CENTRALIZUOTO VALDYMO IR ŽURNALINIŲ ĮVYKIŲ REGISTRAVIMO, SAUGOJIMO IR ANALIZĖS SISTEMA
TECHNINĖ SPECIFIKACIJA

Nr.	Specifikacija	Reikalavimai	Tiekėjo siūloma *(pildo tiekėjas)*
1.	Įrangos pavadinimas	–	Quantum Force 3970 Security Gateway
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.	Valdymas	• Sprendimas turi būti valdomas per grafinę sąsają. • Turi būti galimybė sukurti kelių administratorių paskyras, suteikiant skirtingą prieigos lygį. • Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba. • Turi būti galimybė smulkiai apibrėžti administratoriaus teises pvz.: o teisė keisti sisteminius įrenginio nustatymus; o teisė kurti, keisti saugumo taisykles; o teisė kurti, keisti taisyklių objektus; o teisė konfigūruoti saugumo patikrų nustatymus;	• Sprendimas yra valdomas per grafinę sąsają. • Yra galimybė sukurti kelių administratorių paskyras, suteikiant skirtingą prieigos lygį. • Administratorių prieigos teisės yra kontroliuojamos rolių pagalba. • Yra galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; • teisė generuoti ataskaitas.

		○ teisė peržiūrėti įvykių žurnalus; ○ teisė peržiūrėti ataskaitas; ○ teisė generuoti ataskaitas. • Turi būti galimybė vienu metu jungtis ir pokyčius įgyvendinti keliems administratoriams. • Turi veikti mechanizmas įgyvendinantis kelių administratorių įgyvendintų pokyčių patikrą ir suderinamumo vertinimą. • Administratorių įgyvendinami pokyčiai turi būti detaliai išsaugomi, įskaitant pokyčių įgyvendinimo laiką ir veiksmus.	• Yra galimybė vienu metu jungtis ir pokyčius įgyvendinti keliems administratoriams. • Veikia mechanizmas įgyvendinantis kelių administratorių įgyvendintų pokyčių patikrą ir suderinamumo vertinimą. • Administratorių įgyvendinami pokyčiai yra detaliai išsaugomi, įskaitant pokyčių įgyvendinimo laiką ir veiksmus.
Reikalavimai ugniasienės valdymui			
6.	Valdomi įrenginiai	• Siūlomas sprendimas turi gebėti pilnai valdyti siūlomą ugniasienę ir turėti visas reikiamas tam licencijas. • Sprendimas turi be papildomų licencijų leisti valdyti visą sprendimą apimantį ugniasienę ir modulius. • Sprendimas turi būti pilnai suderinamas su siūloma ugniasiene. Siūlant kito gamintojo sprendimą privaloma pateikti oficialų ugniasienės gamintojo patvirtinimą dėl pilno suderinamumo. Suderinamumas turi apimti ir bendrą garantinį aptarnavimą	• Siūlomas sprendimas geba pilnai valdyti siūlomą ugniasienę ir turi visas reikiamas tam licencijas. • Sprendimas be papildomų licencijų leidžia valdyti visą sprendimą apimantį ugniasienę ir modulius. • Sprendimas yra pilnai suderinamas su siūloma ugniasiene. Suderinamumas apima ir bendrą garantinį aptarnavimą
7.	Valdymas	• Sprendimas turi būti valdomas per grafinę sąsają. • Turi būti galimybė sukurti kelių administratorių paskyras, suteikiant skirtingą prieigos lygį. • Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba.	• Sprendimas valdomas per grafinę sąsają. • Yra galimybė sukurti kelių administratorių paskyras, suteikiant skirtingą prieigos lygį. • Administratorių prieigos teisės yra kontroliuojamos rolių pagalba. • Yra galimybė smulkiai apibrėžti administratoriaus teises pvz.:

		• Turi būti galimybė smulkiai apibrėžti administratoriaus teises pvz.:
		  ○ teisė keisti sisteminius įrenginio nustatymus;
		  ○ teisė kurti, keisti saugumo taisykles;
		  ○ teisė kurti, keisti taisyklių objektus;
		  ○ teisė konfigūruoti saugumo patikrų nustatymus;
		  ○ teisė peržiūrėti įvykių žurnalus;
		  ○ teisė peržiūrėti ataskaitas;
		  ○ teisė generuoti ataskaitas.
		• Turi būti galimybė vienu metu jungtis ir pokyčius įgyvendinti keliems administratoriams.
		• Turi veikti mechanizmas įgyvendinantis kelių administratorių įgyvendintų pokyčių patikrą ir suderinamumo vertinimą.
		• Administratorių įgyvendinami pokyčiai turi būti detaliai išsaugomi, įskaitant pokyčių įgyvendinimo laiką ir veiksmus.
			• teisė keisti sisteminius įrenginio nustatymus;
			• teisė kurti, keisti saugumo taisykles;
			• teisė kurti, keisti taisyklių objektus;
			• teisė konfigūruoti saugumo patikrų nustatymus;
			• teisė peržiūrėti įvykių žurnalus;
			• teisė peržiūrėti ataskaitas;
			• teisė generuoti ataskaitas.
			• Yra galimybė vienu metu jungtis ir pokyčius įgyvendinti keliems administratoriams.
			• Turi veikti mechanizmas įgyvendinantis kelių administratorių įgyvendintų pokyčių patikrą ir suderinamumo vertinimą.
			• Administratorių įgyvendinami pokyčiai detaliai išsaugomi, įskaitant pokyčių įgyvendinimo laiką ir veiksmus.

8.	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. • Centralizuotam valdymui turi būti naudojama saugi, šifruota komunikacija su ugniasienėmis.	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. • Centralizuotam valdymui naudojama saugi, šifruota komunikacija su ugniasienėmis.

