

**Сатып алынатын қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)**

Тапсырыс берушінің атауы:	"Digital Silk Road Company" жауапкершілігі шектеулі серіктестігі
Ұйымдастырушының атауы:	"Digital Silk Road Company" жауапкершілігі шектеулі серіктестігі
Конкурстың №:	№ 17783095-1
Конкурстың атауы:	Ашық конкурс тәсілімен бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулерді электрондық мемлекеттік сатып алуды ұйымдастыру және өткізу туралы
Лоттың нөмірі:	№ 88115788-OK1
Лоттың атауы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	582950.000.000001
Қызметтің атауы:	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	3168750
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	3168750
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	

Қызмет көрсету мерзімі	шарт жасасқан күннен бастап 15 күнтізбелік күн өткеннен кейін 2026 жылғы 31 желтоқсанға дейін
Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Техникалық тапсырма соңғы нүктелердегі қауіптерді анықтау және оларға ден қою жүйесіне (EDR) Сандық талап: 250 дана жұмыс станциясы. Соңғы нүктелерді қорғау шешіміне қойылатын функционалдық талаптар № Функционалдық талаптар Сәйкес келеді Иә / Жоқ Ескертпелер 1 Ұсынылатын шешім келесі клиенттік операциялық жүйелерді қолдауы тиіс: • Android 5 немесе одан жаңа • Apple iOS/iPadOS 9.0 немесе одан жаңа • Arm құрылғыларындағы Windows, S Mode режиміндегі Windows • Windows 8.1 (32-bit, 64-bit), Windows To Go қоса алғанда • Windows 8.1 update for April 2014 (32-bit, 64-bit) • Windows 8.1 update for August 2014 (32-bit, 64-bit) • Windows Embedded 8.1 Pro, Industry Pro және Industry Enterprise (32-bit, 64-bit) • Windows 10 (32-bit, 64-bit) • Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit) • Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit) • Windows 10 Oct 2018 Update (Version 1809) (32-bit, 64-bit) • Windows 10 June 2019 Update (Version 1903) (32-bit, 64-bit) • Windows 10 December 2019 Update (Version 1909) (32-bit, 64-bit) • Windows 10 May 2020 Update (Version 2004) (32-bit, 64-bit) • Windows 10 October 2020 Update (Version 20H2) (32-bit, 64-bit) • Windows 10 May 2021 Update (Version 21H1) (32-bit, 64-bit) • Windows 10 November 2021 Update (Version 21H2) (32-bit, 64-bit) • Windows 11 September 2022 Update (Version 22H2) (64-bit) • Windows 11 October 2023 Update (Version 23H2) (64-bit) • Mac OS X 12.x, 13, 14.x 2 Ұсынылатын шешім келесі виртуалды орталарды қолдауы тиіс: • Microsoft Azure • Amazon Web Services (AWS) EC2 • Amazon Workspaces • Citrix Studio Version 2009.0.0 • Nutanix AOS 5.15 (LTS) • Oracle Cloud Infrastructure (OCI) • VMware WS 5.0, GSX 3.2 немесе одан жаңа, ESX 2.5 немесе одан жаңа • VMware ESXi 5.5 – 6.7 • Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 Hyper-V, 2019 • Citrix XenServer 5.6 немесе одан жаңа • Oracle компаниясының VirtualBox 3 Шешім зиянды бағдарламалық қамтылымды (БҚ), соның ішінде вирустарды, құрттарды, трояндық бағдарламаларды, тыңшылық БҚ-ны, жарнамалық БҚ-ны (Adware) және руткиттерді нақты уақыт режимінде анықтап, бұғаттауы тиіс. 4 Соңғы нүктелерге арналған шешім белгілі қауіптерге арналған сигнатуралардан бөлек мінез-құлықтық талдауды, сондай-ақ осалдықтарға эвристикалық тәсілді қамтуы тиіс. Шешім белгісіз қосымшалардың жағымды және жағымсыз мінез-құлқын бағалап, белгісіз қауіптерден (zero-day) қорғау үшін ережелерге негізделген конфигурацияларды құру қажеттілігінсіз анықтау сапасын арттыруы және жалған іске қосылуларды азайтуы тиіс. 5 Шешімнің желіаралық экраны Ethernet, Token Ring, IPX/SPX, AppleTalk және NetBEUI қоса алғанда, желілік хаттамаларға рұқсат беру немесе оларды бұғаттау мүмкіндігіне ие болуы тиіс. Хаттама драйверлерін (мысалы, VMware, WinPcap) бұғаттау мүмкіндігі, сондай-ақ адаптерлерге тән ережелер (мысалы, Ethernet, Wireless, VPN) болуы тиіс. 6 Ұсынылатын IPS шешімі тапсырыс берушіге қажет болған жағдайда Snort негізіндегі форматта IPS сигнатураларын өңдеуге
--	---

және құруға мүмкіндік беруі тиіс. 7 Шешім Windows Class ID негізінде құрылғыларды, соның ішінде USB, Infrared, Bluetooth, Serial, Parallel, FireWire, SCSI және PCMCIA құрылғыларын бұғаттау мүмкіндігіне ие болуы тиіс. 8 Шешім сондай-ақ құрылғыларды бұғаттау және көрсетілген құрылғылар үшін оқу/жазу/орындау құқықтарын беру мүмкіндігіне ие болуы тиіс. 9 Шешім қосымшаларды талдауды, процестерді бақылауды, файлдар мен тізілімге қолжетімділікті бақылауды, сондай-ақ модульдер мен DLL бақылауын қамтамасыз етуі тиіс. 10 Ұсынылатын шешім келесі желілік триггерлердің AND/OR логикалық шарттарына байланысты икемді және әртүрлі қауіпсіздік саясаттарын қолдануға мүмкіндік беруі тиіс:

- IP-мекенжай (ауқым немесе маска)
- DNS-сервер
- DHCP-сервер
- WINS-сервер
- Шлюз мекенжайы
- TMP-токеннің болуы (аппараттық токен)
- DNS-атау IP-мекенжайға шешіледі
- Policy Manager-ге қосылу
- Желілік қосылым түрі (сымсыз, VPN, Ethernet, dial-up)

11 Ұсынылатын IPS шешімі бір сигнатура үшін NIPS (желілік) және HIPS (хосттық) жүйелерін Generic Exploit Blocking (GEB) технологиясымен біріктіріп, барлық нұсқалардан проактивті қорғауды, қосымшалардың қолжетімділігін түйіршікті бақылауды және жоғарыда аталған мінез-құлықтық технологияны қамтамасыз етуі тиіс. 12 Ұсынылатын Anti-Spyware шешімі руткиттерден жоғары деңгейде қорғау мақсатында дискіні raw-сканерлеуді орындау үшін Windows файлдық жүйесін айналып өту және NTFS томына тікелей қол жеткізу мүмкіндігіне ие болуы тиіс. 13 System Lock Down — шешім жүйедегі әрбір орындалатын файлдың іздерін (fingerprint) жасау арқылы жүйені «бұғаттау» мүмкіндігіне ие болуы тиіс. Одан кейін ол барлық іске қосылған қосымшаларды бақылап, агентте сәйкес ізі жоқ кез келген қосымшаның жұмысын тоқтата алады. 14 DoS-шабуылдарды анықтау және олардан қорғау — жүйенің қолжетімділігін және/немесе тұрақтылығын бұзуға бағытталған аномальды желілік мінез-құлықтың әртүрлі нысандарынан жүйені қорғауы тиіс. 15 Анти-спуфинг — өзінің IP немесе MAC-мекенжайын жалғандаған хакердің жүйесіне деректердің жіберілуінен деректер берілісін қорғауы тиіс. 16 Агент процестердің орындалу тізбектерін анықтау және бұғаттау мүмкіндігіне ие болуы тиіс. Ол зиянды қосымша сенімді қосымшаны іске қосып, содан кейін желіге қол жеткізу үшін осы қосымшаның сенім артықшылықтарын пайдалануға әрекеттенген жағдайды анықтауы тиіс. 17 Қосымшаларды басып алудан қорғау (Anti-application hijacking) — хакерлер мен веб-сайттардың жекелеген компьютерлердің операциялық жүйесі мен браузерін сәйкестендіруіне жол бермеуі тиіс. 18 Кодты енгізу шабуылдарының алдын алу — зиянды қосымшалардың қосымшалардың шығыс желіаралық экранын айналып өту үшін сенімді қосымшаларға код енгізуіне жол бермеу. 19 Хаттама адаптері арқылы жасалатын шабуылдардың алдын алу — зиянды қосымшалардың шығыс желіаралық экранды айналып өту үшін өзінің хаттама адаптерін пайдалануына жол бермеу. 20 Ұсынылатын антивирустық шешім Virus Bulletin 100 марапатынан бірде-бір рет құр қалмауы және оны қатарынан 41 реттен

