KOMPIUTERINIŲ DARBO VIETŲ IR TARNYBINIŲ STOČIŲ APSAUGOS IR KONTROLĖS PROGRAMINĖS ĮRANGOS 2000 LICENCIJŲ VIEŠOJO PIRKIMO-PARDAVIMO SUTARTIS

(investicijų projektas „Integruotos muitinės informacinės sistemos aprūpinimas reikiamomis standartinės programinės įrangos licencijomis“)

2017 m. liepos 4 d. Nr. 11B-99

Vilnius

Uždaroji akcinė bendrovė „Fortevento“ (toliau – Pardavėjas), atstovaujama direktoriaus Aurelijaus Šaltenio, veikiančio pagal bendrovės įstatus, ir Muitinės departamentas prie Lietuvos Respublikos finansų ministerijos (toliau – Pirkėjas), atstovaujamas generalinio direktoriaus Arūno Adomėno, veikiančio pagal Muitinės departamento prie Lietuvos Respublikos finansų ministerijos nuostatus, patvirtintus Lietuvos Respublikos finansų ministerijos 1998 m. liepos 10 d. įsakymu Nr. 171, toliau kartu vadinami Šalimis, sudarė kompiuterinių darbo vietų ir tarnybinių stočių apsaugos ir kontrolės programinės įrangos 2000 licencijų viešojo pirkimo-pardavimo sutartį (toliau – Sutartis).

I. SUTARTIES DALYKAS

1.1. Pardavėjas įsipareigoja perduoti Pirkėjo nuosavybėn Sutarties 1 priede nurodytą programinę įrangą *Sophos Endpoint Protection Advanced* su licencija (toliau – Prekė) ir teise į atnaujinimus 36 (trisdešimt šešių) mėnesių laikotarpiui, o Pirkėjas sumokėti už prekes ir Sutartyje nurodytomis sąlygomis ir tvarka.

1.2. Prekės turi būti pristatytos, instaliuotos ir įdiegtos per 5 (penkias) darbo dienas nuo Sutarties įsigaliojimo dienos.

1.3. Prekių pristatymas, instaliavimas ir įdiegimas įforminamas pasirašant Prekių perdavimo-priėmimo aktą (Sutarties 3 priedas) ir/arba licencijavimo sutartį ar kitą dokumentą.

1.4. Prekių pristatymo vieta – Muitinės informacinių sistemų centras, Vytenio g. 7, LT-03113 Vilnius.

II. ŠALIŲ PAREIŠKIMAI IR GARANTIJOS

2.1. Kiekviena iš Šalių pareiškia ir garantuoja kitai Šaliai, kad:

2.1.1. Šalis yra tinkamai įsteigta ir teisėtai veikia pagal Lietuvos Respublikos įstatymus;

2.1.2. Šalis atliko visus teisinius veiksmus, būtinus, kad Sutartis būtų tinkamai sudaryta ir galiotų, bei turi visus teisės aktais numatytus leidimus, licencijas, darbuotojus, reikalingus prekei pateikti ir paslaugoms teikti;

2.1.3. sudarydama Sutartį, Šalis neviršija savo kompetencijos ir nepažeidžia ją saistančių įstatymų, kitų privalomų teisės aktų, taisyklių, statutų, teismo sprendimų, įstatų, nuostatų, potvarkių, įsipareigojimų ir susitarimų;

2.2. Pardavėjas užtikrina ir atsako, kad jo perduodamos Prekės nepažeidžia trečiųjų asmenų patentinių, pramoninių, autorių ar kitų intelektinės nuosavybės teisių ir kad Pirkėjas nepatirs jokių išlaidų ar nuostolių dėl reikalavimų arba įpareigojimų, susijusių su intelektinės nuosavybės teisėmis į Sutarties dalyką, išskyrus atvejus, kai toks pažeidimas atsiranda dėl Pirkėjo kaltės.

III. SUTARTIES KAINA IR ATSISKAITYMO TVARKA

3.1 Bendra Sutarties kaina yra 54 692,00 Eur (penkiasdešimt keturi tūkstančiai šeši šimtai devyniasdešimt du eurai 00 ct), įskaitant pridėtinės vertės mokestį (toliau – PVM) (Sutarties 2 priedas).

3.2. Į bendrą Sutarties kainą įskaityta Prekių kaina ir visi mokesčiai ir visos Pardavėjo išlaidos, įskaitant, bet neapsiribojant transporto, pakavimo, komplektavimo, pakrovimo, tranzito, iškrovimo, išpakavimo, tikrinimo, draudimo ir kitomis su prekių teikimu susijusiomis išlaidomis bei visomis su dokumentų, kurių reikalauja Pirkėjas, rengimu ir pateikimu susijusiomis išlaidomis.

3.3. Bendra Sutarties kaina yra fiksuota ir Sutarties vykdymo laikotarpiu nekeičiama. Pardavėjui už pristatytas Prekes mokėtina Sutartyje nurodyta fiksuota kaina dėl kainų lygio pasikeitimo ir mokesčių pasikeitimo (išskyrus PVM) nebus perskaičiuojama. Sutartyje nurodyta fiksuota kaina gali būti perskaičiuota ją didinant arba mažinant tik tuo atveju, jei pasikeičia PVM mokėjimą reglamentuojantys teisės aktai, darantys tiesioginę įtaką Sutartyje nurodytai fiksuotai kainai. Sutartyje nurodyta kaina gali būti pakeista tik Šalių rašytiniu susitarimu, pasirašytu Šalių įgaliotų atstovų ir patvirtintu Šalių antspaudais. Perskaičiuota Prekės kaina įsigalioja kitą dieną po to, kai Sutarties Šalys rašytiniu susitarimu juos pakeičia.

3.4. Pardavėjui už pateiktas Prekes apmokama neviršijant einamiesiems metams investicijų projektui „Integruotos muitinės informacinės sistemos aprūpinimas reikiamomis standartinės programinės įrangos licencijomis“ teisės aktų nustatyta tvarka patvirtintos (patikslintos) asignavimų sumos per 30 (trisdešimt) kalendorinių dienų po pasirašyto priėmimo–perdavimo akto (-ų) pagrindu išrašytos PVM sąskaitos faktūros (-ų) gavimo dienos.

3.5. Pirkėjas mokėtiną sumą už pristatytas Prekes moka pavedimu į Pardavėjo nurodytą banko sąskaitą. Pardavėjas apie banko sąskaitos pasikeitimus raštu privalo informuoti Pirkėją nedelsdamas, bet ne vėliau kaip per 5 (penkias) darbo dienas nuo banko sąskaitos pasikeitimo dienos.

3.6. Mokėjimas atliekamas eurais.

3.7. Šalių rašytiniu susitarimu, pasirašytu Šalių įgaliotų atstovų ir patvirtintu Šalių antspaudais, gali būti nustatyta kita mokėjimo tvarka dėl Pirkimo objektui sustabdyto, sumažinto/padidinto Pirkėjui finansavimo.

