დანართი N2

ტექნიკური დავალება

შესყიდვის ობიექტი – არსებული ანტივირუსის პროგრამული პაკეტის - „Sophos Endpoint Protection - Advanced“ ლიცენზიის შესყიდვა ერთი წლის ვადით, რომლის განმავლობაშიც მიმწოდებელმა უნდა უზრუნველყოს ანტივირუსის განახლებების ბაზაზე და მწარმოებლის მხარდაჭერის პორტალზე შემსყიდველის წვდომა.

ანტივირუსული პროგრამა და მისი ცენტრალური მართვის სისტემა უნდა შეიცავდეს შემდეგ ფუნქციონალურ კომპონენტებს:

- თავსებადობა Microsoft Windows-ის კომპიუტერულ ოპერაციულ სისტემებთან: Windows 10, 8.1, 8, სერვერებთან Windows Server 2019, 2016, 2012, Linux სისტემებთან - RedHat, Debian, Ubuntu, Suse, ვირტუალიზაციის პლათფორმებთან VMware vSphere/ESX, Microsoft Hyper-V Server, Citrix XenServer;

- სერვერზე ცენტრალური მართვის და ადმინისტრირების სისტემის ინსტალირების შესაძლებლობა, რომელიც თავსებადია Windows Server 2019, 2016, 2012, ვირტუალიზაციის პლათფორმების მხარდაჭერა vSphere, VMWare ESX/ESXi , მონაცემთა ბაზების მხარდაჭერა - SQL 2012, 2014, 2016, 2017, 2019;

- ანტივირუს და ანტისპამ დაცვა Microsoft Exchange სერვერისთვის;
- ანტივირუსული დაცვა ყველა ტიპის ვირუსული საშიშროებისგან - Threats (worms, viruses, trojans) Potentially unwanted applications (PUA), Rootkits, Suspicious files, Suspicious behavior, Buffer overflows, Malicious web content. Host Intrusion Prevention System (HIPS) ფუნქციონალის არსებობა;
- Zero-day უცნობი საშიშროებების აღმოჩენის საშუალება, პროგრამული კოდის ქცევითი ანალიზის შემოწმების და მახასიათებლების მიხედვით, შეაჩეროს უცნობი საშიშროება იქამდე სანამ მისი კოდი გაეშვება;
- პერსონალური ფაერვოლი (Firewall) - ცნობილი და უცნობი საშიშროების შეჩერება აქტიური პორტების მონიტორინგის საშუალებით. სანრო პორტების და პროტოკოლების სიის შექმნის შესაძლებლობა, TCP და UDP სესიების შემოწმება, კრიტიკული შემთხვევების გამოტანა ადმინისტრირების პანელზე და ტრაფიკის ლოგების მონიტორინგის საშუალება;
- კომპიუტერის აპლიკაციების და სხვადასხვა პროგრამების კონტროლი და საჭიროებისამებრ ბლოკირება (მაგ. P2P, file sharing, VoIP, Games და სხვა);
- დაცვის უზრუნველყოფამ უნდა გამოავლინოს სხვადასხვა აპლიკაციების/პროგრამების კრიტიკული განახლებები (Patch Assesment) (მაგ: Microsoft, Adobe, Java, Apple, Citrix, Skype და სხვა), კომპიუტერში დაყენებული პროგრამების შემოწმებას შესაძლო საფრთხეების შეღწევადობაზე. კრიტიკული განახლებების პრიორიტიზირება რისკების მიხედვით;
- ინფორმაციის მატარებლებისა და გარე მოწყობილობების კონტროლი და ბლოკირების საშუალება - Device Control (USB, CD/DVD, Wirelss, Bluetooth);

- ნებისმიერ ინტერნეტ ბრაუზერში გახსნილი ვებ-გვერდების სკანირება მავნე კოდებსა და პროგრამებზე და URL ფილტრაცია/ბლოკირება. Malicious traffic detection და Buffer overflow detection შესაძლებლობა;

- Web Control - ვებ-რესურსებისადმი წვდომის მართვის შესაძლებლობა, დაბლოკილი ან ნებადართული ვებ-გვერდების სიის შექმნა. Download Reputation ინტერნეტ ბრაუზერიდან გადმოწერის დროს ფაილების შემოწმება;

- DLP ტექნოლიგია - მონაცემთა/ინფორმაციის დაკარგვის ან გადინების პრევენცია. - სენსიტიური ან კონფიდენციალური ინფორმაციის ქსელში და გარე მოწყობილობებზე გადაცემის მონიტორინგის საშუალება, სხვადასხვა წესების დანერგვა;

- ერთი ინტერფეისით მართოს დომენის და ჯგუფებში არსებული კომპიუტერები;

- კლიენტის კომპიუტერზე არსებული აპლიკაციების მართვა (ავტორიზაცია/დე-ავტორიზაცია);

- სპეციფიკური წესების დანერგვის საშუალება სხვადასხვა ჯგუფებისათვის;

- ანტივირუსული პროგრამული უზრუნველყოფის ერთი სალიცენზიო ფაილი (გასაღები) მინიმუმ 120 მომხმარებელზე;

- ლიცენზია უნდა იყოს აქტიური მიწოდებიდან 1 წლის განმავლობაში;

- ანტივირუსულ პროგრამულ უზრუნველყოფას უნდა გააჩნდეს სერტიფიკატი, რომელიც ადასტურებს მის გამოყენების უფლების გადაცემას შემსყიდველზე;

- პროგრამის საექსპლუატაციო დოკუმენტაცია ინგლისურ ენაზე;

- მწარმოებლის მომხმარებელზე ორიენტირებული გამოყოფილი ტექ. მხარდაჭერის საშუალება ინგლისურ ენაზე ელ-ფოსტის ან ტელეფონით 24x7-ზე.

შენიშვნა: პრეტენდენტის მიერ წარმოდგენილი შესყიდვის ობიექტის შესაბამისობის დადგენა სატენდერო დოკუმენტაციაში ზემოთ მითითებულ მოთხოვნებთან მოხდება პროდუქტის მწარმოებლის ოფიციალურ ვებ–გვერდზე განთავსებულ ინფორმაციაზე დაყრდნობით.