TVŪD > PIRKIMO DOKUMENTAI > PASIŪLYMO FORMA

Papildomos antivirusinės programinės įrangos licencijos Nr. IRD-A59-77

Turto valdymo ir ūkio departamentui
prie Lietuvos Respublikos vidaus reikalų ministerijos
Teikiama CVP IS priemonėmis

2022-02-22 Nr. PSL220719EDR1-01
(Data, Nr.)

Vilnius
(Vieta)

1 lentelė. Tiekėjo rekvizitai:

Tiekėjo pavadinimas ir kodas	Blue Bridge MSP, UAB, 301489547
Tiekėjo adresas	J. Jasinskio g. 16A, LT-03163 Vilnius
PVM mokėtojo kodas	LT100003708514
Bankas ir sąskaitos numeris	LT89 2140 0300 0280 5128 Luminor Bank AS
Telefono Nr., internetinis puslapis, el. paštas	+37052526060, www.bluebridge.lt, info@bluebridge.lt
Asmens, pateikusio pasiūlymą CVP IS priemonėmis, vardas, pavardė, pareigos[1]	, pardavimų
Ryšiams su Vykdytoju palaikyti skiriamo asmens vardas, pavardė, pareigos ir kontaktiniai telefonai	A

2 lentelė. Su pasiūlymu pateikiami dokumentai:

Eil. Nr.	Pateikto dokumento pavadinimas	Ar dokumente yra konfidenciali* informacija	Jeigu taip, kokiu pagrindu atitinkamas dokumentas yra konfidencialus?	Lapų skaičius
1.	Ši pasiūlymo forma	Ne	-	24
2.	Įgaliojimas	Ne	-	1
3.	Raštas _Konfidencialu.pdf)	Taip	Komercinė-gamybinė paslaptis	2
4.	Gamintojo raštas	Ne	-	2
5.	Raštas dėl pagalbos tarnybos	Ne	-	1

* Informacija, nurodyta VPĮ 20 straipsnio 2 dalies 1, 2, 3, 4 punktuose negali būti nurodoma ir nebus laikoma konfidencialia. Tiekėjas gali nurodyti, kuri informacijos dalis pasiūlyme yra konfidenciali. Tiekėjo su pasiūlymu teikiamų dokumentų informacijos konfidencialumas gali būti nustatomas tik pagrįstais atvejais. Jeigu kils abejonių dėl tiekėjo pasiūlyme nurodytos informacijos konfidencialumo, Vykdytojas prašys tiekėją per nurodytą terminą, kuris negali

[1] Jeigu pasiūlymą pasirašo ne tiekėjo vadovas, pasiūlyme pateikiama įgaliojimo skaitmeninė kopija.

būti trumpesnis kaip 5 darbo dienos, pagrįsti jos konfidencialumą. Jei tokia informacija pasiūlyme nebus nurodyta, Vykdytojas laikys, kad bet kuri pasiūlyme pateikta informacija nėra konfidenciali, išskyrus informaciją, kurią atskleidus būtų pažeisti Asmens duomenų teisinės apsaugos įstatymo reikalavimai ar Tiekėjo įsipareigojimai pagal su trečiaisiais asmenimis sudarytas sutartis.

3 lentelė. Informacija apie rėmimąsi kitų subjektų pajėgumais. Vykdant pirkimo sutartį bus pasitelkiami šie ūkio subjektai.

Eil. Nr.	Ūkio subjekto (-ų), kvazisubtiekėjo[2], trečiojo asmens[3], kurių pajėgumais remiamasi, pavadinimas (-ai)	Ūkio subjektas pasitelkiamas, siekiant atitikti kvalifikacijos reikalavimą *(Tiekėjas nurodo reikalavimo Nr. pagal SS)*	Pirkimo sutarties dalis, kuriai vykdyti pasitelkiamas ūkio subjektas, EUR arba proc.	Koks pateikiamas įrodymas dėl išteklių prieinamumo[4]
1.	....	....		....
2.	....	....		....

4 lentelė. Reikalavimai susiję su nacionaliniu saugumu.

Šis punktas paliekamas pasiūlymo formoje, jeigu taikomi SS nustatyti VPĮ 47 straipsnio 9 d reikalavimai, susiję su nacionaliniu saugumu:
Jeigu taikomi, tai dėl kiekvieno pasitelkiamo subtiekėjo tiekėjas turi papildomai pateikti atskirą, to (-ų) subtiekėjo (-ų) tinkamai užpildytą ir pasirašytą EBVPD formą). ***Informacija apie subtiekėjus (jeigu žinoma):***

Eil. Nr.	Subtiekėjo (-ų)[5], kurio (-ių) pajėgumais tiekėjas nesiremia, pavadinimas (-ai), kontaktiniai duomenys ir jų atstovai[6]	Nurodoma, kokius sutartinius įsipareigojimus vykdys	Apimtis EUR arba proc.
1.	....	....	....
2.	....	....	....

