Kvietimo pateikti pasiūlymą 1 priedas
„Konkretaus pasiūlymo forma“

ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS IR MOBILIŲ ĮRENGINIŲ VALDYMO PROGRAMINĖS ĮRANGOS PALAIKYMO PASLAUGŲ KONKRETUS PIRKIMAS PPR-855

KONKRETUS PASIŪLYMAS

2024-11-19
Vilnius

Išteklių agentūra prie Lietuvos Respublikos vidaus reikalų ministerijos

Teikiama CVP IS priemonėmis

1. INFORMACIJA APIE TIEKĖJĄ

Tiekėjo pavadinimas ir kodas	Blue Bridge MSP, UAB, 301489547
Tiekėjo adresas	J. Jasinskio g. 16A, LT-03163 Vilnius
Bankas ir sąskaitos numeris	AB SEB bankas LT047044060006233634
Telefono Nr., internetinis puslapis, el. paštas	+370 5 252 6060, https://bluebridge.lt, info@bluebridge.lt
Asmens, pateikusio pasiūlymą CVP IS priemonėmis, vardas, pavardė, pareigos[1]	viešųjų pirkimų specialistė

2. INFORMACIJA APIE ŽINOMUS SUBTIEKĖJUS IR JIEMS PERDUODAMĄ VYKDYTI SUTARTIES DALĮ *(pildoma, jei DPS tiekėjas pasitelkia subtiekėjus)*

Eil. Nr.	Subtiekėjo pavadinimas, juridinio asmens kodas, adresas	Sutarties objekto dalies, perduodamos vykdyti subtiekėjui, aprašymas
1.	-	-
2.	-	-
...		

3. INFORMACIJOS ANKSČIAU TEIKTAME (-UOSE) DOKUMENTUOSE PATVIRTINIMAS

Patvirtiname, kad anksčiau pirkimo vykdytojui mūsų teiktame (-uose):

☒ EBVPD *(A dalies. DPS sukūrimas 3 priedas)* nurodyta informacija yra nepasikeitusi;

☒ Nacionalinio saugumo reikalavimų atitikties deklaracijoje *(A dalies. DPS sukūrimas 7 priedas)* nurodyta informacija yra nepasikeitusi;

☒ Tiekėjo deklaracijoje dėl Tarybos Reglamente (ES) 2022/576 nustatytų sąlygų nebuvimo *(A dalies. DPS sukūrimas 8 priedas)* nurodyta informacija yra nepasikeitusi.

☒ Tiekėjo deklaracijoje *(A dalies. DPS sukūrimas 9 priedas)* nurodyta informacija yra nepasikeitusi.

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

☐ Anksčiau pirkimo vykdytojui mūsų teiktame (-uose) *[... DPS tiekėjas nurodo dokumentą (-us), kuriame (-iuose)* informacija yra pasikeitusi, atnaujintą *[dokumento (-ų) pavadinimas]* teikiame kartu su šiuo konkrečiu pasiūlymu *[nepildoma, jeigu nauji dokumentai neteikiami].*

4. PASIŪLYMO TECHNINIAI DUOMENYS.

Eil. Nr.	**Pavadinimas, parametras**	**Minimalūs reikalavimai, parametrai**	**Siūlomi parametrai** *(nurodyti parametrų, rodiklių reikšmes. Pateikti nuorodas į viešai skelbiamą informaciją, patvirtinančių dokumentų kopijas, jeigu reikalaujama. Apsiribojimas vien įrašais „atitinka“ ir/arba „taip“ negalimas. Pildoma teikiant pasiūlymą)*
Bendrieji reikalavimai			
1.	DPS tiekėjas turi būti siūlomos įrangos gamintojas arba būti įgaliotas gamintojo atstovas arba turi būti sudaręs atitinkamą sutartį su kitu ūkio subjektu, turinčiu teisę teikti siūlomos įrangos palaikymo, priežiūros paslaugas.	DPS tiekėjas turi pateikti dokumentą, patvirtinantį, kad DPS tiekėjas yra siūlomos įrangos gamintojas (pateikiama DPS tiekėjo pažyma), ar įgaliotas siūlomos įrangos gamintojo atstovas (pateikiami oficialų atstovavimą patvirtinantys dokumentai), turintis teisę teikti siūlomos įrangos palaikymo, priežiūros paslaugas, arba yra sudaręs atitinkamą bendradarbiavimo sutartį su kitu ūkio subjektu, turinčiu atitinkamas gamintojo suteiktas teises (pateikiama patvirtinančios sutarties su kita įmone, turinčia teisę atstovauti siūlomos įrangos gamintoją, skaitmeninė kopija bei ūkio subjektui, su kuriuo sudaryta bendradarbiavimo sutartis, gamintojo išduotas įgaliojimas).	Pateikiamas dokumentas, patvirtinantis, kad DPS tiekėjas yra siūlomos įrangos gamintojo atstovas "Sophos raštas dėl partnerystės.pdf".
Reikalavimai pirkimo objektui			
Kompiuterizuotų darbo vietų (KDV) apsauga ir kontrolė, preliminarus licencijų naudotojui skaičius – 16405 vnt.			
1.	Antivirusinės programinės įrangos paskirtis	Centralizuotai apsaugoti kompiuterizuotas darbo vietas (KDV), įskaitant mobilias darbo vietas, nuo visų rūšių virusų, šnipinėjimo ir kenksmingų programų (*spyware*), „adware“ ir „ransomware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo	Centralizuotai apsaugo kompiuterizuotas darbo vietas (KDV), įskaitant mobilias darbo vietas, nuo visų rūšių virusų, šnipinėjimo ir kenksmingų programų (spyware), „adware“ ir „ransomware“ tipo žalingų programų, „rootkits“, potencialiai

		programų, išorinių įsibrovimų ir programišių atakų.	nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų, išorinių įsibrovimų ir programišių atakų.
2.	Integruotos saugumo funkcijos	• antivirusinė apsauga nuo žalingų programų; • kategorijomis paremta naršymo kontrolė; • išorinių kompiuterinės darbo vietos sąsajų kontrolė; • kompiuterizuotai darbo vietai skirtas ugniasienės valdymas; • 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); • apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas; • priežasties-pasekmės analizės įrankis (angl. root cause analysis tool); • nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams skirtą centralizuoto valdymo įrankį.	Integruotos saugumo funkcijos: • antivirusinė sistema apsaugai nuo žalingų programų; • kategorijomis paremta naršymo kontrolė; • išorinių kompiuterinės darbo vietos sąsajų kontrolė; • kompiuterinei darbo vietai skirtas ugniasienės valdymas; • 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); • apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas; • priežasties-pasekmės analizės įrankis (angl. root cause analysis tool); • Nurodyto funkcionalumo užtikrinimui yra pateikiami keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams skirtą centralizuoto valdymo įrankį.
3.	Palaikomos operacinės sistemos	Ne mažiau kaip: Windows 10 Pro 32 /64 bit, Windows 11 Pro 32 /64 bit. Gamintojas turi licencijų galiojimo laikotarpiu garantuoti palaikymą ir naujų apsaugos programų versijų pateikimą naujai išleidžiamoms Microsoft operacinėms sistemoms.	Siūlomas sprendimas užtikrina antivirusinę apsaugą darbo vietų Windows (nuo Windows 8) bei Mac (nuo 10.12) operacinių sistemų platformoms. Gamintojas licencijų galiojimo laikotarpiu garantuoja palaikymą ir naujų apsaugos programų versijų

			pateikimą naujai išleidžiamoms Microsoft operacinėms sistemoms.
4.	Virtualių KDV palaikymas	Antivirusinė apsauga turi palaikyti virtualias kompiuterizuotas darbo vietas minimaliai šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): VMware vSphere / ESX; VMware Worktation; VMware View; Microsoft Hyper-V Server.	Antivirusinė apsauga palaiko virtualias kompiuterines darbo vietas/tarnybines stotis minimaliai šiose platformose (be atskiros licencijos virtualios infrastruktūros apsaugai): • VMware vSphere / ESX • VMware Worktation • VMware View • Microsoft Hyper-V Server • Citrix XenServer • Citrix XenApp
5.	Antivirusinės programinės įrangos funkcionalumas	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.	Sistema atlieka žalingų veiksmų stebėseną ir aptinka dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo yra analizuojamas jos elgesys.
		Sistema turi gebėti sustabdyti bent 20 exploit technikų įskaitant: APC naudojimo (Application Procedure Calls); privilegijų eskalavimo ataka (privilege escalation).	Sistema geba sustabdyti bent 20 exploit technikų įskaitant: • APC naudojimo (Application Procedure Calls) • Privilegijų eskalavimo ataka (privilege escalation).
		Sistema turi gebėti sustabdyti šias aktyvių kenkėjų technikas: Prieigos raktų ar slaptažodžių vagystė (credential theft); Kodo urvo naudojimas (code cave).	Sistema geba sustabdyti šias aktyvių kenkėjų technikas: • Prieigos raktų ar slaptažodžių vagystė (credential theft) • Kodo urvo naudojimas (code cave).
		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 prognozuoja kiek labai tas failas pavojingas, taip pat geba palyginti failą su jau žinomais pavojingais ar žinomais gerais failais. Tuomet pagal visą surinktą informaciją nuspręndžia ar vykdyti failą.
		Sistema turi aptikti kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės	Sistema gali aptikti kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės

