**SİNCAN AĞIZ VE DİŞ SAĞLIĞI MERKEZİ BİR YIL SÜRELİ CİHAZ DAHİL AĞ GÜVENLİK SİSTEMİ VE ANTİVİRÜS**

**KORUMA YAZILIMI HİZMET ALIMI**

**Güvenlik Duvarı**

1 Kurum bilişim ağı güvenliği ve yönetimi için her bölge için l(bir) adet olmak üzere

konumlandırılacaktır.

2 **l{Bir)Yıl** süreyle, destek, veritabanı ve sürüm güncellemeleriyle teklif edilecektir

3 Teklif edilecek ürün yedekli (Htgh-Available) olarak çalışabilecek yetenekte olacaktır,

4 Cihazlar donanım yazılım bütünleşik olup, firmware cihaz üzerinde gelmelidir.

5 Firmware yaşam döngüsü, alınacak destek, güncelleme hizmeti süresince işletilecek,

yazılımların yeni sürümlere yükseltilmesi, veritabanlarının güncellenmesi, uygulama

imzalarının güncellenmesi sözleşme kapsamında ücretsiz gerçekleştirilecektir. Ürünler, bu

işlemleri İnternet üzerinden otomatik veya offline olarak yapabilmelidir. Yükseltme ve

güncelleme işlemleri sırasında cihazın kapatılması, bakıma alınması veya tümden yeniden

başlatılması gibi gereksinimler bulunmayacaktır.

6 Hizmet vermek için kullanılacak ürünlerde, kullanıcı sayısı, kura! sayısı, VPN / SSL VPN Client

sayısı gibi lisans sınırları bulunmayacak, tüm yapı sınırsız kullanıcılı olacaktır.

7 Ürünlerde IP/Mac eşlemeleri, LDAP ve Active Directory (Aktif Dizin) kullanıcılarına göre izinler

uygulana bilmelidir.

8 Kullanılacak güvenlik ürünleri, Avrupa Birliği veya Türkiye menşeiliyse, Avrupa Birliği Marka

Tescil Belgesine ve üretimin yapıldığı ülkeden alınmış Kapasite Raporuna sahip olmalıdır.

9 Ürünler en az 2(îki) yıl garanti kapsamında olacaktır. Teklif edilen ürünlerle ilgili, alınacak

destek hizmeti süresince 5gün x 9saat uzaktan destek verilecektir.

10 Teklif edilen ürünler en az EA14+ güvenlik seviyesinde sertifikalı olmalıdır.

11 Ürünle ilgili eğitim, en az ileri seviye ürün sertifikalarına sahip üretici personelleri tarafından

verilecektir.

12 Ağda konumlandırılacak güvenlik cihazı üreticisi, en az bir kez Tübitak Ortak Kriterler Test

Merkezinde veya uluslararası geçerliliği olan diğer Ortak Kriterler Test merkezlerinde

sertifikasyon sürecinden geçmiş, ARGE süreçlerini sertifikasyona göre uyguluyor olmalıdır.

13 Güvenlik Duvarı uygulama katmanında tarama yapabilen, SPI (Stateful Packet Inspection)

özelliğinde olacaktır.

14 Web-arabirimi veya kendine özel yönetim uygulama (GUI) arabirimi üzerinden, tek tek elle

tanımlama yapmadan, otomatik, tüm ağ IP-MAC adreslerini sabitîeme özelliğini

desteklemelidir.

15 Köprü(Bridge), Yönlendirîci(Router) olarak çalışabilmek, NAT PAT dönüşümlerini

yapabilmelidir.

16 Ethernet portlarınm her birini LAN, WAN, DMZ için kullanılabilir olup, iki veya daha fazla

porta WAN çıkışı görevi verilebilecektir. WAN çıkışlarının yedeklîliğî tanımlanabilmelîdir.

17 Birden fazla WAN hattı olması halinde VPN bağlantılarının bu hatlar üzerinden otomatik

yedekli şekilde çalışmasını sağlayabilecektir. Bîr WAN hattı koptuğunda VPN bağlantısını

diğer hatta aktarabilecektir.

