

**Сатып алынатын тауарлардың техникалық ерекшелігі
(тапсырыс беруші толтырады)**

Тапсырыс берушінің атауы:	"Нұрсұлтан Назарбаев халықаралық әуежайы" акционерлік қоғамы
Ұйымдастырушының атауы:	"Нұрсұлтан Назарбаев халықаралық әуежайы" акционерлік қоғамы
Конкурстың №:	№ 17792618-1
Конкурстың атауы:	Бағдарламалық жасақтаманы сатып алу. Тел.: 8 (7172) 777-377, 777-177
Лоттың нөмірі:	№ 88075217-OK1
Лоттың атауы	Бағдарламалық қамтамасыз ету
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*:	620129.000.000000
Тауардың атауы*:	Бағдарламалық қамтамасыз ету
Өлшем бірлігі*:	Дана
Саны (көлемі)*:	1
Қосылған құн салығын есептемегенде бірлік бағасы*:	19602187.93
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома*:	19602187.93
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс*:	

Жеткізу шарттары (сәйкес ИНКОТЕРМС 2010)*	DDP термині келу орнын көрсете отырып қолданылады. Бұл сатып алушының елінде көрсетілген жерге тауар жеткізілгеннен кейін сатушының жауапкершілігі аяқталатынын білдіреді. Жүктерді жеткізу бойынша барлық тәуекелдер, барлық шығыстар (салықтар, баждар және т.б.), импорт кезінде төленетін баждар мен басқа да төлемдерді қоса алғанда, тауардың бүлінуі мен жоғалуы үшін жауапкершілік осы уақытқа дейін сатушыға жүктеледі, сатушы сонымен қатар кедендік тазартуға жауап береді
Жеткізу мерзімі*	шартқа қол қойылған күннен бастап 15 күнтізбелік күн өткен соң, 30 күнтізбелік күн ішінде
Жеткізу орны*	711210000, Астана қ., Есіл ауданы Қабанбай батыр даңғылы 119, әуежай
Аванстық төлем мөлшері*:	0
Ұлттық стандарттардың атауы, ал олар болмаған жағдайда сатып алынатын тауарларға арналған мемлекетаралық стандарттар. Ұлттық және мемлекетаралық стандарттар болмаған кезде мемлекеттік сатып алуды нормалауды ескере отырып, сатып алынатын тауарлардың талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары көрсетіледі.	жоқ
Тұрғын емес мақсаттағы ғимараттарды, құрылыстарды, үй-жайларды, авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған шарт жасасу күніне дейін (үш жылға дейін) шығарылған жылы болуға тиіс	
Кепілдік мерзімі (айлармен)	24

