ТЕХНИКАЛЫҚ СИПАТТАМА

1271253 сатып алу бойынша
Бағалы ұсыныстарға сұраным тәсілімен

Лот № (21 У, 4582980) Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Тапсырыс беруші: "Құрық Порты" ЖШС
Ұйымдастырушы: "Құрық Порты" ЖШС

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	21 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер, Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Қосымша сипаттама	"Лицензиялық кілті 153 бірлікке арналған, 1 жыл мерзімге арналған антивирустық бағдарламалық қамтамасыз ету"
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Маңғыстау облысы, Қарақия ауданы, Құрық с.о., Құрық с., участок Сарша, строение 636
Жеткізу шарттары	-
Жеткізу мерзімі	01.2027 бастап 12.2027 дейін (қоса алғанда)
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

№ п/п	**Мазмұны**
1	**Сатып алынатын қызметтердің сипаттамасы**
	1.1 Trend Micro антивирустық бағдарламалық жасақтамасы. 1 жыл мерзімге 153 жұмыс орнына арналған лицензиялық кілті бар соңғы нүктелер мен серверлерді қорғау жүйесі.
2	**Сатып алынатын қызметтердің талап етілетін функционалдық, техникалық, сапалық, пайдалану сипаттамалары**
	2.1. Өнім беруші бағдарламалық жасақтама вендорының ресми серіктесі болуы тиіс. Қазақстан Республикасының аумағында тіркелген кәсіпкерлік қызметті жүзеге асыратын жеке тұлға немесе заңды тұлға болуы керек.

Өнім беруші жеткізілетін бағдарламалық жасақтамаға кепіл дік мерзімін және лицензияларды бір жыл бойы сүйемелдеу ді (қолдауды) қамтамасыз етуі тиіс.

2.2. Жалпы талаптар

- Шешім файлсыз шабуылдарды, криптомайнингті ж әне ботнет /вымогатель (бопсалаушы) бағдарламаларды қоса а лғанда, әртүрлі заманауи зиянды бағдарламаларды к еңейтілген автоматты түрде анықтауды және оларға ден қоюды қамтамасыз етуі тиіс.
- Шешім бұлтты ортада (SaaS) орналасуы тиіс.
- Шешім бұлтты инфраструктураның қауіпсіздігін ба сқару үшін ISO 27001 сертификатына ие болуы тиіс.
- Шешім Windows, macOS жұмыс станцияларын, сондай- ақ Windows және Linux серверлерін қорғауға арналғ ан бірыңғай консольді ұсынуы тиіс.
- Басқару жүйесі веб- консоль түрінде жүзеге асырылуы, браузерлердің ба рлық өзекті нұсқаларын қолдауы және әкімшілік мі ндеттерді орындау үшін қосымша компоненттерді т алап етпеуі тиіс.
- Шешім журналдар, қауіптерді талдау, басқарылаты н өнімдердің /құрылғылардың күйі және орналастыру тұрғысына н орталықтандырылған басқару функцияларын қамт амасыз етуі тиіс.
- Шешім басқарылатын өнімдермен / құрылғылармен бірге қолданыла алатын қауіптерд і талдауды орталықтандыры басқару функцияларын қамтамасыз етуі тиіс.
- Пайдаланушылар өздерінің іздеу критерийлерін ан ықтай алуы үшін, шешім лог журналдары бойынша егжей- тегжейлі іздеу сүзгілерін қамтамасыз етуі тиіс.
- Шешім барлық басқарылатын өнімдер / құрылғылар үшін өнім жаңартуларын, соның ішін де түзетулерді, патчтарды және прошивка жаңартул арын орталықтандырылған түрде басқаруға және ор наластыруға мүмкіндік беруі тиіс.
- Шешім басқарылатын өнімдер / құрылғылар үшін қауіптерді анықтаудың орталықт андырылған шолуын қамтамасыз етуі тиіс.
- Шешім өнімнің/құрылғының атын, IP- мекенжайын, қосылу күйін, қосымшалар нұсқалары н және т. б. қоса алғанда, барлық басқарылатын өнімдер мен құрылғылардың ағаш тәрізді немесе соған баламалы көрінісіне ие болуы тиіс.
- Шешім басқарылатын өнімдердің /құрылғылардың барлық қосылған функциялары ме н қосымша модульдері үшін лицензияларды басқар уды қамтамасыз етуі тиіс.
- Шешім басқарылатын өнімдер / құрылғылар үшін саясаттарды импорттау /экспорттау механизмін қамтамасыз етуі тиіс.

- Шешім әкімшілендіру, тергеу, сондай-ақ операциялық мақсаттар үшін рөлдік қолжетімділікті бақылауды қамтамасыз етуі тиіс.
- Шешім пайдаланушылардың әрекеттерінің тарихын қарау үшін аудит журналы функциясын қамтамасыз етуі тиіс.
- Шешім қолданыстағы және реттелетін үлгілерден жүктеп алынатын есептерді құру мүмкіндігіне ие болуы тиіс.
- Браузер арқылы қауіпсіз қолжетімділік үшін SSL негізіндегі шифрлауды қолдайды.
- Көпфакторлы аутентификацияны (MFA) қолдау мүмкіндігі.
- Жүйе машиналар бойынша деректерді синхрондау үшін LDAP-пен жұмыс істеуді қолдауы тиіс.
- Жүйе домендік пайдаланушылардың жүйеге кіруін қамтамасыз ету үшін LDAP-пен жұмыс істеуді қолдауы тиіс.
- Шешім тапсырыс берушінің SIEM-шешімімен бірігу мүмкіндігіне ие болуы тиіс.
- Басқару жүйесі қауіптер мен инциденттер туралы пошта арқылы хабардар етудің кіріктірілген құралдарына ие болуы тиіс.
- Шешім қолданбалы бағдарламалау интерфейсі (API) арқылы үшінші тарап бағдарламаларымен бірігу мүмкіндігіне ие болуы тиіс.

2.3 Соңғы нүктелерді қорғауға қойылатын талаптар

Шешім бір агент аясында келесі функцияларды қамтамасыз ете алуы тиіс: антивирустық БЖ, HIPS, деректердің жоғалуының алдын алу (DLP), қосымшаларды бақылау, құрылғыларға қолжетімділікті бақылау және EDR.

Шешім күдікті файлдарды, IP-мекенжайлар мен URL-мекенжайларды, егер ол болса, жергілікті немесе бұлтты песочница (sandbox) ортасына жібере алу мүмкіндігіне ие болуы тиіс.

Шешім агентті Windows және macOS операциялық жүйелеріне, сондай-ақ виртуалды жұмыс үстелі ортасына орнатуды қолдай алуы тиіс.

Әртүрлі қолдау көрсетілетін процедураларды қолдана отырып агентті оңай орналастыру (мысалы, веб-орнату, агенттің орнату пакеті, Windows қашықтан орнату, Microsoft System Center Configuration Manager және т.б.).

