DESCRIEREA PRODUSULUI

Soluția de securitate ofera o securitate centralizata pentru asigurarea unei protecții împotriva virușilor, a programelor spion, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor coduri periculoase.

Soluția de securitate conține:

- consola de management cu o baza de date inclusa care este non-relațională, pentru o funcționare cat mai rapida, fără a fi nevoie de licențe adiționale. Posibilitatea instalării și configurării de la distanță a tuturor componentelor antivirusului pentru stații de lucru din interiorul rețelei, precum și pentru generarea de rapoarte legate de acestea.
- Pachetul de instalare va fi livrat ca o mașina virtuala bazata pe sistem de operare Linux securizat care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licența suplimentara pentru sistemul de operare. Imaginea de tip „template" se va putea importa in:
  a) VMware vSphere
  b) Citrix XenServer
  c) Microsoft Hyper-V
  d) Red Hat Enterprise Virtualization
  e) KVM
  f) *Oracle VM*.
- Soluția este scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașina virtuala.
- Soluția include adițional si un modul de balansare (load balancer) pentru cazurile in care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing si performanta/redundanta).
- Soluția include un mecanism de configurare a disponibilității pentru serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe mașini virtuale.
- Soluția ofera posibilitatea integrării cu Active Directory 2003 si versiuni mai recente.
- Ofera administratorilor de rețea posibilitatea identificării rapide a incidentelor legate de prezența unor programe periculoase și să poată aplica diverse politici de securitate.
- Interfața consolei de management este in limba romana, adițional limba engleza si altele.
- Interfața clientului de securitate, care se instalează pe stații si servere la fel va fi in limba romana, adițional limba engleza si altele.
- Se va acorda manual de instalare si de administrare a produsului in limba romana.
- Soluția permite creșterea pe aceeași licența un număr nelimitat de dispozitive.

Soluția include:

- Scanare automată a fișierelor, a memoriei și a cheilor de regiștri Windows înainte de instalarea pe sisteme.
- Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare trebuie sa includă actualizări de tip: ciclu rapid si ciclu lent.
- Tehnologii de detectare, dezinfectare și trimitere în carantină a virușilor, programelor spion de tip adware/spyware, troienilor și rootkit-urilor, de asemenea detectarea atacurilor de tip zero-day de tip exploit (atacuri directionate).

- Posibilitatea de a programa scanări imediate sau la cererea utilizatorului pentru a evalua gradul de infectare al sistemului. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fișiere mai mari de „ x " MB, mărimea fișierelor putând fi definita de administratorul

soluției, De asemenea posibilitatea definirii pana la minim 16 nivele de profunzime pentru scanarea in arhive.

- Produsul antimalware poate fi configurat sa folosească scanarea in Cloud si parțial scanarea locala.
- Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare, fie scanare locala sau scanare hybrida.
- Soluția oferă protecție in timp real pe mașinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.
- Soluția trimite în carantină fișierele suspecte sau infectate, în vederea reducerii riscului de propagare. Astfel administratorul va putea alege pentru fișiere infectate sau suspecte următoarele: interzice accesul, dezinfectează, ștergere, muta fișierele in carantina, nicio acțiune si alte acțiuni alternative.
- Protecție firewall individuală pentru utilizatorii de la distanță și ocazionali.
- Risc redus de infectare prin scanarea în timp real a traficului internet a tuturor stațiilor de lucru.
- Creșterea productivității și a nivelului de securitate prin blocarea accesului utilizatorilor la anumite site-uri ori prin blocarea posibilității de a transmite email-uri conținând date confidențiale.
- Colectarea de date despre amenințările informatice actuale de la toate stațiile de lucru și serverele din rețea cu ajutorul interfeței panoului de control.
- Management și configurare de la distanță, în conformitate cu politica de securitate.
- Configurarea, evaluarea, instalarea și îndepărtarea aplicațiilor la nivel de sistem.
- Niveluri multiple de protecție avansată, soluția va permite configurarea setărilor anti malware prin intermediul politicilor din consola de magement.