18 Cihaz üzerine bîr USB 3G Modem takıldığında, bu hattı bîr WAN çıkışı olarak görebilmelidir.

19 Servis kalitesi protokolü (QoS) ve bant genişliği yönetimi (Bandwidth Management)

desteklemelidir.

20 Erişim, denetim ve yetkilendirme sistemine sahip olacaktır.

21 DHCP sunucu görevini üstlenebilecektir.

22 VPN işlemlerinde IPSec, PPTP, L2TP, 3DES, AES, MD5, SHA-1 ve PKI desteklenmelidir.

23 Kurumsal uygulamalara güvenli uzak bağlantılar kurabilmek için SSL VPN altyapısı

sağlamalıdır. Ürün aynı marka SSL VPN istemci yazılımlarıyla birlikte sunulacaktır.

24 Ürünler yeni nesil özelliklere sahip olacak, dahili bir DPI motoru ve en az 2000 adet uygulama

imzasıyla birlikte sunulacaktır. Application Control özellikleriyle, uygulama kontrolü

yapabilmelidir.

25 Sistem MS Active Directory ile entegre olarak kişi ve grup firewall kurak yazılmasına olanak

sağlayacaktır. Tutulan kayıtlarda kullanıcı ismi yer alacaktır. Bu sayede trafiği yaratan kullanıcı

isim ile takibinin yapılabilmesine olanak sağlayacaktır

26 Ürün üzerinde uygulanmış 10 eski konfîgürasyona ürün ara yüzünden geri dönülebilmelidir.

Cihaza özel ayarların yedeğinin alınabilmesi ve yedekten geri yükleyebilme mümkün

olmalıdır.

27 Saldırı Önleme Sistemi, en az 5000 adet saldırı imzasını veritabanında bulundurmalıdır.

28 Saldırıların tespitinde dâhili bir saldırı veritabanından taramanın yanında, anormallik tespiti

(anomaly detection) de yapabilmelidir.

29 Ürünler dahili olarak en az 50 GB log depolayabilmek, e-imza kanununda belirtildiği özelliklere

sahip nitelikli bir zaman damgasıyla işlenerek saklanabilmelidir. Dahilî olarak bu maddenin

sağlanamaması halinde aynı işlevleri yerine getirmek üzere, ürünlerle aynı marka, en az 1.500

log/sn log yazma performansına sahip bir loğlama çözümü, ürün adeti kadar teslim

edilmelidir.

30 İstenmesi halinde üretilen loğlar oluştuğu anda veya belli zaman aralıklarında merkezi loğlama

sistemine yoîlanabilecektir. Ürün, loğlarını syslog sunuculara gönderebilmek ve SNMP

arabirimi ile haberleşebilmelidir.

31 Raporlama sistemi, web tabanlı Özel bir ekrana sahip olacak ve buradan istenen sıklıkta ve

içerikte düzenli raporlar istenebilecektir.

32 Önceden tanımlanmış rapor bulunmalıdır. Tanımlanmış raporlar, içeriğine göre

daraitılabilmelidir.

33 Html, pdf ve benzer doküman formatlarında rapor üretebilmeiidir. Üreticinin ekleyeceği diğer

rapor tipleri güncellemeler île sisteme yüklenebiliyor olmalıdır.

34 Ürün, genel kullanıma açık laboratuarlar ve kablosuz ağlar için Kimlik No, Mac adresi, Şifre

yetkilendirmesi yapabilmeli, dahilî veritabanım, Aktif Dizin, RADIUS gibi kullanıcı

verltabaniarını bu amaçla kullanabilmeli ve bunların kanunen geçerli nitelikli zaman damgalı

log kayıtlarını tutabilmelîdir.

35 Sistem, SMS ile şifre istenerek yetkilendirmeyi desteklemelidir. SMS ile yetkilendirme

metodunda, kayıtlar GSM no ile ilişkîlendirilerek takip edilebilecektir.

