REKOMENDACIJOS ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS TECHNINEI SPECIFIKACIJAI

Eil. Nr.	Parametras	Minimali reikšmė
1.	Licencijų skaičius	250 vnt.
2.	Programinės įrangos tipas	Kompiuterinių darbo vietų, serverių, mobiliųjų ir planšetinių įrenginių apsauga nuo virusų ir šnipinėjimo programų, su ugniasiene ir pašto apsauga. Centralizuotas darbo vietų kietųjų diskų šifravimas. Papildoma apsauga nuo išpirkos reikalaujančių kenkėjų ir nulinės dienos atakų su debesyje valdoma smėliadėžės technologija. Kompiuterinių darbo vietų ir serverių ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo programinė įranga su centralizuotu valdymu (angl. *Extended Detection and Response, XDR*). Visi programinės įrangos sprendimai privalo būti valdomi iš vieno gamintojo administravimo konsolės(-ių) debesijoje.
3.	Programinės įrangos gamintojas	Turi būti nurodytas. Siekiant visapusiško suderinamumo vykdant centralizuotą stebėseną ir valdant visas išplėstines antivirusinės infrastruktūros apsaugos sistemas, visi pateikti apsaugos nuo virusų, apsaugos nuo el. šiukšlių, kietųjų diskų šifravimo produktai, smėliadėžė debesyje ir įrenginių ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo programinė įranga turi būti pagaminta to paties gamintojo.
4.	Programinės įrangos paketo pavadinimas	Turi būti nurodytas.
5.	Palaikomos operacinės sistemos	Kompiuterinės darbo vietos: *Microsoft Windows 11 32-bitų ir 64-bitų.* *Microsoft Windows 10 32-bitų ir 64-bitų.* *Microsoft Windows 8.1 32-bitų ir 64-bitų.* *Microsoft Windows 8 32-bitų ir 64-bitų.* *Microsoft Windows 7 32-bitų ir 64-bitų.* Mobilieji įrenginiai: *Android 6 ir naujesnės.*

		iOS 9 ir naujesnės. *iPadOS 13 ir naujesnės.* Windows serveriai: *Microsoft Windows Server 2025 (Server Core ir Desktop Experience).* *Microsoft Windows Server 2022 (Server Core ir Desktop Experience).* *Microsoft Windows Server 2019 (įskaitant Server Core, Desktop Experience ir Essentials).* *Microsoft Windows Server 2016 (įskaitant Server Core, Desktop Experience, Storage Server ir Essentials).* *Microsoft Windows Server 2012 R2 (įskaitant Storage Server ir Essentials).* *Microsoft Windows Server 2012 (įskaitant Storage Server, Essentials, Foundation ir MultiPoint).* Turi būti palaikomos virtualios aplinkos: *Microsoft Hyper-V Server 2012 ir naujesnė.* *VMware vSphere/ESXi 6.5 ir naujesnė.* *VMware Workstation 9 ir naujesnė.* *VMware Player 7 ir naujesnė.* *Oracle VirtualBox 6.0 ir naujesnė.* Sprendimas su VMware ESXi turi palaikyti VMware Horizon 7.x ir 8.0 versijas. Nuotolinio administravimo konsolė saugumo sprendimams turi palaikyti (diegiant organizacijos viduje): *Microsoft Windows Server 2012 64-bitų.* *Microsoft Windows Server 2012 Core 64-bitų.* *Microsoft Windows Server 2012 R2 64-bitų.* *Microsoft Windows Server 2012 R2 Core 64-bitų.* *Microsoft Windows Storage Server 2012 R2 64-bitų.* *Microsoft Windows Server 2016 64-bitų.* *Microsoft Windows Storage Server 2016 64-bitų.* *Microsoft Windows Server 2019 64-bitų.*