	астам алуы тиіс. 21 Ұсынылатын дербес желіаралық экран шешімі Gartner Magic Quadrant квадрантының жоғарғы бөлігінде орналасуы тиіс. 22 Antivirus және Antispyware саясаттарында өндірістік желіде қолдану кезінде дұрыс теңгерімді қамтамасыз ету үшін әдепкі бойынша «Жоғары қауіпсіздік» және «Жоғары өнімділік» таңдау опциялары болуы тиіс. 23 Жоспарланған антивирустық сканерлеулер ноутбуктар батареядан жұмыс істеген кезде кейінге қалдырылуы/қайта жоспарлануы тиіс. 24 Антивирусте zero-day қауіптерінен қорғау үшін трояндарды, құрттарды және кейлоггерлерді анықтауға арналған мінез-құлықтық сканерлеу технологиясы болуы тиіс. Сезімталдық деңгейі сканерлеу жиілігін баптау мүмкіндігімен реттелуі тиіс. 25 Антивирустық шешімде интернет-браузерді қорғау функциясы болуы тиіс, ал қауіпсіздік тәуекелінің деңгейі өзгерген кезде бастапқы бет реттелетін болуы тиіс. 26 Ұсынылатын шешімде электрондық поштаға арналған плагин болуы тиіс, ол тіркемелерді, соның ішінде zip-файлдарды сканерлеп, зиянды БҚ-ны пошта жәшігіне түскенге дейін жоюы тиіс, сондай-ақ Microsoft Outlook, Lotus Notes және Outlook Express клиенттерін қоса алғанда, электрондық поштаның POP3-трафигін сканерлей алуы тиіс. 27 Desktop Firewall ережелері Ethernet, wireless, Dial-up, VPN (Microsoft PPTP, Nortel, Cisco) қоса алғанда, адаптерлерге байланысты бапталуы тиіс. 28 Desktop Firewall ережелері экран сақтағышының күйіне («Қосулы» және «Өшірулі») байланысты бапталуы тиіс. 29 Desktop Firewall саясаттары уақыт пен апта күніне байланысты бапталуы тиіс. 30 Өнімде дайын саясаттар болуы тиіс, соның ішінде: барлық алмалы-салмалы дискілерді тек оқу режиміне ауыстыру, алмалы-салмалы дискілерден бағдарламаларды іске қосуды бұғаттау, клиенттердің файлдары мен тізілім кілттерін қорғау, USB-дискілерге жазылған файлдарды журналға тіркеу, hosts файлына өзгерістер енгізуді бұғаттау. 31 Басқару серверінде қажет болған жағдайда әртүрлі орналасқан жерлер үшін әртүрлі әкімшілерді тағайындай отырып, бірнеше домен қосу мүмкіндігі болуы тиіс. Әрбір домен бір ғана басқару серверін және дерекқорды пайдалануы тиіс. Мұндай бөліну бір доменнің деректерін басқа доменнің әкімшілері көруіне жол бермейді. Әкімшілер басқа домендердің мазмұнын емес, тек өз доменінің мазмұнын көре және басқара алады. 32 Желінің өткізу қабілетін үнемдеу үшін клиенттерде басқару серверіне жүктелетін журнал жазбаларының ең көп санын баптау мүмкіндігі болуы тиіс. 33 Өнімде бастапқы DHCP- және NetBIOS-трафикті қоспағанда, желіаралық экран іске қосылғанға дейін және ол тоқтатылғаннан кейін барлық трафикті бұғаттауға арналған қауіпсіздік параметрі болуы тиіс. 34 Ұсынылатын антивирустық шешім файлдарды бүкіл әлем бойынша осы файлды пайдаланатын пайдаланушылар саны бойынша анықтау мүмкіндігіне ие болуы тиіс. 35 Браузерге басып кірудің алдын алу: антивирус браузерлер арқылы жүзеге асырылатын зиянды жүктеулерді бұғаттай алуы тиіс. 36 Ұсынылатын антивирустық шешім файлдарды цифрлық қолтаңба, файлдың жасы, таралу деңгейі және осыған ұқсас
--	--

	атрибулттар негізінде саралауы тиіс. 37 Антивирус клиентінде антивирус консоліне қосылған кезде көрінетін индикатор болуы тиіс. 38 Антивирус консолінде жалпыға қолжетімді желідегі вирустардың күйін көрсететін қауіптер индикаторы (threat cone) болуы тиіс. 39 Ұсынылатын шешімде соңғы нүкте агентінің құрамында deception (алдау) функциясы болуы тиіс. 40 Ұсынылатын шешімде сол агенттің құрамында жад эксплойттарынан қорғау (Memory exploit mitigation) болуы тиіс. 41 Ұсынылатын шешімде сол агентті пайдалана отырып EDR функциясы болуы тиіс. 42 Ұсынылатын шешімде бірыңғай агент құрамында endpoint deception болуы тиіс. 43 Ұсынылатын шешімде талаптарға сәйкес келмейтін немесе ескірген соңғы нүктелерді анықтайтын және түзететін Host Integrity функциясы болуы тиіс. 44 Ұсынылатын шешімде файлдарды талдау және мінез-құлықтық талдау кезінде тиімді озық машиналық оқыту болуы тиіс. 45 Ұсынылатын шешімде ішкі немесе шығыс желілік шабуылдарды, коммуникацияларды және браузер мен желі деңгейіндегі қауіптерді олар дискіге түсіп, орындалғанға дейін бұғаттауға және анықтауға қабілетті Host IPS болуы тиіс. 46 Соңғы нүкте агенті араласудан немесе ажыратудан қорғалуы тиіс. 47 Ұсынылатын шешімде опция ретінде бұлттық басқару консолі болуы тиіс. Соңғы нүктелердегі қауіптерді анықтау және оларға ден қою (Endpoint Detection and Response) 48 Endpoint Detection and Response жасанды интеллект негізіндегі аналитиканы, тергеу playbook-тарын және теңдесі жоқ қауіптер туралы барлау деректерін пайдалана отырып, барлық соңғы нүктелердегі басып кірулерді анықтауы, іздеуі, оқшаулауы және жоюы тиіс, сондай-ақ бірыңғай агент түрінде Endpoint Protection-мен интеграцияланған болуы тиіс. EDR келесі мүмкіндіктерге ие болуы тиіс: Анықтау және айқындау — бұзушылықты анықтау уақытын қысқарту және оның ауқымын жедел анықтау • Күдікті әрекетті айқындау, инциденттерді анықтау және басымдықтарын белгілеу үшін машиналық оқыту мен мінез-құлықтық аналитиканы қолдану • Күдікті скриптер мен жад эксплойттары бойынша инциденттерді автоматты түрде айқындау және құру • Процестер жадын талдау арқылы жадқа негізделген шабуылдарды айқындау Тергеу және шектеу — инциденттерге ден қою жөніндегі мамандардың өнімділігін арттыру және қауіптерді шектеуді қамтамасыз ету • Соңғы нүкте әрекетін үздіксіз жазу арқылы инцидентті толық қайта жаңғыртуды қамтамасыз ету, соңғы нүктенің нақты процестерін қарау • Нақты уақыт режимінде барлық соңғы нүктелер бойынша компрометация индикаторларын іздеу арқылы қауіптерді аулау • Тергеу барысында соңғы нүктені карантинге қою арқылы ықтимал компрометацияланған соңғы нүктелерді шектеу Жою — соңғы нүктелерді жедел қалпына келтіру және қауіптің қайталануына жол бермеу • Зардап шеккен барлық соңғы нүктелерде зиянды файлдар мен оларға байланысты артефактілерді жою • Соңғы нүктедегі файлдардың қара және ақ тізімдері • Кеңейтілген есептілік инциденттерді жою жөніндегі есептер үшін кез келген кестені экспорттауға мүмкіндік береді Интеграция және автоматтандыру —
--	---