Сатып алынатын тауардың талап етілетін функционалдық, техникалық, сапалық, пайдалану және өзге де сипаттамаларының сипаттамасы	"Мемлекеттік сатып алу туралы" Қазақстан Республикасы Заңының 12 – бабы 4-тармағының 2-тармақшасына сәйкес, осы сатып алу wallix РАМ артықшылықты қол жеткізуді басқару жөніндегі бұрын сатып алынған және белгіленген бағдарламалық қамтамасыз етуге қолданыстағы лицензияны (бұдан әрі - Шешім) толық жинақтау болып табылады.. Шешім Тапсырыс берушінің инфрақұрылымына енгізілген және ақпараттық қауіпсіздік талаптарына сәйкес артықшылықты қолжетімділікті басқаруды және сессияларды бақылауды қамтамасыз ету үшін пайдаланылады. Ұзарту функционалдылықты сақтау, техникалық қолдау құқықтарын қамтамасыз ету және нормативтік талаптарға сәйкестік үшін қажет. Жеткізуші РАМ WALLIX бойынша қолда бар 1 (лицензия) - 10 (пайдаланушылар) санында жаңартуға лицензия беруге міндетті. Лицензияның қолданылу мерзімі-24 ай. Бағдарламалық жасақтама төмендегі сипаттамаларға сәйкес келуі керек: 1. СЕАНС АРТЫҚШЫЛЫҚТАРЫН БАСҚАРУ Шешімдер прокси режимінде жұмыс істеуі керек, әкімшіге РАМ шешімімен қорғалған жүйелерде агенттерді орнатудың қажеті жоқ. Дәлелді база үшін орындалған іс-қимылдардың шартсыздығы және материалды қорғау бойынша қауіпсіздік функцияларын пайдалануға мүмкіндік беретін артықшылықты пайдаланушылардың (командалар мен орындалған іс-қимылдар) сессияларын жазу және бақылау. Шешім Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure сияқты бұлттық платформаларда іске асыруды қолдауы керек. Ол сондай-ақ виртуалды ортаны қолдауы керек: ядроға негізделген Виртуалды машина (KVM), Microsoft Hyper-V, OpenStack, VMware vSphere. Тәуелсіз аппараттық платформаны пайдалану мүмкіндігі де сақталуы керек. Шешім белгілі бір операциялық жүйеге орнатуды қажет етпей, бірыңғай жүйе ретінде жеткізілуі керек. Өндіруші бүкіл жүйені, яғни операциялық жүйені де, қолданба деңгейін де қолдауы керек. Шешім бастапқыда SSH және RDP протоколдарының PROXY және SSH / TELNET / RLOGIN / RDP / VNC қосылымдарын PROXY-ден қорғалған жүйелерге қолдауы керек. Стандартты емес протоколдар үшін (бастапқыда шешіммен қолдау көрсетілмейді) пайдаланушыға тек клиент пен оның ресурстары көрінетін етіп орнату серверінде осындай протоколды қолдайтын Клиентті шақыру мүмкіндігі болуы керек. Стандартты емес протоколдар мен оларды клиент шақыруы үшін шешім Microsoft RemoteApp технологиясын қолдауы керек. Профиль параметрлеріне байланысты әкімші, пайдаланушы, аудитор рұқсаттарын тағайындау мүмкіндігі. Аудитор қол жеткізген жағдайда, пайдаланушы профилі, ең болмағанда, таңдалған пайдаланушы топтары мен жүйенің мақсатты топтарының жазбаларына олар үшін конфигурацияланған артықшылықты есептік жазбалармен бірге кіруді шектеу мүмкіндігін ұсынуы керек. Пайдаланушы профилінің конфигурациясы бастапқы IP-мекен-жайға негізделген кіріс қосылымдарын сүзу мүмкіндігін қамтуы керек, яғни тағайындалған профилі бар пайдаланушылар үшін кіруді басқару тізімдерін (ACL) құру. Шектеу анықтамасы пішімге рұқсат беруі керек: IP мекенжайы, желі мекенжайы және желі маскасы немесе толық домен атауы (FQDN). Шешім таңдалған
--	---