IV. ŠALIŲ ĮSIPAREIGOJIMAI

4.1. Pardavėjas įsipareigoja:

4.1.1. Prekes ir visus su Prekėmis susijusius dokumentus pristatyti per 5 (penkias) darbo dienas nuo Sutarties įsigaliojimo dienos;

4.1.2. Prekes ir visus su Prekėmis susijusius dokumentus pateikti adresu: Vytenio g. 7, Vilnius, Pirkėjo darbo valandomis;

4.1.3. užtikrinti iš Sutarties vykdymo metu gautos ir su Sutarties vykdymu susijusios informacijos konfidencialumą ir apsaugą;

4.1.4. be raštiško išankstinio Pirkėjo sutikimo neatskleisti jokiam kitam asmeniui iš Pirkėjo vykdant Sutartį gautos informacijos, duomenų, gautų dokumentų turinio nepriklausomai nuo to, kokiu būdu ir forma (žodine, rašytine, elektronine, kita) tokia informacija, duomenys, dokumentai Pardavėjui buvo pateikti ar jis juos sužinojo vykdydamas Sutartį. Ši nuostata galioja net ir nutraukus sudarytą Sutartį ar jai pasibaigus;

4.1.5. nutraukus Sutartį ar jai pasibaigus, ne vėliau kaip per 30 (trisdešimt) dienų sunaikinti visą iš Pirkėjo gautą ar Sutarties vykdymo metu sužinotą informaciją, duomenis, dokumentus (nepriklausomai nuo jų formos ir turinio), išskyrus, jeigu Lietuvos Respublikos įstatymai reikalauja, kad tokia informacija, duomenys, dokumentai būtų išsaugoti;

4.1.6. nenaudoti Pirkėjo ženklų ar pavadinimo jokioje reklamoje, leidiniuose ar kitur be išankstinio raštiško Pirkėjo sutikimo;

4.1.7. be rašytinio išankstinio Pirkėjo sutikimo nekeisti subtiekėjų. Užtikrinti, kad naujas subtiekėjas atitiktų tuos kvalifikacinius reikalavimus, kurie buvo nustatyti Konkurso sąlygose. Subtiekėjo (-ų) keitimo tvarkos pažeidimas laikomas esminiu Sutarties sąlygų pažeidimu;

4.1.8. tinkamai vykdyti kitus įsipareigojimus, numatytus Sutartyje ir Sutarties prieduose bei Lietuvos Respublikos teisės aktuose.

4.2. Pirkėjas įsipareigoja:

4.2.1. priimti Prekes, jeigu jos atitinka šios Sutarties reikalavimus;

4.2.2. apmokėti už Prekės Sutarties III skyriuje nustatyta tvarka;

4.2.3. suteikti informaciją ir/ar dokumentus, būtinus Sutarčiai vykdyti;

4.2.4. tinkamai vykdyti kitus įsipareigojimus, numatytus Sutartyje ir jos prieduose.

4.3. Pardavėjas turi teisę:

4.3.1. minėti Sutarties vykdymo faktą ir Sutarties objektą savo kvalifikacijos pagrindimo tikslais dalyvaudamas viešuosiuose pirkimuose ir konkursuose;

4.3.2. Sutarties ir jos priedų turinį atskleisti Pardavėjo bankams, draudimo bendrovėms, auditoriams, su kuriais Pardavėjas yra sudaręs konfidencialios informacijos apsaugos susitarimus.

4.4. Pirkėjas turi teisę informaciją apie Sutarties turinį bei ją vykdančio Pardavėjo duomenis teikti asmenims, kurie pagal Lietuvos Respublikoje galiojančius teisės aktus turi teisę tokią informaciją gauti.

V. SUTARTIES ŠALIŲ ATSAKOMYBĖ

5.1. Jei Pardavėjas dėl savo kaltės vėluoja pristatyti Prekes, jis sumoka Pirkėjui už kiekvieną uždelstą dieną 0,03 (trijų šimtųjų) procento dydžio delspinigius nuo laiku nepristatytų Prekių vertės.

5.2. Jeigu Pirkėjas neatsiskaito su Pardavėju Sutartyje nustatytais terminais, jis sumoka Pardavėjui 0,03 (trijų šimtųjų) procento dydžio delspinigius nuo laiku nesumokėtos sumos už kiekvieną pavėluotą dieną. Pirkėjas, dėl nuo jos nepriklausančių priežasčių, negalėjęs laiku atsiskaityti su Pardavėju, delspinigių nemoka.

5.3. Šalis, dėl kurios veiksmų kita Šalis patiria nuostolius, privalo atlyginti tik tos Šalies patirtus tiesioginius nuostolius.

5.4. Delspinigių sumokėjimas neatleidžia Šalių nuo sutartinių įsipareigojimų vykdymo.

VI. NENUGALIMA JĖGA (*FORCE MAJEURE*)

6.1. Šalis nėra laikoma atsakinga už bet kokių įsipareigojimų pagal Sutartį neįvykdymą ar dalinį neįvykdymą, jeigu Šalis įrodo, kad tai įvyko dėl neįprastų aplinkybių, kurių Šalys negalėjo kontroliuoti ir protingai numatyti, išvengti ar pašalinti jokiomis priemonėmis.

6.2. Nenugalimos jėgos aplinkybėmis laikomos aplinkybės, nurodytos Civilinio kodekso 6.212 str. ir Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklėse, patvirtintose Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840. Nustatydamos nenugalimos jėgos aplinkybes šalys vadovaujasi Lietuvos Respublikos Vyriausybės 1997 m. kovo 13 d. nutarimu Nr. 222 „Dėl nenugalimos jėgos (*force majeure*) aplinkybes liudijančių pažymų išdavimo tvarkos patvirtinimo“.

6.3. Esant nenugalimos jėgos aplinkybėms, Sutarties Šalys Lietuvos Respublikos teisės aktuose nustatyta tvarka yra atleidžiamos nuo atsakomybės už sutartyje numatytų prievolių neįvykdymą, dalinį neįvykdymą arba netinkamą įvykdymą, o įsipareigojimų vykdymo terminas pratęsiamas. Šalis, prašanti ją atleisti nuo atsakomybės, privalo pranešti kitai Šaliai raštu apie nenugalimos jėgos aplinkybes nedelsdama, bet ne vėliau kaip per 3 (tris) darbo dienas nuo tokių aplinkybių atsiradimo ar paaiškėjimo, pateikdama įrodymus, kad ji ėmėsi visų pagrįstų atsargumo priemonių ir dėjo visas pastangas, kad sumažintų išlaidas ar neigiamas pasekmes, taip pat pranešti galimą įsipareigojimų įvykdymo terminą.

6.4. Pranešimo taip pat reikalaujama, kai išnyksta įsipareigojimų nevykdymo pagrindas. Pagrindas atleisti šalį nuo atsakomybės atsiranda nuo nenugalimos jėgos aplinkybių atsiradimo momento arba, jeigu laiku nebuvo pateiktas pranešimas, nuo pranešimo pateikimo momento. Jeigu Šalis laiku neišsiunčia pranešimo arba neinformuoja, ji privalo kompensuoti kitai Šaliai žalą, kurią ši patyrė dėl laiku nepateikto pranešimo arba dėl to, kad nebuvo jokio pranešimo.

VII. SUBTIEKĖJAI

7.1. Pardavėjas Sutarties vykdymui gali pasitelkti subtiekėjus, tačiau už tinkamą ir kokybišką Sutarties vykdymą Pirkėjui visiškai atsako Pardavėjas.