Шешім келесі Windows ОЖ қолдауы тиіс:

Windows 8.1

Windows 10

Windows 11

macOS операциялық жүйесінің келесі нұсқалары қолданылуы тиіс:

Catalina (10.15)

Big Sur (11)

Monterey (12)

Ventura (13)

Sonoma (14)

2.4 Зиянды бағдарламалардан қорғау

- Жеткізілетін БЖ резиденттік антивирустық монито ринге ие болуы тиіс.
- Белгісіз қауіптерді анықтау үшін бағдарламаларды і ске қосудан немесе құжаттарды ашудан бұрын және олардың барысында машиналық оқыту модулінің б олуы.
- Шешім белгіленген белсенділіксіз күндер саны өтке ннен кейін басқару серверінен агенттерді автоматты түрде жою мүмкіндігіне ие болуы тиіс.
- Шешім Windows тізілімдегі зиянды өзгерістерді жо юға, зиянды файлдарды жоюға /карантинге жіберуге және іске қосылған зиянды пр оцестерді тоқтатуға мүмкіндік беруі тиіс.
- Зиянды бағдарламалардың түрлеріне байланысты (т рояндар / құрттар, әзіл- қалжың бағдарламалар, мистификациялар, вирустар және т. б.) әртүрлі сканерлеу әрекеттерін орындау мүмкінді гі.
- Шешім эксплойттарды пайдаланатын шабуылдарға тән зиянды бағдарламалардың әрекетін анықтау үші н мінез- құлықты мониторингпен қамтамасыз етуі тиіс.
- Тыңшылық (spyware) және жарнамалық (adware) ба ғдарламалар компьютерге орнатылып, іске қосылға ннан кейін де оларды анықтай және жоя алуы тиіс.
- Зиянды бағдарламалардан тұрақты қорғауды қамта масыз етеді және клиенттің басқару серверіне қосы лғанына не қосылмағанына қарамастан жаңартулар ды орындай алады.
- Соңғы нүктенің Интернетке қосылғанына не қосыл мағанына қарамастан, зиянды бағдарламалардан тұ рақты қорғауды қамтамасыз етеді.
- Шешім вендордың беделдік қызметтері арқылы зия нды веб-сайттар мен URL- мекенжайларға қолжетімділікті бұғаттай алу мүмкін дігіне ие болуы тиіс.
- Шешім рұқсат етілген (ақ тізім) және бұғатталған (қ ара тізім) URL-мекенжайлар тізімін қолдауы тиіс.
- Шешім басқару және бақылау серверлеріне (C&C) қ осылу әрекеттерін бұғаттай алу мүмкіндігіне ие бол уы тиіс.
- Шешім рұқсат етілген (ақ тізім) және бұғатталған (қ ара тізім) IP-мекенжайлар тізімін қолдауы тиіс.
- Шешім компьютерді рұқсатсыз шифрлаудан және ө згертуден қорғай алу мүмкіндігіне ие болуы тиіс.
- Шешім бопсалаушы бағдарламалармен (вымогатели) әдетте байланысты процестерді бұғаттай алу мүмк індігіне ие болуы тиіс.
- Шешім бопсалаушы бағдарлама өзгерткен файлдың автоматты түрде сақтық көшірмесін жасау және қа лпына келтіру мүмкіндігіне ие болуы тиіс.

- Шешім операциялық жүйедегі, жұмыс құжаттарындағы немесе орнатылған қосымшадағы ерекше өзгерістерді бақылау мақсатында соңғы нүктелерді үнемі қадағалау үшін мінез-құлықты мониторингпен қамтамасыз етуі тиіс.
- Ұсынылатын шешім зілзалалы (зиянды) бағдарламаларды кеңейтілген түрде анықтау үшін күдікті пайдалы деректерді пайдаланушының араласуынсыз автоматты түрде песочницаға (sandbox) жіберу мүмкіндігін ұсынуы тиіс.
- Шешім мақұлданған (ақ тізімге енгізілген) файл, файл кеңейтімі және каталог үшін сканерлеуден алып тастауды қолдауы тиіс.
- Шешімде зиянды бағдарламаларды орындауға дейін және орындау (іске қосу) кезінде көп деңгейлі қорғанысты қамтамасыз ететін машиналық оқыту технологиясы болуы тиіс.
- Шешім антивирус агентімен байланысты процестер мен қызметтерді тоқтату әрекеттерін бұғаттай алу мүмкіндігіне ие болуы тиіс.
- Шешім антивирус агентімен байланысты тізілімдерді (реєстр) өзгерту, жою немесе жаңаларын қосу әрекеттерін бұғаттай алу мүмкіндігіне ие болуы тиіс.
- Шешім келесі мүмкіндіктері бар вирустық індеттердің автоматты түрде алдын алуды қолдауы тиіс:
    - кәсіпорынды басқару консолінен нақты шабуылдар үшін саясат ұсыныстарын алады және саясатты басқа басқарылатын серверлерге таратады;
    - папкаларға қолжетімділікті жабу мүмкіндігі;
    - қолжетімділікті «тек оқу үшін» режиміне реттеу мүмкіндігі;
    - белгілі бір TCP / UDP порттарын немесе порттар диапазонын бұғаттау мүмкіндігі;
    - файл аты (аттары) бойынша қолжетімділікті бұғаттау мүмкіндігі.
- Шешім басқа бағдарламаларға немесе пайдаланушыларға антивирустық агенттің файлдарын жоюға, өзгертуге немесе өшіруге тыйым салу мүмкіндігіне ие болуы тиіс.

2.5 Виртуалды патчинг (Виртуалды түзету)

- Шешім соңғы нүктелердің ОЖ-не бағытталған желілік осалдықтардан соңғы нүктелерді қорғауы тиіс.
- Шешім ОЖ жаңарту патчтарының болмауынан туындайтын жұқтыру қаупінің әсерін азайтуы тиіс.
- Шешім ресми патч қолжетімді болғанға немесе орнатылғанға дейін белгілі және белгісіз осалдықтарды виртуалды түрде түзеу үшін хост негізіндегі басып кірудің алдын алу жүйесіне (HIPS) ие болуы тиіс.
- Ұсынылатын шешім қосымша агент операцияларынсыз немесе үшінші тарап өндірушілерімен интеграциясыз виртуалды түзеу функционалдығын қамтамасыз етуі тиіс.
- HIPS жұмысының бірқатар алдын ала дайындалған ережелер бойынша жұмыс істеу мүмкіндігі;
- Ұсынылатын шешім пайдаланушының таңдауы негізінде ережені қосу немесе өшіру мүмкіндігіне ие болуы тиіс.
- Ұсынылатын шешім HIPS жұмысы үшін қауіпсіздік тұрғысынан немесе өнімділік тұрғысынан оңтайландырылған профильді таңдау мүмкіндігіне ие болуы тиіс.
- Ұсынылатын шешім осалдықтардан қорғау механизмінің үзілісте (в разрыв / inline) және мониторинг режимінде жұмыс істеу мүмкіндігіне ие болуы тиіс;
- Шешім RAT (Remote Access Trojan) және фантомдық қосылымдарды анықтап, бұғаттауы тиіс.
- Шешім ортақ SMB ресурсы жүктемесіне зиянды жүктеуді бұғаттау мүмкіндігіне ие болуы тиіс.
- Шешім қашықтағы PowerShell қабығын (shell) анықтап, бұғаттай алуы тиіс.
- Шешім Psexec және Paexec сияқты бүйірлік жылжуды (lateral movement) бұғаттай алуы тиіс, бұл ретте ақ тізімге енгізілген белгілі бір серверлер үшін бұған рұқсат беру функционалдығын қамтамасыз етуі тиіс.
- Белгілі және белгісіз осалдықтардың эксплойттарын бұғаттау мүмкіндігі болуы тиіс.