пайдаланушылар тобын мақсатты жүйелердің көрсетілген тобына жатқызу арқылы қол жеткізу саясатын анықтауға мүмкіндік беруі керек. Жазылған деректерді алдын ала қарау сеанстың бейнежазбасын және барлық сеанс метадеректерін (RDP) көрсететін жазбаның транскрипциясын, сондай-ақ консоль үшін көрсетілетін деректердің толық жазбасын (SSH) қамтуы керек. Нақты уақыттағы қосылымды бақылау, оның ішінде сеансты дереу тоқтату мүмкіндігімен нақты уақыт режимінде көру мүмкіндігі. Жергілікті пайдаланушылар мен әкімшілер парольдерінің ережелер жиынтығын (саясатын) басқару. Таңдалған пайдаланушы топтары үшін сеанс жазбасын қосу / өшіру мүмкіндігі. Браузерде арнайы плагин орнатуды қажет етпестен, кем дегенде SSH және RDP сеанстары үшін веб-портал, браузер арқылы кіруді теңшеу мүмкіндігі. Шешім пайдаланушының ақпаратын синхрондауды қажет етпестен Microsoft Active Directory интеграциясын қамтамасыз етеді. Бұл дегеніміз, Active Directory пайдаланушысы пайдаланушылар тобына автоматты түрде қосылады, сонымен бірге PAM шешімімен танылады. IP мекенжайын, DNS атауын көрсету арқылы мақсатты жүйелерді анықтау мүмкіндігі немесе желілік IP мекенжайы мен желі маскасы арқылы көрсету мүмкіндігі. RDP сеанстары үшін "метадеректер" туралы ақпаратты қамтуы керек: - белсенді терезені өзгерту; - Windows ОЖ терезесінде берілген батырманы таңдау операциясы; - "радио түймесі" түріндегі батырмаларды таңдау немесе терезеде "құсбелгі" опциясын таңдау әрекеті; - Windows ОЖ терезесінде мәтін өрісінің мазмұнын өзгерту; - процестің басталуы және аяқталуы; - Windows ОЖ алмасу буфері арқылы файлдарды бөлісу; - Windows ОЖ-нің қайта бағытталған желілік ресурстары арқылы файлдарды бөлісу. RDP сеанстары үшін Microsoft Windows серверінің мақсатты жүйесінде шектеулі TCP қосылымдарын блоктау мүмкіндігі. Сеанстар үшін RDP-Microsoft Windows серверінің мақсатты жүйесінде таңдалған процестерді блоктау мүмкіндігі. SSH және RDP сеанстары үшін орындалатын командалар үшін тұрақты өрнек үлгілерін жасау мүмкіндігі және егер мұндай үлгі анықталса, әрекеттердің бірін орнату мүмкіндігі: сеансты аяқтау немесе үлгіні анықтау туралы хабарлама жіберу. SSH және RDP үшін орындалатын командалардың шаблондарын орнату қол жеткізілетін пайдаланушылар топтарын құру деңгейінде немесе Pам шешімімен қорғалған және басқарылатын мақсатты жүйелер тобы деңгейінде орындалуы керек. Пайдаланушы орнатқан RDP сеансын бөлісу мүмкіндігін қолдау аудитор / әкімші, бұл толық өзара әрекеттесу деп түсініледі - пернетақтадан таңбаларды енгізу және тінтуірдің қозғалысы. Шешім жүйе пайдаланушыларының сертификат арқылы аутентификациясын және мақсатты жүйеге кірген кезде бірдей сертификатты пайдалануды қамтамасыз етуі керек. Жүйені ICAP протоколы бойынша AV / DLP шешімдерімен біріктіру мүмкіндігі. Сеанстар кезінде енгізілген құпия сөздерді құпия сөзді енгізу өрістерінде немесе пайдаланушы тіркелгісін басқару терезесінде енгізу курсорын табу арқылы қорғау.>Login / пароль, X. 509 сертификаты, SSH кілті бойынша пайдаланушының

