BİRİM FİYAT TEKLİF CETVELİ

İdarenin Adı :ÜNİBEL ÖZEL EĞİTİM V E BİLGİ TEKNOLOJ SAN VE TİC.A.Ş.
Doğrudan Temin Numarası :20DT186510
Malın Adı :ANTİVİRÜS (KASPERSKY) LİSANS ALIMI

	A			B	
Sıra No	Mal Kaleminin Adı ve Kısa Açıklaması	Birimi	Miktarı	Teklif Edilen Birim Fiyat (Para birimi belirtilerek)	Tutarı (Para birimi belirtilerek)
1	ANTİVİRÜS (KASPERSKY ENDPOINT SECURITY FOR BUSİNES SELECT) LİSANS ALIMI 965 ADET	yıl	1		
Toplam Tutar (K.D.V Hariç)					

Adı - SOYADI / Ticaret unvanı
Kaşe ve İmza

İDARİŞARTNAME:

1-Teklifinizi en geç 07/04/2020 tarihine saat 14.00'a kadar **ÜNİBEL A.Ş** İdari binaya faks , e posta veya kapalı zarf ile teslim ediniz.
2-Teklifiniz KDV hariç ve Birim Fiyat Toplam Bedel olarak veriniz. Teklif mektubu ve teknik şartnamenin her sayfasını kaşeleyip imzalayınız.
3- Teklif mektubunda vermiş olduğunuz fiyatlar, şartname aksine bir süre yoksa **..30....** gün süreyle geçerli olacaktır.
3.1-Teklif mektubunuzda teklif edilen mal ve/ veya hizmetin toplam tutarı 4734 Sayılı Kamu İhale Kanunu (3 g istisna maddesi) ile alımı yapılacağından Son Fiyat'ınızı yazınız.
3.2 Taahhüt edilen mal/veya hizmet, ekli şartnamelerde aksine bir süre yoksa tebliğ tarihinden itibaren en geç **(10)** takvim günü içinde ilgili Müdürlüğe teslim edilecektir. Teslim süresinin bitiminde taahhüdün yerine getirilmemesi halinde ilgili müdürlükçe taahhüdün **15** (On beş gün) içinde yerine getirilmesi için yükleniciye ihtar çekilir. Bu süre içinde taahhüdün yerine getirilmesi halinde, geciken her gün için toplam tutarın Binde üçü oranında ceza uygulanır. Bu sürenin bitiminde taahhüdün yerine getirilmemesi durumunda idare tek taraflı olarak alımdan vazgeçebilir.
3.3 Mal ve / veya hizmetin teslimi ve kabulünü müteakip ekli şartnamelerde aksine bir süre yoksa en geç bir ay içinde ödeme yapılacaktır.
3.4 Teklif veren firmalar, yukarıdaki şartlarla birlikte varsa teknik şartname ve /veya numunedeki özellikleri aynen kabul etmiş sayılır.
3.5 Teklif mektubunun faks ile iletilmesi durumunda faks tarih ve saatinin güncel olmaması halinde teklif değerlendirmeye alınmayacaktır.
3.6, Kanun gereği 5.000 (beşbin) Türk lirasını aşan kısım ve İDARE'nin gerek gördüğü hallerde YÜKLENİCİ Vergi Dairesi borcu yoktur belgesi ibraz etmek zorundadır.
3.7 İdare, yapılan piyasa araştırması sonucunda verilen bütün teklifleri reddetmekte, yeniden piyasa araştırması yapmakta veya alımı iptal etmekte serbesttir. Bu durumda idare herhangi bir yükümlülük altına girmez.