2.6 Деректердің жоғалуының алдын алу модулі (DLP)

- Ұсынылатын шешім агентпен қосымша операцияларсыз немесе үшінші тарап интеграциясынсыз DLP функционалдығын қамтамасыз ете алуы тиіс және антивирус агентіне біріктірілуі тиіс.
- Біріктірілген DLP клиенттердің деректерін қорғауды қамтамасыз етеді, ол келесі функцияларды қамтиды:
    - Жеке деректерді желіде немесе одан тыс жерлерде қорғайды.
    - Құрылғыларды басқарудың кеңейтілген мүмкіндіктері USB-накопительдер және басқа тасымалдағыштар арқылы деректердің сыртқа кетуінен қорғайды.
    - Құрылғылардың, қолданбалардың және файл түрлерінің ең кең ауқымын қамтиды.
    - Үлкен айқындық пен құқықтық қолдану арқылы талаптардың сақталуына ықпал етеді. Мысалы: GDPR, PCI / DSS, PII, GLBA, HIPAA, PDPA, ISMS және т.б.
- Ұсынылатын шешім конфиденциалды деректердің сыртқа кетуінен қорғаудың базалық функционалдығына ие болуы тиіс: Word, Excel құжаттарынан, түйінді сөздер (кілт сөздер) бойынша, тұрақты өрнектер (регулярные выражения) бойынша, мәтіндегі белгілі бір сөздердің бір-біріне жақын орналасуы бойынша.
- Ұсынылатын шешім файл кеңейтімі бойынша конфиденциалды деректердің сыртқа кетуінен қорғаудың базалық функционалдығына ие болуы тиіс.
- Конфиденциалды деректердің сыртқа кетуінен қорғау функционалдығы төмендегілерді орындай алуы тиіс: берілген фактіні журналда тіркеу; пайдаланушыға ескерту жасау; орталықтандырылған журналда конфиденциалды ақпаратты берудің өндірістік қажеттілігін тіркеуге мүмкіндік беретін енгізу өрісі бар пайдаланушыға ескерту жасау; пайдаланушыға конфиденциалды ақпаратты беру қажет болған себептердің бірін әкімшілер алдын ала анықтаған себептердің ішінен орталықтандырылған журналда тіркеуге мүмкіндік беретін дайын жауап нұсқалары бар пайдаланушыға ескерту жасау.
- Конфиденциалды деректердің сыртқа кетуінен қорғау функционалдығы жұмыс станциясына түсетін жүктемені болдырмау үшін антивируспен бірге бірыңғай агент құрамында болуы тиіс, сондай-ақ қосымша лицензияны талап етпеуі тиіс.
- Шешім реттелетін DLP үлгілеріне, деректер идентификаторларын импорттау және экспорттау мүмкіндігіне ие болуы тиіс және DLP өрнегін қоса алуы тиіс.
- Шешім тыныштық күйіндегі (at rest) және қозғалыстағы (in transit) қорғалған деректерді автоматты түрде шифрлау үшін соңғы нүктелерді шифрлау шешімімен бірігу мүмкіндігіне ие болуы тиіс.

2.7 Құрылғыларға қолжетімділікті бақылау

- Құрылғыларға қолжетімділікті басқару конфигурациясы басқару консолінен орталықтандырылған түрде орындалуы тиіс.
- Ереже бұзылған кезде шешім клиенттік компьютерде хабарлама көрсетуі тиіс.
- Шешім құрылғыларды бақылау ережесінің бұзылуын тіркеу мүмкіндігіне ие болуы тиіс.
- Шешім сенімді құрылғыларды қосу мүмкіндігіне ие болуы тиіс.
- Шешім оқу, оқу / жазу, жазу және қолжетімділікке тыйым салу құқықтарын тағайындау арқылы соңғы нүктелердегі құрылғыларға қолжетімділікті шектеу мүмкіндігіне ие болуы тиіс. Шектелуі мүмкін құрылғылар мыналарды қамтуы тиіс:
    - USB-накопительдер (автоматты іске қосуды (автозапуск) да өшіруге болады)
    - Желілік ресурстар
    - CD / DVD
    - Камералар
    - Принтерлер

2.8 Хост негізіндегі желілік экран (Брандмауэр)

- Шешім орталықтандырылған түрде басқарылатын брандмауэр саясаттарына ие болу мүмкіндігін қамтамасыз етуі тиіс.
- Шешім желілік вирустарды / құрттарды (черви) анықтап, бұғаттай алу мүмкіндігіне ие болуы тиіс.
- Шешім желілік вирус үлгілерін орталықтандырылған түрде жаңарту мүмкіндігіне ие болуы тиіс.
- Шешім онлайн / офлайн режимдегі клиент үшін әртүрлі брандмауэр саясаттарын анықтай алу мүмкіндігіне ие болуы тиіс.
- Шешім ереже бұзылған жағдайда брандмауэр журналдарын жасау мүмкіндігіне ие болуы тиіс.
- Шешім клиенттің экранында пайдаланушыларға желілік экран ережесінің бұзылуы туралы хабарлама көрсетуі тиіс.
- Шешім хабарламаның мазмұнын өзгерту мүмкіндігіне ие болуы тиіс.
- Шешім індеттердің (эпидемиялардың) алдын алуды іске қосу кезінде соңғы нүктені оқшаулау мүмкіндігіне ие болуы тиіс.

2.9 Қосымшаларды бақылау

- Шешім реттелетін бұғаттау саясаттары, ақ және қара тізімдер көмегімен зиянды БЖ іске қосылуын бұғаттау мүмкіндігіне ие болуы тиіс.
- Шешім қосымша агенттерді немесе үшінші тарап интеграциясын қолданбай қосымшаларды басқару функционалдығын қамтамасыз ете алуы тиіс.
- Шешім белгіленген күдікті қосымшаларды қолмен (әкімші немесе қауіпсіздік қызметінің қызметкері) немесе автоматты түрде (песочница есебі арқылы) бұғаттай алу мүмкіндігіне ие болуы тиіс.
- Ұсынылатын шешім SHA1 және SHA2 хэш мәндерін импорттауды қолдауы және солардың орындалуын бұғаттауға / рұқсат етуге тиіс.
- Шешім қауіптерді анықтау және тексерілген қосымшалардың өзекті дерекқор қолдауын қамтамасыз ету үшін миллиондаған қосымша оқиғаларының деректерін өзара салыстыра алуы тиіс.