		centrus (angl. command and control center) ir jį blokuoti.	centrus (angl. command and control center) ir jį blokuoti.
		Sistema turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus.	Sistema leidžia nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus.
		Siūlomas sprendimas turi galėti automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų.	Siūlomas sprendimas gali automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų.
		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.	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.
		Siūloma saugumo sistema turi galėti skenuoti archyvuotas rinkmenas.	Siūloma saugumo sistema gali skenuoti archyvuotas rinkmenas.
		Sistema turi gebėti atpažinti failo tipą, t.y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį.	Sistema geba atpažinti failo tipą, t.y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį.
		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).	Saugumo sistema gali blokuoti įtartinas rinkmenas minimaliai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).
		Siūlomo sprendimo nustatymų turi būti negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises kompiuteryje.	Siūlomo sprendimo nustatymų negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises kompiuteryje.
6.	Reikalavimai sistemos centralizuotam valdymui, administravimui ir konfigūravimui	Siūlomo sprendimo centralizuoto valdymo konsolė turi galėti valdyti apsaugos sistemas Windows bei Mac platformose.	Siūlomo sprendimo centralizuoto valdymo konsolė gali valdyti apsaugos sistemas Windows bei Mac platformose.
		Siūlomo sprendimo kompiuterizuotų darbo vietų atnaujinimas turi galėti vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir turi būti numatyta galimybė kompiuterizuotoms darbo vietoms parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai	Siūlomo sprendimo kompiuterinių darbo vietų atnaujinimas gali vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir yra numatyta galimybė kompiuterinėms darbo vietoms parsisiųsti automatiškai

		atnaujinimus gavo iš gamintojo serverio internete.	atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.
		Turi būti galimybė numatyti pirminį ir antrinį 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.	Siūlomoje sistemoje yra galimybė numatyti pirminį ir antrinį 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 gali parsisiųsti iš gamintojo serverio internetu.
		Siūlomas sprendimas turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus sistema išsiųstų el. paštu įspėjimą.	Siūlomas sprendimas leidžią nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus sistema išsiųstų el. paštu įspėjimą.
		Siūlomo sprendimo centralizuoto valdymo konsolė turi integruotis su Active Directory.	Siūlomo sprendimo centralizuoto valdymo konsolė integruojasi su Active Directory.
		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.
		Siūlomas sprendimas turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą.	Siūlomas sprendimas leidžia rolėmis su skirtingomis administravimo teisėmis paremtą administravimą.
		Siūlomas sprendimas turi galėti registruoti administratoriaus veiksmus auditavimo tikslais.	Siūlomas sprendimas gali registruoti administratoriaus veiksmus auditavimo tikslais.
		Siūlomas sprendimas turi turėti integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją esančią saugumo sistemos duomenų bazėje.	Siūlomas sprendimas turi integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją esančią saugumo sistemos duomenų bazėje.
7.	Reikalavimai išorinių kompiuterio sąsajų ir aplikacijų kontrolės funkcionalumui	Siūlomas sprendimas turi leisti nustatyti, kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams.	Siūlomas sprendimas leidžia nustatyti kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams.
		Siūlomas sprendimas turi galėti kontroliuoti minimaliai šio tipo išorinius įrenginius: išorinės atminties talpos įrenginius; CD ir DVD įrenginius; Floppy įrenginius;	Siūlomas sprendimas gali kontroliuoti minimaliai šio tipo išorinius įrenginius: • išorinės atminties talpos įrenginius;

		Infraraudonąją jungtimi prijungiamus įrenginius; Wifi įrenginius; Bluetooth jungtimi prijungiamas įrenginius.	• CD ir DVD įrenginius; • Floppy įrenginius; • Infraraudonąją jungtimi prijungiamus įrenginius; • Wifi įrenginius; • Bluetooth jungtimi prijungiamas įrenginius.
		Siūlomas sprendimas turi galėti priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms	Siūlomas sprendimas gali priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms
		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; Leisti įrenginiui prisijungti tik „skaitymo“ režime.	Siūlomas sprendimas gali 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 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.
		Sistema turi leisti kontroliuoti programas (ang. application). Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. torrent, p2p), greitųjų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai.	Sistema leidžia kontroliuoti programas (ang. application). Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. torrent, p2p), greitųjų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai.
		Sistema turi užtikrinti automatinį kontroliuojamų programų atnaujintų naujomis versijomis aptikimą ir blokavimą.	Sistema užtikrina automatinį kontroliuojamų programų atnaujintų naujomis versijomis aptikimą ir blokavimą.
8.	Reikalavimai duomenų nutekėjimo prevencijos	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.

	funkcionalumui (angl. Data loss prevention)	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.
		Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles.	Siūloma sistema leidžia pačiai organizacijai nustatyti turinį kontrolei ir taisykles.
		Saugumo sistema turi galėti registruoti veiksmus su kontroliuojamomis rinkmenomis.	Saugumo sistema gali registruoti veiksmus su kontroliuojamomis rinkmenomis.
		Saugumo sistema turi galėti leisti nustatyti teisę vartotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami.	Saugumo sistema gali leisti nustatyti teisę vartotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai yra registruojami.
		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 programas.	Saugumo sistema gali 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 programas.
		Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.	Siūloma sistema turi jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.
9.	Reikalavimai kompiuterio ugniasienės funkcionalumui	Siūloma sistema turi gebėti valdyti Windows firewall ugniasienę. Valdant iš saugumo sistemos centralizuotos valdymo konsolės.	Siūloma sistema geba valdyti Windows firewall ugniasienę. Valdant iš saugumo sistemos centralizuotos valdymo konsolės.
		Sistemos ugniasienės nustatymo metu turi būti galima naudoti mokymosi režimus (tik stebėti ir rinkti statistiką arba kontroliuoti tinklo profilius).	Sistemos ugniasienės nustatymo metu galima naudoti mokymosi režimus (tik stebėti ir rinkti statistiką arba kontroliuoti tinklo profilius).
		Turi gebėti taikyti skirtingas saugumo nustatymo politikas esant organizacijos tinkle ir už organizacijos tinklo perimetro.	Siūloma sistema geba taikyti skirtingas saugumo nustatymo politikas esant organizacijos tinkle ir už organizacijos tinklo perimetro.
		Sistema turi turėti galimybę izoliuoti save nuo aplinkinių įrenginių jei joje aptinkamas kenksmingas kodas ar ataka.	Sistema turi galimybę izoliuoti save nuo aplinkinių įrenginių jei joje

			aptinkamas kenksmingas kodas ar ataka.
10.	Reikalavimai tinklalapių filtravimo funkcionalumui	Siūloma sistema turi turėti galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas.	Siūloma sistema turi galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas.
		Turi būti ne mažiau nei sekančios kategorijos: Socialinių tinklų; Suaugusiųjų bei potencialiai nepriimtinų svetainių; Didelio pralaidumo reikalaujančių svetainių; Produktyvumą įtakojančių svetainių; Su darbu susijusių svetainių. Aukščiau išvardintos kategorijos turėtu būti toliau detalizuojamos į nemažiau kaip 3 subkategorijas kiekvienai kategorijai. Filtravimo politika turi būti nustatoma sistemos centrinėje valdymo konsolėje pagal vartotojų grupes.	Siūlomoje sistemoje yra ne mažiau nei sekančios kategorijos: • Socialinių tinklų • Suaugusiųjų bei potencialiai nepriimtinų svetainių • Didelio pralaidumo reikalaujančių svetainių • Produktyvumą įtakojančių svetainių • Su darbu susijusių svetainių Aukščiau išvardintos kategorijos yra toliau detalizuojamos į nemažiau kaip 3 subkategorijas kiekvienai kategorijai. Filtravimo politika yra nustatoma sistemos centrinėje valdymo konsolėje pagal vartotojų grupes.
		Turi būti numatyta galimybė įtraukti organizacijos numatytas internetines svetaines.	Yra numatyta galimybė įtraukti organizacijos numatytas internetines svetaines.
		Sistema turi galėti siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.	Sistema gali siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.
		Siūloma sistema turi realiu laiku blokuoti prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas.	Siūloma sistema realiu laiku blokuoja prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas.
		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.	Siūloma sistema turi galimybę apskaičiuoti atsisiunčiamos iš interneto rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoja arba nerekomenduoja atsisiųsti šią rinkmeną. Reputacija yra apskaičiuojama bent pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.
Papildomas išplėstinio aptikimo ir atsako (XDR) funkcionalumas, preliminarus licencijų naudotojui skaičius – 16405 vnt.			

