almamakta serbestir.
- Malın/ İşin teslim süresi ..... (.....) İş günüdür.

KABUL VE TAAHHÜT EDERİM.

TEKLİF VERMEYE YETKİLİ
KİŞİ/FİRMA
ADI SOYADI-KAŞE-İMZA

TEYİT EDENİN	
Adı Soyadı =	Teyidi yapılan Mal Alımı / Hizmet Alımı / yapım işinin teyit tarihinden itibaren (.....) iş günü içerisinde teslimi yapılacaktır.
Ünvanı =	
İmzası =	
TARİH =	

ANTIVIRUS YAZILIMI ALIMI TEKNİK ŞARTNAMESİ

MERKEZİ YÖNETİM YAZILIMI

1. Alım yapılacak antivirüs yazılımı; bilgisayarları, sunucuları ve mobil cihazları uzaktan yönetebilecek merkezi yönetim konsoluna sahip olmalıdır.
2. Merkezi yönetim yazılımı, aşağıda detayları belirtilen tüm özellikleri Türkçe dil desteği bulunan tek bir Web arayüzü üzerinden yapabilmelidir.
3. Merkezi yönetim konsolu ve modülleri Windows ve Linux işletim sistemlerine kurulabilmelidir. Yönetim konsolu ayrıca bir Linux tabanlı virtual appliance olarak üretici web sitesinden indirilebilmelidir.
4. Merkezi yönetim yazılımı Microsoft Azure Marketplace üzerinde ürün olarak bulunmalıdır.
5. Merkezi Yönetim Yazılımı aşağıdaki işletim sistemlerine kurulabilmelidir
    - Windows Server 2012, R2 ve 2016
    - Windows 10
    - Ubuntu 12.04, 14.04, 16.04
    - RHEL ve CENTOS 5, 6, 7
    - SLED ve SLES 11, 12
    - OpenSuse 13
    - Debian 7, 8
    - Fedora 19, 20, 23
6. Merkezi yönetim konsolu, veritabanı sunucusu olarak Microsoft SQL Server ve MySQL desteklemelidir.
7. Active Directory ile entegre olup domain içerisindeki bilgisayarlar otomatik olarak yönetim konsolunda listelenmeli ve bu bilgisayar ve sunuculara uzaktan agent ve antivirüs kurulumu yapabilmelidir.
8. Yönetim konsolu üzerinden, Agent yüklü makinelerin aşağıdaki özellikleri görüntülenmelidir ve bu bilgiler istenildiği zaman PDF, CSV ve PostScript formatında raporlanabilmelidir.
    - Üretici
    - Model
    - Ağ Adaptörü IP Adresi
    - İşletim Sistemi Adı
    - İşletim Sistemi Versiyon Numarası
    - İşletim Sistemi Dili
    - İşletim Sistemi Saat Dilimi
    - Oturum Açmış Kullanıcı Adı
9. Bilgisayarlar, sunucular ve mobil cihazlardan toplanan tehdit günlükleri merkezi yönetim yazılımı veritabanında barındırılmalı ve veritabanında ne kadar süre saklanacağı seçilebilmelidir
10. Yönetim yazılımı üzerinden tehditler, bilgisayar koruma durumları, antivirüs yüklü olmayan makineler gibi detaylı raporlar .PDF, CSV, PS formatında çıktı alınabilmeli ve bu raporlar düzenli olarak yerel diske kaydedilebilmeli veya bir eposta adresine gönderilebilmelidir.
11. Yönetim konsolu üzerinden Agent yüklenmiş makinelere aşağıda açıklanan komutlar uzaktan gönderilebilmelidir.

- **Bilgisayar Tarama Komutu**:Yönetim konsoluna bağlı bilgisayarlarda istenilen zamanda virüs taraması başlatabilmelidir.
- **Yazılım Yükleme Komutu**:Yönetim konsoluna bağlı Windows, Linux ve Mac OS işletim sistemlerine antivirüs yazılımını kurabilmelidir. Windows bilgisayarlara MSI tabanlı 3. parti uygulamaları HTTP ve Dosya Paylaşımı(SMB) üzerinden uzaktan kurabilmelidir.
- **Yazılım Kaldırma:** Bilgisayarda yüklü MSI tabanlı uygulamaları uzaktan kaldırabilmelidir.
- **Mesaj Gönderme Komutu**: Windows bilgisayarlar ve Android/IOS işletim sistemine sahip mobil cihazların ekranında belirtilen metin mesajını görüntülemelidir.
- **Windows ve Linux Shell Komutu**: Windows ve Linux bilgisayarlara istenen Shell(komut satırı) komutlarını gönderip çalıştırabilmelidir. Örn: Ipconfig /flushdns
- **Bilgisayarları Kapatma ve Yeniden Başlatma**:Konsola bağlı bilgisayarlarda uzaktan kapatma ve yeniden başlatma yapabilmelidir.