Techninės specifikacijos reikalavimas	Įrodantys dokumentai
Tiekėjas privalo įrodyti, kad prekės ar paslaugos nekelia grėsmės nacionaliniam saugumui, kad nėra žemiau nurodytų aplinkybių: 1) techninės ar programinės įrangos gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose; 2) techninės ar programinės įrangos priežiūra ar palaikymas būtų vykdomas iš VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.	Iš tiekėjo KARTU SU PASIŪLYMU privalo PATEIKTI šiuos dokumentus: 1) jeigu techninės ar programinės įrangos priežiūrą ir palaikymą vykdantis asmuo arba gamintojas ar jį kontroliuojantis asmuo yra juridinis asmuo, pateikiama juridinio asmens vadovo patvirtinta juridinio asmens steigimo dokumentų kopija, Juridinių asmenų registro išplėstinis išrašas su istorija arba atitinkami valstybės narės ar trečiosios šalies dokumentai; 2) jeigu techninės ar programinės įrangos priežiūrą ir palaikymą vykdantis asmuo arba gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo, pateikiama jo asmens tapatybę patvirtinančio dokumento (tapatybės kortelės ar paso) kopija, leidimo verstis atitinkama ūkine veikla patvirtinančio dokumento (pavyzdžiui, verslo liudijimo, individualios veiklos

[2] Taikoma, jei kvalifikacijai įrodyti tiekėjas pasitelkia kvazisubtiekėjus, kurie pasiūlymo pateikimo metu nėra tiekėjo darbuotojai, tačiau jie bus įdarbinti laimėjimo ir Sutarties sudarymo atveju.
[3] Taikoma, jeigu kvalifikacijai atitikti tiekėjas naudosis Tiekėjo kvalifikacijos reikalavimų nustatymo metodikos 8.3 punkte nurodytų trečiųjų asmenų, kurie tiesiogiai aktyviai, savo veiksmais neprisidės prie pirkimo vykdytojo poreikio įsigyti pirkimo objektą tenkinimo, priemonėmis.
[4] Tiekėjas turi pateikti įrodymą (nurodytą BS 7.2 punkte), kuriame nurodoma, kuo ir kokia dalimi bus remiamasi kitų ūkio subjektų pajėgumais ir patvirtinantį, kad tiekėjas jų pajėgumais, priemonėmis galės naudotis visą sutarties vykdymo laikotarpį.
[5] Subtiekėjo pasitelkimas nekeičia tiekėjo atsakomybės dėl numatomos sudaryti Sutarties įvykdymo, todėl bet kokiu atveju tiekėjas pilnai prisiima atsakomybę už subtiekėjų veiklą vykdant sutartį

	pažymėjimo ir pan.) kopija ir pažyma apie deklaruotą gyvenamąją vietą arba atitinkami valstybės narės ar trečiosios šalies dokumentai.
Nurodomi pateikiami dokumentai:	_Konfidencialu.pdf

5 lentelė. Tiekėjo techninis pasiūlymas:

Eil. Nr.	Pavadinimas, parametras	Minimalūs reikalavimai	Prekių pavadinimas ir rodiklių reikšmės (įvardinant tikslius prekių gamintojų ir prekių modelių pavadinimus bei rodiklių reikšmes) apsiribojimas vien įrašais „atitinka“ ir/arba „taip“ negalimas Tiekėjas turi įrašyti tikslų, nedviprasmišką aprašymą ir pateikti patvirtinančių dokumentų skenuotas kopijas ar nuorodas, pagal kuriuos būtų galima objektyviai įvertinti atitiktį reikalavimui)
1.	Antivirusinės programinės įrangos paskirtis	Centralizuotai apsaugoti kompiuterizuotas darbo vietas (KDV) ir serverius nuo visų rūšių virusų, šnipinėjimo ir kenksmingų programų (*spyware*), išorinių įsibrovimų ir programišių atakų. Užtikrinti mobilių KDV valdymą, apsaugoti nuo rinkmenas užkoduojančių žalingos programinės įrangos (angl. *ransomware*). Turi būti valdoma iš „Sophos“ centrinio valdymo konsolės.	Centralizuotai apsaugo kompiuterizuotas darbo vietas (KDV) ir serverius nuo visų rūšių virusų, šnipinėjimo ir kenksmingų programų (*spyware*), išorinių įsibrovimų ir programišių atakų. Užtikrina mobilių KDV valdymą, apsaugo nuo rinkmenas užkoduojančių žalingos programinės įrangos (angl. *ransomware*). Yra valdoma iš „Sophos“ centrinio valdymo konsolės. https://www.sophos.com/en-us/products/endpoint-antivirus/tech-specs

2.	Gamintojas, pavadinimas	Turi būti nurodytas antivirusinės programos pavadinimas ir tiksli nuoroda į gamintojo interneto puslapį, kuriame pateikta visa informacija apie siūlomą prekę.	Sophos InterceptX Advanced https://www.sophos.com/en-us/products/endpoint-antivirus/tech-specs Sophos Central Intercept X Advanced for Server https://www.sophos.com/en-us/products/server-security/tech-specs Sophos Central Mobile Advanced https://www.sophos.com/en-us/products/mobile-control
3.	Antivirusinės programinės įrangos diegimas	Turi būti centrinio valdymo konsolė, užtikrinanti centralizuotą antivirusinės programinės įrangos ir mobilių KDV valdymą, turi būti sukonfigūruota siūlomo gamintojo debesijos aplinkoje. Programinės įrangos konfigūravimą turi užtikrinti specialistas, kurio kvalifikacija turi būti patvirtinta siūlomos programinės įrangos gamintojo išduotu sertifikatu arba lygiaverčiu dokumentu.	Yra centrinio valdymo konsolė, užtikrinanti centralizuotą antivirusinės programinės įrangos ir mobilių KDV valdymą, sukonfigūruota siūlomo gamintojo debesijos aplinkoje. https://www.sophos.com/en-us/products/sophos-central Programinės įrangos konfigūravimą užtikrins specialistas, kurio kvalifikacija yra patvirtinta siūlomos programinės įrangos gamintojo išduotu sertifikatu.
4.	Bendrieji reikalavimai	Turi turėti tokias integruotas funkcijas: • antivirusinę sistemą apsaugai nuo žalingų programų; • kategorijomis paremtą naršymo kontrolę;	Turi tokias integruotas funkcijas: • antivirusinę sistemą apsaugai nuo žalingų programų; • kategorijomis paremtą naršymo kontrolę; • išorinių kompiuterizuotos darbo vietos sąsajų kontrolę; • kompiuterizuotai darbo vietai skirtos ugniasienės valdymą; • aplikacijų kontrolės funkcionalumą; • mobilių įrenginių valdymo funkcionalumą; • apsaugos nuo interneto grėsmių ir filtravimo funkcionalumą;

