ANTİVİRÜS YAZIMIMI TEKNİK ŞARTNAMESİ (Ek2)

1. YÖNETİM KONSOLU (MANAGEMENT CONSOLE)

1.1. Kurulum ve Konfigürasyon

1.1.1. Bu kurulum paketi tek sanal cihaz (virtual appliance) gibi bütün roles/services 'leri iletmeli ve aşağıdaki sanallaştırma platformlarını desteklemeli

1.1.1.1. VMware vSphere, View;

1.1.1.2. Citrix XenServer, XenDesktop, VDI-in-a-Box;

1.1.1.3. Microsoft Hyper-V;

1.1.1.4. Red Hat Enterprise Virtualization;

1.1.1.5. Kernel-based Virtual Machine or KVM;

1.1.1.6. Oracle VM.

Gerektiğinde antivirus ürünü geliştiricisinden (antivirus product developer) istenirse diğer sanal platformları da desteklemelidir.

1.1.2. Sanallaştırılmış ortamlar için tarama makineleri ayrı olarak Web arayüzünden indirilebilir olmalı.

1.1.3. Herhangi bir roles/services tek başına ya da aynı sanal makineye diğer roles/services 'le birlikte yüklenebilir şekilde olmalı.

1.1.4. Ana roller Database Server, Communication Server, Update Server, Web Server için benzer olmalıdır.

1.1.5. Aynı role sahip birden fazla makineye yükleme durumları için ek olarak balance module içermelidir.

1.2. Genel Özellikler

1.2.1. Esnek Lisanslama (lisanslı her farklı servis ve farklı son kullanma tarihleri için ayrı ürün anahtarı verilebilir ve bütün girilmiş ürün anahtarlarının kaydı tutulması gerekmektedir.)

1.2.2. Basit mimari güncelleme - sadece güncellemeye butonuna tıklayarak tüm roller ve servisler gerekli paketlere güncelleştirilebilir olmalı.

1.2.3. Talep üzerine yönetici seçtiği istemci paketlerini istenilen band genişliği aralığın da güncelleyebilecek şekil bir yapıya sahip olmalı .

1.2.4. Bildirimler her zaman ana menüde göstermeli, okunmamış mesajlar vurgulanır, mail olarak gönderilir, önemli sorunlar (major issues) yöneticiye uyarı biçiminde göndermelidir. (licensing issues, outbreak alerts, and outdated machines)

1.3. İzleme ve Raporlama için Kontrol Paneli

1.3.1. Portlar tabanları özel isme göre, rapor tipine göre, rapor hedefine göre, spesifik her rapor çeşidine göre ayarlanabilir olmalı.

1.3.2. Çoklu sayfalar içermeli.

1.3.3. Eklemelere, silmelere ve yeniden sıralandırmayı desteleyecek yapıya sahip olmalı.

1.4. Network Envanteri – güvenlik yönetim görevleri.

1.4.1. Active Directory, VMware vCenter, Citrix Xen ile entegre edilmiş ve bu platformlarda bulunan envanteri içe aktarmalı, Yönetici Active Directory entegresi için senkronizasyon zaman aralığını tanımlayabilmeli (saatlik).

1.4.2. Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM ile uyumlu ve sanal makineler Network Discovery yoluyla erişilebilir olmalıdır.

1.4.3. Sanal iş istastonları ve sunucular için Network discovery Active Directory Vmware vCenter, Citrix Xen ile entegre edilmemiş makineleri bulmalıdır.

1.4.4. Hostname, İşletim systemi ve IP adresi tarafından gerçek zamanlı arama, sıralama Filtreleme gibi özelliklere sahip olmalıdır.

1.4.5. Antivirüs ürününün uzaktan kuruluma ve aynı şekilde uzaktan kaldırmaya elverişli olmalıdır.

1.4.6. Antivirüs ürünü elle ayarlanabilir yükleme paketleri içermelidir.

1.4.7. Uzaktan görev atama ayarları içermelidir.

1.4.8. Uzaktan Workstations ya da server yeniden başlatma görevi içermelidir.

1.4.9. Merkezi görev sonuçları için ayrı bölüm olmalı ve her alt görev içinde detaylandırılabilecek şekilde yapıya sahip olmalıdır.

1.4.10. Her seviyeye kural (Policy) belirlenebilir olmalı.

1.4.11. Powerful Policy atama opsiyonları: Policy devralmalarının yapılandırılması, zorla Policy yapılandırması vb. Opsiyonlar mevcut olmalı.

1.4.12. Detaylandırılmış yönetilen nesnelerin özellikleri: İsim, IP, İşletim Sistemi, Grup, Atanmış Policyler, son kötü amaçlı yazılım durumu, son tarama günlüklerini içermelidir.