9.	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.
10.	Stebėjimo funkcionalumas	• Turi būti centralizuoto įrenginių stebėjimo funkcionalumas. • Valdomų įrenginių stebėjimas, tinklo srautų stebėjimas, įtartinos veiklos stebėjimas, VPN tunelių stebėjimas bei automatinis pranešimų administratoriams pateikimas.	• Yra centralizuoto įrenginių stebėjimo funkcionalumas. • Valdomų įrenginių stebėjimas, tinklo srautų stebėjimas, įtartinos veiklos stebėjimas, VPN tunelių stebėjimas bei automatinis pranešimų administratoriams pateikimas.
11.	Žurnalinių įvykių surinkimas ir stebėjimas	• Sprendimas turi kaupti žurnalinius įvykius iš ugniasienės. • 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.	• Sprendimas kaupia žurnalinius įvykius iš ugniasienės. • 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.
12.	Integracija	Sprendimas turi gebėti integruotis per API su kritinės infrastruktūros duomenų tinklo stebėjimo sistema bei: • Priimti duomenis apie atrastus įrenginius, įskaitant: aprašą, IP adresą, gamintoją, tipą, bei šiuos duomenis įkelti į centrinę objektų duomenų bazę. • Priimti duomenis apie atrastus įrenginių pažeidžiamumus, bei pasiūlyti administratoriui įsilaužimo prevencijos	Sprendimas geba integruotis per API su kritinės infrastruktūros duomenų tinklo stebėjimo sistema bei: • Priimti duomenis apie atrastus įrenginius, įskaitant: aprašą, IP adresą, gamintoją, tipą, bei šiuos duomenis įkelti į centrinę objektų duomenų bazę. • Priima duomenis apie atrastus įrenginių pažeidžiamumus, bei pasiūlyti administratoriui įsilaužimo prevencijos taisykles blokuojančius šių pažeidžiamumų išnaudojimą.

		taisykles blokuojančius šių pažeidžiamumų išnaudojimą.	
13.	Žurnalinių įvykių apimtis	• Sprendimas turi priimti ir apdoroti ne mažiau kaip 3 GB žurnalinių įvykių per dieną. • Kaupiamų žurnalinių įvykių apimtis ne mažiau 3 mėn.	• Sprendimas turi priimti ir apdoroti ne mažiau kaip 3 GB žurnalinių įvykių per dieną. • Kaupiamų žurnalinių įvykių apimtis ne mažiau 3 mėn.
Reikalavimai kompiuterinių darbo vietų saugos sprendimo valdymui			
14.	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 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 suteikia 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.
15.	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

		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 darbo vietoms, serveriams ar jų grupėms.	licencijuotuose 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. • Galimybė 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. • Integracija su Microsoft Active Directory, galimybė kurti politika ir atlikti visus

		• Integracija su Microsoft Active Directory, galimybė kurti politika ir atlikti visus administracinius veiksmus direktorijos vartotojams ir jų grupėms. Nuolatinė direktorijos sinchronizacija.	administracinius veiksmus direktorijos vartotojams ir jų grupėms. Nuolatinė direktorijos sinchronizacija.
Įvykių surinkimo ir analizės funkcionalumas			
16.	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.	• Yra 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.
17.	Grėsmių aptikimo ir analizės funkcionalumas	• Turi būti grėsmių aptikimo funkcionalumas. Funkcionalumas turi veikti visos sutarties 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. • Informacijos iš valdomų įrenginių ugniasienės, IPS, antivirusinės srauto kontrolės, bot aptikimo, failų emuliavimo, URL filtravimo ir	• Yra grėsmių aptikimo funkcionalumas. Funkcionalumas veikia visos sutarties 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. • Informacijos iš valdomų įrenginių ugniasienės, IPS, antivirusinės srauto kontrolės, bot aptikimo, failų emuliavimo, URL filtravimo ir aplikacijų

		aplikacijų kontrolės modulių surinkimo funkcionalumas.	kontrolės modulių surinkimo funkcionalumas.
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	Du dubliuojantys maitinimo šaltiniai užtikrinantys aukštą patikimumą.	Du dubliuojantys maitinimo šaltiniai užtikrinantys aukštą patikimumą.
22.	Prievadai	•Ne mažiau 16 vnt. 1GE RJ-45 prievadų. •Ne mažiau dviejų 2.5Gbe RJ-45 prievadų. •Ne mažiau 8 SFP prievadų SFP moduliams įrengti. •Ne mažiau 4 SFP+ prievadų SFP+ moduliams įrengti. •Ne mažiau dviejų USB prievadų. •Ne mažiau vieno console tipo prievado. •Ne mažiau vieno 1GE RJ-45 prievado valdymui ir ne mažiau vieno 1GE RJ45 prievado aukšto patikimumo srauto sinchronizacijai. •Su įrenginiu turi būti pateikti ne mažiau kaip 2 vnt. SFP+ SR optinių modulių skirti duomenis perduoti 850nm šviesos bangos ilgiu daugiamode skaidula ne mažiau kaip 300 metrų atstumu. Optiniai moduliai turi būti to paties gamintojo kaip ir siūlomi ugniasienės moduliai.	• 16 vnt. 1GE RJ-45 prievadų. • 2 vnt. 2.5Gbe RJ-45 prievadų. • 8 SFP prievadų SFP moduliams įrengti. • 4 SFP+ prievadų SFP+ moduliams įrengti. •2 vnt. USB prievadų. •1 vnt. console tipo prievado. •1 vnt. 1GE RJ-45 prievado valdymui ir ne mažiau vieno 1GE RJ45 prievado aukšto patikimumo srauto sinchronizacijai. •Su įrenginiu pateiktiami 2 vnt. SFP+ SR optinių modulių skirti duomenis perduoti 850nm šviesos bangos ilgiu daugiamode skaidula ne mažiau kaip 300 metrų atstumu. Optiniai moduliai to paties gamintojo kaip ir siūlomi ugniasienės moduliai.
23.	Vidinė atmintis	Ne mažiau 480 GB.	480 GB.
24.	Ugniasienės pralaidumas	Ne mažiau 38 Gbps su realiu tinklo srautu.	40 Gbps su realiu tinklo srautu.
25.	IPSec VPN pralaidumas	Ne mažiau 12 Gbps.	13 Gbps.
26.	Apsaugos nuo įsilaužimų pralaidumas (IPS) HTTP srautui	Ne mažiau 17 Gbps su realiu tinklo srautu.	17 Gbps su realiu tinklo srautu.
27.	Bendras IPS bei Aplikacijų kontrolės pralaidumas (NGFW)	Ne mažiau 12 Gbps su realiu tinklo srautu.	12,5 Gbps su realiu tinklo srautu.
28.	Bendras ugniasienės,	Ne mažiau 4 Gbps su realiu tinklo srautu.	4,25 Gbps su realiu tinklo srautu.