		Microsoft Windows Server 2022 64-bitų. *Microsoft Windows Server 2025 64-bitų.* Nuotolinė saugumo sprendimų administravimo konsolė turi būti suderinama su naršyklėmis: • *Mozilla Firefox* • *Microsoft Edge* • *Google Chrome* • *Opera*
6.	Palaikomos operacinės sistemos ir duomenų bazės ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo programinei įrangai	Kompiuterinės darbo vietos: *Microsoft Windows 8.1 32-bitų ir 64-bitų.* *Microsoft Windows 10 32-bitų ir 64-bitų.* *Microsoft Windows 11 32-bitų ir 64-bitų.* Serveriai: *Microsoft Windows Server 2012 64-bitų.* *Microsoft Windows Server 2012 R2 64-bitų.* *Microsoft Windows Server 2016 64-bitų.* *Microsoft Windows Server 2019 64-bitų.* *Microsoft Windows Server 2022 64-bitų.* *Microsoft Windows Server 2025 64-bitų.* Nuotolinio administravimo konsolė (diegiant organizacijos viduje) turi palaikyti diegimą į: *Microsoft Windows Server 2012 64-bitų.* *Microsoft Windows Server 2012 R2 64-bitų.* *Microsoft Windows Server 2016 64-bitų.* *Microsoft Windows Server 2019 64-bitų.* *Microsoft Windows Server 2022 64-bitų.* *Microsoft Windows Server 2025 64-bitų.* Nuotolinio administravimo konsolė turi būti suderinama su duomenų bazėmis: *MySQL 5.7.40 ir naujesnėmis.*

		MySQL 8.0.31 ir naujesnėmis. *Microsoft SQL Server 2017 ir naujesnėmis.* Web administravimo konsolė turi būti suderinama su naršyklėmis: *Mozilla Firefox.* *Google Chrome.* *Microsoft Edge.*
7.	Veikimo kokybės reikalavimai	Programinės įrangos gamintojas turi turėti ISO 27001:2013 standartus atitinkančias sertifikacijas arba lygiavertį. Programinės įrangos gamintojas turi turėti SOC 2 Type 2 standartus atitinkančias sertifikaciją arba lygiavertę. Gamintojo programinė įranga turi būti įvertinta/sertifikuota „Endpoint Prevention & Response (EPR) Test 2025 - AV Comparatives“ tyrime arba lygiaverčiame. Kibernetinių grėsmių aptikimo analizė turi būti pagrįsta pagal MITRE ATT&CK® metodologiją arba lygiavertę. Gamintojo programinė įranga turi būti įvertinta/sertifikuota „EDR Detection Validation Certification - AV-Comparatives“ 2025m. tyrime arba lygiaverčiame.
8.	Administravimo konsolės(-ių) aktyvavimas ir diegimas	Turi būti galimybė administravimo konsolę(-es) debesyje aktyvuoti gamintojo dedikuotoje paskyroje. Turi būti galimybė administravimo konsolę apsaugoti dviejų veiksnių autentifikacijos (angl. *Two Factor Authentication*) apsaugos sluoksniu.
9.	Diegimo metodai	Kompiuterinėms darbo vietoms turi būti galimybės: - Įdiegti programinę įrangą centralizuotai iš valdymo konsolės. - Įdiegti programinę įrangą lokaliai iš diegimo laikmenos. - Įdiegti programinę įrangą per *Active Directory Group Policy* nustatymus.

10.	Būtini kompiuterinių darbo vietų apsaugos funkciniai moduliai	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų, grėsmių. Įsilaužimų prevencijos modulis (HIPS). Išorinių laikmenų apsaugos modulis. Galimybė atstatyti užkrėstą kompiuterį į ankstesnę būseną. Įsilaužimų blokatorius. Skydas nuo išpirkos reikalaujančių kenkėjų. Ugniasienė. Kietųjų diskų šifravimo modulis. Saugios naršyklės modulis. Sprendimas turi leisti pasirinkti, kuriuos apsaugos modulius aktyvuoti.
11.	Funkciniai reikalavimai kompiuterinių darbo vietų antiviruso moduliui	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų; Sprendime turi turėti tokias nuskaitymo parinktis: - Išmanusis nuskaitymas. - Kontekstinio meniu nuskaitymas. - Giluminis nuskaitymas. - Prie kompiuterio prijungtų išorinių laikmenų nuskaitymas (pvz. CD/DVD/USB). Galimybė vykdyti euristinį (angl. *heuristic*) nežinomų failų skenavimą. Galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo. Ugniasienės modulis – programinė įranga, sauganti nuo įsilaužimų. Apsaugos nuo elektroninių šiukšlių modulis (*Anti-SPAM*). Apsaugos nuo botnet tinklų modulis. Turi būti galimybė valdyti šiuos įrenginius: disko atminties įrenginius, CD/DVD, USB spausdintuvus, Bluetooth įrenginius, lustinių kortelių skaitytuvus, skenavimo, įrenginius, modemus, LPT/COM prievadus, nešiojamuosius įrenginius. Įsilaužimų prevencijos modulis (HIPS). Turi būti integruota saugi naršyklė. Turi būti WMI ir viso registro nuskaitymas. Turi būti galimybė grafinę vartotojo sąsają pasirinkti lietuvių kalba. Kompiuterinių darbo vietų antivirusinės programos dokumentacija turi