1.	Reikalavimai funkcionalumui	Turi būti grėsmių aptikimas realiuoju laiku.	Siūlomoje sistemoje yra grėsmių aptikimas realiuoju laiku.
		Turi būti SQL užklausų formavimo ir vykdymo funkcionalumas siūlomo sprendimo valdymo įrankyje.	Siūlomoje sistemoje yra SQL užklausų formavimo ir vykdymo funkcionalumas siūlomo sprendimo valdymo įrankyje.
		Turi būti redaguojami SQL užklausų šablonai grėsmių aptikimui.	Siūlomoje sistemoje yra redaguojami SQL užklausų šablonai grėsmių aptikimui.
		Turi būti SQL užklausų planavimas ir paleidimas iš anksto numatytu periodiškumu.	Siūlomoje sistemoje yra SQL užklausų planavimas ir paleidimas iš anksto numatytu periodiškumu.
		Turi būti įtartinų įvykių aptikimo ir prioretizavimo funkcionalumas priskiriantis kategoriją pagal MITRE Attack struktūrą, bei priskiriantis kritiškumo lygį įvykiui.	Siūlomoje sistemoje yra įtartinų įvykių aptikimo ir prioretizavimo funkcionalumas priskiriantis kategoriją pagal MITRE Attack struktūrą, bei priskiriantis kritiškumo lygį įvykiui.
		Turi būti prieiga prie saugomo įrenginio duomenų saugyklos diske.	Siūlomoje sistemoje yra prieiga prie saugomo įrenginio duomenų saugyklos diske.
		Turi būti palaikomi kelių to paties gamintojo naudojamų produktų duomenų šaltiniai (pvz. ugniasienė, el. pašto apsauga) kuriuose būtų galima vykdyti SQL užklausas.	Siūlomoje sistemoje yra palaikomi kelių to paties gamintojo naudojamų produktų duomenų šaltiniai (pvz. ugniasienė, el. pašto apsauga) kuriuose būtų galima vykdyti SQL užklausas.
		Turi būti galimybė su papildomomis licencijomis integruoti ir gauti saugumo informaciją iš/su trečiųjų šalių tapatybės valdymo, tinklo grėsmių aptikimo, ugniasienių, e-pašto apsaugos, darbo stočių apsaugos sistemomis bei ne mažiau kaip su šiais viešosios debesijos paslaugų tiekėjais: Trend Micro; Fortigate; Checkpoint; Microsoft; Palo Alto Networks; Veeam; Acronis Cyber Protect.	Siūlomoje sistemoje yra galimybė su papildomomis licencijomis integruoti ir gauti saugumo informaciją iš/su trečiųjų šalių tapatybės valdymo, tinklo grėsmių aptikimo, ugniasienių, e-pašto apsaugos, darbo stočių apsaugos sistemomis bei viešosios debesijos paslaugų tiekėjais: • Trend Micro • Fortigate • Checkpoint • Microsoft • Palo Alto Networks • Darktrace • Okta • Duo • Veeam • Acronis Cyber Protect

		Turi būti debesijos duomenų ežero (angl. data lake) saugykla kurioje kaupiama ir laikoma informacija apie saugomus įrenginius (angl. endpoint) ne mažiau 90 dienų.	Siūlomoje sistemoje yra debesijos duomenų ežero (angl. data lake) saugykla kurioje kaupiama ir laikoma informacija apie saugomus įrenginius (angl. endpoint) ne mažiau 90 dienų.
		Turi būti mašininio mokymosi, pagrįsto dirbtiniais neuroniniais tinklais (ang. Deep Learning), kenkėjiškų programų analizė.	Siūlomoje sistemoje yra mašininio mokymosi, pagrįsto dirbtiniais neuroniniais tinklais (ang. Deep Learning), kenkėjiškų programų analizė.
		Turi būti tyrimams atlikti tinkamų (angl. forensic) duomenų eksportavimo funkcionalumas, su galimybe eksportuoti duomenis į Amazon S3 duomenų saugyklą.	Siūlomoje sistemoje yra tyrimams atlikti tinkamų (angl. forensic) duomenų eksportavimo funkcionalumas, su galimybe eksportuoti duomenis į Amazon S3 duomenų saugyklą.
		Turi būti nuotolinė prieiga iš produkto valdymo aplinkos prie kompiuterio (angl. endpoint) grėsmių tyrimui ir pašalinimui.	Siūlomoje sistemoje yra nuotolinė prieiga iš produkto valdymo aplinkos prie kompiuterio (angl. endpoint) grėsmių tyrimui ir pašalinimui.
		Turi būti funkcionalumas leidžiantis kompiuterio (angl. endpoint) izoliaciją pagal poreikį.	Siūlomoje sistemoje yra funkcionalumas leidžiantis kompiuterio (angl. endpoint) izoliaciją pagal poreikį.
Serverių apsauga ir kontrolė, preliminarus licencijų serveriui skaičius – 100 vnt.			
1.	Bendrieji reikalavimai	Siūlomas apsaugos sprendimas turi turėti integruotas sekančias saugumo funkcijas: antivirusinė sistema apsaugai nuo žalingų programų; kategorijomis paremta naršymo kontrolė; išorinių prievadų kontrolė; serverio ugniasienės valdymas; aplikacijų kontrolės funkcionalumas; apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; duomenų nutekėjimo prevencijos funkcionalumas; centralizuota saugumo komponentų valdymo konsolė; apsaugos nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention); apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas;	Siūlomas apsaugos sprendimas turi integruotas sekančias saugumo funkcijas: • antivirusinė sistema apsaugai nuo žalingų programų; • kategorijomis paremta naršymo kontrolė; • išorinių prievadų kontrolė; • serverio ugniasienės valdymas; • aplikacijų kontrolės funkcionalumas; • apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; • duomenų nutekėjimo prevencijos funkcionalumas; • centralizuota saugumo komponentų valdymo konsolė;

		priežasties-pasekmės analizės įrankis (angl. root cause analysis tool). Nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams skirtą centralizuoto valdymo įrankį.	• apsaugos nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention); • apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas; • priežasties-pasekmės analizės įrankis (angl. root cause analysis tool); Nurodyto funkcionalumo užtikrinimui yra pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams skirtą centralizuoto valdymo įrankį.
2.	Palaikomos operacinės sistemos	Ne mažiau kaip: Windows Server 2008 R2, SBS 2011, 2012. 2012 R2, 2016, 2019 ir 2022 Linux: Amazon Linux, Amazon Linux 2, CentOS 7/8, Debian 9/10, Oracle Linux 7/8, Red Hat Enterprise Linux 7/8, SUSE Linux Enterprise Server 12/15, Ubuntu 18/20 LTS.	Siūlomas sprendimas užtikrina antivirusinę apsaugą Windows Server: 2008 R2, SBS 2011, 2012. 2012 R2, 2016, 2019 ir 2022 Linux: Amazon Linux, Amazon Linux 2, CentOS 7/8, Debian 9/10, Oracle Linux 7/8, Red Hat Enterprise Linux 7/8, SUSE Linux Enterprise Server 12/15, Ubuntu 18/20 LTS.
3.	Virtualių serverių palaikymas	Siūlomas sprendimas turi palaikyti virtualias tarnybines stotis minimaliai šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): VMware vSphere / ESX; VMware Worktation; VMware View; Microsoft Hyper-V Server.	Siūlomo sprendimo antivirusinė apsauga palaiko virtualias kompiuterines darbo vietas/tarnybines stotis minimaliai šiose platformose (be atskiros licencijos virtualios infrastruktūros apsaugai): • VMware vSphere / ESX • VMware Worktation • VMware View • Citrix XenServer • Citrix XenApp • Microsoft Hyper-V Server.
4.	Antivirusinės programinės įrangos funkcionalumas	Siūloma sistema turi užtikrinti apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų.	Siūloma sistema užtikrina apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų.
		Sistema turi galėti proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms.	Sistema gali proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms.