12. Yönetim yazılımının Agent'ını bilgisayarlara kurmak için aşağıdaki kurulum yöntemlerini desteklenmelidir.
    - **Uzaktan Kurulum**:Yönetim konsolu, Active Directory üzerinden bulduğu makinelere uzaktan kendi Agent yazılımını kurabilmelidir.
    - **GPO ve SSCM** :Uzaktan Yönetim konsolu, Active Directory GPO ve SSCM üzerinden Agent kurulumu yapmaya olanak sağlayan konfigurasyon dosyasını oluşturabilmelidir
    - **Script Dosyası:**Windows, Linux ve Mac OS işletim sistemerine Agent kurabilen script dosyası konsol üzerinden çıkartılabilmelidir.
    - **.EXE Dosyası**: İçerisinde agent ve antivirüs kurulum dosyalarına bulunduran bir .exe paketi çıkartılabilmelidir. Bu paket oluşturulurken içerisine lisans ve konfigurasyonlar gömülebilmelidir.
13. Merkezi Yönetim Konsolu Android ve iOS işletim sistemleri için Mobile Device Management(MDM) özelliği içermelidir.
14. Android mobil cihazlarda aşağıda açıklaması yapılan işlemleri yapabilmelidir:
    - **Antivirus**: Kötü amaçlı Android uygulamalarını tespit edip ve temizler.
    - **Anti-Theft**: Çalınmaya karşı koruma özelliği ile uzaktan cihaz kilitleme, GPS üzerinden konum bulma, siren çaldırma, güvenilir sim kart belirleme özelliklerini sağlama.
    - **Anti-phishing**:Mobil tarayıcılarda girilen web sitelerini tarayarak oltalama saldırılarını önler.
    - **Uygulama Kontrolü**:Telefonlara yüklenen uygulamaları kısıtlar. Kısıtlama; uygulama ismine, kategorisine ve uygulama izinlerine göre belirlenebilir
    - **Yüklü Uygulamalar**:Android cihazda yüklü uygulamaların listesi yönetim konsoluna gönderilir ve yönetim konsolunda görüntülenebilir.
15. iOS mobil cihazlarda aşağıda tanımları yapılan özellikler bulunmalıdır:
    - **Anti-Theft**: Çalınmaya karşı koruma özelliği ile iOS cihaz uzaktan kilitlenip kilidi açılabilmeli ve cihaz içindeki tüm kişisel verileri silen bir komut gönderilebilmelidir.
    - **Uygulama Kontrolü**: Uygulama kontrolü özelliği ile uygulama beyaz listesi ve kara listesi oluşturulabilmelidir.
    - **iCloud Denetimi**: Kullanıcının iCloud hesabı ile yapabileceği işlemleri kısıtlayan bir özellik bulunmalıdır.
    - **Cihaz Yönetimi**: iOS cihazlara uzaktan WIFI, VPN, HTTP Proxy, Mail Hesapları, Kişiler, Takvim, Google hesabı bilgileri gönderilebilmelidir.

16. Yönetim yazılımı oluşturduğu günlükleri depolamak için Syslog server ve native IBM Qradar desteği bulunmalıdır.
17. Windows bilgisayarlarda yüklü olan antivirüs programlarını otomatik olarak tespit ederek kaldırabilen bir özellik içermelidir.