2.10 Серверлерді қорғауға қойылатын талаптар

- Қолдау көрсетілетін платформалар (агент) — Windows:
  - Windows Server 2012 / Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server 2022
- Қолдау көрсетілетін платформалар (агент) — Linux:
  - Red Hat Enterprise Linux 6/7/8/9
  - CentOS 6/7/8
  - Amazon Linux / Amazon Linux 2
  - Amazon Linux 2023 (64-bit)
  - Amazon Linux 2023 (AWS ARM-based Graviton 2)
  - AlmaLinux 8/9
  - Rocky Linux 8/9
  - Oracle Linux 6/7/8/9
  - Solaris 10 Updates 4–6 / Updates 7-10 / Update 11
  - Solaris 11.0 / Solaris 11.2–11.3 / Solaris 11.4
  - SUSE Linux Enterprise Server 12/15
  - Ubuntu 16.04 / Ubuntu 18.04 / Ubuntu 20.04 / Ubuntu 22.04
  - Debian 8/9/10/11
  - Cloud Linux 5/6/7
  - AIX 6.1 TL 9 немесе одан кейінгі нұсқалары
- Жүйе Windows платформалары үшін агенттерді автоматты түрде орналастыруға арналған арнайы скриптерді генерациялауды қолдауы тиіс.
- Жүйе Linux платформалары үшін агенттерді автоматты түрде орналастыруға арналған арнайы скриптерді генерациялауды қолдауы тиіс.
- Жүйе Solaris платформалары үшін агенттерді автоматты түрде орналастыруға арналған арнайы скриптерді генерациялауды қолдауы тиіс.
- Басқару сервері бірнеше VMware vCenter-мен жұмыс істеуді қолдауы тиіс.

- Жүйе агентті қолмен сбростау (қолданыстан шығару / саясаттарды ажырату, басқару жүйесінен ажырату) мүмкіндігіне ие болуы тиіс.
- Басқару жүйесі қорғалатын жүйелерді шарттардың кең ауқымы бойынша ерікті топтарға біріктіру үшін құралдарға ие болуы тиіс.
- Жүйе кеңейтілген шарттар мен оқиғалар тізімі (машина инфрақұрылымда пайда болды, машина бір хосттан екіншісіне ауысты, машина қосылды, машинаның IP мекенжайы өзгерді) негізінде мақсатты жүйелерге сәйкес келетін қорғау ережелері жиынтығын автоматты түрде қолдану мүмкіндігіне ие болуы тиіс.
- Агент барынша жеңілдетілген ядро (функционалдық модульдерсіз) түрінде таратылуы тиіс.
- Агент қосылған қорғаныс функциялары мен саясаттар негізінде серверден функционалдық модульдерді жүктеп алу мүмкіндігіне ие болуы тиіс.
- Агент сервермен екі жақты режимде де (сервер де, агент те қосылымды бастай алады), сондай-ақ бір жақты режимде (тек сервер немесе тек агент қосылымды бастай алады) деректер алмасу мүмкіндігіне ие болуы тиіс.
- Агент графикалық бөлігін толығымен жасыра отырып (соқыр режимде) жұмыс істеу мүмкіндігіне ие болуы тиіс.
- Агент командалық жолдан басқаруды қолдауы тиіс.
- Агент тек командалық жол арқылы (парольді қоса алғанда) өшірілетін кіріктірілген өзін-өзі қорғау механизмдеріне ие болуы тиіс.
- Агентті басқару серверіне бастапқы байланыстырусыз орнату мүмкіндігі болуы тиіс (виртуалды машиналар мен орнату образдарының стандартты шаблоннарына енгізу үшін).
- Агенттің командалық жол құралдары көмегімен басқару серверіне байланысу мүмкіндіктері болуы тиіс.
- Агенттің командалық жол құралдары көмегімен апаттық түрде сбростау (қалпына келтіру) мүмкіндіктері болуы тиіс.

2.11 Зиянды кодтан қорғауға қойылатын талаптар

- Жүйе қорғалатын жүйелерге толық және жылдам антивирустық тексеруді қолмен іске қосу мүмкіндігіне ие болуы тиіс.
- Репутациялық бағалауды қолдана отырып антивирустың жұмыс істеуі («жеңіл агенттер»).
- Объектінің жаһандық таралу өлшемдері және іске қосылу саны бойынша репутациясын тексеру.
- (Оқшауланған жүйелер үшін) агенттердің өзінде сигнатуралар бойынша қауіптерді бағалаудың классикалық моделін қолдана отырып антивирустың жұмыс істеуі.
- VMware ортасында (vShield Endpoint) агентсіз технологияны қолдана отырып жұмыс істеу.
- Агентсіз режимде файлдарды тексеруді дедупликациялау үшін агентсіз құралдарды пайдалану (VMware ортасында кэштеу).

- Кэштің өмір сүру мерзімін және агентсіз тексеру үшін алып тастауларды баптау.
- Әкімшінің агенттік қорғаныс кезінде де, сондай-ақ агентсіз режимде де объектілерді карантиннен шығару мүмкіндігі.
- Windows және Linux басқаруындағы жүйелер үшін нақты уақыт режиміндегі антивирустық қорғаныс.
- Windows және Linux үшін антивирустық тексерулерді кесте бойынша іске қосу.
- Windows және Linux үшін антивирустық тексерулерді қолмен іске қосу.
- Антивирустық тексерудің уақыт шекараларын (басталу уақытын да, аяқталу уақытын да) белгілеу мүмкіндігі.
- Нақты уақыт режимінде тексеру режимдерін (жазу /оқу, тек жазу, тек оқу) белгілеу мүмкіндігі.
- Агенттерді пайдалану кезінде жадты бақылауды қамтамасыз етілуі.
- Ерекше белгілері бойынша белгісіз қауіптерді анықтауға арналған мінез-құлықтық талдау (поведенческий анализ).
- Деректерді шифрлау әрекеттерін жүйелі түрде қадағалау негізінде шифрлаушылардан (вымогатели) қорғау.
- Шифрлау әрекеттері байқалған құжаттардың сақтық көшірмелерін автоматты түрде жасау, сондай-ақ жүйе шифрлаушы іздерінен тазартылғаннан кейін оларды қалпына келтіру.
- Файлдарды іске қосудан бұрын машиналық оқыту моделі бойынша қауіптерді бағалау.
- Песочница (sandbox) бар болған жағдайда, күдікті объектілерді тексеруге беру және «песочницалар» вердикты негізінде кейіннен оларды бұғаттау үшін динамикалық талдау жүйесімен («песочницамен») біріктіру.
- Архивтердің ішіндегі файлдарды тексеру.
- Тексеруге енгізілетін папкалар мен файлдарды нақты көрсету мүмкіндігі.
- Тексеруден алып тасталатын папкаларды, файлдарды, кеңейтілімдерді, процестерді нақты көрсету мүмкіндігі.
- Ақ тізімді қосу мүмкіндігімен құрылғыларды бақылау мүмкіндігі.
- Қорғалатын жүйелердің әртүрлі топтары үшін тираждау мақсатында тексеру үшін қосылатын /алынып тасталатын объектілердің дайын тізімдерімен жұмыс істеу мүмкіндігі.
- Қолмен және жоспарланған тексерулер үшін агент тұтынатын процессор уақытының ең жоғары мәнін баптау.
- Көп ағынды (многопоточная) антивирустық тексеруді баптау.
- Агенттік қорғаныс режимінде репутациялық бағалау негізінде зиянды ресурсқа қолжетімділікті бұғаттау.
- Бұғаттаудың іске қосылу сезімталдығын реттеу үшін шекті мәндерді баптау.
- Бұғаттау кезінде шығарылатын хабарламаны баптау мүмкіндігі.