	аутентификациясы. Аутентификация хаттамаларын қолдау: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, TACACS +. Мақсатты жүйелердің таңдалған тобына бекітушілердің көрсетілген санымен қосылу үшін жұмыс процесінің қосымша келісімін орнату мүмкіндігі. Кіру уақытына байланысты қосымша рұқсатты орнату мүмкіндігі, мысалы, мақұлдау дүйсенбіден жұмаға дейін сағат 8.00-ден 16.00-ге дейін қажет емес, ал қалған күндер мен сағаттар үшін мақұлдау қажет. 2. ҚҰПИЯ СӨЗ МЕНЕДЖЕРІ Белгілі бір хосттар немесе тіркелгі топтары үшін SSH құпия сөздері мен кілттерін автоматты түрде айналдыру мүмкіндігі. Автоматты SSH құпия сөздері мен кілттері үшін Ерекшеліктер жасау мүмкіндігі. Мақсатты жүйелерде парольдерді автоматты түрде өзгерту кестелерін құру. Бір реттік парольдер жасаңыз және оларды қолданғаннан кейін автоматты түрде ауыстырыңыз. Құпия сөздерді өзгерту үшін теңшелетін саясаттарды / талаптарды жасау мүмкіндігі: - таңбалардың қажетті минималды саны; - әкімші көрсеткен таңбаларды алып тастау; - бас және кіші әріптерді міндетті түрде пайдалану; - арнайы таңбаларды міндетті түрде пайдалану. Әртүрлі хост топтары немесе тіркелгі топтары үшін әртүрлі құпия сөзді өзгерту саясаттарын орнату мүмкіндігі. Көрсетілген уақыт кезеңі ішінде парольдің қолданылу мерзімін орнату. Файлдардағы құпия сөздерді жасыру немесе шифрын ашу арқылы бақылау. Келесі жүйелер үшін SSH құпия сөздерін немесе кілттерін өзгертуге мүмкіндік беретін плагиндерді ұсыну: AIX, F5 BIG IP, SAP IQ, AWS IAM, Checkpoint, ESX, Fortinet Fortigate, HP ILO, MS SQL Server, acacle, Stormshield, Teradata, Unix, Micorsoft Windows, Cisco, Dell iDRAC, IBM 3270, Juniper SRX, LDAP, MySQL, Palo Alto PA-500, Grafana. Шешім кем дегенде REST API көмегімен құпия сөзді өзгертуге рұқсат беруі керек. 3. ҚОЛ ЖЕТКІЗУДІ БАСҚАРУ ПОРТАЛЫ Жүйеге қосымша шешім болуы керек-кем дегенде веб-шолғышта SSH және RDP протоколдары үшін қосылымдарды басқаруды жүзеге асыратын веб-портал. Қосылу операциясын іске асыру тек HTML5 қолдайтын веб-шолғышты қолдану арқылы, плагиндерді орнатуды қажет етпестен (мысалы, flash, java) жүзеге асырылуы керек. Веб-шолғышты қолдау: Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox. Шешім келесі ОЖ-нің бірінде орнатылған қосымша ретінде жеткізілуі керек: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016 (x64), Red Hat Enterprise Linux, CentOS 6.6, Red Hat Enterprise Linux, CentOS 7.1, Debian 8. (amd64). Шешім браузер арқылы PSM-ге қол жеткізуден басқа, іздеу функциясы деп аталатын нәрсені қамтамасыз етуі керек, бір немесе бірнеше PSM даналары үшін жазылған сеанстардың метадеректерін Ғаламдық іздеу. Аутентификация хаттамаларын қолдау: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, SAML. Лицензия кем дегенде 10 пайдаланушыға кіруге рұқсат беруі керек. Лицензия бірнеше қол жетімді портал даналарын орнатуға мүмкіндік беруі керек, мысалы, бір дананы кіру мақсаттары үшін (PSM), ал екіншісін аудит мақсаттары үшін (ғаламдық іздеу метадеректері) пайдалануға болады. 4.
--	---

