1. **შესყიდვის ობიექტი**

 შესყიდვის ობიექტს წარმოადგენს ანტივირუსული დაცვის, ანტისპამის და ვებ პროქსის პროგრამული უზრუნველყოფა:

1. თანამშრომლების კომპიუტერების, სერვერების ანტივირუსული დაცვის პროგრამული უზრუნველყოფა - რაოდენობა 500 კომპიუტერი/სერვერი;
2. ელექტრონული ფოსტის ანტივირუსული/ანტისპამის პროგრამული უზრუნველყოფა - რაოდენობა 500 საფოსტო ყუთი;
3. ვებ პროქსის პროგრამული უზრუნველყოფა - 500 მომხმარებელი
4. წარმოდეგნილი პროდუქტების ლიცენზიიების მოქმედების ვადა უნდა იყოს შეძენიდან მინიმუმ 1 წელი
5. **არსებული მდგომარეობა**
* ბანკის თანამშრომლების სამუშაო ადგილებზე და სასერვერო ინფრასტრუქტურაში ინსტალირებულია Symantec Endpoint Protection – 500 მომხარებელი;
* ელექტრონული ფოსტის ანტივირუსული დაცვის და ანტისპამის სისტემა წარმოდგენილია Symantec Messaging Gateway -ს სახით - 500 მომხარებელი;
* ვებ პროქსი Mcafee Web Gateway - 500 მომხარებელი;

