

## PREKIŲ PIRKIMO – PARDAVIMO SUTARTIES SPECIALIOJI DALIS

**Akcinė bendrovė Lietuvos paštas**, pagal Lietuvos Respublikos įstatymus teisėtai įregistruota ir veikianti akcinė bendrovė, juridinio asmens kodas 121215587, PVM mokėtojo kodas LT212155811, registruotos buveinės adresas J. Jasinskio g. 16, LT-03500 Vilnius, Lietuvos Respublika, apie kurią duomenys kaupiami ir saugomi VĮ Registrų centras, atstovaujama Verslo ir technologijų plėtros padalinio direktoriaus , veikiančio pagal 2021 m. sausio 4 d. įgaliojimą Nr. 1-2021-00001 (toliau – Pirkėjas), ir **UAB ATEA**, pagal Lietuvos Respublikos įstatymus teisėtai įregistruota ir veikianti uždaroji akcinė bendrovė, juridinio asmens kodas 122588443, PVM mokėtojo kodas LT225884413, registruotos buveinės adresas J. Rutkausko g.6, LT-05132 Vilnius, Lietuvos Respublika, duomenys apie kurią kaupiami ir saugomi VĮ Registrų centras, atstovaujama IT projektų koordinatoriaus , veikiančio pagal įmonės direktoriaus 2020-09-09 išduotą įgaliojimą Nr. I-200909/1 (toliau – Tiekėjas), Pirkėjas ir Tiekėjas kiekvienas atskirai toliau vadinamas Šalimi, bendrai vadinami Šalimis, sudarė šią prekių pirkimo - pardavimo sutartį (toliau – Sutartis).

### 1. BENDROSIOS NUOSTATOS IR SUTARTIES OBJEKTAS

- 1.1. Tiekėjas įsipareigoja Sutartyje numatytais sąlygomis suteikti antivirusinės apsaugos programinės įrangos licencijų nuomą (toliau – licencijų nuoma arba prekės) Pirkėjui, o Pirkėjas įsipareigoja sumokėti už šias nuomos paslaugas Tiekėjui Sutartyje nurodytais sąlygomis ir terminais.
- 1.2. Ši Sutartis sudaryta pasibaigus pirkimui, kuriame ekonomiškai naudingiausias pasiūlymas išrinktas pagal kainą.
- 1.3. Sutarties BD yra neatskiriama šios Sutarties dalis. Sutarties BD yra pasiekama adresu <https://www.post.lt/lt/viesieji-pirkimai>. Esant prieštaravimams tarp viešai paskelbtos Sutarties BD ir viešojo pirkimo, kurio pagrindu buvo sudaryta ši Sutartis dokumentuose nurodytos Sutarties BD, taikoma pastaroji.
- 1.4. Sutarties aiškinimo ir taikymo tikslais Sutarties BD 2.1 punkte yra nustatyta Sutarties dokumentų pirmenybės tvarka.

### 2. PREKIŲ KIEKIS IR KAINA

- 2.1. Pagal šią Sutartį Pirkėjui tiekama licencijų nuoma, aprašyta Techninėje specifikacijoje (Sutarties SD priedas Nr. 2).
- 2.2. Sutarčiai taikomas kainos apskaičiavimo būdas – fiksuota kaina. Licencijų nuomų kiekis, kurį už fiksuotą kainą įsigyja Pirkėjas, nurodytas Sutarties SD priede Nr.3 .
- 2.3. Bendra Sutarties kaina yra 52 181,25 eurų (*penkiasdešimt du tūkstančiai vienas šimtas aštuoniasdešimt vienas euras 25 ct*), įskaitant PVM. Bendrą Sutarties kainą sudaro:
  - 2.3.1. Licencijų nuomų kaina – 43 125,00 eurų (keturiasdešimt trys tūkstančiai vienas šimtas dvidešimt penki eurai 00 ct), neįskaitant PVM;
  - 2.3.2. Pridėtinės vertės mokestis (PVM) – 21 % – 9 056,25 eurų (devyni tūkstančiai penkiasdešimt šeši eurai 25 ct).

### 3. PREKIŲ KOKYBĖ

- 3.1. Licencijų nuomos kokybė turi atitikti Sutartyje, Techninėje specifikacijoje nurodytus reikalavimus ir teisės aktų, reglamentuojančių Prekių kokybės, saugos, tiekimo reikalavimus bei standartus.
- 3.2. Licencijų nuomos perdavimo - priėmimo ar Sutarties vykdymo laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 3 kalendorinių dienų terminas.
- 3.3. Licencijų nuomos trūkumais laikomi neatitikimai Sutarties, Techninės specifikacijos reikalavimams ir teisės aktams, reglamentuojantiems Licencijų kokybę ir (ar) tiekimą.

### 4. RĖMIMASIS KITŲ ŪKIO SUBJEKTŲ PAJĖGUMAIS

- 4.1. Sutartis iš Tiekėjo pusės vykdoma jungtinės veiklos pagrindu: NE.
- 4.2. Kai Tiekėjas Pirkimo procedūrų metu atitiktai Pirkimo sąlygose nustatytiems reikalavimams įrodyti rėmėsi kitų ūkio subjektų ekonominiais ir finansiniais pajėgumais, Tiekėjas ir ūkio subjektai, kurių pajėgumais Tiekėjas rėmėsi, prisiima solidarią atsakomybę už Sutarties įvykdymą.
- 4.3. Tiekėjas Sutarčiai vykdyti turi teisę pasitelkti Subtiekėjus tik tai Sutarties daliai, kurią nurodė Pasiūlyme. Tiekėjas Pasiūlyme nurodė Sutarties dalį, kuriai bus pasitelkiami Subtiekėjai: NE.

## **5. PREKIŲ PRISTATYMO TERMINAI IR PERDAVIMO - PRIĖMIMO TVARKA**

- 5.1. Licencijų nuoma teikiama Techninės specifikacijos nustatytais terminais ir tvarka.
- 5.2. Užsakymai teikiami Sutarties SD priede Nr. 1 nurodytu Tiekėjo elektroniniu paštu ir laikomi gautais po 24 valandų nuo Užsakymo išsiuntimo Tiekėjui elektroniniu paštu.
- 5.3. Už vėlavimą suteikti licencijų nuomą per Sutarties SD 0 punkte nustatytą terminą ir / ar ištaisyti jų trūkumus per Sutarties SD 3.2 punkte nustatytą terminą, Tiekėjas, Pirkėjui pareikalavus, moka Pirkėjui 10 (dešimties) procentų eurų dydžio baudą nuo Sutarties vertės už kiekvieną uždelstą dieną.

## **6. MOKĖJIMAI, PINIGINĖS PRIEVOLĖS IR SULAIKYMAI**

- 6.1. Pirkėjas sumoka Tiekėjui už faktiškai suteiktą licencijų nuomą per 30 (trisdešimt) kalendorinių dienų nuo Sąskaitos gavimo dienos.
- 6.2. Tiekėjas per 5 darbo dienas nuo prekių pateikimo pateikia Pirkėjui Sąskaitą už faktiškai pristatytas Prekes.
- 6.3. Maksimalus netesybų ir atlyginamų nuostolių dydis, Tiekėjo mokėtinas pagal šią Sutartį, negali viršyti Sutarties SD 2.3 punkte nurodytos bendros Sutarties kainos.