	ЛИЦЕНЗИЯЛАУ Ұсынылатын өнім өндірушінің ТМД-дағы дистрибуциясының ресми арнасы арқылы жеткізілуі тиіс. Ұсынылған бағдарламалық жасақтама жүйені жеткізген күні өндіруші жариялаған соңғы нұсқа болуы керек. Жүйе Linux және Windows серверлері, коммутаторлар, маршрутизаторлар және басқару консолі сияқты қосымшалар сияқты белсенді желілік құрылғылар сияқты шексіз мақсаттарды қорғай алуы керек. Жүйеге бір уақытта кемінде 10 пайдаланушыға кіруге рұқсат беру. Лицензия техникалық қолдауды қамтуы керек. Әлеуетті өнім берушіге қойылатын талаптар: Әлеуетті өнім беруші Мемлекеттік сатып алуды жүзеге асыру қағидаларына 4-қосымшаның 2) тармақшасының 7) тармақшасының негізінде конкурсқа өтінім құрамында Қазақстан Республикасының аумағында БҚ жеткізу құқығына вендордан авторизациялық хат ұсынуға тиіс. Хатта конкурсқа лоттың нөмірі және Шешімнің өнім берушіге лицензиялардың қолданылу мерзімі аяқталғанға дейінгі мерзімнен кем емес техникалық қолдауы болуы тиіс. Техникалық қолдау кем дегенде жұмыс күндері (дүйсенбіден жұмаға дейін) сағат 8.00-ден 19.00-ге дейін (мемлекеттік мерекелерден басқа) ұсынылуы керек. Жеткізушіге қолдау ағылшын тілінде беріледі. Техникалық мәселені ашу кем дегенде екі байланыс арнасы арқылы мүмкін болуы керек: арнайы телефон нөмірі арқылы және ашық өтінімнің күйін қашықтан хабарлауға және бақылауға мүмкіндік беретін веб-шолғыш арқылы қол жетімді техникалық қолдау порталы арқылы. Ұсынылатын техникалық қолдау шеңберінде Тапсырыс беруші сұраулар санын шектемей, техникалық көмек туралы ақаулар мен сұраулар туралы хабарлай алуы тиіс. Техникалық қолдау порталына кіру кем дегенде 2 пайдаланушы тіркелгісіне берілуі керек. Билеттерді өңдеу, кем дегенде, техникалық мәселелерді шешуді және жүйені орнатуды қамтуы керек. Жаңа ашық билетке жауап беру уақыты 2 жұмыс күнінен аспауы керек. Техникалық қолдау жүйесі жүйенің ағымдағы нұсқаларына және жаңартуларына, сондай – ақ техникалық құжаттамаға-кем дегенде жүйенің Пайдаланушы және әкімші нұсқаулықтарына қол жеткізуге кепілдік беруі керек.
Ілеспе қызметтер (қажет болған жағдайда көрсетіледі) (тауарларды монтаждау, баптау, оқыту, тексеру және сынау)	

Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді)	
---	--

Ескертпе:

1. Функционалдық, техникалық, сапалық, пайдалану, өзге де сипаттамалар, ілеспе қызметтер және орындаушыға қосымша шарттар бойынша әрбір талап жеке жолда көрсетіледі.
 2. Осы техникалық ерекшелікте әлеуетті өнім берушіге қойылатын біліктілік талаптарын белгілеуге жол берілмейді.
 3. Өзге құжаттарда техникалық ерекшелік талаптарын белгілеуге жол берілмейді.
- *мәліметтер мемлекеттік сатып алу жоспарынан тартылады (автоматты түрде көрсетіледі).

**Техническая спецификация
закупаемых товаров
(заполняется заказчиком)**

Наименование заказчика	Акционерное общество "Международный аэропорт Нурсултан Назарбаев"
Наименование организатора	Акционерное общество "Международный аэропорт Нурсултан Назарбаев"
№ конкурса:	№ 17792618-1
Наименование конкурса:	Приобретение программного обеспечения. Тел.: 8 (7172) 777-377, 777-177
Номер лота:	№ 88075217-ОК1
Наименование лота:	Программное обеспечение
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*:	620129.000.000000
Наименование товара*:	Программное обеспечение
Единица измерения*:	Штука
Количество (объем)*:	1
Цена за единицу, без учета налога на добавленную стоимость*:	19602187.93
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*:	19602187.93
Условия поставки (в соответствии с ИНКОТЕРМС 2010)*:	DDP термин употребляется с указанием места прибытия. Он означает, что ответственность продавца заканчивается после того, как товар доставлен в указанное место в стране покупателя. Все риски, все расходы по доставке груза (налоги, пошлины и т. д.), ответственность за порчу и потерю товара, включая пошлины и прочие выплаты, выплачиваемые при импорте, до этого момента несёт продавец, также он несёт ответственность за таможенную очистку.
Срок поставки*:	по истечении 15 календарных дней со дня подписания договора, в течение 30 календарных дней
Место поставки товара*:	711210000, г.Астана, район Есиль проспект Кабанбай батыра 119, аэропорт