	зерттеушілер үшін көріністерді біріздендіру, деректер мен жұмыс процестерін оркестрлеу • Инциденттер туралы деректер мен әрекеттерді Splunk және ServiceNow қоса алғанда, қолданыстағы SOC инфрақұрылымына оңай интеграциялау • Инциденттер playbook-тарының автоматтандырылған ережелері арқылы тәжірибелі зерттеушілердің үздік тәжірибелері мен талдауын қайталау • Артефактілерді автоматтандырылған жинау арқылы соңғы нүкте әрекетін терең көру мүмкіндігіне ие болу 49 Әлеуетті өнім беруші платформа құрамында анықтауға, валидациялауға және карантинге қоюға мүмкіндік беретін соңғы нүктелерге арналған шешімге ие болуы тиіс. Барлық функционал корпоративтік желіге VPN-қосылымды талап етпей, корпоративтік желі ішінде де, одан тыс жерде де жұмыс істеуі тиіс. 50 Ұсынылатын платформа өз шешімі шеңберінде анықтау мен қорғаудың бірнеше технологиясын қолдауы және zero-day пен белгісіз қауіптерді анықтау үшін файлды детонациялау кезінде қосымша payload-сыз, файлдың зияндылығын анықтау үшін белгілі файлдар мен олардың мінез-құлқының дерекқорын пайдаланатын сигнатуралық қозғалтқышты қамтуы тиіс. 51 Шешімде карантинге қою мен жоюдың екі кезеңді процесі болуы тиіс. 52 Шешім соңғы нүкте агенті жаңартуларының жаңа нұсқаларын тарату мүмкіндігіне ие болуы тиіс. 53 Соңғы нүкте агенттері анықтау, triage және карантинге қою мақсатында корпоративтік желі ішінде де, одан тыс жерде де басқарылуы тиіс. 54 Endpoint Detection and Response шешімі виртуалды орындауды жүзеге асыратын басқа қауіпсіздік құрылғыларынан zero-day қауіптері туралы ақпарат алу мүмкіндігіне ие болуы тиіс. 55 Endpoint Detection and Response шешімі пайдаланушылық компрометация индикаторларын (IOC) қабылдауы тиіс. 56 Соңғы нүкте агенті соңғы нүктеде бар Adware, вирустар және бағдарламалық қамтылым осалдықтары сияқты қауіптерден қорғау мүмкіндігіне ие болуы тиіс. 57 Анықталған зиянды БҚ-ға толық криминалистикалық талдау жүргізу және кәсіпорын қызметкерлеріне келесі ақпаратты ұсыну мүмкіндігі: • Хосттағы өзгерістер туралы толық есеп (Comprehensive Host Modification Report) • Зиянды БҚ-ның бинарлық файлдарының көшірмесі • Зиянды БҚ байланысуға әрекеттенетін барлық орындарды көрсететін толық URL тізбектері • Кәсіпорындағы зиянды БҚ оқиғалары туралы түрі, хосты және әрекеті бойынша бөлінген жиынтық есептер • Зиянды БҚ-ның бұрын БЕЛГІЛІ немесе БЕЛГІСІЗ қауіп екендігін жедел талдау • Басқа қорғау құралдары осы қауіпке қарсы қаншалықты тиімді болатынын көрсететін қауіптілік деңгейі туралы ақпарат 58 Ұсынылатын шешім қосымша агенттерді орналастыру/интеграциялау қажеттілігінсіз барлық соңғы нүкте клиенттерінде зиянды файлды бұғаттау/қара тізімге қосу үшін қажетті ережелерді/саясаттарды динамикалық түрде жасауы тиіс. 59 Шешім зиянды деп танылған файлдарды басқа желілік орынға автоматты түрде карантинге орналастыру мүмкіндігіне ие болуы тиіс. 60 Шешім соңғы нүктелерге арналған шешімге файл хеші сияқты компрометация индикаторларын (IOC) беру мүмкіндігіне ие болуы тиіс, осылайша ол ұқсас файлдардың ағымдағы
--	--

	және болашақ анықталуларын бұғаттай алады. 61 Шешім ядро деңгейіндегі руткиттерді (Kernel level rootkits) анықтай алуы тиіс. 62 Шешім reflective DLL injection-ды өңдей алуы тиіс. 63 Шешім зиянды файлды әртүрлі атаулармен берілген жағдайда да әртүрлі соңғы нүктелерде сәйкестендіре алуы тиіс. 64 Шешім барлық соңғы нүктелердегі күдікті немесе зиянды файлдардың бірыңғай көрінісін ұсынуы тиіс. 65 Шешім жою және тергеу процестеріне көмектесу үшін бүкіл әлем бойынша жиналған барлау ақпараты негізінде файлдардың беделін ұсынуы тиіс. 66 Шешім әкімшіге файлдарды зиянды БҚ-ның динамикалық талдауына жіберу мүмкіндігін беруі тиіс. 67 Шешім соңғы нүктелерде файлдарды ақ немесе қара тізімге қосу мүмкіндігін беруі тиіс. 68 Соңғы нүкте агенті EDR серверлерінде файлдардың беделін тексеруді қолдауы тиіс. 69 Соңғы нүкте агенті қауіптерді бұғаттауды, жоюды және карантинге қоюды қолдауы тиіс. 70 Соңғы нүкте агенті жүйенің өнімділігіне әсер етпеуі тиіс. 71 Соңғы нүкте агенті соңғы нүктелерге бағытталған желілік қауіптерден қорғау үшін host-based intrusion prevention мүмкіндіктерін ұсынуы тиіс. 72 Соңғы нүкте агенті соңғы нүктелер үшін browser-based intrusion prevention мүмкіндіктерін ұсынуы тиіс. 73 Соңғы нүктелерге арналған шешім барлық соңғы нүктелерден файлдар, тізілім кілттері, сондай-ақ домендер мен URL бойынша компрометация индикаторларын (IOC) орта бойынша терең іздеуді қолдауы тиіс. 74 Соңғы нүктелерге арналған шешім бірыңғай басқару панелінен зиянды файлдарды қара тізімге қосу және жою мүмкіндігіне ие болуы тиіс. 75 Шешім одан әрі жұқтырудың алдын алу үшін бірыңғай басқару панелінен соңғы нүктелерді карантинге қою мүмкіндігіне ие болуы тиіс. 76 Соңғы нүктелерге арналған шешім қауіптер мен зиянды БҚ туралы ақпаратты қолданыстағы антивирустық шешіммен салыстыруы (корреляциялауы) және антивирустық шешімнің қорғау күйі негізінде EDR инциденттерінің басымдығын арттыруы немесе төмендетуі тиіс. 77 Ұсынылатын АРТ шешімі сондай-ақ соңғы нүктедегі қауіптерді анықтауға, валидациялауға, шектеуге және жоюға мүмкіндік беретін, платформа құрамындағы соңғы нүктелердің қолданыстағы қорғанысын қолдауы тиіс. 78 Соңғы нүкте агенті соңғы нүктелерді қорғау құралымен интеграциялануы және соңғы нүктеге қандай да бір жаңа агентті орнатуды талап етпеуі тиіс. 79 Соңғы нүктелерге арналған EDR шешімі соңғы нүктелердің қолданыстағы қорғанысын немесе өзінің меншікті құралдарын пайдалана отырып, соңғы нүктедегі қауіптерді жою мүмкіндігіне ие болуы тиіс. 80 Соңғы нүктелерге арналған EDR шешімі белгісіз зиянды БҚ-ны анықтап, оны желілік EDR шешіміне тәуелсіз түрде соңғы нүктелерден виртуалды орындауға жібере алуы тиіс. 82 Соңғы нүктелерге арналған EDR шешімі пайдаланушы корпоративтік желі ішінде немесе одан тыс жерде болған кезде, корпоративтік желіге VPN-қосылымды талап етпей, соңғы нүктелердегі қауіптерді анықтай, валидациялай, шектей және жою алуы тиіс. 83 Ұсынылатын шешім соңғы нүктелерді шектеуді қолдауы тиіс, ал шектеу операциялары рөлдік
--	---