**შესყიდვის ობიექტის ტექნიკური მოთხოვნები:**

|  |  |
| --- | --- |
| **კომპიუტერების/სერვერების ანტივირუსული დაცვის პროგრამული უზრუნველყოფა:** | **რაოდენობა** |
| **ძირითადი ფუნქციონალი** |  |
| 1. დაცვის პროგრამული უზრუნველყოფა თავსებადი უნდა იყოს შემდეგ ოპერაციულ სისტემებთან:
* **Windows Operating Systems:**
	+ Windows 7 (32-bit, 64-bit);
	+ Windows 7 Embedded;
	+ Windows 8 (x86 platforms, 32-bit, 64-bit);
	+ Windows 8.1;
	+ Windows 10:
	+ Windows Server 2008 (32-bit, 64-bit, including R2);
	+ Windows Server 2012 (32-bit, 64-bit, including R2);
	+ Windows Server 2016;
	+ Windows Server 2019;
* **Linux Operating Systems (32-bit and 64-bit versions):**
	+ Red Hat Enterprise Linux;
	+ CentOS;
	+ Ubuntu;
	+ Fedora;
* **Virtual Environments:**
	+ VMware ESXi 6.5 , 6.7; 7
1. დაცვის პროგრამულ უზრუნველყოფას უნდა გააჩნდეს დაცვის მრავალდონიანი არქიტექტურა და შეიცავდეს შემდეგ ფუქნციონალს:
	1. ანტივირუსული, spyware, worms, Trojans, bots, rootkits, adware შემოწმებას რეალურ დროში და მოთხოვნების შესაბამისად;
	2. ფაილების რეპუტაციულ ანალიზს;
	3. ელექტრონული ფოსტის გზავნილების შემოწმების შესაძებლობას;
	4. ლოკალური Web ტრაფიკის შემოწმებას;
	5. ქსელის დაცვის მოდულს (Network Intrusion Prevention, URL and Firewall Polices);
	6. აპლიკაციების და პერიფერიული მოწყობილობების კონტროლი (Application and Device Control);
	7. System Lockdown - სამუშაო ადგილების აპლიკაციების კონტროლის ფუნციონალი, „თეთრი“ და „შავი“ სეიბის საშუალებით აპლიკაციების მართვის საშუალება;
	8. Power Eraser (პროგრამების წაშლის ინსტრუმენტი) - ინსტრუმენტი, რომლის საშუალებითაც შესაძლებელია დისტანციურად აღმოიფხვრას მავნე და საფრთხის შემცველი პროგრამები;
	9. Host Integrity - უზრუნველყობს სამუშაო ადგილების პროგრამული უზრუნველყოფების მთლიანობას და უცვლელობას, აღმოაჩინოს არაავტორიზებული ცვლილებები, იზოლირება გაუკეთოს სისტემებს რომლების არ შეესაბამებიან მოთხოვნებს;
	10. ინტერგირებადი იყოს EDR/ATP სისტემასთან;
2. დაცვის პროგრამულ უზრუნველყოფას უნდა გააჩნდეს Signatureless ტექნოლოგიების გამოყენება როგორიც არიან:
	1. ოპერატიული მეხსიერების კონტროლი (Memory Exploit Mitigation) – zore-day ექსპლოიტების ბლოკირება;
	2. პროგრამული უზრუნველყოფის ქცევის კონტროლი (Application Behavioral Control);
	3. ახალი, უცნობი საფრთხეების აღმოჩენა (Advanced Machine Language (AML))
 | 1 |
|  |
| **ზოგადი მოთხოვნები** |
| 1. დაცვის პროგრამულ უზრუნველყოფას უნდა გააჩნდეს დამატებითი ფუნქციონალი, როგორიც არის:
	1. რეპუტაციის ანალიზი (Reputation Analysis);
	2. გლობალური ინტელექტუალური ქსელის გამოყენება (Global Intelligence Network (GIN));
	3. Sandbox გამოყენება დამალული, პოლიმორფული მავნე კოდის აღმოჩენისათვის;
2. დაცვის პროგრამულ უზრუნველყოფას უნდა გააჩნდეს Endpoint firewall-ს ფუნქციონალი, რომლის მართვა უნდა ხორციელდებოდეს ცენტრალიზებულად;
3. დაცვის პროგრამული უზრუნველყოფა უნდა იყოს ცენტრალიზებულად მართვადი, გააჩნდეს ანტივირუსული დაცვის სისტემის ცენტრალიზებულად მართის საშუალება;
4. მოთხოვნის თანახმად, დამატებით შესაძლებელი უნდა იყოს Advanced Threat Protection ფუნქციონალის ჩართვა (დეტექტირება, ფაილების ნახვა და ავტირთვა ATP სისტემაში შემდგომი ანალიზისათვის, ადმინისტრირების ბრძანებების გაგზავნა სამუშაო ადგილებზე (endpoints), ფაილების დამატება თეთრ/შავ სიებში და ა.შ.), რომელიც ინტეგრირებული უნდა იყოს ანტივირუსული დაცვის სისტემასთან და არ უნდა საჭიროებდეს სამუშაო ადგილებზე დამატებითი აგენტების ინსტალაციას;
5. ლიცენზიით გათვალისწინებული მომხმარებლების რაოდენობის გადაჭარბების შემთხვევაში, დაცვის პროგრამული უზრუნველყოფა უნდა იძლეოდეს შესაბამის შეტყობინებას და შეუფერხებლად აგრძელებდეს სრულფასოვან ფუნქციონირებას;
6. დაცვის პროგრამულ უზრუნველყოფას უნდა გააჩნდეს ანტივირუსული ბაზების განახლების ცენტრალიზებული შესაძლებლობა პროდუქტის ფუნქციონირების მთელ პერიოდში;
7. ლიცენზიის მოქმედების განმავლობაში, მიმწოდებლის მიერ შემოთავაზებული პროგრამული უზრუნველყოფის მწარმოებლის მიერ ახალი ვერსიის გამოცემის შემთხვევაში უნდა იყოს შესაძლებელი შემსყიდველის მიერ პროდუქტის განახლება მწარმოებლის ოფიციალური გვერდიდან ჩამოტვირთვის საშუალებით, დამატებითი ანაზღაურების გარეშე;
8. შემოთავაზებული პროგრამული უზრუნველყოფა კომპანია „Gartner“-ს 2018, 2019 და 2020 შეფასებით უნდა იყოს წარმოდგენილი „Magic Quadrant for Endpoint Protection Platforms“ ლიდერის კვადრატში;
 |
| **ლიცენზიები და მხარდაჭერა*** 1 წლიანი განახლებების სერვისი 500 მომხმარებლის მხარდაჭერით რომელიც უნდა მოიცავდეს ზემოთ აღნიშნულ ფუნქციონალს