Размер авансового платежа* **:	0 %
Наименование национальных стандартов, а при их отсутствии межгосударственных стандартов на закупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров, с учетом нормирования государственных закупок.	отсутствуют
Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора за исключением приобретения здания, строения, сооружения, помещения, имеющих нежилое назначение, авиационной техники	
Гарантийный срок (в месяцах)	24

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	В соответствии с пп. 2) п. 4) статьи 12 Закона Республики Казахстан «О государственных закупках», данная закупка является доукомплектованием действующей лицензии на ранее приобретённое и установленное программное обеспечение по управлению привилегированным доступом Wallix PAM (далее – Решение). Решение внедрено в инфраструктуру Заказчика и используется для обеспечения управления привилегированным доступом и контроля сессий в соответствии с требованиями информационной безопасности. Продление необходимо для сохранения функциональности, обеспечения прав на техническую поддержку и соответствия нормативным требованиям. Поставщик обязан предоставить лицензии на обновление имеющегося ПО PAM Wallix в количестве 1 (лицензий) - 10 (пользователей). Срок действия лицензии – 24 месяца. Программное обеспечение должно соответствовать нижеуказанным характеристикам: 1. УПРАВЛЕНИЕ ПРИВИЛЕГИЯМИ СЕАНСА Решения должны работать в режиме ПРОКСИ, без необходимости для администратора устанавливать агенты в системах, защищенных решением PAM. Запись и контроль сессий привилегированных пользователей (команд и выполненных действий), позволяющие использовать функции безопасности по безусловности выполненных действий и защите материала для доказательной базы. Решение должно поддерживать реализацию на облачных платформах, таких как Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure. Оно также должен поддерживать виртуальные среды: виртуальную машину на основе ядра (KVM), Microsoft Hyper-V, OpenStack, VMware vSphere. Также должна поддерживаться возможность использования самостоятельной аппаратной платформы. Решение должно поставляться как единая система, без необходимости установки в конкретной операционной системе. Производитель должен поддерживать всю Систему, то есть как операционную систему, так и уровень приложений. Решение должно изначально поддерживать подключения для протоколов SSH и RDP к PROXY и SSH / TELNET / RLOGIN / RDP / VNC от PROXY к защищаемым системам. Для нестандартных протоколов (изначально не поддерживаемых решением) должна существовать возможность вызова клиента, поддерживающего такой протокол на инсталляционном сервере таким образом, чтобы пользователю были видны только клиент и его ресурсы. Для нестандартных протоколов и их вызова клиентом решение должно поддерживать технологии для Microsoft RemoteApp. Возможность назначения прав доступа администратора, пользователя, аудитора, в зависимости от настроек профилей. В случае доступа аудитора профиль пользователя должен, по крайней мере, предлагать возможность ограничения доступа к записям выбранных групп пользователей и целевых групп системы вместе с настроенными для них привилегированными учетными записями. Конфигурация профиля пользователя должна включать возможность фильтрации входящих соединений на основе исходного IP-адреса, то есть, создание списков управления доступом (ACL) для пользователей с назначенным профилем. Определение ограничения должно разрешать формат: IP-адрес,
--	---