1.5. Kurallar (Policyler)

1.5.1. Her servis için tek bir şablon olmalı.

1.5.2. Her güvenlik hizmetini devreye sokmak / devreden ve antimalware tarama, saldırı tespit ile iki yönlü güvenlik duvarı, ağ erişim kontrolü, uygulama kontrolü, web erişim kontrolü, şifreleme, cihaz konumu, kimlik doğrulama uygulama ve eylemleri gibi işlevleri yapılandırmak için özel seçenekleri ile yapılandırılabilir ilke şablonları olmalıdır. Malware ve tespit uyumlu olmayan cihazlar söz konusu olduğunda alınacak, uzaktan kilit gibi, kilidini kaldır, sil gibi seçenekleri barındırmalıdır.

1.6. Raporlar

1.6.1. Farklı çok sayıda rapor seçeneği olmalı.

1.6.2. Tek sayfa kullanım kolaylığı: özetler ve detaylar aynı sayfanın içinde, aktif özet bölümü olmalı ve filtreler tıklayarak seçilir olmalı.

1.6.3. Planlanmış raporlar, istenilen kullanıcılara console yetkisi olmadanda gönderilebilir olmalı.

1.6.4. Planlanmış raporları sadece ilgili her kullanıcıya sırasıyla mail gönderebilecek şekilde tanımlama yapılabilmelidir.

1.6.5. Planlanmış bir raporun tüm oluşturulan örneklerini arşivmeli.

1.6.6. Özetleri .pdf, ayrıntıları .csv dosyası olarak dışarı aktarabilmeli.

1.7. Karantina

1.7.1. Ayarlanabilir lokasyon ile uzaktan restore ve silme özelliği olmadır.

1.7.2. İstendiğindeRestored files için exclusions list oluşturulabilmelidir.

1.7.3. Dosya indirme, sadecec vShield ile entegre olmuş makineler için geçerli olmalı.

1.8. Kullanıcılar:

1.8.1. Rol tabanlı yönetime sahip olmalı.

1.8.2. Çoklu önceden tanımlanmış türleri: Root, yönetici ve reporter şeklinde.

1.8.2.1. Root: Çözüm bileşenlerini yönetmeli.

1.8.2.2. Administrator: Güvenlik servislerini yönetmeli.

1.8.2.3. Reporter: İzler ve rapor oluşturabilir olmalı.

1.8.3. Kullanıcı listesi Microsoft Active Directory'den içeri aktarma özelliği olmalıdır.

1.8.4. Bir kullanıcının yönetmesine izin verilen hizmetleri, nesneleri seçmek ve yönetici hedef hakları için ayrıntılı yapılandırma içerir. Yönetim konsolunda gösterilen bilgilerin gelişmiş güvenliği için, her tür kullanıcıya otomatik olarak oturum kapatma imkanı sağlar.

1.9. Loglar

1.9.1. Uyumlu bir şekilde kullanıcı eylemlerini (hareketlerini) kaydeder.

1.9.2. Her kullanıcı işlemleri için detaylı loglama yapmalıdır.

1.9.3. Karmaşık arama yapma özelliğine sahip olmalıdır.

1.10. Güvenlik Sertifikaları

1.10.1. Yönetim konsoluna erişim korumalı olmalıdır (https).

1.10.2. Merkezi yönetim konsolundan web sunucusu, lisanslı bir sertifika yetkilisi tarafından veya kendi kuruluş tarafından verilen dijital sertifika alma izin vermelidir. Sertifika alma sezgisel ve merkezi yönetim konsolu şeklinde olmalıdır.

1.10.3. Yönetim ve mobil cihazlar (IOS) iletişim dijital sertifika ile, tespit yapılmalıdır. Bu sertifikalar yetkili Onay Makamı (Certification Authority) tarafından ya da kendi kuruluş tarafından imzalanacaktır.

1.10.4. Çözüm sertifikaları hakkında merkezi konsolun bilgi göstermesi gerekmektedir: adı, ihraç yetkisi,verilen sertifikaların verilmesi ve son kullanma tarihi tarihi.

2. FİZİKSEL WORKSTATIONS VE SERVERLAR İÇİN KORUMA 2.1. Minimal ve eliminatory özellikleri

2.1.1. Tek bir program içerisinde hem ajan hem antivirüs motoru içermesi.

2.1.2. Kaynak tüketimini en aza indirmek için, antivirüs ürünleri, özel modüllere kurulumu izin vermelidir. (Web erişim kontrol modülü olmadan veya Güvenlik Duvarı modülü olmadan antivirüs ürünü yüklenebilmesi.)

2.2. Sistem Gereksinimleri asağıdaki listedeki gibi olmalı

2.2.1. Workstation işletim sistemleri: Windows 8.1, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3), Mavericks (10.9.x), Mountain Lion (10.8.x), Lion (10.7.x)

2.2.2. Tablet ve gömülü işletim sistemleri: Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded with Service Pack 2, Windows XP Tablet PC Edition.

