UAB „ATEA“
J. Rutkausko g. 6, 05132 Vilnius
Tel. (8-5) 2397830 Faks. (8-5) 2397831

Luminor Bank AS Lietuvos skyrius
Banko kodas: 21400
Atsisk. sąskaita: LT032140030001327814
Įm. kodas 122588443
PVM mokėtojo kodas: LT225884413

VšĮ Kėdainių pirminės sveikatos priežiūros centrui

PASIŪLYMAS DĖL LICENCIJŲ PALAIKYMO PASLAUGŲ

2022-09-26 Kaunas

Tiekėjo pavadinimas */Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai/*	UAB ATEA
Įmonės kodas	J. Rutkausko g. 6, 05132 Vilnius
Tiekėjo adresas */Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai/*	122588443
Už pasiūlymą atsakingo asmens vardas, pavardė	Valentinas Bylina
Telefono numeris	Mob. +370-682-55024
El. pašto adresas	valentinas.bylina@atea.lt

/Pastaba. Pildoma, jei tiekėjas ketina pasitelkti subrangovą (-us), subtiekėją (-us)ar suteikėją (-us)/

Subtiekėjo (-ų) pavadinimas (-ai)	
Subtiekėjo (-ų) adresas (-ai)	
Įsipareigojimų dalis (procentais), kuriai ketinama pasitelkti subtiekėją (-us)	

1. Šiuo pasiūlymu pažymime, kad sutinkame su visomis neskelbiamos apklausos sąlygomis, nustatytomis šiose apklausos sąlygose bei kituose pirkimo dokumentuose (jų paaiškinimuose, papildymuose, patikslinimuose).

2. Siūlomos Prekės visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus.

3. Pasirašydami CVP IS elektroninėmis priemonėmis pateiktą pasiūlymą, patvirtiname, kad dokumentų skaitmeninės kopijos ir CVP IS elektroninėmis priemonėmis pateikti duomenys yra tikri.

1 lentelė.

Eil. Nr.	Pavadinimas	Perkamas kiekis	1 mėn. kaina 1 licencijai, Eur be PVM	Viso Eur be PVM
1	**2**	**3**	**4**	**5 = (3 x 4)x36 mėn.**
1.	„Symantec Endpoint Protection“ licencijos (arba lygiavertės) pratęsimas („Symantec Endpoint Protection“ licencijos pratęsimas 3 metams)	10 vnt.	2,28	820,80
2.			**Viso Eur, be PVM**	**820,80**

2 lentelė.

Eil. Nr.	Pavadinimas	Perkamas kiekis	1 mėn. kaina, Eur be PVM	Palaikymo kaina iki 2025.03.31 Eur be PVM
1	**2**	**3**	**4**	**5 = 3 x 4**
1.	Sophos XG 135 ugniasienės licencijų (Xstream Protection , Email Protection , Webserver Protection) arba lygiaverčių pratęsimas vienam įrenginiui (Sophos XG 135 ugniasienės licencijų (Xstream Protection , Email Protection , Webserver Protection) pratęsimas vienam įrenginiui iki 2025.03.31)	1 vnt.	4071,20	4071,20
2.			**Viso Eur, be PVM**	**4071,20**
			Bendra pasiūlymo kaina be PVM *(1 ir 2 lentelės, 2 eilutė)*	**4892,00**
			PVM	**1027,32**
			Bendra pasiūlymo kaina su PVM	**5919,32**

Pastaba: visos kainos nurodomos ne daugiau kaip 2 skaičiai po kablelio, tikslumu.

Pasiūlymo kaina – 5919,32 Eur su PVM (penki tūkstančiai devyni šimtai devyniolika Eur, 32 ct.), iš jų PVM sudaro 1027,32 Eur (tūkstantis dvidešimt septyni Eur, 32 ct.).

Į šią sumą turi būti įskaityti visi mokesčiai ir visos kitos dalyvio išlaidos reikalingos tinkamam paslaugų atlikimui.

Kartu su pasiūlymu pateikiami šie dokumentai (pasirašydamas pasiūlymą ar kiekvieną dokumentą patvirtinu, kad dokumentų skaitmeninės kopijos yra tikros) ir ši pasiūlyme nurodyta informacija yra konfidenciali:

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius	Konfidenciali informacija dokumente (nurodyti psl.)	Pastabos
1.	Valentinas_Bylina_igaliojimas_KONFIDENCIALU.pdf	1	1	---

Pastaba: Pildyti tuomet, jei bus pateikta konfidenciali informacija. Teikėjas negali nurodyti, kad konfidenciali yra pasiūlymo kaina arba, kad visas pasiūlymas yra konfidencialus. Tiekėjui nenurodžius, kokia informacija yra konfidenciali (dokumento puslapius), laikoma, kad konfidencialios informacijos pasiūlyme nėra.

Kartu su pasiūlymu pateikiami šie dokumentai:

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius
1.	Valentinas_Bylina_igaliojimas_KONFIDENCIALU.pdf	1
2.	Techninė_licencijos_uzpildyta.pdf	21

Pasiūlymas galioja 60 dienų.

Valentinas Bylina — Pardavimo projektų vadovas

(Tiekėjo arba jo įgalioto asmens vardas, pavardė, parašas)

Techninė specifikacija

Eil. Nr.	Komponento pavadinimas	Reikalaujama charakteristika	Siūloma charakteristika, gamintojas, modelis, kodas
I.			
1.1	„Symantec Endpoint Protection“ licencijos 10 vnt. darbo/tarnybinių stočių (arba lygiavertės) pratęsimas 3 metams. Turima licencija „S7847760141“ galiojo iki 2022.06.24.	10 licencijų pratęsimas: Virtualizuotų tarnybinių tinklo stočių apsaugos programinė įranga. Sistemos paskirtis: • Organizacijai priklausančių virtualizuotų tarnybinių stočių apsauga nuo išorės ir vidinių grėsmių (kompiuteriniai virusai, šnipinėjimo programos, įsilaužimai, informacijos nutekėjimas) Siūlomas apsaugos sprendimas turi apimti: • 10 virtualizuotos tarnybinės stotys. Programinės įrangos versija: • Turi būti siūloma naujausia, gamintojo svetainėje oficialiai paskelbta, programinės įrangos versija. Pagrindinės sistemos funkcijos (komponentai): • Darbo vietų kompiuterių ir serverių apsauga nuo kompiuterinių virusų ir šnipinėjimo programų; • Tarnybinių stočių apsauga nuo įsilaužimų (firewall); • Įsilaužimų prevencijos mechanizmas; • Programų ir aplikacijų paleidimo kontrolė; • Turi gebėti skenavimo metu indeksuoti tarnybinėse stotyse esančias bylas ir praleisti patikrintų bylų skenavimą jeigu jos nėra pakitusios po paskutinio patikrinimo; • Turi turėti galimybę naudoti bendrą tinklinį indeksą, kurio dėka vienoje tarnybinėje stotyje patikrintos bylos nebūtų skanuojamos kitoje tarnybinėje stotyje; • Turi palaikyti virtualizaicjos technologijas ir automatiškai atpažinti virtualizuotas tanybines stotis; • Turi būti galimybė sudaryti programų „baltajį sąrašą“ ir leisti užkraiti tik šiame sąraše esančias programas, visų kitų programų paleidimas būtų draudžiamas. Tarnybinių stočių apsaugos programinės įrangos darbo terpė: • Windows Server 2003 (32bit, 64bit) • Windows Server 2008 (32bit, 64bit) • Windows Server 2012 • Windows Server 2019 Gamintojas turi garantuoti palaikymą	„Symantec Endpoint Protection“ licencijos 10 vnt. darbo/tarnybinių stočių pratęsimas 3 metams. 10 licencijų pratęsimas: Virtualizuotų tarnybinių tinklo stočių apsaugos programinė įranga. Sistemos paskirtis: • Organizacijai priklausančių virtualizuotų tarnybinių stočių apsauga nuo išorės ir vidinių grėsmių (kompiuteriniai virusai, šnipinėjimo programos, įsilaužimai, informacijos nutekėjimas) Siūlomas apsaugos sprendimas apima: • 10 virtualizuotos tarnybinės stotys. Programinės įrangos versija: • Siūloma naujausia, gamintojo svetainėje oficialiai paskelbta, programinės įrangos versija. Pagrindinės sistemos funkcijos (komponentai): • Darbo vietų kompiuterių ir serverių apsauga nuo kompiuterinių virusų ir šnipinėjimo programų; • Tarnybinių stočių apsauga nuo įsilaužimų (firewall); • Įsilaužimų prevencijos mechanizmas; • Programų ir aplikacijų paleidimo kontrolė; • Geba skenavimo metu indeksuoti tarnybinėse stotyse esančias bylas ir praleisti patikrintų bylų skenavimą jeigu jos nėra pakitusios po paskutinio patikrinimo; • Turi galimybę naudoti bendrą tinklinį indeksą, kurio dėka vienoje tarnybinėje stotyje patikrintos bylos nebūtų skanuojamos kitoje tarnybinėje stotyje; • Palaiko virtualizaicjos technologijas ir automatiškai atpažįsta virtualizuotas tanybines stotis; • Galimybė sudaryti programų „baltajį sąrašą“ ir leisti užkraiti tik šiame sąraše esančias programas, visų kitų programų paleidimas būtų draudžiamas. Tarnybinių stočių apsaugos programinės įrangos darbo terpė: • Windows Server 2003 (32bit, 64bit) • Windows Server 2008 (32bit, 64bit)