TEKLİFİ VEREN KİŞİNİN, FİRMANIN:

Adı, Ünvanı :
Adres :
Tel/Faks :

Genel gereksinimler

Devlet kurumlarında uygulanmaya yönelik anti-virüs koruması, 4'ten az olmayacak bir kontrol ve spesifikasyon gereksinimleri seviyesinde ilgili Devlet Teknik Komisyonunun "Bilgiye yetkisiz erişimin engellenmesi. Bölüm 1. Bilgi koruma yazılımı. Beyan edilmeyen olasılıkların olmaması durumunda kontrol seviyesine göre sınıflandırma yönergeleri gereksinimlerine uygun olarak yetkili bir makam tarafından onaylanmalıdır (FSTEC veya Teknoloji ve İhracat Kontrolü için Federal Hizmetler veya FSTEC).

İşlenen bilginin gizlilik seviyesine bakmaksızın anti-virüs korumanın ortak bir aracı tüm bir kurum dahilinde kullanılmalıdır- Uzak bölgelerde yer alanlar dahil olmak üzere, ortak bir anti-virüs koruma sistemine bağlı olmayan bağımsız PC'ler entegre bir yazılım tarafından korunmalı ve bu yazılım her türlü kötü amaçlı programlara (anti-virüs), istenmeyen e-postalara (kişisel istenmeyen e-posta önleyici) ve ağ saldırılarına (kişisel güvenlik duvarı) karşı koruma sağlamak ve anti-virüs korumasının ortak araçlarına dahil edilme imkanına sahip olmalıdır.

Yönetim araçları dahil olmak üzere tüm anti-virüs ürünlerinin program arabirimi İngilizce olmalıdır.

Yönetim araçları dahil olmak üzere tüm anti-virüs ürünleri İngilizce dilinde içeriğe bağlı bir yardım sistemine sahip olmalıdır.

Anti-virüs koruma ürünü asgari şunları içermeli/desteklemelidir:

- iş istasyonları ve sunucular için anti-virüs koruma yazılımı;
- e-posta ve internet ağ geçitleri için anti-virüs koruma yazılım;
- istenmeyen toplu e-posta - istenmeyen postadan koruyan kullanıcı koruma yazılımı;
- mobil cihazlar (akıllı telefonlar) için anti-virüs koruma yazılımı;
- merkezi yönetim, izleme ve güncelleme yazılımı;
- kötü amaçlı program ve saldırıların güncellenmiş imza veri tabanı;
- İngilizce dilinde işletim kılavuzu

Istenilen tüm ürün altapısında kullanan iş istasyonları için anti-virüs koruma sistem yazılımı aşağıdaki işletim sistemleri üzerinde sistemlerin sürümlerinden bağımsız 32/64 bit olarak sorunsuz çalışmalıdır:

Lisans geçerlilik süresi boyunca versiyon guncellemeri ucretsiz sunulmalıdır

Microsoft Windows ailesine ait işletim sistemlerini kullanan iş istasyonları ve sunucular için anti-virüs koruma yazılımı için gereksinimler

Microsoft Windows ailesine ait işletim sistemlerini kullanan iş istasyonları için anti-virüs koruma sistem yazılımı aşağıdaki işletim sistemleri üzerinde sistemlerin sürümlerinden bağımsız 32/64 bit olarak sorunsuz çalışmalıdır:

Istemci sistemleri; Windows 7, Vista, Windows 8, Windows 8.1, Windows 10 istemci sistemleri

Server sistemleri : Windows Server 2003, Windows Server 2003R2, Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2 , Windows Server 2016, Windows Server 2019

Eposta sistemleri: Windows Exchange Server 2007, Windows Exchange Server 2010, Windows Exchange Server 2013, Windows Exchange Server 2016, Windows Exchange Server 2019

Microsoft Windows ailesine ait işletim sistemlerini kullanan iş istasyonları ve sunucular için anti-virüs koruma yazılımı aşağıdaki işlevselliklere sahip olmalıdır:

- yerleşik anti-virüs izlemesi;
- ağ saldırı koruma yazılımı;
- daha önce bilinmeyen kötü amaçlı yazılımın tanımlanmasına ve engellenmesine imkan veren sezgisel çözümleyici;
- gizli işlemlerin algılanması;
- kullanıcı veya yöneticinin talebine göre ve belli bir çizelgeye göre anti-virüs taraması;
- PKLITE, LZEXE, DIET, EXEPACK, vb. programlar kullanılarak paketlenmiş dosyaların anti-virüs kontrolü ve temizlenmesi;

- şifre korumalı dosyalar dahil olmak üzere RAR, ARJ, ZIP, CAB, LHA, JAR, ICE biçimlerini kullanan arşivlerde dosyaların anti-virüs kontrolü ve temizlenmesi;
- Bilgisayarda kullanılan uygulamalar ve çatıştırılabilir dosyalar hakkında, bulut bilişim tabanlı teknoloji kullanılarak çevirim içi kipte karar alma becerisi;
- e-posta yazışmalarının kötü amaçlı yazdım ve istenmeyen postadan korunması. Aşağıdaki iletişim kurallarına dayanan trafiğin taranması:
- Kullanılan e-posta istemcisinden bağımsız olarak, IMAP, SMTP, POP3;
- E-posta istemcisinden bağımsız olarak NNTP (sadece virüs taraması);
- Microsoft Office Outlook ve The Bat! e-posta programlarında yer alan eklentilerin çalıştırılmasının bir parçası olarak iletişim kuralı türünden (MAPI, HTTP dahil) bağımsız olarak;
- HTTP trafiğinin korunması— kullanıcı bilgisayarına HTTP/FTP iletişim kuralı yoluyla giren tüm nesnelerin taranması;
- Komut dosyalarının taranması — İnternet dahil, kullanıcı bilgisayarda çalışırken başlatılan diğer WSH komut dosyalarının (JavaScript, Visual Basic Script, vb.) yanı sıra Microsoft Internet Explorer tarafından geliştirilen tüm komut dosyalarının taranması;
- internet sohbet istemcileri ile çalışırken güvenliği temin etmek için, ICQ ve MSN trafiğinin taranması;
- görevlerin çizelgeye göre ve/veya işletim sisteminin yüklenmesinden hemen sonra başlatılması;
- kötü amaçlı yazılım tarafından değiştirilen sistem kayıt defteri değerlerinin otomatik olarak geri alınması seçeneği ile birlikte, sistem kayıt defterindeki değişikliklere ve davranış analizine dayanan henüz bilinmeyen kötü amaçlı yazılımlara karşı koruma;
- Uygulamaların sisteme zararlı olabilecek eylemlerini önleyen ve sistem kaynaklarına ve korunan verilere erişimini denetleyen uygulama denetimi özelliği;
- izinsiz giriş tespit ve önleme sistemi (IDS/IPS) ile birlikte bir güvenlik duvarı kullanarak bilgisayar korsam saldırılarına karşı koruma ve kablosuz ağlar dahil olmak üzere her türlü bilgisayar ağında çalışırken daha popüler uygulamalar için ağ etkinliği kuralları;
- IPv6 protokol desteği;
- maskeleme programlarından, ödemeli sitelerdeki yeniden arama programlarından korunma, reklam başlıklarının, açılır pencerelerin ve web sitelerinden indirilen kötü amaçlı senaryoların engellenmesi, e, dolandırıcılık sitelerinin tanımlanması;
- Uygulamaların çalıştırılma işlemlerini aşağıdaki kurallara göre belirleyen kurutum/başlangıç denetimi. uygulamanın çalıştırılabilir dosyasının bulunduğu klasör yolu, meta data (uygulamanın çalıştırılabilir dosyasının gerçek adı, uygulamanın sürücü üzerinde bulunan çalıştırılabilir dosyasının adı, uygulamanın çalıştırılabilir dosyasının sürümü, uygulama adı ve uygulama üreticisi), uygulamanın çalıştırılabilir dosyasının MD5 hash bilgisi;
- kullanıcının harici giriş/çıkış cihazları ile çalışması üzerinde kontrol, harici USB taşıyıcılara, çoklu ortam cihazlarına ve diğer veri depolama cihazlarına erişimin sınırlandırılması;
- otomatik çalıştırma işlevselliğinin engellenmesi;
- en son kontrolden beri durumu değişmeyen nesneleri atlayarak tarama sürecinin hızlandırılması;
- Zayıf noktalan taranması için özelleştirilmiş bir görev, sonuçlar rapor olarak alınabilmelidir