  |  |

|  |  |
| --- | --- |
| **ელექტრონული ფოსტის ანტივირუსული/ანტისპამის დაცვისთვის პროგრამული უზრუნველყოფა:** | **რაოდენობა** |
| **ძირითადი ფუნქციონალი** |  |
| 1. დაცვის პროგრამული უზრუნველყოფა რეალიზებული უნდა იყოს საფოსტო Gateway-ის სახით და გააჩნდეს შემავალი და გამავალი საფოსტო გზავნილების:
	1. რეალურ დროში ანტივირუსული შემოწმება;
	2. რეალურ დროში ანტისპამის შემოწმება;
	3. DoS შეტევის აღკვეთა;
	4. დამატებით, მოთხოვნების შესაბამისად საფოსტო გზავნილების შიფრაცია;
2. დაცვის პროგრამულ უზრუნველყოფას უნდა ქონდეს დაცვის პერსონალიზირებული წესების რეალიზაციის და მართვის შესაძლებლობა, ანტისპამის წესების „აგრესიულობის“ კონტროლი. მომხმარებელს უნდა ქონდეს შესაძლებლობა აკონტროლის რამდენად ეფექტურია წესები მის გარემოსათვის. მომხმარებელს უნდა ქონდეს პოლიტიკის განსაზღვრის შესაძლებლობა, ბაზირებული მათ მიერ არასასურველი საფოსტო გზავნილების განსაზვრით;
3. დაცვის პროგრამულ უზრუნველყოფას უნდა ქონდეს საფოსტო გზავნილების რეპუდაციული ანალიზის შესაძლებლობა;
4. დაცვის პროგრამულ უზრუნველყოფას უნდა გააჩნდეს ცენტრალიზებული მართვის შესაძლებლობა, რომელის რეალიზებულია Web ინტერფეისის სახით, რომლის საშუალებით:
5. შესაძლებელი იქნება სისტემის სრული ადმინისტრირება და მართვა;
6. Web კონსოლიდან ტენდენციების, შეტევების სტატისტიკის და ინციდენტების ნახვა;
 | 1 |
|  |  |
| **ზოგადი მოთხოვნები** |  |
| 1. დაცვის პროგრამულ უზრუნველყოფას უნდა ქონდეს ჯამური, დეტალური გენერაციის რეპორტების შესაძლებლობა, რომელიც მოგვცემს სისტემის მუშაობის ეფექტურობის დემონტრაციის საშუალებას;
2. დაცვის პროგრამული უზრუნველყოფა რეალიზებული უნდა იყოს ლოგირების შესაძლებლობები;
3. სისტემას უნდა ქონდეს TLS პროტოკოლის მხარდაჭერა რის საშუალებით უზრუნველყოფილი იქნება დაშიფრული საკომუნიკაციო არხის მუშაობის უზრუნველყოფა სხვა საფოსტო სერვერებთან;
4. დაცვის პროგრამულ უზრუნველყოფას უნდა გააჩნდეს საფოსტო გზავნილების შიფრაციის სისტემასთან ინტეგრაციის შესაძლებლობა;
5. დაცვის პროგრამული უზრუნველყოფა რეალიზებული უნდა იყოს ვირტუალური მანქანის VMware ESX 6.5/6.7 -ს სახით;
6. ლიცენზიით გათვალისწინებული მომხმარებლების რაოდენობის გადაჭარბების შემთხვევაში დაცვის პროგრამული უზრუნველყოფა უნდა იძლეოდეს შესაბამის შეტყობინებას და შეუფერხებლად აგრძელებდეს სრულფასოვან ფუნქციონირებას;
7. დაცვის პროგრამულ უზრუნველყოფას უნდა გააჩნდეს ანტივირუსული ბაზების განახლების ცენტრალიზებული შესაძლებლობა პროდუქტის ფუნქციონირების მთელ პერიოდში;
8. ლიცენზიის მოქმედების განმავლობაში, მიმწოდებლის მიერ შემოთავაზებული პროგრამული უზრუნველყოფის მწარმოებლის მიერ ახალი ვერსიის გამოცემის შემთხვევაში უნდა იყოს შესაძლებელი შემსყიდველის მიერ პროდუქტის განახლება მწარმოებლის ოფიციალური გვერდიდან ჩამოტვირთვის საშუალებით, დამატებითი ანაზღაურების გარეშე;
 |  |
| **ლიცენზიები და მხარდაჭერა*** 1 წლიანი განახლებების სერვისი 500 მომხმარებლის მხარდაჭერით რომელიც უნდა მოიცავდეს ზემოთ აღნიშნულ ფუნქციონალს