		būti pateikta lietuvių kalba. Turi leisti įjungti ir naudoti „Intel® Threat Detection Technology“, kad būtų galima aptikti išpirkos reikalaujančių kenkėjų atakas naudojant procesoriaus telemetriją, užtikrinti didesnį aptikimo efektyvumą, sumažinti klaidingai teigiamų įspėjimų skaičių ir padidinti matomumą sudėtingų vengimo metodų nustatymui. Turi galėti veikti su palaikomais „Intel®“ procesoriais. Sprendimas turi turėti funkciją, leidžiančią aptikti išpirkos reikalaujančių programų veiklą ir automatiškai atkurti jų pažeistus failus į pirminę būseną sukuriant momentines atsargines failų kopijas ir galiausiai atkurti užšifruotus failus po aptikimo. Funkcija turi veikti be vartotojo įsikišimo, būti valdoma centralizuotai per administravimo konsolę ir veikti darbo vietoje nepriklausomai nuo interneto ryšio.
12.	Funkciniai reikalavimai darbo vietų ugniasienei	Turi apsaugoti nuo nepageidaujamų tinklo išorinių atakų pagal nustatytus kriterijus (pagal prievadus (*port*), programas) ribojant atakos šaltinio prieigą. Turi būti apsauga nuo *brute-force* atakų. Darbo vietų ugniasienės valdymas turi būti atliekamas centralizuotai administravimo konsolės pagalba.
13.	Funkciniai reikalavimai mobiliųjų telefonų ir planšetinių kompiuterių antiviruso moduliui	Turi užtikrinti apsaugą nuo virusų ir kitų kenkėjiškų programų. Turi turėti galimybę skenuoti tiek vidinę, tiek išorinę (*micro SD* kortelių) įrenginio atmintį. Skenuoti tam tikrus nustatytus aplankus. Praradus įrenginį, turi būti galimybė nuotoliniu būdu gauti įrenginio buvimo koordinates, užrakinti ir apsaugoti nuo galimybės nesankcionuotai naudotis įrenginiu, saugiai ištrinti kontaktus, žinutes ir duomenis išorinėje laikmenoje (*micro SD*). Turi būti galimybė apsaugoti įrenginį sukčiavimo atveju. Turi būti galimybė nuotoliniu būdu įrenginyje paleisti sireną. Turi turėti apsaugos modulį nuo brukalų, leidžiantį apsaugoti įrenginį nuo nepageidaujamų skambučių ar SMS/MMS žinučių. Turi būti galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo.
14.	Funkciniai reikalavimai smėliadėžės debesyje	Galiniuose įrenginiuose turi būti aktyvuojama nuotoliniu būdu naudojant administravimo konsolę.

	paslaugai	Turi būti galimybė įtartinus failus į smėliadėžę debesyje teikti tiek rankiniu, tiek automatiniu būdu. Visi į smėliadėžę išsiųsti failai turi būti fiksuojami administravimo konsolėje. Turi būti galimybė gauti ataskaitas apie išsiųstus įtartinus failus. Turi būti galimybė nustatyti terminą, kiek dienų gali būti saugomi įtartini failai smėliadėžėje. Turi būti galimybė drausti/leisti dokumentų siuntimą į smėliadėžę.
15.	Funkciniai reikalavimai mobiliųjų įrenginių valdymo moduliui	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Valdymas turi būti įgyvendintas saugumo sprendimų administravimo konsolėje kuriant politikas, kurias galima priskirti įrenginiams ar įrenginių grupėms. Turi būti įgyvendinta galimybė užblokuoti mobiliąsias programėles arba jų kategorijas. Galimybė riboti programų naujinimąsi. Turi turėti galimybę uždrausti atstatyti įrenginio gamyklinius parametrus. Turi turėti galimybę uždrausti keisti įrenginio sisteminius parametrus. Turi turėti galimybę uždrausti pašalinti tam tikras mobiliąsias programėles. Turi turėti galimybę stebėti WI-FI, GPS, *Roaming* būklę. Turi turėti galimybę masiškai visiems telefonams siusti informacinį pranešimą tiesiai į ekraną. Turi turėti galimybę atvaizduoti įrenginyje sudiegtas mobiliąsias programėles ir jų versijas bei jas valdyti. Turi turėti galimybę užrakinti/atrakinti mobiluįį įrenginį per nuotolį be vartotojo pagalbos. Turi būti galimybė aktyvuoti patikimos SIM kortelės autentifikaciją. Turi būti galimybė įgalinti įrenginio šifravimą.
16.	Funkciniai reikalavimai darbo vietų šifravimo moduliui	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Valdymas turi būti įgyvendintas kuriant politikas, kurias galima priskirti įrenginiams ar įrenginių grupėms.

