

UÇ NOKTA GÜVENLİĞİ ÜRÜN GRUBU KRİTERLERİ (EPP)

ÖNEMLİ NOT:

1- Kırmızı renkli başlık **ZORUNLU** ise altındaki bütün **zorunlu** maddeler karşılanmalı,
2- Kırmızı renkli başlık **OPSİYONEL** ise üretici başlık altındaki maddeleri karşılamak zorunda değildir,
fakat ilgili opsiyonel başlığı karşıladığını iddia eden üreticiler, başlıkların altında belirtilmiş olan tüm kriterleri sağlamalıdır.
Karşılanan opsiyonel başlıklar sertifikada belirtilecektir.

No	Başlık/Soru	ZORUNLU	OPSİYONEL
TO	1-Temel Özelliklerin; Güvenlik, Fonksiyon ve Performans Testleri		
TO_UNA	A - Uç Nokta Antivirüs		
TO_UNA_AG	1. Antivirüs Güvenlik ve Fonksiyon Testleri	Z	
TO_UNA_AG_ZY	1.1 Zararlı Yazılım ve Gerçek Zamanlı Koruma	Z	
TO_UNA_AG_ZY_1	Test öncesi, test sırasında ve sonrası ürünün internet erişimi tam mı?	Z	
TO_UNA_AG_ZY_2	Test öncesi ürün varsayılan ayarları mı kullanıyordu?	Z	
TO_UNA_AG_ZY_3	Zararlı Yazılımlara karşı koruma özelliği bulunuyor mu ve koruma başarılı mı?	Z	
TO_UNA_AG_ZY_4	Gerçek zamanlı koruma özelliği bulunuyor mu?	Z	
TO_UNA_AG_ZY_5	Sezgisel/Heuristic tehdit algılama özelliği bulunuyor mu ve koruma başarılı mı?	Z	
TO_UNA_AG_ZY_6	Kötü amaçlı yazılım kaldırma/karantinaya alma özelliği bulunuyor mu?	Z	
TO_UNA_AG_ZY_7	Talep üzerine ve erişim esnasında tarama özelliği bulunuyor mu?	Z	
TO_UNA_AG_ZY_8	Uygulama engelleme özelliğine bulunuyor mu?	Z	
TO_UNA_AG_ZY_9	Çevrimdışı ortamda koruma özelliği bulunuyor mu?	Z	
TO_UNA_AG_ZY_10	Kendini koruma özelliği(Servis güvenliği kontrolü) bulunuyor mu?	Z	
TO_UNA_AG_ZY_11	Bulut tabanlı koruma desteği var mı?	Z	
TO_UNA_AG_IK	1.2 İçerik Kontrolü	Z	
TO_UNA_AG_IK_1	Oltalama (Anti-Phishing) testi başarılı mı?	Z	
TO_UNA_AG_IK_2	Dolandırıcılık (Fraud) saldırılarına karşı koruyabiliyor mu?	Z	
TO_UNA_AG_IK_3	SSL sertifikalı web adresleri taranıyor mu?	Z	
TO_UNA_AG_IK_4	Zararlı sitelere girişi engelleyebiliyor mu?	Z	
TO_UNA_DO	2. Diğer Özellikler Fonksiyon Testleri	Z	

TO_UNA_DO_CK	2.1 Cihaz Kontrolü	Z	
TO_UNA_DO_CK_1	Eğer üründe cihaz kontrolü özelliği bulunuyorsa son kullanıcı bilgisayarına takılan donanımların kullanımlarını kural tabanlı özelliğine sahip mi?	Z	
TO_UNA_DO_GD	2.2 Güvenlik Duvarı	Z	
TO_UNA_DO_GD_1	Eğer üründe Güvenlik Duvarı özelliği bulunuyorsa uygulamanın ağ ve internet erişimi kontrol edilebiliyor mu?	Z	
TO_UNA_DO_GD_2	Eğer üründe Güvenlik Duvarı özelliği bulunuyorsa Bilinen uygulamalara otomatik erişim izni veriliyor mu?	Z	
TO_UNA_DO_GD_3	Eğer üründe Güvenlik Duvarı özelliği bulunuyorsa Port taramasına karşı koruma var mı?	Z	
TO_UNA_DO_EK	2.3 E-Posta Koruması	Z	
TO_UNA_DO_EK_1	Eğer üründe E-posta koruma özelliği bulunuyorsa Mail üzerinden gelen tehditlere karşı savunması başarılı mı?	Z	
TO_UNA_DO_G	2.4 Güncelleme	Z	
TO_UNA_DO_G_1	Çevrimdışı ortamlarda güncelleme desteği devam ediyor mu?	Z	
TO_UNA_DO_G_2	Her 24 saat içerisinde en az 1 güncelleme alıyor mu?	Z	
TO_UNA_DO_G_3	İmza veritabanı artımlı güncellenebiliyor mu?	Z	
TO_UNA_DO_G_4	Ürün güncellemesi bulut veya güncelleme sunucuları üzerinden dağıtılabiliyor mu?	Z	
TO_UNA_DO_KK	2.5 Kurulum ve Kaldırma	Z	
TO_UNA_DO_KK_1	GPO veya IP ile kurulumu destekliyor mu?	Z	
TO_UNA_DO_KK_2	Yönetim paneli üzerinden veya sunucusu üzerinden yükleme ve kaldırma gibi işlevleri destekliyor mu?	Z	
TO_UNA_DO_KK_3	Uzaktan kurulum uygulamaları ile uyumlu mu?	Z	
TO_UNA_DO_KK_4	Kaldırma aracı desteği var mı?	Z	
TO_UNA_DO_DIS	2.6 Desteklenen İşletim Sistemleri (Aşağıdakilerden en az 1'ini desteklemelidir)	Z	
TO_UNA_DO_DIS_1	Windows desteği var mı?	Z	
TO_UNA_DO_DIS_2	macOS desteği var mı?	Z	
TO_UNA_DO_DIS_3	Linux dağıtımlarına desteği var mı?	Z	
TO_UNA_K	3. Kullanılabilirlik (Usability)	Z	
TO_UNA_K_1	False/positive alarmlar, exclusion veya white liste(hariç tutma) alınabiliyor mu?	Z	
TO_UNA_K_2	Taramalar sırasında zararsız yazılımlar etkileniyor mu?	Z	
TO_UNA_UNHY	4. Uç Nokta Hata Yönetimi	Z	
TO_UNA_UNHY_1	Ürünün hata yönetimi/denetimi günlüklemeleri/loglamaları yapılıyor mu?	Z	
TO_UNA_PT	5. Performans Testleri Ürüne ilişkin aşağıdaki testler yapılarak performans raporu alınmalıdır.	Z	