		ir naujų apsaugos programų versijų pateikimą naujoms, techninio aptarnavimo laikotarpiu išleidžiamoms, Microsoft operacinėms sistemoms (serveriams, darbo vietoms) Apsaugos programinė įranga turi būti suderinama su šiomis virtualizacijos terpėmis: • Microsoft Hyper-V; • VmWare vSphere Server (ESXi); • Citrix XenServer. Funkciniai reikalavimai apsaugos nuo kompiuterinių virusų komponentui: Komponento paskirtis: kompiuterių apsauga nuo kompiuterinių virusų ir šnipinėjimo programų. • Įdiegti antivirusinės programinės įrangos moduliai turi apsaugoti savo procesus nuo sustabdymo arba automatiškai juos vėl paleisti, jei šie kokiu nors neleistinu būdu buvo sustabdyti; • Turi gebėti aptikti ir neutralizuoti neautorizuotas programas, kurios bando gauti sisteminę ir konfidencialią informaciją: virusus, kirminus (worms), „rootkits“, „Trojos arklius“ (Trojans), šnipinėjimo programas (spyware), klaviatūros paspaudimų surinkėjus (key loggers), piktybines reklamines programas (adware, identifikuoti pik-tybines programas (dialers, joke programs, remote access ir hack); • Turi turėti euristinį grėsmių aptikimo mechanizmą; • Turi sugebėti aptikti ir sustabdyti atakas iki virusų aprašų (virus definition) išleidimo (zero-day attacks); • Turi turėti galimybę aptikti grėsmes ir sustabdyti įtartinus procesus, vykstančius kompiuterio operatyvioje atmintyje iki sukeliant jiems žalą, atminties skenavimo metu nutraukti aptiktus procesus, kurie gali sukelti grėsmę sistemos darbui; • Turi turėti lokalaus ir centralizuoto „karantino“ pasirinkimo galimybę; • Turi turėti galimybę vykdyti kompiuterio sistemos ir failų skenavimą pagal tvarkaraštį arba inicijavus administratoriaus nurodymu iš valdymo konsolės; • Turi turėti galimybę atlikti išorinių informacijos laikmenų skenavimą;	• Windows Server 2012 • Windows Server 2019 Gamintojas garantuoja palaikymą ir naujų apsaugos programų versijų pateikimą naujoms, techninio aptarnavimo laikotarpiu išleidžiamoms, Microsoft operacinėms sistemoms (serveriams, darbo vietoms) Apsaugos programinė įranga suderinama su šiomis virtualizacijos terpėmis: • Microsoft Hyper-V; • VmWare vSphere Server (ESXi); • Citrix XenServer. Funkciniai reikalavimai apsaugos nuo kompiuterinių virusų komponentui: Komponento paskirtis: kompiuterių apsauga nuo kompiuterinių virusų ir šnipinėjimo programų. • Įdiegti antivirusinės programinės įrangos moduliai apsaugo savo procesus nuo sustabdymo arba automatiškai juos vėl paleidžia, jei šie kokiu nors neleistinu būdu buvo sustabdyti; • Geba aptikti ir neutralizuoti neautorizuotas programas, kurios bando gauti sisteminę ir konfidencialią informaciją: virusus, kirminus (worms), „rootkits“, „Trojos arklius“ (Trojans), šnipinėjimo programas (spyware), klaviatūros paspaudimų surinkėjus (key loggers), piktybines reklamines programas (adware, identifikuoti pik-tybines programas (dialers, joke programs, remote access ir hack); • Turi euristinį grėsmių aptikimo mechanizmą; • Sugeba aptikti ir sustabdyti atakas iki virusų aprašų (virus definition) išleidimo (zero-day attacks); • Turi galimybę aptikti grėsmes ir sustabdyti įtartinus procesus, vykstančius kompiuterio operatyvioje atmintyje iki sukeliant jiems žalą, atminties skenavimo metu nutraukti aptiktus procesus, kurie gali sukelti grėsmę sistemos darbui; • Turi lokalaus ir centralizuoto „karantino“ pasirinkimo galimybę; • Turi galimybę vykdyti kompiuterio sistemos ir failų skenavimą pagal tvarkaraštį arba inicijavus administratoriaus nurodymu iš valdymo konsolės;

Techninė specifikacija

		• Siūlomos antivirusinės sistemos gamintojas turi būti sėkmingai išlaikęs bent vieną Virus Bulletin 2012 metų testą VB100 arba lygiavertį; • Turi turėti operatyvaus automatinio atsinaujinimo funkciją; • Turi būti operatyvus ataskaitų formavimas apie rastus virusus į valdymo konsolę. • Komponentas turi būti valdomas iš bendros valdymo konsolės. • Turi būti galimybė uždrausti vartotojams, darbo vietose turintiems administravimo teises, standartinėmis OS priemonėmis sustabdyti antivirusinės programinės įrangos tarnybą. Funkciniai reikalavimai apsaugos nuo įsilaužimų komponentui Komponento paskirtis: kompiuterių apsauga nuo galimų įsilaužimų į sistemą. • Ugniasienė turi apsaugoti nuo nepageidaujamų tinklo išorinių atakų, t.y. pagal nustatytus kriterijus (pagal prievadus (port) ir programas) turi riboti atakos šaltinio prieigą. • Komponentas turi būti valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai įsilaužimų prevencijos komponentui Komponento paskirtis: kompiuterių apsauga nuo galimų įsilaužimų į sistemą. • Turi turėti HIPS (Host Intrusion Prevention System). • Turi turėti per tinklą gaunamų paketų analizę, palyginti su galimų įsilaužimų scenarijais; • Turi turėti nuolatinį galimų įsilaužimo scenarijų papildymą (atnaujinimą) kartu su virusų aprašais; • Turi turėti kompiuteryje veikiančių procesų stebėjimą, analizę ir blokavimą, jei tipinis procesas bando atlikti sau nebūdingą funkciją (pvz., spausdinimo procesas bando kreiptis į internetą); • Turi turėti potencialiai pavojingų programų, jų instaliacinių paketų identifikavimą kompiuteriuose jų skanavimo metu, galimybę juos ištrinti arba padėti į „karantiną“; • Komponentas turi būti valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai periferinių įrenginių kontrolės komponentui:	• Turi galimybę atlikti išorinių informacijos laikmenų skenavimą; • Siūlomos antivirusinės sistemos gamintojas sėkmingai išlaikęs vieną Virus Bulletin 2012 metų testą VB100; • Turi operatyvaus automatinio atsinaujinimo funkciją; • Operatyvus ataskaitų formavimas apie rastus virusus į valdymo konsolę. • Komponentas valdomas iš bendros valdymo konsolės. • Galimybė uždrausti vartotojams, darbo vietose turintiems administravimo teises, standartinėmis OS priemonėmis sustabdyti antivirusinės programinės įrangos tarnybą. Funkciniai reikalavimai apsaugos nuo įsilaužimų komponentui Komponento paskirtis: kompiuterių apsauga nuo galimų įsilaužimų į sistemą. • Ugniasienė apsaugo nuo nepageidaujamų tinklo išorinių atakų, t.y. pagal nustatytus kriterijus (pagal prievadus (port) ir programas) riboja atakos šaltinio prieigą. • Komponentas valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai įsilaužimų prevencijos komponentui Komponento paskirtis: kompiuterių apsauga nuo galimų įsilaužimų į sistemą. • Turi HIPS (Host Intrusion Prevention System). • Turi per tinklą gaunamų paketų analizę, palyginti su galimų įsilaužimų scenarijais; • Turi nuolatinį galimų įsilaužimo scenarijų papildymą (atnaujinimą) kartu su virusų aprašais; • Turi kompiuteryje veikiančių procesų stebėjimą, analizę ir blokavimą, jei tipinis procesas bando atlikti sau nebūdingą funkciją (pvz., spausdinimo procesas bando kreiptis į internetą); • Turi potencialiai pavojingų programų, jų instaliacinių paketų identifikavimą kompiuteriuose jų skanavimo metu, galimybę juos ištrinti arba padėti į „karantiną“; • Komponentas valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai periferinių