7.2. Pardavėjas visiškai atsako už kokybišką Sutarties vykdymą ir atlikimą laiku, taip pat visiškai atsako už bet kurių trečiųjų asmenų, kuriuos jis gali samdyti Sutarties vykdymui, darbą. Susitarimas, pagal kurį Pardavėjas dalies savo įsipareigojimų, numatytų Sutartyje, vykdymui pasitelkia trečiuosius asmenis, yra laikomas subtiekimo sutartimi, kuris turi atitikti žemiau nurodytus reikalavimus:

7.2.1. toks susitarimas turi būti rašytinis;

7.2.2. Pardavėjas Sutarčiai vykdyti, išskyrus 7.2.3 punkte numatytą atvejį, turi pasitelkti tik tuos subtiekėjus, kurie numatyti Pardavėjo pasiūlyme. Pirkėjo sutikimas, kad sutartiniams įsipareigojimams vykdyti būtų pasitelkiamas subtiekėjas, neatleidžia Pardavėjo nuo jokių jo įsipareigojimų pagal Sutartį;

7.2.3. Sutarties vykdymo metu, kai subtiekėjai netinkamai vykdo įsipareigojimus Pardavėjui, taip pat tuo atveju, kai subtiekėjai nepajėgūs vykdyti įsipareigojimų Pardavėjui dėl iškeltos restruktūrizavimo, bankroto bylos, bankroto proceso vykdymo ne teismo tvarka, inicijuotos priverstinio likvidavimo ar susitarimo su kreditoriais procedūros arba jiems vykdomų analogiškų procedūrų ar kitais atvejais, Pardavėjas gali pakeisti subtiekėjus. Apie tai Pardavėjas iš anksto raštu turi informuoti Pirkėją, nurodydamas subtiekėjų pakeitimo priežastis ir būsimus subtiekėjus, kurie turi atitikti konkurso sąlygose nustatytus subtiekėjui taikomus reikalavimus. Subtiekėjų keitimas įforminamas abiejų Sutarties Šalių pasirašomu susitarimu. Šis susitarimas tampa neatskiriama Sutarties dalimi.

7.2.4. Šios sąlygos dėl subtiekimo taikomos tik tuomet, jei pasiūlyme Pardavėjas nurodė, kad subtiekėjus pasitelks.

7.3. Nei viena šios Sutarties Šalis neturi teisės perleisti savo teisių ir pareigų, kylančių iš šios Sutarties, tretiesiems asmenims.

VIII. ŠALIŲ GINČŲ SPRENDIMO TVARKA

8.1. Bet koks ginčas ir (ar) reikalavimas, kylantis iš Sutarties ar susijęs su ja ar iš šios Sutarties pažeidimo, nutraukimo ar negaliojimo, bus sprendžiamas Šalių tarpusavio susitarimu.

8.2. Šalims nepasiekus susitarimo per 30 (trisdešimt) kalendorinių dienų, toks ginčas ar reikalavimas, kylantis iš Sutarties ar susijęs su Sutartimi, jos pažeidimu, nutraukimu ir negaliojimu, bus sprendžiamas teismine tvarka atitinkamame teisme, teritorinį teismingumą nustatant pagal Pirkėjo buveinę.

IX. SUTARTIES GALIOJIMAS, PAKEITIMAS, PAPILDYMAS, NUTRAUKIMAS

9.1. Sutartis įsigalioja nuo pasirašymo dienos ir galioja 36 (trisdešimt šešis) mėnesius.

9.2. Sutarties sąlygos Sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias Sutarties sąlygas, kurias pakeitus nebūtų pažeisti Lietuvos Respublikos viešųjų pirkimų įstatymo 3 straipsnyje nustatyti principai. Sutarties sąlygų keitimu nebus laikomas Sutarties sąlygų koregavimas joje numatytomis aplinkybėmis, jei šios aplinkybės nustatytos aiškiai ir nedviprasmiškai bei buvo pateiktos konkurso sąlygose. Tais atvejais, kai Sutarties sąlygų keitimo būtinybės nebuvo įmanoma numatyti rengiant konkurso sąlygas ir (ar) Sutarties sudarymo metu, Sutarties Šalys gali keisti tik neesmines Sutarties sąlygas. Esminės Sutarties sąlygos (Sutarties objektas, kainodaros taisyklės, Sutarties trukmė) negali būti keičiamos visą Sutarties vykdymo laikotarpį. Sutarties sąlygos gali būti keičiamos tik rašytiniu Šalių susitarimu.

9.3. Sutartis gali būti nutraukta:

9.3.1. rašytinių Šalių susitarimu;

9.3.2. Pirkėjas, raštu įspėjęs Pardavėją prieš 14 (keturiolika) kalendorinių dienų, Sutartį gali nutraukti šiais atvejais:

9.3.2.1. kai Pardavėjas nevykdo arba netinkamai vykdo savo sutartinių įsipareigojimų ir/ar nepašalina arba netinkamai pašalina Pirkėjo raštu nurodytus trūkumus;

9.3.2.2. kai Pardavėjas yra likviduojamas, sustabdo ūkinę veiklą;

9.3.2.3. kai Pardavėjas teismo sprendimu pripažintas kaltu dėl sukčiavimo, korupcijos ar kitų panašaus pobūdžio veikų padarymo;

9.3.2.4. kai keičiasi Pardavėjo organizacinė struktūra – juridinis statusas, pobūdis ar valdymo struktūra ir tai gali turėti įtakos tinkamam Sutarties įvykdymui;

9.3.2.5. kitais atvejais, jeigu Sutarties neįmanoma vykdyti dėl nuo Pirkėjo nepriklausančių aplinkybių (sustabdytas arba sumažintas finansavimas ir kt.).

9.3.3. Pardavėjas, raštu įspėjęs Pirkėją prieš 14 (keturiolika) kalendorinių dienų, gali nutraukti Sutartį, kai Pirkėjas nevykdo savo įsipareigojimų daugiau kaip 90 (devyniasdešimt) kalendorinių dienų.

9.4. Pirkėjas po Sutarties nutraukimo parengia ataskaitą apie Sutarties nutraukimo dieną esančią Pardavėjo skolą Pirkėjui ir Pirkėjo skolą Pardavėjui.

9.5. Jei Sutartis nutraukiama Pirkėjo iniciatyva dėl Pardavėjo kaltės, Pirkėjo patirti nuostoliai ar išlaidos išieškomi teisės aktų nustatyta tvarka.

9.6. Sutartį nutraukus dėl Pardavėjo kaltės, be jam priklausančio atlyginimo už pristatytą Prekę, Pardavėjas neturi teisės į kokių nors patirtų nuostolių ar žalos kompensavimą.

X. KITOS SĄLYGOS

10.1. Šalys įsipareigoja nedelsiant informuoti viena kitą apie visus naujus įvykius ir aplinkybes, galinčius turėti įtakos tinkamam Sutarties vykdymui.

10.2. Visi pranešimai, prašymai, rašytiniai reikalavimai ir kiti dokumentai, reikalingi dėl Sutarties, turi būti atlikti raštu ir išsiųsti paštu (registruotu laišku) arba faksimilinio ar elektroninio ryšio priemonėmis, Sutartyje nurodytais Šalių adresais.

10.3. Pirkėjo paskirti už Sutarties vykdymą atsakingi asmenys bei jų kontaktai: Muitinės informacinių sistemų centro Kompiuterių įrangos skyriaus viršininkas Jūrius Bruklys, tel. 236 2324.

10.4. Pardavėjo paskirti už Sutarties vykdymą atsakingi asmenys bei jų kontaktai: Eglė Kibildienė, egle.kibildiene@fortevento.lt; Andrej Orlov, andrej.orlov@fortevento.lt.

10.5. Šalys privalo informuoti viena kitą apie jų teisinio statuso, adresų, telefonų bei faksų numerių, elektroninio pašto adresų, kitų rekvizitų, atsakingų asmenų pasikeitimą ne vėliau kaip per 2 (dvi) darbo dienas jiems pasikeitus.

XI. BAIGIAMOSIOS NUOSTATOS

11.1. Sutartis sudaroma dviem vienodą galią turinčiais egzemplioriais, po vieną kiekvienai Šaliai su priedais, kurie yra neatskiriama Sutarties dalis.

11.2. Sutarčiai ir visoms iš Sutarties atsirandančioms teisėms ir pareigoms taikomi Lietuvos Respublikos įstatymai ir kiti norminiai teisės aktai.

XII. SUTARTIES PRIEDAI

12.1. Kompiuterinių darbo vietų ir tarnybinių stočių apsaugos ir kontrolės programinės įrangos 2000 licencijų pirkimo techninė specifikacija, 1 priedas.

