PASLAUGŲ PIRKIMO-PARDAVIMO SUTARTIS Nr. LEI/22/06/27

2022 m. birželio 27 d.

Kaunas

VšĮ Lietuvos energetikos institutas, įmonės kodas 111955219, kurio registruota buveinė yra Breslaujos g. 3, 44403 Kaunas, atstovaujamas direktoriaus Sigito Rimkevičiaus, veikiančio pagal įstaigos nuostatus (toliau – „**Užsakovas**"), ir

UAB Topologija, įmonės kodas 304751143, kurios registruota buveinė yra Draugystės g. 17-1, LT-51229 Kaunas, atstovaujama direktoriaus Teisučio Šegždos, veikiančio pagal bendrovės įstatus (toliau – **„Paslaugų teikėjas"**),

toliau kiekvienas atskirai gali būti vadinami **„Šalimi"**, o abu kartu – **„Šalimis"**, sudarė šią paslaugų pirkimo-pardavimo sutartį (toliau – **„Sutartis"**) ir susitarė dėl toliau išvardintų sąlygų.

1. SUTARTIES OBJEKTAS

1.1. Sutarties objektas – centralizuoto valdymo ir žurnalinių įvykių registravimo, saugojimo ir analizės sistemos nuomos su priežiūra paslaugos (toliau – paslaugos).
1.2. Perkamų paslaugų savybės apibūdintos Paslaugų teikėjo pasiūlyme (Sutarties 1 priedas).
1.3. Sutartis sudaroma, vadovaujantis viešojo pirkimo, vykdyto Centrinėje viešųjų pirkimų informacinėje sistemoje skelbiamos apklausos būdu, rezultatais.

2. SUTARTIES ŠALIŲ ĮSIPAREIGOJIMAI

2.1. Paslaugų teikėjo teisės ir pareigos:
2.1.1. Įsipareigoja kokybiškai ir operatyviai teikti paslaugas, numatytas Sutartyje ir jos prieduose;
2.1.2. Vykdo teisėtus Užsakovo nurodymus;
2.1.3. Visus dokumentus ir informaciją, gautą pagal Sutartį, laiko konfidencialia ir be išankstinio raštiško Užsakovo sutikimo neturi teisės Užsakovo pateiktų dokumentų perduoti trečiajai šaliai ir neskelbia bei neatskleidžia jokių Sutarties nuostatų, išskyrus atvejus, kai tai būtina vykdant Sutartį;
2.1.4. Užtikrina, kad bet kokio pobūdžio informacija (bet kokioje laikmenoje), kuri jam (jo darbuotojams, specialistams, kitiems atstovams) tapo žinoma paslaugų teikimo metu yra laikoma konfidencialia ir jos atskleidimas suteikia teisę reikalauti žalos atlyginimo;
2.1.5. Nevykdant (netinkamai vykdant) savo sutartines prievoles, Užsakovui pareikalavus, nedelsiant savo sąskaita ištaiso bet kokius trūkumus, susijusius su paslaugų teikimu;
2.1.6. Užtikrina, kad paslaugų pagal Sutartį vykdymą koordinuoja kvalifikuoti specialistai. Taip pat Užsakovui pateikia du skirtingus Paslaugų teikėjo telefono numerius ir elektroninio pašto adresus, kuriais Užsakovas gali pateikti savo užsakymus. Praneša apie įmonės rekvizitų ir užsakymų priėmimo kontaktinio numerio ar adreso pasikeitimą per 5 darbo dienas;
2.1.7. Visiškai atsako už Užsakovui padarytus nuostolius dėl savo darbuotojų kaltės;
2.1.8. Nedelsiant praneša Užsakovui apie bet kokius nukrypimus nuo Sutarties sąlygų ir imasi neatidėliotinų priemonių juos pašalinti;
2.1.9. Saugo Užsakovo galutiniame užsakyme nurodytus asmenų duomenis pagal Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą.
2.1.10. Turi teisę gauti paslaugų kainą su sąlyga, kad jis tinkamai vykdo Sutartį.
2.1.11. Turi ir kitas šios Sutarties bei Lietuvos Respublikoje galiojančių teisės aktų numatytas teises bei pareigas.

2.2. Užsakovo teisės ir pareigos:
2.2.1. Užsakovas įsipareigoja laiku sumokėti Paslaugų teikėjui už suteiktas paslaugas Sutarties 3 dalyje nustatyta tvarka;
2.2.2. Užsakovas suteikia Paslaugų teikėjui visą būtiną informaciją, reikalingą paslaugoms suteikti;
2.2.3. Užsakovas turi teisę kontroliuoti Sutarties vykdymą bei duoti Paslaugų teikėjui nurodymus, kad būtų tinkamai, kokybiškai ir laiku vykdoma Sutartis;
2.2.4. Užsakovas turi ir kitas šios Sutarties bei Lietuvos Respublikoje galiojančių teisės aktų numatytas teises bei pareigas.

3. APMOKĖJIMO SĄLYGOS IR TVARKA, KAINODAROS TAISYKLĖS

3.1. Preliminari maksimali sutarties kaina yra 32321,52 EUR (*Trisdešimt du tūkstančiai trys šimtai dvidešimt vienas euras, penkiasdešimt du centai)*, iš kurios PVM sudaro 5609,52 EUR (*Penki tūkstančiai šeši šimtai devyni eurai, penkiasdešimt du centai*). Į paslaugų kainą įskaičiuotos visos su paslaugų teikimu susijusios išlaidos ir mokesčiai.
3.2. Už tinkamai ir laiku suteiktas paslaugas, atsižvelgiant į pasirašytus paslaugų priėmimo-perdavimo aktus, Užsakovas sumoka per 30 (trisdešimt) kalendorinių dienų nuo sąskaitos faktūros ir išlaidas pagrindžiančių dokumentų gavimo dienos ne dažniau nei kartą per mėnesį. Mokėjimas už paslaugas atliekamas pavedimu į šioje Sutartyje nurodytą Paslaugų teikėjo sąskaitą banke.
3.3. Jeigu paslaugos suteiktos netinkamai, Užsakovas turi teisę atsisakyti vykdyti mokėjimą, raštu informuojant Paslaugų teikėją apie nustatytus trūkumus, o Paslaugų teikėjas įsipareigoja ištaisyti visus Užsakovo nurodytus trūkumus ne vėliau kaip per 3 darbo dienas, nebent Užsakovas nustatytų kitą terminą.
3.4. Sutarties kaina yra fiksuota su peržiūra dėl pasikeitusio PVM dydžio.
3.5. Pasikeitęs pridėtinės vertės mokesčio (PVM) dydis skaičiuojamas nuo atitinkamo teisės akto, kuriuo pakeistas PVM, įsigaliojimo dienos, paslaugų kaina keičiama proporcingai PVM pasikeitimo dydžiui. Perskaičiuota kaina taikoma po perskaičiavimo suteiktoms paslaugoms apmokėti. Pasikeitus kitiems mokesčiams, įkainiai negali būti perskaičiuojami.
3.6. Pakeistos paslaugų kainos įsigalioja tik Šalims pasirašius priedą prie šios Sutarties.
3.7. Sutarties galiojimo laikotarpiu paslaugų aptarnavimo įkainiai dėl bendro kainų lygio kitimo nebus keičiami.

4. ŠALIŲ ATSAKOMYBĖ

4.1. Paslaugų teikėjo atsakomybė yra apribota atsakomybe už tiesioginę žalą (nuostolius, netesybas ir pan.), kurią Užsakovas patirtų dėl Paslaugų teikėjo, jo darbuotojų ir (ar) atstovų arba trečiųjų asmenų tyčios ar didelio nerūpestingumo tiekiant šioje Sutartyje numatytas Paslaugas.
4.2. Paslaugų teikėjas ne laiku suteikęs paslaugas, Užsakovui pareikalavus, sumoka Užsakovui 0,02 % vertės delspinigius, skaičiuojamus už kiekvieną uždelstą dieną, kuomet vėluojama paslaugas teikti pagal suderintą planą.
4.3. Užsakovui dėl savo kaltės nesumokėjus Paslaugų teikėjui už suteiktas paslaugas per šioje Sutartyje nustatytą terminą, Paslaugų teikėjui pareikalavus, Užsakovas moka 0,02 % dydžio delspinigius nuo vėluojamos sumokėti sumos už kiekvieną uždelstą dieną.
4.4. Paslaugų teikėjas negali perleisti tretiesiems asmenims visų ar dalies savo teisių, susijusių su Sutartimi, įskaitant reikalavimo teisę į Užsakovo mokėtinas sumas, be išankstinio Užsakovo rašytinio sutikimo. Be Užsakovo išankstinio rašytinio sutikimo sudaryti sandoriai dėl teisių ar pareigų pagal šią Sutartį perleidimo laikytini niekiniais ir negaliojančiais nuo jų sudarymo momento.