	aplikacijų kontrolės, URL filtravimo, IPS, antivirusinio srauto filtravimo, bot‘ų aptikimo pralaidumas		
29.	Sesijų skaičius	Ne mažiau 7 Milijonų.	7,2 Milijonai.
30.	Naujų sesijų skaičius per sekundę	Ne mažiau 135 000.	140 000.
31.	Aukštas patikimumo funkcionalumas	• Galimybė įsigijus antrą tokį pat įrenginį abu įrenginius sujungti aktyvus/aktyvus arba aktyvus/pasyvus režimais veikiančio aukšto patikimumo telkinį. • Aktyvus/pasyvus režimo atveju sugedus vienam įrenginiui, arba nutrūkus ryšiui su vienu iš įrenginių, turi būti išlaikomos aktyvios sesijos. • Aktyvus/aktyvus režimo atveju įrenginiai turi gebėti tolygiai paskirstyti tarpusavyje apkrovą. • VRRP palaikymas.	• Galimybė įsigijus antrą tokį pat įrenginį abu įrenginius sujungti aktyvus/aktyvus arba aktyvus/pasyvus režimais veikiančio aukšto patikimumo telkinį. • Aktyvus/pasyvus režimo atveju sugedus vienam įrenginiui, arba nutrūkus ryšiui su vienu iš įrenginių, yra išlaikomos aktyvios sesijos. • Aktyvus/aktyvus režimo atveju įrenginiai gebatolygiai paskirstyti tarpusavyje apkrovą. • VRRP palaikymas.
32.	Virtualizavimo funkcionalumas	Galimybė ugniasienę padalinti padalinti į 20 virtualių ugniasienių. Funkcionalumas gali veikti su papildoma licencija, kurios į pasiūlymą įtraukti nereikia.	Yra galimybė ugniasienę padalinti į 20 virtualių ugniasienių. Funkcionalumas gali veikti su papildoma licencija, kuri į pasiūlymą neįtraukta.
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. Ne mažiau 4096 VLAN palaikymas naudojant virtualizaciją. ▪ 802.3ad ryšių apjungimo (angl. „*link aggregation*“) funkcionalumo palaikymas. ▪ *Layer 2* ir *Layer 3* maršrutizavimo funkcionalumas.	▪ 1024 VLAN palaikymas. 4096 VLAN palaikymas naudojant virtualizaciją. ▪ 802.3ad ryšių apjungimo (angl. „*link aggregation*“) funkcionalumo palaikymas. ▪ *Layer 2* ir *Layer 3* maršrutizavimo funkcionalumas. ▪ DHCP funkcionalumo (serverio/kliento) palaikymas.

		▪ 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). ▪ SNMP (Simple Network Management Protocol), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ Galimybė eksploatacijos metu perkelti valdymą į debesų kompiuterija pagrįstą valdymo sprendimą. Licenciją ir perkėlimo paslauga turi būti įskaičiuota į pasiūlymo kainą. Valdymui turi būti naudojama ta pati debesų kompiuterijos platforma kaip ir ugniasienių valdymui.	▪ WEB (HTTP, HTTPS), SSH, konsolė RS-232. ▪ SNMP (*Simple Network Management Protocol*), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ SNMP (Simple Network Management Protocol), palaikomos versijos 1, 2, 3. ▪ Galimybė įkelti ir išeksportuoti įrenginio nustatymus (Backup). ▪ Yra galimybė eksploatacijos metu perkelti valdymą į debesų kompiuterija pagrįstą valdymo sprendimą. Licencija ir perkėlimo paslauga yra įskaičiuota į pasiūlymo kainą. Valdymui naudojama ta pati debesų kompiuterijos platforma kaip ir ugniasienių valdymui.
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	Yra šis funkcionalumas, visos reikiamos licencijos įtrauktos į pasiūlymą: ▪ Ugniasienė ▪ Įsilaužimų prevencija (IPS)

		▪ 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 ▪ Nuotolinio prisijungimo funkcionalumas	▪ 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 ▪ Nuotolinio prisijungimo funkcionalumas
41.	Ugniasienės funkcionalumas	▪ Ugniasienė turi atlikti srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos charakteristikas (angl. *stateful firewall*). ▪ Ugniasienė turi gebėti įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavėjas). ▪ 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.	▪ Ugniasienė atlieka srauto kontrolę pagal įvairius paketų parametrus, identifikuojant sesijų būseną bei jos charakteristikas (angl. *stateful firewall*). ▪ Ugniasienė geba įgyvendinti srauto, sesijų kiekio ribojimo funkcijas taisyklėje nurodytoms charakteristikoms (protokolas, aplikacija, paslauga, siuntėjas, gavėjas). ▪ Atpažįstama 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.	▪ 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

		▪ 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), 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.	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), 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 nepageidaujamos aplikacijos, URL naudojimą, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų aplikacijų ir URL naudojimo	▪ 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, su galimybe redaguoti pranešimo vaizdą bei turinį. ▪ Mechanizmas nepageidaujamų aplikacijų ir URL naudojimo ribojimui (pagal laiką, datas), arba riboti jų greitaveiką.

		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. ▪ Ne mažiau 3000 aplikacijų atpažinimas. Ne mažiau 200 milijonų URL duomenų bazė.	▪ 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. ▪ Daugiau nei 3000 aplikacijų atpažinimas. Daugiau nei 200 milijonų URL duomenų bazė.
44.	Virtualūs privatūs tinklai (VPN)	▪ 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;	▪ 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.

		▪ 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. o statiniai tuneliai, atnaujinami nustatytu periodiškumu.	▪ 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. o 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.	▪ 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.