TO_UNA_PT_1	Dosya kopyalama testi	Z	
TO_UNA_PT_2	Arşivleme ve Arşivden çıkarma testi	Z	
TO_UNA_PT_3	Uygulama yükleme ve kaldırma testi	Z	
TO_UNA_PT_4	Uygulama başlatma testi	Z	
TO_UNA_PT_5	Web erişimi testi	Z	
TO_UNA_PT_6	Tarama sırasında veya uygulama yüklü olduğu durumlarda kaynak tüketimi	Z	
YP	B - Yönetim Paneli Güvenlik ve Fonksiyon Testleri		
YP_GT	1. Güvenlik Testleri	Z	
YP_GT_WT	1.1. Web Tabanlı Yönetim Paneli	Z	
YP_GT_WT_1	Oturum yönetiminde yetkilendirme kontrolü yapılıyor mu?	Z	
YP_GT_WT_2	SQL Injection'a karşı güvende mi?	Z	
YP_GT_WT_3	LDAP Injection'a karşı güvende mi?	Z	
YP_GT_WT_4	Cross-Site Scripting'a karşı güvende mi?	Z	
YP_GT_WT_5	Cross-Site Request Forgery'a karşı güvende mi?	Z	
YP_GT_MT	1.2. Masaüstü Tabanlı Yönetim Paneli	Z	
YP_GT_MT_1	Yönetim paneli eğer masaüstü uygulaması ise bireysel uygulama için gereken kontrolleri sağlıyor mu?	Z	
YP_GT_YP	1.3 Yönetim Paneli Hata Yönetimi	Z	
YP_GT_YP_1	Ürünün hata yönetimi/denetimi günlüklemeleri/loglamaları yapılıyor mu?	Z	
YP_FT	2- Fonksiyon Testleri Aşağıdaki maddeler sertifikasyon başarısı için opsiyonel kriterlerdir.		O
YP_FT_R	2.1 Raporlama		O
YP_FT_R_1	Olayları raporlayabiliyor mu?	Z	
YP_FT_R_2	Raporlar çeşitli zaman aralıklarına göre düzenlenebiliyor mu?	Z	
YP_FT_R_3	Raporlar dosya olarak çıkartılabiliyor mu?	Z	
YP_FT_R_4	Oluşturulan raporlar e-posta olarak gönderilebiliyor mu?	Z	
YP_FT_Y	2.2 Yedekleme		O
YP_FT_Y_1	Ürünün veri tabanı yedeklemesi yapılabiliyor mu?	Z	
YP_FT_G	2.3 Güncellemeler		O
YP_FT_G_1	Ürün versiyon güncellemeleri kontrol merkezinden dağıtılabiliyor mu?	Z	