- Веб-белсенділіктерді бақылау үшін порттарды көрсету мүмкіндігі.
- URL бойынша (домен, URL) «қара» және «ақ» тізімдерді жүргізу мүмкіндігі.
- Өңдеу үшін жаһандық орталықты пайдалану да, жергілікті деңгейде орнатылған репутациялық қызметтер серверлері арқылы жұмыс істеу де.

2.12 Торап деңгейіндегі желілік экран (МСЭ / Хост брандмауэрі)

- Желілік қозғалтқыштың жұмысын таңдау мүмкіндігі — inline (тізбекті) немесе tap (сынақ міндеттері үшін)
- L2 деңгейінде жұмыс істеуді қолдау
- Тақырыптармен (заголовки) және фреймдермен жұмыс істеуді қолдау
- Агенттер базасында жұмыс істеуді қолдау
- Агентсіз режимде жұмыс істеуді қолдау (VMware)
- Алдын ала орнатылған ережелердің болуы
- Барлауды анықтауды қолдау — диапазонды көрсету мүмкіндігі бар порттарды сканерлеу
- МСЭ модулі үшін 1–1024 порттарынан ашық порттарды тексеруді іске қосу мүмкіндігі
- Барлауды анықтауды қолдау — OS Fingerprint (ОС «саусақ ізі»)
- Барлауды анықтауды қолдау — аномальді TCP белсенділіктері (null scan, SYN FIN scan, Xmax scan)
- Барлауды анықтауды қолдау — көздер (источники) бойынша ерекшеліктерді жасау мүмкіндігі
- Интерфейстерді оқшаулауды баптау мүмкіндігі
- Stateful inspection қолдауы
- МСЭ-нің кесте бойынша жұмыс істеу мүмкіндігі
- Тергеу үшін пакет деректерін жинау мүмкіндігі
- Контекстті қолдана отырып жұмыс істеу (желілік орта)
- Желілік қозғалтқыштың жұмысын таңдау мүмкіндігі — bypass (fail open / ақау кезінде ашық) немесе бұғаттау (fail close / ақау кезінде жабық)
- Желілік қозғалтқыштың жұмысын таңдау мүмкіндігі — inline немесе tap (сынақ міндеттері үшін)
- Қосылымдардың максималды санын көрсету мүмкіндігі (TCP, UDP, ICMP)
- Желілік сеанстардың әртүрлі күйлері мен аномалиялар үшін таймауттарды белгілеу мүмкіндігі (SYN_SENT, CLOSED, CLOSING, ACK STORM, ESTABLISHED және т.б.)
- SRC (көз) және DST (бағыт) үшін IP мекенжайлары бірдей қосылымдарды бұғаттау
- Null IP үшін тыйым салуды баптау мүмкіндігі
- TCP қосылымын «қарсылықсыз» (тыныш / «тихий») сбростау мүмкіндігі
- Деректері қайталанатын немесе қиылысатын пакеттер үшін қосылымды сбростауды баптау мүмкіндіктері (evasive retransmit)
- TCP Checksum тексеру мүмкіндіктері
- Пакет фрагменттері үшін минималды мәндерді баптау мүмкіндіктері (fragment offset & size)
- SSL сеанстары үшін минималды мәндерді баптау мүмкіндіктері (time & size)
- SSL трафигі үшін белгісіз протоколды сбростау мүмкіндіктері
- Туннельдерді сүзу мүмкіндіктері (IPv4, IPv6)
- Хостқа жатпайтын MAC мекенжайлары үшін bypass мүмкіндігі

2.13 Қосымшаларды бақылау

- Қосымшаларды бақылау модулінің агент көмегімен жұмыс істеу мүмкіндігі (Windows, Linux)
- «Ақ тізім» режимінде жұмыс істеу режимі («ақ» тізімге кірмейтін барлық қосымшаларды іске қосуға тыйым салу)
- Таңдамалы тыйым салу режимінде жұмыс істеу режимі
- Технологиялық «терезелерді» қолдау (жүйелер мен қосымшаларды жаңартуға байланысты объектілерді іске қосуға және орнатуға рұқсат беру) — мерзімсіз немесе шектеулі уақыт кезеңіне
- Қосымшаларды бақылау модулінің оқиғалар журналынан іске қосуға тыйым салу немесе рұқсат беру мүмкіндігі

2.14 Техникалық қолдау көрсетуге қойылатын талаптар

Техникалық қолдау көрсету:

- Қазақстан Республикасының бүкіл аумағында өндірушінің сертификатталған мамандарымен орыс, қазақ және ағылшын тілдерінде тәулік бойы, мереке және демалыс күндерсіз (24x7) электрондық пошта және Интернет арқылы, сондай-ақ телефон арқылы көрсетілуі тиіс;
- Шешім өндірушісінің веб-сайты орыс немесе ағылшын тілінде болуы тиіс.

Қол қойған	Измуратов Олжас Амандыкович
Қол қойылған күні	12.11.2026

Құжат «Самұрық-Қазына» АҚ сатып алу веб-порталымен құрылған
Документ сформирован веб-порталом закупок АО «Самрук-Қазына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1271253
способом Запрос ценовых предложений

Лот № (21 У, 4582980) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Порт Курык"
Организатор: Товарищество с ограниченной ответственностью "Порт Курык"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	21 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	" Антивирусное программное обеспечение с лицензионным ключом на 153 ед. со сроком на 1 год"
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, Мангистауская область, Каракиянский район, Курыкский с.о., с.Курык, участок Сарша, строение 636
Условия поставки	-
Срок поставки	с 01.2027 по 12.2027 (включительно)
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

№ п/п	
1	**Описание закупаемых услуг**
	1.1 Продление лицензии Антивирусного программного обеспечения Trend Micro - Система защиты конечных точек и серверов на 153 рабочих места со сроком на 1 год.
2	**Требуемые функциональные, технические, качественные, эксплуатационные характеристики закупаемых услуг**
	2.1. Поставщик должен быть официальным партнером вендора программного обеспечения. Физическое лицо, осуществляющее предпринимательскую деятельность или юридическое лицо, зарегистрированные на территории Республики Казахстан.

Поставщик должен предоставить гарантийный срок на поставляемое программное обеспечение и поддержку лицензий в течение одного года.

2.2. Общие требования

- Решение должно обеспечивать расширенное автоматическое обнаружение угроз и реагирование на различные современные вредоносные программы, включая безфайловые атаки, крипто-майнинг и программы-вымогатели.