36 Tutulan loğların 5651, e-imza ve ilgili diğer T.C. kanunlarına uygun olabilmesi için gerekli tüm

loğlama ve raporlama hizmetlerinin verilmesi Yüklenici sorumluluğundadır. Kanunen geçerli

nitelikli zaman damgası tanımı, T.C. e-imza kanununda yapılmıştır.

37 Ürünler, web-arabiriminden (http, https), kendine özel yönetim uygulaması (GUI) arabirimi

üzerinden, konsoldan, telnet ve ssh arabiriminden yönetiiebilir olmalıdır.

38 Ürün GUI tabanlı arayüzleri sürükle-bırak ve kopyala-yapıştır kolaylığında olmalıdır.

39 Ürünlerin raporlama ekranları Türkçe ve İngilizce kullanılabilecektir. Konfîgürasyon ve diğer

yönetim ekranlarının Türkçe kullanılabilmesi tercih sebebidir.

40 GUI arayüz üzerinden veya TFTP ile firmware güncelleme yapılabilmelidir.

41 En az 3,5 Gbps performans (firewall throughput) değerine sahip olmalıdır.

42 Ürün üzerinde 6 adet 100/1000 gigabit olmalıdır.

43 Ürün eş zamanlı oturum sayısı en az 1.000.000 olmalıdır,

44 Hizmet süresinin bitimini takiben cihaz yükleniciye teslim edilecektir.

45 Ödemeler aylık periyodiar halinde yapılacaktır.

**ÂTİVİRÜS YAZILIMI ŞARTNAMESİ**

1.1.

1.2.

1.3.

1.4.

1.5.

1.6.

1.7.

1.8.

1.9.

**1**.**10**.

**1**.**11**.

1**,**12**.**

1.13.

1.14.

1.15.

Program Windows NT,Windows 2000, Windows 2003 , Windows XP, Windows

Vista, Windows 7, Windows 8 ve Windows 2008 (ve R2) üzerinde herhangi bir ek

yazıtım ya da yama yüklemeden tam uyumlu olarak çalışa bitmeli.32 bit ve 64 bit

işletim sistemleri için ayrı yükleme dosyalarına sahip olmalı ve tam uyumlu

çalışmalıdır.

Microsoft Office dokümanları için özel bir doküman koruma modülüne sahip

olmalıdır.

Microsoft Automated Installation Kit (AIK) ile anti virüs kurtarma CD si

haztrlanabilmelidîr.

Anti virüs programının kurulduğu bilgisayar bilgileri ayrıntılı bir şekilde merkezî bir

konsoldan alınabilmelidir.

Program güncellemelerini yöneticinin seçimine göre; normal, önceden yayın ve

geciktirilmiş olmak üzere 3 farklı güncelleme sunucusundan alabilmelidir.

Program, virüs imzalarıyla tanınmayan zararlıları tespit etmek, uygulamaların

istenmeyen davranışları yapmalarını kontrol edebilmek ve kayıt defteri erişimini

sınırlayabilmek için Host Saldırı Önleme Sistemi (HIPS) özelliğine sahip olmalıdır.

Yetkisiz medya aygıtlarının sisteme takılmasını engelleyebilmell, yöneticinin

istediği aygıtlara aygıt serî numarasına bağlı olarak kullanıcılar seçilerek

parametrik izinler verebilmelidir.

Program aygıtları depolama aygıtları, yazıcılar ve klavyeler, bellek kartı okuyucu,

bluetooth olarak ayırıp buna göre izinleri ve yetkileri ayarlayabilmelidir.

Program isteğe bağlı bulut tabanlı tarama teknolojisi UveGrid'i desteklemeli ve bu

sayede yeni virüslere karşı koruma hızını en üst seviye çekebîlmelidir.

Program satın alınan tek bîr paket ile Windows, MacOSX ve Linux platformlarına

koruma sağlayabilmeli ve bu platformlar için koruma yazılımları ayrı bir ücrete

tâbi olmamalıdır.

Ağ kaynaklarını daha verimli kullanabilmek için zamanlanmış güvenlik

görevlerinin belirlenen bir zaman aralığında rastgele çalıştı ra bilmeyi

desteklemelidir.