  |  |

|  |  |
| --- | --- |
| **ვებ პროქსი პროგრამული უზრუნველყოფა:** | **რაოდენობა** |
| **ძირითადი ფუნქციონალი** |  |
| * პროდუქტი წარმოდგენილი უნდა იყოს Virtual Appliance სახით, რომელიც სრულად თავსებადი უნდა VmWare EXS 6.7,7 ჰიპერვიზორთან;
* URL Filtering, ვებ-გვერდების კატეგორიების მიხედვით კლასიფიკაცია (მათ შორის SSL პროტოკოლით დაშიფრული);
* SSL ტრაფიკის ინსპექტირების ფუნქციონალის არსებობა, SSL inspection/HTTPS decryption;
* მომხმარებლების აუტენტიფიკაცია MS AD საშუალებით;
* მომხმარებლებლის, მომხმრებლის ჯგუფების Role-based წვდომების უზრუნველყოფა;
* უსაფრთხოების წესის მომხმარებლის/მომხმარებლების ჯგუფის მიხედვით განსაზღვრა;
* აპლიკაციების კონტროლის ფუქნციონალის უზრუნველყოფა;
* Anti-malware და web რეპუტაციების სერვისის უზრუნველყოფა;
* თეთრი და შავი სიის მექანიზმი (black list, white list), სადაც შესაძლებელი იქნება ნებისმიერი ვებ მისამართის დამატება მიუხედავად იმისა თუ რომელ კატეგორიას ეკუთვნის;
* ვებ გვერდების დაბლოკვა მის კონტენში წინასწარ შედგენილი სიიდან ტერმინების აღმოჩენის შემთხვევაში;
* Predictive machine learning (PML) საშუალების უზრუნველყოფა უცნობი საფრთხეების (malware) დეტექტირებაში;
 | 1 |
|  |
| **ზოგადი მოთხოვნები** |
| 1. მაღალი მდგრადობა (HA) (active-active და active-passive რეჟიმები)
2. SSL ტრაფიკის განტვირთვა (SSL offload)
3. ვებ გვერდების ქეშირება (web caching)
4. ადმინისტრატორის მომხმარებლებისთვის სხვადასხვა როლების მინიჭების საშულება
5. SNMP პროტოკოლების მხარდაჭერა (v1, v2c, v3)
6. ადმინისტრატორის ელფოსტაზე შეტყობინების გაგზავნის ფუნქცია
7. WCCP პროტოკოლის მხარდაჭერა
8. კონფიგურაციის სკრიპტების ატვირთვის საშუალება როგორც ვებიდან ასევე, CLI-დან.
 |
| **ლიცენზიები და მხარდაჭერა*** 1 წლიანი განახლებების სერვისი 500 მომხმარებლის მხარდაჭერით რომელიც უნდა მოიცავდეს ზემოთ აღნიშნულ ფუნქციონალს

  |  |

**დამატებითი პირობები**

იმ შემთხვევაში თუ პრეტენდენტის მიერ შემოთავაზებული იქნება ბანკში უკვე არსებული სისტემების Symantec Endpoint Protection, Symantec Messaging Gateway და Mcafee Web Gateway ლიცენზიების მოწოდება, მიმწოდებელმა ხელშეკრულების გაფორმებიდან 10 სამუშაო დღის ვადაში უნდა უზრუნველყოს შემოთავაზებული პროდუქციის მოწოდება ელექტრონული სახით, რომლის ლიცენზიის მოქმედების ვადა იქნება, ხელშეკრულების გაფორმებიდან, მინიმუმ ერთი წელი.

იმ შემთხვევაში თუ პრეტენდენტის მიერ შემოთავაზებული იქნება ბანკში უკვე არსებული სისტემისაგან განსხვავებული სისტემა, პრეტენდენტის შემოთაზება უნდა ითვალისინებდეს წარმოდგენილი პროდუქტის სრულად დანერგვას და შესყიდვის ობიექტის მიწოდების ვადებს, რაც ჯამში არ უნდა აღემეტებობეს, ხელშეკრულების გაფორმებიდან, 14 სამუშაო დღეს. ასევე პრეტედენტმა უნდა უზრუნველყოს ბანკის პასუხილსმეგებელი თანამშრომლების ტრენინგი წარმოგენილი სისტემის ადმინისტრირებაში და კონფიგურაციაში. წარმოდგენილი ლიცენზიის მოქმედების ვადა, ხელშეკრულების გაფორმებიდან, უნდა იყოს მინიმუმ ერთი წელი. .
აღნიშნულ სამივე შესყიდვის ობიექტზე, შემოთავაზებები განიხილება როგორც ცალ-ცალკე ასევე პაკეტურად.