MASAÜSTÜ VE DİZÜSTÜ BİLGİSAYARLARA KURULACAK ANTİVİRÜS YAZILIMI

1. Teklif edilecek antivirüs yazılımı aşağıda belirtilen işletim sistemlerine kurulabilmelidir.
    - Windows 7, 8, 8.1, 10
    - Mac OS X 10.6, 10.7, 10.8, 10.9 , 10.10 10.11, 10.12, 10.13
    - Debian, Fedora, Mandriva, Red Hat, SuSE
    - RHEL ve CENTOS 5, 6, 7
    - SLED ve SLES 11, 12
    - OpenSuse 13
    - Debian 7, 8
    - Fedora 19, 20, 23
2. Teklif edilecek antivirüs yazılımı bilgisayardaki yerel diskler, taşınabilir cihazlar, ağ paylaşımları, Internet trafiği, e-posta trafiğini ve ağ trafiğini gerçek zamanlı olarak tarayarak virüs, solucan, truva atı, rootkit, adware, spyware, malware ve fidye yazılımı türevlerine karşı bilgisayarları ve sunucuları koruyacaktır.
3. Virüs taraması yapan antivirüs motoru üzerinde taranacak yerler, taranacak dosya boyutu ve uzantısı sınırlamaları, kullanılacak tarama teknolojileri gibi özelleştirmeler yapılabilmelidir.
4. İstenilen dosya ve klasörler antivirüs taraması dışında bırakılabilmelidir.
5. Antivirüs yazılımı, yayılan yeni virüsleri tanımasını sağlayan virüs veritabanı güncellemesini yerel ağdaki merkezi yönetim sunucusundan, internet üzerinden otomatik olarak indirebilmeli veya bilgisayara takılan bir USB bellek üzerinden yükleyebilmelidir.
6. Virüs imza güncellemesi isteğe bağlı olarak önceki bir tarihe çekilebilmeyi desteklemelidir.
7. Virüs imza güncelemeleri isteğe bağlı olarak normal, önceden dağıtım ve gecikmeli dağıtım olarak yüklenebilmelidir.
8. Antivirüs yazılımı isteğe göre virüs tespit ettiğinde kullanıcıya sormadan silecek şekilde ayarlanabilmelidir.Ayrıca antivirüs yazılımı grafik arayüzü, kullanıcı masaüstü ortamında görünmeden sessiz modda çalışabilmelidir.
9. Belirlenecek bir parola antivirüs yazılımının bilgisayardan kaldırılması veya pasif hale getirilmesi engellenebilecektir.
10. Antivirüs tarafından silinen tüm dosyalar yerel karantinaya taşınmalı ve istendiği zaman karantinadan dışarı çıkartılabilmelidir.
11. USB portları üzerinden çalışan depolama aygıtları, taşınabilir cihazlar, yazıcılar, tarayıcılar, akıllı kart okuyucular ve bluetooth cihazların bilgisayara takılmasını engelleyen bir aygıt kontrolü modülü bulunmalıdır. Bu modül sayesinde USB'den çalışan depolama cihazları için aşağıdaki şekilde kısıtlamalar yapılabilecektir.
    - **Engelleme**:Bilgisayara takılan cihaz engellenir ve kullanılamaz.
    - **Salt-Okunur**:Bilgisayara takılan depolama aygıtından dosya okunabilir, depolama aygıtına dosya aktarılamaz.

- **Uyarı**: Bilgisayara USB takıldığında kullanıcıyı uyaran bir ekran çıkmalı, kullanıcı bu ekrana onay vererek USB depolama cihazını kullanmaya devam edebilir.