12.2. Kainos ir kiekiai, 2 priedas.

12.3. Prekių perdavimo-priėmimo akto forma, 3 priedas.

XIII. SUTARTIES ŠALIŲ REKVIZITAI

PIRKĖJAS
Muitinės departamentas prie Lietuvos Respublikos finansų ministerijos
A. Jakšto g. 1, LT-01105 Vilnius
Tel. 266 611, Faks. 266 6005
Juridinio asmens kodas 188656838
A. s. LT37 4010 0424 0007 0037
AB DNB bankas

Generalinis direktorius

A. V.

Arūnas Adomėnas

PARDAVĖJAS
Uždaroji akcinė bendrovė „Fortevento“
Lvovo g. 105A, LT-08104 Vilnius
Tel. 205 9895, Faks. 205 9899
Juridinio asmens kodas 302327313
PVM mokėtojo kodas LT100004630711
A. s. LT177044060006867877
AB SEB bankas

Direktorius

A. V.

Aurelijus Šaltenis

2017 m. liepos 4 d.
Sutarties Nr. 11B-99
1 priedas

KOMPIUTERINIŲ DARBO VIETŲ IR TARNYBINIŲ STOČIŲ APSAUGOS IR KONTROLĖS PROGRAMINĖS ĮRANGOS 2000 LICENCIJŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

Eil. Nr.	Antivirusinės programinės įrangos licencijavimo charakteristikos pavadinimas	Reikalaujama parametro reikšmė	Siūlomos programinės įrangos parametro reikšmė
1.	**Bendri reikalavimai**	1.1. Siūlomas apsaugos sprendimas turi turėti integruotas sekančias saugumo funkcijas: antivirusinė sistema apsaugai nuo žalingų programų; išorinių kompiuterinės darbo vietos sąsajų kontrolė; kompiuterinei darbo vietai skirta ugniasienė; pataisų valdymo funkcionalumas; aplikacijų kontrolės funkcionalumas; apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas; centralizuota saugumo komponentų valdymo konsolė; apsaugos nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention) ir apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas; priežasties-pasekmės analizės įrankis (angl. root cause analysis tool). 1.2. Vienas centralizuoto valdymo įrankis turi galėti valdyti minimaliai šiuos siūlomos programinės įrangos komponentus: antivirusinė sistema; išorinių kompiuterinės	1.1. Siūlomas apsaugos sprendimas turi integruotas sekančias saugumo funkcijas: antivirusinė sistema apsaugai nuo žalingų programų; išorinių kompiuterinės darbo vietos sąsajų kontrolė; kompiuterinei darbo vietai skirta ugniasienė; pataisų valdymo funkcionalumas; aplikacijų kontrolės funkcionalumas; apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas; centralizuota saugumo komponentų valdymo konsolė; apsaugos nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention) ir apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas; priežasties-pasekmės analizės įrankis (angl. root cause analysis tool). 1.2. Vienas centralizuoto valdymo įrankis gali valdyti minimaliai šiuos siūlomos programinės įrangos komponentus: antivirusinė sistema; išorinių kompiuterinės

		darbo vietos sąsajų kontrolė; kompiuterinei darbo vietai skirta ugniasienė; pataisų valdymo funkcionalumas; aplikacijų kontrolės funkcionalumas; apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas. 1.3. Siūlomas sprendimas turi užtikrinti antivirusinę apsaugą Windows, Mac, Linux, operacinių sistemų platformoms. 1.4. Siūlomas sprendimo antivirusinė apsauga turi palaikyti virtualias kompiuterines darbo vietas/tarnybines stotis minimaliai šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): VMware vSphere / ESX; VMware Worktation; VMware View; Citrix XenServer; Citrix XenApp; Microsoft Hyper-V Server; Linux virtualioms tarnybinėms stotims su VMware ar Citrix. 1.5. Licencija turi būti skirta apsaugoti ne mažiau nei 2000 vartotojų. Vartotojui skirta licencija turi apsaugoti ne mažiau nei 3 kompiuteriniai įrenginiai (pav. stalinis kompiuteris, nešiojamas kompiuteris, išmanusis mobilus telefonas, planšetinis kompiuteris), t.y. licencijuojama ne per įrenginį.	darbo vietos sąsajų kontrolė; kompiuterinei darbo vietai skirta ugniasienė; pataisų valdymo funkcionalumas; aplikacijų kontrolės funkcionalumas; apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas. 1.3. Siūlomas sprendimas užtikrina antivirusinę apsaugą Windows, Mac, Linux, operacinių sistemų platformoms. 1.4. Siūloma sprendimo antivirusinė apsauga palaiko virtualias kompiuterines darbo vietas/tarnybines stotis minimaliai šiose platformose (nereikalauja atskiros licencijos virtualios infrastruktūros apsaugai): VMware vSphere / ESX; VMware Worktation; VMware View; Citrix XenServer; Citrix XenApp; Microsoft Hyper-V Server; Linux virtualioms tarnybinėms stotims su VMware ar Citrix. 1.5. Licencija skirta apsaugoti 2000 vartotojų. Vartotojui skirta licencija apsaugo ne mažiau nei 3 kompiuterinius įrenginius (pav. stalinis kompiuteris, nešiojamas kompiuteris, išmanusis mobilus telefonas, planšetinis kompiuteris), t.y. licencijuojama ne per įrenginį.
2.	**Reikalavimai antivirusinės sistemos funkcionalumui**	2.1. Siūloma sistema turi užtikrinti apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų	2.1. Siūloma sistema užtikrina apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų

		programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų; 2.2. Sistema turi galėti proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms; 2.3. Sistema turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys; 2.4. Sistema turi aptikti kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoti; 2.5. Siūlomas sprendimas turi atsinaujinti ne mažiau kaip du kartus per dieną; 2.6. Sistema turi užtikrinti skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu; 2.7. Sistema turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus ir turi būti galimybė skirti nurodyta kompiuterio resursų kiekį šiam skenavimui; 2.8. Siūlomas sprendimas turi galėti automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų; 2.9. Siūloma sistema turi apsaugoti internetines naršykles (tokias kaip „Internet Explorer“, “Edge”, „Firefox“, „Chrome“, „Safari“, “Opera”), blokuojant prieigą prie žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą; 2.10. Sistema turi leisti numatyti išimtis specifinių	programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų; 2.2. Sistema proaktyviai blokuoja virusus prieš pasirodant virusų aprašų duomenų bazėms; 2.3. Sistema atlieka žalingų veiksmų stebėseną ir aptinka dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo analizuojamas jos elgesys; 2.4. Sistema aptinka kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoja; 2.5. Siūlomas sprendimas atsinaujina ne mažiau kaip du kartus per dieną; 2.6. Sistema užtikrina skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu; 2.7. Sistema leidžia nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus ir turi galimybę skirti nurodytą kompiuterio resursų kiekį šiam skenavimui; 2.8. Siūlomas sprendimas automatiškai atlika sistemos išvalymą nuo aptiktų žalingų programų; 2.9. Siūloma sistema apsaugo internetines naršykles (tokias kaip „Internet Explorer“, “Edge”, „Firefox“, „Chrome“, „Safari“, “Opera”), blokuojant prieigą prie žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą; 2.10. Sistema leidžia numatyti išimtis specifinių direktorijų ar