2.2.3. Server işletim sistemleri: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server.

2.2.4. Linux işletim sistemleri: Red Hat Enterprise Linux / CentOS 5.6 veya daha yüksek, Ubuntu 10.04 LTS veya daha yüksek, SUSE Linux Enterprise Server veya daha yüksek, OpenSUSE 11 veya daha yüksek, Fedora 15 or higher and Debian 5.0 veya daha yüksek.

2.3. Yönetim ve uzaktan kurulum

2.3.1. Kurulum öncesi, yönetici sadece istenilen modüllerin de dahil olmak üzere yükleme paketlerini özelleştirebilir olmalı: güvenlik duvarı, içerik kontrolü gibi.

2.3.2. Kurulum çeşitli şekillerde iş istasyonlarına doğrudan veya direk web konsol üzerinden uzaktan yüklenebilir olmalıdır.

2.3.3. WAN trafiğini en aza indirmek için, uzak lokasyondaki makinelerde kurulum yaparken, bu konumlara mevcutta var olan yüklü istemci kullanılarak kurulum gerçekleştirilecektir.

2.3.4. Yönetim Konsolu antivirüs yüklü iş istasyonlarının sayısını ve korumasız olan iş istasyonlarının sayısını bildirmeli.

2.3.5. Yönetim konsolu kontrol paneli yapılandırılabilir portletler / widget içermelidir.

2.3.6. Yönetim konsolu detaylı iş istasyonları / sunucuları hakkında bilgi içermelidir: adı, IP, işletim sistemi yüklü modülleri, uygulanan politikayı, güncelleme bilgileri vb.

2.3.7. Yönetim konsolundan yönetici workstationlar ve serverları tüm virüsten koruma ürünü yapılandırmak için tek bir policy altında toplayabilmelidir.

2.3.8. Hesaplar, yönetici ve Raporlayıcı olmak üzere iki tür olmalı. Yönetici; kullanıcıların gruplar ayarlarını değiştirmek için Raporlayıcı raporları oluşturmak için tahsis edilebilmeli.

2.3.9. Yönetim Konsolu tarafından ayrıntılı bilgi tüm eylemler için olmalı "Log": giriş, düzenlemek, oluşturmak, çıkış taşımak vs.

2.3.10. 32-bit işletim sistemleri ve 64-bit hem de kullanılan tek bir paket oluşturma imkanı olmalıdır. 11) Yönetici grup ve altgrup oluşturma workstationları taşıma gibi özelliklere sahip olmalıdır. 12) Networkte bulunan diğer bilgisayarları bulma özelliği barındırmalıdır.

2.4. Antivirüs ve antispyware modülünün işlevselliği temel özellikleri

2.4.1. Otomatik gerçek zamanlı tarama arşivleri ya da çözeltinin yöneticisi tarafından tanımlanabilir "x" MB dosya boyutundan daha büyük dosyaları tarama ayarlanabilir, ayrıca arşivleri tarayarak maksimum derinlik (16 seviye) tanımlanabilir olmalı.

2.4.2. Davranış sezgisel (heuristic) tarama özelliği olmalı.

2.4.3. Talep ve herhangi bir bilgi depolama ortamı on-access tarama (CD'ler, harici sabit diskler, paylaşılan sürücü). depolama medya cihazları "x" MB'den daha fazla bilgi içeriyorsa tarama işlemi durdurulabilir olmalı.

2.4.4. Workstation düzeyinde gönderilen ve alınan mailleri tarama özelliği olmalıdır.

2.4.5. Veri yolu yapılandırmasında dosya seviyesine kadar tarama yapabilmelidir.

2.4.6. Antivirüs ürünü için, tarama dışlama listesi tanımlama sağlayabilir hem "on-access" hem de "on-demand" belirli klasörler, diskler, dosyalar, uzantıları veya işlemler için, tarama yapabilmelidir.

2.4.7. Casus imzalar (spyware signatures) ve bu programların sezgisel algılama kapsamlı bir veritabanı ile ürün antispyware koruması sunmak zorundadır.

2.4.8. Sistem kaynaklarına aşırı yükleme yapmamak amacıyla virüsten koruma ürünü, bulut içi taramayı ve bunun yanı sıra kısmen de yerel taramayı kullanacak şekilde yapılandırılabilir. Bundan daha ayrıntılı olarak, eğer sistemde yeterli donanım kaynağı yoksa, antivirüs ürünü taramayı bir tarama sunucusu üzerinden yapacak bir şekilde yapılandırılabilir.

2.4.9. Antivirüs tespiti 3 tip olmalıdır: imza tabanlı, sezgisel tabanlı ve sürekli izleme işlemi.

2.4.10. Antivirüs HTTP in yanı sıra SSL taraması yapması gerekir.

2.4.11. Workstationlarda yüklü antivirüsün devamlılığı ve kullanıcının kaldıramaması için şifre ile koruma özelliği olması gerekir.