5. SUTARTIES GALIOJIMAS IR NUTRAUKIMAS

5.1. Sutartis įsigalioja nuo jos pasirašymo dienos ir galioja iki visiško joje numatytų Šalių įsipareigojimų įvykdymo dienos. Paslaugos teikiamos 36 (trisdešimt šešis) mėnesius.
5.2. Užsakovas turi teisę, įspėjęs Paslaugų teikėją prieš 10 dienų, vienašališkai nutraukti šią Sutartį dėl esminio jos pažeidimo. Esminiu Sutarties pažeidimu bus laikomas bet kurio įsipareigojimo pagal šią Sutartį nevykdymas arba netinkamas vykdymas.
5.3. Kitu atveju Sutartis gali būti nutraukta Šalių abipusiu susitarimu arba įstatymų nustatyta tvarka.
5.4. Sutartį nutraukus dėl Paslaugų teikėjo kaltės, Paslaugų teikėjas neturi teisės į kokių nors patirtų nuostolių ar žalos kompensaciją.

6. NENUGALIMA JĖGA (*force majeure*)

6.1. Šalys neatsako už sutartinių įsipareigojimų pagal šią Sutartį nevykdymą ar dalinį neįvykdymą, jeigu tai įvyko dėl nenugalimos jėgos. Nenugalima jėga laikomi neišvengiami ir Šalių nekontroliuojami įvykiai, kurie nebuvo ir negalėjo būti numatyti, kaip tai apibrėžiama Lietuvos Respublikos teisės aktuose. Šalis, kuri negali vykdyti įsipareigojimų dėl nenugalimos jėgos, privalo nedelsiant raštu pranešti apie tai kitai Šaliai. Sutarties vykdymas atidedamas, kol išnyks nenugalimos jėgos aplinkybės. Jeigu šios aplinkybės trunka ilgiau kaip 45 (keturiasdešimt penkias) kalendorines dienas, kiekviena Šalis turi teisę nutraukti Sutartį visiškai arba iš dalies, ir nei viena iš jų neturi teisės pareikalauti iš kitos Šalies padengti nuostolius.

7. ŠALIŲ PAREIŠKIMAI IR GARANTIJOS

7.1. Kiekviena Šalis pareiškia ir garantuoja kitai Šaliai, kad:
7.1.1.Šalis yra tinkamai įsteigta ir teisėtai veikia pagal Lietuvos Respublikos įstatymus.
7.1.2. Šalis atliko visus teisinius veiksmus, būtinus, kad Sutartis būtų tinkamai sudaryta ir galiotų, ir turi visus teisės aktais numatytus leidimus, licencijas, darbuotojus, reikalingus Prekėms tiekti.
7.1.3.Sudarydama Sutartį, Šalis nepažeis ją saistančių įstatymų, taisyklių, nuostatų, potvarkių, įsipareigojimų ar susitarimų.
7.1.4.Ši Sutartis yra Šaliai galiojantis, teisinis ir ją saistantis įsipareigojimas, kurio vykdymo galima pareikalauti pagal Sutarties sąlygas.

8. GINČŲ SPRENDIMAS

8.1. Visi ginčai, nesutarimai ir pretenzijos, kurie gali kilti tarp šalių dėl šios Sutarties, bus sprendžiami derybų keliu. Jei nesutarimų nepavyksta išspręsti derybų keliu per 30 kalendorinių dienų nuo vienos iš šalių pasiūlymo pradėti derybas gavimo dienos, visi ginčai kylantys dėl šios Sutarties sprendžiami Lietuvos Respublikos teisės aktų nustatyta tvarka Lietuvos Respublikos teisme pagal Užsakovo buveinės adresą.
8.2. Sutartyje neaptartoms sąlygoms taikomos Lietuvos Respublikos civilinio kodekso nuostatos.

9. BAIGIAMOSIOS NUOSTATOS

9.1. Sutartis gali būti sudaroma 2 (dviem) egzemplioriais lietuvių kalba, po vieną kiekvienai šaliai. Abu Sutarties egzemplioriai yra vienodos teisinės galios. Sutartis, pasirašyta kvalifikuotu elektroniniu parašu (vienas elektroninis dokumentas), turės tokią pat teisinę galią kaip ir rašytiniu parašu pasirašyta Sutartis.
9.2. Už sutarties vykdymą ir kontrolę Šalys skiria atsakingais šiuos asmenis:
9.2.1.Iš Paslaugų teikėjo pusės: IT inžinierius Paulius Misevičius,tel.+370 659 10069 el. paštas paulius.misevicius@topologija.lt;
9.2.2. Iš Užsakovo pusės: direktoriaus pavaduotojas Rolandas Urbonas, tel. +370 37 401832 el. paštas rolandas.urbonas@lei.lt .

9.3. Bet kokie pranešimai, informacija, dokumentacija ar korespondencija dėl Sutarties ar jos vykdymo turi būti įforminta raštu lietuvių kalba ir išsiųsta Sutartyje nurodytu registruotu paštu ar elektroniniu paštu.

10.SUTARTIES PRIEDAI

10.1. Šios Sutarties priedai yra neatskiriama Sutarties dalis ir sudaro vieną visumą:
10.1.1. Paslaugų teikėjo pasiūlymas (1 priedas).

11. ŠALIŲ REKVIZITAI

PASLAUGŲ TEIKĖJAS	**UŽSAKOVAS**
UAB TOPOLOGIJA	**VšĮ Lietuvos energetikos institutas**
Įmonės kodas 304751143	Įmonės kodas 111955219
PVM mokėtojo kodas LT100011475717	PVM mokėtojo kodas LT119552113
Draugystės g. 17-1, LT-51229 Kaunas	Breslaujos g. 3, 44403 Kaunas
Tel.: 370 698 34 555	Tel.: 8 37 401 805
A. s. Nr. LT777300010154196951	A. s. Nr. LT61 4010 0425 0310 6594
AB Swedbank	Luminor Bank AS
Direktorius Teisutis Šegžda	*Direktorius Sigitas Rimkevičius*
_____	_____
A.V.	A.V.

Uždaroji akcinė bendrovė, Draugystės g. 17-1, LT-51229 Kaunas, Juridinių asmenų registras,
UAB Topologija, 304751143, LT100011475717

Lietuvos energetikos institutas
(Adresatas (perkančioji organizacija))

PASIŪLYMAS
DĖL CENTRALIZUOTO VALDYMO IR ŽURNALINIŲ ĮVYKIŲ REGISTRAVIMO, SAUGOJIMO IR ANALIZĖS SISTEMOS NUOMOS SU PRIEŽIŪRA PASLAUGŲ PIRKIMO

2022 m. birželio 22 d. Nr.1
(Data)
Kaunas
(Sudarymo vieta)

Tiekėjo pavadinimas */Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai/*	UAB Topologija
Tiekėjo adresas */Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai/*	Draugystės g. 17-1, LT-51229 Kaunas
Asmens, atsakingo už pasiūlymą, vardas, pavardė, pareigos	Direktorius Teisutis Šegžda
Telefono numeris	+370 698 34 555
El. pašto adresas	info@topologija.lt

/Pastaba. Pildoma, jei Tiekėjas ketina pasitelkti subrangovą (-us), subtiekėją (-us), ar subteikėją (-us)/

Subrangovo (-ų), subtiekėjo (-ų) ar subteikėjo (-ų) pavadinimas (-ai)	-
Subrangovo (-ų), subtiekėjo (-ų) ar subteikėjo (-ų) adresas (-ai)	-
Įsipareigojimų dalis (procentais), kuriai ketinama pasitelkti subrangovą (-us), subtiekėją (-us) ar subteikėją (-us)	-

Mes siūlome tokias paslaugas ir jų įkainius:

1.Pateikiamas Priedas Nr.1 „Techninė specifikacija“ su tiekėjo užpildyta skiltimi **„Tiekėjo siūloma“.**

2.Pateikiama kainos lentelė:

Eil. Nr.	Paslaugos pavadinimas	Kiekis, mėn.	1 mėnesio nuomos su priežiūra kaina be PVM, Eur	Bendra kaina už nuomą su priežiūra 36 mėn. be PVM, Eur (*3* x *4*)
1	*2*	*3*	*4*	*5*
1	Centralizuoto valdymo ir žurnalinių įvykių registravimo, saugojimo ir analizės sistemos nuoma su priežiūra (*pagal Pirkimo sąlygų 1 priedą „Techninė specifikacija“*)	36	742,00	26712,00
			Viso PVM suma	5609,52
			Bendra kaina už nuomą su priežiūra per 36 mėnesius su PVM, Eur	32321,52

Pastabos:

1) kainos pasiūlyme nurodomos suapvalintos, paliekant du skaitmenis po kablelio.

2) tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, tiekėjas atitinkamų skilčių nepildo ir nurodo priežastis, dėl kurių PVM nemoka.