		direktorijų ar rinkmenų skenavimui; 2.11. Siūloma saugumo sistema turi galėti skenuoti minimaliai šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS cab, rar, tar.; 2.12. Sistema turi gebėti atpažinti failo tipą, t.y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį; 2.13. Sistema turi užtikrinti saugumą nešiojamiems, staliniams kompiuteriams, tarnybinėms stotims, mobiliems įrenginiams; 2.14. Saugumo sistema turi galėti aptikti polimorfines virusų atmainas; 2.15. Saugumo sistema turi galėti blokuoti įtartinas rinkmenas minimaliai pagal tokius kriterijus: Naudojamas dvigubas plėtinys; Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt); 2.16. Siūloma sistema turi galėti atlikti JavaScript emuliaciją ir elgesio analizę siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo; 2.17. Siūloma apsaugos sistema turi užtikrinti „keliaujančių“ kompiuterių saugų darbą internete, t.y. kai kompiuteris yra ne organizacijos tinkle. Sistema turi gebėti patikrinti interneto svetainės turinį prieš jį pateikiant vartotojo internetinei naršyklei, pagal tokius minimalius parametrus: Įvertinti ar lankoma svetainė neįeina į infekuotų ir pavojingų tinklalapių sąrašą; Taikyti svetainių filtravimą pagal kategorijas;	rinkmenų skenavimui; 2.11. Siūloma saugumo sistema skenuoja šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS cab, rar, tar.; 2.12. Sistema geba atpažinti failo tipą, t.y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį; 2.13. Sistema užtikrina saugumą nešiojamiems, staliniams kompiuteriams, tarnybinėms stotims, mobiliems įrenginiams; 2.14. Saugumo sistema aptinka polimorfines virusų atmainas; 2.15. Saugumo sistema blokuoja įtartinas rinkmenas minimaliai pagal tokius kriterijus: Naudojamas dvigubas plėtinys; Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt); 2.16. Siūloma sistema atlieka JavaScript emuliaciją ir elgesio analizę siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo; 2.17. Siūloma apsaugos sistema užtikrina „keliaujančių“ kompiuterių saugų darbą internete, t.y. kai kompiuteris yra ne organizacijos tinkle. Sistema patikrina interneto svetainės turinį prieš jį pateikiant vartotojo internetinei naršyklei, pagal tokius minimalius parametrus: Įvertina ar lankoma svetainė neįeina į infekuotų ir pavojingų tinklalapių sąrašą; Taiko svetainių filtravimą pagal kategorijas;

		2.18. Siūlomo sprendimo nustatymų turi būti negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises kompiuteryje; 2.19. Siūloma saugumo sistema turi palaikyti ir apsaugoti 32/64 bit operacines Windows, Linux sistemas; 2.20. Siūloma sistema turi turėti integruotą karantino paskyrą. Administratorius turi galėti leisti prieigą pasirinktiems vartotojams prie jų karantino paskyros, kur vartotojai minimaliai galėtų atlikti šiuos veiksmus: Išvalyti užkrėstą rinkmeną; Perkelti užkrėstą rinkmeną; Ištrinti užkrėstą rinkmeną. 2.21. Siūlomas produktas informacinių technologijų tyrimo įstaigos Gartner (http://www.gartner.com) 2016 metų duomenimis turi būti tarp lyderiaujančių produktų („Leaders“ kategorijoje) darbo vietų apsaugos platformų grupėje (Magic Quadrant for Endpoint Protection Platforms).	2.18. Siūlomo sprendimo nustatymų negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises kompiuteryje; 2.19. Siūloma saugumo sistema palaiko ir apsaugo 32/64 bit operacines Windows, Linux sistemas; 2.20. Siūloma sistema turi integruotą karantino paskyrą. Administratorius gali leisti prieigą pasirinktiems vartotojams prie jų karantino paskyros, kur vartotojai minimaliai galėtų atlikti šiuos veiksmus: Išvalyti užkrėstą rinkmeną; Perkelti užkrėstą rinkmeną; Ištrinti užkrėstą rinkmeną. 2.21. Siūlomas produktas informacinių technologijų tyrimo įstaigos Gartner (http://www.gartner.com) 2016 metų duomenimis yra tarp lyderiaujančių produktų („Leaders“ kategorijoje) darbo vietų apsaugos platformų grupėje (Magic Quadrant for Endpoint Protection Platforms).
3.	**Reikalavimai saugumo sistemos centralizuoto valdymo, administravimo ir konfigūravimo funkcijoms**	3.1. Siūlomo sprendimo centralizuoto valdymo konsolė turi galėti valdyti apsaugos sistemas šiose platformose: Windows, Mac, Linux; 3.2. Siūlomo sprendimo kompiuterinių darbo vietų atnaujinimas turi galėti vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir turi būti numatyta galimybė kompiuterinėms darbo vietoms parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete; 3.3. Turi būti galimybė numatyti pirminį ir antrinį	3.1. Siūlomo sprendimo centralizuoto valdymo konsolė valdo apsaugos sistemas šiose platformose: Windows, Mac, Linux; 3.2. Siūlomo sprendimo kompiuterinių darbo vietų atnaujinimas vyksta tiesiai iš gamintojo atnaujinimo serverio internetu ir yra numatyta galimybė kompiuterinėms darbo vietoms parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete; 3.3. Yra galimybė numatyti pirminį ir antrinį atnaujinimo

		atnaujinimo serverius, tam, kad jei kompiuterinė darbo vieta yra lokaliame tinkle ji siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris), jei ta pati darbo vieta naudojama už organizacijos tinklo perimetro ribų, atnaujinimus ji turi galėti parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris); 3.4. Turi būti numatyta galimybė kontroliuoti atnaujinimo parsisiuntimui skirtą pralaidumą; 3.5. Siūlomas sprendimas turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus sistema išsiųstų el. paštu įspėjimą; 3.6. Siūlomas sprendimas turi leisti grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus: pagal IP adresą; pagal atnaujinimo būklę; pagal kompiuterio būklę; pagal įspėjamuosius pranešimus ar klaidas; pagal virusų incidentus. 3.7. Turi būti numatyta galimybė sistemos administratoriui nuotoliniu būdu išspręsti problemas pasirenkant vieną ar keletą kompiuterių „vienu mygtuko paspaudimu“ šiems veiksmams: Apsaugoti kompiuterį įdiegiant ar pakartotinai įdiegiant apsaugos programinę įrangą; Priverstinai paleisti atnaujinimą; Paleisti pilną sistemos skenavimą; Pašalinti įspėjamuosius	serverius, tam, kad jei kompiuterinė darbo vieta yra lokaliame tinkle ji siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris), jei ta pati darbo vieta naudojama už organizacijos tinklo perimetro ribų, atnaujinimus ji gali parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris); 3.4. Numatyta galimybė kontroliuoti atnaujinimo parsisiuntimui skirtą pralaidumą; 3.5. Siūlomas sprendimas leidžia nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus sistema išsiųstų el. paštu įspėjimą; 3.6. Siūlomas sprendimas leidžia grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus: pagal IP adresą; pagal atnaujinimo būklę; pagal kompiuterio būklę; pagal įspėjamuosius pranešimus ar klaidas; pagal virusų incidentus. 3.7. Numatyta galimybė sistemos administratoriui nuotoliniu būdu išspręsti problemas pasirenkant vieną ar keletą kompiuterių „vienu mygtuko paspaudimu“ šiems veiksmams: Apsaugoti kompiuterį įdiegiant ar pakartotinai įdiegiant apsaugos programinę įrangą; Priverstinai paleisti atnaujinimą; Paleisti pilną sistemos skenavimą; Pašalinti įspėjamuosius pranešimus;