		Turi būti suderinamumas su *Microsoft Windows 8 / 8.1 / 10 / 11* operacinėmis sistemomis. Turi būti UEFI mikroprogramos (angl. *firmware*) palaikymas. Turi būti TPM (angl. *Trusted Platform Module*) palaikymas Turi būti OPAL diskų palaikymas. Turi turėti galimybę šifruoti visus diskus arba tik krovimosi diską. Turi turėti galimybę centralizuotai nustatyti šifravimo slaptažodžio politiką. Turi būti galimybė centralizuotai politikoje laikinai atjungti šifravimo slaptažodžio reikalavimą. Turi turėti galimybę administratoriui nuotoliniu būdu inicijuoti šifravimo slaptažodžio atkūrimą, blokavimą ir ištrynimą. Turi būti galimybė administratoriui iššifruoti kietąjį diską su gamintojo numatyta atkūrimo programa.
17.	Funkciniai reikalavimai saugumo sprendimų valdymo konsolei	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi bendrauti su galiniais įrenginiais per agentą, kuris gali saugoti politiką ir vykdyti užduotis, kol įrenginys yra neprisijungęs. Serveris turi leisti pridėti įrenginius prie valdymo konsolės naudojant šiuos metodus: - sinchronizavimas su *Active Directory*; - rankiniu būdu įvedus įrenginio vardą arba IP adresą; - patentuota technologija, gebanti aptikti įrenginius tinkle; Serveris turi leisti įdiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo. Serveris turi leisti kurti statines ir dinamines grupes paprastesniam įrenginių administravimui. Serveris turi leisti nuotoliniu būdu vizualizuoti šią įrenginių informaciją: - pagrindinė informacija; - konfigūracija; - atliktos užduotys; - įdiegtos programos; - perspėjimai; - karantinas. Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams.

		Turi būti galimybė nustatyti automatinę produkto ir agento versijos atnaujinimo funkciją. Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo. Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies konfigūracinius nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį. Serveris turi turėti mobiliųjų įrenginių valdymo modulį, kuris leidžia prijungti ir valdyti mobiliuosius įrenginius. Turi turėti galimybę paveldėti taisykles (angl. *policies*) iš aukštesnio lygio nuotolinio administravimo serverio. Turi būti užtikrinta galimybė siųsti informacinius pranešimus į visų rūšių įrenginius, įskaitant stalinius kompiuterius, mobiliuosius įrenginius ar planšetinius kompiuterius. Serveris turi leisti apibrėžti aktyviklį (angl. *trigger*), kuris įvykdytų numatytą veiksmą, kai tam tikras įvykis įvyksta tinkle. Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus. Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų. Turi būti realizuota galimybė keisti grafines naudotojo informacijos juostas realiuoju laiku. Turi būti galimybė prieigos profilius konfigūruoti naudojant skirtingus leidimus skirtingoms užduotims, pvz .: administratorius, ataskaitų kūrėjas, operatorius ir kita. Po 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Po 15 nesėkmingų bandymų vedant netinkamą seanso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Turi būti galimybė nustatyti automatinę agento atnaujinimo funkciją.