## **7. SUTARTIES ĮSIGALIOJIMAS IR GALIOJIMAS**

- 7.1. Ši Sutartis įsigalioja nuo Sutarties pasirašymo dienos ir galioja iki visiško Šalių įsipareigojimų pagal šią Sutartį įvykdymo, bet ne ilgiau kaip 37 (trisdešimt septynis) mėnesius, įskaitant apmokėjimo terminą

## **8. SPECIALIOSIOS SĄLYGOS**

- 8.1. Tiekėjas patvirtina, kad aplinkybės, kilusios dėl koronavirusinės infekcijos (COVID-19) sukeltos nepalankios epidemiologinės situacijos nulemtų Lietuvos Respublikos arba kitų šalių kompetentingų valstybės ir (arba) savivaldybių institucijų priimtų sprendimų, kuriais taikomi ribojimai asmenų judėjimui ir (arba) ūkinei veiklai, nėra laikoma nenugalima jėga (Force Majeure) ir neatleidžia Tiekėjo nuo atsakomybės už sutarties neįvykdymą.
- 8.2. Šalys susitarė, kad jei po sutarties sudarymo atsirastų naujos aplinkybės, kurios apribotų Tiekėjo veiklą daugiau arba kitu būdu, nei yra žinoma sutarties sudarymo metu, ir dėl to Tiekėjas negali vykdyti sutartinių prievolių, tuomet Tiekėjas galėtų būti atleidžiamas nuo civilinės atsakomybės už sutarties nevykdymą, tik Tiekėjui įrodžius, kad aplinkybės, kuriomis remiasi Tiekėjas, yra tokio masto ir tokio pobūdžio, kurio nei vienas rūpestingas ir atidus verslininkas negalėjo kontroliuoti ir numatyti sutarties sudarymo metu, ir kad Tiekėjas, veikdamas atidžiai ir rūpestingai, negalėjo užkirsti kelio šių aplinkybių ar jų pasekmių atsiradimui.
- 8.3. Tiekėjas, negalėdamas vykdyti sutartimi prisiimtų prievolių, privalo pateikti Pirkėjui prašymą sutartyje nustatyta tvarka, įskaitant detalią informaciją, kokios nenumatytos aplinkybės konkrečiai įvyko (pvz., įmonės veikla buvo apribota, valstybės draudžia atitinkamų prekių eksportą ir kt.) ir nurodyti priežastis, patvirtinančias, kad šių sutarties vykdymo sutrikdymų Tiekėjas negalėjo protingai numatyti sutarties sudarymo metu. Tiekėjas, siekdamas būti atleistas nuo civilinės atsakomybės, privalo pateikti visą Pirkėjo prašomą ir sutartyje nurodytą informaciją, bei šią informaciją pagrindžiančius dokumentus.
- 8.4. Bet kokios formos korupcija yra netoleruojama. Pirkėjas turi teisę vienašališkai nutraukti Sutartį, jei Tiekėjas (įskaitant bet kurį iš Tiekėjo darbuotojų, tarpininkų, subtiekiejų, atstovų ir kt.) duoda arba pasiūlo (tiesiogiai arba netiesiogiai) bet kuriam Pirkėjo darbuotojui bet kokią naudą daikto, piniginio atlygio, komisinių, paslaugų arba kitos materialios ar nematerialios naudos forma kaip paskatą arba apdovanojimą už bet kurio su šia Sutartimi susijusio veiksmo atlikimą arba susilaikymą jį atlikti, arba už palankumo arba nepalankumo parodymą arba susilaikymą juos parodyti (kyšį) bet kuriam su šia Sutartimi susijusiam asmeniui. Pirkėjui nutraukus Sutartį šiuo pagrindu, Tiekėjas privalo atlyginti Pirkėjui visas patirtas išlaidas, susijusias su Sutarties vykdymo užbaigimu, bei kompensuoti visus dėl Sutarties nutraukimo patirtus nuostolius.
- 8.5. Savo jėgomis ir lėšomis praveisti mokymus savo darbuotojams vagysčių prevencijos tema bei, Pirkėjui paprašius, pateikti tai įrodančius dokumentus Pirkėjo atstovui prieš pradedant šiems darbuotojams teikti paslaugas.
- 8.6. Užtikrinti, kad vykdant Sutartį Tiekėjo darbuotojai laikytųsi Lietuvos Respublikos teisės aktais nustatytų darbuotojų saugos ir sveikatos ir priešgaisrinės saugos reikalavimų.
- 8.7. Tiekėjas patvirtina ir garantuoja, kad tiek šios Sutarties sudarymu, tiek visu jos galiojimo metu jis, jo akcininkai, vadovybė, susijusios įmonės ir jo subtiekiejai (jeigu taikoma) nėra ir nebus subjektai, dėl kurių įgyvendinamos tarptautinės sankcijos, o taip pat nėra ir nebus sudarę sandorių, kurių vykdymas prieštarautų Lietuvos Respublikoje įgyvendinamoms tarptautinėms sankcijoms. Tiekėjas pareiškia, kad nėra ir visą Sutarties galiojimo laiką nebus susijęs (nebendradarbiaus) su subjektais ir asmenimis, įtrauktais į tarptautinių sankcijų sąrašus, o taip pat užtikrins su atitinkamų sektorių sankcijomis susijusių apribojimų laikymąsi. Kylant

šiam punkte numatytų įsipareigojimų pažeidimo rizikai, Tiekėjas įsipareigoja nedelsiant informuoti apie tai Pirkėją. Šios sąlygos galioja visu Sutarties su Tiekėju (Tiekėjo su subtiekejo/ -ais) galiojimo laikotarpiu. Tiekėjas įsipareigoja, sudarant sutartis su subtiekejais, numatyti reikalavimą laikytis šių nuostatų. Šiame Sutarties punkte nustatytų reikalavimų pažeidimas ir/ ar nesilaikymas laikomas esminiu Sutarties pažeidimu ir suteikia teisę Pirkėjui nedelsiant be įspėjimo nutraukti bet kokią arba visas sutartis su Tiekėju, neprivalant sumokėti jokių baudų, atlyginti jokios žalos ar išmokėti kokios nors kompensacijos ar grąžinti pinigų Tiekėjui ir/ar jo subtiekejui, gali atšaukti bet kurį ar visus Užsakymus ir (arba) visai ar iš dalies sustabdyti, panaikinti bet kurias sutartis su Tiekėju. Esant prieštaravimams tarp šio punkto nuostatų ir Sutarties BD 3.6 punkto nuostatų, pirmenybė teikiama šio punkto nuostatomis.

## **9. PRIEDAI**

9.1. Kiekvienas šios Sutarties priedas yra neatskiriama jos dalis. Kiekviena Šalis gauna po vieną kiekvieno Sutarties priedo egzempliorių.