1) Antivirus
2) Antispam
3) Antispyware
4) Antiphishing
5) Content Filtering
6) Firewall.

- Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web, controlul dispozitivelor, power user.
- Solutia permite aplicarea politicilor pe mașini client, grupuri de masini, domeniu, unitati organizationale.
- Pentru o mai buna protecție a stațiilor si serverelor, solutia include un vaccin anti-ransomware. Acest vaccin va asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea stațiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
- Vaccinul anti-ransomware primește actualizări de la producător, o dată cu actualizarea semnăturilor produsului Antimalware. Politica sa poate fi schimbata automat in funcție de:

a) User-ul logat pe statie
b) IP sau clasa de IP al statiei
c) Gateway-ul alocat
d) DNS serverul alocat
e) Clientul este/nu este in aceeași rețea cu infrastructura de management
f) Tipul rețelei (lan, wireless)
g) Actualizări automate a bazei de date ce conține semnături de viruși.

- Soluția va permite stabilirea actualizării automate a consolei de management prin stabilirea graficilor zilnice, săptămânale sau lunare, dar si prin stabilirea intervalului orar in care acesta se va actualiza. De asemenea, permite si trimiterea unei alerte de ne funcționalitate, cu 30 de minute înainte de actualizare.
- Soluția va dispune de un server de actualizare (update) care face posibila stabilirea componentelor ce vor fi descărcate automat de pe internet, fara intervenția administratorului.

Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor si serverelor pe care rulează sistemul de operare Windows, Linux, Mac.

- Soluția permite stabilirea zonelor de test si critice din cadrul rețelei prin intermediul politicilor din consola de management
- Pentru o urmărire amănunțita a actualizărilor consolei de management, soluția permite vizualizarea unui jurnal de modificări in care sunt precizate istoric: versiunea consolei de management; data versiunii; funcții noi si îmbunătățiri; probleme rezolvate; probleme cunoscute.
- Soluția permite creare unei copii de siguranța a bazei de date a consolei de administrare, la cerere sau programata, putând fi stocata local, pe un server FTP sau in rețea.
- Soluția scaneaza următoarele tipuri minime de sisteme:
- Procesor compatibil Intel® Pentium 1,6 MHz, Memorie RAM: 1 GB
- Sistem de operare, baze de date si browsere web:
- Windows 7, 8.1, 10.
- Să existe posibilitatea ca în cazul trecerii la alt sistem de operare să fie livrat un kit de instalare și certificat de licență pentru produsul nou fără costuri suplimentare.
- Posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale).
- Pentru reducerea la minim a consumului de resurse, aplicația client antivirus trebuie să permită instalarea customizată a modulelor deținut.
- Pentru a nu încărca resursele sistemului produsul antivirus trebuie să conțină un singur motor de scanare și să poată rula scanările programate cu prioritate redusă.
- Actualizarea bazei de semnături de virus si a motoarelor de scanare pe perioada de 12 luni.
- In cazul in care in perioada de 12 luni de licențiere apare o versiune noua a produsului, producătorul va pune la dispoziție versiunea noua gratuit.
- Distribuirea unor mesaje de atenționare de urgență prin e-mail in cazul apariției unor noi viruși distructivi sau cu potențial de răspândire rapida,
- Pentru orice virus pe care producătorul nu îl identifică și dezinfectează se va livra antidotul in cel mai scurt timp posibil de la trimiterea unei mostre a virusului.
- Suport tehnic prin e-mail si mesagerie scrisă, non-stop 24/24 ore, 7/7 zile pe săptămâna, inclusiv in weekend si zilele de sărbătoare legale in limba română asigurat de către producătorul soluției, inclusiv suport din partea partenerului.
- Produsul antivirus oferit ocupa locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST).
- Se va acorda ajutor la instalarea /configurarea si punerea in execuție a produsului pentru stațiile de lucru. De asemenea va instrui administratorii IT din cadrul instituției privind exploatarea produsului.