		▪ 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.	▪ 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.
47.	Nežinomų grėsmių aptikimo (angl. sandboxing) funkcionalumas	▪ Turi būti nežinomų grėsmių patikros funkcionalumas, apimantis failų pateikiamą patikrai į nežinomų grėsmių patikros sprendimą. ▪ Failų pateikimas patikrai iš duomenų srauto. ▪ Failų patikra įgyvendinama gamintojo infrastruktūroje pagrįstoje debesų kompiuterija arba diegiant to paties gamintojo fizinį/programinį sprendimą Perkančiosios organizacijos duomenų centre. ▪ Turi būti galimybė analizuoti šiuos failų tipus: .xz, .7z, .pdf , .tbz2, .bz2, .csv, .CAB, .arj, .cpl , .iqy, .com, .exe , .vbe, .cmd, .swf, .gz , .hwp , .msi, .jar, .pps , .xlt , .app, .dmg, .pkg, .o, .dylib, .msg, .dll , .xls , .xla , .xlam , .xlsb, .xlm, .xltm , .xlsm , .xltx , .xlsx , .xlw, .xll, .ppt, .ppam, .pptm , .sldm, .ppsm , .potm , .pptx, .sldx, .ppsx , .potx , .vbs, .doc, .docx , .dotm , .dot , .ps1, .rar, .rtf, .scr, .lnk, .iso , .slk, .PIF , .tar, .tgz, .udf, .wim, .uue, .vba, .bat, .wsf, .wsh, .zip , .dotx, .docm, .tbz, .tb2. ▪ Turi būti galimybė tikrinti failus vienoje iš arba keliose operacinėse sistemose: Microsoft Windows XP, 7, 8,1, 10 su Microsoft Office	▪ Yra nežinomų grėsmių patikros funkcionalumas, apimantis failų pateikiamą patikrai į nežinomų grėsmių patikros sprendimą. ▪ Failų pateikimas patikrai iš duomenų srauto. ▪ Failų patikra įgyvendinama gamintojo infrastruktūroje pagrįstoje debesų kompiuterija arba diegiant to paties gamintojo fizinį/programinį sprendimą Perkančiosios organizacijos duomenų centre. ▪ Yra galimybė analizuoti šiuos failų tipus: .xz, .7z, .pdf , .tbz2, .bz2, .csv, .CAB, .arj, .cpl , .iqy, .com, .exe , .vbe, .cmd, .swf, .gz , .hwp , .msi, .jar, .pps , .xlt , .app, .dmg, .pkg, .o, .dylib, .msg, .dll , .xls , .xla , .xlam , .xlsb, .xlm, .xltm , .xlsm , .xltx , .xlsx , .xlw, .xll, .ppt, .ppam, .pptm , .sldm, .ppsm , .potm , .pptx, .sldx, .ppsx , .potx , .vbs, .doc, .docx , .dotm , .dot , .ps1, .rar, .rtf, .scr, .lnk, .iso , .slk, .PIF , .tar, .tgz, .udf, .wim, .uue, .vba, .bat, .wsf, .wsh, .zip , .dotx, .docm, .tbz, .tb2. ▪ Yra galimybė tikrinti failus vienoje iš arba keliose operacinėse sistemose: Microsoft Windows XP, 7, 8,1, 10 su Microsoft Office programine įranga (Office 2003, 2010, 2013,

		programine įranga (Office 2003, 2010, 2013, 2016) bei Adobe programine įranga (Adobe 9, 11, DC). ▪ Bylų atsiunčiamų naudojant SSL arba TLS kriptavimą aptikimas. ▪ Maksimalus tikrinamo failo dydis ne mažiau kaip 80 Mb. ▪ Detalios failų patikros ataskaitos, įskaitant elgsenos virtualioje aplinkoje, pateikimas su įvykio informacija.	2016) bei Adobe programine įranga (Adobe 9, 11, DC). ▪ Bylų atsiunčiamų naudojant SSL arba TLS kriptavimą aptikimas. ▪ Maksimalus tikrinamo failo dydis 80 Mb. ▪ Detalios failų patikros ataskaitos, įskaitant elgsenos virtualioje aplinkoje, pateikimas su įvykio informacija.
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.	Nuotolinio prisijungimo funkcionalumas	▪ Galimybė naudotis SSL VPN WEB naršyklės pagalba (be papildomos programinės įrangos).	▪ Galimybė naudotis SSL VPN WEB naršyklės pagalba (be papildomos programinės įrangos).

		▪ Kelių veiksnių vartotojų autentifikavimo palaikymas, įskaitant: o Vartotojas/slaptažodis, naudojant vidinę ugniasienės duomenų bazę arba išorinę vartotojų direktoriją. o SecureID. o RADIUS autentifikaciją. o CAPI slaptažodžių generatorius. o P12 sertifikatus. ▪ Galimybė nustatyti agentams automatinio tunelio užmezgimo nustatymą: o Esant poreikiui pasiekti resursus vidiniame tinkle. o Pagal nutylėjimą. o Tunelio užmezgimas po ryšio nutrūkimo. o Tunelio nutraukimas prisijungus vidiniame tinkle. ▪ Galimybė suteikti agento įrangos virtualiam tinklo prievadui IP adresą iš: o Ugniasienėje numatyto IP adresų rėžio. o Naudojant DHCP relay. o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. ▪ Viso arba dalies kompiuterio srauto maršrutizavimas per ugniasienių sprendimo ugniasienę(es), pagal administratoriaus nustatymus. Maršrutų lentelės pateikimas kompiuteriui pagal nustatytą tinklo topologiją. Turi būti įtrauktos licencijos užtikrinant nuotolinio prisijungimo galimybes ne mažiau 50 vartotojų vienu metu.	▪ Kelių veiksnių vartotojų autentifikavimo palaikymas, įskaitant: o Vartotojas/slaptažodis, naudojant vidinę ugniasienės duomenų bazę arba išorinę vartotojų direktoriją. o SecureID. o RADIUS autentifikaciją. o CAPI slaptažodžių generatorius. o P12 sertifikatus. ▪ Galimybė nustatyti agentams automatinio tunelio užmezgimo nustatymą: o Esant poreikiui pasiekti resursus vidiniame tinkle. o Pagal nutylėjimą. o Tunelio užmezgimas po ryšio nutrūkimo. o Tunelio nutraukimas prisijungus vidiniame tinkle. ▪ Galimybė suteikti agento įrangos virtualiam tinklo prievadui IP adresą iš: o Ugniasienėje numatyto IP adresų rėžio. o Naudojant DHCP relay. o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. ▪ Viso arba dalies kompiuterio srauto maršrutizavimas per ugniasienių sprendimo ugniasienę(es), pagal administratoriaus nustatymus. Maršrutų lentelės pateikimas kompiuteriui pagal nustatytą tinklo topologiją. Įtrauktos licencijos užtikrinant nuotolinio prisijungimo galimybes 50 vartotojų vienu metu.
52.	Žurnalinių įrašų kaupimas	Įvykių žurnalai turi būti kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Turi būti	Įvykių žurnalai kaupiami įrenginyje ir/arba siunčiami į centrinę valdymo tarnybinę stotį. Generuojami žurnaliniai