	әкімшілерді қолдауы тиіс. 84 Соңғы нүктелерге арналған EDR шешімі желіде виртуалды орындауды талдауды жүзеге асыратын құрылғылардан IOC және қауіптер туралы барлау деректерін динамикалық түрде қабылдауы тиіс (мысалы, желілік және email EDR шешімімен интеграция). 85 Ұсынылатын шешім ауқымды түрде тікелей клиенттерде IoC және Threat Hunt сұрауларын қолдауы тиіс. 86 Соңғы нүктелерге арналған EDR шешімі SIEM-мен интеграциялануы тиіс. 87 Соңғы нүктелерге арналған EDR шешімі жүйеге жазылған, бірақ әлі орындалмаған файлдардың бар-жоғын анықтай алуы тиіс. 88 Соңғы нүктелерге арналған EDR шешімі жүйеге түсетін жүктемеге қарамастан, пайдаланушылардың қалыпты жұмысына және соңғы нүктедегі бизнес-операцияларға кедергі келтірмеуі тиіс. 89 Соңғы нүктелерге арналған EDR шешімі мемлекет демеушілік ететін мақсатты шабуылдардағы жоғары дамыған қауіп топтарына байланысты индикаторларды қоса алғанда, қауіптер туралы барлау деректерін тұрақты түрде жаңартып отыруы тиіс. 90 Соңғы нүктелерге арналған EDR шешімінің жаңартулары БҚ-ны орналастырудың стандартты корпоративтік тетіктерімен, сондай-ақ шешімнің өзі ішінде соңғы нүктелерді жаңарту мүмкіндігімен қолдау көрсетілуі тиіс. 91 Шешімді жеткізуші ықтимал жалған іске қосылулардың алдын алу үшін шешімнен бір батырманы басу арқылы күдікті үлгіні талдауға жіберуге мүмкіндік беруі тиіс. 92 Шешім виртуализацияны тани алатын жаңа буын қауіптерін анықтау үшін bare-metal және виртуалды орындау құмсалғышын (sandbox) қолдауы тиіс. 93 Шешімді енгізу қандай да бір жаңа агент қоспауы және соңғы нүкте машинасындағы соңғы нүктелерді қорғаудың бір бөлігі болуы тиіс. 94 Ұсынылатын шешім flight data recorder (ұшу деректерін тіркеуіш) функциясын қолдауы тиіс. Қосымшаларды бақылау (Application Control) 95 Ұсынылатын шешім ортадағы барлық соңғы нүктелерден жиналған барлық қосымшалар мен файлдарды сканерлеу және түгендеу үшін қосымшаларды кешенді анықтауды және түгендеуді қамтамасыз етуі, сондай-ақ әрбір қосымша мен файл туралы, соның ішінде атауы, тәуекелді бағалау, осалдықты бағалау, шығарушысы, беделі, ол анықталған құрылғылар саны және т.б. туралы толық ақпарат ұсынуы тиіс. 96 Ұсынылатын шешім қосымшаларды бақылаудың кешенді саясатын және анықталғандардың ішінен кез келген қосымшаны ақ немесе қара тізімге қосу үшін Logical View көмегімен саясаттарды оңай құруды қамтамасыз етуі тиіс. 97 Endpoint App Control қосымшалардың әртүрлі атрибуттары негізінде қосымшаларға сенімді қамтамасыз етеді, статикалық (мысалы, хеш, жол, шығарушы және сертификат) және динамикалық (мысалы, тәуекелді бағалау және бедел) атрибуттардың біреуі немесе кез келген санының комбинациясы негізінде қосымшаларға рұқсат береді немесе оларды бұғаттайды. 98 App Control саясаты қосымша атауын, жолын, хешін, беделін, шығарушысын, пайдаланушыны, пайдаланушылар тобын және пәрмен жолы параметрлерін қоса алғанда, параметрлердің кең ауқымы бойынша ережелер құруға мүмкіндік беруі тиіс. 99 App Control саясатында «тек мониторинг» режимінде қолдану
--	--

	опциясы болуы тиіс. 100 Ұсынылатын шешім ортада рұқсат етілген қосымшалар мен ортада нақты іске қосылатын қосымшалар арасындағы айырмашылықты талдауы тиіс. 101 Ұсынылатын шешім соңғы нүктелерде БҚ-ны орнатуға немесе жаңартуға құқығы бар сенімді жаңартушыларды (trusted updaters) анықтауға мүмкіндік беруі тиіс, олар анықталған қосымшалар немесе жаңа қосымшалар, шығарушы, каталог, файлдар, пайдаланушылар және пайдаланушылар топтары болуы мүмкін. 102 Ұсынылатын шешім сенімді қосымшалардың осалдықтарын пайдаланудың және жүйелердің сенімсіз қосымшалармен жұқтырылуының алдын алуы тиіс. Қосымшалардың мінез-құлқын оқшаулау (Application Behavior Isolation) 103 Ұсынылатын шешімде құрылғыларды қорғау үшін қосымшалардың мінез-құлқын оқшаулау ережелерінің мүмкіндіктері болуы тиіс. Бұл ережелер оқшаулаудың келесі түрлері бойынша қосымшалардың белгілі бір мінез-құлқына рұқсат береді немесе оны бұғаттайды: • Браузерді оқшаулау (Google Chrome, Firefox, Internet Explorer, Microsoft Edge) • Office оқшаулау • PDF Renderer оқшаулау • Платформаны оқшаулау саясаты, ол мыналарды қамтиды: о ОЖ параметрлері о Jail жалпы параметрлері (жоғары, орташа және төмен оқшаулау) Оқшаулау мыналарды қорғауға арналған ережелерді ұсынады: • Тізілімді қорғау • Файлдарды қорғау • Процестердің өзара әрекеттесуін қорғау • Процестердің орындалуын қорғау • Желілік қолжетімділікті қорғау • Жүйелік шақыруларды қорғау 104 Ұсынылатын шешім қарқындылық деңгейлері негізінде біздің желідегі кез келген күдікті файлдарды анықтауы және анықталған файлдарды ақ немесе қара тізімге қосуға, сондай-ақ Platform Isolation саясаты арқылы күдікті қосымшаны оқшаулауға мүмкіндік беруі тиіс. 105 Ұсынылатын шешім тәуекелді бағалау негізінде портативті қосымшаларды анықтау, түгендеу және оқшаулау мүмкіндігіне ие болуы тиіс. Deception (Алдау / Жалған нысандар) 105 Ұсынылатын шешімде бүкіл орта бойынша «жалған нысандардың» — жалған файлдардың, есептік деректердің, желілік ресурстардың, кэш жазбаларының және соңғы нүктелердің — кең ауқымын орналастыратын deception функциясы болуы тиіс. 106 Ұсынылатын шешімде бірыңғай агент құрамында endpoint deception болуы тиіс. 107 Ұсынылатын шешім қосымшалардың зиянды мінез-құлқын бақылау және ол туралы хабарлау үшін deception техникаларын пайдалануы тиіс. Мобильді құрылғыларға арналған соңғы нүктелерді қорғау (Endpoint Protection for Mobile) 108 Ұсынылатын шешім iOS және Android құрылғыларын қолдауы тиіс. 109 Ұсынылатын шешім iOS және Android басқаруындағы мобильді құрылғыларға жасалатын шабуылдардың алдын алуы тиіс. 110 Ұсынылатын шешім мобильді құрылғыларды Интернетке қосылған кезде де, қосылмаған кезде де зиянды БҚ-дан, желілік қауіптерден және қосымшалар/ОЖ осалдықтарының эксплойттарынан проактивті түрде қорғауы тиіс. 111 Ұсынылатын шешім құрылғылар Интернеттен ажыратылған кезде де неғұрлым жылдам ден қоюды және тұрақты қорғауды қамтамасыз етуі тиіс. 112 Ұсынылатын шешім қауіп анықталған кезде шабуылдарды дереу және автоматты түрде проактивті
--	---

	түрде тойтаруы тиіс. 113 Ұсынылатын шешім басқа ресурстар мен процестерге әсер етпей, тікелей қауіпке нақты әсер етуі және сұрау бойынша іске қосылуы тиіс. 114 Ұсынылатын шешімде тәуекелді қосымшалар тудыратын қауіптерден қорғау әрекеттері болуы тиіс, олар мыналармен шектелмей, мыналарды қамтиды: коммуникацияны бұғаттау, орнатудың алдын алу, зиянды басқару және командалық серверлермен (C&C) коммуникацияны бұғаттау және сезімтал ресурстарға қолжетімділікті бұғаттау. 115 Ұсынылатын шешімде желілік қауіптерден қорғау әрекеттері болуы тиіс, олар мыналармен шектелмей, мыналарды қамтиды: желілік қауіп анықталған кезде VPN-туннельді автоматты түрде іске қосу, сезімтал корпоративтік ресурстарға қолжетімділікті бұғаттау және жалған корпоративтік Wi-Fi қолжетімділік нүктелеріне қолжетімділікті бұғаттау. 116 Ұсынылатын шешімде контенттік қауіптерден қорғау әрекеттері болуы тиіс, олар мыналармен шектелмей, мыналарды қамтиды: барлық трафикті қауіпсіз веб-шлюз арқылы туннельдеу, қалаусыз контентке қолжетімділікті бұғаттау және SMS-фишингтік хабарламаларды бұғаттау. 117 Ұсынылатын шешімде зиянды VPN-дерді автоматты түрде ажыратуға арналған қорғау әрекеті болуы тиіс. 118 Ұсынылатын шешімде always-on немесе on-demand режимінде іске асырылатын VPN-технология болуы тиіс. 119 Ұсынылатын шешімдегі VPN-технология екі тәсілмен жұмыс істеу мүмкіндігіне ие болуы тиіс: 1. Трафик құрылғы мен желі арасында қауіпсіз өтетін шифрланған туннель ретінде. 2. Іріктемелі трафик бұғаттағышы ретінде (VPN арқылы өтетін белгілі бір трафик тасталады және құрылғыдан ешқашан шықпайды). Осы іске асырулардың әрқайсысы always-on немесе on-demand болуы мүмкін. 120 Ұсынылатын шешімде мобильді қауіптердің барлық векторлары бойынша белгілі және zero-day шабуылдарынан көпдеңгейлі мобильді қорғаныс болуы тиіс. 121 Ұсынылатын шешім күдікті желілерден, қосымшалардан және мінез-құлықтан олар зиян келтіргенге дейін қорғауды қамтамасыз етуі тиіс. 122 Ұсынылатын шешім пайдаланушының мобильді тәжірибесіне немесе батареяның жұмыс уақытына теріс әсер етпей, құпиялылық пен өнімділікті қорғауы тиіс. 123 Ұсынылатын шешімде IT-саясаттарды автоматтандырылған түрде қолдану және барлық негізгі қолданыстағы корпоративтік EMM/MDM, SIEM, пошта серверлерімен және VPN-мен кіріктірілген интеграциялар болуы тиіс. 124 Ұсынылатын шешімде көптеген қауіпсіздік шешімдерімен интеграциялау мүмкіндіктері болуы тиіс, олар мыналармен шектелмей, мыналарды қамтиды: WSS, CASB, DLP және Endpoint protection. 125 Ұсынылатын шешім орналастыруда, енгізуде, қызмет көрсетуде және жаңартуда қарапайым болуы тиіс. 126 Ұсынылатын шешім өнімділікке, пайдаланушы тәжірибесіне, құпиялылыққа нөлдік әсер етуі және күдікті қосымшаларды терең талдауды қамтамасыз етуі тиіс. 127 Ұсынылатын шешім кез келген күдікті қосымшалар мен желілерден туындайтын зиянды БҚ-ның әртүрлі белгілі, белгісіз және мақсатты шабуылдарына нақты уақыт режимінде ден қоюды және қорғауды қамтамасыз етуі тиіс. 128 Ұсынылатын шешімде шабуыл кезінде
--	---

