ტექნიკური მონაცემები

მომხმარებლების რაოდენობა: 1020

პროგრამული პაკეტის (ლიცენზიის) ვადა: 1 წელი

შესყიდვის ობიექტის აღწერილობაში, სადაც მითითებულია კონკრეტული სასაქონლო ნიშანი, მოდელი, წარმოშობის წყარო, მწარმოებელი იგულისხმება მსგავსი, ექვივალენტი ან/და უკეთესი მონაცემების.	
ანტივირუსული პროგრამრული უზრუნველყოფა უნდა წარმოადგენდეს მასშტაბირებად გადაწყვეტას, ერთიანი სამართავი კონსოლით;	
ლოკალურად დაყენებული ანტივირუსული პროგრამული უზრუნველყოფის სამართავი კონსოლი უნდა წარმოადგენდეს ვირტუალური მანქანის image-ში ჩაშენებულ კონფიგურირებად Linux Ubuntu ვირტუალურ მოწყობილობას, რომლის დაყენება და გამართვა ხორციელდება CLI-ის (ბრძანების ველის ინტერფეისი) გამოყენებით. ვირტუალური მოწყობილობა უნდა იყოს ხელმისაწვდომი რამდენიმე სახით, და იყოს თავსებადი ვირტუალიზაციის ძირითად პლატფორმებთან (OVA, XVA, VHD, OVF, RAW).	
ანტივირუსული პროგრამრული უზრუნველყოფის მენეჯმენტ კომპონენტს უნდა გააჩნდეს ჩაშენებული მონაცემთა ბაზა;	
ანტივირუსის კლიენტი უნდა ყენდებოდეს როგორც ფიზიკურ, ასევე ვირტუალურ სამუშაო მანქანაზე და სერვერებზე და გააჩნდეს შემდეგი ვირტუალური პლატფორმების მხარდაჭერა:	• VMware vSphere, View; • Citrix XenServer, XenApp, XenDesktop • Microsoft Hyper-V • Red Hat Enterprise Virtualization • Kernel-based Virtual Machine ან KVM • Oracle VM • Nutanix
ანტივირუსული პროგრამული უზრუნველყოფის სამართავი კონსოლი უნდა იყოს ინტეგრირებადი არსებულ სამართავ და მონიტორინგის სისტემებში როგორებიცაა Microsoft Active Directory, VMware vCenter ან Citrix XenServer;	
პროდუქტს უნდა გააჩნდეს VMware/Citrix გარემოში virtual appliances-ის სკანირების ინსტრუმენტებით (Security Servers) remotely deployment ფუნქცია მენეჯმენტ ვებ კონსოლიდან;	
პროდუქტის სამართავი კონსოლის მთავარ მენიუში უნდა აისახებოდეს შეტყობინებები ადმინისტრატორისთვის. გამოყოფილად უნდა ჩანდეს გაუხსნელი შეტყობინებები, და ელექტრონულ ფოსტაზე იგზავნებოდეს გაფრთხილებები ძირითად პრობლემებზე: ლიცენზირების შეცდომები, მოძველებული ბაზები მომხმარებლის მანქანებზე, საეჭვო აქტივოვები;	
Virtual appliances სკანირების ინსტრუმენტებით უნდა იყოს ხელმისაწვდომი ცალკე გადმოსაწერად web ინტერფეისიდან;	
შესაძლებელი უნდა იყოს ნებისმიერი როლის/სერვისის როგორც ცალ-ცალკე ინსტალაცია სხვადასხვა appliance-ზე, ასევე ერთად, ერთი და იგივე ვირტუალურ მანქანაზე;	
პროდუქტი უნდა შეიცავდეს ბალანსირების მოდულს იმ შემთხვევისთვის თუ რამდენიმე მანქანა დაინსტალირებულია ერთიდაიგივე როლისთვის (High Availability, Disaster Recovery, performance და ა.შ.).	
პროდუქტს უნდა გააჩნდეს ინტეგრაცია Active Directory რამდენიმე დომენთან, რამოდენიმე VMware vCenters-თან, რამოდენიმე Citrix Xen Servers-თან და ამ პლატფორმებიდან რეესტრების იმპორტი საშუალება . Active Directory-თან ინტეგრაციისთვის ადმინისტრატორს უნდა შეეძლოს სინქრონიზაციის დროის ინტერვალის განსაზღვრა(საათებში)	
პროდუქტი უნდა იყოს თავსებადი Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM პლატფორმებთან და ვირტუალიზაციის ამ პლატფორმებისთვის ვირტუაური მანქანების აღმოჩენა და რეესტრის შექმნა მენეჯმენტ კონსოლში უნდა ხდებოდეს Network discovery-ს ფუნქციის გამოყენებით .	