		generuojami žurnaliniai įvykiai susiję su ugniasienės funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Atidaromus URL; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; • Žalingus failus; • BotNet veiklą; Turi būti galimybė nustatyti įvykio įrašymą konkrečiai ugniasienės taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams.	įvykiai susiję su ugniasienės funkcionalumu ir susiejami su konkrečiais IP adresais, vartotojais ir pan., įskaitant: • Administratorių veiksmus; • Naudojamas aplikacijas; • Atidaromus URL; • Saugos incidentus; • Sesijas, duomenų srautus pagal šalis, vartotojus ir pan.; • Žalingus failus; • BotNet veiklą; Yra galimybė nustatyti įvykio įrašymą konkrečiai ugniasienės taisyklei, nurodant įrašomo įvykio detalumą bei paketų įrašymą saugos incidentams.
53.	Administratorių paskyros	Administratorių prieigos teisės turi būti kontroliuojamos rolių pagalba. Turi būti galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; teisė generuoti ataskaitas.	Administratorių prieigos teisės kontroliuojamos rolių pagalba. Yra galimybė smulkiai apibrėžti administratoriaus teises pvz.: • teisė keisti sisteminius įrenginio nustatymus; • teisė kurti, keisti saugumo taisykles; • teisė kurti, keisti taisyklių objektus; • teisė konfigūruoti saugumo patikrų nustatymus; • teisė peržiūrėti įvykių žurnalus; • teisė peržiūrėti ataskaitas; teisė generuoti ataskaitas.
54.	Programinės įrangos atnaujinimai	Turi būti. Nemokamai garantinio aptarnavimo laikotarpiu	Yra. Nemokamai garantinio aptarnavimo laikotarpiu
55.	Atnaujinimai pagal nustatytą grafiką (Shedule)	Turi būti	Yra
56.	Garantiniai įsipareigojimai	Tiesioginis gamintojo 36 mėn. nemokamas garantinis aptarnavimas. Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto	Tiesioginis gamintojo 36 mėn. nemokamas garantinis aptarnavimas. Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir

		naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. Gedimo atveju pakaitinė įranga turi būti pristatyta ne vėliau kaip kitą darbo dieną.	problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos. Gedimo atveju pakaitinė įranga pristatoma ne vėliau kaip kitą darbo dieną.
Reikalavimai darbo vietų saugos sprendimui			
57.	Įrangos pavadinimas		Quantum Smart-1 Cloud
58.	Įrangos gamintojas		Check Point Software Technologies
59.	Darbo vietų kiekis	200 darbo vietų ir serverių	200 darbo vietų ir serverių
60.	Aprašymas	Darbo vietų ir serverių saugos programinės įrangos sprendimas kibernetinių atakų aptikimui ir prevencijai. Sprendimas pagrįstas debesų kompiuterija, užtikrinant, kad duomenys bus laikomi infrastruktūroje Europos Sąjungoje. Gamintojo įsipareigojamas paslaugos pasiekiamumas ne mažiau 99,9%. Sprendimas skirtas 700 įrenginių.	Darbo vietų ir serverių saugos programinės įrangos sprendimas kibernetinių atakų aptikimui ir prevencijai. Sprendimas pagrįstas debesų kompiuterija, užtikrinant, kad duomenys bus laikomi infrastruktūroje Europos Sąjungoje. Gamintojo įsipareigojamas paslaugos pasiekiamumas ne mažiau 99,9%. Sprendimas skirtas 700 įrenginių.
61.	Gamintojas	Nurodyti.	Check Point Software Technologies
62.	Įrangos pavadinimas	Nurodyti.	Harmony Endpoint Advanced
63.	Valdymo funkcionalumas	• Visas sprendimo funkcionalumas turi būti valdomas per vieningą grafinę sąsają. • Perkančiajai organizacijai turi būti suteikiama prieiga prie Gamintojo infrastruktūroje esančio sprendimo valdymo. • Turi būti galimybė kurti kelias administratorių paskyras su skirtingu prieigos lygiu (peržiūrėti ir redaguoti, tik peržiūrėti). • Administratorių autentifikavimas turi veikti per	• Visas sprendimo funkcionalumas yra valdomas per vieningą grafinę sąsają. • Perkančiajai organizacijai suteikiama prieiga prie Gamintojo infrastruktūroje esančio sprendimo valdymo. • Yra galimybė kurti kelias administratorių paskyras su skirtingu prieigos lygiu (peržiūrėti ir redaguoti, tik peržiūrėti). • Administratorių autentifikavimas turi veikti per Microsoft Azure AD, Okta, DUO, Google