Siūlomos paslaugos visiškai atitinka pirkimo dokumentų Techninėje specifikacijoje nurodytus reikalavimus (tiekėjas kartu su pasiūlymu pateikia užpildytą techninės specifikacijos lentelę, priedas Nr.1).

Pasiūlyme yra pateikta konfidenciali informacija šiuose dokumentuose*:

Eil. Nr.	Pateikto dokumento pavadinimas	Lapų skaičius
1.	Techninė specifikacija	20
2.	Kvalifikacijos sertifikatai	2

** Pildyti tuomet, jei pasiūlyme yra pateikta konfidenciali informacija.*

Kartu su pasiūlymu pateikiami šie dokumentai ir informacija:

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius
1.	Kvalifikacijos sertifikatai	2

Pasiūlymas galioja iki 2022 m. rugpjūčio 31 d.

Tiekėjo vadovo arba jo įgalioto asmens
vardas, pavardė, pareigos, parašas Direktorius Teisutis Šegžda

CENTRALIZUOTO VALDYMO IR ŽURNALINIŲ ĮVYKIŲ REGISTRAVIMO, SAUGOJIMO IR ANALIZĖS SISTEMA

TECHNINĖ SPECIFIKACIJA

Nr.	**Specifikacija**	**Reikalavimai**	**Tiekėjo siūloma** *(pildo tiekėjas)*
1.	Įrangos pavadinimas	–	5400 Next Generation Theat Prevention Appliance
2.	Įrangos gamintojas	–	Check Point Software Technologies
3.	Įrango paskirtis	Sistema skirta apsaugoti kompiuterinį tinklą bei kompiuterines darbo vietas, kaupti bei analizuoti saugos įvykius. Sprendimas susideda iš: 1. Centralizuoto valdymo sprendimas. 2. Ugniasienė. 3. Darbo vietų saugos sprendimas.	Sistema skirta apsaugoti kompiuterinį tinklą bei kompiuterines darbo vietas, kaupti bei analizuoti saugos įvykius. Sprendimas susideda iš: 1. Centralizuoto valdymo sprendimas. 2. Ugniasienė. 3. Darbo vietų saugos sprendimas.
Bendri reikalavimai			
4.	Valdomi įrenginiai	Siūlomas sprendimas turi gebėti pilnai valdyti: • Siūlomą ugniasienę. • Siūlomą darbo vietų saugos sprendimą.	Siūlomas sprendimas geba pilnai valdyti: • Siūlomą ugniasienę. Siūlomą darbo vietų saugos sprendimą.
5.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Yra. Nemokamai garantinio aptarnavimo laikotarpiu
6.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra
7.	Valdymas	Įrenginys turi būti valdomas per grafinę sąsają. Turi būti galimybė sukurti kelis administratorių paskyras, suteikiant skirtingą prieigos lygį, įskaitant skirtingus įrenginius, jų funkcijas,	Įrenginys valdomas per grafinę sąsają. Yra galimybė sukurti kelis administratorių paskyras, suteikiant skirtingą prieigos lygį, įskaitant skirtingus įrenginius, jų funkcijas,

		skirtingas teises, įskaitant tik peržiūros bei peržiūros/redagavimo teises.	skirtingas teises, įskaitant tik peržiūros bei peržiūros/redagavimo teises.
Plečiamumas			
8.	Valdomų ugniasienių kiekis	Ne mažiau 5	5
9.	Valdomų kompiuterinių darbo vietų kiekis	Ne mažiau 500	500
Reikalavimai ugniasienės valdymui			
10.	Centralizuotas valdymas	Centralizuoto valdymo funkcionalumas turi pilnai valdyti siūlomos ugniasienės funkcionalumą, įskaitant: • Ugniasienės funkcijas. • IPSec VPN funkcijas. • IPS funkcijas. • Aplikacijų kontrolės funkcijas. • URL filtravimo funkcijas. • Bot aptikimo funkcijas. • Antivirusinio srauto filtravimo funkcijas. • Tapatybės matomumo funkcijas. • Tinklo ir maršrutizavimo funkcijas.	Centralizuoto valdymo funkcionalumas pilnai valdo siūlomos ugniasienės funkcionalumą, įskaitant: • Ugniasienės funkcijas. • IPSec VPN funkcijas. • IPS funkcijas. • Aplikacijų kontrolės funkcijas. • URL filtravimo funkcijas. • Bot aptikimo funkcijas. • Antivirusinio srauto filtravimo funkcijas. • Tapatybės matomumo funkcijas. Tinklo ir maršrutizavimo funkcijas.
11.	Centralizuoto konfigūravimo funkcionalumas	• Turi būti centralizuoto konfigūravimo funkcionalumas. • Profilių kūrimas skirtingiems įrenginių tipams automatizuotam įrenginių konfigūravimui. • Administravimo veiklų planavimo ir automatizavimo funkcionalumas konfigūravimo skriptų paleidimui, konfigūracijų atsarginių kopijų darymui, įrenginių perkrovimui.	• Yra centralizuoto konfigūravimo funkcionalumas. • Profilių kūrimas skirtingiems įrenginių tipams automatizuotam įrenginių konfigūravimui. Administravimo veiklų planavimo ir automatizavimo funkcionalumas konfigūravimo skriptų paleidimui, konfigūracijų atsarginių kopijų darymui, įrenginių perkrovimui.
12.	Stebėjimo funkcionalumas	• Turi būti centralizuoto įrenginių stebėjimo funkcionalumas. • Valdomų įrenginių stebėjimas, tinklo srautų stebėjimas, įtartinos veiklos	• Yra centralizuoto įrenginių stebėjimo funkcionalumas. Valdomų įrenginių stebėjimas, tinklo srautų stebėjimas, įtartinos veiklos stebėjimas, VPN tunelių stebėjimas

		stebėjimas, VPN tunelių stebėjimas bei automatinis pranešimų administratoriams pateikimas.	bei automatinis pranešimų administratoriams pateikimas.
Reikalavimai kompiuterinių darbo vietų saugos sprendimo valdymui			
13.	Programinės įrangos diegimas	• Turi būti galimybė programinę įrangą diegti centralizuotai, automatiškai sukuriant instaliacinį failą (MSI paketą) su bazine konfigūracija, apimančią centrinio serverio duomenimis, nustatyta saugos politika bei programinės įrangos komponentais. MSI paketai turi būti tinkami naudoti su Microsoft System Center Configuration Manager įrankiais. • Turi būti galimybę diegti pradinį instaliacinį failą (MSI paketą) su bazine konfigūracija, apimančia centrinio serverio duomenis. Pradinis paketas turi suteikti galimybę įdiegti programinės įrangos komponentus pagal kompiuterinei darbo vietai, serveriui, vartotojui ar jų grupei nustatytą politiką iš centrinio serverio. • Turi būti galimybė eksploatacijos metu, pakeitus politiką, iš centrinio serverio pakeisti KDV programinės įrangos komponentų rinkinį, KDV programinės įrangos versiją visiems ar grupei kompiuterinių darbo vietų, serverių ar vartotojų.	• Yra galimybė programinę įrangą diegti centralizuotai, automatiškai sukuriant instaliacinį failą (MSI paketą) su bazine konfigūracija, apimančią centrinio serverio duomenimis, nustatyta saugos politika bei programinės įrangos komponentais. MSI paketai turi būti tinkami naudoti su Microsoft System Center Configuration Manager įrankiais. • Yra galimybė diegti pradinį instaliacinį failą (MSI paketą) su bazine konfigūracija, apimančia centrinio serverio duomenis. Pradinis paketas turi suteikti galimybę įdiegti programinės įrangos komponentus pagal kompiuterinei darbo vietai, serveriui, vartotojui ar jų grupei nustatytą politiką iš centrinio serverio. Yra galimybė eksploatacijos metu, pakeitus politiką, iš centrinio serverio pakeisti KDV programinės įrangos komponentų rinkinį, KDV programinės įrangos versiją visiems ar grupei kompiuterinių darbo vietų, serverių ar vartotojų.
14.	Centralizuoto valdymo, administravimo ir konfigūravimo funkcionalumas	• Turi būti galimybė valdyti centrinį serverį per WEB naršyklę pasiekiamą grafinę sąsają (WEB-UI) arba administratoriaus darbo vietoje diegiamą programinę įrangą. • Centrinis serveris turi valdyti visas KDV programinės įrangos versijas, visuose įdiegtose ir licencijuotuose	• Yra galimybė valdyti centrinį serverį per WEB naršyklę pasiekiamą grafinę sąsają (WEB-UI) arba administratoriaus darbo vietoje diegiamą programinę įrangą. • Centrinis serveris gali valdyti visas KDV programinės įrangos versijas, visuose įdiegtose ir licencijuotuose