9.2. Sutarties priedai yra:

9.2.1. Sutarties SD priedas Nr. 1 – „Kontaktiniai asmenys“;

9.2.2. Sutarties SD priedas Nr. 2 – „Techninė specifikacija“;

9.2.3. Sutarties SD priedas Nr. 3 – „Licencijų nuomos kiekiai ir kaina“.

## **10. ŠALIŲ REKVIZITAI**

### **Tiekėjas**

#### **UAB ATEA**

J. Rutkausko g. 6, LT-05132 Vilnius

Įmonės kodas: 122588443

PVM kodas: LT225884413

A. s. Nr. LT032140030001327814

Bankas Luminor banks AS, Lietuvos skyrius

Banko kodas 40100

Tel. Nr.: 8 5 239 7830

### **Pirkėjas**

#### **AB Lietuvos paštas**

J. Jasinskio g. 16, 03500 Vilnius

Įmonės kodas: 121215587

PVM kodas: LT212155811

A. s. Nr. LT71 7044 0600 0018 7388

AB SEB bankas

Banko kodas 70440

Tel. Nr.: 8 700 55 400

El. paštas info@post.lt

IT projektų koordinatorius

Verslo ir technologijų plėtros padalinio direktorius

**KONTAKTINIAI ASMENYS**

1.	Už Sutarties vykdymą iš Pirkėjo pusės atsakingas Pirkėjo atstovas	
2.	Už Sutarties ir jos pakeitimų paskelbimą įstatymų nustatyta tvarka yra atsakinga Pirkėjo atstovė	
3.	Už Sutarties vykdymą iš Tiekėjo pusės atsakingas atstovas	
4.	Nesant 1 – 3 punktuose nurodytų atsakingų asmenų, už minėtuose punktuose nurodytų funkcijų vykdymą atsakingais laikomi juos pavaduojantys darbuotojai.	

## TECHNINĖ SPECIFIKACIJA

## 1. SAVOKOS IR SUTRUMPINIMAI

**1.1. Pirkėjas / Perkantysis subjektas – Akcinė bendrovė Lietuvos paštas**

**1.2. Tiekėjas** – ūkio subjektas – fizinis asmuo, privatusis ar viešasis juridinis asmuo, kita organizacija ir jų padalinys arba tokių asmenų grupė, įskaitant laikinas ūkio subjektų asociacijas, su kuriuo Pirkėjas sudarys šio Pirkimo sutartį.

**1.3. Sutartis** – Pirkimo sutartis, sudaroma tarp Tiekėjo ir Pirkėjo dėl šio Pirkimo objekto.

## 2. PIRKIMO OBJEKTAS

2.1. Pirkimo objektas – naudotojų įrangos ir elektroninio pašto apsaugos programinė įranga (toliau – prekės).

2.2. Pirkimo objektas į pirkimo objekto dalis neskaidomas, todėl Tiekėjas privalo teikti pasiūlymą visai žemiau nurodytai pirkimo objekto apimčiai.

2.3. Prekių naudojimo laikotarpis – 36 mėnesiai nuo Sutarties įsigaliojimo dienos.

2.4. Prekių pristatymo vieta – *Vilnius, Jasinskio 16.*

2.5. Prekių kiekiai:

1 lentelė.

Eil. Nr.	Prekės pavadinimas	Prekių kiekis (vnt; pakuotė; pora ar kt. )	Užsakymų teikimas		Prekių pristatymo terminas nuo Sutarties įsigaliojimo
			Taip (žymėti, jei prekių užsakymai bus teikiami pagal poreikį, periodiškai ar kt.)*	Ne (žymėti, jei nurodytu laiku bus pristatytas visas perkamas prekių kiekis)**	
1.	Naudotojų įrenginių ir el.pašto apsaugos programinė įranga	Įrenginių kiekis -2550, el.pašto adresų kiekis - 4000	<input type="checkbox"/>	X	14 k.d.

2.6. Aukščiau esančioje lentelėje nurodytas prekių kiekis yra tikslus ir vykdant Sutartį nesikeis.

2.7. Užsakymų teikimo tvarka:

2.7.1. užsakymai Sutarties galiojimo laikotarpiu neteikiami. Prekės turi būti pristatytos per 1 lentelėje nustatytą terminą.

## 3. REIKALAVIMAI PREKĖMS

2 lentelė

Eil. Nr.	Parametras	Reikalavimai
<b>NAUDOTOJŲ ĮRENGINIŲ APSAUGA</b>		
1.	Licencijų skaičius	2550 naudotojų
2.	Programinės įrangos tipas	Kompiuterinių darbo vietų, serverių, mobiliųjų ir planšetinių įrenginių, apsauga nuo virusų ir šnipinėjimo programų, su ugniasiene, bei apsauga nuo elektroninių šiukšlių. Visi programinės įrangos sprendimai privalo būti valdomi iš vienos administravimo konsolės.
3.	Programinės įrangos gamintojas	Turi būti nurodytas. Visi pateikti apsaugos nuo virusų bei el. šiukšlių produktai turi būti pagaminti to paties gamintojo.
4.	Programinės įrangos pavadinimas ir versija	Turi būti nurodyti.

5.	Palaikoma operacinė sistema	<p>Kompiuterinės darbo vietos:</p> <p><i>Microsoft Windows 10.</i>  <i>Microsoft Windows 8.1.</i>  <i>Microsoft Windows 8.</i>  <i>Microsoft Windows 7.</i>  <i>macOS 10.12 ir naujesnės.</i>  <i>Ubuntu Desktop 18.04 LTS 64-bit.</i>  <i>Ubuntu Desktop 20.04 LTS.</i>  <i>Red Hat Enterprise Linux 7, 8 su įdiegta palaikoma darbalaukio aplinka.</i>  <i>SUSE Linux Enterprise Desktop 15.</i></p> <p>Mobilieji įrenginiai:</p> <p><i>Android 5 (Lollipop) ir naujesnės.</i>  <i>iOS 8 ir naujesnės.</i></p> <p>Serveriai:</p> <p>Windows serveriuose:</p> <ul style="list-style-type: none"> <li>• <i>Microsoft Windows Server 2019 (įskaitant Server Core, Desktop Experience ir Essentials).</i></li> <li>• <i>Microsoft Windows Server 2016 (įskaitant Server Core, Desktop Experience, Storage Server ir Essentials).</i></li> <li>• <i>Microsoft Windows Server 2012 R2 (įskaitant Storage Server ir Essentials).</i></li> <li>• <i>Microsoft Windows Server 2012 (įskaitant Storage Server, Essentials, Foundation ir MultiPoint).</i></li> <li>• <i>Microsoft Windows Server 2008 R2 SP1.</i></li> <li>• <i>Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2).</i></li> <li>• <i>Microsoft Windows MultiPoint Server 2011.</i></li> <li>• <i>Microsoft Windows MultiPoint Server 2010.</i></li> </ul> <p>Pašto serveriuose:</p> <ul style="list-style-type: none"> <li>• <i>Palaikomos pašto serverių versijos:</i></li> <li>• <i>Microsoft Exchange Server 2019 iki CU9.</i></li> <li>• <i>Microsoft Exchange Server 2016 iki CU20.</i></li> <li>• <i>Microsoft Exchange Server 2013 iki CU23 (CU1 ir CU4 yra nepalaikomi).</i></li> <li>• <i>Microsoft Exchange Server 2010 SP1, SP2, SP3 iki RU32.</i></li> <li>• <i>Microsoft Exchange Server 2007 SP1, SP2, SP3.</i></li> <li>• <i>Microsoft Windows Server 2019 (Server Core ir Desktop Experience).</i></li> <li>• <i>Microsoft Windows Server 2016.</i></li> <li>• <i>Microsoft Windows Server 2012 R2.</i></li> <li>• <i>Microsoft Windows Server 2012.</i></li> <li>• <i>Microsoft Windows Server 2008 R2 SP1.</i></li> <li>• <i>Microsoft Windows Small Business Server 2011 SP1 (x64).</i></li> </ul> <p>Linux serveriuose ir kituose nurodytuose:</p> <p><i>RedHat Enterprise Linux (RHEL) 7 ir 8 versijos.</i>  <i>CentOS 7 ir 8 versijos.</i>  <i>Ubuntu Server 16.04/18.04/20.04/ LTS.</i>  <i>Debian 8 ir 9 versijos.</i>  <i>SUSE Linux Enterprise Server (SLES) 12 ir 15 versijos.</i>  <i>Oracle Linux 8.</i>  <i>Amazon Linux 2.</i>  <i>Kerio Control 7.4 ir naujesnės.</i>  <i>Kerio Connect 8 ir naujesnės.</i></p>
----	-----------------------------	---