		Komponento paskirtis: kontroliuoti organizacijoje informacijos kopijavimą į išorinius įrenginius, užkirsti kelią žalingų programų patekimui į vidinius tinklus. • Turi turėti galimybę uždrausti naudoti per USB jungiamus išorinius atminties įrenginius (USB atmintines, išorinius diskus, kt.); • Turi turėti galimybę daryti išimtis, pvz., leisti naudotis tik tam tikro aprašyto tipo USB atmintines; • Turi turėti galimybę uždrausti naudoti Bluetooth įrenginių naudojimą; • Komponentas turi būti valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai aplikacijų kontrolės komponentui: Komponento paskirtis: riboti organizacijoje nepageidaujamų programų naudojimą. • Turi turėti galimybę uždrausti darbo vietose naudoti tam tikras programas (pvz., Skype); • Komponentas turi būti valdomas iš bendros valdymo konsolės. Reikalavimai sistemos konfigūracijai ir diegimui • Turi būti galimybė programinę įrangą diegti centralizuotai iš valdymo konsolės, lokaliai iš laikmenos (arba per tinklą) arba per Active Directory Group Policy nustatymus; • Diegimo metu turi būti galimybė pasirinkti kokie komponentai (apsauga nuo virusų, šnipinėjimo programų, ugniasienė, išorinių įrenginių ir aplikacijų kontrolė, prisijungimo prie tinklo kontrolė) bus diegiami į kompiuterį; • Įdiegus į darbo vietos kompiuterį apsaugos sistemą ši neturi reikalauti papildomo konfigūravimo darbų (nustatyti ryšius su valdymo konsole, nurodyti atnaujinimų dislokacijos vietą, derinti kitus nu-statymus); • Visi serveriuose esantys agentai turi būti valdomi iš bendros centralizuotos konsolės. Funkciniai reikalavimai valdymo konsolei: • Konsolėje turi matytis visi sistemos agentus turintys kompiute riai, jų statusas ir bendra informacija; • Turi turėti centralizuoto „karantino“ serveryje funkcionalumą;	įrenginių kontrolės komponentui: Komponento paskirtis: kontroliuoti organizacijoje informacijos kopijavimą į išorinius įrenginius, užkirsti kelią žalingų programų patekimui į vidinius tinklus. • Turi galimybę uždrausti naudoti per USB jungiamus išorinius atminties įrenginius (USB atmintines, išorinius diskus, kt.); • Turi galimybę daryti išimtis, pvz., leisti naudotis tik tam tikro aprašyto tipo USB atmintines; • Turi galimybę uždrausti naudoti Bluetooth įrenginių naudojimą; • Komponentas valdomas iš bendros valdymo konsolės. Funkciniai reikalavimai aplikacijų kontrolės komponentui: Komponento paskirtis: riboti organizacijoje nepageidaujamų programų naudojimą. • Turi galimybę uždrausti darbo vietose naudoti tam tikras programas (pvz., Skype); • Komponentas valdomas iš bendros valdymo konsolės. Reikalavimai sistemos konfigūracijai ir diegimui • Galimybė programinę įrangą diegti centralizuotai iš valdymo konsolės, lokaliai iš laikmenos (arba per tinklą) arba per Active Directory Group Policy nustatymus; • Diegimo metu galimybė pasirinkti kokie komponentai (apsauga nuo virusų, šnipinėjimo programų, ugniasienė, išorinių įrenginių ir aplikacijų kontrolė, prisijungimo prie tinklo kontrolė) bus diegiami į kompiuterį; • Įdiegus į darbo vietos kompiuterį apsaugos sistemą ši nereikalauja papildomo konfigūravimo darbų (nustatyti ryšius su valdymo konsole, nurodyti atnaujinimų dislokacijos vietą, derinti kitus nu-statymus); • Visi serveriuose esantys agentai valdomi iš bendros centralizuotos konsolės. Funkciniai reikalavimai valdymo konsolei: • Konsolėje matosi visi sistemos agentus turintys kompiuteriai, jų statusas ir bendra informacija; • Turi centralizuoto „karantino“ serveryje funkcionalumą;

		• Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams; • Turi leisti keisti pranešimo (alert) apie aptiktą grėsmę turinį; • Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo; • Turi būti suderinama su Microsoft Active Directory (informacijos apie vartotojus ir kompiuterius sinchronizavimas); • Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies parametrų nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį; • Turi turėti galimybę automatiniu būdu (elektroniniu paštu) valdymo serverio administratorių informuoti apie darbo vietoje įvykusį incidentą; • Turi turėti funkcionalumą nustatyti administravimo taisykles nešiojamiems kompiuteriams, kurie nėra pastoviai prijungti prie vidinio tinklo ir nepasiekia valdymo serverio; • Turi turėti funkcionalumą skenuoti kompiuterių tinklą ir rasti kompiuterius, kurie neturi jokios antivirusinės programinės įrangos; • Turi būti funkcionalumas fiksuoti pranešimus apie sisteminius įvykius ir incidentus, įvykusius klientinėje darbo vietoje ir persiųsti juos į centralizuotą valdymo serverį; • Turi turėti ataskaitų sudarymo įvairiais pjūviais funkcionalumą ir grafinių ataskaitų atvaizdavimą; • Turi turėti galimybę vieną valdymo serverį naudoti dviejų nepriklausomų padalinių kompiuerių valdymui, kai naudojamos atskiros licencijos ir šias organizacijas administruoja skirtingi žmonės, realizuojant šį funkcionalumą tokiu būdu, kad valdymo konsolėje organizacijos viena kitai būtų nematomos ir jos naudotų tik joms skirtas licencijas; • Turi turėti galimybę paskirti pasirinktus organizacijoje esančius kompiuterius atnaujinimų ir diegimo paketų retransliavimui naudojant tik kompiuteriuose jau įdiegta antivirusinę programą ir nediegiant papildomų administravimo serverių.	• Turi centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams; • Leidžia keisti pranešimo (alert) apie aptiktą grėsmę turinį; • Centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo; • Suderinama su Microsoft Active Directory (informacijos apie vartotojus ir kompiuterius sinchronizavimas); • Turi funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies parametrų nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį; • Turi galimybę automatiniu būdu (elektroniniu paštu) valdymo serverio administratorių informuoti apie darbo vietoje įvykusį incidentą; • Turi funkcionalumą nustatyti administravimo taisykles nešiojamiems kompiuteriams, kurie nėra pastoviai prijungti prie vidinio tinklo ir nepasiekia valdymo serverio; • Turi funkcionalumą skenuoti kompiuterių tinklą ir rasti kompiuterius, kurie neturi jokios antivirusinės programinės įrangos; • Funkcionalumas fiksuoti pranešimus apie sisteminius įvykius ir incidentus, įvykusius klientinėje darbo vietoje ir persiųsti juos į centralizuotą valdymo serverį; • Turi ataskaitų sudarymo įvairiais pjūviais funkcionalumą ir grafinių ataskaitų atvaizdavimą; • Turi galimybę vieną valdymo serverį naudoti dviejų nepriklausomų padalinių kompiuerių valdymui, kai naudojamos atskiros licencijos ir šias organizacijas administruoja skirtingi žmonės, realizuojant šį funkcionalumą tokiu būdu, kad valdymo konsolėje organizacijos viena kitai būtų nematomos ir jos naudotų tik joms skirtas licencijas; • Turi galimybę paskirti pasirinktus organizacijoje esančius kompiuterius atnaujinimų ir diegimo paketų retransliavimui naudojant tik kompiuteriuose jau įdiegta antivirusinę programą ir nediegiant

Techninė specifikacija

		Atnaujinimai ir palaikymas Pateikiamoms licencijoms turi būti užtikrinamas 3 (trijų) metų gamintojo palaikymas nuo Programinės įrangos pristatymo Perkančiajai organizacijai dienos, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio: • Operatyviai gauti naujausius virusų aprašus (virus definitions), šnipinėjimo programų aprašus (anti-spyware definitions); • Gauti visus sistemos programų atnaujinimus, pataisymus ir naujas versijas; • Gauti technines konsultacijas ir pagalbą; • Gauti technines konsultacijas ir pagalbą internetu; • Klientinės dalies programinė įranga privalo parsisiųsti atnaujinimus tiesiai iš gamintojo atnaujinimų serverio, centralizuoto valdymo serverio arba kt. klientų; • Programinės įrangos gamintojas privalo turėti internetinį puslapį, kuriame būtų žalingų programų ir jų sukeliamų pažeidžiamumų duomenų bazė, informacija apie produktus; • Standartinės aptarnavimo sąlygos vykdomos pagal licencinės sutarties sąlygas.	papildomų administravimo serverių. Atnaujinimai ir palaikymas Pateikiamoms licencijoms užtikrinamas 3(trijų) metų gamintojo palaikymas nuo Programinės įrangos pristatymo Perkančiajai organizacijai dienos, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio: • Operatyviai gauti naujausius virusų aprašus (virus definitions), šnipinėjimo programų aprašus (anti-spyware definitions); • Gauti visus sistemos programų atnaujinimus, pataisymus ir naujas versijas; • Gauti technines konsultacijas ir pagalbą; • Gauti technines konsultacijas ir pagalbą internetu; • Klientinės dalies programinė įranga parsisiunčia atnaujinimus tiesiai iš gamintojo atnaujinimų serverio, centralizuoto valdymo serverio arba kt. klientų; • Programinės įrangos gamintojas turėti internetinį puslapį, kuriame yra žalingų programų ir jų sukeliamų pažeidžiamumų duomenų bazė, informacija apie produktus; • Standartinės aptarnavimo sąlygos vykdomos pagal licencinės sutarties sąlygas.
II.			
2.1	Turimų Sophos XG 135 ugniasienės licencijų (Xstream Protection , Email Protection , Webserver Protection, visos baigiasi 2022.10.09) arba lygiaverčių pratęsimas vienam įrenginiui iki 2025.03.31	**Licencijos turi tikti ugniasienės įrenginiui, pasižyminčiam šiomis savybėmis.** **Reikalavimai fizinėms sąsajoms:** • Ne mažiau 8 x GbE vario prievadų. • Ne mažiau 1 x GbE SFP prievadų (siųstuvo-imtuvo moduliai parduodami atskirai) • Ne mažiau 2 USB jungčių • Ne mažiau 1 micro USB jungtis • Ne mažiau 1 COM (RJ45) jungtis • Ne mažiau 1 HDMI jungtis	Sophos XG 135 ugniasienės licencijų (Xstream Protection , Email Protection, Webserver Protection) pratęsimas vienam įrenginiui iki 2025.03.31 **Licencijos tinka ugniasienės įrenginiui, pasižyminčiam šiomis savybėmis.** **Reikalavimai fizinėms sąsajoms:** • 8 x GbE vario prievadų. • 1 x GbE SFP prievadų (siųstuvo-imtuvo moduliai parduodami atskirai) • 2 USB jungčių • 1 micro USB jungtis • 1 COM (RJ45) jungtis • 1 HDMI jungtis