		• išorinių kompiuterizuotos darbo vietos sąsajų kontrolę; • kompiuterizuotai darbo vietai skirtos ugniasienės valdymą; • aplikacijų kontrolės funkcionalumą; • mobilių įrenginių valdymo funkcionalumą; • apsaugos nuo interneto grėsmių ir filtravimo funkcionalumą; • apsaugą nuo programinės įrangos klaidos išnaudojimo (angl. *exploit prevention*); • apsaugą nuo failus užkoduojančių virusų (angl. *ransomware prevention*; • duomenų nutekėjimo prevencijos kompiuterizuotoje darbo vietoje funkcionalumą; • priežasties-pasekmės analizės įrankį (angl. *root cause analysis tool*); • centralizuotą saugumo komponentų valdymo konsolę, veikiančią debesijos pagrindu. Nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai,	• apsaugą nuo programinės įrangos klaidos išnaudojimo (angl. *exploit prevention*); • apsaugą nuo failus užkoduojančių virusų (angl. *ransomware prevention*; • duomenų nutekėjimo prevencijos kompiuterizuotoje darbo vietoje funkcionalumą; • priežasties-pasekmės analizės įrankį (angl. *root cause analysis tool*); • centralizuotą saugumo komponentų valdymo konsolę, veikiančią debesijos pagrindu. Nurodyto funkcionalumo užtikrinimui bus pateikti keli produktai, turintys vieną bendrą visiems produktams centralizuoto valdymo įrankį. https://www.sophos.com/en-us/products/endpoint-antivirus/tech-specs https://www.sophos.com/en-us/products/mobile-control

		turintys vieną bendrą visiems produktams ar kelis atskirus centralizuoto valdymo įrankius.	
		Centralizuoto valdymo įrankis turi valdyti ne mažiau kaip šiuos siūlomos programinės įrangos komponentus: • antivirusinę sistemą; • naršymo internete kontrolę; • apsaugos nuo rinkmenas užkoduojančių virusų funkcionalumą; • išorinių kompiuterizuotos darbo vietos sąsajų kontrolę; • kompiuterizuotai darbo vietai skirta ugniasienę; • aplikacijų kontrolės funkcionalumą; • apsaugos nuo interneto grėsmių ir filtravimo funkcionalumą; • duomenų nutekėjimo prevencijos kompiuterizuotoje darbo vietoje funkcionalumą.	Centralizuoto valdymo įrankis valdo šiuos siūlomos programinės įrangos komponentus: • antivirusinę sistemą; • naršymo internete kontrolę; • apsaugos nuo rinkmenas užkoduojančių virusų funkcionalumą; • išorinių kompiuterizuotos darbo vietos sąsajų kontrolę; • kompiuterizuotai darbo vietai skirta ugniasienę; • aplikacijų kontrolės funkcionalumą; • apsaugos nuo interneto grėsmių ir filtravimo funkcionalumą; • duomenų nutekėjimo prevencijos kompiuterizuotoje darbo vietoje funkcionalumą. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/index.html

		Turi palaikyti virtualias KDV ir tarnybines stotis šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): • *VMware vSphere / ESX;* • *VMware Workstation;* • *VMware View;* • *Citrix XenServer;* • *Citrix XenApp;* • *Microsoft Hyper-V Server.*	Palaiko virtualias KDV ir tarnybines stotis šiose platformose (nereikalauja atskiros licencijos virtualios infrastruktūros apsaugai): • *VMware vSphere / ESX;* • *VMware Workstation;* • *VMware View;* • *Citrix XenServer;* • *Citrix XenApp;* *Microsoft Hyper-V Server.* https://support.sophos.com/support/s/article/KB-000034062?language=en_US
		KDV skirtas sprendimas turi apsaugoti ne mažiau kaip 2000 naudotojų. Naudotojui skirta licencija turi apsaugoti daugiau nei vieną kompiuterinį įrenginį t. y. programinė įranga turi būti licencijuojama ne per įrenginį ir viena licencija turėtų tikti apsaugai kelių įrenginių. Programinė įranga turi būti licencijuojama ne per įrenginį ir viena licencija turėtų tikti apsaugai iki 5 vieno naudotojo įrenginių. Pateikiamos licencijos turi apimti visą šioje specifikacijoje aprašytą funkcionalumą.	KDV skirtas sprendimas apsaugos 2300 naudotojų. Naudotojui skirta licencija apsaugos 5 kompiuterinius įrenginius t. y. programinė įranga yra licencijuojama ne per įrenginį ir viena licencija apsaugo kelis įrenginius. Programinė įranga yra licencijuojama ne per įrenginį ir viena licencija tinka apsaugai iki 5 vieno naudotojo įrenginių. Pateikiamos licencijos apima visą šioje specifikacijoje aprašytą funkcionalumą. https://www.sophos.com/en-us/legal/license-entitlement-and-usage-policy
5.	Antivirusinės programos funkcionalumas	Turi užtikrinti apsaugą nuo virusų, *spyware, adware, ransomware* tipo žalingų programų, *rootkits*, potencialiai nepageidaujamų	Užtikrina apsaugą nuo virusų, spyware, adware, ransomware tipo žalingų programų, rootkits, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų.