2.4.12. Kullanıcı güvenliği için, müşteri arama motorları (Search Advisor) ile aranan bağlantıları kontrol seçeneğine sahip olacak anti-phishing modülünü içermelidir.

2.5. Güvenlik Duvarı

2.5.1. Yerel ağ düzeyinde veya internet seviyesinde "stealth modu" ayarlama yeteneği olmalıdır.

2.5.2. Modül yönetici tercihlerine göre yüklenip kaldırılabilir olmalı.

2.5.3. Modül Saldırı Tespit Sistemi (IDS) üzerinde 3 seviyeli yapılandırma içermelidir.

2.6. Karantina

2.6.1. Antivirüs ürünü virüs laboratuarına karantinaya alınan dosyaları otomatik olarak gönderilmesine izin vermelidir.

2.6.2. Karantinaya dosya gönderimi yönetici tarafından önceden belirlenmiş zaman aralığında otomatik olarak yapmalıdır.

2.6.3. Antivirüs ürünü gereksiz depolama alanı işgal etmemek için belirli bir süreden daha önce karantinaya alınan dosyaları otomatik silinmesine izin vermelidir.

2.6.4. Disk üzerinde herhangi başka bir yerden özgün konumuna veya karantinaya bir dosyayı taşımak özelliğine sahip olmalıdır.

2.6.5. Restore edilen dosyaları otomatik olarak tarama dışı bırakılan ögeler arasına ekler ve gerçek zamanlı koruma yeniden karantinaya göndermek için bu dosyaları denetlemeyecek şekilde olmalıdır.

2.6.6. Karantina nesneleri her imza güncellemesinden sonra tarama yapmalıdır.

2.7. Veri Koruması

2.7.1. Belirli kurallar oluşturarak hem HTTP ve SMTP için gizli verileri (pin kartı, banka hesabı, vs.) engellemelidir.

2.8. Kullanıcı Kontrolü

2.8.1. Konsol aşağıdaki özelliklere sahip kullanıcı kontrol modülü ile entegre olmalıdır

2.8.1.1. Belirli istemciler veya istemci grupları için internet erişimi engelleme .

2.8.1.2. Belirli uygulamalara erişimi engelleme.

2.8.1.3. Belirli bir süre için Internet erişimi engelleme.

2.8.1.4. Belirli anahtar kelimeleri içeren web sayfaları engelleme.

2.8.1.5. Yönetici tarafından belirtilen belirli web sayfalarına erişim izni verme.

2.8.1.6. Önceden belirlenmiş bazı kategorilere (örneğin online dating, şiddet, vs.) belirli web sitelerine erişimi kısıtlama.

2.9. Cihaz Kontrolü:

2.9.1. Modül yönetici tarafından yönetim konsolundan yüklenip kaldırılabilir olmalı.

2.9.2. Cihaz kontrol modülünü kullanarak kullanıcıların aşağıda bulunan cihazlara erişimini kontrol edebilmeli

2.9.2.1. Bluetooth Devices

2.9.2.2. CDROM Devices

2.9.2.3. Floppy Disk Drives

2.9.2.4. Security Policies 153

2.9.2.5. IEEE 1284.4

2.9.2.6. IEEE 1394

2.9.2.7. Imaging Devices

2.9.2.8. Modems

2.9.2.9. Tape Drives

2.9.2.10. Windows Portable

2.9.2.11. COM/LPT Ports

2.9.2.12. SCSI Raid m) Printers

2.9.2.13. Network Adapters

2.9.2.14. Wireless Network Adapters

2.9.2.15. Internal and ExternalStorage

2.9.3.Kurallar izin ve engelleme üzerine yapılandırılabilir.

2.9.4.Modül, kuralları tarama dışı bırakma tanımlamanızı sağlar.

2.10. Power Kullanıcı

2.10.1. Modül Yönetim konsolu aracılığıyla yönetici tarafından yüklenip kaldırılabilir.

2.10.2. Power Kullanıcı modülünü kullanan bir kişi Power kullanıcı arayüzüne şifre ile doğrudan giriş yapabilir ve antimalware kullanıcı ayarlarını konfigüre edebilir olmalıdır.

2.10.3. Yönetici Power User arabirimi aracılığıyla kullanıcı tarafından yapılan ayarları yapılandırabilme veya geçersiz imkanına sahip olmalı.

2.11. Güncelleme

2.11.1. Kullanıcıyı uyarmadan, güncellemeden sonra bilgisayar yeniden başlatma için bekle özelliği olmalıdır.

2.11.2. Yerel güncelleme sunucusu kullanarak cascaded güncelleme sistemi olmalıdır.

2.11.3. Kullanıcıları uzak bir konumda güncellemek, güncelleme sunucusu rolüne sahip mevcut bir istemci aracılığıyla yapılabilmelidir.