		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.	Sistema atlieka žalingų veiksmų stebėseną ir aptinka dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo yra analizuojamas jos elgesys.
		Sistema turi gebėti sustabdyti bent 20 exploit technikų įskaitant: APC naudojimo (Application Procedure Calls); Privilegijų eskalavimo ataka (privilege escalation).	Sistema geba sustabdyti bent 20 exploit technikų įskaitant: • APC naudojimo (Application Procedure Calls) • Privilegijų eskalavimo ataka (privilege escalation).
		Sistema turi gebėti sustabdyti šias aktyvių kenkėjų technikas: Prieigos raktų ar slaptažodžių vagystė (credential theft); Kodo urvo naudojimas (code cave).	Sistema geba sustabdyti šias aktyvių kenkėjų technikas: • Prieigos raktų ar slaptažodžių vagystė (credential theft) • Kodo urvo naudojimas (code cave).
		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 prognozuoja kiek labai tas failas pavojingas, taip pat geba palyginti failą su jau žinomais pavojingais ar žinomais gerais failais. Tuomet pagal visą surinktą informaciją nusprendžia ar vykdyti failą.
		Sistema turi aptikti kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoti.	Sistema aptinka kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoja.
		Sistema turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus.	Sistema leidžia nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus.
		Siūlomas sprendimas turi galėti automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų.	Siūlomas sprendimas gali automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų.
		Siūloma sistema turi apsaugoti internetines naršykles (tokias kaip „Internet Explorer“, “Edge”, „Firefox“, „Chrome“, „Safari“, “Opera”), blokuojant prieigą prie žinomų kenksmingų	Siūloma sistema apsaugo internetines naršykles (tokias kaip „Internet Explorer“, “Edge”, „Firefox“, „Chrome“, „Safari“, “Opera”), blokuojant prieigą prie

		tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą.	žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą;.
		Sistema turi leisti numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui.	Sistema leidžia numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui.
		Siūloma saugumo sistema turi galėti skenuoti archyvuotas rinkmenas.	Siūloma saugumo sistema gali skenuoti archyvuotas rinkmenas.
		Sistema turi gebėti atpažinti failo tipą, t.y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį.	Sistema geba atpažinti failo tipą, t.y. atlieka failo tipo nustatymą ne tik pagal failo tipo plėtinį.
		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).	Saugumo sistema gali blokuoti įtartinas rinkmenas minimaliai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).
		Siūlomo sprendimo nustatymų turi būti negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises;	Siūlomo sprendimo nustatymų negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises.
		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).	Saugumo sistema gali blokuoti įtartinas rinkmenas minimaliai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).
5.	Reikalavimai sistemos centralizuotam valdymui, administravimui ir konfigūravimui	Siūlomo sprendimo centralizuoto valdymo konsolė turi galėti valdyti apsaugos sistemas Windows Server bei Linux platformose.	Siūlomo sprendimo centralizuoto valdymo konsolė gali valdyti apsaugos sistemas Windows Server bei Linux platformose.
		Siūlomo sprendimo atnaujinimas turi galėti vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir turi būti numatyta galimybė parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.	Siūlomo sprendimo atnaujinimas gali vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir yra numatyta galimybė parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.

		Turi būti galimybė numatyti pirminį ir antrinį atnaujinimo serverius.	Yra galimybė numatyti pirminį ir antrinį atnaujinimo serverius.
		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.
		Siūlomo sprendimo centralizuoto valdymo konsolė turi integruotis su Active Directory.	Siūlomo sprendimo centralizuoto valdymo konsolė integruojasi su Active Directory.
		Siūlomas sprendimas turi leisti taikyti nustatytąją saugumo politiką grupei valdomų serverių arba individualiems serveriams.	Siūlomas sprendimas leidžia taikyti nustatytąją saugumo politiką grupei valdomų serverių arba individualiems serveriams;
		Siūlomas sprendimas turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą.	Siūlomas sprendimas leidžia rolėmis su skirtingomis administravimo teisėmis paremtą administravimą.
		Siūlomas sprendimas turi galėti registruoti administratoriaus veiksmus auditavimo tikslais.	Siūlomas sprendimas gali registruoti administratoriaus veiksmus auditavimo tikslais.
6.	Reikalavimai išorinių sąsajų ir aplikacijų kontrolės funkcionalumui	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.	Siūlomas sprendimas gali 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.
		Siūlomas sprendimas turi galėti priskirti išorinio įrenginio naudojimo politiką individualiems serveriams ar serverių grupėms.	Siūlomas sprendimas gali priskirti išorinio įrenginio naudojimo politiką individualiems serveriams ar serverių grupėms.
		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; Leisti įrenginiui prisijungti tik „skaitymo“ režime.	Siūlomas sprendimas gali 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 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.
		Sistema turi leisti kontroliuoti programas (ang. application). Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. torrent, p2p), greitųjų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai.	Sistema turi leidžia kontroliuoti programas (ang. application). Sąrašas kontroliuojamų aplikacijų apima, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. torrent, p2p), greitųjų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai.
		Sistema turi užtikrinti automatinį kontroliuojamų programų atnaujintų naujomis versijomis aptikimą ir blokavimą.	Sistema užtikrina automatinį kontroliuojamų programų atnaujintų naujomis versijomis aptikimą ir blokavimą.
		Siūlomas sprendimas turi galėti priskirti aplikacijų naudojimo politiką individualiems serveriams ar serverių grupėms.	Siūlomas sprendimas gali priskirti aplikacijų naudojimo politiką individualiems serveriams ar serverių grupėms.
7.	Reikalavimai duomenų nutekėjimo prevencijos funkcionalumui (angl. Data loss prevention)	Siūloma sistema turi turėti integruotą funkcionalumą duomenų iš serverio tyčinio ar netyčinio praradimo apsaugai.	Siūloma sistema turi integruotą funkcionalumą duomenų iš serverio tyčinio ar netyčinio praradimo apsaugai.
		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.
		Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles.	Siūloma sistema leidžia pačiai organizacijai nustatyti turinį kontrolei ir taisykles.
		Saugumo sistema turi galėti registruoti veiksmus su kontroliuojamomis rinkmenomis.	Saugumo sistema gali registruoti veiksmus su kontroliuojamomis rinkmenomis.
		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 programas.	Saugumo sistema gali 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 programas.

		Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.	Siūloma sistema turi jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.
8.	Reikalavimai ugniasienės funkcionalumui	Siūloma sistema turi gebėti valdyti Windows firewall ugniasienę. Valdant iš saugumo sistemos centralizuotos valdymo konsolės.	Siūloma sistema geba valdyti Windows firewall ugniasienę. Valdant iš saugumo sistemos centralizuotos valdymo konsolės.
		Sistemos ugniasienės nustatymo metu turi būti galima naudoti mokymosi režimus (tik stebėti ir rinkti statistiką arba kontroliuoti tinklo profilius).	Sistemos ugniasienės nustatymo metu galima naudoti mokymosi režimus (tik stebėti ir rinkti statistiką arba kontroliuoti tinklo profilius).
		Turi gebėti taikyti skirtingas saugumo nustatymo politikas esant organizacijos tinkle ir už organizacijos tinklo perimetro.	geba taikyti skirtingas saugumo nustatymo politikas esant organizacijos tinkle ir už organizacijos tinklo perimetro.
		Sistema turi turėti galimybę izoliuoti save nuo aplinkinių įrenginių jei joje aptinkamas kenksmingas kodas ar ataka.	Sistema turi galimybę izoliuoti save nuo aplinkinių įrenginių jei joje aptinkamas kenksmingas kodas ar ataka.
9.	Reikalavimai tinklalapių filtravimo funkcionalumui	Siūloma sistema turi turėti galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas.	Siūloma sistema turi galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas.
		Turi būti ne mažiau nei sekančios kategorijos: Socialinių tinklų; Suaugusiųjų bei potencialiai nepriimtinų svetainių; Didelio pralaidumo reikalaujančių svetainių; Produktyvumą įtakojančių svetainių; Su darbu susijusių svetainių. Aukščiau išvardintos kategorijos turėtu būti toliau detalizuojamos į nemažiau kaip 3 subkategorijas kiekvienai kategorijai. Filtravimo politika turi būti nustatoma sistemos centrinėje valdymo konsolėje pagal vartotojų grupes.	Siūlomoje sistemoje yra ne mažiau nei sekančios kategorijos: • Socialinių tinklų • Suaugusiųjų bei potencialiai nepriimtinų svetainių • Didelio pralaidumo reikalaujančių svetainių • Produktyvumą įtakojančių svetainių • Su darbu susijusių svetainių Aukščiau išvardintos kategorijos gali būti toliau detalizuojamos į nemažiau kaip 3 subkategorijas kiekvienai kategorijai. Filtravimo politika yra nustatoma sistemos centrinėje valdymo konsolėje pagal vartotojų grupes.
		Turi būti numatyta galimybė įtraukti organizacijos numatytas internetines svetaines.	Yra numatyta galimybė įtraukti organizacijos numatytas internetines svetaines.