		aplikacijų, „kirminų“ ir kitų žalingo tipo programų.	https://assets.sophos.com/X24WTUEQ/at/58skspfsh94vjm6nfr78fc3z/sophos-intercept-x-license-guide.pdf
		Sistema turi naudoti genotipo technologiją, kuri gebėtų proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms.	Sistema naudoja genotipo technologiją, kuri geba proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#set-up-threat-protection
		Turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek skaitant, įrašant ar pervadinant failą, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys.	Atlieka žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek skaitant, įrašant ar pervadinant failą, tiek po rinkmenos paleidimo yra analizuojamas jos elgesys. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#deep-learning
		Sistema turi gebėti sustabdyti ne mažiau kaip 20 exploit technikų įskaitant: • APC naudojimo (*Application Procedure Calls*); • Privilegijų eskalavimo ataka (*privilege escalation*).	Sistema geba sustabdyti 20 exploit technikų įskaitant: • APC naudojimo (*Application Procedure Calls*); • Privilegijų eskalavimo ataka (*privilege escalation*). https://assets.sophos.com/X24WTUEQ/at/cpbtrb4w4mfxqf4bn5cx8fh/sophos-comprehensive-exploit-prevention-wp.pdf
		Sistema turi gebėti sustabdyti šifravimo atakas: • Failų kodavimo apsauga (*ransomware*); • Master Boot Record kodavimo apsauga.	Sistema geba sustabdyti šifravimo atakas: • Failų kodavimo apsauga (*ransomware*); • Master Boot Record kodavimo apsauga.

			https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#runtime-protection
		Sistema turi gebėti išanalizuoti paleidžiamojo failo parametrus bei naudojamas funkcijas naudojant neuro-tinklus ir pagal juos prognozuoti kiek labai tas failas pavojingas, taip pat turi gebėti palyginti failą su jau žinomais pavojingais ar žinomais gerais failais. Tuomet pagal visą surinktą informaciją nuspręsti ar vykdyti failą.	Sistema geba išanalizuoti paleidžiamojo failo parametrus bei naudojamas funkcijas naudojant neuro-tinklus ir pagal juos prognozuoti kiek labai tas failas pavojingas, taip pat geba palyginti failą su jau žinomais pavojingais ar žinomais gerais failais. Tuomet pagal visą surinktą informaciją nuspręsti ar vykdyti failą. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#deep-learning
		Turi aptikti kenkėjišką internetinį srautą (angl. *malicious traffic*) į komandų ir kontrolės centrus (angl. *command and control center*) ir jį blokuoti.	Aptinka kenkėjišką internetinį srautą (angl. *malicious traffic*) į komandų ir kontrolės centrus (angl. *command and control center*) ir jį blokuoja. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#runtime-protection
		Turi tikrinti kenkėjišką kodą paleidžiamuosiuose failuose, taip pat dokumentuose turinčiuose aktyvių elementų, tokių kaip makros komandos ir skriptai.	Tikrina kenkėjišką kodą paleidžiamuosiuose failuose, taip pat dokumentuose turinčiuose aktyvių elementų, tokių kaip makros komandos ir skriptai. https://support.sophos.com/support/s/article/KB-000038919?language=en_US
		Turi aptikti kenkėjišką kompiuterio programų elgesį	Aptinka kenkėjišką kompiuterio programų elgesį naudojant sisteminių atakų prevencijos sistemą (angl. *HIPS*).

		naudojant sisteminių atakų prevencijos sistemą (angl. *HIPS*).	https://www.sophos.com/en-us/products/endpoint-antivirus/tech-specs
		Turi atsinaujinti ne mažiau kaip du kartus per dieną.	Atsinaujina 2 kartus per dieną. https://support.sophos.com/support/s/article/KB-000037031?language=en_US
		Turi užtikrinti skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu.	Užtikrina skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#real-time-scanning-local-files-and-network-shares
		Turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus ir turi būti galimybė skirti nurodyta kompiuterio resursų kiekį šiam skenavimui.	Leidžia nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus ir yra galimybė skirti nurodytą kompiuterio resursų kiekį šiam skenavimui. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#scheduled-scanning
		Turi galėti automatiškai atlikti išvalymą nuo aptiktų žalingų programų.	Gali automatiškai atlikti išvalymą nuo aptiktų žalingų programų. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#remediation
		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.	Apsaugo internetines naršykles (*Internet Explorer, Edge, Firefox, Chrome, Safari, Opera*), blokuojant prieigą prie žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/esg/Endpoint-Security-and-Control/concepts/About_Sophos_Web_Protection.html