3. SANALLAŞTIRILMIŞ WORKSTATIONLAR VE SERVERLAR İÇİN KORUMA

3.1. Antivirüs korumasının sanallaştırılmış ortamlarda minimum gereksinimleri aşağıdaki gibi olmalıdır

3.1.1.Ürün VMware vShield ile entegre ve sanal makine üzerinde bir virüsten koruma ürünü kurmadan antivirüs tarama imkanı olmalıdır.

3.1.2.Merkezi yönetim bileşeni çözümü birden fazla VMware vCenters ile bütünleşik çalışması gerekmektedir.

3.1.3.Linux sanal makineleri için gerçek zamanlı ve talebe göre tarama yapabilmelidir.

3.1.4.Ürün envanterleri içeri aktarabilecek şekilde birden fazla Citrix Xen Sunucular ile bütünleştirme özelliğine sahip olmalıdır.

3.1.5.Ürün Microsoft Hyper-V, Red Hat Sanallaştırma Oracle VM si KVM ile bütünleşik çalışmalıdır.

3.1.6.Antivirüs ürünü, aşağıdakileri içeren; tek bir sanal tarama makinesi içermelidir

3.1.6.1. Antivirüs imzalarını içermeli;

3.1.6.2. Bir sanal makine açarken güncel tam koruma sağlamalı;

3.1.6.3. Optimize tarama yapabilmeli.

3.2. Genel Özellikler

3.2.1.Virüsler, casus yazılım, rootkit ve diğer kötü niyetli programların tespiti için farklı yöntemlere sahip olmalıdır.

3.2.2.Üründe bulunan güvenlik sanal cihazının (sercurity virtual device), virüsten koruma imzalarının ve güvenlik sanal cihazı işletim sisteminin otomatik olarak güncellenmesine izin vermelidir.

3.2.3.Ürün güvenlik ana bilgisayar mevcut durumunu bildirmek zorundadır - VM korumalı / korumasız ve sanal cihazlar.

3.3. Minimum sistem gereksinimleri

3.3.1.Sanallaştırma platformları

3.3.1.1. VMware vSphere, 5.5, 5.1, 5.0 P1 (Patch # 474610-1) or 4.1 P3 (433,742- Patch # 3) including ESXi 4.1 and ESXi 5.0 with

3.3.1.2. VMware vCenter Server 5.5, 5.1, 5.0 or 4.1

3.3.1.3. VMware VShield Manager 5.1, 5.0

3.3.1.4. VMware VShield VShield Endpoint Manager yüklü kullanıcı

3.3.1.5. VMware Tools 8.6.0 build 446312

3.3.1.6. VMware View 5.1, 5.0

3.3.1.7. Citrix XenDesktop 5.5, 5.0

3.3.1.8. XenServer 6.0, 5.6 or 5.5 (including Xen Hypervisor)

3.3.1.9. Citrix VDI-in-a-Box 5.x

3.3.1.10. Microsoft Hyper-V Server 2012, 2008 R2 or Windows 2008 R2 (including Hyper-V Hypervisor)

3.3.1.11. Oracle VM 3.0

3.3.1.12. Red Hat Enterprise Virtualization 3.0 (including KVM hypervisor)

3.3.2.System requirements

3.3.2.1. Workstation operating systems: Windows 8.1, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3), Mavericks (10.9.x), Mountain Lion (10.8.x), Lion (10.7.x)

3.3.2.2. Server operating systems: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server

3.3.2.3. Linux: Red Hat Enterprise Linux / CentOS 5.6 or higher, Ubuntu 10.04 LTS or higher, SUSE Linux Enterprise Server 11 or higher, OpenSUSE 11 or higher, Fedora 15 or higher and Debian 5.0 or higher,

3.4. Antivirüs ve antispyware modülünün işlevselliği temel özellikleri

3.4.1.Otomatik gerçek zamanlı tarama arşivleri ya da çözeltinin yöneticisi tarafından tanımlanabilir

3.4.2. Davranış sezgisel tarama yapabilmelidir.

3.4.3.Talep ve herhangi bir bilgi depolama ortamı on-access tarama (CD'ler, harici sabit diskler, paylaşılan sürücü). depolama medya cihazları fazla bilgi içeriyorsa tarama işlemi durdurulabilmelidir.

3.4.4.Workstation düzeyinde gönderilen ve alınan mailleri tarama özelliği olmalıdır.

3.4.5.Veri yolu yapılandırmasında dosya seviyesine kadar tarama yapmalıdır.

3.4.6.Antivirüs ürünü için, tarama dışlama listesi tanımlama sağlayabilir hem "on-access" hem de "on-demand" belirli klasörler, diskler, dosyalar, uzantıları veya işlemler için, tarama yapılabilmelidir.