18.	Funkciniai reikalavimai ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo valdymo konsolei	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi komunikuoti su galiniais įrenginiais per agentą, kuris gali saugoti politiką ir kaupti žurnalinius įrašus, kol įrenginys yra neprisijungęs. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Turi būti stebėsenos skydelis, kuriame galima stebėti naujausią informaciją apie įmonės tinkle įvykusius įtartinus įvykius. Turi būti interaktyviai atvaizduojami įspėjimai, teikiami pagal taisykles apie įtartinus įvykius, kurie įvyko veikiant programinei įrangai. Turi būti numatytųjų taisyklių sąrašas ir galimybė parengti savo taisykles, kuriomis būtų apibūdinamas įtartinas programinės įrangos veikimas. Turi būti automatiškai vykdomas įspėjimų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į kritinius įvykius. Turi būti galimybė nustatyti prioritetinius įspėjimus, kad būtų lanksčiau rūšiuojami ir filtruojami įvykiai. Turi būti galimybė grupuoti įspėjimus pagal skirtingus kriterijus, pvz., tipą, kompiuterį, taisyklę, procesą, rinkmeną. Turi būti galimybė užfiksuoti su informacijos saugumu susijusius incidentus sudarant įtartinus aptikimus, kuriuose būtų pateikta informacijos apie įvykį santrauka (data, laikas ir kur įvykis įvyko (kompiuteris), kuris vartotojas paleido vykdomąjį failą ir koks konkretus procesas sukėlė paleidimą) ir išsami informacija apie kiekvieną iš išvardytų parametrų. Kiekviename įtartiname aptikime turi būti numatytas specialus informacijos skyrius, kuriame pateiktas išsamus taisyklę suaktyvinusio įvykio aprašymas, galimų priežasčių, pavojų ir pasekmių sąrašas bei rekomendacijos dėl būtinų veiksmų tolesnei įvykio analizei vykdyti. Aptikus kritinius incidentus, turi būti galimybė gauti informaciją apie žinomų būdų ir priemonių, kurias anksčiau naudojo įsilaužėliai panašiose situacijose, sąrašą su nuorodomis į atitinkamas MITRE ATT&CK® šaltinio nuorodas, kur galima rasti išsamesnės informacijos apie įsilaužimų taktikas. Turi būti įtartinų aptikimų interaktyvioji sąsaja, leidžianti išsamiau išnagrinėti su informacijos saugumu susijusį incidentą naudojant

		pagrindinius parametrus, kurie yra prieinami bendrajame įtartiname aptikime. Turi būti pateikiama išsami informacija apie taisyklę suaktyvinusį procesą, pvz., procesų medis, failų sistemos ir operacinės sistemos registro pakeitimai, tinklo veikla, ryšiai su URL adresais, papildomai atsisiųsti vykdomieji failai ir išsamus operacinės sistemos įvykių žurnalas. Turi būti galimybė sukurti išsamias atskirų įvykių išimtis, kurios turėtų apimti informaciją apie vykdomųjų failų kontrolines sumas (angl. *hash checksum*), jų buvimo vietą, skaitmeninį parašą (angl *signature*) ir kt. Turi būti galimybė įtraukti pasirinktus EXE / DLL failus į užblokuotųjų sąrašą remiantis kontroline suma, tokiu būdu inicijuojant blokavimą darbo vietose ir serveriuose. Turi būti galimybė nuotoliniu būdu ištrinti visus įtartinus EXE / DLL failus ir perkelti juos į karantiną. Turi būti galimybė atsisiųsti įtartinus failus iš darbo vietų ir serverių tolesnės analizės vykdymui. Turi būti galimybė parengti visų EXE / DLL failų, esančių darbo vietose ir serveriuose, sąrašą tolesnės analizės vykdymui. Turi būti galimybė parengti baltuosius (angl. *whitelist*) / juoduosius (angl. *blacklist*) EXE / DLL failų sąrašus. Turi būti galimybė peržiūrėti išsamią informaciją apie EXE / DLL failus, su jais susijusius įspėjimus, naudojimo statistiką, failų pakeitimus, registrą, sukurtus tinklo ryšius. Turi būti galimybė esant poreikiui atkurti, ištrinti ir atsisiųsti užblokuotų EXE / DLL failų sąrašą išsamesnės analizės vykdymui. Turi būti automatiškai vykdomas EXE / DLL failų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į įtartiną failų elgesį. Turi būti galimybė žymėti EXE / DLL failus kaip patikimus ar saugius ir kaip patikrintus bei išanalizuotus.