		kompiuterinėse darbo vietose ir serveriuose. • Turi būti galimybė pasirinkti naujinimų diegimo būdą: • Gamintojo naujinimo serverių naudojimas tiesioginiam KDV programinės įrangos ir aprašų atnaujinimams. • Centrinio serverio naudojimas KDV programinės įrangos ir aprašų atnaujinimams. • Turi būti galimybė pasirinkti naujinimų diegimo politiką: • Automatinis arba pagal administratoriaus nurodymą, visiems vartotojams/serveriams/kompiuterinėms darbo vietoms arba jų grupėms. • Nustatyti naujinimų diegimų periodiškumą ir pageidaujamą paros laiką. • Turi būti galimybė sistemos administratoriui nuotoliniu būdu atlikti veiksmus visiems arba daliai vartotojų, kompiuterinių darbo vietų ar serverių: • Paleisti priverstinį atnaujinimą. • Paleisti pilną arba dalinį sistemos skenavimą. • Pritaikyti nustatytąją saugumo politiką. • Perkelti pasirinktus kompiuterius į kitą grupę. • Perkrauti arba išjungti kompiuterį. • Atstatyti KDV programinę įrangą. • Atlikti visuotinę arba dalinę sistemų patikrą ieškant failo ar proceso. • Galimybė nustatyti skirtingas saugos politikas bei konkretaus funkcionalumo panaudojimą/diegimą vartotojams, kompiuterinėms	kompiuterinėse darbo vietose ir serveriuose. • Yra galimybė pasirinkti naujinimų diegimo būdą: • Gamintojo naujinimo serverių naudojimas tiesioginiam KDV programinės įrangos ir aprašų atnaujinimams. • Centrinio serverio naudojimas KDV programinės įrangos ir aprašų atnaujinimams. • Yra galimybė pasirinkti naujinimų diegimo politiką: • Automatinis arba pagal administratoriaus nurodymą, visiems vartotojams/serveriams/kompiuterinėms darbo vietoms arba jų grupėms. • Nustatyti naujinimų diegimų periodiškumą ir pageidaujamą paros laiką. • Yra galimybė sistemos administratoriui nuotoliniu būdu atlikti veiksmus visiems arba daliai vartotojų, kompiuterinių darbo vietų ar serverių: • Paleisti priverstinį atnaujinimą. • Paleisti pilną arba dalinį sistemos skenavimą. • Pritaikyti nustatytąją saugumo politiką. • Perkelti pasirinktus kompiuterius į kitą grupę. • Perkrauti arba išjungti kompiuterį. • Atstatyti KDV programinę įrangą. • Atlikti visuotinę arba dalinę sistemų patikrą ieškant failo ar proceso. • Galimybė nustatyti skirtingas saugos politikas bei konkretaus funkcionalumo panaudojimą/diegimą vartotojams, kompiuterinėms darbo vietoms, serveriams ar jų grupėms.

		darbo vietoms, serveriams ar jų grupėms. • Integracija su Microsoft Active Directory, galimybė kurti politika ir atlikti visus administracinius veiksmus direktorijos vartotojams ir jų grupėms. Nuolatinė direktorijos sinchronizacija.	Integracija su Microsoft Active Directory, galimybė kurti politika ir atlikti visus administracinius veiksmus direktorijos vartotojams ir jų grupėms. Nuolatinė direktorijos sinchronizacija.
Įvykių surinkimo ir analizės funkcionalumas			
15.	Įvykių kaupimo ir analizės funkcionalumas	• Turi būti galimybė kaupti įvykius centriniame serveryje. • Galimybė peržiūrėti įvykių įrašus (logs), bei analizuoti atskirus įvykius, įvykius filtruoti pagal pageidaujamus laukus ir norimą informaciją. • Turi būti ataskaitų funkcionalumas, leidžiantis ruošti ataskaitas pagal bet kokią su įrenginiu funkcionalumu susijusią sukauptą istorinę informaciją, vertinant bet kokius rėžius ir informaciją, įskaitant, bet neapsiribojant, vartotojus, jų grupes, įrenginius, aptiktas grėsmes, lankytas svetaines, incidentus ir pan.	• Galimybė kaupti įvykius centriniame serveryje. • Galimybė peržiūrėti įvykių įrašus (logs), bei analizuoti atskirus įvykius, įvykius filtruoti pagal pageidaujamus laukus ir norimą informaciją. Yra ataskaitų funkcionalumas, leidžiantis ruošti ataskaitas pagal bet kokią su įrenginiu funkcionalumu susijusią sukauptą istorinę informaciją, vertinant bet kokius rėžius ir informaciją, įskaitant, bet neapsiribojant, vartotojus, jų grupes, įrenginius, aptiktas grėsmes, lankytas svetaines, incidentus ir pan.
16.	Grėsmių aptikimo ir analizės funkcionalumas	• Turi būti grėsmių aptikimo funkcionalumas. Funkcionalumas turi veikti visu įrenginio garantiniu laikotarpiu be papildomo mokesčio. • Įvykių koreliavimo funkcionalumas aptinkant grėsmes ir incidentus. • Automatizuotas administratorių informavimas apie grėsmes ir incidentus. • Incidentų ir grėsmių analizės funkcionalumas, pateikiant išsamią informaciją apie įvykį, įgyvendinant konkrečių įvykių paiešką, bei įgalinant administratorių imtis veiksmų sulaikant	• Yra grėsmių aptikimo funkcionalumas. Funkcionalumas turi veikti visu įrenginio garantiniu laikotarpiu be papildomo mokesčio. • Įvykių koreliavimo funkcionalumas aptinkant grėsmes ir incidentus. • Automatizuotas administratorių informavimas apie grėsmes ir incidentus. • Incidentų ir grėsmių analizės funkcionalumas, pateikiant išsamią informaciją apie įvykį, įgyvendinant konkrečių įvykių paiešką, bei įgalinant administratorių imtis veiksmų sulaikant grėsmes bei stabdant incidentus.

		grėsmes bei stabdant incidentus. • Informacijos iš valdomų įrenginių ugniasienės, IPS, antivirusinės srauto kontrolės, bot aptikimo, failų emuliavimo, URL filtravimo ir aplikacijų kontrolės modulių surinkimo funkcionalumas.	Informacijos iš valdomų įrenginių ugniasienės, IPS, antivirusinės srauto kontrolės, bot aptikimo, failų emuliavimo, URL filtravimo ir aplikacijų kontrolės modulių surinkimo funkcionalumas.
17.	Našumas	• Ne mažiau 2000 indeksuojamų įvykių per sekundę. • Ne mažiau 10 GB įvykių per dieną.	• 2000 indeksuojamų įvykių per sekundę. 10 GB įvykių per dieną.
Reikalavimai ugniasienei			
18.	Įranga turi būti montuojama į 19 colių spintą	Visos reikalingos montavimui dalys turi būti pateiktos su įranga	Visos reikalingos montavimui dalys pateikiamos su įranga
19.	Įrangos aukštis	Ne daugiau 1 U	1 U
20.	Įrangos maitinimas	100 – 240 V, 50 – 60 Hz	100 – 240 V, 50 – 60 Hz
21.	Maitinimo šaltiniai	Vienas maitinimo šaltinis.	Vienas maitinimo šaltinis.
22.	Prievadai	• Ne mažiau 8 vnt. 1GE RJ-45 prievadų. • Ne mažiau vieno RJ-45 prievado skirto valdymui. • Ne mažiau vieno RJ-45 prievado skirto sinchronizacijai tarp įrenginių aukšto patikimumo poroje. • Ne mažiau dviejų USB prievadų. Ne mažiau vieno console tipo prievado.	• 8 vnt. 1GE RJ-45 prievadų. • vienas RJ-45 prievadas skirtas valdymui. • vienas RJ-45 prievadas skirtas sinchronizacijai tarp įrenginių aukšto patikimumo poroje. • du USB prievadai. Vienas console tipo prievadas.
23.	Vidinė atmintis	Ne mažiau 900 GB.	900 GB.
24.	Ugniasienės pralaidumas	Ne mažiau 20 Gbps 1518 baitų dydžio UDP paketais. Ne mažiau 10 Gbps su realiu tinklo srautu.	20 Gbps 1518 baitų dydžio UDP paketais. 10 Gbps su realiu tinklo srautu.
25.	IPSec VPN pralaidumas	Ne mažiau 2 Gbps.	2 Gbps.