3.4.7.Casus imzalar (spyware signatures) ve bu programların sezgisel algılama kapsamlı bir veritabanı ile ürün antispyware koruması sunmak zorundadır.

3.4.8.Sanal makineleri aşırı yük olmaması için, antivirüs ürün Security Server'a tarama Yükünü üstlenecektir.

3.4.9.Antivirüs tespiti 3 tip olmalıdır: imza tabanlı, sezgisel tabanlı ve sürekli izleme işlemi.

3.4.10. Antivirüs HTTP in yanı sıra SSL tarama yapmalıdır.

3.4.11. Workstationlarda yüklü antivirüsün daha iyi yönetimi için, ürün kaldırma koruması için bir şifre atama seçeneğine yer almalıdır.

3.4.12. Kullanıcı güvenliği için, müşteri arama motorları (Search Advisor) ile aranan bağlantıları kontrol seçeneğine sahip olacak anti-phishing modülünü içermelidir.

3.4.13. Ağa gönderilen trafik miktarı optimizasyonunu sağlamak için, tarama makinesi ve sanal makinede bir önbelleğe alma mekanizması aracılığıyla yapmalıdır.

3.4.14. Tarama makinesinde yük devretme / yük dengeleme bağlantılarını ayarlarını yapan agent bulunmalıdır.

3.4.15. Policyler VMware vCenter kaynak havuzuna uygulanabilir olmalıdır.

3.5. Güvenlik Duvarı

3.5.1. Ürün Yerel ağ düzeyinde veya internet seviyesinde "stealth modu" ayarlama yeteneğine sahip olmalıdır.

3.5.2. Modül yönetici tercihlerine göre yüklenip kaldırabilmelidir.

3.5.3. Modül Saldırı Tespit Sistemi (IDS) üzerinde 3 seviyeli yapılandırma içermelidir.

3.6. Karantina

3.6.1. Antivirüs ürünü gereksiz depolama alanı işgal etmemek için belirli bir süreden daha önce karantinaya alınan dosyaları otomatik silinmesine izin vermelidir.

3.6.2. Disk üzerinde herhangi başka bir yerden özgün konumuna veya karantinaya bir dosyayı taşımak özelliğine sahip olmalıdır.

3.6.3. Yönetici'nin Workstationlara direk indirebilme özelliği olmalıdır.

3.6.4. Her imza güncellemeden sonra karantinaya alınan dosyaları yeniden taramak için yeteneği olmalıdır.

3.6.5. Restore edilen dosyaları otomatik olarak tarama dışı bırakılan öğeler arasına eklemeli ve gerçek zamanlı koruma yeniden karantinaya göndermek için bu dosyaları denetlememeli.

3.6.6. Karantinaya dosya gönderimi yönetici tarafından önceden belirlenmiş zaman aralığında otomatik olarak yapmalıdır.

3.7. Yönetim ve Uzaktan Yükleme

3.7.1. Sanal cihazlar kurulumdan önce özelleştirilebilir olmalı ve bu otomatik olarak birkaç özelliklerine göre ölçeklenebilir olmalıdır.: Hostlarda bulunan sanal makinelerin sayısı, networkler, IP adresleri, ayrılan kaynaklar (CPU, bellek vb).

3.7.2. Kurulum öncesi, yönetici sadece istenilen modüllerin de dahil olmak üzere yükleme paketleri özelleştirebilir olmalıdır: güvenlik duvarı, içerik kontrolü, cihaz kontrolü.

3.7.3. Yönetim konsolu virus koruma çözümünün yüklü olan veya olmayan sanal makinelerin sayısını bildirmelidir. Bunun yanı sıra makine durumlarını da göstermelidir: Açık veya Kapalı.

3.7.4. Sanal makine üzerinde antivirus modülünün aktif olup olmadığını yönetim konsoluna raporlayabilme imkanı sunmalıdır.

3.7.5. En az 100 kullanıcı için kurulabilmeli ve yönetilmelidir

3.8. Veri Koruması

3.8.1. Belirli kurallar oluşturarak hem HTTP ve SMTP için gizli verileri (pin kartı, banka hesabı, vs.) engelleme yapabilmelidir.

3.9. Kullanıcı Kontrolü

3.9.1. Konsol aşağıdaki özelliklere sahip kullanıcı control modülü ile entegre olmalıdır:

3.9.1.1. Belirli istemciler veya istemci grupları için internet erişimi engelleme.

3.9.1.2. Belirli uygulamalara erişimi engelleme.

3.9.1.3. Belirli bir süre için Internet erişimi engelleme.

3.9.1.4. Belirli anahtar kelimeleri içeren web sayfaları engelleme.

3.9.1.5. Yönetici tarafından belirtilen belirli web sayfalarına erişim izni verme.

3.9.1.6. Önceden belirlenmiş bazı kategorilere (örneğin online dating, şiddet, vs.) belirli web sitelerine erişimi kısıtlama.