- Решение должно разворачиваться в облаке (SaaS).

- Решение должно иметь сертификат ISO27001 для управления безопасностью облачной инфраструктуры.

- Решение должно представлять собой единую консоль для защиты рабочих станций с ОС Windows, Mac Os, серверов с ОС Windows и Linux.

- Система управления должна быть реализована в виде веб-консоли, поддерживать все актуальные версии браузеров и не требовать дополнительных компонентов для осуществления административных задач

- Решение должно обеспечивать функции централизованного управления с точки зрения журналов, анализа угроз, состояния управляемых продуктов /устройств и развертывания.

- - Решение должно обеспечивать функции централизованного управления анализом угроз, которые могут использоваться совместно с управляемыми продуктами / устройствами.
- - Решение должно обеспечивать детализированные фильтры поиска по журналам логов, чтобы пользователи могли определять свои собственные критерии поиска.
- - Решение должно иметь возможность централизованно управлять и развертывать обновления продукта, включая исправления, исправления и обновление прошивки, для всех управляемых продуктов / устройств.
- - Решение должно обеспечивать централизованный обзор обнаружения угроз для управляемых продуктов / устройств.
- - Решение должно иметь представление в виде дерева или эквивалентное представление всех управляемых продуктов / устройств, включая имя продукта / устройства, IP-адрес, состояние подключения, версии приложений и т. д.
- - Решение должно обеспечивать управление лицензиями для всех включенных функций и надстроек управляемых продуктов / устройств.
- - Решение должно обеспечивать механизм импорта /экспорта политик для управляемых продуктов / устройств.
- - Решение должно обеспечивать ролевой контроль доступа для целей администрирования, расследования, а также операций.
- - Решение должно обеспечивать функцию журнала аудита для просмотра истории действий пользователей.
- - Решение должно иметь возможность создавать загружаемые отчеты из существующих и настраиваемых шаблонов.
- - Поддерживает шифрование на основе SSL для безопасного доступа через браузер
- - Возможность поддержки многофакторной аутентификации (MFA)
- - Система должна поддерживать работу с LDAP для синхронизации данных по - машинам
- - Система должна поддерживать работу с LDAP для обеспечения доступа доменных пользователей к системе
- - Решение должно иметь возможность интеграции с SIEM-решением заказчика
- - Система управления должна иметь встроенные средства оповещения об угрозах и инцидентах через почту
- - Решение должно иметь возможность интеграции со сторонними программами через интерфейс прикладного программирования (API)

2.3. Требования к защите конечных точек.

- - Решение должно иметь возможность предоставить в одном агенте следующие функции: антивирусное ПО, HIPS, предотвращение потери данных (DLP), контроль приложений, контроль доступа к устройствам и EDR.
- - Решение должно иметь возможность отправлять подозрительные файлы, IP-адреса и URL-адреса в локальную или облачную среду песочницы при ее наличии
- - Решение должно иметь возможность поддерживать установку агента в ОС Windows и MAC, а также в среде виртуального рабочего стола.
- - Простое развертывание агента с использованием различных поддерживаемых процедур (например, веб-установка, пакет установщика агента, удаленная установка Windows, Microsoft System Center Configuration Manager и т. д.)
- - Решение должно поддерживать следующие ОС Windows:
- Windows 8.1
- Windows 10
- Windows 11
- - Должны поддерживаться следующие варианты MAC OS:
- Catalina (10.15)
- Big Sur (11)
- Monterey (12)
- Ventura (13)
- Sonoma (14)

2.4 Защита от вредоносного ПО

- - Поставляемое ПО должно иметь резидентный антивирусный мониторинг
- - Наличие модуля машинного обучения до и во время запуска программ или открытия документов для обнаружения неизвестных угроз
- - Решение должно иметь возможность автоматического удаления агентов из сервера управления после указанного количества дней неактивности
- - Решение должно иметь возможность удалять вредоносные изменения в реестре Windows, удалять /отправлять в карантин вредоносные файлы и останавливать запущенные вредоносные процессы.
- - Возможность выполнять различные действия по сканированию в зависимости от типов вредоносных программ (трояны / черви, шутки, мистификации, вирусы и т. д.)
- - Решение должно иметь возможность мониторинга поведения для обнаружения поведения вредоносных программ, которое является обычным для атак с использованием эксплойтов.
- - Способен обнаруживать и удалять шпионское и рекламное ПО даже после того, как оно установлено и запущено на компьютере.

- - Обеспечивает постоянную защиту от вредоносных программ и может выполнять обновления независимо от того, подключен ли клиент к серверу управления.
- - Обеспечивает постоянную защиту от вредоносных программ независимо от того, подключена ли конечная точка к Интернету.
- - Решение должно иметь возможность блокировать доступ к вредоносным веб-сайтам и URL-адресам по репутационным сервисам вендора.
- - Решение должно поддерживать список одобренных (белый список) и заблокированных (черный список) URL-адресов.
- - Решение должно иметь возможность блокировать попытки подключения к серверам управления и контроля (C&C).
- - Решение должно поддерживать список одобренных (белый список) и заблокированных (черный список) IP-адресов.
- - Решение должно иметь возможность защитить компьютер от несанкционированного шифрования и модификации
- - Решение должно иметь возможность блокировать процессы, обычно связанные с программами-вымогателями.
- - Решение должно иметь возможность автоматического резервного копирования и восстановления файла, измененного программой-вымогателем
- - Решение должно иметь возможность мониторинга поведения, чтобы постоянно отслеживать конечные точки на предмет необычных изменений в операционной системе, рабочих документах или установленном приложении.
- - Предлагаемое решение должно предлагать возможность отправлять подозрительные полезные данные в песочницу при ее наличии автоматически и без вмешательства пользователя для расширенного обнаружения вредоносных программ.
- - Решение должно поддерживать исключение из сканирования для одобренного (внесенного в белый список) файла, расширения файла и каталога.
- - В решении должна быть технология машинного обучения, обеспечивающая многоуровневую защиту до выполнения и во время выполнения (запуска) вредоносных программ.
- - Решение должно иметь возможность блокировать попытки завершить процессы и службы, связанные с агентом антивируса.
- - Решение должно иметь возможность блокировать попытки изменить, удалить или добавить новые реестры, связанные с агентом антивируса
- - Решение должно поддерживать автоматическое предотвращение вирусных эпидемий со следующими возможностями:
- получает рекомендации политики для конкретных атак от консоли управления предприятия и распространяет политику на другие управляемые серверы

- возможность закрывать доступ к папкам
- возможность настройки доступа в режим «только чтение»
- возможность блокировать определенные порты TCP / UDP или диапазон портов
- возможность заблокировать доступ по имени файла (именам)
- Решение должно иметь возможность запретить другим программам или пользователям удалять, изменять или удалять файлы антивирусного агента