Techninė specifikacija

		Reikalavimai fiziniams išmatavimams bei aplinkai: • Galimybė montuoti į standartinę 19 colių spintą. • Montavimo dalys užsakomos atskirai • Galimybė veikti esant 0-40°C temperatūrai • Galimybė veikti esant 10%-90% drėgnumui (nekondensuojantis) • Elektros suvartojimas ne daugiau 19 W (be apkrovos), 21 W (pilna apkrova) • Išorinis maitinimo blokas 100-240 VAC, 50-60 Hz • Galimybė pajungti antrą maitinimo bloką (išorinis)	**Reikalavimai fiziniams išmatavimams bei aplinkai:** • Galimybė montuoti į standartinę 19 colių spintą. • Montavimo dalys užsakomos atskirai • Galimybė veikti esant 0-40°C temperatūrai • Galimybė veikti esant 10%-90% drėgnumui (nekondensuojantis) • Elektros suvartojimas 19 W (be apkrovos), 21 W (pilna apkrova) • Išorinis maitinimo blokas 100-240 VAC, 50-60 Hz • Galimybė pajungti antrą maitinimo bloką (išorinis)
		Reikalavimai tinklo srauto apdorojimo pajėgumams: • Integruotas SDD skirtas vietiniam karantinui, talpyklai (cache) bei žurnalui (log) • Ugniasienės pralaidumas ne mažiau 8 Gbps • Ugniasienės IMIX pralaidumas ne mažiau 5 Gbps • Virtualaus privataus tinklo prieigos vartų pralaidumas ne mažiau 1.18 Gbps • Apsaugos nuo įsiveržimo (IPS) pralaidumas ne mažiau 2.48 Gbps • Next-Generation Ugniasienės (IPS + App Ctrl) pralaidumas ne mažiau 1.2 Gbps • Antivirusinės sistemos skenavimo srauto pralaidumas ne mažiau kaip 1.58 Mbps. • TCP konkurencinių prisijungimų skaičius ne mažiau kaip 6 000 000 • TCP naujų sesijų per sekundę ne mažiau 85 000	**Reikalavimai tinklo srauto apdorojimo pajėgumams:** • Integruotas SDD skirtas vietiniam karantinui, talpyklai (cache) bei žurnalui (log) • Ugniasienės pralaidumas 8 Gbps • Ugniasienės IMIX pralaidumas 5 Gbps • Virtualaus privataus tinklo prieigos vartų pralaidumas 1.18 Gbps • Apsaugos nuo įsiveržimo (IPS) pralaidumas 2.48 Gbps • Next-Generation Ugniasienės (IPS + App Ctrl) pralaidumas 1.2 Gbps • Antivirusinės sistemos skenavimo srauto pralaidumas 1.58 Mbps. • TCP konkurencinių prisijungimų skaičius 6 000 000 • TCP naujų sesijų per sekundę 85 000
		Valdymo ir aukšto patikimumo reikalavimai: • Valdymas turi būti paremtas internetine naršykle be papildomos programinės įrangos įdiegimo. Komunikacija turi būti šifruojama per HTTPS. • Turi būti galimybė sukurti kelis vartotojus įrenginio valdymui (administrator accounts). • Galimybė naudoti dviejų faktorių autentifikavimą administratoriams, vartotojų savitarnos portalui bei VPN prisijungimams. • Administravimas turi būti paremtas rolėmis su galimybe kurti savo roles. Galimybė sukurti rolę kuriai leidžiama	**Valdymo ir aukšto patikimumo reikalavimai:** • Valdymas paremtas internetine naršykle be papildomos programinės įrangos įdiegimo. Komunikacija šifruojama per HTTPS. • Galimybė sukurti kelis vartotojus įrenginio valdymui (administrator accounts). • Galimybė naudoti dviejų faktorių autentifikavimą administratoriams, vartotojų savitarnos portalui bei VPN prisijungimams. • Administravimas paremtas rolėmis su galimybe kurti savo roles. Galimybė sukurti rolę kuriai leidžiama tik peržiūrėti parametrus, bet

		tik peržiūrėti parametrus, bet neleidžiama jų keisti. • Turi būti galimybė keliems administratoriams prisijungti bei daryti pakeitimus vienu metu. • Administratoriaus vartotojas turi būti automatiškai atjungiamas (log off) po tam tikro neveiksnumo (idle) laiko. • Turi būti numatyta galimybė įsigyti centralizuoto valdymo konsolę kelių atskirų ir geografiškai nutolusių saugumo sistemų valdymui tuo pačiu metu iš vieno valdymo centro. Ši platforma turi būti pateikiama kaip virtualus arba fizinis įrenginys. • Turi būti galimybė įrenginį valdyti per API, kad būtų galima sujungti su trečiųjų šalių įrankiais. • Turi būti galimybė valdyti įrenginį per komandinę eilutę. • Turi būti galimybė daryti atsargines nustatymų kopijas lokaliai, į FTP, į e-mail / rankiniu būtų, kas dieną, kas savaitę, kas mėnesį. Turi būti galimybė užkoduoti atsargines kopijas su administratoriaus pasirinktu slaptažodžiu. • Administravimo įrankyje turi būti galimybė klonuoti objektus. • Turi būti patogūs trigdžių šalinimo įrankiai, tokie kaip registro peržiūra (log viewer), paketų surinkimas (packet capture), ugniasienės taisyklių tikrinimas. • Visi atnaujinimai turi būti pateikiami iš sprendimo gamintojo. • Atnaujinimai turėtų būti atsiunčiami automatiškai ir laikomi saugumo sistemoje integruotame diske. Taip pat turi būti galimybė atnaujinimus diegti iš USB atmintinės jei įrenginys neturi interneto prieigos. • Šablonų aprašymų atnaujinimai turi būti atsiunčiami ir įdiegiami automatiškai. • „Firmware“ ir aprašų šablonų įkėlimas gali būti atliekamas pagal iš anksto sudarytą grafiką. • Turi būti siunčiami automatiniai pranešimai apie atsiradusią naują „firmware“ versiją. • Turi būti galimybė grąžinti ankstesnę „firmware“ versiją per grafinę vartotojo sąsają perkrovus įrenginį, bet ne perrašant operacinės sistemos. • Turi būti galimybė naudoti 2 įrenginius aukštam patikimumui	neleidžiama jų keisti. • Galimybė keliems administratoriams prisijungti bei daryti pakeitimus vienu metu. • Administratoriaus vartotojas automatiškai atjungiamas (log off) po tam tikro neveiksnumo (idle) laiko. • Numatyta galimybė įsigyti centralizuoto valdymo konsolę kelių atskirų ir geografiškai nutolusių saugumo sistemų valdymui tuo pačiu metu iš vieno valdymo centro. Ši platforma pateikiama kaip virtualus arba fizinis įrenginys. • Galimybė įrenginį valdyti per API, kad būtų galima sujungti su trečiųjų šalių įrankiais. • Galimybė valdyti įrenginį per komandinę eilutę. • Galimybė daryti atsargines nustatymų kopijas lokaliai, į FTP, į e-mail / rankiniu būtų, kas dieną, kas savaitę, kas mėnesį. Galimybė užkoduoti atsargines kopijas su administratoriaus pasirinktu slaptažodžiu. • Administravimo įrankyje galimybė klonuoti objektus. • Patogūs trigdžių šalinimo įrankiai, tokie kaip registro peržiūra (log viewer), paketų surinkimas (packet capture), ugniasienės taisyklių tikrinimas. • Visi atnaujinimai pateikiami iš sprendimo gamintojo. • Atnaujinimai atsiunčiami automatiškai ir laikomi saugumo sistemoje integruotame diske. Taip pa yra galimybė atnaujinimus diegti iš USB atmintinės jei įrenginys neturi interneto prieigos. • Šablonų aprašymų atnaujinimai atsiunčiami ir įdiegiami automatiškai. • „Firmware“ ir aprašų šablonų įkėlimas atliekamas pagal iš anksto sudarytą grafiką. • Siunčiami automatiniai pranešimai apie atsiradusią naują „firmware“ versiją. • Galimybė grąžinti ankstesnę „firmware“ versiją per grafinę vartotojo sąsają perkrovus įrenginį, bet ne perrašant operacinės sistemos. • Galimybė naudoti 2 įrenginius aukštam patikimumui užtikrinti. Galimi aukšto patikimumo rėžimai: aktyvus-aktyvus bei aktyvus-pasyvus.

		užtikrinti. Galimi aukšto patikimumo rėžimai: aktyvus-aktyvus bei aktyvus-pasyvus. • Turi būti galimybė matyti konfigūracijos pakeitimus.	• Galimybė matyti konfigūracijos pakeitimus.
		Reikalavimai paketų filtrui ir maršrutizavimui: • Išsamus paketų inspektavimas (angl. „deep packet inspection“). • Paketų filtras paremtas prievadais ir zonomis. • NAT (angl. Network Address Translation) maskavimas. • PAT (angl. Port Address Translation). • SNAT (angl. Source Network Address Translation). • DNAT (angl. Destination Network Address Translation). • Pilnas NAT (angl. FullNAT). • NAT išimtys (angl. NoNAT). •1:1 NAT (Network Address Translation). • IP ir MAC adresais paremtas filtravimas. • Turi palaikyti kelių prievadų sugrupavimą (angl. link aggregation) pagrįstą 802.3ad standartu. • Registrų įjungimas/išjungimas taisyklei • Aprašymas/įvardinimas kompiuterių, tinklų ir servisų. • Turi galėti apjungti objektus į grupes. • Turi būti integruotos sistemos registrai/ataskaitos, taip pat registras taisyklių taikymo aktyvumui. • Turi palaikyti statinį ir dinaminį maršrutizavimą (RIP, BGP, OSPF). • Turi palaikyti nepriklausomų grupinio transliavimo protokolų maršrutizavimą. • Turi palaikyti VLAN žymėjimą. • Galimybė blokuoti pagal kilmės šalį (valstybę): * Galimybė nurodyti blokuojamos šalies srauto kryptį (įeinančiam/išeinančiam) srautui; * Nustatomos išimtys. • Turi būti integruota naujos kartos ugniasienės technologija leidžianti filtruoti remiantis aplikacija/paslauga: * Turi būti galima daryti išimtis remiantis vartotoju/IP/ tinklu; * Atpažįstamų aplikacijų duomenų bazę turi sudaryti ne mažiau nei 1000 aplikacijų; * Naujų aplikacijų aprašai turi būti	**Reikalavimai paketų filtrui ir maršrutizavimui:** • Išsamus paketų inspektavimas (angl. „deep packet inspection“). • Paketų filtras paremtas prievadais ir zonomis. • NAT (angl. Network Address Translation) maskavimas. • PAT (angl. Port Address Translation). • SNAT (angl. Source Network Address Translation). • DNAT (angl. Destination Network Address Translation). • Pilnas NAT (angl. FullNAT). • NAT išimtys (angl. NoNAT). •1:1 NAT (Network Address Translation). • IP ir MAC adresais paremtas filtravimas. • Palaiko kelių prievadų sugrupavimą (angl. link aggregation) pagrįstą 802.3ad standartu. • Registrų įjungimas/išjungimas taisyklei • Aprašymas/įvardinimas kompiuterių, tinklų ir servisų. • Gali apjungti objektus į grupes. • Integruotos sistemos registrai/ataskaitos, taip pat registras taisyklių taikymo aktyvumui. • Palaiko statinį ir dinaminį maršrutizavimą (RIP, BGP, OSPF). • Palaiko nepriklausomų grupinio transliavimo protokolų maršrutizavimą. • Palaiko VLAN žymėjimą. • Galimybė blokuoti pagal kilmės šalį (valstybę): * Galimybė nurodyti blokuojamos šalies srauto kryptį (įeinančiam/išeinančiam) srautui; * Nustatomos išimtys. • Integruota naujos kartos ugniasienės technologija leidžianti filtruoti remiantis aplikacija/paslauga: * Galima daryti išimtis remiantis vartotoju/IP/ tinklu; * Atpažįstamų aplikacijų duomenų bazę sudaro 1000 aplikacijų; * Naujų aplikacijų aprašai atnaujinami automatiškai;