		Microsoft Azure AD, Okta, DUO, Google Workspace platformas, RADIUS ir SAML autentifikavimą. • Galimybė įvykius perduoti į SIEM ir įvykių valdymo sprendimus, naudojant syslog formatą. • Politikos turi būti kuriamos vartotojams, mašinoms bei jų grupėms taip, kad būtų galima nustatyti skirtingą diegiamą funkcionalumą, konfigūracijas skirtingoms grupėms. • Turi būti galimybė naudoti skirtingus administratorių teisių lygius, priskirti teises koreguoti politikas. Gamintojas turi užtikrinti, kad visi duomenys būtų saugomi debesų kompiuterijos infrastruktūroje esančioje Europos Sąjungoje.	Workspace platformas, RADIUS ir SAML autentifikavimą. • Galimybė įvykius perduoti į SIEM ir įvykių valdymo sprendimus, naudojant syslog formatą. • Politikos gali būti kuriamos vartotojams, mašinoms bei jų grupėms taip, kad būtų galima nustatyti skirtingą diegiamą funkcionalumą, konfigūracijas skirtingoms grupėms. • Yra galimybė naudoti skirtingus administratorių teisių lygius, priskirti teises koreguoti politikas. Gamintojas užtikrina, kad visi duomenys būtų saugomi debesų kompiuterijos infrastruktūroje esančioje Europos Sąjungoje.
64.	Programinės įrangos diegimas	Turi palaikyti Windows 11, Windows 10 32bit/64bit, Windows 7 64 bit, Windows server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, 2025, macOS Ventura, macOS Monterey, macOS Big Sur, macOS Catalina, macOS Sonoma, macOS Sequia, Ubuntu, CentOS, OpenSUSE, Debian operacines sistemas.	Palaiko Windows 11, Windows 10 32bit/64bit, Windows 7 64 bit, Windows server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, 2025, macOS Ventura, macOS Monterey, macOS Big Sur, macOS Catalina, macOS Sonoma, macOS Sequia, Ubuntu, CentOS, OpenSUSE, Debian operacines sistemas.
65.	Apsaugos nuo grėsmių funkcionalumas	Turi turėti tokias integruotas funkcijas: • Antivirusinė apsauga. • Darbo vietos ugniasienę. • Prievadų valdymą. • Aplikacijų kontrolę. • Apsaugą nuo pažeidžiamumų išnaudojimo grėsmių (angl. Exploit). • Apsaugą nuo elektroninio sukčiavimo (Phishing). • Apsaugą nuo ransomware tipo duomenis užkoduojančių virusų. • Organizacijos prisijungimo duomenų naudojimo kontrolę. • Apsaugą nuo botnet tinklų kenkėjiškos programinės įrangos.	Turi tokias integruotas funkcijas: • Antivirusinė apsauga. • Darbo vietos ugniasienę. • Prievadų valdymą. • Aplikacijų kontrolę. • Apsaugą nuo pažeidžiamumų išnaudojimo grėsmių (angl. Exploit). • Apsaugą nuo elektroninio sukčiavimo (Phishing). • Apsaugą nuo ransomware tipo duomenis užkoduojančių virusų. • Organizacijos prisijungimo duomenų naudojimo kontrolę. • Apsaugą nuo botnet tinklų kenkėjiškos programinės įrangos. • Apsaugą nuo grėsmių pagal tipinius žalingo kodo veikimo modelius.

		• Apsaugą nuo grėsmių pagal tipinius žalingo kodo veikimo modelius. • Incidentų analizės įrankį. • Apsauga nuo nežinomų grėsmių. • URL filtravimo funkcionalumą. • Apsaugą nuo slaptažodžių perpanaudojimo. • Nuotolinio prisijungimo prie įsigijamų ugniasienių. Linux šeimos operacinėms sistemos pakankamas šis funkcionalumas: • Apsaugą nuo grėsmių pagal tipinius žalingo kodo veikimo modelius. Antivirusinė apsauga.	• Incidentų analizės įrankį. • Apsauga nuo nežinomų grėsmių. • URL filtravimo funkcionalumą. • Apsaugą nuo slaptažodžių perpanaudojimo. • Nuotolinio prisijungimo prie įsigijamų ugniasienių. Linux šeimos operacinėms sistemos pakankamas šis funkcionalumas: • Apsaugą nuo grėsmių pagal tipinius žalingo kodo veikimo modelius. Antivirusinė apsauga.
66.	Antivirusinė apsauga.	• Failų ir procesų stebėjimas ir žinomų žalingų failų bei procesų šalinimas/karantinavimas. • Galimybė nustatyti periodinius pilnas sistemos patikras (skanavimus), nustatant jų periodiškumą ir skanuojamas failinės sistemos vietas.	• Failų ir procesų stebėjimas ir žinomų žalingų failų bei procesų šalinimas/karantinavimas. • Galimybė nustatyti periodinius pilnas sistemos patikras (skanavimus), nustatant jų periodiškumą ir skanuojamas failinės sistemos vietas.
67.	Darbo vietos ugniasienę.	• Įeinančio ir išeinančio srauto kontrolė IP adresams, jų rėžiams, protokolams, prievadams. • Centralizuotas ugniasienės politikos valdymas per vartotojus ir jų grupes. • Galimybe kurti kelias politikas, galiojančias kompiuteriui esant vidiniame tinkle ir už jo ribos. • Darbo vietos atitikties vertinimas pagal programinės įrangos versiją, operacinės sistemos atnaujinimus, neleistinų aplikacijų naudojimą, žinomus su kompiuteriu susijusius incidentus. Ribotos ugniasienės politikos pritaikymas neatitinkantiems įrenginiams.	• Įeinančio ir išeinančio srauto kontrolė IP adresams, jų rėžiams, protokolams, prievadams. • Centralizuotas ugniasienės politikos valdymas per vartotojus ir jų grupes. • Galimybe kurti kelias politikas, galiojančias kompiuteriui esant vidiniame tinkle ir už jo ribos. • Darbo vietos atitikties vertinimas pagal programinės įrangos versiją, operacinės sistemos atnaujinimus, neleistinų aplikacijų naudojimą, žinomus su kompiuteriu susijusius incidentus. Ribotos ugniasienės politikos pritaikymas neatitinkantiems įrenginiams. • Galimybė naudoti ugniasienių valdymo serveryje nustatytus objektų aprašus. • Galimybė aptikti viešosios prieigos tinklus, bei taikyti

