DOĞUŞ ÜNİVERSİTESİ

MERKEZİ UZAKTAN YÖNETİLEBİLİR GÜVENLİK YAZILIMI (ANTİVİRÜS)

TEKNİK ŞARTNAMESİ

1. AMAÇ

Bu teknik şartname, Doğuş Üniversitesi bünyesinde kullanılan tüm istemci ve sunucu sistemlerinde merkezi olarak yönetilebilecek, ağdan bağımsız çalışabilen ve sanallaştırma destekli gelişmiş güvenlik özelliklerine sahip kurumsal güvenlik yazılımı (antivirüs/endpoint protection) tedarikini tanımlamak amacıyla hazırlanmıştır.

2. KAPSAM

- Tüm istemci bilgisayarlar, dizüstü sistemler, sanal makineler ve sunucular
- Kuruma ait yerleşkelerdeki tüm segmentlerdeki cihazların güvenliği
- Offline (ağ dışı) durumlarda da çalışabilen yapılar
- Minimum**1.485 lisans**

3. GENEL TEKNİK ÖZELLİKLER

3.1 Merkezi Yönetim

- Tüm istemcilerin tek bir merkezi arayüz üzerinden izlenebilmesi ve yönetilebilmesi
- Cihaz durumu, tehdit geçmişi, yazılım sürümleri ve güvenlik açıklarının raporlanabilmesi
- Uzak masaüstü bağlantısı ve cihaz üzerinde işlem yapılabilmesi (dosya silme, yeniden başlatma vb.)
- Kullanıcıya görünmeden arka planda çalışan "stealth mode" servis desteği
- Web tabanlı yönetim arayüzü, çok seviyeli kullanıcı yetkilendirme (admin/read-only)

3.2 Tehdit Algılama ve Koruma

- Gerçek zamanlı virüs, malware, trojan, spyware, rootkit, zero-day tehdidi algılama
- Sandboxing: bilinmeyen uygulamaları sanal ortamda analiz ederek davranışsal koruma
- Antivirüs motoru güncellemelerinin otomatik ve zamanlanabilir olması
- WIPS/WIDS desteği ile sahte yazılım ve zararlı aktivitelerin algılanması

3.3 Sanallaştırma ve İzolasyon

- "Containment" özelliği ile şüpheli uygulamaların izole edilmesi
- DeepFreeze vb. yapılarla uyumluluk, sanal ortamda analiz edebilme
- İzole ortamda işlem yaparak istemciye zarar vermeden analiz imkânı

3.4 Yama ve Güncelleme Yönetimi

- Windows ve 3. parti yazılım yamalarını merkezi olarak takip etme ve güncelleme
- Kritik güvenlik açıklarının takibi ve otomatik giderilmesi
- Zamanlı yama/paket yayını ve test ortamı desteği

3.5 Prosedür ve Dosya Yönetimi

- Uzak uçlara toplu dosya gönderme, betik/prosedür çalıştırma
- Yazılım kaldırma, yükleme veya konfigürasyon işlemlerinin merkezi uygulanması
- Otomasyon desteği: belirli koşullarda belirli eylemlerin tetiklenmesi

3.6 Uyum ve Performans

- Windows, MacOS ve Linux istemcilerle uyumluluk
- Masaüstü ve mobil sistemlerde koruma sunabilme
- Ağ bağlantısı olmadan da (offline) çalışabilme
- Kurulu cihazların performansını düşürmemeli, minimum kaynak tüketimi ile çalışmalıdır

4. LİSANSLAMA

- Minimum 3 yıl lisans süresi sağlanmalıdır
- Merkezi yönetim paneli bulut veya lokal opsiyonlu olmalıdır
- Güncel tehdit veritabanı ile entegre, sık güncellenen yapı olmalıdır
- Gerekli lisansların kapsamı, süresi ve teknik detayları açıkça belirtilmelidir
- Yıllık abonelik ya da süreli lisanslama modeli ile çalışan teklifler kabul edilmeyecektir

5. GARANTİ VE DESTEK

- Satıcı, yazılımın kurulum ve yapılandırma desteğini sağlamalıdır
- Garanti süresince üretici tarafından sağlanan yazılım desteği ve güvenlik güncellemeleri devam etmelidir
- Resmi distribütör üzerinden tedarik edilen ürünler kabul edilecektir, paralel ithalat veya yurtdışı garantili ürünler kabul edilmeyecektir
- Temel kurulum ve kullanım dokümanları Türkçe ve İngilizce olarak yazılı şekilde teslim edilmelidir