		atnaujinami automatiškai; * Dinaminis aplikacijų blokavimas remiantis rizikos klase ir produktyvumo indeksacija. • DHCP palaikymas: * Turi būti integruotas DHCP serveris; * Statinis išdavimas (static lease); * Turi būti integruotas DHCP persiuntimas (angl. relay). • Interneto prievadų (WAN) balansavimo reikalavimai: * Turi automatiškai balansuoti srautą tarp kelių interneto prievadų. * Turi būti įdiegtas interneto prievadų diagnozavimo mechanizmas. * Sugedus pagrindiniam interneto prievadui turi automatiškai persijungti į atsarginę interneto liniją.	* Dinaminis aplikacijų blokavimas remiantis rizikos klase ir produktyvumo indeksacija. • DHCP palaikymas: * Integruotas DHCP serveris; * Statinis išdavimas (static lease); * Integruotas DHCP persiuntimas (angl. relay). • Interneto prievadų (WAN) balansavimo reikalavimai: * Automatiškai balansuoja srautą tarp kelių interneto prievadų. * Įdiegtas interneto prievadų diagnozavimo mechanizmas. * Sugedus pagrindiniam interneto prievadui automatiškai persijungia į atsarginę interneto liniją.
		Srauto prioritizavimo ir valdymo reikalavimai: • Galimybė prioritizuoti (Quality of Service) srautą pagal kompiuterį, servisą bei vartotoją. • Galimybė vartotojams nustatyti persiunčiamų duomenų kvotas. Bendra kvota ir arba periodinė kvota. • Galimybė taikyti VoIP optimizacijas. • Galimybė naudoti DSCP žymes.	**Srauto prioritizavimo ir valdymo reikalavimai:** • Galimybė prioritizuoti (Quality of Service) srautą pagal kompiuterį, servisą bei vartotoją. • Galimybė vartotojams nustatyti persiunčiamų duomenų kvotas. Bendra kvota ir arba periodinė kvota. • Galimybė taikyti VoIP optimizacijas. • Galimybė naudoti DSCP žymes.
		Reikalavimai vartotojų autentifikavimui: • Vietiniai vartotojai (valdomi ir laikomi saugumo sistemoje) • Turi palaikyti šiuos autentikavimo metodus: * RADIUS * TACACS+ * LDAP * eDirectory • Turi palaikyti skaidrų tarpinės tarnybinės stoties autentikavimą (NTLM) arba autentikavimą su kompiuteryje įdiegtu agentu. • Turi turėti autentikavimo agentus šioms operacinėms sistemoms: * Windows * Mac OS X * Linux 32/64 • Galimybė naudoti kelis autentifikacijos būdus paraleliai, pavyzdžiui kelis Active Directory serverius. • Reikalavimai vartotojų autentifikacija skaidriame rėžime: * Active Directory SSO; * Autentifikacija vietiniame portale.	**Reikalavimai vartotojų autentifikavimui:** • Vietiniai vartotojai (valdomi ir laikomi saugumo sistemoje) • Palaiko šiuos autentikavimo metodus: * RADIUS * TACACS+ * LDAP * eDirectory • Palaiko skaidrų tarpinės tarnybinės stoties autentikavimą (NTLM) arba autentikavimą su kompiuteryje įdiegtu agentu. • Turi autentikavimo agentus šioms operacinėms sistemoms: * Windows * Mac OS X * Linux 32/64 • Galimybė naudoti kelis autentifikacijos būdus paraleliai, pavyzdžiui kelis Active Directory serverius. • Reikalavimai vartotojų autentifikacija skaidriame rėžime: * Active Directory SSO; * Autentifikacija vietiniame portale.

		• Turi turėti vienkartinių slaptažodžių funkcionalumą (angl. OTP) per RADIUS/TACACS/LDAP (išoriniai) arba per integruota (vidini) Reikalavimai vidinei OTP fukcijai: * vienkartinio slaptažodžio aplikacija (angl. OTP) skirta Android ir iOS; * turi būti be papildomos licencijos išoriniam OTP serveriui * Turi būti galimybė pradinius nustatymus atlikti per savitarnos portalą * Turi palaikyti trečių šalių fizinius. • OTP įrenginius. • Vienkartinių slaptažodžių funkcionalumas turi veikti su šiomis įrenginio funkcijomis: * IPSec nuotolinė prieiga; * SSL VPN; * Vartotojų savitarnos portalas; * Administratoriaus WEB konsolė. • Google Chromebook autentifikavimo palaikymas kai naudojama Active Directory ir Google Gsuite.	• Turi vienkartinių slaptažodžių funkcionalumą (angl. OTP) per RADIUS/TACACS/LDAP (išoriniai) arba per integruota (vidini) Reikalavimai vidinei OTP fukcijai: * vienkartinio slaptažodžio aplikacija (angl. OTP) skirta Android ir iOS; * be papildomos licencijos išoriniam OTP serveriui * Galimybė pradinius nustatymus atlikti per savitarnos portalą * Palaiko trečių šalių fizinius. • OTP įrenginius. • Vienkartinių slaptažodžių funkcionalumas veikia su šiomis įrenginio funkcijomis: * IPSec nuotolinė prieiga; * SSL VPN; * Vartotojų savitarnos portalas; * Administratoriaus WEB konsolė. • Google Chromebook autentifikavimo palaikymas kai naudojama Active Directory ir Google Gsuite.
		Turi būti vartotojų savitarnos portalas, kuris minimaliai galėtų atlikti šiuos veiksmus: • * Parsisiųsti VPN prieigos klientą ir jo konfigūracinį failą * Sužinoti WiFi prieigos informaciją * Pakeisti vartotojo slaptažodį * Patikrinti asmeninę interneto naršymo ataskaitą * Peržiūrėti elektroninio pašto žinutes esančias karantine * Susikonfigūruoti dviejų faktorių autentifikaciją su QR kodu	**Vartotojų savitarnos portalas, kuris minimaliai gali atlikti šiuos veiksmus:** • * Parsisiųsti VPN prieigos klientą ir jo konfigūracinį failą * Sužinoti WiFi prieigos informaciją * Pakeisti vartotojo slaptažodį * Patikrinti asmeninę interneto naršymo ataskaitą * Peržiūrėti elektroninio pašto žinutes esančias karantine * Susikonfigūruoti dviejų faktorių autentifikaciją su QR kodu
		Reikalavimai virtualaus privataus tinklo technologijai: • Turi palaikyti Cisco klientus • PPTP prisijungimas (Client-to-Site architektūroje) • L2TP per IPSec prisijungimas (Client-to-Site architektūroje) • Turi palaikyti Windows IPSec Tunnel modulį • Reikalavimai standartiniams IPSec prisijungimams „Site-to-Site“ architektūroje: * IPSec tunelio aprašymas keliems vietiniams/nutolusiems tinklams; * „Site-to-Site“ VPN galimybė tarp dviejų sistemų turinčių dinaminius IP abiejose pusėse.	**Reikalavimai virtualaus privataus tinklo technologijai:** • Palaiko Cisco klientus • PPTP prisijungimas (Client-to-Site architektūroje) • L2TP per IPSec prisijungimas (Client-to-Site architektūroje) • Palaiko Windows IPSec Tunnel modulį • Reikalavimai standartiniams IPSec prisijungimams „Site-to-Site“ architektūroje: * IPSec tunelio aprašymas keliems vietiniams/nutolusiems tinklams; * „Site-to-Site“ VPN galimybė tarp dviejų sistemų turinčių dinaminius IP abiejose pusėse.