		Sistema turi galėti siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.	Sistema gali siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.
		Siūloma sistema turi realiu laiku blokuoti prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas.	Siūloma sistema realiu laiku blokuoja prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas.
		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.	Siūloma sistema turi galimybę apskaičiuoti atsisiunčiamos iš interneto rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoti arba nerekomenduoti atsisiųsti šią rinkmeną. Reputacija yra apskaičiuojama bent pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.
10.	Papildomas išplėstinio aptikimo ir atsako (XDR) funkcionalumas	Turi būti grėsmių aptikimas realiuoju laiku.	Siūlomoje sistemoje yra grėsmių aptikimas realiuoju laiku.
		Turi būti SQL užklausų formavimo ir vykdymo funkcionalumas siūlomo sprendimo valdymo įrankyje.	Siūlomoje sistemoje yra SQL užklausų formavimo ir vykdymo funkcionalumas siūlomo sprendimo valdymo įrankyje.
		Turi būti redaguojami SQL užklausų šablonai grėsmių aptikimui.	Siūlomoje sistemoje yra redaguojami SQL užklausų šablonai grėsmių aptikimui.
		Turi būti SQL užklausų planavimas ir paleidimas iš anksto numatytu periodiškumu.	Siūlomoje sistemoje yra SQL užklausų planavimas ir paleidimas iš anksto numatytu periodiškumu.
		Turi būti įtartinų įvykių aptikimo ir prioretizavimo funkcionalumas priskiriantis kategoriją pagal MITRE Attack struktūrą, bei priskiriantis kritiškumo lygį įvykiui.	Siūlomoje sistemoje yra įtartinų įvykių aptikimo ir prioretizavimo funkcionalumas priskiriantis kategoriją pagal MITRE Attack struktūrą, bei priskiriantis kritiškumo lygį įvykiui.
		Turi būti prieiga prie saugomo įrenginio (angl. endpoint) duomenų saugyklos diske.	Siūlomoje sistemoje yra prieiga prie saugomo įrenginio (angl. endpoint) duomenų saugyklos diske.
		Turi būti palaikomi kelių to paties gamintojo naudojamų produktų duomenų šaltiniai (pvz. ugniasienė, el. pašto apsauga) kuriuose būtų galima vykdyti SQL užklausas.	Siūlomoje sistemoje yra palaikomi kelių to paties gamintojo naudojamų produktų duomenų šaltiniai (pvz. ugniasienė, el. pašto apsauga) kuriuose būtų galima vykdyti SQL užklausas.
		Turi būti galimybė su papildomomis licencijomis integruoti ir gauti saugumo informaciją iš/su	Siūlomoje sistemoje yra galimybė su papildomomis licencijomis

		trečiųjų šalių tapatybės valdymo, tinklo grėsmių aptikimo, ugniasienių, e-pašto apsaugos, darbo stočių apsaugos sistemomis bei ne mažiau kaip su šiais viešosios debesijos paslaugų tiekėjais: Trend Micro; Fortigate; Checkpoint; Microsoft; Palo Alto Networks; Veeam; Acronis Cyber Protect.	integruoti ir gauti saugumo informaciją iš/su trečiųjų šalių tapatybės valdymo, tinklo grėsmių aptikimo, ugniasienių, e-pašto apsaugos, darbo stočių apsaugos sistemomis bei viešosios debesijos paslaugų tiekėjais: • Trend Micro • Fortigate • Checkpoint • Microsoft • Palo Alto Networks • Darktrace • Okta • Duo • Veeam • Acronis Cyber Protect
		Turi būti debesijos duomenų ežero (angl. data lake) saugykla kurioje kaupiama ir laikoma informacija apie saugomus įrenginius ne mažiau 90 dienų.	Siūlomoje sistemoje yra debesijos duomenų ežero (angl. data lake) saugykla kurioje kaupiama ir laikoma informacija apie saugomus įrenginius ne mažiau 90 dienų.
		Turi būti mašininio mokymosi, pagrįsto dirbtiniais neuroniniais tinklais (ang. Deep Learning), kenkėjiškų programų analizė.	Siūlomoje sistemoje yra mašininio mokymosi, pagrįsto dirbtiniais neuroniniais tinklais (ang. Deep Learning), kenkėjiškų programų analizė.
		Turi būti tyrimams atlikti tinkamų (angl. forensic) duomenų eksportavimo funkcionalumas, su galimybe eksportuoti duomenis į Amazon S3 duomenų saugyklą.	Siūlomoje sistemoje yra tyrimams atlikti tinkamų (angl. forensic) duomenų eksportavimo funkcionalumas, su galimybe eksportuoti duomenis į Amazon S3 duomenų saugyklą.
		Turi būti nuotolinė prieiga iš produkto valdymo aplinkos prie serverio grėsmių tyrimui ir pašalinimui.	Siūlomoje sistemoje yra nuotolinė prieiga iš produkto valdymo aplinkos prie serverio grėsmių tyrimui ir pašalinimui.
11.	Failų integralumo stebėjimas	Kritinių Windows operacinės sistemos failų pakeitimų stebėjimas ir prevencija.	Siūlomoje sistemoje yra kritinių Windows operacinės sistemos failų pakeitimų stebėjimas ir prevencija.
		Galimybė nustatyti papildomas stebėjimo lokacijas / katalogus.	Siūlomoje sistemoje yra galimybė nustatyti papildomas stebėjimo lokacijas / katalogus.
		Galimybė nustatyti išimtis.	Siūlomoje sistemoje yra galimybė nustatyti išimtis.

12.	Serveryje įdiegtų programų stebėjimas, naujų diegimų draudimas	Galimybė automatiškai išanalizuoti serveryje įdiegtas programas bei sukurti „baltąjį sąrašą“ (angl.: whitelist).	Siūlomoje sistemoje yra galimybė automatiškai išanalizuoti serveryje įdiegtas programas bei sukurti „baltąjį sąrašą“ (angl.: whitelist).
		Galimybė uždrausti programų nesančių baltajame sąraše diegimą ar paleidimą.	Siūlomoje sistemoje yra galimybė uždrausti programų nesančių baltajame sąraše diegimą ar paleidimą.
		Galimybė laikinai pridėti papildomą programą į baltąjį sąrašą neatjungiant bendro draudimo.	Siūlomoje sistemoje yra galimybė laikinai pridėti papildomą programą į baltąjį sąrašą neatjungiant bendro draudimo.
Mobilių įrenginių apsauga ir kontrolė, preliminarus licencijų skaičius – 10061 vnt.			
1.	Bendrieji reikalavimai	Sistema turi turėti kelių lygių valdymą (angl. multi-tenancy), kai įrenginius ir jų administratorius galima išskirti į smulkesnes organizacijas, kurių valdymas vyksta nepriklausomai viena nuo kitos.	Sistema turi kelių lygių valdymą (angl. multi-tenancy), kai įrenginius ir jų administratorius galima išskirti į smulkesnes organizacijas, kurių valdymas vyksta nepriklausomai viena nuo kitos.
		Sprendimas turi integruotis su Microsoft Active Directory ir Microsoft Azure Active Directory.	Sprendimas integruojasi su Microsoft Active Directory ir Microsoft Azure Active Directory.
		Sprendimą valdantiems administratoriams turi būti galima priskirti roles suteikiančias skirtingas administracines teises.	Sprendimą valdantiems administratoriams galima priskirti roles suteikiančias skirtingas administracines teises.
		Siūloma saugos sistema privalo gebėti valdyti minimaliai šias operacines sistemas: iOS 14 ir naujesnės; iPad OS 14 ir naujesnės; Android 8.0 ir naujesnės; Windows 10 ir naujesnes; macOS 10.15 ir naujesnes; Chrome OS 77 ir naujesnės.	Siūloma saugos sistema geba valdyti minimaliai šias operacines sistemas: • iOS 14 ir naujesnės. • iPad OS 14 ir naujesnės. • Android 8.0 ir naujesnės. • Windows 10 ir naujesnes. • macOS 10.15 ir naujesnes. • Chrome OS 77 ir naujesnės.
2.	Reikalavimai prietaisų įtraukimui (angl. device enrollment)	Sprendimas turi turėti šiuos būdus prietaisų įtraukimui į valdymo konsolę: Prietaisų įtraukimas išsiunčiant laiškus galutiniams vartotojams; Prisijungus prie savitarnos portalo; Pasinaudojant Apple Configurator; Pasinaudojant Apple DEP; Pasinaudojant Android Zero-touch; Pasinaudojant Samsung Knox; Pasinaudojant aprūpinimo paketu (angl. provisioning package).	Sprendimas turi šiuos būdus prietaisų įtraukimui į valdymo konsolę: • Prietaisų įtraukimas išsiunčiant laiškus galutiniams vartotojams. • Prisijungus prie savitarnos portalo. • Pasinaudojant Apple Configurator. • Pasinaudojant Apple DEP.