		pranešimus; Priverstinai pritaikyti nustatytąją saugumo politiką; Perkelti pasirinktus kompiuterius į kitą grupę (taisyklės turi būti taikomos automatiškai pagal naują grupę); Ištrinti kompiuterį iš sąrašo. 3.8. Siūlomo sprendimo centralizuoto valdymo konsolė turi integruotis su Active Directory ir veiksmai atliekami direktorijoje turi būti sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole. Pašalinus vartotoją ar grupę iš Active Directory, tie patys įrašai automatiškai turi būti pašalinami ir iš saugumo sprendimo centralizuoto valdymo konsolės; 3.9. Siūlomas sprendimas turi leisti taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams; 3.10. Siūlomas sprendimas turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą. Roles turi būti galimybė susikurti pačiai organizacijai ir neturi būti ribojamas jų skaičius; 3.11. Siūlomas sprendimas turi galėti registruoti administratoriaus veiksmus auditavimo tikslais; 3.12. Siūlomas sprendimas turi turėti integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją esančią saugumo sistemos duomenų bazėje. Ataskaitos turi būti generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate. Ataskaitas turi būti galima automatiškai išsiųsti el. paštu minimaliai šiais	Priverstinai pritaikyti nustatytąją saugumo politiką; Perkelti pasirinktus kompiuterius į kitą grupę (taisyklės turi būti taikomos automatiškai pagal naują grupę); Ištrinti kompiuterį iš sąrašo. 3.8. Siūlomo sprendimo centralizuoto valdymo konsolė integruojasi su Active Directory ir veiksmai atliekami direktorijoje turi būti sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole. Pašalinus vartotoją ar grupę iš Active Directory, tie patys įrašai automatiškai pašalinami ir iš saugumo sprendimo centralizuoto valdymo konsolės; 3.9. Siūlomas sprendimas leidžia taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams; 3.10. Siūlomas sprendimas leidžia rolėmis su skirtingomis administravimo teisėmis paremtą administravimą. Roles galima susikurti pačiai organizacijai ir neribojamas jų skaičius; 3.11. Siūlomas sprendimas gali registruoti administratoriaus veiksmus auditavimo tikslais; 3.12. Siūlomas sprendimas turi integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudoja visą informaciją esančią saugumo sistemos duomenų bazėje. Ataskaitos generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate. Ataskaitas galima automatiškai išsiųsti el.paštu minimaliai šiais formatais: pdf, html, doc, xls, rtf, xml;

		formatais: pdf, html, .doc, xls, rtf, xml; 3.13. Siūlomo sprendimo centralizuoto valdymo konsolę minimaliai turi būti galima įdiegti šiose platformose: Windows 7; Windows Server 2003; Windows Server 2008; Windows Server 2012. Taip pat turi būti palaikomos minimaliai šios virtualizavimo platformos: vSphere; VMWare ESX/ESXi; VMWare Workstation; VMWare Server; Citrix XenServer; Hyper-V 2008/2008 R2/2012/2012 R2.	3.13. Siūlomo sprendimo centralizuoto valdymo konsolę galima įdiegti šiose platformose: Windows 7; Windows Server 2003; Windows Server 2008; Windows Server 2012. Taip pat palaikomos minimaliai šios virtualizavimo platformos: vSphere; VMWare ESX/ESXi; VMWare Workstation; VMWare Server; Citrix XenServer; Hyper-V 2008/2008 R2/2012/2012 R2.
4.	**Reikalavimai išorinių kompiuterinės darbo vietos sąsajų ir aplikacijų kontrolės funkcionalumui**	4.1. Siūlomas sprendimas turi galėti leisti nustatyti kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams; 4.2. Siūlomas sprendimas turi galėti kontroliuoti minimaliai šio tipo išorinius įrenginius: išorinės atminties talpos įrenginius; CD ir DVD įrenginius; Floppy įrenginius; Infraraudonąją jungtimi prijungiamus įrenginius; Wifi įrenginius; Bluetooth jungtimi prijungiamas įrenginius; 4.3. Siūlomas sprendimas turi galėti priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms; 4.4. Siūlomas sprendimas turi galėti atlikti sekančius veiksmus įrenginiams: leisti prijungti visus to paties modelio įrenginius; leisti naudoti įrenginį pagal jo unikalų identifikacijos numerį; leisti įrenginiui prisijungti pilnomis teisėmis;	4.1. Siūlomas sprendimas leidžia nustatyti kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams; 4.2. Siūlomas sprendimas kontroliuoja šio tipo išorinius įrenginius: išorinės atminties talpos įrenginius; CD ir DVD įrenginius; Floppy įrenginius; Infraraudonąją jungtimi prijungiamus įrenginius; Wifi įrenginius; Bluetooth jungtimi prijungiamas įrenginius; 4.3. Siūlomas sprendimas priskiria išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms; 4.4. Siūlomas sprendimas atlieka sekančius veiksmus įrenginiams: leisti prijungti visus to paties modelio įrenginius; leisti naudoti įrenginį pagal jo unikalų identifikacijos numerį; leisti įrenginiui prisijungti pilnomis teisėmis;

		leisti įrenginiui prisijungti tik „skaitymo“ režime; 4.5. Siūlomas sprendimas turi turėti galimybę blokuoti “bridge” režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos; 4.6. Siūlomo sprendimo įrenginių kontrolei pasiekti turi būti valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės; 4.7. Sistema turi leisti kontroliuoti programas (ang. application) siekiant užtikrinti tinklo resursų išnaudojimą ir saugumą. Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. torrent, p2p), greitųjų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai; 4.8. Sistema turi užtikrinti automatinį kontroliuojamų programų atnaujinimą naujomis versijomis, automatinį programų aptikimą ir blokavimą; 4.9. Turi būti numatyta galimybė siūlomas aplikacijas skirstyti į kategorijas (ne mažiau kaip 10 kategorijų); 4.10. Siūlomas sprendimas turi galėti priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms; 4.11. Siūlomo sprendimo aplikacijų kontrolei pasiekti turi būti valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.	leisti įrenginiui prisijungti tik „skaitymo“ režime; 4.5. Siūlomas sprendimas gali blokuoti “bridge” režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos; 4.6. Siūlomo sprendimo įrenginių kontrolei pasiekti valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės; 4.7. Sistema leidžia kontroliuoti programas (ang. application) siekiant užtikrinti tinklo resursų išnaudojimą ir saugumą. Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. torrent, p2p), greitųjų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai; 4.8. Sistema užtikrina automatinį kontroliuojamų programų atnaujinimą naujomis versijomis, automatinį programų aptikimą ir blokavimą; 4.9. Numatyta galimybė siūlomas aplikacijas skirstyti į kategorijas (ne mažiau kaip 10 kategorijų); 4.10. Siūlomas sprendimas gali priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms; 4.11. Siūlomo sprendimo aplikacijų kontrolei pasiekti valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.
5.	**Reikalavimai duomenų nutekėjimo prevencijos**	5.1. Siūloma sistema turi turėti integruotą funkcionalumą duomenų iš kompiuterinės	5.1. Siūloma sistema turi integruotą funkcionalumą duomenų iš kompiuterinės