		• Turi palaikyti NAT-Traversal funkcionalumą. • Turi būti palaikomi šie šifravimo algoritmai: * DES bei 3DES; * AES/Rijndael (128, 192 bei 256 Bit); * SHA1 bei SHA2 (256, 384, 512 Bit); * DH Grupės 1,2,5,14 * Blowfish bei TwoFish; * Serpent; * MD5. • SSL VPN prisijungimai (Client-to-Site architektūroje): * Turi dirbti su tarpinėmis tarnybinėmis stotimis ir NAT maršrutizatoriais; * Turi galėti priskirti kliento IP iš adresų sąrašo (pool); * Tunelio modulis (galimybė naudoti visus intraneto servisus). • SSL VPN prisijungimai (Site-to-Site architektūroje): * Turi dirbti su tarpinėmis tarnybinėmis stotimis ir NAT maršrutizatoriais; * Turi priskirti kliento IP iš adresų sąrašo (pool); * Tunelio modulis (galimybė naudoti visus intraneto servisus); • * Prisijungimai į abi kryptis.	• Palaiko NAT-Traversal funkcionalumą. • Palaikomi šie šifravimo algoritmai: * DES bei 3DES; * AES/Rijndael (128, 192 bei 256 Bit); * SHA1 bei SHA2 (256, 384, 512 Bit); * DH Grupės 1,2,5,14 * Blowfish bei TwoFish; * Serpent; * MD5. • SSL VPN prisijungimai (Client-to-Site architektūroje): * Dirba su tarpinėmis tarnybinėmis stotimis ir NAT maršrutizatoriais; * Gali priskirti kliento IP iš adresų sąrašo (pool); * Tunelio modulis (galimybė naudoti visus intraneto servisus). • SSL VPN prisijungimai (Site-to-Site architektūroje): * Dirba su tarpinėmis tarnybinėmis stotimis ir NAT maršrutizatoriais; * Priskiria kliento IP iš adresų sąrašo (pool); * Tunelio modulis (galimybė naudoti visus intraneto servisus); • * Prisijungimai į abi kryptis.
		Reikalavimai integruotoms saugumo sistemoje ataskaitoms bei registrui ir įspėjimo pranešimams: • Ataskaitų kešavimas kietajame sistemos diske (galioja tik modeliams su SSD disku) • Turi būti pateikiama grafinė informacija apie įrangą (CPU, kietąjį diską, tinklą...); • Turi būti pateikiama grafinė informacija apie vartotojų interneto vartojimą (persiųstų MB kiekį, top siuntėjai, top puslapiai ...) ir tinklo utilizaciją. • Ataskaitų informacijos anonimizavimo (maskavimo) galimybė (el.pašto) (vartotojo vardas/IP adresas, pašto domenas ir pašto adresai turėtų būti uždengiami). Atrakinimas šios informacijos turėtų vykti dviejų slaptažodžių pagalba. • Galimybė eksportuoti atsakaitas HTML, PDF, Excel (XLS) formatais. • Registras turi būti galimas keliuose išoriniuose Syslog serveriuose • Registras centriniame ataskaitų	**Reikalavimai integruotoms saugumo sistemoje ataskaitoms bei registrui ir įspėjimo pranešimams:** • Ataskaitų kešavimas kietajame sistemos diske (galioja tik modeliams su SSD disku) • Pateikiama grafinė informacija apie įrangą (CPU, kietąjį diską, tinklą...); • Pateikiama grafinė informacija apie vartotojų interneto vartojimą (persiųstų MB kiekį, top siuntėjai, top puslapiai ...) ir tinklo utilizaciją. • Ataskaitų informacijos anonimizavimo (maskavimo) galimybė (el.pašto) (vartotojo vardas/IP adresas, pašto domenas ir pašto adresai turėtų būti uždengiami). Atrakinimas šios informacijos vyksta dviejų slaptažodžių pagalba. • Galimybė eksportuoti atsakaitas HTML, PDF, Excel (XLS) formatais. • Registras galimas keliuose išoriniuose Syslog serveriuose • Registras centriniame ataskaitų serveryje • Atskiri registrų failai skirtingiems

		serveryje • Atskiri registrų failai skirtingiems moduliams • Įspėjimo pranešimas per SNMP Trap (SNMPv2 ir SNMPv3 palaikymas)	moduliams • Įspėjimo pranešimas per SNMP Trap (SNMPv2 ir SNMPv3 palaikymas
		Reikalavimai įsiveržimo aptikimo ir prevencijos sistemai: • Turi būti integruota apsauga nuo atsisakymo aptarnauti atakų (angl. DoS); • Rankinis pavienių atakų išjungimas • Galimybė nustatyti apsaugą remiantis pagal atakas į operacines sistemas • Galimybė nustatyti išimtis IDS taisyklių taikymui tinklams ir kompiuteriams • Anomalijų aptikimas (apsauga nuo nulinės dienos atakų) • Prievadų skanavimo aptikimas • Atskiri registrų lygiai IDS ir IPS dalims • Turi būti integruota apsauga nuo komunikacijos su žalingomis valdymo tarnybinėmis stotimis (angl. Botnet command and control server) • Turi būti automatiniai šablonų atnaujinimai • Sistema turi galėti aptikti pažengusius pavojus, tokius, kaip botnet tinklai ar komandų ir kontrolės serverius, keliais mechanizmais (minimaliai ugniasienės, DNS, IPS, web proksi) • SYN Flood aptikimas: * Turi būti numatyta galimybė daryti išimtis;	**Reikalavimai įsiveržimo aptikimo ir prevencijos sistemai:** • Integruota apsauga nuo atsisakymo aptarnauti atakų (angl. DoS); • Rankinis pavienių atakų išjungimas • Galimybė nustatyti apsaugą remiantis pagal atakas į operacines sistemas • Galimybė nustatyti išimtis IDS taisyklių taikymui tinklams ir kompiuteriams • Anomalijų aptikimas (apsauga nuo nulinės dienos atakų) • Prievadų skanavimo aptikimas • Atskiri registrų lygiai IDS ir IPS dalims • Integruota apsauga nuo komunikacijos su žalingomis valdymo tarnybinėmis stotimis (angl. Botnet command and control server) • Automatiniai šablonų atnaujinimai • Sistema gali aptikti pažengusius pavojus, tokius, kaip botnet tinklai ar komandų ir kontrolės serverius, keliais mechanizmais (minimaliai ugniasienės, DNS, IPS, web proksi) • SYN Flood aptikimas: * Numatyta galimybė daryti išimtis; * Registrai; * Syn Flood normos reguliavimas; * Pagal šaltinį (source)/ paskirtį

		* Registrai; * Syn Flood normos reguliavimas; * Pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas. UDP Flood aptikimas: * Turi būti numatyta galimybė daryti išimtis; * Registrai; * UDP Flood normos reguliavimas; * Pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas. • ICMP Flood aptikimas: * Turi būti numatyta galimybė daryti išimtis; * Registrai; * ICMP Flood normos reguliavimas; * Pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas.	(destination)/ maišytas nustatymas. UDP Flood aptikimas: * Numatyta galimybė daryti išimtis; * Registrai; * UDP Flood normos reguliavimas; * Pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas. • ICMP Flood aptikimas: * Numatyta galimybė daryti išimtis; * Registrai; * ICMP Flood normos reguliavimas; * Pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas.

Techninė specifikacija

		Ugniasienės bei kompiuterio apsaugos suderinamumas / sinchronizavimas: • Galimybė diegti galutinio kompiuterio apsaugos agentą (gali būti su atskira licencija), kuris apima tokį funkcionalumą: * Apsauga nuo kenkėjiškų programų * Apsauga nuo išnaudojimų panaudojimo ("Anti-Exploit") * Web filtravimą * Pažeidžiamumų skenavimą * Galinio įrenginio programinės įrangos inventorizavimą * Aplikacijų ugniasienę * Galimybę naudoti dviejų faktorių autentifikaciją. • Agentas turi gebėti susieti ir integruoti galinio įrenginio apsaugą su perkama ugniasiene bei užtikrinti įrenginio identifikavimą, automatiškai jį karantinuoti užkrėtimo atveju, atvaizduoti jį tinklo struktūroje, leisti centralizuotai jį valdyti ir taikyti skirtingus konfigūravimo profilius, taip pat užtikrinti žurnalinių įrašų kaupimą. Turi integruotis su tapatybių šaltiniu Microsoft Active Directory. • Agentas turi veikti WINDOWS, MAC OS X, LINUX operacinėse sistemose, Windows OS atveju išvardinti reikalavimai turi būti realizuoti pilna apimti, likusių OS atveju gali būti vykdomi dalinai.	**Ugniasienės bei kompiuterio apsaugos suderinamumas / sinchronizavimas:** • Galimybė diegti galutinio kompiuterio apsaugos agentą (su atskira licencija), kuris apima tokį funkcionalumą: * Apsauga nuo kenkėjiškų programų * Apsauga nuo išnaudojimų panaudojimo ("Anti-Exploit") * Web filtravimą * Pažeidžiamumų skenavimą * Galinio įrenginio programinės įrangos inventorizavimą * Aplikacijų ugniasienę * Galimybę naudoti dviejų faktorių autentifikaciją. • Agentas geba susieti ir integruoti galinio įrenginio apsaugą su perkama ugniasiene bei užtikrinti įrenginio identifikavimą, automatiškai jį karantinuoti užkrėtimo atveju, atvaizduoti jį tinklo struktūroje, leisti centralizuotai jį valdyti ir taikyti skirtingus konfigūravimo profilius, taip pat užtikrinti žurnalinių įrašų kaupimą. Integruojasi su tapatybių šaltiniu Microsoft Active Directory. • Agentas veikia WINDOWS, MAC OS X, LINUX operacinėse sistemose, Windows OS atveju išvardinti reikalavimai realizuoti pilna apimti, likusių OS atveju vykdomi dalinai.
		VPN veikiantis per naršyklę: • Turi palaikyti be klientų VPN: * Turi veikti naršyklės pagrindu; * Turi nereikalauti įskiepių (plugin), naršyklės priedėlių (add-on), papildomų aplikacijų; * Turi palaikyti RDP, VNC, Telnet, SSH, HTTP/S protokolus.	**VPN veikiantis per naršyklę:** • Palaiko be klientų VPN: * Veikia naršyklės pagrindu; * Nereikalauja įskiepių (plugin), naršyklės priedėlių (add-on), papildomų aplikacijų; * Palaiko RDP, VNC, Telnet, SSH, HTTP/S protokolus.