პროდუქტს უნდა გააჩნდეს antimalware და antispyware მოდულები შემდეგი ფუნქციებით:

- ქცევითი ევრისტიკული სკანირება და პროცესების მონიტორინგი;
- Cloud scanning და Machine Learning ტექნოლოგიები;
- Anti-ransomware და anti-exploit ტექნოლოგიები;
- სკანირების მეთოდის კონფიგურაცია ;
- Antimalware მოდულის გააჩნია გამონაკლისების სიის განსაზღვრის შესაძლებლობა, როგორც "on-access" ასევე "on-demand" სკანირების დროს კონკრეტული საქაღალდე, დისკი, ფაილი, გაფართოებასა თუ პროცესისთვის;
- Antimalware მოდული შეიცავს საკნირების ერთ ინსტრუმენტს გეგმიური სკანირებისთვის დაბალი პრიორიტეტით, რომელიც ავტომატურად გაითიშება სამუშაო სადგურების სკანირების შემდეგ;
- Antimalware მოდულს გააჩნია malware საშიშროების აღმოჩენის მინიმუმ 4 ტიპი: signature-based, heuristic based, processes continuous monitoring და cloud scanning.
- Antimalware მოდულს გააჩნია HTTP და SSL სკანირების შესაძლებლობა;
- პროდუქტი შეიცავს სამუშაო სადგურზე დაყენებული კლიენტის პაროლით დაცვის ფუნქციას;
- პროდუქტი შეიცავს antiphishing მოდულს, რომელიც შეამოწმებს საძიებო სისტემების საშუალებით მოძებნილ ბმულებს (Search Advisor);

პროდუქტს უნდა გააჩნდეს Advanced Threat Control მოდული, ისეთი სახის საფრთხეებისგან დასაცავად, რომლის აღმოჩენა შეუძლებელია ევრისტიკული მეთოდით. მოდულმა უნდა განახორციელოს გაშვებული პროცესების მუდმივი მონიტორინგი და საეჭვო აქტივობების შეფასება, ესეთების როგორიცაა: პროცესის ტიპის დაფარვის მცდელობა, კოდის შესრულება პროცესის მეხსიერების სივრცეში (მეხსიერების გამოყენება პრივილიგირებული ესკალაციისთვის), რეპლიკაცია, ფაილების გადაადგილება, ტექნოლოგიური პროცესების სიებში ელემენტების დამალვა და ა.შ. თითოეული საეჭვო ქცევა იწვევს პროცესის რეიტინგის ზრდას და ადმინისტრატორთან გაფრთხილების შეტყობინების გაგზავნას;

პროდუქტი უნდა აძლევდეს არჩევის საშუალებას, თუ რომელი კლიენტი აღმოაჩენს სხვა კომპიუტერებს ქსელიდან;

სინქრონიზაციისთვის განკუთვნილი აგენტი უნდა შედიოდეს ანტიმალვერ კლიენტის კონპლექტაციაში და არ უნდა იყოს წარმოდგენილი როგორც ცალკე კომპონენტი;

გადაწყვეტილების ადმინისტრატორს უნდა შეეძლოს ავტომატური რეალურ დროში სკანირების (realtime scanning) რეჟიმების შეცვლა, კერძოდ გამოტოვოს „X" MB ზომაზე დიდი არქივები/ფაილები და ასევე შეეძლოს სკანირების სასურველი სიღრმის (16 დონე) მითითება.

ადმინისტრატორს უნდა შეეძლოს სკანირების ინსტრუმენტების კონკრეტულ ამოცანაზე მორგება და ჰქონდეს საშუალება აირჩიოს სკანირების რამდენიმე ტექნოლოგიის შორის:	ლოკალური სკანირება (Local Scan), როცა სკანირება ხორციელდება ლოკალურად მომხმარებლის მოწყობილობაზე. ლოკალური სკანირების ტექნოლოგია გამოიყენება მძლავრ მოწყობილობებზე, და ყველა სიგნატურა და ინსტრუმენტი ინახება ლოკალურად. ჰიბრიდული სკანირება (Hybrid Scan) Light Engines (Public Cloud) ინსტრუმენტების გამოყენებით სიგნატურების და ინსტრუმენტების ნაწილი ლოკალურად ინახება, ნაწილობრივ , in the-cloud scanning ფუნქციის გამოყენებით. ცენტრალიზებული სკანირება (Central Scan) , რომლის შემთხვევაში სიგნატურები საერთოდ არ ინახება ლოკალურად.