		<p><i>IBM Lotus Domino 6.5.4 ir naujesnės. HCL Domino 11.</i></p> <p>Turi būti palaikomos virtualios aplinkos: <i>Microsoft Hyper-V Server 2012 ir naujesnė. VMware vSphere/ESXi 5.5 ir naujesnė. VMware Workstation 9 ir naujesnė. Oracle VirtualBox 5.2 ir naujesnė. Citrix 7 ir naujesnė.</i> Sprendimas turi palaikyti VMware vMotion ir vCenter technologijas.</p> <p>Nuotolinio administravimo konsolė turi veikti:</p> <p><i>Microsoft Windows Server 2012 x64. Microsoft Windows Server 2012 x64 Core. Microsoft Windows Server 2012 x64 R2. Microsoft Windows Storage Server 2012 x64 R2. Microsoft Windows Server 2012 x64 R2 Core. Microsoft Windows Server 2016 x64. Microsoft Windows Storage Server 2016 x64. Microsoft Windows Server 2019 x64. Microsoft Windows Small Business Server 2011 Standard (x64). Microsoft Windows Small Business Server 2011 Essentials (x64).</i></p> <p><i>Linux: RHEL, Debian, Ubuntu, SLED, SLES, OpenSUSE, Fedora ir CentOS bei dauguma kitų RPM ir DEB paketų valdymu pagrįstų platinamų programų.</i></p> <p>Nuotolinė administravimo konsolė suderinta su naršyklėmis:</p> <ul style="list-style-type: none"> <li>• Mozilla Firefox 69 ir naujesnės versijos.</li> <li>• Microsoft Edge 44 ir naujesnės versijos.</li> <li>• Google Chrome 77 ir naujesnės versijos.</li> <li>• Opera 63 ir naujesnė.</li> <li>• Safari 13.x ir naujesnės versijos.</li> </ul>
6.	Veikimo kokybės reikalavimai	<p>Programinės įrangos gamintojas turi turėti ISO 9001:2000 arba lygiavertį ir ISO 27001 arba lygiavertį standartą.</p> <p>Siūlomo produkto gamintojas turi būti <i>Leaders</i> arba <i>Challengers</i> kategorijose 2021 metų "Gartner Magic Quadrant for Endpoint Protection Platforms".</p> <p>„AV-TEST“ verslo produktų apžvalgos ir sertifikavimo ataskaitoje gamintojo saugumo sprendimai kuriuos ketina įsigyti Pirkėjas, skirti „Windows“, turi būti įvertinti „TOP Product“ įvertinimu, remiantis 2021 m. rugpjūčio, rugsėjo mėn. atliktais testais „Protection“, „Performance“, „Usability“ kategorijose.</p>

7.	Administravimo konsolės diegimas	Administravimo konsolė turi būti pateikiama kaip virtuali mašina. Jai neturi būti reikalingos operacinės sistemos licencijos.
8.	Diegimo metodai	Kompiuterinėms darbo vietoms turi būti galimybės: <ul style="list-style-type: none"> <li>- diegti programinę įrangą centralizuotai iš valdymo konsolės.</li> <li>- diegti programinę įrangą lokaliai iš diegimo laikmenos.</li> <li>- diegti programinę įrangą per <i>Active Directory Group Policy</i> nustatymus.</li> </ul>
9.	Būtinai kompiuterinių darbo vietų apsaugos funkciniai moduliai	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų, grėsmių. Įsilaužimų prevencijos modulis (HIPS). Išorinių laikmenų apsaugos modulis. Galimybė atstatyti užkrėstą kompiuterį į ankstesnę būseną. Įsilaužimų blokatorius. Ugniasienė. Sprendimas turi leisti pasirinkti, kuriuos apsaugos modulius įdiegti.
10.	Funkciniai reikalavimai kompiuterinių darbo vietų antiviruso moduliui	Antiviruso modulis – programinė įranga, sauganti nuo kenkėjiškų programų; Sprendimas turi užtikrinti centralizuotai atliktų nustatymų veikimą ir kompiuteriui esant neprisijungus prie centralizuotų nustatymų valdymo konsolės; Sprendime turi turėti tokias nuskaitymo parinktis: <ul style="list-style-type: none"> <li>- Išmanusis nuskaitymas.</li> <li>- Kontekstinio meniu nuskaitymas.</li> <li>- Giluminis nuskaitymas.</li> <li>- Išimamų medijų nuskaitymas (pvz CD/DVD/USB), kurie šiuo metu prijungti prie kompiuterio.</li> <li>- Atlikti paskutinį kartą naudotą nuskaitymą.</li> </ul> Galimybė vykdyti euristinį (heuristic) nežinomų failų skenavimą. Galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo, bei išinstaliavimo. Ugniasienės modulis – programinė įranga, sauganti nuo įsilaužimų. Apsaugos nuo elektroninių šiukšlių modulis (Anti-SPAM). Turi būti galimybė valdyti šiuos įrenginius: disko atminties įrenginius, CD/DVD, USB spausdintuvus, FireWire saugyklas, Bluetooth įrenginius, lustinių kortelių skaitytuvus, vaizdavimo įrenginius, modemus, LPT/COM prievadus, nešiojamuosius įrenginius. Sprendimas turi leisti/neleisti naudoti įrenginius pagal šiuos kriterijus: tiekėjas, modelis, serijinis numeris. Saugojimo įrenginiams sprendimas turi leisti nustatyti šiuos naudojimo leidimus: skaityti/rašyti, blokuoti, tik skaityti, įspėti. Įsilaužimų prevencijos modulis (HIPS) turi turėti šiuos režimus: automatinis, išsamusis, interaktyvusis, politika pagrįstas, mokymosi. Galimybė centralizuotai riboti prieigą prie internetinių šaltinių. Turi būti galimybė grafinę vartotojo sąsają pasirinkti lietuvių kalba. Kompiuterinių darbo vietų antivirusinės programos dokumentacija turi būti pateikta lietuvių kalba. Turi būti integruota saugi naršyklė. Turi būti WMI ir viso registro nuskaitymas.