2.5 Виртуальный патчинг

- Решение должно защищать конечные точки от сетевых уязвимостей, нацеленных на ОС конечных точек.
- Решение должно снижать подверженность риску заражения из-за отсутствия патчей обновления ОС
- Решение должно иметь систему предотвращения вторжений (HIPS) на основе хоста для виртуального исправления известных и неизвестных уязвимостей до того, как исправление станет доступным или развернутым.
- Предлагаемое решение должно обеспечивать функциональность виртуального исправления без дополнительных операций агента или интеграции со сторонними производителями.
- Возможность работы HIPS по ряду заранее подготовленных правил;
- Предлагаемое решение должно иметь возможность включения или выключения правила на основе выбора пользователя.
- Предлагаемое решение должно иметь возможность выбора профиля для работы HIPS: оптимизированного с точки зрения безопасности или с точки зрения производительности
- Предлагаемое решение должно иметь возможность работы механизма защиты от уязвимостей в разрыв и на мониторинг;
- Решение должно обнаруживать и блокировать RAT (Remote Access Trojan) и фантомные подключения
- Решение должно иметь возможность блокировать вредоносную загрузку на общий ресурс SMB.
- Решение должно уметь обнаруживать и блокировать удаленную оболочку PowerShell.
- Решение должно иметь возможность блокировать боковое движение, такое как Psexec и Paexec, в то же время позволяя функциональности разрешать то же самое с определенных серверов из белого списка.
- Должен иметь возможность блокировать известные и неизвестные эксплойты уязвимостей.

2.6 Модуль предотвращения потери данных

- - Предлагаемое решение способно обеспечить функциональность DLP без дополнительных операций с агентом или сторонней интеграции и должен быть интегрирован в агент антивируса.
- - Интегрированный DLP обеспечивает защиту данных клиентов, которая включает в себя следующие функции:

• Защищает личные данные - в сети или за ее пределами.

• Расширенные возможности управления устройствами защищают от утечки данных через USB-накопители и другие носители.

• Охватывает самый широкий спектр устройств, приложений и типов файлов.

• Способствует соблюдению требований с большей наглядностью и правоприменением. Например. GDPR, PCI / DSS, PII, GLBA, HIPAA, PDPA, ISMS и т. д.

- - Предлагаемое решение должно иметь возможность базового функционала защиты от утечек конфиденциальных данных: из документов Word, Excel, по ключевым словам, регулярным выражениям, близости определенных слов друг к другу в тексте
- - Предлагаемое решение должно иметь возможность базового функционала защиты от утечек конфиденциальных данных по расширению файлов
- - Функционал защиты от утечек конфиденциальных данных должен уметь: фиксация факта передачи в журнале; уведомление пользователя; уведомление пользователя с полем ввода, которое позволяет зафиксировать в централизованном журнале производственную необходимость для передачи конфиденциальной информации; уведомление пользователя с готовыми вариантами ответа, которое позволяет зафиксировать в централизованном журнале одну из предопределенных администраторами причин, по которой пользователю потребовалось передать конфиденциальную информацию
- - Функционал от утечек конфиденциальных данных должен идти в составе единого агента с антивирусом во избежание нагрузки на рабочую станцию, а также не требовать дополнительной лицензии
- - Решение должно иметь настраиваемые шаблоны DLP, возможность импорта и экспорта идентификаторов данных и добавить выражение DLP.
- - Решение должно иметь возможность интегрироваться с решением для шифрования конечных точек для автоматического шифрования защищенных данных в состоянии покоя и в движении.

2.7 Контроль доступа к устройствам

- - Конфигурация управления доступом к устройствам должна выполняться централизованно с консоли управления.
- - Решение должно отображать уведомление на клиентском компьютере, когда происходит нарушение.
- - Решение должно иметь возможность регистрировать нарушение контроля устройств.
- - Решение должно иметь возможность добавления доверенных устройств.
- - Решение должно иметь возможность ограничивать доступ к устройствам на конечных точках путем назначения прав на чтение, чтение / запись, запись и запрет доступа. Устройства, которые могут быть ограничены, должны включать следующее:
- USB-накопители (также можно отключить автозапуск)
- Сетевые ресурсы
- CD / DVD
- Камеры
- Принтеры

2.8 Межсетевой экран на основе хоста

- - Решение должно иметь возможность централизованно управляемых политик брандмауэра
- - Решение должно иметь возможность обнаруживать и блокировать сетевые вирусы / черви
- - Решение должно иметь возможность централизованного обновления сетевых шаблонов вирусов
- - Решение должно иметь возможность определять разные политики брандмауэра для онлайн / офлайн-клиента
- - Решение должно иметь возможность создания журналов брандмауэра при нарушении
- - Решение должно отображать уведомление о нарушении межсетевого экрана для пользователей на экране клиента
- - Решение должно иметь возможность изменять содержание уведомления
- - Решение должно иметь возможность изолировать конечную точку при запуске предотвращения эпидемий.

2.9 Контроль приложений.

- - Решение должно иметь возможность блокировать запуск вредоносного ПО с помощью настраиваемых политик блокировки, белых и черных списков.
- - Решение должно иметь возможность обеспечить функциональность управления приложениями без использования дополнительных агентов или сторонней интеграции.
- - Решение должно иметь возможность вручную (администратором или сотрудником службы безопасности) или автоматически (через отчет песочницы) заблокировать помеченные подозрительные приложения.
- - Предлагаемое решение должно поддерживать импорт значений хэша SHA1 и SHA2 и блокировать / разрешать выполнение этого же
- - Решение должно уметь сопоставлять данные из миллионов событий приложений, чтобы идентифицировать угрозы и поддерживать актуальную базу данных проверенных приложений.

2.10 Требования к защите серверов.

- - Поддерживаемые платформы (агент) - Windows
- Windows Server 2012/Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

- Поддерживаемые платформы (агент) - Linux

- Red Hat Enterprise Linux 6/7/8/9
- CentOS 6/7/8
- Amazon Linux/ Amazon Linux 2
- Amazon Linux 2023 (64-bit)
- Amazon Linux 2023 (AWS ARM-based Graviton 2)
- AlmaLinux 8/9
- Rocky Linux 8/9
- Oracle Linux 6/7/8/9
- Solaris 10 Updates 4–6/ Updates 7-10/Update 11
- Solaris 11.0/ Solaris 11.2–11.3/ Solaris 11.4
- SUSE Linux Enterprise Server 12/15
- Ubuntu 16.04/Ubuntu 18.04/Ubuntu 20.04/Ubuntu 22.04
- Debian 8/9/10/11
- Cloud Linux 5/6/7
- AIX 6.1 TL 9 or later
- - Система должна иметь поддержку генерации специальных скриптов для автоматического разворачивания агентов под платформы Windows
- - Система должна иметь поддержку генерации специальных скриптов для автоматического разворачивания агентов под платформы Linux
- - Система должна иметь поддержку генерации специальных скриптов для автоматического разворачивания агентов под платформы Solaris
- - Сервер управления должен поддерживать работу с более, чем одним VMware vCenter