12. Bilgisayara takılan USB depolama cihazlarında otomatik olarak tarama başlatılabilmelidir.
13. Bilgisayardaki HTTP/HTTPS trafiği taranmalı ve denetlenen URL'ler üzerinde anahtar kelime bazlı ve alan adı bazlı engelleme yapılabilmelidir.
14. Bilgisayarda istenilen zamanda ve aralıklarda otomatik virüs taraması başlatılabilmelidir ve virüs taraması zamanlayıcısı aşağıdaki fonksiyonları desteklemelidir.
    - Taramadan sonra bilgisayarda otomatik olarak Kapatma, Yeniden Başlatma, Uyku Modu ve Hazırda Bekleme işlevlerini yapabilmelidir ve kullanıcının bu işlevleri engelleyip engelleyememesi ayarlanabilmelidir.
    - Kullanıcının, zamanlanan taramayı belirtilecek dakika kadar duraklatabilmesini desteklemelidir.
    - Dizüstü bilgisayarlar bataryada çalışıyorsa taramayı atlamayı desteklemelidir.
    - Tarama belirli bir zaman aralığında rastgele başlamayı desteklemelidir.
15. Aşağıda listelenen özelliklere sahip bir HIPS(Host Bazlı Saldırı Önleme) modülü bulunmalıdır.
    - Bilgisayarda çalışan uygulamaların davranış analizini yaparak Cryptolocker gibi fidye yazılımlarını engelleyebilmelidir.
    - Windows kayıt defterini denetlemeli ve belirli kayıt defteri anahtarlarında yapılacak değişiklikler oluşturulacak kural ile engellenmeli ve girişimler kayıt altına alınmalıdır.
    - Yolu belirtilen .exe dosyasının çalıştırılması bir kural ile engellenebilmelidir.
    - Bilgisayara yeni bir sürücü yükleme bir kural ile engellenebilmelidir.
    - Windows başlangıcında çalışacak olan uygulamalarda bir değişiklik meydana geldiğinde bildirim çıkartabilmelidir.
16. POP3/POP3s ve IMAP/IMAPS eposta protokollerini gerçek zamanlı olarak tarayarak gelen ve giden epostalarda virüs taraması yapabilmelidir.
17. Bilgisayardaki gelen/giden ağ trafiğini tarayan, isteğe göre gelen/giden bağlantı kuralları oluşturulabilecek bir güvenlik duvarı modülü bulunmalıdır.
18. Bilgisayarın kurduğu botnet trafiğini ağ seviyesinde tespit edip engelleyebilen ayrı bir botnet engelleyici modül bulunmalıdır.
19. Bilgisayara gelen/giden ağ paketlerini tarayarak aşağıda belirtilen saldırılara karşı koruma sağlayacak bir IDS(Intrusion Detection Systems) modülü bulunmalıdır.
    - DNS ve ARP poisoning attack
    - Port Scanning Attack
    - Eternalblue Exploit Attack
20. Windows istemcilerine kurulacak antivirüs Microsoft Outlook, Thundebird gibi eposta istemcileri için istenmeyen e-posta(spam) engelleyici bulundurmalıdır. Modül tarafından tespit edilen istenmeyen e-postalar İstenmeyen Eposta klasörüne otomatik taşınmalıdır.
21. İstenmeyen e-posta engelleyici modül üzerinde Genel Kara Liste, Genel Beyaz Liste, Kullanıcı Kara Listesi ve Kullanıcı Beyaz Listesi tanımlanabilinmelidir. Kullanıcılar Outlook üzerindeki e-postalara tıklayıp istenmeyen e-posta olarak işaretleyebilmelidir.
22. Microsoft Outlook ve Windows Live Mail için otomatik olarak kurulan bir eklentisi bulunmalı. Bu eklenti sayesinde kullanıcı istediği epostayı tekrar antivirüs taramasından geçirebilmelidir.

23. Bulut tabanlı bir itibar veritabanı özelliğine sahip olmalı ve istenen dosyanın ilk görülme tarihi ve kullanım sıklığı görüntülenebilmelidir.
24. Web tarayıcılar, Microsoft Office bileşenleri, PDF okuyucuları ve eposta istemcilerinin açıklarından faydalanan exploit ve 0day saldırılarını engelleyebilecek bir Exploit engelleme modülü bulunmalıdır.
25. Bilgisayar kilit moduna girdiğinde, ekran koruyucu devreye girdiğinde veya kullanıcı oturumu kapatıldığında otomatik olarak bilgisayar taraması yapabilmelidir. Dizüstü bilgisayarlar bataryada çalışıyorsa taramayı atlayabilmelidir.
26. Bilgisayarlarda virüs taraması yapabilmek için önyüklenebilir bir kurtarma ortamının ISO dosyası üreticinin web sitesinden hazır olarak indirilebilmelidir. CD veya USB belleğe yazdırılan ISO dosyası ile bilgisayardaki işletim sistemi taranabilecektir.