Techninė specifikacija

		Reikalavimai interneto saugumo funkcionalumui: • Turi būti galimos išimtys šaltinio IP/Tinklams; • Maksimalus skenuojamo failo dydis nustatomas pagal poreikį • Web turinio filtro praleidimas pagal poreikį (blokuojamiems URL) • Turi būti integruoti nemažiau nei du virusų skenavimo varikliai su skirtingomis virusų aprašų bazėmis. Turi būti galimybė naudoti abu skenavimo variklius tuo pačiu metu. • Pirminės tarpinės tarnybinės stoties palaikymas: * Vartotojų autentifikacija pirminėje tarpinėje tarnybinėje stotyje; * Neribotas pirminių tarpinių tarnybinių stočių skaičius; * Pirminės tarpinės tarnybinės stoties pasirinkimas remiantis tokiais parametrais, kaip šaltinio IP, vartotojas/grupė vartotojų, laikas, domenas, URL. • HTTP tarpinės tarnybinės stoties PAC failų talpinimas: * Auto-config kliento per DHCP; * Auto-config kliento per DNS. • Antivirusinė apsauga skirta: * HTTP atsiuntimams; * HTTPS atsisiuntimams; * FTP atsisiuntimams (per naršyklę); * FTP atsisiuntimams (komandinė eilutė/FTP klientas) (skaidrus FTP tarpinės tarnybinės stoties). • Skirtingų saugumo profilių konfigūravimas: * Atskyrimas paremtas vietine autentifikacija; * Atskyrimas paremtas LDAP direktorija; * Atskyrimas paremtas AD SSO; * Atskyrimas paremtas eDirectory SSO; * Atskyrimas paremtas tinklu (vartotojo IP adresas); * Autentifikacija per RADIUS; * Autentifikacija per TACACS+. • Reikalavimai filtravimui ir blokavimui: * Pagal URL kategorijas; * Pagal baltą sąrašą; * Pagal juodą sąrašą; * Pagal Java/JavaScript/ActiveX; * MIME tipo tikrinimas proksio apžiūra (magic lookup). * Pagal failų plėtinius (.exe, .gif, …);	**Reikalavimai interneto saugumo funkcionalumui:** • Galimos išimtys šaltinio IP/Tinklams; • Maksimalus skenuojamo failo dydis nustatomas pagal poreikį • Web turinio filtro praleidimas pagal poreikį (blokuojamiems URL) • Integruoti du virusų skenavimo varikliai su skirtingomis virusų aprašų bazėmis. Galimybė naudoti abu skenavimo variklius tuo pačiu metu. • Pirminės tarpinės tarnybinės stoties palaikymas: * Vartotojų autentifikacija pirminėje tarpinėje tarnybinėje stotyje; * Neribotas pirminių tarpinių tarnybinių stočių skaičius; * Pirminės tarpinės tarnybinės stoties pasirinkimas remiantis tokiais parametrais, kaip šaltinio IP, vartotojas/grupė vartotojų, laikas, domenas, URL. • HTTP tarpinės tarnybinės stoties PAC failų talpinimas: * Auto-config kliento per DHCP; * Auto-config kliento per DNS. • Antivirusinė apsauga skirta: * HTTP atsiuntimams; * HTTPS atsisiuntimams; * FTP atsisiuntimams (per naršyklę); * FTP atsisiuntimams (komandinė eilutė/FTP klientas) (skaidrus FTP tarpinės tarnybinės stoties). • Skirtingų saugumo profilių konfigūravimas: * Atskyrimas paremtas vietine autentifikacija; * Atskyrimas paremtas LDAP direktorija; * Atskyrimas paremtas AD SSO; * Atskyrimas paremtas eDirectory SSO; * Atskyrimas paremtas tinklu (vartotojo IP adresas); * Autentifikacija per RADIUS; * Autentifikacija per TACACS+. • Reikalavimai filtravimui ir blokavimui: * Pagal URL kategorijas; * Pagal baltą sąrašą; * Pagal juodą sąrašą; * Pagal Java/JavaScript/ActiveX; * MIME tipo tikrinimas proksio apžiūra (magic lookup). * Pagal failų plėtinius (.exe, .gif, …); * Pagal MIME dokumentų tipą (iš

		* Pagal MIME dokumentų tipą (iš serverio): * Turi būti integruota šnipinėjimo programinę įranga aptinkanti sistema (turi tikrinti įeinantį srautą ir "skambinimą namo" (išeinantį) srautą); * Pagal potencialiai nepageidaujamą aplikaciją; * Remiantis aplikacijų lygiu (L7 ugniasienė); * Pagal nežinomą (neįtrauktas į kategoriją) tinklalapį; * Filtravimas paremtas laiko parametru arba diena. • URL filtro funkcionalumo reikalavimai: * Kategorijų grupės neribotos; * Reputacija paremtas URL blokavimas; * Leisti/blokuoti kategorijas remiantis laiko parametru arba diena; * Turi būti daugiau nei 90 skirtingų kategorijų; * URL duomenų bazės užklausos realiu laiku (nėra poreikio duomenų bazės atnaujinimams); * URL filtras juodo sąrašo rėžime (viskas leidžiama išskyrus nepasirinktas kategorijas) arba balto sąrašo rėžimas (viską blokuoti išskyrus pasirinktas kategorijas); * Pasirenkamos išimtys remiantis tokiais parametrais, kaip: Šaltinis/Tikslas/Domenas/Serveris/ Kategorija	serverio): * Integruota šnipinėjimo programinę įranga aptinkanti sistema (tikrina įeinantį srautą ir "skambinimą namo" (išeinantį) srautą); * Pagal potencialiai nepageidaujamą aplikaciją; * Remiantis aplikacijų lygiu (L7 ugniasienė); * Pagal nežinomą (neįtrauktas į kategoriją) tinklalapį; * Filtravimas paremtas laiko parametru arba diena. • URL filtro funkcionalumo reikalavimai: * Kategorijų grupės neribotos; * Reputacija paremtas URL blokavimas; * Leisti/blokuoti kategorijas remiantis laiko parametru arba diena; * Daugiau nei 90 skirtingų kategorijų; * URL duomenų bazės užklausos realiu laiku (nėra poreikio duomenų bazės atnaujinimams); * URL filtras juodo sąrašo rėžime (viskas leidžiama išskyrus nepasirinktas kategorijas) arba balto sąrašo rėžimas (viską blokuoti išskyrus pasirinktas kategorijas); * Pasirenkamos išimtys remiantis tokiais parametrais, kaip: Šaltinis/Tikslas/Domenas/Serveris/ Kategorija

Techninė specifikacija

		Reikalavimai elektroninio pašto saugumo funkcionalumui: • SMTP prieigos vartų rėžimas • Skaidrus rėžimas (MX įrašo konfigūravimas nėra būtinas) • El.pašto persiuntimas su „round robin“ • SMTP autentifikacija (el.paštas priimamas tik tada jei vartotojas yra autentifikuotas) • Antivirusinė apsauga skirta SMTP, POP3, IMAP • 2 ar daugiau integruoti skirtingų gamintojų virusų aprašų bazės • Gaunančiųjų domenų skaičius neribotas • Antispam apsauga SMTP,POP3, IMAP srautui • Administratorius turi galėti konfigūruoti POP3 žinutę (pvz. rastas virusas) pagal poreikius. • Neturi būti licencinių apribojimų konkurenciniams el.pašto prisijungimams. • Pašto maršruto konfigūravimas: * Prieš-srautinis pašto persiuntimas su autentifikacija; * MX-paremtas maršrutizavimas; * Atskiri pašto prieigos vartai domenui; * Atskiri pašto serveriai domenui. • TLS palaikymas: * Konfigūruojamas dedikuotam pašto serveriui; * Konfigūruojamas dedikuotam domenui; * TLS sertifikatas gali būti keičiamas. * Galimybė išjungti TLS tam tikriems pašto serveriams • Reikalavimai Anti-SPAM apsaugai: * Galimi filtro veiksmai “Ištrinti”, “Įspėti”, “Ignoruoti” ir “Karantinuoti”; * Galimybė keisti pridedamą žymę “SPAM” el.pašto pavadinimo laukelyje; * Anti-Spam siuntėjų globalus baltas sąrašas; * Anti-Spam siuntėjo baltas sąrašas kiekvienam el.pašto gavėjui (nustatomas pačio vartotojo); * Anti-Spam siuntėjo juodas sąrašas kiekvienam el.pašto gavėjui (nustatomas pačio vartotojo); * Juodi/Balti sąrašai gali būti keičiami administratoriaus. • El.pašto filtravimas turi būti atliekamas remiantis:	**Reikalavimai elektroninio pašto saugumo funkcionalumui:** • SMTP prieigos vartų rėžimas • Skaidrus rėžimas (MX įrašo konfigūravimas nėra būtinas) • El.pašto persiuntimas su „round robin“ • SMTP autentifikacija (el.paštas priimamas tik tada jei vartotojas yra autentifikuotas) • Antivirusinė apsauga skirta SMTP, POP3, IMAP • 2 integruotos skirtingų gamintojų virusų aprašų bazės • Gaunančiųjų domenų skaičius neribotas • Antispam apsauga SMTP,POP3, IMAP srautui • Administratorius gali konfigūruoti POP3 žinutę (pvz. rastas virusas) pagal poreikius. • Nėra licencinių apribojimų konkurenciniams el.pašto prisijungimams. • Pašto maršruto konfigūravimas: * Prieš-srautinis pašto persiuntimas su autentifikacija; * MX-paremtas maršrutizavimas; * Atskiri pašto prieigos vartai domenui; * Atskiri pašto serveriai domenui. • TLS palaikymas: * Konfigūruojamas dedikuotam pašto serveriui; * Konfigūruojamas dedikuotam domenui; * TLS sertifikatas keičiamas. * Galimybė išjungti TLS tam tikriems pašto serveriams • Reikalavimai Anti-SPAM apsaugai: * Galimi filtro veiksmai “Ištrinti”, “Įspėti”, “Ignoruoti” ir “Karantinuoti”; * Galimybė keisti pridedamą žymę “SPAM” el.pašto pavadinimo laukelyje; * Anti-Spam siuntėjų globalus baltas sąrašas; * Anti-Spam siuntėjo baltas sąrašas kiekvienam el.pašto gavėjui (nustatomas pačio vartotojo); * Anti-Spam siuntėjo juodas sąrašas kiekvienam el.pašto gavėjui (nustatomas pačio vartotojo); * Juodi/Balti sąrašai keičiami administratoriaus. • El.pašto filtravimas atliekamas remiantis:

		* Reputacijos duomenų bazės rezultatais realiu laiku; * RBL (Realtime Blackhole Lists); * Atvirkštinio DNS tikrinimas; * Gavėjo adreso tikrinimas pagal Active Directory bei per SMTP į pašto serverį; * SPF (Sender Policy Framework) tikrinimas; * BATV (Bounce Address Tag Verification); * Įtraukimo į pilką sąrašą galimybė (Greylisting); * Failų plėtinių filtravimas; * Teksto analizė (raktažodžiai/ekspresijos); * MIME dokumento tipo tikrinimas prisegtam dokumentui; * Neskanuojamų dokumentų blokavimas (pav. Apsaugotų slaptažodžiu pdf); * Pagal maksimalų el.pašto dydį. • Reikalavimai duomenų nutekėjimo prevencijai el.pašto sraute: * Pagal nustatytą taisyklių sąrašą (kreditinių kortelių numeriai ar pan.) * Turi būti suderinama su reguliariomis išraiškomis (angl. Regular expressions) arba pagal nustatomą žodyną; * Turi būti galimybė nustatyti el.pašto užšifravimo iššaukimą, jei atitinka aprašyto jautraus turinio taisyklę. • Spam valdymas: * Spam el.laiškų atmetimas iš karto (atmetimas prieš priimant); * Galimybė siųsti asmeninę kasdieninę ataskaitą apie blokuotą el.paštą kiekvienam vartotojui atskirai; * Viena kasdieninė ataskaita vartotojui, netgi jei vartotojas turi daugiau nei vieną el.pašto adresą sistemoje (konsoliduota ataskaita apie nepageidaujamus el.laiškus); * Galimybė ataskaitos tekstą nustatyti pagal vartotojo poreikius; * Palaikomi vidiniai el.pašto sąrašai; * Vartotojas turi galėti išlaisvinti el.paštą iš karantino pats; * Vartotojas turi turėti galimybę pats valdyti baltus sąrašus; * Vartotojas turi turėti galimybę pats valdyti juodus sąrašus. • Integruoto el.pašto šifravimo ir dešifravimo funkcijos reikalavimai: * Galimybė Importuoti	* Reputacijos duomenų bazės rezultatais realiu laiku; * RBL (Realtime Blackhole Lists); * Atvirkštinio DNS tikrinimas; * Gavėjo adreso tikrinimas pagal Active Directory bei per SMTP į pašto serverį; * SPF (Sender Policy Framework) tikrinimas; * BATV (Bounce Address Tag Verification); * Įtraukimo į pilką sąrašą galimybė (Greylisting); * Failų plėtinių filtravimas; * Teksto analizė (raktažodžiai/ekspresijos); * MIME dokumento tipo tikrinimas prisegtam dokumentui; * Neskanuojamų dokumentų blokavimas (pav. Apsaugotų slaptažodžiu pdf); * Pagal maksimalų el.pašto dydį. • Reikalavimai duomenų nutekėjimo prevencijai el.pašto sraute: * Pagal nustatytą taisyklių sąrašą (kreditinių kortelių numeriai ar pan.) * Suderinama su reguliariomis išraiškomis (angl. Regular expressions) arba pagal nustatomą žodyną; * Galimybė nustatyti el.pašto užšifravimo iššaukimą, jei atitinka aprašyto jautraus turinio taisyklę. • Spam valdymas: * Spam el.laiškų atmetimas iš karto (atmetimas prieš priimant); * Galimybė siųsti asmeninę kasdieninę ataskaitą apie blokuotą el.paštą kiekvienam vartotojui atskirai; * Viena kasdieninė ataskaita vartotojui, netgi jei vartotojas turi daugiau nei vieną el.pašto adresą sistemoje (konsoliduota ataskaita apie nepageidaujamus el.laiškus); * Galimybė ataskaitos tekstą nustatyti pagal vartotojo poreikius; * Palaikomi vidiniai el.pašto sąrašai; * Vartotojas gali išlaisvinti el.paštą iš karantino pats; * Vartotojas turi galimybę pats valdyti baltus sąrašus; * Vartotojas turi galimybę pats valdyti juodus sąrašus. • Integruoto el.pašto šifravimo ir dešifravimo funkcijos reikalavimai: * Galimybė Importuoti

		raktus/sertifikatus; * Auto importavimo funkcionalumas sertifikatų iš "patikimų išorinių CA; * Kiekvienam vartotojui formuojama šifravimo/dešifravimo/pasirašymo politika; * PDF rinkmenos tipu paremtas el.pašto šifravimas, šifravimą turi būti galima atlikti per Outlook priedėlį; * PDF rinkmena paremtas šifravimas gali būti vykdomas automatiškai susiejus su duomenų nutekėjimo prevencijos funkcionalumu el.pašte.	raktus/sertifikatus; * Auto importavimo funkcionalumas sertifikatų iš "patikimų išorinių CA; * Kiekvienam vartotojui formuojama šifravimo/dešifravimo/pasirašymo politika; * PDF rinkmenos tipu paremtas el.pašto šifravimas, šifravimą galima atlikti per Outlook priedėlį; * PDF rinkmena paremtas šifravimas vykdomas automatiškai susiejus su duomenų nutekėjimo prevencijos funkcionalumu el.pašte.
		Reikalavimai web aplikacijų saugumo funkcionalumui: • Atvirkštinės tarpinės tarnybinės stoties funkcionalumas (aplikacijų lygio prieigos vartai) • Turi būti atliekama gilių nuorodų pateikimo kontrolė • Direktorijos sankirtos prevencija • Apsauga nuo SQL injekcijų • Formų stiprinimo apsauga • Apsauga nuo tarptinklinių scenarijų atakų (XSS) • Dviguba antivirusinė apsauga • Reputacija paremtas blokavimas (TOR tinklai, anonymazeriai...) • Sausainukų (Cookie) pasirašymas su skaitmeniniu parašu • Automatinis tarnybinės stoties skanavimas web tarnybinės stoties identifikavimui • Apkrovos balansavimas lankytojų išskirstymui per kelias tarnybines stotis • Turi būti realizuotas HTTPS palaikymas: * HTTP iš naršyklės->HTTPS į galutinę sistemą (backend); * HTTPS iš naršyklės->HTTPS į galutinę sistemą (backend); * HTTPS iš naršyklės->HTTP į galutinę sistemą (HTTPS offlaoding);	**Reikalavimai web aplikacijų saugumo funkcionalumui:** • Atvirkštinės tarpinės tarnybinės stoties funkcionalumas (aplikacijų lygio prieigos vartai) • Atliekama gilių nuorodų pateikimo kontrolė • Direktorijos sankirtos prevencija • Apsauga nuo SQL injekcijų • Formų stiprinimo apsauga • Apsauga nuo tarptinklinių scenarijų atakų (XSS) • Dviguba antivirusinė apsauga • Reputacija paremtas blokavimas (TOR tinklai, anonymazeriai...) • Sausainukų (Cookie) pasirašymas su skaitmeniniu parašu • Automatinis tarnybinės stoties skanavimas web tarnybinės stoties identifikavimui • Apkrovos balansavimas lankytojų išskirstymui per kelias tarnybines stotis • Realizuotas HTTPS palaikymas: * HTTP iš naršyklės->HTTPS į galutinę sistemą (backend); * HTTPS iš naršyklės->HTTPS į galutinę sistemą (backend); * HTTPS iš naršyklės->HTTP į galutinę sistemą (HTTPS offlaoding); * SAN (Subject Alt. Name) sertifikatų

		* SAN (Subject Alt. Name) sertifikatų palaikymas; * Tarpinių CA sertifikatų palaikymas; * Galimybė pačių pasirašytų sertifikatų generavimas įrenginyje. • Autentifikacijos perkėlimas (angl. Offloading): * Autentifikacija per bazinę autentifikaciją proksyje; * Prisijungimo rekvizitų perdavimas į galinį (angl. Backend) serverį (per bazinę autorizaciją); * OTP palaikymas; * Autentifikacija turi būti konfigūruojama tarnybinei stočiai/URL. • Turi būti integruotas URL stiprinimo variklis: * Informacija gali būti nuskaitoma iš sitemap.xml; * Automatiškai/periodiškai.	palaikymas; * Tarpinių CA sertifikatų palaikymas; * Galimybė pačių pasirašytų sertifikatų generavimas įrenginyje. • Autentifikacijos perkėlimas (angl. Offloading): * Autentifikacija per bazinę autentifikaciją proksyje; * Prisijungimo rekvizitų perdavimas į galinį (angl. Backend) serverį (per bazinę autorizaciją); * OTP palaikymas; * Autentifikacija konfigūruojama tarnybinei stočiai/URL. • Integruotas URL stiprinimo variklis: * Informacija nuskaitoma iš sitemap.xml; * Automatiškai/periodiškai.