- - Система должна иметь возможность ручного сброса агента (отключение политик, отвязывание от системы управления)
- - Система управления должна иметь инструменты для объединения защищаемых систем в произвольные группы по широкому набору признаков (условий)
- - Система должна иметь возможность автоматического применения релевантных целевым системам наборов правил защиты на основе расширенного списка условий и событий (машина появилась в инфраструктуре, машина переместилась с хоста на хост, машина включилась, у машины произошла смена IP)
- - Агент должен распространяться в виде максимально облегченного ядра (без функциональных модулей)
- - Агент должен иметь возможность подгрузки функциональных модулей с сервера на основе включённых защитных функций и политик
- - Агент должен иметь возможность обмена данными с сервером как в двустороннем режиме (как сервер, так и агент могут инициировать соединение), так и в одностороннем режиме (только сервер, или только агент может инициировать соединение)
- - Агент должен иметь возможности работы с полным сокрытием графической части
- - Агент должен поддерживать управление из командной строки
- - Агент должен иметь встроенные механизмы самозащиты, отключаемые только из командной строки (включая пароль)
- - Агент должен иметь возможность установки без первичной привязки к серверу управления (для включения его в стандартные шаблоны виртуальных машин и установочных образов)
- - Агент должен иметь возможности привязки к серверу управления с помощью инструментов командной строки
- - Агент должен иметь возможности аварийного сброса с помощью инструментов командной строки.

2.11 Требования к защите от вредоносного кода.

- - Система должна иметь возможность ручного запуска полной и быстрой антивирусной проверки защищаемых систем
- - Работа антивируса с использованием репутационной оценки ("легкие агенты")
- - Проверка репутации по критериям глобальной распространённости объекта и числу запусков
- - Работа антивируса с использованием классической модели оценки угроз по сигнатурам на самих агентах (для изолированных систем)
- - Работа с использованием безагентной технологии в среде Vmware (vShield Endpoint)
- - Использование безагентных средств для дедубликации проверки файлов в безагентном режиме (кэширование в среде Vmware)

- - Настройки срока жизни кеша и исключения для безагентной проверки
- - Возможность извлечения объектов из карантина администратором как в случае агентной защиты, так и в безагентном режиме
- - Антивирусная защита в реальном времени для систем под управлением Windows и Linux
- - Запуск антивирусных проверок по расписанию для Windows и Linux
- - Запуск антивирусных проверок вручную для Windows и Linux
- - Возможность задания временных границ антивирусной проверки (как время старта, так и время окончания)
- - Возможность задания режимов проверки в реальном времени (запись/чтение, только запись, только чтение)
- - Обеспечение контроля памяти при использовании агентов
- - Поведенческий анализ для выявления неизвестных угроз по специфическим признакам
- - Защита от шифровальщиков на основе системного отслеживания попыток зашифровать данные
- - Автоматическое создание резервных копий документов, в отношении которых были замечены попытки их зашифровать, а также их восстановление после очистки системы от следов шифровальщика
- - Оценка угроз по модели машинного обучения до запуска файлов
- - Интеграция с системой динамического анализа ("песочницей") для передачи подозрительных объектов на проверку и последующей их блокировки на основе вердикта "песочниц" при наличии песочницы
- - Проверка файлов внутри архивов
- - Возможность явно задать включаемые в проверку папки и файлы
- - Возможность явно задать исключаемые из проверки папки, файлы, расширения, процессы
- - Возможность контроля устройств с возможностью добавления белого списка.
- - Возможность работать с готовыми списками включаемых/исключаемых для проверки объектов, чтобы тиражировать их для различных групп защищаемых систем
- - Настройка максимально потребляемого процессорного времени агентом для ручных и плановых проверок
- - Настройка многопоточной антивирусной проверки
- - Блокирование доступа к вредоносным ресурсам на основе репутационной оценки в режиме агентной защиты
- - Настройка пороговых значений для регулирования чувствительности срабатывания блокировки
- - Возможность настройки выводимого сообщения при блокировке

- - Возможность указания портов для мониторинга веб активностей
- - Возможность ведения "чёрных" и "белых" списков по URL (домен, URL,)
- - Использование как глобального центра для обработки, так и работа через локально установленные сервера репутационных сервисов

2.12 Межсетевой экран уровня узла

- - Возможность выбора работы сетевого движка - inline или tap (для тестовых задач)
- - Поддержка работы на L2 уровне
- - Поддержка работы с заголовками и фреймами
- - Поддержка работы на базе агентов
- - Поддержка работы в безагентном режиме (VMware)
- - Наличие предустановленных правил
- - Поддержка обнаружения разведки - сканирование портов с возможностью указания диапазона
- - Возможность запуска проверки открытых портов с 1–1024 порты для модуля МСЭ
- - Поддержка обнаружения разведки - OS Fingerprint
- - Поддержка обнаружения разведки - аномальные TCP активности (null scan, SYN FIN scan, Xmax scan)
- - Поддержка обнаружения разведки - возможность создания исключений по источникам
- - Возможность настройки изоляции интерфейсов
- - Поддержка stateful inspection
- - Возможность работы МСЭ по расписанию
- - Возможность сбора данных пакета для расследования
- - Работа с поддержкой контекста (сетевое окружение)
- - Возможность выбора работы сетевого движка - bypass (fail open) или блокировка (fail close)
- - Возможность выбора работы сетевого движка - inline или tap (для тестовых задач)
- - Возможность указания максимального числа соединений (TCP, UDP, ICMP)
- - Возможность задать таймауты для различных состояний сетевых сессий и аномалий (SYN_SENT, CLOSED, CLOSING, ACK STORM, ESTABLISHED и других)
- - Блокировка соединений с идентичными IP для SRC и DST
- - Возможность настройки запрета для Null IP
- - Возможность "тихого" сброса TCP соединения
- - Возможности настройки сброса соединения для пакетов с дублирующимися или перекрывающимися данными (evasive retransmit)
- - Возможности проверки TCP Checksum
- - Возможности настройки минимальных значений для фрагментов пакета (fragment offset & size)
- - Возможности настройки минимальных значений для SSL сессий (time & size)
- - Возможности сброса неизвестного протокола для SSL трафика
- - Возможности фильтрации туннелей (IPv4, IPv6)
- - Возможность bypass для MAC адресов, не относящихся к хосту

2.13 Контроль приложений

	• - Возможность работы модуля контроля приложений с помощью агента (Windows, Linux) • - Режим работы в режиме "белого списка" (запрет запуска всех приложений, не входящих в "белый" список) • - Режим работы в режиме избирательного запрета • - Поддержка технологических "окон" (разрешение на запуск и установку объектов, связанных с обновлением систем и приложений) - бессрочно или на ограниченный период времени • - Возможность запрета или разрешения запуска из журнала событий модуля контроля приложений **2.14 Требования к технической поддержке.** Техническая поддержка должна: • - предоставляться на русском, казахском и английском языке сертифицированными специалистами производителя на всей территории Республики Казахстан круглосуточно без праздников и выходных (24x7) по электронной почте и через Интернет, а также по телефону; - Web-сайт производителя решения должен быть на русском или английском языке.

Подписал	Измуратов Олжас Амандыкович
Дата подписания	12.11.2026