	funkcionalumui (angl. Data loss prevention)	darbo vietos tyčinio ar netyčinio praradimo apsaugai; 5.2. Sistema turi leisti nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pav. neleisti su tam tikra žyma dokumento siųsti el. paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa); 5.3. Siūlomos sistemos duomenų kontrolės funkcionalumas turi būti valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės; 5.4. Siūloma sistema turi turėti gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę; 5.5. Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles pasinaudojant nustatymo vedliu; 5.6. Saugumo sistema turi galėti registruoti veiksmus su kontroliuojamomis rinkmenomis; 5.7. Saugumo sistema turi galėti leisti nustatyti teisę vartotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami; 5.8. Saugumo sistema turi galėti atlikti minimaliai duomenų kontrolę per šiuos komunikacijos kanalus: Siunčiant duomenis kaip priedėlį per el. pašto klientą; Siunčiant/įkeliant duomenis per internetinę naršyklę; Siunčiant duomenis per greitųjų žinučių apsikeitimo	darbo vietos tyčinio ar netyčinio praradimo apsaugai; 5.2. Sistema leidžia nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pav. neleisti su tam tikra žyma dokumento siųsti el. paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa); 5.3. Siūlomos sistemos duomenų kontrolės funkcionalumas valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės; 5.4. Siūloma sistema turi gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę; 5.5. Siūloma sistema leidžia pačiai organizacijai nustatyti turinį kontrolei ir taisykles pasinaudojant nustatymo vedliu; 5.6. Saugumo sistema registruoja veiksmus su kontroliuojamomis rinkmenomis; 5.7. Saugumo sistema leidžia nustatyti teisę vartotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai registruojami; 5.8. Saugumo sistema atlieka duomenų kontrolę per šiuos komunikacijos kanalus: Siunčiant duomenis kaip priedėlį per el. pašto klientą; Siunčiant/įkeliant duomenis per internetinę naršyklę; Siunčiant duomenis per greitųjų žinučių apsikeitimo programas;

		programas; 5.9. Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė; 5.10. Duomenų kontrolės modulis turi sąveikauti su programų kontrolės ir įrenginių kontrolės moduliais, leidžiant sukurti minėtų modulių išimtis atsižvelgiant į duomenų kontrolės poreikį.	5.9 Siūloma sistema turi jau paruoštus šablonus, pagal kuriuos atliekama duomenų nutekėjimo kontrolė; 5.10. Duomenų kontrolės modulis sąveikauja su programų kontrolės ir įrenginių kontrolės moduliais, leidžiant sukurti minėtų modulių išimtis atsižvelgiant į duomenų kontrolės poreikį.
6.	**Reikalavimai kompiuterinei darbo vietai skirtos ugniasienės funkcionalumui**	6.1. Siūlomos sistemos klientinė ugniasienė turi būti valdoma centralizuotai iš saugumo sistemos centralizuoto valdymo konsolės; 6.2. Sistemos ugniasienės nustatymai turėtų būti atliekami naudojant nustatymų vedlį centralizuotai arba lokaliai; 6.3. Sistemos ugniasienės nustatymo metu turi būti galima naudoti mokymosi režimus (aktyviai valdyti aplikacijas ir prievadus arba tik stebėti ir rinkti statistiką); 6.4. Sistemos ugniasienė turi galėti taikyti skirtingas saugumo nustatymo politikas kompiuteriui esant organizacijos tinkle ir kompiuteriui už organizacijos tinklo perimetro. Minimaliai identifikuoti ar kompiuteris yra organizacijos tinkle ar už jo pagal šiuos parametrus: Nustatymas pagal DNS; Nustatymas pagal prieigos vartų MAC adresą. 6.5. Ugniasienėje turi būti numatyta galimybė naudoti išsamų paketų inspektavimą; 6.6. Sistemos ugniasienės funkcionalumo dalis turi siųsti ataskaitas į centrinę sistemos valdymo konsolę.	6.1. Siūlomos sistemos klientinė ugniasienė valdoma centralizuotai iš saugumo sistemos centralizuoto valdymo konsolės; 6.2. Sistemos ugniasienės nustatymai atliekami naudojant nustatymų vedlį centralizuotai arba lokaliai; 6.3. Sistemos ugniasienės nustatymo metu galima naudoti mokymosi režimus (aktyviai valdyti aplikacijas ir prievadus arba tik stebėti ir rinkti statistiką); 6.4. Sistemos ugniasienė taiko skirtingas saugumo nustatymo politikas kompiuteriui esant organizacijos tinkle ir kompiuteriui už organizacijos tinklo perimetro. Identifikuoti ar kompiuteris yra organizacijos tinkle ar už jo pagal šiuos parametrus: Nustatymas pagal DNS; Nustatymas pagal prieigos vartų MAC adresą. 6.5. Ugniasienėje numatyta galimybė naudoti išsamų paketų inspektavimą; 6.6. Sistemos ugniasienės funkcionalumo dalis siunčia ataskaitas į centrinę sistemos valdymo konsolę.
7.	**Reikalavimai pataisų valdymo**	7.1. Siūloma sistema turi turėti integruotą pataisų valdymo	7.1. Siūloma sistema turi integruotą pataisų valdymo

	funkcionalumui	funkciją, kuri leistų identifikuoti trūkstamas pataisas pagal pavojingumo prioritetą centrinėje sistemos valdymo konsolėje, nurodant kokie pažeidžiamumai susiję su pataisa ir pateikiant tiesioginę nuorodą į pažeidžiamumo aprašą tinklapyje cve.mitre.org; 7.2. Siūlomas sprendimas turi ieškoti pataisų minimaliai šių gamintojų programinėje įrangoje ir operacinėse sistemose: Adobe, Apple, Sun Java, Firefox, Microsoft, QuickTime, RealPlayer; 7.3. Siūlomas sprendimas turi galėti identifikuoti kompiuterius, kuriuose nebuvo įdiegtos pataisos; 7.4. Siūlomas sprendimas turi galėti pateikti pažeidžiamumų audito išvadą apie kompiuterį; 7.5. Siūlomos sistemos pataisų valdymo funkcionalumas turi būti valdomas iš tos pačios vartotojo sąsajos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.	funkciją, kuri leistų identifikuoti trūkstamas pataisas pagal pavojingumo prioritetą centrinėje sistemos valdymo konsolėje, nurodant kokie pažeidžiamumai susiję su pataisa ir pateikiant tiesioginę nuorodą į pažeidžiamumo aprašą tinklapyje cve.mitre.org; 7.2. Siūlomas sprendimas turi ieškoti pataisų minimaliai šių gamintojų programinėje įrangoje ir operacinėse sistemose: Adobe, Apple, Sun Java, Firefox, Microsoft, QuickTime, RealPlayer; 7.3. Siūlomas sprendimas identifikuoja kompiuterius, kuriuose nebuvo įdiegtos pataisos; 7.4. Siūlomas sprendimas pateikia pažeidžiamumų audito išvadą apie kompiuterį; 7.5. Siūlomos sistemos pataisų valdymo funkcionalumas valdomas iš tos pačios vartotojo sąsajos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.
8.	**Reikalavimai tinklalapių filtravimo funkcionalumui**	8.1. Siūloma sistema turi turėti galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas; 8.2. Turi būti ne mažiau nei 12 kategorijų ir filtravimo politika turi būti nustatoma sistemos centrinėje valdymo konsolėje pagal kompiuterių vartotojų grupes; 8.3. Turi būti numatyta galimybė įtraukti organizacijos numatytas internetines svetaines ar IP adresus, t.y. susikurti savo filtravimo kategorijas; 8.4. Sistema turi galėti siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę;	8.1. Siūloma sistema turi galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas; 8.2. Yra 14 kategorijų ir filtravimo politika nustatoma sistemos centrinėje valdymo konsolėje pagal kompiuterių vartotojų grupes; 8.3. Yra numatyta galimybė įtraukti organizacijos numatytas internetines svetaines ar IP adresus, t.y. susikurti savo filtravimo kategorijas; 8.4. Sistema siunčia informaciją apie blokuotas svetaines į centrinio valdymo konsolę;