Program, güncellemelerin bilgisayar üzerinde yol açabileceği olası sorunları

önleyebilmek için, bir sorun ya da uyumsuzluk anında eski tarihli imzalara

dönebilmeyi desteklemelidir.

Ağ erişim güvenliği için Microsoft NAP (Network Access Protection) ile tam

entegre olarak çalışabîlmelidir.

Program, zararlı yazılımları tespit edebilmek için geleneksel imzaların yanı sıra

akıllı jenerik imzalar, pasif sezgisel tarama ve gelişmiş sezgisel tarama

yöntemlerinin tümünü kullanan tek bir tarama motoruna sahip olmalı ve bu

sayede bilinen tehditleri tespit ederken bilinmeyen tehditleri de hatalı alarm

üretmeden tespit edebilmelidir.

Program, mevcut donanımlar üzerinde herhangi ek bir yatırım gereksinimi

gerektirmeden uyumlu çalışabilme!!, minimum sistem kaynağı kullanımıyla

maksimum sistem korumasını sağlayabilmelidir.

1.16. Programın isteğe-bağlı virüs tarama özelliği, istenildiği zaman düşük öncelikli

olarak arka planda çalıştırılabilmeli böylece kullanıcı sistemde çalışırken de

performans düşmeden tarama işlemi yapılabilmelidir.

1.17. Programın hem Türkçe hem de İngilizce sürümü bulunmalı ve aynı lisansla her iki

dil sürümü de kullanılabilmelidir.

1.18. Programın kayıtlı tüm ayarlan hem istemci arabirim ile hem de konsol aracılığıyla

kolayca bir XML dosya olarak yedeklenebilip gerektiğinde XML dosya kolayca geri

başka bir sisteme taşınabllmeiidir. Bu dosya aynı zamanda kurulum parametreleri

olarak kullanılabilmelidir.

1.19. HTTP,HTTPS ve POP3,POP3S iletişim kuralları kullanan uygulamalarla entegre

olarak bu iletişim kurallarını otomatik olarak tarayabllme özelliğine sahip

olmalıdır,

1.20. Gelen ve giden tüm postaların taranması yaygın e-posta istemcileri Microsoft

Outlook, Outlook Express, Mozilla Thunderbird ve Windows Mail ile tam entegre

olarak çalışa bilmelidir.

1.21. Programın yönetim konsolunda rol tabanlı ayrıntılı yetkiler tanımlanabilmeli ve bu

yetkilere göre kullanılabilmeli ve kullanıcı aktivlteleri izlenebiimelidir.

1.22. Güvenlik duvarı, gerçek zamanlı koruma, web erişimi koruması ve istemci e-posta

koruması gibi koruma modüllerini uzaktan etkinleştirebilmeli ve devre dışı

bıraktiabilmelidir.

1.23. Yönetim konsolünde değişik istemci özelliklerine göre değişekn dinamik grup

tanımları yapılabilmeli, böylece istemcilerin bu gruplara otomatik olarak eklenip

çıkarılması sağlanmalıdır.

1.24. Kurumsal ağ üzerindeki güvenlik olaylarını tek bir noktadan grafiksel olarak takip

edebilmek için yönetim konsolünden ayrı olarak web tabanlı bir anlık rapor paneli

bulunmalıdır.

1.25. Program, CSV, txt, Windows olay günlüğü formatlarında günlükleri uç noktalarda

saklayabilmelidir.

1.26. Günlüklerin ve raporlama bölümü parametreleri isteğe göre ayarlanabilmeli ve

raporlar 50 farklı ön tanımlı şablon üzerinden tanımlanabilmelidlr,

1.27. Çıkarılabilir aygıtlar ile ilgili tüm eylemler Aygıt Kontrol Raporları sayesinde

ayrıntılı olarak kolayca raporlanabilmelldir.

1.28. Program log toplama ve yorumlama aracı RSA Envision ile t am uyumlu bîr

eklentiye sahip olmalıdır.