		Turi leisti numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui.	Leidžia numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#scanning-exclusions
		Turi galėti skenuoti ne mažiau kaip šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS cab, rar, tar.	Gali skenuoti šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS cab, rar, tar. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/esg/Endpoint-Security-and-Control/tasks/Configure_right-click_scanning.html
		Turi gebėti atpažinti failo tipą, t. y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį.	Geba atpažinti failo tipą, t. y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/esg/Endpoint-Security-and-Control/tasks/Specify_on-demand_scanning_file_types.html?hl=file%2Ctypes
		Turi užtikrinti saugumą nešiojamiems ir staliniams kompiuteriams, tarnybinėms stotims, mobiliems įrenginiams.	Užtikrina saugumą nešiojamiems ir staliniams kompiuteriams, tarnybinėms stotims, mobiliems įrenginiams. https://www.sophos.com/en-us/products/endpoint-antivirus
		Turi galėti aptikti polimorfines virusų atmainas.	Gali aptikti polimorfines virusų atmainas. https://ai.sophos.com/projects/behavioral-detection/ https://www.sophos.com/en-us/products/endpoint-antivirus/tech-specs
		Turi galėti blokuoti įtartinas rinkmenas mažiausiai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju	Gali blokuoti įtartinas rinkmenas mažiausiai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).

		plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).	https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/esg/Endpoint-Security-and-Control/concepts/welcome.html?hl=file%2Ctype
		Turi galėti atlikti *JavaScript* emuliaciją ir elgesio analizę, siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo.	Gali atlikti *JavaScript* emuliaciją ir elgesio analizę, siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo. https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophosnotallmalwaredetectioniscreatedequalwpna.pdf
		Turi užtikrinti „keliaujančių“ kompiuterių saugų darbą internete, t. y. kai kompiuteris yra ne organizacijos tinkle. Turi gebėti patikrinti interneto svetainės turinį, prieš jį pateikiant naudotojo internetinei naršyklei, pagal tokius parametrus: • Įvertinti, ar lankoma svetainė nepatenka į infekuotų ir pavojingų tinklalapių sąrašą; • Taikyti svetainių filtravimą pagal kategorijas.	Užtikrina „keliaujančių“ kompiuterių saugų darbą internete, t. y. kai kompiuteris yra ne organizacijos tinkle. Geba patikrinti interneto svetainės turinį, prieš jį pateikiant naudotojo internetinei naršyklei, pagal tokius parametrus: • Įvertinti, ar lankoma svetainė nepatenka į infekuotų ir pavojingų tinklalapių sąrašą; • Taikyti svetainių filtravimą pagal kategorijas. https://assets.sophos.com/X24WTUEQ/at/58skspfsh94vjm6nfr78fc3z/sophos-intercept-x-license-guide.pdf
		Turi būti negalima išjungti sistemos nustatymų eiliniam naudotojui, įskaitant naudotojus, turinčius lokalaus administratoriaus teises kompiuteryje.	Negalima išjungti sistemos nustatymų eiliniam naudotojui, įskaitant naudotojus, turinčius lokalaus administratoriaus teises kompiuteryje. https://support.sophos.com/support/s/article/KB-000036377?language=en_US

		Turi palaikyti ir apsaugoti 32/64 bit *Windows, bei 64 bit macOS* operacines sistemas.	Palaiko ir apsaugo 32/64 bit *Windows, bei 64 bit macOS* operacines sistemas. https://support.sophos.com/support/s/article/KB-000035144?language=en_US https://support.sophos.com/support/s/article/KB-000034670?language=en_US
		Turi turėti integruotą karantino paskyrą. Administratorius turi galėti leisti prieigą pasirinktiems naudotojams prie jų karantino paskyros, kur naudotojai minimaliai galėtų atlikti šiuos veiksmus: • Išvalyti užkrėstą rinkmeną; • Perkelti užkrėstą rinkmeną; • Ištrinti užkrėstą rinkmeną.	Turi integruotą karantino paskyrą. Administratorius gali leisti prieigą pasirinktiems naudotojams prie jų karantino paskyros, kur naudotojai minimaliai galėtų atlikti šiuos veiksmus: • Išvalyti užkrėstą rinkmeną; • Perkelti užkrėstą rinkmeną; • Ištrinti užkrėstą rinkmeną. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/esg/Endpoint-Security-and-Control/concepts/What_is_Quarantine_manager.html
		Siūlomas produktas informacinių technologijų tyrimo įstaigos *Gartner* (http://www.gartner.com) 2021 metų duomenimis turi būti tarp lyderiaujančių produktų (*Leaders* kategorijoje) darbo vietų apsaugos platformų grupėje (*Magic Quadrant for Endpoint Protection* *Platforms*).	Siūlomas produktas informacinių technologijų tyrimo įstaigos *Gartner* (http://www.gartner.com) 2021 metų duomenimis yra tarp lyderiaujančių produktų (*Leaders* kategorijoje) darbo vietų apsaugos platformų grupėje (*Magic Quadrant for Endpoint Protection* https://www.sophos.com/en-us/report/magic-quadrant-endpoint-protection-platforms
6.	Apsaugos nuo failus užkoduojančių virusų (angl. *ransomware prevention*) funkcionalumas	Siūlomas sprendimas turi turėti funkcionalumą skirtą apsaugai nuo failus užkoduojančių virusų ir turi būti valdomas iš centralizuotos valdymo konsolės.	Siūlomas sprendimas turi funkcionalumą skirtą apsaugai nuo failus užkoduojančių virusų ir yra valdomas iš centralizuotos valdymo konsolės. Palaikoma – Funkcija Vadinasi „Cryptoguard“