	корпоративтік активтерді автоматтандырылған түрде қорғау болуы тиіс. 129 Ұсынылатын шешімде қосымшалар, желілер және ОЖ үшін машиналық оқытуды пайдалана отырып беделді тексеру мүмкіндігі болуы тиіс. 130 Ұсынылатын шешімде кез келген SIEM шешімімен интеграциялауға арналған әрекеттердің кешенді журналдары болуы тиіс. 131 Ұсынылатын шешімде сигнатуралар, статикалық/динамикалық талдау, мінез-құлық, құрылым, рұқсаттар, дереккөз және т.б. негізінде қосымшаларды талдау мүмкіндігі болуы тиіс. 132 Ұсынылатын шешімде зиянды iOS профильдерін анықтау, бұғаттау және жою функциясы болуы тиіс. 133 Ұсынылатын шешімде құпиялылықты бұзбай Man-in-the-Middle шабуылдарын, SSL деңгейін төмендетуді және контентпен манипуляцияларды анықтау мүмкіндігі болуы тиіс. 134 Ұсынылатын шешімде құрылғыларды түзетілмеген белгілі осалдықтардың болуына бақылау және қосымшалар мен операциялық жүйелердегі zero-day осалдықтарын анықтау мүмкіндігі болуы тиіс. 135 Ұсынылатын шешім үшінші тарап шешімдеріне тәуелді болмай, заманауи операциялық жүйелер үшін мобильді қауіптерден қорғауды қамтамасыз етуі тиіс. Active Directory 136 Ұсынылатын шешім бұзушылықтарды дербес шектеуді, инциденттерге ден қоюды және домен қауіпсіздігін бағалауды қамтамасыз ету үшін соңғы нүктеден Active Directory-ді тиімді қорғау арқылы жасырын шабуылдарға немесе APT-ге қарсы тұруы тиіс. 137 Ұсынылатын шешім ұйымның Active Directory құрылымын толық көлемде (серверлер, соңғы нүктелер, қосымшалар, пайдаланушылар, филиалдар, атау беру келісімдері, конфигурациялар, атрибуттар және т.б.) дербес зерделеуі тиіс. 138 Ұсынылатын шешім шынайы және шектеусіз обфускация жасай алуы тиіс. 139 Ұсынылатын шешім Active Directory процестерін, контекстін және әрекетін runtime-бағалауды орындай алуы тиіс. 140 Ұсынылатын шешімде жоғары дәлдіктегі хабарламалар және шабуылды автоматты түрде бұғаттау мүмкіндігі болуы тиіс. 141 Ұсынылатын шешім шабуылдаушы орындаған барлау, есептік деректерді ұрлау және көлденең жылжудың нақты кезеңдерін тіркейтін және шабуылдар тізбегін құжаттайтын нақты уақыттағы криминалистикалық есептілікті ұсынуы тиіс. 142 Ұсынылатын шешім бұзушылықты нақты уақыт режимінде шектеу үшін соңғы нүктедегі зиянды процесті автоматты түрде тоқтата алуы және оны басқа процесті тудыру, жадтың басқа бөлігін қайта жазу, барлау пәрмендерін орындау немесе желімен байланысу мүмкіндігінен айыруы тиіс. 143 Ұсынылатын шешімде доменді дұрыс емес конфигурациялар, осалдықтар және persistence тұрғысынан үздіксіз тексеру, доменді шабуылдаушы тұрғысынан көрсету және тәуекелдерді дереу төмендетуге мүмкіндік беру мүмкіндігі болуы тиіс. 144 Ұсынылатын шешім AD қорғанысы және ML негізіндегі deception технологиясы арқылы көлденең жылжудың алдын алуы тиіс. 145 Ұсынылатын шешімде домен конфигурациясы, артықшылықты есептік жазбалар, қауіпсіздік параметрлері, GPO, соңғы нүктелер, домен контроллері және Kerberos туралы толық ақпарат жинау үшін шабуылдарды симуляциялауды пайдаланатын автоматтандырылған бағалау процесі
--	---

	болуы тиіс. 146 Ұсынылатын шешім AD-дегі және бүкіл домендік ортадағы дұрыс емес конфигурациялар мен бэкдорлардың болуы тұрғысынан доменнің және Active Directory құрылымының әрбір құрамдас бөлігін дербес талдауы тиіс. Басқару және есептілік (Management and Reporting) 153 Шешім бірыңғай агент пакеті және жаңарту тетігі құрамында орналастырылуы, әкімшіленуі және жаңартылуы тиіс. Өнімнің барлық талап етілетін функционалына қол жеткізу үшін агентті бірнеше рет орналастыру және жаңартуларды алу қажеттілігі болмауы тиіс. 154 Ұсынылатын шешімде Cloud, On-Prem және Hybrid нұсқаларында орналастыру мүмкіндігі болуы тиіс. 155 Басқарылмайтын соңғы нүктелерді тауып, толық қорғау үшін бірыңғай жеңіл агентті орналастыру. 156 Қауіпсіздік пен сәйкестікті тексерулер бірыңғай әкімшілендіру сервері мен консоль арқылы басқарылуы тиіс. 157 Шешім қажет болған жағдайда пайдаланушының есептік деректері бойынша аутентификацияға қосымша ретінде басқару консолінің аутентификациясы үшін RSA-мен интеграцияны қамтамасыз етуі, сондай-ақ LDAP, Syslog және Active Directory-мен интеграциялануы тиіс. 158 Өртүрлі орындарда орнатылған басқару серверлері саясаттар мен журналдарды репликациялайтын Multi-Server архитектурасында белгіленген аралықтар арқылы деректерді, журналдарды және контентті репликациялау мүмкіндігіне ие болуы тиіс. 159 Пайдаланушылар агентті жоя алмауы үшін агентте жоюдан құпиясөзбен қорғау, қызметті ажыратуға арналған құпиясөз және клиенттің GUI-ін ашуға арналған құпиясөз мүмкіндігі болуы тиіс. 160 Агент әкімші жүйеге кірген жағдайда да қызметті тоқтатудан қорғау мүмкіндігіне ие болуы тиіс. 161 Жаңарту тетігі клиенттер контентін басқару серверінен, ішкі жаңарту серверлерінен, вендордың сыртқы жаңарту серверлерінен, сондай-ақ басқару сервері мен топтағы клиенттер арасында прокси рөлін атқаратын клиенттен және Microsoft SMS сияқты үшінші тарап құралдарын пайдалана отырып жаңартуды қамтуы тиіс. 162 Ұсынылатын антивирустық шешімде физикалық және виртуалды клиенттер үшін бірыңғай және бір ғана агент болуы тиіс.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	