FİZİKSEL VE SANAL SUNUCULARA KURULACAK ANTİVİRÜS YAZILIMI

1. Teklif edilecek antivirüs yazılımı aşağıda belirtilen işletim sistemlerine işletim sistemi seviyesinde, sanallaştırma platformlarına ise host seviyesinde kurulabilmelidir.
    - Microsoft Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016
    - Microsoft Windows Storage Server 2008 R2 Essentials SP1 / 2012 / 2012 R2
    - Microsoft Windows Small Business Server 2003 (x86) / 2003 R2 (x86) / 2008 (x64) / 2011 (x64)
    - Microsoft Windows Server 2012 Essentials / 2012 R2 Essentials
    - Microsoft MultiPoint Server 2010 / 2011
    - Windows MultiPoint Server 2012
    - Debian, Fedora, Mandriva, Red Hat, SuSE
    - VMware vSphere 5.5, 6.0 ve 6.5
    - Windows Server 2008 R2 Hyper-V, Windows Server 2012 Hyper-V, Windows Server 2012 R2 Hyper-V, Windows Server 2016 Hyper-V
2. Windows sunuculara kurulacak antivirüs yazılımı Microsoft Azure Marketplace üzerinde ürün olarak bulunmalıdır.
3. Teklif edilecek antivirüs yazılımı fiziksel ve sanal sunuculardaki yerel diskler, taşınabilir cihazlar, ağ paylaşımları, Internet trafiği ve e-posta trafiğini gerçek zamanlı olarak tarayarak virüs, solucan, truva atı, rootkit, adware, spyware, malware ve fidye yazılımı türevlerine karşı koruyacaktır.
4. Virüs taraması yapan antivirüs motoru üzerinde taranacak yerler, taranacak dosya boyutu ve uzantısı sınırlamaları, kullanılacak tarama teknolojileri gibi özelleştirmeler yapılabilmelidir.
5. Kurulacak antivirüs yazılımı Windows Server üzerindeki IIS, SQL Server, Exchange Server, Sharepoint, Hyper-V, Kerio Connect ve Kerio Control uygulamalarını tespit edip, bu uygulamaların hassas dosyalarını ve veritabanı dosyalarını otomatik olarak antivirüs taraması dışında tutan bir özellik bulundurmalıdır.
6. İstenilen dosya ve klasörler antivirüs taraması dışında bırakılabilmelidir.
7. Windows sunuculara kurulacak antivirüs yazılımı dosyaları tarama dışında bırakabilmenin yanında istenilen windows işlemini(process) tarama dışında bırakabilmeye imkan tanımalıdır.

8. Windows Hyper-V ana makinesine kurulacak antivirüs yazılımı, bu ana makine üzerinde çalışan sanal sunuculara herhangi bir program kurmaya gerek kalmadan antivirüs taraması yapabilmelidir.
9. Windows Terminal Sunucularda, oturum açan her kullanıcı için antivirüs grafik arayüzünün çalışmasını engelleyen bir terminal modu bulunmalıdır.
10. Vmware vShield ve NSX ürünlerine entegre olarak sanal makineleri bir agent kurulmadan tarayabilmelidir.
11. Sunucularda virüs taraması yapabilmek için önyüklenebilir bir kurtarma ortamının ISO dosyası üreticinin web sitesinden hazır olarak indirilebilmelidir. CD veya USB belleğe yazdırılan ISO dosyası ile bilgisayardaki işletim sistemi taranabilecektir.
12. Web tarayıcılar, Microsoft Office bileşenleri, PDF okuyucuları ve eposta istemcilerinin açıklarından faydalanan exploit ve 0day saldırılarını engelleyebilecek bir Exploit engelleme modülü bulunmalıdır.
13. Belirlenecek bir parola antivirüs yazılımının bilgisayardan kaldırılması veya pasif hale getirilmesi engellenebilecektir.

NOT1: Teknik şartnameye asgari düzeyde uygun marka bağımsız tüm güvenlik yazılımları teklif edilebilir, ancak teklif edilen ürünün teklifle birlikte bildirilmesi gerekmektedir. Teklif edilen ürün, İdaremiz muayene kabul komisyonunca teknik şartnameye ve mevcut sistemimize uygunluğu incelendikten sonra kabul edilecektir.

NOT2: İdaremizin herhangi bir ürün için herhangi bir firmayı "register" olarak kayıt etme/önerme gibi bir durumu bulunmamaktadır. Bu gibi durumlar İdaremiz tarafından onaylanmamakta olup, tamamen dağıtıcı firmanın sorumluluğundadır.