11.	Funkciniai reikalavimai darbo vietų ugniasienei	<p>Turi apsaugoti nuo nepageidaujamų tinklo išorinių atakų, pagal nustatytus kriterijus (pagal prievadus (<i>port</i>), programas) ribojant atakos šaltinio prieigą.</p> <p>Ugniasienė turi leisti/neleisti prisijungti, remiantis bet kuriuo iš šių režimų: automatinis, interaktyvus, politika pagrįstas, mokymosi.</p> <p>Darbo vietų ugniasienės valdymas turi būti atliekamas centralizuotai administravimo konsolės pagalba.</p>
12.	Funkciniai reikalavimai pašto serveriams	<p>Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų.</p> <p>Turi būti galimybė realiu laiku skenuoti visus prisegtus archyvus ir atlikti neutralizavimo veiksmus žinomų formatų byloms.</p> <p>Turi būti galimybė automatiškai skenuoti POP3, IMAP, MAPI ir HTTP protokolus nuo kenkėjiško turinio.</p> <p>Programinė įranga turi turėti galimybę sustabdyti/pratęsti skenavimą.</p> <p>Turi būti rezidentinės euristicinės bei veiksmų analizės galimybės.</p> <p>Programinė įranga turi turėti keletą pasirinkimų, ką daryti su aptikta prisegta byla (neutralizuoti, ištrinti, talpinti į karantiną).</p> <p>Programinė įranga turi turėti apsaugą nuo el. šiukšlių, paremtą gamintojo surinkta duomenų baze apie brukalų siuntėjus, baltaisiais, juodaisiais ir pilkaisiais sąrašais.</p> <p>Turi būti galimybė administratoriui nurodyti specialią direktoriją, į kurią bus siunčiami visi infekuoti laiškai.</p> <p>Turi būti užtikrinta integracija su <i>Active Directory</i>.</p> <p>Turi būti galimybė keisti, apsaugos nuo el. šiukšlių nustatymus, taip pat galimybę vykdyti įvairias užduotis (antiviruso aprašų duomenų bazės atnaujinimas, nustatymai skirti apsaugoti antivirusinę programinę įrangą serveryje) iš centralizuoto valdymo įrankio.</p> <p>Turi būti galimybė eksportuoti valdymo konsolės nustatymus ir juos panaudoti pakartotinio diegimo metu.</p> <p>Galimybė matyti detalias sistemos būklės ataskaitas valdymo konsolėje. Turi būti pateikti tokie duomenys: paskutinio atnaujinimo laikas ir rezultatas, virusų aprašų kiekis, skenavimo variklio versija ir aktyvūs programos moduliai.</p> <p>Turi būti galimybė gauti detalias ataskaitas apie skenavimo veiksmus.</p> <p>Turi būti galimybė administratoriui el. paštu gauti pranešimus apie sistemos įvykius: aptikus netinkamus laiškus, aptiktus kenkėjiškus archyvus ar atakas.</p> <p>Turi būti galimybė automatiškai atnaujinti antivirusų aprašų duomenų bazę tiesiogiai iš interneto arba centralizuotu būdu, siekiant išvengti per didelės tinklo apkrovos bei tinklo sutrikimų.</p> <p>Turi būti galimybė nustatyti atnaujinimų vietą, internetu naudojant <i>proxy</i> (su vartotojo vardu ir slaptažodžiu).</p> <p>Turi būti galimybė atlikti Office 365 pašto dėžutės nuskaitymą.</p> <p>Turi turėti funkciją nesiųsti atmetimo žinutės laiško siuntėjui (Backscatter protection).</p> <p>Turi būti galimybė siųsti pašto karantino ataskaitas nurodytiems vartotojams ir administratoriams.</p> <p>Turi turėti galimybę sinchronizuoti informaciją ir konfigūraciją tarp administravimo konsolės ir pašto serverio(-ių).</p> <p>Turi turėti galimybę integruotis su trečiųjų šalių nuotolinio stebėjimo ir valdymo programine įranga (RMM).</p> <p>Turi būti galimybė eksportuoti žurnalo įrašus į <i>syslog</i></p>

		<p>serverį, kurie galėtų būti panaudojami su kitomis saugumo informacijos ir įvykių valdymo sistemomis (SIEM) ir žurnalų valdymo sprendimais.</p> <p>Turi turėti funkciją blokuoti pašto serverio tinklo ryšį.</p> <p>Turi turėti mašininio mokymųsi paremtą apsaugą - gebėti skenuoti failus, paštą ir tinklo srautą.</p> <p>Turi turėti apsaugą nuo sukčiavimo apsimetant kitu laiško siuntėju (spoofing).</p>
13.	Funkciniai reikalavimai mobiliųjų telefonų ir planšetinių kompiuterių antiviruso moduliui	<p>Turi užtikrinti apsaugą nuo virusų ir kitų kenkėjiškų programų.</p> <p>Turi turėti galimybę skenuoti tiek vidinę, tiek išorinę (<i>micro SD</i> kortelių) įrenginio atmintį. Skenuoti tam tikrus nustatytus aplankus.</p> <p>Praradus įrenginį, turi būti galimybė nuotoliniu būdu gauti įrenginio buvimo koordinatas, užrakinti ir apsaugoti nuo galimybės nesankcionuotai naudotis įrenginiu, saugiai ištrinti kontaktus, žinutes ir duomenis išorinėje laikmenoje (<i>micro SD</i>).</p> <p>Turi būti galimybė apsaugoti įrenginį sukčiavimo atveju.</p> <p>Turi būti galimybė nuotoliniu būdu įrenginyje paleisti sireną.</p> <p>Turi turėti apsaugos modulį nuo brukalų, leidžiantį apsaugoti įrenginį nuo nepageidaujamų skambučių ar SMS/MMS žinučių.</p> <p>Turi būti galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo.</p>
14.	Funkciniai reikalavimai virtualizuotų aplinkų antiviruso moduliui	<p>Sprendimas turi būti valdomas per administravimo konsolę.</p> <p>Turi gebėti atlikti on-access ir on-demand skenavimo užduotis.</p> <p>Turi gebėti atskirti jau nuskaitytus failus vienoje virtualioje mašinoje ir pakartotinai jų nenuskaityti nuo kitų virtualių mašinų per tą patį hipervizorių.</p> <p>Turi turėti galimybę nustatyti proceso išimtis.</p> <p>Turi turėti galimybę siūlomo sprendimo atnaujinimus ir modulius talpinti už virtualių mašinų ribų, kad grąžinant sistemas į ankstesnę momentinę kopiją atnaujinimai nebūtų parsijęti pakartotinai ir atstatymo laikas būtų trumpesnis.</p> <p>Turi būti įgyvendinta galimybė skenuoti išjungtas virtualias mašinas.</p> <p>Jei sprendimas įdiegiamas klasterinėje aplinkoje, turi būti galimybė sukonfigūruoti taip, kad automatiškai dubliuotų savo nustatymus bei būtų valdomas lyg vienas, tuo pačiu išvengiant rankinio nustatymų replikavimo tarp virtualių mazgų klasteryje.</p> <p>Privalo sugebėti užtikrinti virtualių mašinų, įdiegtų Microsoft Azure aplinkoje, apsaugą.</p>
15.	Funkciniai reikalavimai mobiliųjų įrenginių valdymo moduliui	<p>Turi palaikyti centralizuotą administravimą nuotoliniu būdu.</p> <p>Valdymas įgyvendintas kuriant politikas, kurios vėliau priskiriamos įrenginiams ar įrenginių grupėms.</p> <p>Turi būti įgyvendinta galimybė užblokuoti mobiliąsias programėles arba jų kategorijas.</p> <p>Galimybė riboti programų naujinimąsi.</p> <p>Turi turėti galimybę uždrausti atstatyti įrenginio gamyklinius parametrus.</p> <p>Turi turėti galimybę uždrausti keisti įrenginio sisteminius parametrus.</p> <p>Turi turėti galimybę uždrausti pašalinti tam tikras mobiliąsias programėles.</p> <p>Turi turėti galimybę stebėti WI-FI, GPS, Roaming</p>