		Turi būti galimybė tiesiogiai iš konsolės vykdyti papildomos informacijos apie failus sparčiąją paiešką trečiųjų šalių ištekliuose, tokiuose kaip „Virus Total“ arba lygiaverčiuose. Turi būti galimybė parengti visų skriptų, kurie buvo vykdomi darbo vietose ir serveriuose, sąrašą. Turi būti galimybė grupuoti skriptus pagal skirtingus kriterijus, tokius kaip pirminis procesas, pirmasis antrinis procesas, komandinė eilutė. Turi būti galimybė žymėti patikrintus skriptus kaip patikimus ar saugius. Turi būti galimybė gauti su skripto turiniu susijusią informaciją apie pasitelktus EXE / DLL failus, procesus, sugeneruotus antrinių procesų sąrašus, failų pakeitimus, registrus, užmegztus tinklo ryšius. Turi būti automatiškai vykdomas skriptų paskirstymas pagal kritiškumo lygį, leidžiant greitai nustatyti ir reaguoti į įtartiną elgesį. Turi būti galimybė atvaizduoti kompiuterių sąrašą ir išsamią informaciją apie veiksmus, EXE / DLL failus ir skriptus. Turi būti galimybė nuotoliniu būdu atlikti darbo vietos perkrovimą arba visiškai ją išjungti. Turi būti galimybė iš nuotolinės valdymo konsolės darbo vietai paleisti antivirusinės programos greitąjį skenavimą. Turi būti galimybė iš nuotolinės valdymo konsolės atlikti darbo vietos operacinės sistemos būsenos momentinę nuotrauką, kurioje būtų užfiksuota informacija apie visus tuo metu vykstančius procesus ir tinklo ryšius, bei pateikiama informacija apie kritinį operacinės sistemos registro turinį, operacinės sistemos planavimo priemonės užduotis, operacinės sistemos vartotojus ir jų privilegijas, operacinės sistemos kritinių failų, pvz., „hosts“, „win.ini“ ir kt., turinį, bei visa išsami informacija apie operacinę sistemą ir įdiegtą programinę įrangą. Turi būti galimybė kurti ir išsaugoti paieškos užduotis visoje duomenų bazėje, kurioje renkami duomenys iš visų valdomų kompiuterių, įskaitant bet kokius parametrus (net kelis simbolius iš vykdomosios

		komandinės eilutės) ir naudojant įvairius filtrus.
19.	Kiti reikalavimai	Sprendimas turi turėti mechanizmą, kuris leidžia pašalinti bet kurį kitą saugumo sprendimą, esantį galiniame įrenginyje. Šis mechanizmas turi būti: - Integruotas į saugumo sprendimą. - Pateiktas kaip atskiras įrankis. - Pasiekiamas per saugumo sprendimų centralizuotą administravimo konsolę.
20.	Atnaujinimai	Klientinės dalies programinė įranga privalo turėti funkcionalumą parsisiųsti atnaujinimus tiesiai iš: - Gamintojo atnaujinimų serverio. - Centralizuoto valdymo serverio. - Kitų klientų. Klientinės dalies programinė įranga privalo turėti funkcionalumą veikti kaip atnaujinimų serveris kitiems klientams tam, kad būtų galima taupyti tinklo pralaidumo resursus. Turi būti galimybė nustatyti automatinę saugumo produkto atnaujinimo funkciją.
21.	Aktualumo reikalavimas	Pateikiamoms licencijoms turi būti užtikrinamas gamintojo palaikymas sutarties galiojimo laikotarpiu, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (angl. *signature*), virusų paieškos mechanizmo (angl. *engine*) atnaujinimus bei atsisiųsti ir diegtis naujausias programinės įrangos versijas.
22.	Versija	Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete.
23.	Dokumentacija	Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras.
24.	Gamintojo aptarnavimo (angl. support) sąlygos	Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių, rusų ir anglų kalbomis. Gamintojo atstovas turi suteikti ne mažiau 2 valandas konsultacijų produkto diegimo ir atnaujinimo klausimais, kurios turi būti įvykdytos ne vėliau kaip 30 dienų nuo licencijų aktyvavimo dienos.

		Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių, rusų ir anglų kalbomis.
25.	Reikalavimai programinės įrangos naudojimo taisyklėms (licencijavimui)	Licencija turi suteikti teisę pakartotinai diegti siūlomą programinę įrangą neišnaudojant papildomos licencijos. Programinės įrangos licencijavimo taisyklėse licencija turi būti nepririšama prie aparatūrinės įrangos. Licencijos įsigijimo metu turi būti pateiktas vienas licencijos raktas, tinkantis visiems įrenginiams, nepriklausomai nuo licencijos įsigijimo kiekio bei įrenginio tipo.

_____