сетевой адрес и сетевая маска или полное доменное имя (FQDN). Решение должно позволять определять политику доступа, путем отнесения выбранной группы пользователей к указанной группе целевых систем. Предварительный просмотр записанных данных должен включать видеозапись сеанса и расшифровку записи, показывающую все метаданные сеанса (RDP), а также полную запись отображаемых данных для консоли (SSH). Мониторинг соединения в реальном времени, в том числе возможность просмотра сеанса в реальном времени с возможностью его немедленного прекращения. Управление наборами правил (политиками) паролей локальных пользователей и администраторов. Возможность включения / отключения записи сеанса для выбранных групп пользователей. Возможность настройки доступа через веб-портал, браузер, по крайней мере, для сессий SSH и RDP, без необходимости установки специального плагина в браузере. Решение обеспечивает интеграцию с Microsoft Active Directory без необходимости синхронизации информации пользователя. Это означает, что пользователь Active Directory добавляется в группу пользователей автоматически, в то же время распознается решением PAM. Возможность определения целевых систем путем указания IP-адреса, DNS-имени или возможность указания по сетевому IP-адресу и маске сети. Для сеансов RDP «метаданные» должны содержать информацию о: - изменении активного окна; - операцию выбора задаваемой кнопки в окне ОС Windows; - операцию выбора кнопок типа "радио-кнопка" или выбора опции "флажок" в окне; - изменении содержимого текстового поля в окне ОС Windows; - начале и завершении процесса; - обмене файлами через буфер обмена ОС Windows; - обмене файлами через перенаправленные сетевые ресурсы ОС Windows. Для сеансов RDP - возможность блокировать ограничивающие TCP-соединения в целевой системе сервера Microsoft Windows. Для сеансов RDP - возможность блокировать выбранные процессы в целевой системе сервера Microsoft Windows. Для сеансов SSH и RDP, возможность создавать шаблоны регулярных выражений для выполняемых команд, и, если такой шаблон обнаруживается, возможность установить одно из действий: завершение сеанса или отправка уведомления об обнаружении шаблона. Задание шаблонов выполняемых команд для SSH и RDP должно выполняться на уровне создания групп пользователей, для которых создается доступ, или на уровне группы целевых систем, доступ к которой защищен и контролируется PAM-решением. Поддержка функции совместного использования сеанса RDP, установленного пользователем с правами аудитор / администратор, что понимается как полное взаимодействие - ввод символов с клавиатуры и движения мыши. Решение должно обеспечивать аутентификацию пользователей системы с помощью сертификата и использование того же сертификата при входе в целевую систему. Возможность интеграции Системы с AV / DLP решениями по протоколу ICAP. Защита паролей, введенных во время сеансов, путем обнаружения курсора ввода в полях ввода пароля или в окне управления учетными записями пользователей. Аутентификация