			• Pasinaudojant Android Zero-touch. • Pasinaudojant Samsung Knox. • Pasinaudojant aprūpinimo paketu (angl. provisioning package).
		Sprendimas turi automatiškai priskirti prietaisui teises ir grupes pagal naudotojų grupę esančią kompanijos naudotojų direktorijoje.	Sprendimas automatiškai priskiria prietaisui teises ir grupes pagal naudotojų grupę esančią kompanijos naudotojų direktorijoje.
		Sprendimas turi suteikti galimybę kurti automatinius diegimo paketus asmeniniams ir įmonės įrenginiams.	Sprendimas turi galimybę kurti automatinius diegimo paketus asmeniniams ir įmonės įrenginiams.
3.	Reikalavimai savitarnos (angl. Self Service) funkcionalumui	Sprendimas turi suteikti naudotojui galimybę priregistruoti naują prietaisą.	Sprendimas suteikia naudotojui galimybę priregistruoti naują prietaisą.
		Galimybę nuotoliniu būdu ištrinti visą informaciją (angl. wipe) iš įrenginio.	Siūlomas sprendimas turi galimybę nuotoliniu būdu ištrinti visą informaciją (angl. wipe) iš įrenginio.
		Galimybę nuotoliniu būdu užrakinti įrenginį.	Siūlomas sprendimas turi galimybę nuotoliniu būdu užrakinti įrenginį.
		Galimybę pažiūrėti prietaiso lokaciją.	Siūlomas sprendimas turi galimybę pažiūrėti prietaiso lokaciją.
		Galimybę atstatyti (angl. reset) prietaiso slaptažodį ir aplikacijų slaptažodžius (Android App Protection).	Siūlomas sprendimas turi galimybę atstatyti (angl. reset) prietaiso slaptažodį ir aplikacijų slaptažodžius (Android App Protection).
		Stebėti įrenginio statusą ir atitikties (angl. compliance) informaciją.	Siūlomas sprendimas gali stebėti įrenginio statusą ir atitikties (angl. compliance) informaciją.
4.	Įrenginiuose įdiegtos valdymo aplikacijos funkcijos	Iš įdiegtos aplikacijos įrenginiuose naudojai turi turėti galimybę pasiekti įmonės programėlių parduotuvę (angl. app store).	Iš įdiegtos aplikacijos įrenginiuose naudojai turi galimybę pasiekti įmonės programėlių parduotuvę (angl. app store).
		Įdiegta valdymo programa turi naudotojams rodyti politikos neatitikimus ir suteikti patarimus kaip išspręsti politikos neatitikimus.	Įdiegta valdymo programa naudotojams rodo politikos neatitikimus ir suteikti patarimus kaip išspręsti politikos neatitikimus.
		Įdiegta valdymo programa turi naudotojams rodyti žinutes siunčiamas iš serverio.	Įdiegta valdymo programa naudotojams rodo žinutes siunčiamas iš serverio.

		Įdiegta valdymo programa turi suteikti kontaktinę informaciją techninio atsakingo žmogaus.	Įdiegta valdymo programa suteikia kontaktinę informaciją techninio atsakingo žmogaus.
		Įdiegta valdymo programa turi suteikti galimybę naudotojui paleisti įrenginio sinchronizavimą.	Įdiegta valdymo programa turi galimybę naudotojui paleisti įrenginio sinchronizavimą.
5.	Reikalavimai aplikacijų valdymo funkcijoms	Sprendimas turi suteikti galimybę diegti aplikacijas į įrenginius nuotoliniu būdu nereikalaujant naudotojo veiksmų.	Sprendimas suteikia galimybę diegti aplikacijas į įrenginius nuotoliniu būdu nereikalaujant naudotojo veiksmų.
		Sprendimas turi suteikti galimybę išdiegti aplikacija iš įrenginių nuotoliniu būdu nereikalaujant naudotojo veiksmų.	Sprendimas suteikia galimybę išdiegti aplikacija iš įrenginių nuotoliniu būdu nereikalaujant naudotojo veiksmų.
		Sprendimas turi suteikti sąrašą visų įrenginyje įdiegtų aplikacijų.	Sprendimas suteikia sąrašą visų įrenginyje įdiegtų aplikacijų.
		Sprendimas turi palaikyti Apple VPP.	Sprendimas palaiko Apple VPP.
		Sprendimas turi tūrėti galimybę uždrausti diegti aplikacijas į įrenginį.	Sprendimas turi galimybę uždrausti diegti aplikacijas į įrenginį.
		Sprendimas turi tūrėti galimybę uždrausti ištrinti aplikacijas iš įrenginio.	Sprendimas turi galimybę uždrausti ištrinti aplikacijas iš įrenginio.
		Sprendimas turi tūrėti galimybę uždrausti pasirinktoms programoms veikti.	Sprendimas turi galimybę uždrausti pasirinktoms programoms veikti.
6.	Reikalavimai saugumo funkcionalumui	Sprendimas turi aptikti Jailbreak ir Rooting įrenginiuose.	Sprendimas aptinka Jailbreak ir Rooting įrenginiuose
		Sprendimas turi suteikti galimybę nuotoliniu būdu: Ištrinti visą informaciją esančia įrenginyje (angl. wipe); Užrakinti įrenginį; Parodyti įrenginio lokaciją.	Sprendimas suteikia galimybę nuotoliniu būdu: • Ištrinti visą informaciją esančia įrenginyje (angl. wipe) • Užrakinti įrenginį. • Parodyti įrenginio lokaciją.
		Sprendimas turi suteikti galimybę priverstinai nustatyti slaptažodžio sudėtingumą, ilgį, reikalinga kiekį didžiųjų/mažųjų raidžių, skaičių, simbolių.	Sprendimas suteikia galimybę priverstinai nustatyti slaptažodžio sudėtingumą, ilgį, reikalinga kiekį didžiųjų/mažųjų raidžių, skaičių, simbolių.
		Sprendimas turi suteikti galimybę nustatyti įrenginio neaktyvumo laiką po kurio yra prašoma slaptažodžio.	Sprendimas suteikia galimybę nustatyti įrenginio neaktyvumo laiką po kurio yra prašoma slaptažodžio.
		Sprendimas turi suteikti galimybę nustatyti maksimalų bandymų kiekį įvesti slaptažodį neteisingai, kurį pasiekus įrenginys bus atstatytas.	Sprendimas suteikia galimybę nustatyti maksimalų bandymų kiekį įvesti slaptažodį neteisingai, kurį pasiekus įrenginys bus atstatytas.