3.10. Cihaz Kontrolü:

3.10.1. Modül yönetici tarafından yönetim konsolundan yüklenip kaldırılabilir olmalıdır.

3.10.2. Cihaz kontrol modülünü kullanarak kullanıcıların aşağıda bulunan cihazlara erişimini kontrol etmelidir:

3.10.2.1. Bluetooth Devices
3.10.2.2. CDROM Devices
3.10.2.3. Floppy Disk Drives
3.10.2.4. Security Policies 153
3.10.2.5. IEEE 1284.4
3.10.2.6. IEEE 1394
3.10.2.7. Imaging Devices
3.10.2.8. Modems
3.10.2.9. Tape Drives
3.10.2.10. Windows Portable
3.10.2.11. COM/LPT Ports
3.10.2.12. SCSI Raid
3.10.2.13. Printers
3.10.2.14. Network Adapters
3.10.2.15. Wireless Network Adapters
3.10.2.16. Internal and External Storage

3.10.3. Kurallar izin ve engelleme üzerine yapılandırılabilir olmalıdır.

3.10.4. Modül, kurallarında tarama dışı bırakma özelliğine sahip olmalıdır.

3.11. Power Kullanıcı:

3.11.1. Modül Yönetim konsolu aracılığıyla yönetici tarafından yüklenip kaldırılabilir olmalıdır.

3.11.2. Power Kullanıcı modülünü kullanan bir kişi Power kullanıcı arayüzüne şifre ile doğrudan giriş yapabilme ve antimalware kullanıcı ayarlarını yapılandıracak yetkiye sahip olmalıdır.

3.11.3. Yönetici Power User arabirimi aracılığıyla kullanıcı tarafından yapılan ayarları yapılandırabilme veya geçersiz kılma imkanına sahip olmalıdır.

3.12. Güncelleme:

3.12.1. Kullanıcıyı uyarmadan, güncellemeden sonra bilgisayar yeniden başlatma için beklemek özelliği olmalıdır.

3.12.2. Yerel güncelleme sunucusu kullanarak cascaded güncelleme sistemi olmalıdır.

3.12.3. Kullanıcıları uzak bir konumda güncellemek, güncelleme sunucusu rolüne sahip mevcut bir istemci aracılığıyla yapılabilmelidir.

4. SMARTPHONE AYGITLARI IÇIN GÜVENLİK

4.1. Minimum Sistem Gereksinimleri

4.1.1.Apple iPhones ve iPad tabletler (iOS 5.1+)

4.1.2.Google Android akıllı telefonlar tabletler (2.2+)

4.2. Özellikler

4.2.1.Active Directory kullanıcı ile cihaz ilişkilendirmek izin verir.

4.2.2.Kurulum; Kurulum detayları ile, kullanıcıya bir e-posta göndererek yapılır.

4.2.3.Yönetim konsoluna Cihaz aktivasyonu QR kodu kullanarak yapılacaktır.

4.2.4.Yükleme Paketleri Apple App Store ve Google Play üzerindne indirilebilir.

4.2.5.Aşağıdaki işlemler alınabilir:

4.2.5.1. Zorunlu ekran kilidi ve doğrulama;

4.2.5.2. Cihazın kilit açılması

4.2.5.3. Fabrika ayarlarına geri döndürmek

4.2.5.4. Cihaz yeri tespiti

4.2.5.5. Cihaz taraması (Androidler için)

4.2.5.6. Cihaz belleği şifrelemesi (encryption) (androidler için)

4.2.6.Yönetim konsolu aktif, inaktif, bağlı olmayan rootlanmamış ya da jailbreak yapılmamış cihazları raporlar.

4.3. Güvenlik Ayarları:

4.3.1.Bir cihaz istenen ayarlara uygun değilse, aşağıdaki eylemler alınabilir:

4.3.1.1. Reddetmek

4.3.1.2. Erişimi engellemek

4.3.1.3. Cihazı kilitlemek

4.3.1.4. Fabrika ayarlarına geri döndürmek

4.3.1.5. Yönetim konsolundan cihazı kaldırmak

4.3.2. Bir parola ile cihazlar kilitlenebilir. Bu şifreler aşağıdakiler gibi yapılandırılabilir:

4.3.2.1. Basit veya karmaşık şifre (İşletim Sistemine özgü);

4.3.2.2. Numara ve karakterler;

4.3.2.3. Minimum karakter sayısı yönetici tarafından tanımlanabilir;

4.3.2.4. Minimum özel karakter sayısı yönetici tarafından tanımlanabilir;

4.3.2.5. Periyodik olarak şifre yenileme süresi, yönetici tarafından tanımlanabilir;

4.3.2.6. Parola yeniden kısıtlama ayarlama;

4.3.2.7. Yanlış şifre girişimlerinin sayısının denetlenmesi;

4.3.2.8. Yönetici tarafından tanımlanan belirli bir dakikadan sonra cihazı kilitleme Dönemi.

4.3.3.Çeşitli profiller Wi-Fi bağlantısı veya VPN (sadece iOS işletim sistemi) için güvenlik kurallarını kurmak değil, aynı zamanda belirli bazı web sitelerine erişim ile ilgili olan, kurallar oluşturulabilir.