26.	Apsaugos nuo įsilaužimų pralaidumas (IPS) HTTP srautui	Ne mažiau 3.5 Gbps su realiu tinklo srautu.	3.5 Gbps su realiu tinklo srautu.
27.	Bendras IPS bei Aplikacijų kontrolės pralaidumas (NGFW)	Ne mažiau 3 Gbps su realiu tinklo srautu.	3 Gbps su realiu tinklo srautu.
28.	Bendras ugniasienės, aplikacijų kontrolės, URL filtravimo, IPS, antivirusinio srauto filtravimo, bot‘ų aptikimo pralaidumas	Me mažiau 900 Mbps su realiu srautu.	900 Mbps su realiu srautu.
29.	Sesijų skaičius	Ne mažiau 6 Milijonų.	6 Milijonai.
30.	Naujų sesijų skaičius per sekundę	Ne mažiau 145 000.	145 000.
31.	Ugniasienės našumo skaičiavimo metodika ir vertinimas	Realus tinklo srautas turi atitikti šias sąlygas ir konfigūraciją: • Srauto sandara: o ~90% įvairaus WEB srauto (iš jų iki 40% jpg, iki 20% kiti duomenys, iki 30% video srauto). o ~5% DNS srauto. o ~5% kiti protokolai (SMTP, FTP, POP3 ir pan.) • Skirtingo dydžio paketai atitinkantys realias sąlygas. • Įjungtas įvykių įrašymas. • Įjungtas saugumo funkcionalumas (Ugniasienė, Įsilaužimų prevencija (IPS), Aplikacijų ir URL kontrolė,	Realus tinklo srautas atitinka šias sąlygas ir konfigūraciją: • Srauto sandara: o ~90% įvairaus WEB srauto (iš jų iki 40% jpg, iki 20% kiti duomenys, iki 30% video srauto). o ~5% DNS srauto. o ~5% kiti protokolai (SMTP, FTP, POP3 ir pan.) • Skirtingo dydžio paketai atitinkantys realias sąlygas. • Įjungtas įvykių įrašymas. • Įjungtas saugumo funkcionalumas (Ugniasienė, Įsilaužimų prevencija (IPS), Aplikacijų ir URL kontrolė,

		antivirusinis srauto filtravimas, bot‘ų aptikimas). Ugniasienės našumo parametrai turi būti skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą.	antivirusinis srauto filtravimas, bot‘ų aptikimas). Ugniasienės našumo parametrai skaičiuojami nenaudojant ugniasienių funkcijos ir konfigūracijų, įjungiančių tik dalies sesijos paketų, ar dalies sesijų patikrą.
32.	Sistemos virtualizavimas	Turi būti galimybė praplėsti funkcionalumą padalinant įrenginį į 10 virtualių įrenginių. Virtualūs įrenginiai turi užtikrinti pilną valdymo, politikų izoliavimą, bei galimybę riboti virtualaus įrenginio resursų išnaudojimą. Funkcionalumas gali būti įgyvendinamas su atskira licencija, į pasiūlymą įtraukti nereikia.	Yra galimybė praplėsti funkcionalumą padalinant įrenginį į 10 virtualių įrenginių. Virtualūs įrenginiai užtikrina pilną valdymo, politikų izoliavimą, bei galimybę riboti virtualaus įrenginio resursų išnaudojimą. Funkcionalumas įgyvendinamas su atskira licencija
33.	Vartotojų skaičius	Neribotas	Neribotas
34.	Darbo režimai	• Skaidrus (L2); • Maršrutizavimo (L3); Stebėjimo (*monitoring*), prijungus prie tinklo šliuzo SPAN prievado.	• Skaidrus (L2); • Maršrutizavimo (L3); Stebėjimo (*monitoring*), prijungus prie tinklo šliuzo SPAN prievado.
35.	Tinklo funkcionalumas	▪ Ne mažiau 1024 VLAN palaikymas. ▪ 802.3ad ryšių apjungimo (angl. „*link aggregation*“) funkcionalumo palaikymas. ▪ *Layer 2* ir *Layer 3* maršrutizavimo funkcionalumas. DHCP funkcionalumo (serverio/kliento) palaikymas.	▪ 1024 VLAN palaikymas. ▪ 802.3ad ryšių apjungimo (angl. „*link aggregation*“) funkcionalumo palaikymas. ▪ *Layer 2* ir *Layer 3* maršrutizavimo funkcionalumas. DHCP funkcionalumo (serverio/kliento) palaikymas.
36.	Unicast ir Multicast maršurizavimas	• OSPFv2 ir v3 protokolų palaikymas. • BGP palaikymas. • RIP palaikymas. • Statinis maršrutizavimas, multicast maršrutizavimas, maršrutizavimas pagal nustatytas taisykles (angl. „policy based“). PIM-SM, IGMP v2 ir v3 protokolų palaikymas.	• OSPFv2 ir v3 protokolų palaikymas. • BGP palaikymas. • RIP palaikymas. • Statinis maršrutizavimas, multicast maršrutizavimas, maršrutizavimas pagal nustatytas taisykles (angl. „policy based“). PIM-SM, IGMP v2 ir v3 protokolų palaikymas.

37.	Tinklo adresų transliavimas (NAT)	Statinio NAT bei PAT palaikymas.	Statinio NAT bei PAT palaikymas.
38.	Valdymas	▪ WEB (HTTP, HTTPS), SSH, konsolė RS-232. ▪ SNMP (*Simple Network Management Protocol*), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ Centralizuoto valdymo palaikymas, saugi komunikacija su centralizuoto valdymo sprendimu. ▪ SNMP (Simple Network Management Protocol), palaikomos versijos 1, 2, 3. Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup).	▪ WEB (HTTP, HTTPS), SSH, konsolė RS-232. ▪ SNMP (*Simple Network Management Protocol*), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ Centralizuoto valdymo palaikymas, saugi komunikacija su centralizuoto valdymo sprendimu. ▪ SNMP (Simple Network Management Protocol), palaikomos versijos 1, 2, 3. Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup).
39.	Sertifikatų palaikymas	▪ Pasirašytų sertifikatų importavimas ir naudojamų sertifikatų eksportavimas (PKCS #12). Vidinės bei išorinės sertifikatų išdavimo *paslaugos (angl. Certificate authority)* išduotų sertifikatų palaikymas.	▪ Pasirašytų sertifikatų importavimas ir naudojamų sertifikatų eksportavimas (PKCS #12). Vidinės bei išorinės sertifikatų išdavimo *paslaugos (angl. Certificate authority)* išduotų sertifikatų palaikymas.
40.	Saugos funkcijos	Privalo būti šis funkcionalumas, visos reikiamos licencijos įtrauktos į pasiūlymą: ▪ Ugniasienė ▪ Įsilaužimų prevencija (IPS) ▪ Aplikacijų ir URL kontrolė ▪ Virtualūs privatūs tinklai ▪ Vartotojų atpažinimas ▪ Virusų ir kompiuterių zombių tinklų (BotNet) prevencija ▪ Šifruoto srauto (SSL/TLS) inspektavimas ▪ Failų perdavimo kontrolė El. pašto patikra nuo brukalų ir žalingo kodo	Yra šis funkcionalumas, visos reikiamos licencijos įtrauktos į pasiūlymą: ▪ Ugniasienė ▪ Įsilaužimų prevencija (IPS) ▪ Aplikacijų ir URL kontrolė ▪ Virtualūs privatūs tinklai ▪ Vartotojų atpažinimas ▪ Virusų ir kompiuterių zombių tinklų (BotNet) prevencija ▪ Šifruoto srauto (SSL/TLS) inspektavimas ▪ Failų perdavimo kontrolė El. pašto patikra nuo brukalų ir žalingo kodo
41.	Ugniasienės funkcionalumas	▪ Ugniasienė turi atlikti srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną	▪ Ugniasienė atitinka srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos

		bei jos charakteristikas (angl. *stateful firewall*). ▪ Ugniasienė turi gebėti įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavės). ▪ Turi būti atpažįstama bent 150 iš anksto aprašytų paslaugų ir protokolų. ▪ Ugniasienės taisyklių panaudojimo statistikos atvaizdavimas taisyklių eiliškumo optimizavimui. ▪ Galimybė ugniasienės taisykles taikyti tam tikru laiku (datos, laikas). ▪ HTTP/HTTPS proxy palaikymas. Galimybė aprašyti savo protokolus bei paslaugas.	charakteristikas (angl. *stateful firewall*). ▪ Ugniasienė geba įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavės). ▪ Atpažįstama bent 150 iš anksto aprašytų paslaugų ir protokolų. ▪ Ugniasienės taisyklių panaudojimo statistikos atvaizdavimas taisyklių eiliškumo optimizavimui. ▪ Galimybė ugniasienės taisykles taikyti tam tikru laiku (datos, laikas). ▪ HTTP/HTTPS proxy palaikymas. Galimybė aprašyti savo protokolus bei paslaugas.
42.	Įsilaužimų prevencijos (IPS) funkcionalumas	▪ Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai turi apimti: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas. o Protokolų anomalijų aptikimas. o Aplikacijų anomalijų aptikimas. ▪ Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitąveiką. ▪ Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas ugniasienės apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties). Nustatymas neturi būti įjungtas pagal nutylėjimą. ▪ Darbo režimų taisyklių rinkiniams palaikymas: detektuoti incidentus (IDS),	▪ Įsilaužimų aprašai bei įsilaužimų aptikimo mechanizmai apima: o Bandymų išnaudoti žinomus pažeidžiamumus aptikimas. o Protokolų anomalijų aptikimas. o Aplikacijų anomalijų aptikimas. ▪ Skirtingų IPS taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greita ▪ +veiką. ▪ Galimybė išjungti IPS apsaugą viršijus administratoriaus nustatytas ugniasienės apkrovos ribas (procesoriaus(ų) bei operatyviosios atminties). Nustatymas neturi būti įjungtas pagal nutylėjimą. ▪ Darbo režimų taisyklių rinkiniams palaikymas:

		blokuoti su incidentu susijusią komunikaciją (IPS). ▪ Galimybė įrašyti su incidentu susijusius paketus suveikus IPS taisyklėms. ▪ IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas.	detektuoti incidentus (IDS), blokuoti su incidentu susijusią komunikaciją (IPS). ▪ Galimybė įrašyti su incidentu susijusius paketus suveikus IPS taisyklėms. ▪ IPS aprašų ir mechanizmų aprašymas naudojant įprastas sintakses (pvz.: SNORT sintaksę). Srautų blokavimas pagal šalį, automatinis šalių IP adresų rėžių atpažinimas.
43.	Aplikacijų ir URL kontrolė	▪ Galimybė kurti aplikacijų ir URL taisykles naudojant kelias kategorijas vienoje taisyklėje. ▪ Skirtingų URL, aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms, URL, arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidujamos aplikacijos, URL naudojimą. ▪ Mechanizmas nepageidaujamų aplikacijų ir URL naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ar URL ribojimą. ▪ Aplikacijų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis aplikacijų aprašų atnaujinimas. Galimybė aprašyti savo aplikacijas.	▪ Galimybė kurti aplikacijų ir URL taisykles naudojant kelias kategorijas vienoje taisyklėje. ▪ Skirtingų URL, aplikacijų bei jų kategorijų taisyklių pritaikymas vartotojams bei jų grupėms. ▪ Galimybė taikyti skirtingus veiksmus nepageidaujamoms aplikacijoms, URL, arba jų grupėms/kategorijoms: o blokuoti, o informuoti vartotojus apie nepageidaujamos aplikacijos, URL naudojimą. ▪ Mechanizmas nepageidaujamų aplikacijų ir URL naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką. ▪ Galimybė sukurti šabloną vartotojo informavimui apie aplikacijos ar URL ribojimą. ▪ Aplikacijų atpažinimas bei ribojimas, nepriklausomai nuo naudojamų prievadų bei kitų tinklo parametrų. ▪ Automatinis aplikacijų aprašų atnaujinimas. Galimybė aprašyti savo aplikacijas.
44.	Virtualūs privatūs tinklai (VPN)	▪ Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. *certificate authority*). ▪ IPSEC protokolo palaikymas.	▪ Galimybė naudoti vidinę arba išorinę sertifikatų išdavimo paslaugą (angl. *certificate authority*). ▪ IPSEC protokolo palaikymas.

		▪ DES, 3DES, CAST AES128, AES256 kriptavimo standartų palaikymas. ▪ MD5, SHA1, SHA256, SHA384 duomenų vientisumo patikros algoritmų palaikymas. ▪ Diffie-Hellman grupių palaikymas: o Group 1 (768 bitų), o Group 2 (1024 bitų), o Group 5 (1536 bitų), o Group 14 (2048 bitų), o Group 19, o Group 20. • Palaikoms virtualių privačių tinklų topologijos: o Tinklelis (visi taškai užmezga VPN tunelius su visais). o Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais). o Kelių centrinių taškų palaikymas, užmezgant VPN tunelį su: ▪ arčiausiai esančiu centriniu tašku; ▪ pagal nustatytą prioritetą; ▪ balansuojant VPN tinklo apkrovą. ▪ aukšto patikimumo užtikrinimas naudojant kelis centrinius taškus. • Galimybė nustatyti VPN tunelių būvį: o tuneliai užmezgami pagal poreikį, vykstat komunikacijai su nutolusiu tašku,	▪ DES, 3DES, CAST AES128, AES256 kriptavimo standartų palaikymas. ▪ MD5, SHA1, SHA256, SHA384 duomenų vientisumo patikros algoritmų palaikymas. ▪ Diffie-Hellman grupių palaikymas: o Group 1 (768 bitų), o Group 2 (1024 bitų), o Group 5 (1536 bitų), o Group 14 (2048 bitų), o Group 19, o Group 20. • Palaikomos virtualių privačių tinklų topologijos: o Tinklelis (visi taškai užmezga VPN tunelius su visais). o Žvaigždė (nutolę taškai užmezga VPN tunelius su centriniais taškais). o Kelių centrinių taškų palaikymas, užmezgant VPN tunelį su: ▪ arčiausiai esančiu centriniu tašku; ▪ pagal nustatytą prioritetą; ▪ balansuojant VPN tinklo apkrovą. ▪ aukšto patikimumo užtikrinimas naudojant kelis centrinius taškus. • Galimybė nustatyti VPN tunelių būvį: o tuneliai užmezgami pagal poreikį, vykstat komunikacijai su nutolusiu tašku, panaikinami po nustatyto laiko. statiniai tuneliai, atnaujinami nustatytu periodiškumu.

		panaikinami po nustatyto laiko. statiniai tuneliai, atnaujinami nustatytu periodiškumu.	
45.	Vartotojų atpažinimo funkcionalumas	▪ Galimybė atpažinti bei autentifikuoti vartotojus. ▪ Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP. ▪ Galimybė kurti vartotojų duomenų bazę ugniasienėje. ▪ Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų grupių atpažinimas bei taisyklių grupėms pritaikymas. Galimybė atpažinti vartotojus virtualių darbo vietų sprendimuose (Citrix, Microsoft, VMWare), bei skirtingus vartotojus Microsoft Terminaliniuose serveriuose. Funkcionalumas gali būti įgyvendintas naudojant klientinę programinę įrangą.	▪ Galimybė atpažinti bei autentifikuoti vartotojus. ▪ Autentifikacija naudojant RADIUS mechanizmą, skaitmeninius sertifikatus, LDAP. ▪ Galimybė kurti vartotojų duomenų bazę ugniasienėje. ▪ Microsoft Active Directory palaikymas vartotojų autentifikacijai, vartotojų srautų atpažinimui bei taisyklių pritaikymui. Vartotojų grupių atpažinimas bei taisyklių grupėms pritaikymas. Galimybė atpažinti vartotojus virtualių darbo vietų sprendimuose (Citrix, Microsoft, VMWare), bei skirtingus vartotojus Microsoft Terminaliniuose serveriuose. Funkcionalumas gali būti įgyvendintas naudojant klientinę programinę įrangą.
46.	Virusų ir kompiuterių zombių tinklų (BotNet) prevencijos funkcionalumas	▪ BotNet žalingos komunikacijos identifikavimas ir blokavimas pagal žinomų žalingų IP adresų ir domenų aprašus, generuojamų duomenų srautų charakteristikas. ▪ Žalingo kodo aptikimas bei prevencija duomenų srautuose. ▪ Virusų komunikacijos (savireplikacijos, komunikavimo su centrinio valdymo pultu) prevencija. ▪ DNS tuneliavimo atakų prevencija. ▪ Prieigos prie užkrėstų svetainių prevencija. Skirtingų taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.),	▪ BotNet žalingos komunikacijos identifikavimas ir blokavimas pagal žinomų žalingų IP adresų ir domenų aprašus, generuojamų duomenų srautų charakteristikas. ▪ Žalingo kodo aptikimas bei prevencija duomenų srautuose. ▪ Virusų komunikacijos (savireplikacijos, komunikavimo su centrinio valdymo pultu) prevencija. ▪ DNS tuneliavimo atakų prevencija. ▪ Prieigos prie užkrėstų svetainių prevencija. Skirtingų taisyklių ir metodikų rinkinių taikymas skirtingiems tinklo objektams (potinkliams, IP adresų rėžiams, serveriams ir pan.), optimizuojant ugniasienės greitaveiką.