ვირტუალური ინფრასტრუქტურისთვის:	❯ გადაწყვეტილების ცენტრალური მენეჯმენტ კომპონენტი უნდა ინტეგრირდებოდეს მრავალ VMware vCenters-თან. ❯ რეალურ დროში (real time) და მოთხოვნილებისამებრ (on demand) სკანირების საშუალება Linux ვირტუალური მანქანებისტვის პროდუქტს უნდა გააჩნდეს რამდენიმე Citrix Xen Servers-თან ინტეგრირების საშუალება (რეესტრების პროდუქტში იმპორტირების ფუნქციით). ❯ პროდუქტს უნდა გააჩნდეს Microsoft Hyper-V, Red Hat Virtualization, Oracle VM და KVM-თან ინტეგრირების ფუნქცია. ❯ VDI გარემოში ანტიმალვეარ (antimalware) კლიენტი ინსტალირდება მხოლოდ golden image და რეკომპოსის გარეშე ❯ ყველა ვირტუალური მანქანა უნდა აისახებოდეს კონსოლში როგორც დაცული დამატებითი ინსტრუმენტის გაშვების გარეშე. ❯ პროდუქტი უნდა შეიცავდეს ერთ ვირუალურ მანქანას, რომელიც უზრუნველყოფს სკანირების ოპტიმიზაციას კეშირების მექანიზმის მეშვეობით.
სოლუშენს უნდა გააჩნდეს ანტიმალვეარ კლიენტის კონფიგურაციის საშუალება;	
პროდუქტს უნდა გააჩნდეს offline update-ის გაკეთების შესაძლებლობა იზოლირებულ ინფრასტრუქტურებში. განახლებების მიღება და გავრცელება შესაძლებელია USB HDD/USB Stick, File server, FTP საშუალებით;	
პოლიტიკების მინიჭება შესაძლებელი უნდა იყოს VMware vCenter-ის რესურსების გაერთიანებაზე (resource pool)	
პროდუქტს უნდა გააჩნდეს კონფიდენციალური მონაცემების (pin card, bank account და ა.შ.) დაბლოკვის ფუნქცია როგორც HTTP ასევე SMTP-თვის სპეცილური წესების(rules) შექმნის გზით.	
მომხმარებლების კონტროლი:	სამართავ კონსოლს უნდა გააჩნდეს ჩაშენებული მომხმარებლების კონტროლის მოდული შემდეგი მინიმალური მახასიათებლებით: ❯ ინტერნეტზე წვდომის დაბლოკვა ცალკე მომხმარებლებისთვის ან მომხმარებელთა ჯგუფებისთვის; ❯ განსაზღვრულ აპლიკაციებზე წვდომის დაბლოკვა. ❯ დროის კონკრეტული პერიოდისთვის ინტერნეტზე წვდომის დაბლოკვა ❯ ადმინისტრატორის მიერ მითითებული სპეციფიურ ვებგვერდებზე წვდომა. ❯ კონკრეტულ ვებ-საიტებზე წვდომის შეზღუდვა წინასწარ დადგენილი კატეგორიების მიხედვით(მაგ. ონლაინ გაცნობა, ძალადობა და ა.შ.)
ანტივირუსული პროგრამრული უზრუნველყოფის კლიენტს უნდა შეეძლოს შემდეგი ოპერაციული სისტემების დაცვა და მათთან უნდა იყოს თავსებადი:	Workstation operating systems: ❯ Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3) Server operating systems: ❯ Windows Server 2012, 2012 R2, 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 Virtualization platforms: ● VMware vSphere,6.5,6.0, 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: – VMware vCenter Server 6.5, 6.0, 5.5, 5.1, 5.0 or 4.1 – VMware VShield Manager 5.5, 5.1, 5.0 – VMware VShield VShield Endpoint Manager installed on host – VMware Tools 8.6.0 build 446312 or newer