		Sprendimas turi galimybę nustatyti slaptažodžio galiojimo laiką.	Sprendimas suteikia galimybę nustatyti slaptažodžio galiojimo laiką.
		Administratorius turi galėti nustatyti naują slaptažodį įrenginiui.	Administratorius gali nustatyti naują slaptažodį įrenginiui.
		Sprendimas turi gebėti aktyvuoti saugyklos šifravimą.	Sprendimas geba aktyvuoti saugyklos šifravimą.
		Sprendimas turi blokuoti aplikacijų diegimą iš nežinomų šaltinių.	Sprendimas blokuoja aplikacijų diegimą iš nežinomų šaltinių.
		Sprendimas turi suteikti galimybę blokuoti: Wi-Fi; Bluetooth; Informacijos perdavimą per Bluetooth; Informacijos perdavimą per NFC; Blokuoti USB prijungimą; Kamerą.	Sprendimas suteikia galimybę blokuoti: • Wi-Fi. • Bluetooth. • Informacijos perdavimą per Bluetooth. • Informacijos perdavimą per NFC. • Blokuoti USB prijungimą. • Kamerą.
		Sprendimas turi suteikti galimybę blokuoti: iTunes Store; Google Play; Windows Store; Naršykles; Kameros pasiekimą; Trečiųjų šalių el. pašto aplikacijas; iCloud; Rankinį Wi-Fi konfigūravimą; Automatinį prisijungimą prie Wi-Fi (angl. Wi-Fi auto-connect); Prietaisą naudoti kaip Wi-Fi prieigos tašką (angl. hotspot); Naudoti pirštо anspaudą, kad atrakinti įrenginį; Paskyros keitimą; Naudotojui atstatyti įrenginį; Naudotojui pašalinti prietaisą iš valdymo sistemos (angl. unenroll); Ekrano kopijų (angl. screenshot) darymą; Kopijuoti/įklijuoti; Uždelsti arba uždrausti operacinės sistemos atnaujinimų darymą.	Sprendimas suteikia galimybę blokuoti: • iTunes Store. • Google Play. • Windows Store. • Naršykles. • Kameros pasiekimą. • Trečiųjų šalių el. pašto aplikacijas. • iCloud. • Rankinį Wi-Fi konfigūravimą. • Automatinį prisijungimą prie Wi-Fi (angl. Wi-Fi auto-connect). • Prietaisą naudoti kaip Wi-Fi prieigos tašką (angl. hotspot). • Naudoti pirštо anspaudą, kad atrakinti įrenginį. • Paskyros keitimą. • Naudotojui atstatyti įrenginį. • Naudotojui pašalinti prietaisą iš valdymo sistemos (angl. unenroll). • Ekrano kopijų (angl. screenshot) darymą. • Kopijuoti/įklijuoti.

			• Uždelsti arba uždrausti operacinės sistemos atnaujinimų darymą.
7.	Reikalavimai apsaugai nuo virusų bei kitų grėsmių (Android įrenginiams)	Sprendimas turi galėti sudiegti ir valdyti programinę įrangą skirtą apsaugai nuo virusų bei kitų grėsmių.	Sprendimas gali sudiegti ir valdyti programinę įrangą skirtą apsaugai nuo virusų bei kitų grėsmių.
		Apsauga nuo virusų turi turėti šias funkcijas: Tikrinti instaliuojamas bei jau suinstaliuotas programas; Identifikuoti galimai nepriimtinas programas; Skanuoti sistemines programas ir programas, sudiegtas į duomenų talpyklą.	Apsauga nuo virusų turi šias funkcijas: • Tikrinti instaliuojamas bei jau suinstaliuotas programas • Identifikuoti galimai nepriimtinas programas • Skanuoti tiek sistemines programas kiek programas sudiegtas į duomenų talpyklą.
		Kitos apsaugos funkcijos: Galimybė aptikti man-in-the-middle atakas; Integruotas TOTP ir HOTP autentifikatorius galintis vienu metu valdyti keletą prieigų; Integruotas QR kodų skaitytuvas galintis patikrinti QR kode esančią informaciją.	Sprendimas turi kitas apsaugos funkcijos: • Galimybė aptikti man-in-the-middle atakas • Integruotas TOTP ir HOTP autentifikatorius galintis vienu metu valdyti keletą prieigų • Integruotas QR kodų skaitytuvas galintis patikrinti QR kode esančią informaciją.
		Reikalavimai saugos funkcijų valdymui: Valdymas turi vykti per tą pačią valdymo konsolę kaip ir visas siūlomas sprendimas; Galimybė nustatyti skirtingus nustatymus įrenginių grupėms; Galimybė nustatyti periodinio skanavimo dažnumą; Galimybė pasirinkti ar ieškoti galimai nepriimtinų programų ir ar leisti vartotojui naudoti tas programas; Galimybė nurodyti visuomet leidžiamų programų sąrašą; Galimybė kontroliuoti prieigą prie darbo aplinkai netinkamų puslapių pagal kategoriją bei juodąjį / baltąjį sąrašus; Galimybė įjungti / išjungti man-in-the-middle atakų tikrinimą; Galimybė apriboti kada vykdomas debesija paremtas atnaujinimas, mažiausiai tokie pasirinkimai: „Visuomet“, „Tik prisijungus prie bevielio“, „Visuomet išskyrus kai naudojamas roaming“.	Sprendimas atitinka šiuos reikalavimus saugos funkcijų valdymui: • Valdymas turi vykti per tą pačią valdymo konsolę kaip ir visas siūlomas sprendimas • Galimybė nustatyti skirtingus nustatymus įrenginių grupėms • Galimybė nustatyti periodinio skanavimo dažnumą • Galimybė pasirinkti ar ieškoti galimai nepriimtinų programų ir ar leisti vartotojui naudoti tas programas • Galimybė nurodyti visuomet leidžiamų programų sąrašą • Galimybė kontroliuoti prieigą prie darbo aplinkai netinkamų puslapių pagal

			kategoriją bei juodąjį / baltąjį sąrašus. • Galimybė įjungti / išjungti man-in-the-middle atakų tikrinimą. • Galimybė apriboti kada vykdomas debesija paremtas atnaujinimas, mažiausiai tokie pasirinkimai: „Visuomet“, „Tik prisijungus prie bevielio“, „Visuomet išskyrus kai naudojamas roaming“.
8.	Reikalavimai įrenginio konfigūracijai	Sprendimas turi suteikti galimybę nustatyti Microsoft Exchange nustatymus el. paštui.	Sprendimas suteikia galimybę nustatyti Microsoft Exchange nustatymus el. paštui.
		Sprendimas turi suteikti galimybę nustatyti IMAP ir POP nustatymus el. paštui.	Sprendimas suteikia suteikti galimybę nustatyti IMAP ir POP nustatymus el. paštui.
		Sprendimas turi suteikti galimybę sukonfigūruoti Proxy nustatymus.	Sprendimas suteikia galimybę sukonfigūruoti Proxy nustatymus.
		Sprendimas turi suteikti galimybę nustatyti Wi-Fi nustatymus.	Sprendimas suteikia galimybę nustatyti Wi-Fi nustatymus.
		Sprendimas turi suteikti galimybę nustatyti VPN nustatymus.	Sprendimas suteikia galimybę nustatyti VPN nustatymus.
		Sprendimas turi suteikti galimybę diegti sertifikatus.	Sprendimas suteikia galimybę diegti sertifikatus.
		Sprendimas turi suteikti galimybę išdalinti prietaisams žymes (angl. bookmarks).	Sprendimas suteikia galimybę išdalinti prietaisams žymes (angl. bookmarks).
		Sprendimas turi suteikti galimybę priverstinai atlikti iOS atnaujinimą.	Sprendimas suteikia galimybę priverstinai atlikti iOS atnaujinimą
		Sprendimas turi suteikti galimybę konfigūruoti iOS užrakto ekraną (angl. lock screen) ir namų ekraną (angl. home screen).	Sprendimas suteikia galimybę konfigūruoti iOS užrakto ekraną (angl. lock screen) ir namų ekraną (angl. home screen).
		Sprendimas turi suteikti galimybę įrenginį naudoti kiosko režime (angl. kiosk mode).	Sprendimas suteikia galimybę įrenginį naudoti kiosko režime (angl. kiosk mode).
		Sprendimas turi suteikti galimybę valdyti aplikacijų teises (angl. premissions).	Sprendimas suteikia galimybę valdyti aplikacijų teises (angl. premissions).
		Sprendimas turi gebėti išnaudoti Android Enterprise funkcionalumus valdant tiek visą įrenginį tiek konteinerį (Android Enterprise Work Profile).	Sprendimas geba išnaudoti Android Enterprise funkcionalumus valdant tiek visą įrenginį tiek konteinerį (Android Enterprise Work Profile).