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

Наименование заказчика	Товарищество с ограниченной ответственностью "Digital Silk Road Company"
Наименование организатора	Товарищество с ограниченной ответственностью "Digital Silk Road Company"
№ конкурса:	№ 17783095-1
Наименование конкурса:	Об организации и проведении электронных государственных закупок услуг по предоставлению лицензий на право использования программного обеспечения способом открытого конкурса
Номер лота:	№ 88115788-OK1
Наименование лота:	Услуги по предоставлению лицензий на право использования программного обеспечения
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	582950.000.000001
Наименование услуги:	Услуги по предоставлению лицензий на право использования программного обеспечения
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	3168750
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	3168750
Срок оказания услуги:	по истечении 15 календарных дней с даты заключения договора по 31 декабря 2026 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Техническое задание для системы обнаружения и реагирования на конечных точках (EDR) Количественное требование: 250 шт рабочих станций. Функциональные требования к решению защиты конечных точек № Функциональные требования Соответствует Да / Нет Комментарии 1 Предлагаемое решение должно поддерживать следующие клиентские операционные системы: • Android 5 или новее • Apple iOS/iPadOS 9.0 или новее • Windows на устройствах Arm, Windows в режиме S Mode • Windows 8.1 (32-bit, 64-bit), включая Windows To Go • Windows 8.1 update for April 2014 (32-bit, 64-bit) • Windows 8.1 update for August 2014 (32-bit, 64-bit) • Windows Embedded 8.1 Pro, Industry Pro и Industry Enterprise (32-bit, 64-bit) • Windows 10 (32-bit, 64-bit) • Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit) • Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit) • Windows 10 Oct 2018 Update (Version 1809) (32-bit, 64-bit) • Windows 10 June 2019 Update (Version 1903) (32-bit, 64-bit) • Windows 10 December 2019 Update (Version 1909) (32-bit, 64-bit) • Windows 10 May 2020 Update (Version 2004) (32-bit, 64-bit) • Windows 10 October 2020 Update (Version 20H2) (32-bit, 64-bit) • Windows 10 May 2021 Update (Version 21H1) (32-bit, 64-bit) • Windows 10 November 2021 Update (Version 21H2) (32-bit, 64-bit) • Windows 11 September 2022 Update (Version 22H2) (64-bit) • Windows 11 October 2023 Update (Version 23H2) (64-bit) • Mac OS X 12.x, 13, 14.x 2 Предлагаемое решение должно поддерживать следующие виртуальные среды: • Microsoft Azure • Amazon Web Services (AWS) EC2 • Amazon Workspaces • Citrix Studio Version 2009.0.0 • Nutanix AOS 5.15 (LTS) • Oracle Cloud Infrastructure (OCI) • VMware WS 5.0, GSX 3.2 или новее, ESX 2.5 или новее • VMware ESXi 5.5 – 6.7 • Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 Hyper-V, 2019 • Citrix XenServer 5.6 или новее • VirtualBox от Oracle 3 Решение должно обнаруживать и блокировать вредоносное ПО в режиме реального времени, включая вирусы, черви, троянские программы, шпионское ПО, рекламное ПО (Adware) и руткиты. 4 Решение для конечных точек должно включать поведенческий анализ помимо сигнатур для известных угроз, а также эвристический подход к уязвимостям. Решение должно оценивать как хорошее, так и плохое поведение неизвестных приложений, повышая качество обнаружения и снижая ложные срабатывания без необходимости создания конфигураций на основе правил для защиты от неизвестных угроз (zero-day). 5 Межсетевой экран решения должен иметь возможность разрешать или блокировать сетевые протоколы, включая Ethernet, Token Ring, IPX/SPX, AppleTalk и NetBEUI. Должна быть возможность блокировать драйверы протоколов (например, VMware, WinPcap), а также иметь правила, специфичные для адаптеров — например, Ethernet, Wireless, VPN. 6 Предлагаемое решение IPS должно позволять заказчику редактировать и создавать сигнатуры IPS в формате, основанном на Snort, при необходимости. 7 Решение должно иметь возможность блокировать устройства на основе
---	--

	Windows Class ID, включая USB, Infrared, Bluetooth, Serial, Parallel, FireWire, SCSI и PCMCIA. 8 Решение также должно иметь возможность блокировать устройства и предоставлять права чтения/записи/выполнения для указанных устройств. 9 Решение должно обеспечивать анализ приложений, контроль процессов, контроль доступа к файлам и реестру, а также контроль модулей и DLL. 10 Предлагаемое решение должно позволять развёртывание гибких и различных политик безопасности в зависимости от логических условий AND/OR следующих сетевых триггеров: • IP-адрес (диапазон или маска) • DNS-сервер • DHCP-сервер • WINS-сервер • Адрес шлюза • Наличие TMP-токена (аппаратный токен) • DNS-имя разрешается в IP • Подключение к Policy Manager • Тип сетевого соединения (беспроводное, VPN, Ethernet, dial-up) 11 Предлагаемое решение IPS должно объединять NIPS (сетевой) и HIPS (хостовый) с Generic Exploit Blocking (GEB) для одной сигнатуры, обеспечивая проактивную защиту от всех вариантов, гранулярный контроль доступа приложений и упомянутую выше поведенческую технологию. 12 Предлагаемое решение Anti-Spyware должно иметь возможность обходить файловую систему Windows и иметь прямой доступ к тому NTFS для выполнения raw-сканирования диска с целью превосходной защиты от руткитов. 13 System Lock Down — решение должно иметь возможность «блокировать» систему путём создания отпечатков (fingerprint) каждого исполняемого файла в системе. Затем оно может контролировать все запущенные приложения и завершать любое приложение, для которого у агента нет совпадающего отпечатка. 14 Обнаружение и защита от DoS-атак — должно защищать систему от различных форм аномального сетевого поведения, направленного на нарушение доступности и/или стабильности системы. 15 Анти-спуфинг — должно защищать передачу данных от отправки на систему хакера, который подделал свой IP или MAC-адрес. 16 Агент должен иметь возможность обнаруживать и блокировать цепочки выполнения процессов. Он должен обнаруживать, когда вредоносное приложение пытается запустить доверенное приложение и затем использовать привилегии доверия этого приложения для доступа к сети. 17 Защита от перехвата приложений (Anti-application hijacking) — должно предотвращать идентификацию операционной системы и браузера отдельных компьютеров хакерами и веб-сайтами. 18 Предотвращение атак с внедрением кода — предотвращать внедрение вредоносными приложениями кода в доверенные приложения для обхода исходящего межсетевого экрана приложений. 19 Предотвращение атак через адаптер протокола — предотвращать использование вредоносными приложениями собственного адаптера протокола для обхода исходящего межсетевого экрана. 20 Предлагаемое антивирусное решение не должно ни разу провалить награду Virus Bulletin 100 и должно получить её более 41 раза подряд. 21 Предлагаемое решение персонального межсетевого экрана должно находиться в верхней части квадранта Gartner Magic Quadrant. 22 Политики Antivirus и Antispyware должны по умолчанию иметь
--	--

	опции выбора «Высокая безопасность» и «Высокая производительность» для обеспечения правильного баланса при развёртывании в производственной сети. 23 Запланированные антивирусные сканирования должны откладываться/переназначаться, когда ноутбуки работают от батареи. 24 Антивирус должен иметь поведенческую технологию для сканирования на наличие троянов, червей и кейлоггеров для защиты от zero-day угроз. Уровень чувствительности должен настраиваться с возможностью кастомизации частоты сканирования. 25 Антивирусное решение должно иметь защиту интернет-браузера, а домашняя страница должна быть настраиваемой при изменении уровня риска безопасности. 26 Предлагаемое решение должно иметь плагин для электронной почты, который сканирует вложения, включая zip-файлы, удаляя вредоносное ПО до попадания в почтовый ящик, и должно уметь сканировать POP3-трафик электронной почты, включая клиенты Microsoft Outlook, Lotus Notes и Outlook Express. 27 Правила Desktop Firewall должны настраиваться в зависимости от адаптеров, включая Ethernet, wireless, Dial-up, VPN (Microsoft PPTP, Nortel, Cisco). 28 Правила Desktop Firewall должны настраиваться в зависимости от состояния хранителя экрана («Вкл» и «Выкл»). 29 Политики Desktop Firewall должны настраиваться в зависимости от времени и дня недели. 30 Продукт должен иметь готовые политики, включая: сделать все съёмные диски только для чтения, блокировать запуск программ со съёмных дисков, защищать файлы и ключи реестра клиентов, логировать файлы, записанные на USB-диски, блокировать изменения в файле hosts. 31 Сервер управления должен иметь возможность добавлять несколько доменов при необходимости для разных локаций с назначением разных администраторов. Каждый домен должен использовать один и тот же сервер управления и базу данных. Такое разделение предотвращает просмотр данных одного домена администраторами другого. Администраторы могут просматривать и управлять содержимым только своего домена, но не содержимым других доменов. 32 Для экономии пропускной способности сети клиенты должны иметь возможность настройки максимального количества записей логов, загружаемых на сервер управления. 33 Продукт должен иметь настройку безопасности для блокировки всего трафика до запуска межсетевого экрана и после его остановки, за исключением начального DHCP- и NetBIOS-трафика. 34 Предлагаемое антивирусное решение должно иметь возможность определять файлы по количеству пользователей, использующих этот файл по всему миру. 35 Предотвращение вторжений в браузер: антивирус должен быть способен блокировать вредоносные загрузки через браузеры. 36 Предлагаемое антивирусное решение должно ранжировать файлы на основе цифровой подписи, возраста файла, распространённости и подобных атрибутов. 37 Клиент антивируса должен иметь видимый индикатор при подключении к консоли антивируса. 38 Консоль антивируса должна иметь индикатор угроз (threat cone), показывающий статус вирусов в публичной сети. 39 Предлагаемое решение
--	---