		<p>duomenis.</p> <p>Turi turėti galimybę masiškai visiems telefonams siusti informacinį pranešimą tiesiai į ekraną.</p> <p>Turi turėti galimybę matyti įrenginyje sudiegtas mobiliąsias programėles ir jų versijas bei jas valdyti.</p> <p>Turi turėti galimybę blokuoti galimas tekstines žinutes bei skambučius.</p> <p>Turi užtikrinti galimybę nuotoliniu būdu įdiegti mobiliąsias programėles be vartotojo pagalbos.</p> <p>Turi turėti galimybę užrakinti/atrakinti mobilųjį įrenginį per nuotolį be vartotojo pagalbos.</p>
16.	Funkciniai reikalavimai valdymo konsolei	<p>Turi palaikyti centralizuotą administravimą nuotoliniu būdu.</p> <p>Serveris turi bendrauti su galutiniais įrenginiais per Agentą, kuris gali saugoti politiką ir vykdyti užduotis, kol įrenginys yra neprisijungęs.</p> <p>Serveris turi leisti pridėti įrenginius prie valdymo konsolės naudojant šiuos metodus:</p> <ul style="list-style-type: none"> <li>- sinchronizavimas su Active Directory;</li> <li>- rankiniu būdu įvedus įrenginio vardą arba IP adresą;</li> <li>- patentuota technologija, gebanti aptikti įrenginius tinkle;</li> </ul> <p>Serveris turi leisti sudiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo.</p> <p>Serveris turi leisti kurti statines ir dinamines grupes lengvesniam įrenginių administravimui.</p> <p>Serveris turi leisti nuotoliniu būdu vizualizuoti šią įrenginių informaciją:</p> <ul style="list-style-type: none"> <li>- pagrindinė informacija;</li> <li>- konfigūracija;</li> <li>- atliktos užduotys;</li> <li>- įdiegtos programos;</li> <li>- perspektyvos;</li> <li>- karantinas.</li> </ul> <p>Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams.</p> <p>Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo.</p> <p>Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies konfigūracinius nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį.</p> <p>Turi turėti antrinio nuotolinio administravimo serverio nustatymo galimybę – nustojus veikti vienam nuotolinio administravimo serveriui, administravimas automatiškai turi pereiti kitam nuotolinio administravimo serveriui.</p> <p>Serveris turi turėti mobiliųjų įrenginių valdymo modulį, kuris leidžia prijungti ir valdyti mobiliuosius įrenginius.</p> <p>Privalo turėti techninės priežiūros įrankį: įrankių kontrolės, duomenų bazės perkėlimo, kopijavimo, duomenų bazės lentelių išvalymo.</p> <p>Turi turėti galimybę paveldėti taisykles (Policies) iš aukštesnio lygio nuotolinio administravimo serverio.</p> <p>Turi būti užtikrinta galimybė siųsti informacinius pranešimus į visų rūšių įrenginius, įskaitant stalinius kompiuterius, mobiliuosius įrenginius ar planšetinius kompiuterius.</p> <p>Turi būti užtikrinta galimybė realiu laiku siųsti valdymo konsolėje gautus įvykius siųsti į centralizuotą įvykių valdymo sistemą (SIEM) Qradar.</p> <p>Serveris turi leisti apibrėžti aktyvąjį, kuris įvykdytų numatytą veiksmą, kai tam tikras įvykis įvyksta tinkle.</p>

		<p>Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus.</p> <p>Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje.</p> <p>Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų.</p> <p>Turi būti realizuota galimybė keisti grafines naudotojo informacijos juostas realiuoju laiku.</p> <p>Turi būti galimybė prieigos profilius konfigūruoti naudojant skirtingus leidimus skirtingoms užduotims, pvz. : administratorius, ataskaitų kūrėjas, operatorius ir kita.</p> <p>Po 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso.</p> <p>Po 15 nesėkmingų bandymų vedant netinkamą seanso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso.</p> <p>Turi būti galimybė nustatyti automatinę Agento atnaujinimo funkciją.</p>
17.	Kiti reikalavimai	<p>Sprendimas turi turėti mechanizmą, kuris leidžia pašalinti bet kurį kitą saugumo sprendimą, esantį galiniame įrenginyje. Šis mechanizmas turi būti:</p> <ul style="list-style-type: none"> <li>- Integruotas į saugumo sprendimą;</li> <li>- Pateiktas kaip atskiras įrankis;</li> <li>- Pasiekiamas per centralizuotą administravimo konsolę;</li> </ul>
18.	Atnaujinimai	<p>Klientinės dalies programinė įranga privalo turėti funkcionalumą parsisiųsti atnaujinimus tiesiai iš:</p> <ul style="list-style-type: none"> <li>- Gamintojo atnaujinimų serverio,</li> <li>- Centralizuoto valdymo serverio,</li> <li>- Kitų klientų.</li> </ul> <p>Klientinės dalies programinė įranga privalo turėti funkcionalumą veikti kaip atnaujinimų serveris kitiems klientams tam, kad būtų galima taupyti tinklo pralaidumo resursus.</p> <p>Turi būti galimybė nustatyti automatinę saugumo produkto atnaujinimo funkciją.</p>
19.	Aktualumo reikalavimas	<p>Pateikiamoms licencijoms turi būti užtikrinamas gamintojo palaikymas sutarties galiojimo laikotarpiu, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (<i>signature</i>), virusų paieškos mechanizmo (<i>engine</i>) atnaujinimus.</p> <p>Programinės įrangos gamintojas privalo turėti internetinį puslapį, kuriame būtų žalingų programų ir jų sukeltų pažeidžiamumų duomenų bazė, informacija apie produktus. Informacija turi būti paskelbta lietuvių ir/ar anglų kalba.</p>
20.	Versija	Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete.
21.	Diegimo failas	<p>Turi būti galimybė diegimo failą atsisiųsti internetu.</p> <p>Tiekėjas turi pateikti bent tris skirtingus valdymo serverio diegimo formatus:</p> <ul style="list-style-type: none"> <li>- Viskas viename;</li> <li>- Įdiegimas pagal programos komponentus;</li> <li>- Virtuali mašina;</li> </ul>
22.	Dokumentacija	Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras.
23.	Gamintojo aptarnavimo (angl. support) sąlygos	Gamintojas ar jo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių ir/ar anglų kalbomis.