	пользователя по логину / паролю, сертификату X.509, ключу SSH. Поддержка протоколов аутентификации: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, TACACS +. Возможность установить дополнительное согласование рабочего процесса для подключений к выбранной группе целевых систем указанным количеством утверждающих. Возможность установить дополнительное разрешение доступа в зависимости от времени входа в систему, например одобрение не требуется с понедельника по пятницу с 8:00 до 16:00, а для всех остальных дней и часов одобрение требуется. 2. МЕНЕДЖЕР ПАРОЛЕЙ Возможность автоматической ротации паролей и ключей SSH для определенных хостов или групп учетных записей. Возможность создавать исключения для автоматических паролей и ключей SSH. Создание расписаний для автоматической смены паролей в целевых системах. Создание одноразовых паролей и их автоматическая замена после использования. Возможность создавать собственные политики / требования для смены паролей: - требуемое минимальное количество символов; - исключение символов, указанных администратором; - обязательное использование букв верхнего и нижнего регистра; - обязательное использование специальных символов. Возможность устанавливать разные политики смены паролей для разных групп хостов или групп учетных записей. Установка срока действия пароля в течение указанного периода времени. Контроль паролей в файлах путем их сокрытия или расшифровки. Предоставление плагинов, позволяющих изменять пароли или ключи SSH для следующих систем: AIX, F5 BIG IP, SAP IQ, AWS IAM, Checkpoint, ESX, Fortinet Fortigate, HP iLO, MS SQL Server, ORACLE, Stormshield, Teradata, Unix. , Microsoft Windows, Cisco, Dell iDRAC, IBM 3270, Juniper SRX, LDAP, MySQL, Palo Alto PA-500, Grafana. Решение должно разрешать смену пароля с использованием как минимум REST API. 3. ПОРТАЛ УПРАВЛЕНИЯ ДОСТУПОМ В дополнение к Системе должно быть решение - веб-портал, который реализует управление подключениями, по крайней мере, для протоколов SSH и RDP в веб-браузере. Реализация операции подключения должна осуществляться только с использованием веб-браузера с поддержкой HTML5, без необходимости установки плагинов (например, flash, java). Поддержка веб-браузеров: Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox. Решение должно поставляться в виде приложения, установленного на одной из следующих ОС: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016 (x64), Red Hat Enterprise Linux, CentOS 6.6, Red Hat Enterprise Linux, CentOS 7.1, Debian 8. (amd64). Решение, помимо доступа к PSM с помощью браузера, должно обеспечивать так называемую функцию поиска, глобальный поиск метаданных записанных сеансов для одного или нескольких экземпляров PSM. Поддержка протоколов аутентификации: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, SAML. Лицензия должна разрешать доступ не менее 10 пользователям. Лицензия должна позволять установку экземпляров портала с множественным доступом, чтобы, например, один экземпляр можно
--	--

	было использовать для целей доступа (PSM), а другой - для целей аудита (метаданные глобального поиска). 4. ЛИЦЕНЗИРОВАНИЕ Предлагаемая продукция должна поставляться через официальный канал дистрибуции Производителя в СНГ. Предлагаемое программное обеспечение должно быть последней версией, опубликованной Производителем на дату поставки Системы. Система должна быть способна защитить неограниченное количество целей, например Серверы Linux и Windows, активные сетевые устройства, такие как коммутаторы, маршрутизаторы и приложения, например консоли управления и др. Разрешить доступ к Системе одновременно не менее 10 пользователям. Решение должно иметь техническую поддержку поставщика сроком не менее, чем до конца срока действия лицензий ПО. Техническая поддержка должна предоставляться как минимум в рабочие дни. Поддержка поставщика предоставляется в том числе на английском языке. Открытие технической проблемы должно быть возможно по крайней мере с помощью двух каналов связи: через выделенный номер телефона и через портал технической поддержки, доступный через веб-браузер, позволяющий удаленно сообщать и отслеживать статус открытой заявки. В рамках предоставляемой Технической поддержки Заказчик должен иметь возможность сообщать о сбоях и запросах о технической помощи без ограничения количества запросов. Доступ к portalу технической поддержки должен быть предоставлен как минимум 2 учетным записям пользователей. Обработка билетов должна, как минимум, включать решение технических проблем и настройку системы. Время ответа на новый открытый тикет не может превышать 2 рабочих дней. Служба технической поддержки должна гарантировать доступ к текущим версиям Системы и обновлениям, а также к технической документации – как минимум, к руководствам пользователя и администратора Системы. Требования к потенциальному поставщику: Потенциальный поставщик на основании пп. 7) п. 2) Приложения 4 к Правилам осуществления государственных закупок, в составе заявки на конкурс должен предоставить авторизационное письмо от вендора на право поставки ПО на территории Республики Казахстан. В письме должен быть указан номер лота на конкурс и точное название Заказчика.
Сопутствующие услуги (указываются при необходимости) (монтаж, наладка, обучение, проверки и испытания товаров)	

Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	
--	--

Примечание

1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.
 2. Установление в настоящей технической спецификации квалификационных требований, предъявляемых к потенциальному поставщику, не допускается.
 3. Установление требований технической спецификации в иных документах не допускается.
- * сведения подтягиваются из плана государственных закупок (отображаются автоматически).