		optimizuojant ugniasienės greitąveiką.	
47.	Nežinomų grėsmių aptikimo (angl. sandboxing) funkcionalumas	▪ Turi būti ateityje įgyvendinti nežinomų grėsmių patikros funkcionalumas, apimantis failų pateikiamą patikrai į nežinomų grėsmių patikros sprendimą. ▪ Failų pateikimas patikrai iš duomenų srauto bei el. laiškų (p. 23). Failų patikrai turi būti naudojamas programinis arba fizinis sprendimas diegiamas Perkančiosios organizacijos duomenų centre.	▪ Turi būti ateityje įgyvendinti nežinomų grėsmių patikros funkcionalumas, apimantis failų pateikiamą patikrai į nežinomų grėsmių patikros sprendimą. ▪ Failų pateikimas patikrai iš duomenų srauto bei el. laiškų (p. 23). Failų patikrai yra naudojamas programinis arba fizinis sprendimas diegiamas Perkančiosios organizacijos duomenų centre.
48.	El. pašto apsauga	▪ El. pašto apsauga nuo brukalų, žalingų priedų (angl. *attachment*), bei žalingų nuorodų. Galimybė pateikti el. laiškų priedus patikrai pagal p. 21 nustatytą funkcionalumą.	▪ El. pašto apsauga nuo brukalų, žalingų priedų (angl. *attachment*), bei žalingų nuorodų. Galimybė pateikti el. laiškų priedus patikrai pagal p. 21 nustatytą funkcionalumą.
49.	Šifruoto srauto (SSL/TLS) inspektavimas	▪ Šifruoto SSL ir TLS srauto dekriptavimas ir patikra. ▪ Šifruoto srauto patikra turi įgyvendinti visas reikalavimuose išvardintas saugos funkcijas. ▪ *Perfect Forward Secrecy* palaikymas. AES-NI procesoriaus instrukcijų naudojimas šifravimo operacijoms (jeigu palaiko hipervizorius ir naudojamo serverio procesorius).	▪ Šifruoto SSL ir TLS srauto dekriptavimas ir patikra. ▪ Šifruoto srauto patikra įgyvendina visas reikalavimuose išvardintas saugos funkcijas. ▪ *Perfect Forward Secrecy* palaikymas. AES-NI procesoriaus instrukcijų naudojimas šifravimo operacijoms (jeigu palaiko hipervizorius ir naudojamo serverio procesorius).
50.	Failų perdavimo kontrolė	• HTTPS, SMTP ir FTP protokolais perduodamų bylų aptikimas ir kontrolė. • Galimybė kontroliuoti perduodamus failų tipus, blokuoti nepageidaujamų failų tipų perdavimą. Galimybė kontroliuoti failų turinį pagal raktažodžius arba duomenų formatus, duomenų nutekėjimo ar jautrių duomenų perdavimo prevencijai.	• HTTPS, SMTP ir FTP protokolais perduodamų bylų aptikimas ir kontrolė. • Galimybė kontroliuoti perduodamus failų tipus, blokuoti nepageidaujamų failų tipų perdavimą. Galimybė kontroliuoti failų turinį pagal raktažodžius arba duomenų formatus, duomenų nutekėjimo ar jautrių duomenų perdavimo prevencijai.
51.	Žurnalinių įrašų kaupimas	Įvykių žurnalai turi būti kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Turi būti generuojami žurnaliniai įvykiai, susiję su ugniasienės	Įvykių žurnalai kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Generuojami žurnaliniai įvykiai, susiję su ugniasienės funkcionalumu ir

		funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan.	susiejami su konkrečiais IP adresais, vartotojais ir pan.
52.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Yra. Nemokamai garantinio aptarnavimo laikotarpiu
53.	Atnaujinimai pagal nustatyta grafiką (Shedule)	Turi būti	Yra
Reikalavimai darbo vietų saugos sprendimui			
54.	Darbo vietų kiekis	200 darbo vietų ir serverių	200 darbo vietų ir serverių
55.	Programinės įrangos paskirtis	Darbo vietų ir tarnybinių stočių apsaugos nuo grėsmių programinė įranga (toliau – "KDV programinė įranga").	Darbo vietų ir tarnybinių stočių apsaugos nuo grėsmių programinė įranga (toliau – "KDV programinė įranga").
56.	Specifikacija	Nurodyti sprendimo pavadinimą, produkto ir visų sudedamųjų licencijų gamintojo produktų kodus. Pateikti trumpą aprašymą ką kiekviena licencija ar komponentas suteikia ir kaip atitinka reikalavimus. Pateikti tikslią nuorodą į gamintojo interneto puslapį, kuriame pateikta visa informacija apie siūlomą sprendimą.	SandBlast Agent Next Generation AV - Advanced threat protection and automated endpoint forensic analysis for all malware types CPEP-SBA-NGAV Pateikiama tiksli nuoroda į gamintojo interneto puslapį, kuriame pateikta visa informacija apie siūlomą sprendimą: https://www.checkpoint.com/products/advanced-endpoint-protection/
57.	Programinės įrangos diegimas	Turi palaikyti Windows 7, 8, 10, Windows Server 2008 R2, 2012, 2012 R2, 2016 operacines sistemas.	Palaiko Windows 7, 8, 10, Windows Server 2008 R2, 2012, 2012 R2, 2016 operacines sistemas.
58.	Apsaugos nuo grėsmių funkcionalumas	Turi turėti tokias integruotas funkcijas: • Apsaugą nuo žinomų grėsmių/žalingo kodo. • Apsaugą nuo nežinomų grėsmių (grėsmių emuliavimas). • Apsaugą nuo ransomware tipo duomenis užkoduojančių virusų. • Apsaugą nuo pažeidžiamumų išnaudojimo grėsmių (angl. Exploit). • Apsaugą nuo elektroninio sukčiavimo (Phishing).	Turi tokias integruotas funkcijas: • Apsaugą nuo žinomų grėsmių/žalingo kodo. • Apsaugą nuo nežinomų grėsmių (grėsmių emuliavimas). • Apsaugą nuo ransomware tipo duomenis užkoduojančių virusų. • Apsaugą nuo pažeidžiamumų išnaudojimo grėsmių (angl. Exploit). • Apsaugą nuo elektroninio sukčiavimo (Phishing).

		• Organizacijos prisijungimo duomenų naudojimo kontrolę. • Apsaugą nuo botnet tinklų kenkėjiškos programinės įrangos. • Apsaugą nuo grėsmių pagal tipinius žalingo kodo veikimo modelius. Incidentų analizės įrankį.	• Organizacijos prisijungimo duomenų naudojimo kontrolę. • Apsaugą nuo botnet tinklų kenkėjiškos programinės įrangos. • Apsaugą nuo grėsmių pagal tipinius žalingo kodo veikimo modelius. Incidentų analizės įrankį.
59.	Apsaugos nuo žinomų grėsmių/žalingo kodo funkcionalumas	Galimybė aptikti ir blokuoti žinomas grėsmes pagal aprašus (angl. signatures), naudojant euristinę analizę arba veiklos modelio atpažinimą.	Galimybė aptikti ir blokuoti žinomas grėsmes pagal aprašus (angl. signatures), naudojant euristinę analizę arba veiklos modelio atpažinimą.
60.	Apsaugos nuo nežinomų grėsmių (grėsmių emuliavimas) funkcionalumas	• Failų (atsiunčiamų, įrašomų, kopijuojamų ir pan.) patikra išoriniame grėsmių emuliavimo sprendime. • Patikra turi būti įgyvendinama aktyvinant failus skirtingose saugiose virtualiose operacinėse sistemose (Windows 7, 8, 10), naudojant skirtingų versijų PĮ paketus (pvz.: skirtingas MS Office versijas). • Patikros metu turi būti vertinama failų veikla susijusi su failinėmis sistemomis, registrais, procesais arba mezgamomis tinklo sesijomis. • CPU lygio pažeidžiamumų panaudojimo atpažinimas (pvz.: Return Oriented Programming). • Aptikus grėsmę faile, jo tolimesnis naudojimas turi būti blokuojamas, o pakartotinis failo patekimas Perkančiosios organizacijos kompiuterinėse darbo vietose ir serveriuose turi būti blokuojamas automatiškai. • Programinė įrangos licencija turi apimti emuliavimą sprendimo gamintojo debesų kompiuterijos	• Failų (atsiunčiamų, įrašomų, kopijuojamų ir pan.) patikra išoriniame grėsmių emuliavimo sprendime. • Patikra turi būti įgyvendinama aktyvinant failus skirtingose saugiose virtualiose operacinėse sistemose (Windows 7, 8, 10), naudojant skirtingų versijų PĮ paketus (pvz.: skirtingas MS Office versijas). • Patikros metu vertinama failų veikla susijusi su failinėmis sistemomis, registrais, procesais arba mezgamomis tinklo sesijomis. • CPU lygio pažeidžiamumų panaudojimo atpažinimas (pvz.: Return Oriented Programming). • Aptikus grėsmę faile, jo tolimesnis naudojimas yra blokuojamas, o pakartotinis failo patekimas Perkančiosios organizacijos kompiuterinėse darbo vietose ir serveriuose turi būti blokuojamas automatiškai. • Programinė įrangos licencija apima emuliavimą sprendimo gamintojo debesų kompiuterijos infrastruktūroje. Grėsmių emuliavimo sprendimas nėra ribotas failų