24.	Reikalavimai programinės įrangos naudojimo taisyklėms (licencijavimui)	Licencija turi suteikti teisę perdiegti siūlomą programinę įrangą neišnaudojant papildomos licencijos. Programinės įrangos licencijavimo taisyklėse licencija turi būti nepirinama prie aparatūrinės įrangos. Turi būti įgyvendinti vienas iš virtualių mašinų licencijavimo būdų: a) pagal virtualias mašinas (VM); b) pagal fizines mašinas (Host); c) pagal procesorių (CPU).
<b>NAUDOTOJŲ EL. PAŠTO APSAUGA</b>		
Eil. Nr.	Parametras	Minimali reikšmė
1.	Licencijų skaičius	4000 el. pašto naudotojų
2.	Programinės įrangos tipas	El. pašto serverių ir el. pašto vartotojų dėžučių apsauga nuo įvairaus kenkėjiško turinio, šnipinėjimo programų, elektroninių šiukšlių įskaitant užkrėstus el. laiško(-ų) priedus. Visi programinės įrangos sprendimai privalo būti valdomi iš vienos administravimo konsolės.
3.	Programinės įrangos gamintojas	Turi būti nurodytas.
4.	Programinės įrangos pavadinimas ir versija	Turi būti nurodyti.
5.	Serverių palaikomos operacinės sistemos	Palaikomos pašto serverių versijos: <i>Microsoft Exchange Server 2019 iki CU9</i> <i>Microsoft Exchange Server 2016 iki CU20</i> <i>Microsoft Exchange Server 2013 iki CU23 (CU1 ir CU4 yra nepalaikomi)</i> <i>Microsoft Exchange Server 2010 SP1, SP2, SP3 iki RU32</i> <i>Microsoft Exchange Server 2007 SP1, SP2, SP3</i> Palaikomos operacinės sistemos: <i>Microsoft Windows Server 2019 (Server Core ir Desktop Experience)</i> <i>Microsoft Windows Server 2016</i> <i>Microsoft Windows Server 2012 R2</i> <i>Microsoft Windows Server 2012</i> <i>Microsoft Windows Server 2008 R2 SP1</i> <i>Microsoft Windows Small Business Server 2011 SP1 (x64)</i> Konsolę galima naudoti šiose žiniatinklio naršyklėse: • Mozilla Firefox 69 ir naujesnės versijos • Microsoft Edge 44 ir naujesnės versijos • Google Chrome 77 ir naujesnės versijos • Opera 63 ir naujesnė • Safari 13.x ir naujesnės versijos
6.	Veikimo kokybės reikalavimai	Programinės įrangos gamintojas turi turėti ISO 9001:2000 arba lygiavertį ir ISO 27001 arba lygiavertį standartą. Siūlomo produkto gamintojas turi būti <i>Leaders</i> arba <i>Challengers</i> kategorijose 2020 metų Gartner Magic Quadrant for Endpoint Protection Platforms.
7.	Administravimo konsolės diegimas	Administravimo konsolė turi būti pateikiama kaip virtuali mašina. Jai neturi būti reikalingos operacinės sistemos licencijos.
8.	Diegimo metodai	Į el. pašto serverius turi būti galimybė:  - diegti programinę įrangą centralizuotai iš valdymo konsolės; - diegti programinę įrangą lokaliai iš diegimo laikmenos;

9.	Funkciniai reikalavimai pašto serveriams	<p>Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų.</p> <p>Antispam komponentas - saugantis nuo el. šiukšlių</p> <p>Anti-phishing - modulis, kuris filtruoja netinkamą turinį ir apsaugo nuo asmens duomenų vagystės.</p> <p>Turi būti galimybė realiu laiku skenuoti visus prisegtus failus ir atlikti neutralizavimo veiksmus (blokuoti, karantinuoti, gydyti ir kt) žinomų formatų byloms.</p> <p>Turi turėti galimybę blokuoti gaunamus ir siunčiamus laiškus su prisegtais padidintos rizikos failais - vykdomosiomis programomis, MS Office ir Acrobat failais, kuriuose yra aktyvus tyrinys (active content), archyvais, kuriuose yra aukščiau paiminėti failai, bet kokio tipo šifruotais failais.</p> <p>Turi turėti galimybę blokuoti gaunamus ir siunčiamus laiškus su laiško komentare ar turinyje esančiais nuoroda, tekstu ar kelių tekstų junginiais ;</p> <p>Turi turėti galimybę blokuoti gaunamus ir siunčiamus laiškus su prisegtais failais pagal nurodytų failų išplėtimą, failo pavadinimą ar failo pavadinime esančią teksto dalį ar šabloną;</p> <p>Turi būti galimybė automatiškai skenuoti POP3, IMAP, MAPI ir HTTP protokolus nuo kenkėjiško turinio.</p> <p>Programinė įranga turi turėti galimybę sustabdyti/pratęsti skenavimą.</p> <p>Turi būti rezidentinės euristicinės bei veiksmų analizės galimybės.</p> <p>Programinė įranga turi turėti keletą pasirinkimų, ką daryti su aptikta prisegta byla (neutralizuoti, ištrinti, talpinti į karantiną).</p> <p>Programinė įranga turi turėti apsaugą nuo el. šiukšlių, paremtą gamintojo surinkta duomenų baze apie brukalų siuntėjus, baltaisiais, juodaisiais ir pilkaisiais sąrašais.</p> <p>Programinė įranga turi turėti galimybę operatyviai blokuoti el. pašto siuntėją ar siuntėjų grupes naudojant konkrečius adresus ar jų šablonus; Turi būti galimybė administratoriui nurodyti specialią direktoriją, į kurią bus siunčiami visi infekuoti laiškai.</p> <p>Turi būti užtikrinta integracija su <i>Active Directory</i>.</p> <p>Turi būti galimybė keisti, apsaugos nuo el. šiukšlių nustatymus, taip pat galimybę vykdyti įvairias užduotis (antiviruso aprašų duomenų bazės atnaujinimas, nustatymai skirti apsaugoti antivirusinę programinę įrangą serveryje) iš centralizuoto valdymo įrankio.</p> <p>Turi būti galimybė eksportuoti valdymo konsolės nustatymus ir juos panaudoti pakartotinio diegimo metu.</p> <p>Galimybė matyti detalias sistemos būklės ataskaitas valdymo konsolėje. Turi būti pateikti tokie duomenys: paskutinio atnaujinimo laikas ir rezultatas, virusų aprašų kiekis, skenavimo variklio versija ir aktyvūs programos moduliai.</p> <p>Turi būti galimybė gauti detalias ataskaitas apie skenavimo veiksmus.</p> <p>Turi būti galimybė administratoriui el. paštu gauti pranešimus apie sistemos įvykius: aptikus netinkamus laiškus, aptikus kenkėjiškus archyvus ar atakas.</p> <p>Turi būti galimybė automatiškai atnaujinti antivirusų aprašų duomenų bazę tiesiogiai iš interneto arba centralizuotu būdu, siekiant išvengti per didelės tinklo apkrovos bei tinklo sutrikimų.</p> <p>Turi būti galimybė nustatyti atnaujinimų vietą, internetu naudojant <i>proxy</i> (su vartotojo vardu ir slaptažodžiu).</p> <p>Turi būti galimybė atlikti Office 365 pašto dėžutės</p>
----	--	---