	– VMware NSX 6.2.4 (6.3 for Linux support) or newer ● VMware View 5.1, 5.0 or newer ● Citrix XenDesktop 5.5, 5.0 or newer ● XenServer 7.1, 7.0, 6.0, 5.6 or 5.5 (including Xen Hypervisor) ● Citrix XenApp ● Microsoft Hyper-V Server 2012, 2008 R2 or Windows 2008 R2 (including Hyper-V Hypervisor) ● Oracle VM 3.0 ● Red Hat Enterprise Virtualization 3.0 (including KVM hypervisor) Operating systems for virtual machines (32/64 bit): ● Windows 10, 8.1, 8, Windows 7, Windows Vista, Windows XP (SP3) ● Windows Server 2016, 2012, Windows Server 2008, Windows Server 2008 R2 Protection for Virtualized Workstations and Servers 14 ● Windows Server 2003, Windows Server 2003 R2 ● Oracle Solaris 11, 10 ● Linux distributions: – Red Hat Enterprise Linux 6 or higher – CentOS 6 or higher – Ubuntu 12.04 or higher – SUSE Linux Enterprise Server 11 or higher – OpenSUSE 12, 11 – Fedora 16, 15 – Debian 7.0 or higher
ცენტრალიზებული მენეჯმენტ სერვერის მოწოდება ხდება Linux თვითკონფიგურირებადი virtual appliance-ის სახით, რომელიც მოიცავს ყველა როლს/სერვისს. VMware vSphere, Citrix XenServer და Microsoft Hyper-V ჰიპერვიზორების მხარდაჭერით. მენეჯმენტ სერვერი უნდა შედგებოდეს მინიმუმ შემდეგი როლებისაგან:	⁾ Database Server ⁾ Update Server ⁾ Web Console ⁾ Communication Server
ანტივირუსულ პროგრამულ უზრუნველყოფას უნდა გააჩნდეს მინიმუმ შემდეგი მახასიათებლები:	Antivirus და Antimalware სიგნატურების განახლებადი ბაზით, ევრისტიკული ანალიზისა და პროცესების უწყვეტი მონიტორინგის ფუნქციით: ⁾ Two-way firewall IDS / IPS ფუნქციით; ⁾ Search Advisor და Web filtering-ის ფუნქციები; ⁾ მონაცემთა დაცვის ფუნქცია; ⁾ User web და application control ფუნქციები; Power user და Restricted user რეჟიმები. ⁾ კარანტინის ლოკალური და დაშორებული მართვა; ⁾ უსაფრთხოების ინდივიდუალური და ჯგუფური პოლიტიკების გამოყენების ფუნქცია; ⁾ Network discovery და mass remote install ფუნქციები; ⁾ Device Control და USB scanning ფუნქცია; ⁾ სხვა ანტივირუსული პროგრამული უზრუნველყოფის ავტომატური აღმოჩენისა და წაშლის ფუნქცია; ⁾ პროდუქტის დისტანციური ინსტალაციის ფუნქცია ქსელში არსებული კლიენტიდან Endpoint Relay-ს როლის გამოყენებით.

	• WAN ტრაფიკის შემცირებისთვის სამართავ კონსოლში შესრულებული ქმედებების აუდიტის ფუნქცია; • Email გაფრთხილებების ფუნქცია. • მონიტორინგის პანელის და რეპორტინგის ფუნქცია.
მენეჯმენტ სერვერი უნდა შეიცავდეს ბალანსირების მოდულს, მენეჯმენტ სერვერის High Availability-სათვის, Disaster Recovery-ისათვის და ასევე წარმადობისათვის	
ცენტრალიზებულ მენეჯმენტ სერვერს უნდა გააჩნდეს Active Directory-სთან ინტეგრაციის საშუალება.	
მენეჯმენტ სერვერის როლების დაყენება შესაძლებელი უნდა იყოს როგორც ერთი virtual appliance-ის სახით, აგრეთვე ცალ ცალკე virtual appliance-ების სახით.	
პროდუქტის სრული მართვა (Management) უნდა ხდებოდეს ვებ-ინტერფეისიდან.	
ანტივირუსის კლიენტების სამართავად არ უნდა იყოს საჭირო დამატებითი პროგრამული უზრუნველყოფის დაყენება. კლიენტის მანქანებზე უნდა დაყენდეს მხოლოდ ერთი პაკეტი.	
ანტივირუსი შეიცავს მინიმუმ შემდეგ კომპონენტებს: Antimalware, Antivirus, ორმხრივი პერსონალური Firewall და Host-based intrusion detection and prevention HIDS/HIPS, Device და Content Control, Antiphishing და Antispyware.	
პროდუქტის Firewall-ს უნდა გააჩნდეს მინიმუმ შემდეგი მახასიათებლები: • Stealth mode-ის დაყენების შესაძლებლობა ლოკალური ქსელის ან ინტერნეტის დონეზე; • შეიცავდეს 3 დონეზე კონფიგურირებად Intrusion Detection System (IDS) სისტემას;	
ანტივირუსის კლიენტი ხელს არ უშლის Cisco Easy VPN კლიენტს სტაბილურ და გამართულ მუშაობაში.	