1.29. Program entegre Unilicense özelliği ile Mac , Windows ve Linux sistemler için

ayrıca lisans istemeden kullanılabilmelidir,

1.30. Program tek bir noktadan konsol ile uzaktan kurulabilmen, kaldırılabilmeli ve

yönetîlebilmelidir.

1.31. Program tüm bileşenleri için ayrı günlük dosyaları tutabilme!! ve bu günlük

dosyalan yönetim konsolundan kolayca izlenebiimelidir.

1.32. Geniş raporlama seçeneklerine sahip olmalı, belirli tarihler arası, istemciye göre,

virüs tipine göre v.b. kriterlere göre ayrıntılı raporlar alınabilmelidir.

1.33. Program yönetim konsolünde istemcilerin MAC adresi de görülebilmeii ve bu

sütun üzerinden işlem yapılabilmelidir.

1.34. Yönetim sunucusuna bağlanmak isteyen istemcilerin güvenliği için yönetim

sunucusu şifre doğrulamayı desteklemeli sadece yetkili şifreye sahip istemcilerden

bağlantı kabul edilebilmelidir.

1.35. İstemci sayısının fazlalığı ve lokasyon çokluğu ve uzaklığı durumlarında bîrden

fazla yönetim sunucu kurup bunları birbirine replike etmeyi ve tek bir noktadan

yönetmeyi desteklemelidir.

1.36. Ağ ortamında, ağ trafiğini korumak ve hızlı güncellemeler için merkezi tek veya

birden fazla güncelleme dağıtabîlme özelliğine sahip olmalıdır.

1.37. Kullanıcılar Floppy disk, hard disk, flash disk ve ağ sürücüleri üzerinde virüs

taraması yapabilmelidir.

1.38. İstenildiğinde kaldırılabilir medya sürücülerine (USB disk v.b.) erişim

engellenebîlmeli ve ayrıca istenen cihazlara ayrıcalık tanmabilmelidîr.

1.39. Kullanıcı bilgisayarlar üzerinde gerçek zamanlı tarama yapan bir modül sürekli

çalışmalı ve işletim sistemi çekirdeğine yapılan tüm erişimleri kontrol

edebilmelidir. Hard disk, Floppy disk, Flash disk ve diğer tüm yerel diskler

üzerindeki bir dosya üzerinde yapılan her işlemi(açma, değiştirme, yazma,

okuma) takip etmelidir.

1.40. Antivirüs programı kendi dosyalarını durdurmak ve değiştirmek isteyen zararlı

yazılımlara karşı sürekli güncellenebilir bir savunma mekanizmasına sahip

olmalıdır.

1.41. Gerçek zamanlı taramada ön tanımlı olarak tüm dosya tipleri taramaya dahil

edilmeli (Tüm sistem dosyaları, tüm sıkıştırılmış dosya formatları, tüm imaj dosya

formatları, v.b.) istenirse bazı dosya tiplerinin, dosyaların ve klasörlerinin tarama

dışı bırakılması sağlanabilmelidir.

1.42. Tarama için dosya büyüklüğü, dosya tarama zamanaşımı limitleri istenildiği gibi

belirlenebilmelidlr.

1.43. Arşiv dosyalarını taramada, sıkştırma katı ve dosya boyutu belirienebllmelidir.

1.44. Tarama ve temizlemede kolaylık sağlamak için 3 konumdan oluşan bir temizleme

sistemi olmalı.

1.45. Bilgisayara gelen giden SSL trafiğini tarayabilmelidir.

1.46. Daha önce başka bir virüs programı olmayan temiz sistemlerde yüklendikten

sonra bilgisayarın yeniden açılıp kapanması gerekmemelidir.

1.47. Güncellemeden sonra bilgisayarın kapatılıp açılma ihtiyacı olmamalıdır.

1.48. Kullanılacak yazılımın Virüs, Trojan ve Spyware konusunda Checkmark Level

1 (Tespit) ve Level 2(Temizieme) sertifikası bulunmalıdır.