		• Galimybė naudoti ugniasienių valdymo serveryje nustatytus objektų aprašus. • Galimybė aptikti viešosios prieigos tinklus, bei taikyti ugniasienės išimtis WEB autentifikacijai.	ugniasienės išimtis WEB autentifikacijai.
68.	Prievadų valdymas.	• Pajungiamų USB, Bluetooth įrenginių kontrolė. • Konkrečių USB ir Bluetooth įrenginių ar jų grupių naudojimo kompiuteriuose kontrolė. • Galimybė aprašyti savo įrenginius ir jų grupes pagal įrenginio duomenis (serijos numerį), arba kompiuterio žurnaliniuose įrašuose (*logs*) kaupiamą informaciją.	• Pajungiamų USB, Bluetooth įrenginių kontrolė. • Konkrečių USB ir Bluetooth įrenginių ar jų grupių naudojimo kompiuteriuose kontrolė. • Galimybė aprašyti savo įrenginius ir jų grupes pagal įrenginio duomenis (serijos numerį), arba kompiuterio žurnaliniuose įrašuose (*logs*) kaupiamą informaciją.
69.	Aplikacijų kontrolė.	• Aplikacijų generuojamo srautų kontrolė, leidžiant/neleidžiant konkrečios aplikacijos srautus. • Aplikacijų paleidimo kontrolė, leidžiant/neleidžiant paleisti konkrečias aplikacijas.	• Aplikacijų generuojamo srautų kontrolė, leidžiant/neleidžiant konkrečios aplikacijos srautus. • Aplikacijų paleidimo kontrolė, leidžiant/neleidžiant paleisti konkrečias aplikacijas.
70.	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.
71.	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.
72.	Apsaugos nuo ransomware tipo duomenis užkoduojančių	• Apsauga nuo žinomų ir nežinomų ransomware tipo virusų.	• Apsauga nuo žinomų ir nežinomų ransomware tipo virusų.

	virusų funkcionalumas	• Ransomware tipo virusų atpažinimas pagal veikimo modelius. • Galimybė atstatyti iki aptikimo užkoduotus failus.	• Ransomware tipo virusų atpažinimas pagal veikimo modelius. • Galimybė atstatyti iki aptikimo užkoduotus failus.
73.	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.
74.	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 požymus, ir jos blokavimas.
75.	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.
76.	Apsauga nuo nežinomų grėsmių	• Visų operuojamų 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, 10,11), 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.	• Visų operuojamų failų (atsiunčiamų, įrašomų, kopijuojamų ir pan.) patikra išoriniame grėsmių emuliavimo sprendime. • Patikra yra įgyvendinama aktyvinant failus skirtingose saugiose virtualiose operacinėse sistemose (Windows 7, 8, 10,11), naudojant skirtingų versijų PĮ paketus (pvz.: skirtingas MS Office versijas). • Patikros metu yra 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. • Programinės įrangos licencija turi leisti integraciją su to paties arba suderinamo kito gamintojo failų emuliavimo įrenginiu Perkančiosios organizacios infrastruktūroje. Siūlant galimybę diegti kito gamintojo suderinamą sprendimą privaloma pateikti nuorodą į viešai prieinamą informaciją patvirtinančią suderinamumo faktą. Suderinamumas turi būti įgyvendinamas per API, integruojant programinę įrangą su sprendimu tokiu būdu, kad diegiant sprendimą nereikėtų atlikti pokyčių infrastruktūroje, arba naudoti tokių sprendinių kaip „message transfer agent“, „file proxy“ ir pan. • Programinė įrangos licencija turi apimti emuliavimą sprendimo gamintojo debesų kompiuterijos infrastruktūroje. • Turi būti atliekama šių failų tipų analizė: .xz, .7z, .pdf , .udf, .qcow, .sh, .tbz2, .bz2, .csv, .CAB, .arj, .cpl , .iqy, .elf, .com, .exe , .xar, .swf, .gz , .hwp , .msi, .img, .xlt , .pps , .app, .dmg, .pkg, .o, .dyli, .msg, .dll , .xls , .xla , .xlam, .xlsb, .xlm, .xltm, .xlsm, .xltx, .xlsx, .xlw, .xll, .one, .ppt, .ppam, .pptm, .sldm, .ppsm, .potm, .pptx, .sldx, .ppsx, .potx, .doc, .docx, .dotm, .dot , .ps1, .rar, .rtf, .scr,	• 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 yra blokuojamas automatiškai. • Programinės įrangos licencija leidžia integraciją su to paties gamintojo failų emuliavimo įrenginiu Perkančiosios organizacios infrastruktūroje. • Programinė įrangos licencija apima emuliavimą sprendimo gamintojo debesų kompiuterijos infrastruktūroje. • Yra atliekama šių failų tipų analizė: .xz, .7z, .pdf , .udf, .qcow, .sh, .tbz2, .bz2, .csv, .CAB, .arj, .cpl , .iqy, .elf, .com, .exe , .xar, .swf, .gz , .hwp , .msi, .img, .xlt , .pps , .app, .dmg, .pkg, .o, .dyli, .msg, .dll , .xls , .xla , .xlam, .xlsb, .xlm, .xltm, .xlsm, .xltx, .xlsx, .xlw, .xll, .one, .ppt, .ppam, .pptm, .sldm, .ppsm, .potm, .pptx, .sldx, .ppsx, .potx, .doc, .docx, .dotm, .dot , .ps1, .rar, .rtf, .scr, .lnk, .slk, .PIF , .iso , .tar, .tgz, .udf, .wim, .uue, .bat, .wsf, .zip , .dotx, .docm, .tbz, .tb2. • Yra grėsmių išvalymo funkcionalumas, šalinantis potencialiai žalingą turinį (skriptus, macros ir pn.) iš failų arba vartotojui pateikiamus failus konvertuojant į nekenksmingus .pdf tipo failus. • Grėsmių išvalymo funkcionalumas palaiko .pdf, .doc, .docx, .ppt, .pptx failų tipus. • Yra galimybė detaliai aprašyti iš failų šalinamą aktyvų turinį, įskaitant failus ir objektus įklijuotus į failų vidų, duomenų bazių užklausas, macros ir kitą