YP_FT_G_2	Çevrimdışı ortamlarda güncelleme desteği devam ediyor mu?	Z	
YP_FT_AO	2.4 Ağ Ortamları		O
YP_FT_AO_1	Kontrol merkezi internetten bağımsız olarak çevrimdışı ortamda hizmet sağlayabiliyor mu?	Z	
YP_FT_YD	2.5 Yük Dengeleme		O
YP_FT_YD_1	Yönetim merkezi ulaşılmaması durumunda eş zamanlı hizmet veren yedek yönetim merkezi sunucusu var mı?	Z	
YP_FT_YD_2	Yedek yönetim merkezi sunucusu yönetim merkezinin bütün görevini yerine getirebiliyor mu?	Z	
YP_FT_IS	2.6 İşletim Sistemleri		O
YP_FT_IS_1	Yönetim panelinin Windows veya Linux desteği var mı?	Z	
YP_FT_T	2.7 Tarayıcılar		O
YP_FT_T_1	Güncel Microsoft tabanlı tarayıcı desteği var mı?	Z	
YP_FT_T_2	Güncel Mozilla Firefox desteği var mı?	Z	
YP_FT_T_3	Güncel Google Chrome desteği var mı?	Z	
YP_FT_ADE	2.8 Aktif Dizin Entegrasyonu		O
YP_FT_ADE_1	Merkezi yönetim konsolu AD bağlantısını sağlıyor mu?	Z	
YP_FT_SE	2.9 SIEM Entegrasyonu		O
YP_FT_SE_1	SIEM, Sylog gibi log toplama ve korelasyon sistemleri ile entegre olabiliyor mu?	Z	
YP_FT_KBY	2.10 Kural Bazlı Yönetim		O
YP_FT_KBY_1	Kurulan uygulamaların kural tabanları tek merkezden kontrol edilebiliyor mu?	Z	
YP_FT_KBY_2	Gruplara atanan kurallar sonradan eklenen cihazlara uygulanabiliyor mu?	Z	
YP_FT_KBY_3	Dinamik gruplara atanan kurallar her eklenen cihazı etkiliyor mu?	Z	
YP_FT_KBY_4	Tarama planlaması, cihaz kontrolü, zararlı yazılım engellemesi ve istisnai tanımlamalar, blacklist/whitelist yapılabiliyor mu?	Z	
YP_FT_UNGA	2.11 Uç Nokta Görev Atama		O
YP_FT_UNGA_1	Görev ile ajan kaldırılabilir mi?	Z	
YP_FT_UNGA_2	Görev ile yeniden başlatma veya kapatma işlevleri uygulanabilir mi?	Z	
YP_FT_UNGA_3	Görev ile tarama başlatılabilir mi?	Z	
YP_FT_UNGA_4	Görev ile kural atanabilir mi?	Z	
YP_FT_UNGA_5	Görevler zamanlanmış bir şekilde atanabilir mi?	Z	
YP_FT_Y	2.12 Yetkilendirme		O

YP_FT_Y_1	Yönetici, raporlama yöneticisi, vb. yetki sınıflarına ayrılmış roller var mı?	Z	
YP_FT_Y_2	Roller kapsamı dışında özelleştirilebiliyor mu?	Z	
YP_FT_DK	2.13 Denetim Kayıtları		O
YP_FT_DK_1	Oturum açma kapama kayıtları tutuluyor mu?	Z	
YP_FT_DK_2	Kullanıcı yetki kayıtları tutuluyor mu?	Z	
YP_FT_DK_3	Kural değişikliği, silme, atama kayıtları tutuluyor mu?	Z	
YP_FT_DK_4	Uç nokta üzerinde yapılan değişiklik kayıtları tutuluyor mu?	Z	
YP_FT_BU	2.14 Bilgilendirme ve Uyarılar		O
YP_FT_BU_1	Ürün versiyon güncelleme bildirimleri gönderiliyor mu?	Z	
YP_FT_BU_2	İmza veri tabanı versiyon kontrolleri yapılabiliyor mu?	Z	
YP_FT_BU_3	Lisans kullanım süresi takip edilebiliyor mu?	Z	
YP_FT_BU_4	Zararlı yazılım tespiti bildirimleri gönderiliyor mu veya kontrolleri yapılabiliyor mu?	Z	
YP_FT_BU_5	Sürüm notları paylaşılıyor mu?	Z	
YP_FT_L	2.15 Lisanslama		O
YP_FT_L_1	Müşteri ihtiyaçlarına göre esnek mi?	Z	
YP_FT_L_2	Çevrimiçi ve Çevrimdışı ortamlarda çalışabiliyor mu?	Z	
YP_FT_A	2.16 Ayarlar		O
YP_FT_A_1	Erişim adres bilgisi görüntülenebiliyor mu?	Z	
YP_FT_A_2	Proxy ayarları var mı?	Z	
YP_FT_A_3	E-posta hizmeti ayarları var mı?	Z	
YP_FT_A_4	Lisans ile ilgili ayarlar var mı?	Z	
YP_FT_UD	Ürün Dökümantasyonu		O
YP_FT_UD_1	Ürün dökümantasyonu için Türkçe ve İngilizce dil desteği var mı? Diğer diller açıklama kısmına yazılmalı.	Z	
YP_FT_UD_2	Hızlı kurulum, ürün özellikleri gösteren elektronik özet kitapçık ve yönetici el kitabı var mı?	Z	
YP_FT_UD_3	Üreticinin ürüne ilişkin bilgi deposu ve çağrı sistemi v.b. web sayfaları var mı?	Z	