Windows Update üzerinden zorlama yoluyla Microsoft uygulamalarının güncellenmesi;

- dosya alanını tararken kullanıcı için rahat çalışma koşutlarını temin etmek için PC kaynaklarının kullanıcı tarafından esnek kullanımı;
- bilgisayarın kritik bölümlerinin bağımsız görev olarak taranmasının ayarlanması;
- otomatik koruma uygulaması, bir uygulama hizmetinin yetkisiz bir şekilde uzaktan yönetimine karşı koruma ve ayrıca şifre ile uygulama parametresine erişim koruması, kötü amaçlı yazılım, suçlu veya amatör kullanıcıların korumayı devre dış bırakmasını engelleme;

- hangi anti-virüs bileşeninin kurulacağını seçme imkanı:
- merkezi yönetim sisteminee yönetim.

Akıllı telefonlar için anti-virüs koruma yazılımı için gereksinimler

Akıllı telefonlar için anti-virüs koruma yazılımı aşağıdaki işletim sistemlerinde çalışmalıdır:

Android sistemler	:	Android 4.4 ve diğer üst sürümlerce destkeleniyor olmalıdır
IOS sistemler	:	IOS 10 ve diğer üst sürümlerce destkeleniyor olmalıdır
Windows mobile	:	Windows 6.1 ve diğer üst sürümlerce destkeleniyor olmalıdır

Akıllı telefonlar için anti-virüs koruma yazılımı aşağıdaki işlevselliklere sahip olmalıdır:

- akıllı telefon dosya sisteminin aşağıdaki şekilde sürekli olarak kontrolü, engelleme ve tarama:
  kişisel bilgisayar ile senkronizasyon ve bir tarayıcı üzerinden dosya indirme işlemi sırasında kablosuz bağlantılar (infrared bağlantı noktası, Bluetooth), EMS ve MMS kablosuz bağlantıları yoluyla aktarılan tüm gelen nesneler;
- akıllı telefonda açılan dosyalar;
- akıllı telefon ara yüzünden kurulan programlar.
- kullanıcının isteği üzerine veya bir çizelgeye göre akıllı telefon veya bağlı bellek genişletme kartı üzerindeki dosya sistem nesnelerinin taranması;
- karantina deposundaki virüslü nesneleri güvenilir bir şekilde ayırma:
- kötü amaçlı programları ararken ve tehlikeli nesneleri silerken, kullanılan anti-virüs veri tabanını güncelleme;
- istenmeyen SMS ve MMS iletilerinin engellenmesi:
- klasör ve bellek kartlarının şifrelenmesi;
- kullanıcıya telefon rehberi girişleri, SMS'ler ve çağrı kayıtları dahil olmak üzere, belirli bir kişi ile ilgili her şeyi kolay bir şekilde gizleme ve açığa çıkarma olanağı sağlayan gizlilik koruması;
- hırsızlığa koruma işlevi gerçekleştirme; örneğin mobil cihazın bloke edilmesi, verilerin ve kişilerin silinmesi, kayıp cihazın yerinin belirlenebilmesi ve ayrıca kayıp cihazın kimde olduğunun saptanması.