		.lnk, .slk, .PIF , .iso , .tar, .tgz, .udf, .wim, .uue, .bat, .wsf, .zip , .dotx, .docm, .tbz, .tb2. • Turi būti grėsmių išvalymo funkcionalumas, šalinantis potencialiai žalingą turinį (skriptus, macros ir pn.) iš failų arba vartotojui pateikiamus failus konvertuojant į nekenksmingus .pdf tipo failus. • Grėsmių išvalymo funkcionalumas turi palaikyti .pdf, .doc, .docx, .ppt, .pptx failų tipus. • Turi būti galimybė detaliai aprašyti iš failų šalinamą aktyvų turinį, įskaitant failus ir objektus įklijuotus į failų vidų, duomenų bazių užklausas, macros ir kitą programinį kodą, javascript skriptus. • Vartotojui turi būti suteikta galimybe atsisiųsti originalų failą tuo atveju, jeigu po patikros nustatyta kad failas ir jo turinys saugus.	programinį kodą, javascript skriptus. • Vartotojui yra suteikta galimybe atsisiųsti originalų failą tuo atveju, jeigu po patikros nustatyta kad failas ir jo turinys saugus.
77.	URL filtravimo funkcionalumas	• URL filtravimas pagal kategorijas. • Nepageidaujamų URL blokavimas. • URL filtravimas turi turėti galimybę veikti dviem režimais: naršyklės režimu, kai URL filtravimas atliekamas pačioje naršyklėje (palaikomos Chrome, Edge, Firefox, Internet Explorer naršyklės); operacinės sistemos režimu, kai funkcionalumas nepriklauso nuo naudojamos naršyklės. • Galimybė koreguoti pranešimus vartotojams apie blokuojamas svetaines, juos rašyti lietuvių kalba.	• URL filtravimas pagal kategorijas. • Nepageidaujamų URL blokavimas. • URL filtravimas turi galimybę veikti dviem režimais: naršyklės režimu, kai URL filtravimas atliekamas pačioje naršyklėje (palaikomos Chrome, Edge, Firefox, Internet Explorer naršyklės); operacinės sistemos režimu, kai funkcionalumas nepriklauso nuo naudojamos naršyklės. • Galimybė koreguoti pranešimus vartotojams apie blokuojamas svetaines, juos rašyti lietuvių kalba.
78.	Apsauga nuo slaptažodžių perpanaudojimo	• Programinė įranga turi kaupti vartotojų slaptažodžių maišos kodus svetainėms nurodytoms administratoriaus. Kaupimas turi būti įgyvendinamas saugiu	• Programinė įranga kaupia vartotojų slaptažodžių maišos kodus svetainėms nurodytoms administratoriaus. Kaupimas įgyvendinamas saugiu būdu,

		būdu, užtikrinant duomenų saugumą, ir tik pačiame įrenginyje. • Turi būti blokuojami vartotojų bandymai panaudoti slaptažodžius iš apibrėžtų svetainių ir aplikacijų kitose, su Perkančiosios organizacijos veikla, nesusijusiose svetainėse.	užtikrinant duomenų saugumą, ir tik pačiame įrenginyje. • Blokuojami vartotojų bandymai panaudoti slaptažodžius iš apibrėžtų svetainių ir aplikacijų kitose, su Perkančiosios organizacijos veikla, nesusijusiose svetainėse.
79.	Nuotolinio prisijungimo prie įsigijamų ugniasienių.	• Nuotolinis prisijungimas prie įsigijamų ugniasienių naudojant IPSec VPN. • Kelių veiksnių vartotojų autentifikavimo palaikymas, įskaitant: o Vartotojas/slaptažodis, naudojant vidinę ugniasienės duomenų bazę arba išorinę vartotojų direktoriją. o SecureID. o RADIUS autentifikaciją. o CAPI slaptažodžių generatorius. o P12 sertifikatus. • Automatinis tunelio užmezgimas pagal administratoriaus nustatymus: o Esant poreikiui pasiekti resursus vidiniame tinkle. o Pagal nutylėjimą. o Tunelio užmezgimas po ryšio nutrūkimo. o Tunelio nutraukimas prisijungus vidiniame tinkle. • Galimybė suteikti programinės įrangos virtualiam tinklo prievadui IP adresą iš: o Ugniasienėje numatyto IP adresų rėžio. o Naudojant DHCP *relay.* o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. • Viso arba dalies kompiuterio srauto maršrutizavimas per	• Nuotolinis prisijungimas prie įsigijamų ugniasienių naudojant IPSec VPN. • Kelių veiksnių vartotojų autentifikavimo palaikymas, įskaitant: o Vartotojas/slaptažodis, naudojant vidinę ugniasienės duomenų bazę arba išorinę vartotojų direktoriją. o SecureID. o RADIUS autentifikaciją. o CAPI slaptažodžių generatorius. o P12 sertifikatus. • Automatinis tunelio užmezgimas pagal administratoriaus nustatymus: o Esant poreikiui pasiekti resursus vidiniame tinkle. o Pagal nutylėjimą. o Tunelio užmezgimas po ryšio nutrūkimo. o Tunelio nutraukimas prisijungus vidiniame tinkle. • Galimybė suteikti programinės įrangos virtualiam tinklo prievadui IP adresą iš: o Ugniasienėje numatyto IP adresų rėžio. o Naudojant DHCP *relay.* o Priskiriant konkretiems vartotojams ir jų grupėms konkrečius IP adresus ar jų rėžius. Viso arba dalies kompiuterio srauto maršrutizavimas per ugniasienes, pagal administratoriaus nustatymus. Maršrutų lentelės pateikimas kompiuteriui pagal nustatytą tinklo topologiją.

		ugniasienes, pagal administratoriaus nustatymus. Maršrutų lentelės pateikimas kompiuteriui pagal nustatytą tinklo topologiją.	
80.	Paslaugos teikimo laikotarpis ir gamintojo įsipareigojimai	Tiesioginis gamintojo 36 mėn. nemokamas garantinis aptarnavimas. Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. • Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos.	Tiesioginis gamintojo 36 mėn. nemokamas garantinis aptarnavimas. Programinės įrangos palaikymas (teisė gauti klaidų taisymus, taip pat naujesnes programinės įrangos versijas), teisė kreiptis į gamintoją iškilus problemai (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) darbo dienomis, internetu, elektroniniu paštu, faksu arba telefonu. • Prieiga prie gamintojo internetiniame puslapyje esančių techninių resursų, tarp jų ir programinės įrangos bibliotekos.