		8.5. Siūloma sistema turi realiu laiku blokuoti prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas; 8.6. Siūloma sistema turi turėti galimybę apskaičiuoti atsisiunčiamos iš interneto rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoti arba nerekomenduoti atsisiųsti šią rinkmeną. Reputacija turi būti apskaičiuojama bent pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.	8.5. Siūloma sistema realiu laiku blokuoja prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas; 8.6. Siūloma sistema turi galimybę apskaičiuoti atsisiunčiamos iš interneto rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoti arba nerekomenduoti atsisiųsti šią rinkmeną. Reputacija apskaičiuojama pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.
9.	**Reikalavimai tinklo talpyklų apsaugai**	9.1. Siūlomas sprendimas turi turėti funkcionalumą skirtą tinklo talpyklų apsaugai nuo kenkėjiškos programinės įrangos minimaliai šioms talpyklų sistemoms: **NetApp;** EMC; Sun.	9.1. Siūlomas sprendimas turi funkcionalumą skirtą tinklo talpyklų apsaugai nuo kenkėjiškos programinės įrangos minimaliai šioms talpyklų sistemoms: **NetApp;** EMC; Sun.
10.	**Reikalavimai apsaugos nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention) ir apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumui (skirta apsaugoti iki 100 įrenginių)**	10.1. Apsauga nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention); 10.2. Sistema turi aptikti kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoti; 10.3. Siūlomas sprendimas turi apsaugoti nuo šio tipo programinės įrangos klaidos išnaudojimo atakų: DEP; ASLR; Null Dereference Protection; Heap Spray Allocation; Dynamic Heap Spray; Stack Pivot; Stack Exec; Reflective DLL Injection; WoW64; Hollow Process;	10.1. Apsauga nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention); 10.2. Sistema aptinka kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoti; 10.3. Siūlomas sprendimas turi apsaugoti nuo šio tipo programinės įrangos klaidos išnaudojimo atakų: DEP; ASLR; Null Dereference Protection; Heap Spray Allocation; Dynamic Heap Spray; Stack Pivot; Stack Exec; Reflective DLL Injection; WoW64; Hollow Process;

		DLL Hijacking; Squiblydoo AppLocker Bypass; 10.4. Siūloma sistema aptikusi programinės įrangos klaidos išnaudojimo žalingą kodą turi jį automatiškai pašalinti; 10.5. Siūlomas sprendimas turi blokuoti žalingo kodo virusus be virusų aprašų duomenų bazių (angl. signatureless exploit prevention); 10.6. Siūlomas sprendimas turi apsaugoti nuo failus užkoduojančių virusų (angl. ransomware prevention).	DLL Hijacking; Squiblydoo AppLocker Bypass; 10.4. Siūloma sistema aptikusi programinės įrangos klaidos išnaudojimo žalingą kodą jį automatiškai pašalina; 10.5. Siūlomas sprendimas blokuoja žalingo kodo virusus be virusų aprašų duomenų bazių (angl. signatureless exploit prevention); 10.6. Siūlomas sprendimas apsaugo nuo failus užkoduojančių virusų (angl. ransomware prevention).
11.	**Reikalavimai analizės įrankiui (skirta apsaugoti 100 vnt. įrenginių)**	11.1. Siūlomas sprendimas turi turėti atakos analizės įrankį; 11.2. Turi būti galimybė generuoti ir pateikti ataskaitas apie sustabdytas programinės įrangos klaidos išnaudojimo arba failus užkoduojančių virusų atakas.	11.1. Siūlomas sprendimas turi atakos analizės įrankį; 11.2. Yra galimybė generuoti ir pateikti ataskaitas apie sustabdytas programinės įrangos klaidos išnaudojimo arba failus užkoduojančių virusų atakas.
12	**Kiti reikalavimai**	12.1. Pateikiamos licencijos ir jų palaikymas turi apimti visą šioje specifikacijoje aprašytą funkcionalumą, nė vienas reikalavimas negali būti dengiamas papildomai įsigyjamomis licencijomis ar aptarnavimo (palaikymo) mokesčiais.	12.1. Pateikiamos licencijos ir jų palaikymas apima visą šioje specifikacijoje aprašytą funkcionalumą, nė vienas reikalavimas negali būti dengiamas papildomai įsigyjamomis licencijomis ar aptarnavimo (palaikymo) mokesčiais.
13	**Palaikymas**	13.1. Turi būti užtikrintas siūlomos saugumo programinės įrangos atnaujinimas, virusų aprašų ir kitų duomenų bazių atnaujinimas 36 mėnesius; 13.2. Turi būti teikiama programinės įrangos gamintojo techninio palaikymo paslauga 24 valandas per parą, septynias dienas per savaitę 36 mėnesių laikotarpiui.	13.1. Užtikrintas siūlomos saugumo programinės įrangos atnaujinimas, virusų aprašų ir kitų duomenų bazių atnaujinimas 36 mėnesius; 13.2. Teikiama programinės įrangos gamintojo techninio palaikymo paslauga 24 valandas per parą, septynias dienas per savaitę 36 mėnesių laikotarpiui.

PIRKĖJAS
Muitinės departamentas prie Lietuvos Respublikos finansų ministerijos

Generalinis direktorius

Arūnas Adomėnas

PARDAVĖJAS
Uždaroji akcinė bendrovė „Fortevento“

Direktorius A. V.

Aurelijus Šaltenis

2017 m. liepos 4 d.
Sutarties Nr. 11B-99
2 priedas

KAINOS IR KIEKIAI

Eil. Nr.	Prekės pavadinimas		Mato vnt.	Kiekis	Vieneto, Eur, be PVM	kaina, Eur, be PVM
1	*2*		*3*	*4*	*5*	*6=5x4*
1.	Kompiuterinių darbo vietų ir tarnybinių stočių apsaugos ir kontrolės programinė įranga *Sophos Endpoint Protection Advanced*, iš jų:		Darbo vieta	2 000		
	1.1.	Kompiuterinių darbo vietų ir tarnybinių stočių apsaugos ir kontrolės programinė įranga be teisės naudotis atakos analizės įrankiu	Darbo vieta	1 900	21,60	41 040,00
	1.2.	Kompiuterinių darbo vietų ir tarnybinių stočių apsaugos ir kontrolės programinė įranga su teise naudotis atakos analizės įrankiu	Darbo vieta	100	41,60	4 160,00
					Bendra kaina, Eur, be PVM:	45 200,00
					PVM suma, Eur:	9 492,00
					IŠ VISO, Eur, su PVM :	54 692,00

PIRKĖJAS
Muitinės departamentas prie Lietuvos Respublikos finansų ministerijos

Generalinis direktorius

A. V.

Arūnas Adomėnas

PARDAVĖJAS
Uždaroji akcinė bendrovė „Fortevento“

Direktorius

A. V.

Aurelijus Šaltenis

2017 m. liepos 4 d.
Sutarties Nr. 11B-99
3 priedas

PERDAVIMO-PRIĖMIMO AKTO FORMA

201 m. mėn. d.

Vilnius

_____ (Pardavėjas) perduoda, o Muitinės departamentas prie Lietuvos Respublikos finansų ministerijos (Pirkėjas) priima toliau nurodytas pagal 2017 m. _____ d. sutartį Nr. _____ į Vytenio g. 7, Vilnius pristatytas ir įdiegtas Prekes.

Eil. Nr.	Prekių (paslaugų) pavadinimas, kodas	Vieneto kaina Eur be PVM	Vieneto kaina Eur su PVM	Kiekis	Suma Eur su PVM
1					
	Iš viso:				
	SUMA:				

(suma žodžiais: _____ eurų ___ ct)

_____ _____ _____

(Pardavėjo įgalioto atstovo pareigos) (Parašas) (Vardas, pavardė)

20__ m. _____ d.

_____ _____ _____

(Pirkėjo įgalioto atstovo pareigos) (Parašas) (Vardas, pavardė)

20__ m. _____ ____ d.