			https://assets.sophos.com/X24WTUEQ/at/58skspfsh94vjm6nfr78fc3z/sophos-intercept-x-license-guide.pdf
		Turi blokuoti failus užkoduojančius virusus be virusų aprašų duomenų bazių (angl. *signatureless prevention*);	Blokuoja failus užkoduojančius virusus be virusų aprašų duomenų bazių (angl. *signatureless prevention*); https://assets.sophos.com/X24WTUEQ/at/58skspfsh94vjm6nfr78fc3z/sophos-intercept-x-license-guide.pdf
		Turi stebėti visus vykstančius šifravimo procesus ir blokuoti tik tuos šifravimo procesus, kurie yra inicijuoti failus užkoduojančių virusų, t.y. iš neautorizuotų procesų.	Stebi visus vykstančius šifravimo procesus ir blokuoja tik tuos šifravimo procesus, kurie yra inicijuoti failus užkoduojančių virusų, t.y. iš neautorizuotų procesų. Esant false-positive aptikimui, yra galimybė sukurti išimtį reikiamam procesui. https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/EndpointProtection/ThreatProtectionPolicy/index.html#ransomware-protection-exclusions
		Jeigu sprendimas aptinka žalingą šifravimo procesą leisdamas užšifruoti tam tikrą kiekį failų, sprendimas prieš tai turi sukurti tų failų kopijas ir patalpinti laikiname podėlyje. Jeigu neautorizuotas procesas buvo užblokuotas, užšifruoti failai turi būti automatiškai atkuriami.	Jeigu sprendimas aptinka žalingą šifravimo procesą leisdamas užšifruoti tam tikrą kiekį failų, sprendimas prieš tai sukuria tų failų kopijas ir patalpina laikiname podėlyje. Jeigu neautorizuotas procesas buvo užblokuotas, užšifruoti failai gali būti automatiškai atkuriami. https://support.sophos.com/support/s/article/KB-000036287?language=en_US
7.	Sistemos centralizuotas valdymas, administravimas ir konfigūravimas	Siūlomo sprendimo centralizuoto valdymo konsolė turi valdyti apsaugos sistemas šiose platformose: *Windows ir Mac.*	Siūlomo sprendimo centralizuoto valdymo konsolė valdo apsaugos sistemas šiose platformose: *Windows ir Mac.* https://support.sophos.com/support/s/article/KB-000035144?language=en_US https://support.sophos.com/support/s/article/KB-000034670?language=en_US

		Siūlomo sprendimo atnaujinimas KDV turi vykti tiesiai iš gamintojo atnaujinimo serverio internetu, o taip pat turi būti galimybė automatiškai parsisiųsti atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.	Siūlomo sprendimo atnaujinimas KDV gali vykti tiesiai iš gamintojo atnaujinimo serverio internetu, o taip pat yra galimybė automatiškai parsisiųsti atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete. https://support.sophos.com/support/s/article/KB-000035498?language=en_US
		Turi būti galimybė numatyti pirminį ir antrinį atnaujinimo serverius. Jei KDV yra lokaliame tinkle, tai KDV siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris). Jei ta pati KDV naudojama už organizacijos tinklo perimetro ribų, tai atnaujinimus turi galėti parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris).	Yra galimybė numatyti pirminį ir antrinį atnaujinimo serverius. Jei KDV yra lokaliame tinkle, tai KDV siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris). Jei ta pati KDV naudojama už organizacijos tinklo perimetro ribų, tai atnaujinimus gali parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris). https://support.sophos.com/support/s/article/KB-000035498?language=en_US
		Siūlomas sprendimas turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus, sistema išsiųstų el. paštu įspėjimą.	Siūlomas sprendimas leidžia nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus, sistema išsiųstų el. paštu įspėjimą. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/Overview/GlobalSettings/AlertEmailSettings/index.html
		Siūlomas sprendimas turi leisti grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje	Siūlomas sprendimas leidžia grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus: • *Active Directory Organization Unit*; • OS tipą/versiją;

		minimaliai pagal šiuos parametrus: • *Active Directory Organization Unit*; • OS tipą/versiją; • Pagal IP adresą; • Pagal atnaujinimo būklę; • Pagal kompiuterio būklę.	• Pagal IP adresą; • Pagal atnaujinimo būklę; • Pagal kompiuterio būklę https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/Devices/Computers/index.html
		Turi būti 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; • Priverstinai pritaikyti nustatytąją saugumo politiką; • Perkelti pasirinktus kompiuterius į kitą grupę (taisyklės turi būti taikomos automatiškai pagal naują grupę); • Ištrinti kompiuterį iš sąrašo.	Yra 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; • Priverstinai pritaikyti nustatytąją saugumo politiką; • Perkelti pasirinktus kompiuterius į kitą grupę (taisyklės turi būti taikomos automatiškai pagal naują grupę); • Ištrinti kompiuterį iš sąrašo. https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/Devices/Computers/DeviceDetailsComputers/index.html