1.49. Kullanıcı tarafında Antivirüs istenildiğinde "Sessiz Kip"te çaiışabilmeli, antivirüs

uyarıları sadece sistem yöneticisine yönlendirliebîlmeiidîr.

1.50. Tarama sırasında tespit edilen virüslü dosyalar karantinaya alınabilmeiidîr.

İstenirse karantinadan belirli bir iokasyona geri aiınabîlmeiî ya doğrudan ya da

yönetim sunucusu aracılığıyla virüs analiz laboratuarlarına gönderilebilmelidir.

1.51. Karantinaya alınan virüslü dosyalar özel kriptolanmış bir klasöre otomatik olarak

kopyalanmak ve bu dosya içinde durduğu süre içinde virüs aktif durumda

olmamalıdır.

1.52. Programda bir uyarı oluşturulduğunda ilgili mesaj e-posta ya da Windows

Messenger aracılığıyla istenilen kullanıcılara veya adreslere iletilebümelîdir.

1.53. Programı esneklik ve tam sistem güvenliği açısından mobil kullanıcıların hem

firma içindeyken hem de firma dışına çıktıklarında otomatik olarak

güncellemelerini sağlanmalıdır.

1.54. Programının yönetim konsolu Windows NT /2000 / 2003/ 2008/ XP / Vista *7*

sistemlere kurulabilmek ve Windows tabanlı ayrı bir uygulama olmalıdır. Konsol

MMC tabanlı veya web

1.55. Programın yönetim konsolu ve sunucusu verilerini Microsoft Access, Microsoft SQL

Server, MySQL Server ve Oracle database lerin tamamında saklayabilir olmalıdır.

1.56. Programın yönetim konsolu, istemcilerde ve sunucu üzerinde oluşan olayları sahip

olduğu Uyarı Yöneticisi (Notification Manager) aracılığıyla istenildiğinde mail ile

,Messenger ile ve SNMP aracılığı İle yöneticiler gönderebilmeli.

1.57. Programın yönetim konsoiundeki Politika Yöneticisi(Poiicy Manager) aracılığıyla

hiyerarşik politikalar (policy) tanımlanabilmeli, bu politikalar istenilen grup,

kullanıcıya uygulanabilmen, oluşturulan politikalar istenildiğinde Politika

Yöneticisi(Policy Manager) aracılığı ile birleştiriiebiimell.

1.58. Programının yönetim konsolundan ağ içerisindeki kullanıcıların antivirus yazılımı

ayarlamaları ister ayrı ayrı, ister gruplar halinde yapılıp, ilgili kullanıcılara

dağıtılabilmelidir,

1.59. Programın sunucu bileşeni istenildiğinde WindowsNT Windows XP , Windows Vista

ve Windows 7 gibi sunucu işletim sistemi olmayan sistemlere de kurulabilmelidir.

1.60. Antivirus Programının tutacağı log süreleri ve boyutları kullanıcı tarafından

belirlenilebilmelidir.

1.61. Antivirus programı istemcisi, ajan(agent) olmamalı, gerektiğinde lisans bilgileri

girilerek yerel sunucudan bağımsız olarak çalışabllmetidir.

1.62. Antivirus programı istenirse, gelen ve giden maillerin altına, mailin hangi virüs

imza veri tabanı ile tarandığını ekieyebllmelidir.

1.63. Antivirus programı yüklemeler için e-mail ile gönderilebilecek yada bir

paylaşımdan çalıştırılabilecek bir exe dosyası oluşturabilme)! ve bu dosya 500 KB'

dan daha büyük olmamalıdır.

1.64. Antivirus yönetim konsolundan uzaktan yükleme yapılabildiği gibi kaldırma işlemi

de desteklenmelidir.

1.65. Antivirus yönetim konsolu istemci makinelerin grup bilgilerini active directory

içerisinden alabilmelidir.

1.66. Antivirus yönetim konsolu aynı kuruma ait birden fazla lisansı yönetimsel olarak

kullanabilmelidir.

1.67. Antivirus Programı île ilgili teknik destek ücretsiz, Türkçe ve yurtdışı kaynaklı

olarak İngilizce verilebilmelidir.