		infrastruktūroje. Grėsmių emuliavimo sprendimas neturi būti ribotas failų kiekiu per laiką, failų dydžiu ar pan. Turi būti atliekama šių failų tipų analizė: .bz2, .CAB, .csv, .com, .cpl, .dmg, .doc, .docx, .dot, .dotx, .dotm, .docm, .dylib, .exe, .gz, .hwp, .iso, .iqy, .jar, .js, .o, .PIF, .pdf, .pkg, .ppt, .pptx, .pps, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .ps1, .rar, .rtf, .scr, .Seven-Z, .sldx, .sldm, .slk, .swf, .tar, .tbz2, .tbz, .tb2, .tgz, .xlt, .xls, .xlsx, .xlm, .xltx, .xlsm, .xltm, .xlsb, .xla, .xlam, .xll, .xlw, .xz, .zip.	kiekiu per laiką, failų dydžiu ar pan. Turi būti atliekama šių failų tipų analizė: .bz2, .CAB, .csv, .com, .cpl, .dmg, .doc, .docx, .dot, .dotx, .dotm, .docm, .dylib, .exe, .gz, .hwp, .iso, .iqy, .jar, .js, .o, .PIF, .pdf, .pkg, .ppt, .pptx, .pps, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .ps1, .rar, .rtf, .scr, .Seven-Z, .sldx, .sldm, .slk, .swf, .tar, .tbz2, .tbz, .tb2, .tgz, .xlt, .xls, .xlsx, .xlm, .xltx, .xlsm, .xltm, .xlsb, .xla, .xlam, .xll, .xlw, .xz, .zip.
61.	Apsaugos nuo ransomware tipo duomenis užkoduojančių virusų funkcionalumas	• Apsauga nuo žinomų ir nežinomų ransomware tipo virusų. • Ransomware tipo virusų atpažinimas pagal veiklos modelius. Galimybė atstatyti iki aptikimo užkoduotus failus.	• Apsauga nuo žinomų ir nežinomų ransomware tipo virusų. • Ransomware tipo virusų atpažinimas pagal veiklos modelius. Galimybė atstatyti iki aptikimo užkoduotus failus.
62.	Apsaugos nuo pažeidžiamumų išnaudojimo grėsmių (angl. Exploit) funkcionalumas	• Apsauga nuo programinės įrangos pažeidžiamumų išnaudojimo. Galimybė automatiškai išjungti programinę įrangą, kurios pažeidžiamumus bandoma išnaudoti.	• Apsauga nuo programinės įrangos pažeidžiamumų išnaudojimo. Galimybė automatiškai išjungti programinę įrangą, kurios pažeidžiamumus bandoma išnaudoti.
63.	Apsaugos nuo elektroninio sukčiavimo (Phishing) funkcionalumas	• Apsauga nuo žinomų ir nežinomų elektroninio sukčiavimo svetainių ir jų turinio. • Nežinomų elektroninio sukčiavimo svetainių aptikimas pagal: IP ir domeno reputaciją, pateikiamų duomenų (URL, teksto, išvaizdos URL) panašumus su žinomomis svetainėmis. Duomenų įvesties blokavimas įtartinoms ir žinomoms elektroninio sukčiavimo svetainėms.	• Apsauga nuo žinomų ir nežinomų elektroninio sukčiavimo svetainių ir jų turinio. • Nežinomų elektroninio sukčiavimo svetainių aptikimas pagal: IP ir domeno reputaciją, pateikiamų duomenų (URL, teksto, išvaizdos URL) panašumus su žinomomis svetainėmis. Duomenų įvesties blokavimas įtartinoms ir žinomoms elektroninio sukčiavimo svetainėms.

64.	Organizacijos prisijungimo duomenų naudojimo kontrolės funkcionalumas.	Galimybė analizuoti organizacijos vartotojų naudojamus prisijungimo duomenis, bei blokuoti organizacijos sistemų prisijungimo duomenų panaudojimą trečiųjų šalių svetainėse ir aplikacijose.	Galimybė analizuoti organizacijos vartotojų naudojamus prisijungimo duomenis, bei blokuoti organizacijos sistemų prisijungimo duomenų panaudojimą trečiųjų šalių svetainėse ir aplikacijose.
65.	Apsaugos nuo botnet tinklų kenkėjiškos programinės įrangos funkcionalumas	Žinomų ir nežinomų botnet tinklų kenkėjiškos programinės įrangos aptikimas pagal veiklos požymus, ir jos blokavimas.	Žinomų ir nežinomų botnet tinklų kenkėjiškos programinės įrangos aptikimas pagal veiklos požymius, ir jos blokavimas.
66.	Apsaugos nuo grėsmių pagal tipinius žalingo kodo veikimo modelius funkcionalumas	• Grėsmių aptikimas, klasifikavimas bei blokavimas pagal veikimo modelius. Žalingų rašmenų (angl. Script) aptikimas ir blokavimas.	• Grėsmių aptikimas, klasifikavimas bei blokavimas pagal veikimo modelius. Žalingų rašmenų (angl. Script) aptikimas ir blokavimas.
67.	Incidentų analizės įrankio funkcionalumas	• Galimybė aprašyti savo incidentų aprašus (angl. IoC, indicators of compromise). • Galimybė po incidento nustatyti žalą (duomenų nutekėjimą, užšifruotus duomenis, įvesties duomenų fiksavimo atvejus ir pan.). • Galimybė atsekti visą incidento eigą, nuo ištakų ir priežasčių iki pasekmių. Galimybė incidento eigą atvaizduoti grafiškai.	• Galimybė aprašyti savo incidentų aprašus (angl. IoC, indicators of compromise). • Galimybė po incidento nustatyti žalą (duomenų nutekėjimą, užšifruotus duomenis, įvesties duomenų fiksavimo atvejus ir pan.). • Galimybė atsekti visą incidento eigą, nuo ištakų ir priežasčių iki pasekmių. Galimybė incidento eigą atvaizduoti grafiškai.
68.	Licencijų terminas	Licencijos turi galioti visą sutarties galiojimo laikotarpį.	Licencijos galioja visą sutarties galiojimo laikotarpį.
69.	Garantiniai įsipareigojimai	Tiesioginis gamintojo 36 mėn. nemokamas aptarnavimas. Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. Siūlomo sprendimo gamintojo licencijų galiojimo laikotarpiu turi užtikrinti teisę be papildomo	Tiesioginis gamintojo 36 mėn. nemokamas aptarnavimas. Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos.

		mokesčio operatyviai gauti naujausius virusų aprašus (signature), virusų paieškos mechanizmo (engine) atnaujinimus bei naujausias programinės įrangos versijas, naudotis grėsmių emuliavimo debesų kompiuterijos infrastruktūra, gauti prieigą prie gamintojo žinių bazės. Turi būti teikiama programinės įrangos gamintojo techninio palaikymo paslauga darbo dienomis, darbo metu el. paštu, telefonu ar per serviso WEB sistemą anglų kalba. Paslaugos teikėjas priežiūros paslaugas privalės teikti perkančiosios organizacijos buveinėje: Breslaujos g. 3, Kaunas. Jeigu sutarties galiojimo metu perkančiojoje organizacijoje atsiranda padaliniai kitais adresas, tiekėjas juose taip pat turi užtikrinti paslaugų teikimą. Teikėjas turi skirti ne mažiau nei 2 kvalifikuotus specialistus diegti ir priežiūros paslaugas teikti siūlomo gamintojo sprendimui. Pateikiami galiojantys gamintojo išduoti sertifikatai įrodantys kvalifikaciją. Sutrikimus tiekėjas privalo reaguoti per 15 min. Sutrikimai turi būti pašalinti per vieną valandą nuo jos įregistravimo.	Siūlomo sprendimo gamintojo licencijų galiojimo laikotarpiu užtikrina teisę be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (signature), virusų paieškos mechanizmo (engine) atnaujinimus bei naujausias programinės įrangos versijas, naudotis grėsmių emuliavimo debesų kompiuterijos infrastruktūra, gauti prieigą prie gamintojo žinių bazės. Teikiama programinės įrangos gamintojo techninio palaikymo paslauga darbo dienomis, darbo metu el. paštu, telefonu ar per serviso WEB sistemą anglų kalba. Paslaugos teikėjas priežiūros paslaugas teiks perkančiosios organizacijos buveinėje: Breslaujos g. 3, Kaunas. Jeigu sutarties galiojimo metu perkančiojoje organizacijoje atsiranda padaliniai kitais adresas, tiekėjas juose taip pat turi užtikrinti paslaugų teikimą. Teikėjas skiria 2 kvalifikuotus specialistus diegti ir priežiūros paslaugas teikti siūlomo gamintojo sprendimui. Pateikiami galiojantys gamintojo išduoti sertifikatai įrodantys kvalifikaciją. Sutrikimus tiekėjas reaguoja per 15 min. Sutrikimai pašalinti per vieną valandą nuo jos įregistravimo.