		Sprendimas turi gebėti išnaudoti Samsung Knox funkcionalumus.	Sprendimas geba išnaudoti Samsung Knox funkcionalumus.
		Sprendimas turi suteikti galimybę nuotoliniu būdu prisijungti prie įrenginių. Reikalinga papildoma Teamviewer licencija.	Sprendimas suteikia galimybę nuotoliniu būdu prisijungti prie įrenginių. Reikalinga papildoma Teamviewer licencija.
9.	Reikalavimai ataskaitoms ir žurnalams	Sprendimas turi suteikti galimybę eksportuoti ataskaitą apie turimą inventorių.	Sprendimas suteikia galimybę eksportuoti ataskaitą apie turimą inventorių.
		Sprendimas turi suteikti galimybę eksportuoti visas ataskaitas ir žurnalus, bent XLS ir CSV formatais.	Sprendimas suteikia galimybę eksportuoti visas ataskaitas ir žurnalus, bent XLS ir CSV formatais.
		Sprendimas turi pateikti žurnalus visų administratorių atliktų veiksmų.	Sprendimas pateikia žurnalus visų administratorių atliktų veiksmų.
		Sprendimas turi turėti kenkėjiškų programų (angl. malware) ataskaitas.	Sprendimas turi kenkėjiškų programų (angl. malware) ataskaitas.
		Sprendimas turi turėti ataskaitas apie prietaisus neatitinkančius perkančios kompanijos nustatymų.	Sprendimas turi ataskaitas apie prietaisus neatitinkančius perkančios kompanijos nustatymų.
		Sprendimas turi pateikti prietaisų ataskaitas.	Sprendimas turi prietaisų ataskaitas.
		Sprendimas turi pateikti aplikacijų ataskaitas.	Sprendimas turi aplikacijų ataskaitas.
		Sprendimas turi pateikti sertifikatų ataskaitas.	Sprendimas turi sertifikatų ataskaitas.
		Sprendimas minimaliai turi pateikti šią informaciją apie įrenginius: Vidinės atminties išnaudotą /laisvą kiekį; Akumuliatoriaus pakrovimo lygį; SIM kortelės IMSI; Šiuo metu naudojamą mobilų tinklą; Operacinės versiją; Sąrašą įdiegtų profilių.	Sprendimas pateikia šią informaciją apie įrenginius: • Vidinės atminties išnaudotą/laisvą kiekį. • Akumuliatoriaus pakrovimo lygį. • SIM kortelės IMSI • Šiuo metu naudojamą mobilų tinklą • Operacinės versiją • Sąrašą įdiegtų profilių.

5. PASIŪLYMO KAINA:

Eil. Nr.	Antivirusinės programinės įrangos licencijų pavadinimas	Preliminarus licencijų skaičius, vnt.	1 mėnesio 1 licencijos palaikymo kaina, EUR be PVM	12 mėnesių palaikymo kaina nurodytam licencijų skaičiui, EUR be PVM	36 mėnesių palaikymo kaina nurodytam licencijų skaičiui, EUR be PVM
1	*2*	*3*	*4*	*5*	*6*

1.	Antivirusinės programos „Sophos Central Intercept X Advanced“ licencijų be XDR funkcionalumo naudotojui palaikymas	16405	0,74	145 676,40	437 029,20
2.	Papildomas XDR funkcionalumo naudotojui palaikymas	16405	0,75	147 645,00	442 935,00
3.	Antivirusinės programos „Sophos Central Intercept X Advanced“ licencijų su XDR serveriui palaikymas	100	1,99	2 388,00	7 164,00
4.	Mobilių įrenginių valdymo programinės įrangos „Sophos Central Mobile Advanced“ licencijų palaikymas	10061	0,43	51 914,76	155 744,28
				Bendra pasiūlymo kaina EUR be PVM:	1 042 872,48
				PVM:	219 003,22
				Bendra pasiūlymo kaina* EUR su PVM:	1 261 875,70

***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.**

Pastaba.

Tiekėjo pasiūlymo kaina ir preliminarūs (lyginamieji) paslaugų kiekiai naudojami tik pasiūlymų vertinimui ir nebus laikomi maksimaliais. Perkančioji organizacija neįsipareigoja įsigyti nurodyto šių paslaugų kiekio. Sutartyje nurodytų paslaugų įsigijimas bus vykdomas pagal perkančiosios organizacijos poreikį, tiekėjo pasiūlyme nurodytais įkainiais EUR be PVM.

*Viešojo pirkimo pardavimo sutartis bus sudaroma vadovaujantis Kainodaros taisyklių nustatymo metodikos, patvirtintos Viešųjų pirkimų tarnybos direktoriaus 2017 m. birželio 28 d. Įsakymu Nr. 1S-95 „Dėl kainodaros taisyklių nustatymo metodikos patvirtinimo“, 17.2 punkto nuostatomis. Maksimali pirkimui skirta lėšų suma pirkimo dokumentuose nurodytų paslaugų įsigijimui tiekėjo pasiūlyme nurodytais įkainiais – **1 049 586,78 EUR be PVM (1 270 000,00 EUR su PVM)**.*

Jeigu tiekėjo pasiūlyme nurodyta bendra pasiūlymo kaina viršys maksimalią pirkimui skirtą lėšų sumą toks pasiūlymas bus laikomas nepriimtinu ir atmetamas.

Taikomas PVM dydis (%):	*21%*
PVM lengvatos/nemokėjimo teisinis pagrindas (jei taikoma):	-
Konkretaus pasiūlymo kaina žodžiais:	*vienas milijonas du šimtai šešiasdešimt vienas tūkstantis aštuoni šimtai septyniasdešimt penki eurai 70 euro centų su PVM*

6. PRIDEDAMI DOKUMENTAI IR INFORMACIJA APIE KONFIDENCIALUMĄ. (*Jei nenurodyta kitaip, visi dokumentai teikiami su konkrečiu pasiūlymu CVP IS priemonėmis):*

Eil. Nr.	Dokumentas	Ar dokumente yra konfidencialios[2] informacijos?	Paaiškinimas, kokia konkreti informacija dokumente yra	Lapų skaičius

[2] *Informacija, nurodyta VPĮ 20 straipsnio 2 dalies 1, 2, 3, 4 punktuose negali būti nurodoma ir nebus laikoma konfidencialia nepriklausomai nuo to, kad tiekėjas ją nurodė šioje lentelėje. 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, Komisija prašys tiekėją per nurodytą terminą, kuris negali būti trumpesnis kaip 3 darbo dienos,*

		(Taip / Ne)	konfidenciali ir kodėl	
1	*2*	*3*	*4*	*5*
1.	Ši konkretaus pasiūlymo forma	Ne	-	28
2.	Atitiktį techninės specifikacijos 6 punkto reikalavimui įrodantys dokumentai	Ne	-	1
3.	Jungtinės veiklos sutarties kopija *(jei teikia ūkio subjektų grupė)*	-	-	-
4.	Ketinimų protokolas ar subtiekimo sutartis (ar kiti dokumentai), *(jei tiekėjui yra žinomi ketinami pasitelkti subtiekėjai konkretaus pirkimo sutarties vykdymui)*	-	-	-
5.	Pasirašytas EBVPD *(jei anksčiau teiktame (-uose) EBVPD informacija yra pasikeitusi)*	-	-	-
6.	Nacionalinio saugumo reikalavimų atitikties deklaracija, Tiekėjo deklaracija dėl ES reglamento, Tiekėjo deklaracija, kt. dok., *(jei anksčiau teiktame (-uose) informacija yra pasikeitusi)*	-	-	-
7.	Įgaliojimo ar kito dokumento, suteikiančio teisę pateikti ir (ar) pasirašyti konkretų pasiūlymą bei kitus dokumentus, kopija (*jeigu konkretų pasiūlymą pateikia ir ar dokumentus pasirašo ne tiekėjo, ūkio subjektų grupės dalyvių, subtiekėjų ar ūkio subjektų, kurių pajėgumais tiekėjas remiasi, vadovas)*	Ne	-	1
...	*....nurodomi kiti pateikiami dokumentai (jeigu teikiami)*	-	-	-

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. Konkretaus pasiūlymo dokumentuose pateikti duomenys ir informacija yra teisinga ir apima viską, ko reikia tinkamam sutarties įvykdymui; Šis pasiūlymas galioja tiek, kiek nustatyta konkretaus pirkimo (B dalis. Konkretaus pirkimo sąlygos) sąlygose. Taip pat, patvirtinu, kad dokumentų skaitmeninės kopijos ir elektroninėmis priemonėmis pateikti duomenys yra tikri.

Viešųjų pirkimų specialistė		
(DPS tiekėjo arba jo įgalioto asmens pareigų pavadinimas)	(Parašas)	(Vardas, pavardė)

pagrįsti jos konfidencialumą. Jei tokia informacija pasiūlyme nebus nurodyta, Komisija laikys, kad bet kuri pasiūlyme pateikta informacija nėra konfidenciali, išskyrus informaciją, kurią atskleidus būtų pažeisti Tiekėjo įsipareigojimai pagal su trečiaisiais asmenimis sudarytas sutartis