	должно иметь функцию deception (обмана) в составе агента конечной точки. 40 Предлагаемое решение должно иметь защиту от эксплойтов памяти (Memory exploit mitigation) в составе того же агента. 41 Предлагаемое решение должно иметь функцию EDR с использованием того же агента. 42 Предлагаемое решение должно иметь endpoint deception в составе единого агента. 43 Предлагаемое решение должно иметь Host Integrity, который выявляет и исправляет несоответствующие или устаревшие конечные точки. 44 Предлагаемое решение должно иметь эффективное продвинутое машинное обучение при анализе файлов и поведенческом анализе. 45 Предлагаемое решение должно иметь Host IPS, способный блокировать и обнаруживать внутренние или исходящие сетевые атаки, коммуникации и угрозы на уровне браузера и сети до того, как они попадут на диск и будут выполнены. 46 Агент конечной точки должен быть защищён от вмешательства или отключения. 47 Предлагаемое решение должно иметь облачную консоль управления в качестве опции. Обнаружение и реагирование на конечных точках (Endpoint Detection and Response) 48 Endpoint Detection and Response должен обнаруживать, искать, изолировать и устранять вторжения на всех конечных точках с использованием аналитики на базе ИИ, playbook-ов расследования и непревзойдённой разведки угроз, и должен быть интегрирован с Endpoint Protection в виде единого агента. EDR должен иметь следующие возможности: Обнаружение и выявление — сокращение времени обнаружения нарушения и быстрое определение масштаба • Применение машинного обучения и поведенческой аналитики для выявления подозрительной активности, обнаружения и приоритизации инцидентов • Автоматическое выявление и создание инцидентов для подозрительных скриптов и эксплойтов памяти • Выявление атак на основе памяти с анализом памяти процессов Расследование и сдерживание — повышение продуктивности специалистов по реагированию на инциденты и обеспечение сдерживания угроз • Обеспечение полного воспроизведения инцидента с непрерывной записью активности конечной точки, просмотр конкретных процессов конечной точки • Охота за угрозами путём поиска индикаторов компрометации по всем конечным точкам в реальном времени • Сдерживание потенциально скомпрометированных конечных точек во время расследования с помощью карантина конечной точки Устранение — быстрое восстановление конечных точек и предотвращение возвращения угрозы • Удаление вредоносных файлов и связанных артефактов на всех затронутых конечных точках • Чёрный и белый списки файлов на конечной точке • Расширенная отчётность позволяет экспортировать любую таблицу для отчётов по устранению инцидентов Интеграция и автоматизация — унификация представлений для исследователей, оркестрация данных и рабочих процессов • Лёгкая интеграция данных об инцидентах и действий в существующую инфраструктуру SOC, включая Splunk и ServiceNow • Воспроизведение лучших практик и анализа опытных исследователей с помощью автоматизированных правил playbook инцидентов •
--	--

	Получение глубокой видимости активности конечной точки с помощью автоматизированного сбора артефактов 49 Респондент должен иметь в составе платформы решение для конечных точек, позволяющее обнаружение, валидацию и карантин. Вся функциональность должна работать как в корпоративной сети, так и вне её, без требования VPN-подключения к корпоративной сети. 50 Предлагаемая платформа должна поддерживать несколько технологий обнаружения и защиты в рамках своего решения и должна включать сигнатурный движок, использующий базу данных известных файлов и их поведения для определения вредоносности файла, без дополнительного payload при детонации файла для обнаружения zero-day и неизвестных угроз. 51 Решение должно иметь двухэтапный процесс карантина и устранения. 52 Решение должно иметь возможность распространять новые версии обновлений агента конечной точки. 53 Агенты конечных точек должны управляться как в корпоративной сети, так и вне её для целей обнаружения, triage и карантина. 54 Решение Endpoint Detection and Response должно иметь возможность получать информацию о zero-day угрозах от других устройств безопасности, выполняющих виртуальное исполнение. 55 Решение Endpoint Detection and Response должно принимать пользовательские индикаторы компрометации (IOC). 56 Агент конечной точки должен иметь возможность защищать от угроз, таких как Adware, вирусы и уязвимости программного обеспечения, существующих на конечной точке. 57 Возможность полного криминалистического анализа выявленного вредоносного ПО и предоставления следующей информации сотрудникам предприятия: • Полный отчёт об изменениях на хосте (Comprehensive Host Modification Report) • Копия бинарных файлов вредоносного ПО • Полные цепочки URL, указывающие все места, с которыми вредоносное ПО пытается связаться • Сводные отчёты о событиях вредоносного ПО на предприятии с разбивкой по типу, хосту и активности • Немедленный анализ, является ли вредоносное ПО ранее ИЗВЕСТНОЙ или НЕИЗВЕСТНОЙ угрозой • Информация о серьёзности, показывающая, насколько эффективны были бы другие средства защиты против этой угрозы 58 Предлагаемое решение должно динамически генерировать необходимые правила/политики для блокировки/добавления в чёрный список вредоносного файла на всех клиентах конечных точек без необходимости развёртывания/интеграции с дополнительными агентами. 59 Решение должно иметь возможность автоматически помещать признанные вредоносными файлы в карантин в другое сетевое расположение. 60 Решение должно иметь возможность передавать индикаторы компрометации (IOC), такие как хеш файла, в решение для конечных точек, чтобы оно могло блокировать текущие и будущие обнаружения похожих файлов. 61 Решение должно уметь обнаруживать руткиты уровня ядра (Kernel level rootkits). 62 Решение должно уметь обрабатывать reflective DLL injection. 63 Решение должно уметь идентифицировать вредоносный файл на разных конечных точках, даже если он представлен под разными именами. 64 Решение должно
--	--

	предоставлять единое представление подозрительных или вредоносных файлов на всех конечных точках. 65 Решение должно предоставлять репутацию файлов на основе разведывательной информации, собранной по всему миру, для помощи в процессах устранения и расследования. 66 Решение должно предоставлять администратору возможность отправлять файлы на динамический анализ вредоносного ПО. 67 Решение должно предоставлять возможность добавлять файлы в белый или чёрный список на конечных точках. 68 Агент конечной точки должен поддерживать проверку репутации файлов на серверах EDR. 69 Агент конечной точки должен поддерживать блокировку, удаление и карантин угроз. 70 Агент конечной точки не должен влиять на производительность системы. 71 Агент конечной точки должен предоставлять возможности host-based intrusion prevention для защиты от сетевых угроз, нацеленных на конечные точки. 72 Агент конечной точки должен предоставлять возможности browser-based intrusion prevention для конечных точек. 73 Решение для конечных точек должно поддерживать глубокий поиск по окружению индикаторов компрометации (IOC) со всех конечных точек по файлам, ключам реестра, а также доменам и URL. 74 Решение для конечных точек должно иметь возможность добавлять в чёрный список и удалять вредоносные файлы из единой панели управления. 75 Решение должно иметь возможность помещать конечные точки в карантин из единой панели управления для предотвращения дальнейшего заражения. 76 Решение для конечных точек должно коррелировать информацию об угрозах и вредоносном ПО с существующим антивирусным решением и приоритизировать или понижать приоритет инцидентов EDR на основе статуса защиты антивирусным решением. 77 Предлагаемое решение APT также должно поддерживать текущую защиту конечных точек в составе платформы, позволяющую обнаружение, валидацию, сдерживание и устранение угроз на конечной точке. 78 Агент конечной точки должен интегрироваться с защитой конечных точек и не требовать установки какого-либо нового агента на конечной точке. 79 Решение EDR для конечных точек должно иметь возможность устранять угрозы на конечной точке с использованием существующей защиты конечных точек или собственных инструментов. 80 Решение EDR для конечных точек должно уметь обнаруживать неизвестное вредоносное ПО и отправлять его на виртуальное исполнение с конечных точек независимо от сетевого решения EDR. 82 Решение EDR для конечных точек должно уметь обнаруживать, валидировать, сдерживать и устранять угрозы на конечных точках, когда пользователь находится в корпоративной сети или вне её, без требования VPN-подключения к корпоративной сети. 83 Предлагаемое решение должно поддерживать сдерживание конечных точек, а операции сдерживания должны поддерживать ролевых администраторов. 84 Решение EDR для конечных точек должно динамически принимать IOC и разведку угроз от устройств, выполняющих анализ виртуального исполнения в сети (например, интеграция с сетевым и email-решением EDR). 85
--	--