		<p>nuskaitymą</p> <p>Turi turėti funkciją nesiųsti atmetimo žinutės laiško siuntėjui (Backscatter protection).</p> <p>Turi būti galimybė siųsti pašto karantino ataskaitas nurodytiems vartotojams ir administratoriams.</p> <p>Turi turėti galimybę sinchronizuoti informaciją ir konfigūraciją tarp administravimo konsolės ir pašto serverio(-ių).</p> <p>Turi turėti galimybę integruotis su trečiųjų šalių nuotolinio stebėjimo ir valdymo programine įranga (RMM).</p> <p>Turi būti galimybė eksportuoti žurnalo įrašus į syslog serverį, kurie galėtų būti panaudojami su kitomis saugumo informacijos ir įvykių valdymo sistemomis (SIEM) ir žurnalų valdymo sprendimais.</p> <p>Turi turėti funkciją blokuoti pašto serverio tinklo ryšį.</p> <p>Turi turėti mašininio mokymosi paremta apsaugą - gebėti skenuoti failus, paštą ir tinklo srautą.</p> <p>Turi turėti apsaugą nuo sukčiavimo apsimetant kitu laiško siuntėju (spoofing).</p>
10.	Funkciniai reikalavimai valdymo konsolėi	<p>Turi palaikyti centralizuotą administravimą nuotoliniu būdu.</p> <p>Serveris turi bendrauti su galutiniais įrenginiais per Agentą, kuris gali saugoti politiką ir vykdyti užduotis, kol įrenginys yra neprisijungęs.</p> <p>Serveris turi leisti pridėti įrenginius prie valdymo konsolės naudojant šiuos metodus:</p> <ul style="list-style-type: none"> <li>- sinchronizavimas su Active Directory;</li> <li>- rankiniu būdu įvedus įrenginio vardą arba IP adresą;</li> <li>- patentuota technologija, gebanti aptikti įrenginius tinkle;</li> </ul> <p>Serveris turi leisti sudiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo.</p> <p>Serveris turi leisti kurti statines ir dinamines grupes lengvesniam įrenginių administravimui.</p> <p>Serveris turi leisti nuotoliniu būdu vizualizuoti šią įrenginių informaciją:</p> <ul style="list-style-type: none"> <li>- pagrindinė informacija;</li> <li>- konfigūracija;</li> <li>- atliktos užduotys;</li> <li>- įdiegtos programos;</li> <li>- perspektyvos;</li> <li>- karantinas;</li> </ul> <p>Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams.</p> <p>Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo.</p> <p>Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies konfigūracinius nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį.</p> <p>Turi turėti antrinio nuotolinio administravimo serverio nustatymo galimybę – nustojus veikti vienam nuotolinio administravimo serveriui, administravimas automatiškai turi pereiti kitam nuotolinio administravimo serveriui.</p> <p>Privalo turėti techninės priežiūros įrankį: įrankių kontrolės, duomenų bazės perkėlimo, kopijavimo, duomenų bazės lentelių išvalymo.</p> <p>Turi turėti galimybę paveldėti taisykles (Policies) iš aukštesnio lygio nuotolinio administravimo serverio.</p> <p>Turi būti užtikrinta galimybė siųsti informacinius pranešimus į visų rūšių įrenginius, įskaitant stalinius kompiuterius, mobiliuosius įrenginius ar planšetinius kompiuterius.</p>

		<p>Serveris turi leisti apibrėžti aktyvklį, kuris įvykdytų numatytą veiksmą, kai tam tikras įvykis įvyksta tinkle. Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus.</p> <p>Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje.</p> <p>Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų.</p> <p>Turi būti realizuota galimybė keisti grafines naudotojo informacijos juostas realiuoju laiku.</p> <p>Turi būti galimybė prieigos profilius konfigūruoti naudojant skirtingus leidimus skirtingoms užduotims, pvz .: administratorius, ataskaitų kūrėjas, operatorius ir kita.</p> <p>Po 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso.</p> <p>Po 15 nesėkmingų bandymų vedant netinkamą senso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso.</p>
12.	Atnaujinimai	<p>Klientinės dalies programinė įranga privalo turėti funkcionalumą parsisiųsti atnaujinimus tiesiai iš:</p> <ul style="list-style-type: none"> <li>- Gamintojo atnaujinimų serverio,</li> <li>- Centralizuoto valdymo serverio,</li> <li>- Kitų klientų.</li> </ul> <p>Klientinės dalies programinė įranga privalo turėti funkcionalumą veikti kaip atnaujinimų serveris kitiems klientams tam, kad būtų galima taupyti tinklo pralaidumo resursus.</p> <p>Turi turėti funkcionalumą automatiškai atnaujinti programinę įrangą.</p>
13.	Aktualumo reikalavimas	<p>Pateikiamoms licencijoms turi būti užtikrinamas gamintojo palaikymas sutarties galiojimo laikotarpiu, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (<i>signature</i>), virusų paieškos mechanizmo (<i>engine</i>) atnaujinimus.</p> <p>Programinės įrangos gamintojas privalo turėti internetinį puslapį, kuriame būtų žalingų programų ir jų sukeltų pažeidžiamumų duomenų bazė, informacija apie produktus. Informacija turi būti paskelbta lietuvių ir/ar anglų kalba.</p>
14.	Versija	Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete.
15.	Diegimo failas	<p>Turi būti galimybė diegimo failą atsisiųsti internetu.</p> <p>Pardavėjas turi pateikti bent tris skirtingus valdymo serverio diegimo formatus:</p> <ul style="list-style-type: none"> <li>- Viskas viename;</li> <li>- Įdiegimas pagal programos komponentus;</li> <li>- Virtualus prietaisas;</li> </ul>
16.	Dokumentacija	Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras.
17.	Gamintojo aptarnavimo (angl. support) sąlygos	Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių ir/ar anglų kalbomis.



18.	Reikalavimai programinės įrangos naudojimo taisyklėms (licencijavimui)	Licencija turi suteikti teisę perdiegti siūlomą programinę įrangą neišnaudojant papildomos licencijos. Programinės įrangos licencijavimo taisyklėse licencija turi būti neprišama prie aparatūrinės įrangos.
-----	--	--

**LICENCIJŲ NUOMOS KIEKIAI IR KAINA**

Eil. Nr.	Prekių pavadinimas	Mato vnt.	Kiekis	Vieneto kaina Eur be PVM	Bendra suma Eur be PVM
1	Naudotojų įrenginių (2 550vnt) ir el. pašto (4 000vnt) apsaugos programinė įranga	paketas	1	43 125,00	52 181,25