Anti-virüs koruma yönetim sistemi için gereksinimler

Microsoft Windows ve Novell Netware platformları, Linux işletim sistemleri, MAC OS dosya sunucuları ve iş istasyonları, Microsoft Windows Mobile ve Symbian platformu üzerinde çalışan mobil cihazlar üzerinde oluşturulan tüm korunmuş kaynaklar için yönetim yazılımı aşağıdaki işletim sistemleri üzerinde çalışmalıdır:

Yönetim sunucusu:

- Microsoft Windows Server 2012 R2 ve üstü

Yönetim sunucusu aşağıdaki veri taban: yönetim sistemlerini kullanmalıdır:

- Microsoft SQL Server 2008 r2 ve üstü:
- MySQL 5.5 ve üstü

Yönetim aracısı:

- Microsoft Windows Server 2003 ve üstü tüm sğrğmler
- Microsoft Windows 7 Professional/Enterprise/Ultimate (x32/x64) ve üstü tüm sürümler

Microsoft Windows iş istasyonları ve sunucuları. Microsoft Windows Mobile ve IOS platformu üzerinde çalışan mobil cihazlar üzerinde oluşturulan tüm korunmuş kaynaklar için yönetim yazılımı aşağıdaki işlevselliklere sahip olmalıdır:

- tek bir dağıtım diskinden anti-virüs koruma sistemi kurulumu;
- korunmuş bileşen sayısına bağlı olarak kurulumun seçimi;
- Etkin Dizin yapısına bağlı olarak mantıksal ağ gruplarının oluşturulması;
- Atanmamış bilgisayarların, yönetilen bilgisayarlar grubuna otomatik olarak yeniden konumlandırılması;
- anti-virüs koruma yazılımının merkezi olarak kurulumu/güncellemesi/silinmesi, yazılım işlemlerinin ayarlanması, yönetilmesi, raporların ve istatistiksel bilgilerin görüntülenmesi;
- uyumsuz yazılımların merkezi olarak silinmesi;
- Uygulamaların çalıştırılma işlemlerini aşağıdaki kurallara göre belirleyen merkezi kurulum/başlangıç denetimi: uygulamanın çalıştırılabilir dosyasının bulunduğu klasör yolu, meta data (uygulamanın çalıştırılabilir dosyasının gerçek adı, uygulamanın sürücü üzerinde bulunan çalıştırılabilir dosyasının adı, uygulamanın çalıştırılabilir dosyasının sürümü, uygulama adi ve uygulama üreticisi), uygulamanın çalıştırılabilir dosyasının MD5 hash bilgisi;
- Önceden belirlenmiş kategorilere göre internet sitelerinin denetimini sağlayan ve veri tiplerine göre karşıdan dosya yüklemelerini kısıtlayan merkezileştirilmiş internet denetimi;
- çeşitli anti-virüs koruma yazılım kurulumu yöntemleri: uzaktan yöntemler - RPC, GPO, giriş komut dosyası, ağ aracısı, yerel yöntem - bağımsız kurulum paketi;
- uygulama veri tabanlarının en son sürümlerinden anti-virüs koruma yazılımının uzaktan kurulumu
- anti-virüs koruma yazılımı ve anti-virüs veri tabanlarının otomatik güncellemesi
- otomatik lisans dağıtım;
- Ağdaki bilgisayarlar için zayıf nokta taraması, yazılımlarda tespit edilen zayıf noktalar için rapor sağlama, Windows Update üzerinden Microsoft uygulamalarının güncellemelerini zorlama;
- istemci makinelerine dağıtım öncesinde yönetim sunucusu kaynaklarını kullanarak yüklenen güncellemelerin testi; alınmasından hemen sonra kullanıcı iş istasyonlarına güncellemelerin teslimi;
- Tek bir konak makinede çalışan çok sayıda sanal makinenin yük dengelemesi için sanal makine tanıma sistemi;
- Harici USB veri taşıyıcılarına, çoklu ortam cihazlarına ve diğer veri depolama cihazlarına erişimi kısıtlayan, kimlik belirleyicilere göre güvenli cihazlar yaratan ve cihazlara belirtilen kullanıcıların erişiminin sağlandığı, kullanıcıların harici girdi/çıktı (input/output) cihazlarına erişiminin merkezi denetimi;
- yönetici ve operatör rollerinin ve ayrıca her seviyede sunulan rapor biçimlerinin ayarlanma seçeneği ile birlikte, çok seviyeli bir yönetim sisteminin oluşturulması;
- Yönetim konsolu üzerinden, ağdaki bilgisayarların bulut bilişim sistemine erişiminin sağlanması;
- iletişim kanalları ve teknik bilgi taşıyıcıları aracılığıyla, farklı kaynaklardan yazılım ve anti-virüs veri tabanlarını güncelleme;
- Sanal köle yönetim sunucuları oluşturma özelliği;
- anti-virüs koruma durumu hakkında bilgilerin merkezi olarak toplanması ve raporların oluşturulması;
- Ağ'da kullanılan donanım cihazlarının envanter bilgisinin çıkarılması;
- Ağ'da kurulu olan uygulamaların envanter bilgisinin çıkarılması;
- kurulu anti-virüs koruma uygulamalarının çalışması ile ilgili olaylar hakkında bildirim mekanizmasının mevcudiyeti ve bunlar hakkında e-posta ayarlanması;
- istemci bilgisayarlarına kurulu tüm uygulamalar hakkında bilgilerin merkezi olarak toplanması;
- Cisco NAC ve Microsoft NAP ile entegrasyonu;