		Siūlomo sprendimo centralizuoto valdymo konsolė turi integruotis su Microsoft Active Directory ir veiksmai atliekami direktorijoje turi būti sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole. Pašalinus naudotoją ar grupę iš Active Directory, tie patys įrašai automatiškai turi būti pašalinami ir iš saugumo sprendimo centralizuoto valdymo konsolės.	Siūlomo sprendimo centralizuoto valdymo konsolė integruojasi su Microsoft Active Directory ir veiksmai atliekami direktorijoje yra sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole. Pašalinus naudotoją ar grupę iš Active Directory, tie patys įrašai automatiškai bus pašalinami ir iš saugumo sprendimo centralizuoto valdymo konsolės https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/DirectoryService/index.html
		Siūlomas sprendimas turi leisti taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams;	Siūlomas sprendimas leidžia taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/Policies/AboutPolicies/index.html
		Siūlomas sprendimas turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą;	Siūlomas sprendimas leidžia rolėmis su skirtingomis administravimo teisėmis paremtą administravimą. https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/RoleManagement/index.html
		Siūlomas sprendimas turi galėti registruoti administratoriaus veiksmus auditavimo tikslais;	Siūlomas sprendimas registruoja administratoriaus veiksmus auditavimo tikslais. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/Overview/LogsReports/Logs/AuditLogs/index.html
		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	Siūlomas sprendimas turi integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudoja visą informaciją esančią saugumo sistemos duomenų bazėje. Ataskaitos gali būti generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate. Ataskaitas galima automatiškai išsiųsti el.paštu minimaliai šiais formatais: pdf, csv; https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/Overview/LogsReports/Reports/index.html

		rankiniu būdu ir pateikiamos grafiniame formate. Ataskaitas turi būti galima automatiškai išsiųsti el.paštu minimaliai šiais formatais: pdf, csv;	
8.	Išorinių KDV sąsajų ir aplikacijų kontrolė	Siūlomas sprendimas turi leisti nustatyti, kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams.	Siūlomas sprendimas leidžia nustatyti, kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/ConfigureDeviceControl/index.html
		Siūlomas sprendimas turi galėti kontroliuoti ne mažiau kaip šio tipo išorinius įrenginius: • išorinės atminties talpos įrenginius (įrenginiai pajungiami per USB2/3 prievadus); • CD ir DVD įrenginius; • Floppy įrenginius; • Infraraudonąją jungtimi prijungiamus įrenginius; • *Wifi* įrenginius; • *Bluetooth* jungtimi prijungiamus įrenginius.	Siūlomas sprendimas kontroliuoja šio tipo išorinius įrenginius: • išorinės atminties talpos įrenginius (įrenginiai pajungiami per USB2/3 prievadus); • CD ir DVD įrenginius; • Floppy įrenginius; • Infraraudonąją jungtimi prijungiamus įrenginius; • *Wifi* įrenginius; • *Bluetooth* jungtimi prijungiamus įrenginius. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/ConfigureDeviceControl/index.html
		Siūlomas sprendimas turi leisti priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.	Siūlomas sprendimas leidžia priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms. https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/index.html

			https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/Policies/EditPolicies/index.html
		Siūlomas sprendimas turi leisti atlikti 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.	Siūlomas sprendimas leidžia atlikti 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. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/ConfigureDeviceControl/index.html
		Siūlomas sprendimas turi turėti galimybę blokuoti *„bridge“* režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos.	Siūlomas sprendimas turi galimybę blokuoti *„bridge“* režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/ConfigureDeviceControl/index.html
		Siūlomo sprendimo įrenginių kontrolei pasiekti turi būti valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.	Siūlomo sprendimo įrenginių kontrolei pasiekti yra valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/index.html

		Sistema turi leisti kontroliuoti programas (ang. *applications*), 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 t.t.	Sistema leidžia kontroliuoti programas (ang. *applications*), siekiant užtikrinti tinklo resursų išnaudojimą ir saugumą. Sąrašas kontroliuojamų aplikacijų apima bet neapsiriboja, tokiomis aplikacijomis, kaip rinkmenų keitimosi programos (pav. *torrent, p2p*), greitųjų žinučių apsikeitimo programos (pav. *Skype*), žaidimai ir t.t. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/ConfigureAppControl/index.html
		Sistema turi užtikrinti automatinę kontroliuojamų programų naujų versijų atnaujinimo kontrolę, automatinį programų aptikimą ir blokavimą.	Sistema užtikrina automatinę kontroliuojamų programų naujų versijų atnaujinimo kontrolę, automatinį programų aptikimą ir blokavimą. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/ConfigureAppControl/index.html
		Turi būti galimybė aplikacijas skirstyti į kategorijas (ne mažiau kaip 40 kategorijų).	Yra galimybė aplikacijas skirstyti į kategorijas (40 kategorijų). https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/ConfigureAppControl/index.html
		Siūlomas sprendimas turi galėti priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.	Siūlomas sprendimas gali priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/ComputerGroups/index.html

8.1.	Duomenų nutekėjimo prevencijos (angl. *Data loss prevention*) funkcionalumas	Siūloma sistema turi turėti integruotą funkcionalumą duomenų iš kompiuterinės darbo vietos tyčinio ar netyčinio praradimo apsaugai.	Siūloma sistema turi integruotą funkcionalumą duomenų iš kompiuterinės darbo vietos tyčinio ar netyčinio praradimo apsaugai. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html
		Sistema turi leisti nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pav. neleisti dokumento su tam tikra žyma siųsti el. paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa ir pan.)	Sistema leidžia nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pav. neleisti dokumento su tam tikra žyma siųsti el. paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa ir pan.) https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html
		Siūlomos sistemos duomenų kontrolės funkcionalumas turi būti valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.	Siūlomos sistemos duomenų kontrolės funkcionalumas yra valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html
		Siūloma sistema turi turėti gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę.	Siūloma sistema turi gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html

		Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles, pasinaudojant nustatymo vedliu.	Siūloma sistema leidžia pačiai organizacijai nustatyti turinį kontrolei ir taisykles, pasinaudojant nustatymo vedliu. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html
		Siūloma sistema turi registruoti veiksmus su kontroliuojamomis rinkmenomis.	Siūloma sistema registruoja veiksmus su kontroliuojamomis rinkmenomis. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html
		Sistema turi leisti nustatyti teisę naudotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami.	Sistema leidžia nustatyti teisę naudotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai yra registruojami. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html
		Siūloma sistema turi atlikti duomenų kontrolę ne mažiau kaip 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.	Siūloma 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. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html
		Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.	Siūloma sistema turi paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė. https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/EndpointProtection/datalossprevention/index.html

6 lentelė. Tiekėjo finansinis pasiūlymas:

Eil. Nr.	Antivirusinės programinės įrangos licencijų pavadinimas	Minimalus planuojamas licencijų kiekis, vnt.	Maksimalus planuojamas licencijų kiekis, vnt. *	1 licencijos 1 mėnesio kaina, EUR be PVM	1 licencijos 12 mėnesių kaina, EUR be PVM (5x12)	Minimali bendra suma iki 2022-12-31 Eur be PVM (3x5x(pilnų mėnesių skaičiaus iki 2022-12-31))	Maksimali bendra suma iki 2022-12-31 Eur be PVM (4x5x(pilnų mėnesių skaičiaus iki 2022-12-31))	Minimali bendra suma iki 2024-12-31 Eur be PVM (7+(3x6)+(3x6))	Maksimali bendra suma iki 2024-12-31 Eur be PVM (8+(4x6)+(4x6))
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**
1.	Antivirusinės programos „*Sophos Central Intercept X Advanced*“ licencijos kompiuterinei darbo vietai	2000	2300	0,66	7,92	6 600,00	7 590,00	38 280,00	44 022,00
2.	Antivirusinės programos „*Sophos Central Intercept X Advanced*“ licencijos serveriui	91	162	1,65	19,8	750,75	1 336,50	4 354,35	7 751,70
3.	Mobilių įrenginių valdymo programinės įrangos „*Sophos Central Mobile Advanced*“ licencijos	20	70	0,39	4,68	39,00	136,50	226,20	791,70
							Pasiūlymo kaina, Eur be PVM:	**42 860,55**	**52 565,40**
							PVM:	**9 000,72**	**11 038,73**
							Bendra pasiūlymo kaina EUR su PVM:	**51 861,27**	**63 604,13**

*Nurodytas kiekis yra preliminarus, skirtas pasiūlymui apskaičiuoti, taip pat atitinkamų licencijų įkainiams nustatyti. Perkančioji organizacija lentelėje nurodytas licencijas pirks pagal poreikį, pagal tiekėjo pasiūlytus įkainius. Sutarties vertė yra iki 69 000 Eur su PVM. Minimali pirkimui skiriama lėšų suma – 56 000 Eur su PVM. Maksimali pirkimui skiriama lėšų suma – 69,000 Eur su PVM.

**Į kainą turi būti įskaičiuota PVM, kiti mokesčiai bei visos kitos išlaidos. Tiekėjas turi nurodyti kainą EUR su PVM, jei jis yra PVM mokėtojas arba EUR be PVM, jei teikėjas yra ne PVM mokėtojas. Kaina nurodoma ne daugiau kaip 2 skaitmenų po kablelio tikslumu.

Taikomas PVM dydis (%):	*21%*
PVM lengvatos/nemokėjimo teisinis pagrindas (jei taikoma):	*[Pildo tiekėjas]*
Pasiūlymo kaina žodžiais:	*Maksimali bendra pasiūlymo kaina – šešiasdešimt trys tūkstančiai šeši šimtai keturi eurai, 13 centų.* *Minimali bendra pasiūlymo kaina – penkiasdešimt vienas tūkstantis aštuoni šimtai šešiasdešimt vienas euras, 27 centai*

Patvirtiname, kad atidžiai perskaitėme visus sąlygų, techninės specifikacijos reikalavimus ir įsipareigojame jų laikytis vykdydami sutartį jeigu teisės aktų nustatyta tvarka būsime pripažinti laimėtoju. Taip pat įsipareigojame laikytis ir kitų Lietuvos Respublikoje galiojančių pirkimo objektui bei viešojo pirkimo sutarčiai taikomų teisės aktų reikalavimų. Šis pasiūlymas galioja 5 mėnesius nuo pasiūlymų pateikimo termino pabaigos. Pateikdamas CVP IS priemonėmis pateiktą pasiūlymą patvirtinu, kad dokumentų skaitmeninės kopijos ir elektroninėmis priemonėmis pateikti duomenys yra tikri, teisingi ir apima viską, ko reikia tinkamam sutarties įvykdymui.

(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)	(Parašas*[6])	(Vardas, pavardė)

*[6] **Parašas nėra privalomas.**