4.3.4.Wi-Fi profilleri aşağıdaki seçenekleri içerecektir:

4.3.4.1. Network güvenliği türü yanı sıra Genel - SSID tanımlanacak;

4.3.4.2. TCP/IP ayarları – Ipv4 ve IPv6 protokolleri için

4.3.4.3. Proxy ayarları – kapalı konumuna getirilecek otomatik veya manuel konfigüre edilecek

4.3.5.Web sitelerine erişimi (Android işletim sistemi) ile ilgili profilleri gibi özellikler şunlardır:

4.3.5.1. Belirli web sitelerine erişim, engelleme veya programlama izini belirli gün ve saatte olabilir.

4.3.5.2. Erişilen veya engellenen spesifik websiteleri için istisnalar eklenebilir.

4.3.6.Web sitelerine erişimi (iOS işletim sistemi) ile ilgili profilleri seçenekleri etkinleştirmek veya devre dışı bırakmak şunlar için geçerlidir:

4.3.6.1. Safari Browser kullanımı;

4.3.6.2. Otomatik tamamlama seçenekleri;

4.3.6.3. Kötü niyetli web sitelerini erişirken kullanıcıları uyarır;

4.3.6.4. JavaScript;

4.3.6.5. Pop-ups;

4.3.6.6. Çerezler;

5. MICROSOFT EXCHANGE MAIL SUNUCULARI İÇİN GÜVENLİK

5.1. Ürün, Microsoft Exchange e-posta sunucuları ile entegre ederek antimalware, (anti phishing dahil) antispam yanı sıra ekleri ve içerik filtreleme sunacak. Ayrıca, talep üzerine Exchange veritabanlarını taramak da mümkün olacak.

5.2. Ürün e-posta sunucusunun genel performansını etkilemeden, gerçek zamanlı ekleri ve içerik filtreleme sunacak.

5.3. Talep üzerine zararlı yazılım önleme very tabanı saatlik olarak güncelleme yapar.

5.4. İmza tabanlı algılama yanı sıra, antimalware koruma modülü sezgisel bileşeni içermelidir, uygulamalar yürütülür ve analiz edileceği bir sanal kutusu simüle etmesi gerekir böylece sistem yeni virüslere karşı korunmuş olacaktır.

5.5. Ürün bir eki kötü niyetli olarak işaretler ise bu durumda farklı konfigürasyonlar yapılabilmelidir: Desenfekte etmek, silmek, karantinaya taşımak gibi.

5.6. İmzalar ve sezgisel algılama kullanarak dayanarak, ürün gizli veri kaybını önlemek amacıyla anti-spyware koruması sunması gerekir.

5.7. Ürün antispam koruma sunacak. Antispam imzalarının internet üzerinden güncelleştirilmesi gerekir.

5.8. Anti-spam modülü, spam mesajlar için kullanılacak bilinen URL'ler ile bir veritabanı kullanman bir URL filtresi içerecektir, hem de otomatik olarak Kiril veya Asya karakterleri kullanan e-posta algılamak için bir filtre içerecektir.

5.9. Ürün, mesaj göndermek için kullanıldığı bilinen e-posta sunucularının listesini içeren çevrimiçi veritabanları ile senkronize ederek dolandırıcılığı algılayan bir RBL filtresi içerecektir.

5.10. Anti-spam bileşeni saldırganlık yapılandırma ve filtreler kullanmanıza izin verir. Bir spam eposta tespit ettiğinde ürünü farklı seçenekler sunacak: Silme, Başka bir e-posta adresie yönlendirme, spam olarak işaretleme, karantinaya taşıma gibi.

5.11.Ürün kullanıcılarını kandırmak için özgün e-postaları kopyalamak girişimlerini tespit edecek ve gizli verileri elde etmek için anti-phishing koruması sağlayacaktır.

5.12.Ürün kullanıcılarının anti-malware, anti-spam, kullanıcılar için içerik ve ek filtreleme politikaları ve grubu tanımlamak için tercihler içerecektir.

5.13.Ürünü doğrudan Internet'ten veya bir proxy üzerinden, ya da ağ üzerinde yerel olarak yüklü bir güncelleştirme sunucusundan güncelleme mümkün olacaktır.

5.14.Ürün anti-malware ve anti spam olaylarla ilgili raporlar sunacaktır.

5.15.Ürün, kullanılan fiziksel / sanal noktaları aynı yönetim konsolu üzerinden yönetilmeyi sağlayacaktır.