- raporların PDF ve XML dosya biçimlerinde dışa aktarılması;
- anti-virüs yazılımının kurulu olduğu tüm ağ kaynakları üzerinde yedekleme depolama ve karantina konumları nesnelerinin merkezi olarak yönetilmesi;
- yönetim sistemi yedek kopyalarını oluşturma olanağı;
- Windows Faiiover Clustering desteği;
- İnternet Konsolu (Web-Console) üzerinden anti-virüs koruma yönetimin ve izlemesinin sağlanması;
- virüs salgını ortaya çıktığında kontrol altına almak için, sistem mevcudiyeti.

Anti-virüs veri tabanlarını güncelleme gereksinimleri

Güncellenmiş anti-virüs veri ttabanları aşağıdaki işlevselliklere sahip olmalıdır:

- bir takvim günü boyunca 24 kezden az olmayacak şekilde anti-virüs veri tabanlarının istenmeyen postadan korunma veri tabanlarının en az 5 dakikada bir düzenli olarak güncellenmesi;
- iletişim kanalları aracılığıyla ve belirlenmiş elektronik veri taşıyıcıları ile çeşitli güncelleme yolları;
- elektronik dijital imzalar kullanarak güncellemelerin bütünlüğünün ve doğruluğunun kontrolü.

İşletim kılavuzlarının gereksinimleri

Yönetim araçları dahil olmak üzere tüm anti-virüs koruma yazılımları için işletim kılavuzu, aşağıdakiler dahil olmak üzere hükümet standartları gereksinimlerine uygun olarak İngilizce dilinde hazırlanmış belgele i içermelidir:

• kullanıcı (yönetici) klavuzu.

Anti-virüs ürünleri ile teslim edişmiş belgeler, ilgili anti-virüs koruma ürününün kurulumu, ayan ve işletimini ayrıntılı bir şekilde açıklamalıdır.

Teknik destek gereksinimleri

Anti-virüs koruma yazılımı için teknik destek:

Türkiye'de, Hafta içi 5 gün 09:00-18:00 saatleri arasında, Cumartesi günleri 10:00 -16:00 saatleri arasında telefon, e-posta ve internet yoluyla anti-virüs koruma ürün geliştiricisi ve ortaklarının onaylı uzmanları tarafından Türkçe dilinde sunulmalıdır;

Anti-Virüs Koruma Yazılımı geliştiricisinin internet sitesinde, Anti-Virüs Koruma Yazılımı için teknik desteğe has özel bir bölümü olmalı, bilgi veri tabanları ile güncellenmeli ve ayrıca yazılım ürün kullanıcılarına yönelik Türkçe dilinde bir forum da olmalıdır.