	Предлагаемое решение должно поддерживать запросы IoC и Threat Hunt непосредственно на клиентах в масштабе. 86 Решение EDR для конечных точек должно интегрироваться с SIEM. 87 Решение EDR для конечных точек должно уметь обнаруживать наличие файлов, которые были записаны в систему, но ещё не были выполнены. 88 Решение EDR для конечных точек не должно мешать нормальной работе пользователей и бизнес-операциям на конечной точке, независимо от нагрузки на систему. 89 Решение EDR для конечных точек должно регулярно обновлять разведку угроз, включая индикаторы, связанные с высокоразвитыми группами угроз в государственно спонсируемых целевых атаках. 90 Обновления решения EDR для конечных точек должны поддерживаться стандартными корпоративными механизмами развёртывания ПО, а также возможностью выполнять обновления конечных точек внутри самого решения. 91 Поставщик решения должен позволять отправку подозрительного образца на анализ одним нажатием кнопки из решения во избежание потенциальных ложных срабатываний. 92 Решение должно поддерживать bare-metal и виртуальную песочницу исполнения для обнаружения нового поколения угроз, осведомлённых о виртуализации. 93 Внедрение решения не должно добавлять какой-либо новый агент и должно быть частью защиты конечных точек на машине конечной точки. 94 Предлагаемое решение должно поддерживать flight data recorder (регистратор данных полёта). Контроль приложений (Application Control) 95 Предлагаемое решение должно обеспечивать комплексное обнаружение и инвентаризацию приложений для сканирования и инвентаризации всех приложений и файлов, собранных со всех конечных точек в окружении, и предоставлять подробную информацию о каждом приложении и файле, включая имя, оценку риска, оценку уязвимости, издателя, репутацию, количество устройств, на которых оно обнаружено, и т.д. 96 Предлагаемое решение должно обеспечивать комплексную политику контроля приложений и простое создание политик с Logical View для добавления любого приложения из обнаруженных в белый или чёрный список. 97 Endpoint App Control обеспечивает доверие к приложениям на основе различных атрибутов приложений, разрешая или блокируя приложения на основе одного или комбинации любого количества статических (например, хеш, путь, издатель и сертификат) и динамических (например, оценка риска и репутация) атрибутов. 98 Политика App Control должна позволять создание правил по широкому диапазону параметров, включая имя приложения, путь, хеш, репутацию, издателя, пользователя, группу пользователей и параметры командной строки. 99 Политика App Control должна иметь опцию применения в режиме «только мониторинг». 100 Предлагаемое решение должно анализировать разницу между приложениями, разрешёнными в окружении, и приложениями, которые реально запускаются в окружении. 101 Предлагаемое решение должно позволять определять доверенных обновляющих (trusted updaters), которыми могут быть обнаруженные приложения или новые приложения, издатель, каталог,
--	---

	файлы, пользователи и группы пользователей, которые могут устанавливать или обновлять ПО на конечных точках. 102 Предлагаемое решение должно предотвращать эксплуатацию доверенных приложений и предотвращать заражение систем недоверенными приложениями. Изоляция поведения приложений (Application Behavior Isolation) 103 Предлагаемое решение должно иметь возможности правил изоляции поведения приложений для защиты устройств. Эти правила разрешают или блокируют определённое поведение приложений следующих типов изоляции: • Изоляция браузера (Google Chrome, Firefox, Internet Explorer, Microsoft Edge) • Изоляция Office • Изоляция PDF Renderer • Политика изоляции платформы, которая включает: о Настройки ОС о Общие настройки jail (высокая, средняя и низкая изоляция) Изоляция предоставляет правила для защиты следующего: • Защита реестра • Защита файлов • Защита взаимодействия процессов • Защита выполнения процессов • Защита сетевого доступа • Защита системных вызовов 104 Предлагаемое решение должно обнаруживать любые подозрительные файлы в нашей сети на основе уровней интенсивности и позволять добавлять обнаруженные файлы в белый или чёрный список, а также изолировать подозрительное приложение с помощью политики Platform Isolation. 105 Предлагаемое решение должно иметь возможность обнаруживать, инвентаризировать и изолировать портативные приложения на основе оценки риска. Deception (Обман / Приманки) 105 Предлагаемое решение должно иметь функцию deception с развёртыванием широкого спектра «приманок» — поддельных файлов, учётных данных, сетевых ресурсов, записей кэша и конечных точек — по всему окружению. 106 Предлагаемое решение должно иметь endpoint deception в составе единого агента. 107 Предлагаемое решение должно использовать техники deception для мониторинга и уведомления о вредоносном поведении приложений. Защита конечных точек для мобильных устройств (Endpoint Protection for Mobile) 108 Предлагаемое решение должно поддерживать устройства iOS и Android. 109 Предлагаемое решение должно предотвращать атаки на мобильные устройства под управлением iOS и Android. 110 Предлагаемое решение должно проактивно защищать мобильные устройства от вредоносного ПО, сетевых угроз и эксплойтов уязвимостей приложений/ОС, как с подключением к Интернету, так и без него. 111 Предлагаемое решение должно обеспечивать более быструю реакцию и постоянную защиту, даже когда устройства отключены от Интернета. 112 Предлагаемое решение должно проактивно отражать атаки немедленно и автоматически при обнаружении угрозы. 113 Предлагаемое решение должно воздействовать точно на угрозу, не затрагивая другие ресурсы или процессы, и активироваться по требованию. 114 Предлагаемое решение должно иметь действия защиты от угроз рискованных приложений, включая, но не ограничиваясь: блокировку коммуникации, предотвращение установки, блокировку коммуникации с вредоносными серверами командования и управления (C&C) и блокировку доступа к чувствительным ресурсам.
--	--

	115 Предлагаемое решение должно иметь действия защиты от сетевых угроз, включая, но не ограничиваясь: автоматический запуск VPN-туннеля при обнаружении сетевой угрозы, блокировку доступа к чувствительным корпоративным ресурсам и блокировку доступа к поддельным корпоративным Wi-Fi точкам доступа. 116 Предлагаемое решение должно иметь действия защиты от контентных угроз, включая, но не ограничиваясь: туннелирование всего трафика через безопасный веб-шлюз, блокировку доступа к нежелательному контенту и блокировку SMS-фишинговых сообщений. 117 Предлагаемое решение должно иметь действие защиты для автоматического отключения вредоносных VPN. 118 Предлагаемое решение должно иметь VPN-технология, реализуемую в режиме always-on или on-demand. 119 VPN-технология в предлагаемом решении должна иметь возможность работать двумя способами: 1. Как зашифрованный туннель, через который трафик безопасно проходит между устройством и сетью. 2. Как селективный блокировщик трафика (определённый трафик, проходящий через VPN, сбрасывается и никогда не покидает устройство). Каждая из этих реализаций может быть always-on или on-demand. 120 Предлагаемое решение должно иметь многоуровневую мобильную защиту от известных и zero-day атак по всем векторам мобильных угроз. 121 Предлагаемое решение должно обеспечивать защиту от подозрительных сетей, приложений и поведения до того, как они смогут причинить вред. 122 Предлагаемое решение должно защищать конфиденциальность и продуктивность без негативного влияния на мобильный опыт пользователя или время работы батареи. 123 Предлагаемое решение должно иметь автоматизированное применение IT-политик и встроенные интеграции со всеми основными существующими корпоративными EMM/MDM, SIEM, почтовыми серверами и VPN. 124 Предлагаемое решение должно иметь возможности интеграции со многими решениями безопасности, включая, но не ограничиваясь: WSS, CASB, DLP и Endpoint protection. 125 Предлагаемое решение должно быть простым в развёртывании, внедрении, обслуживании и обновлении. 126 Предлагаемое решение должно иметь нулевое влияние на продуктивность, опыт пользователя, конфиденциальность и обеспечивать глубокий анализ подозрительных приложений. 127 Предлагаемое решение должно обеспечивать реагирование и защиту в реальном времени от различных известных, неизвестных и целевых атак вредоносного ПО от любых подозрительных приложений и сетей. 128 Предлагаемое решение должно иметь автоматизированную защиту корпоративных активов при атаке. 129 Предлагаемое решение должно иметь возможность проверки репутации с использованием машинного обучения для приложений, сетей и ОС. 130 Предлагаемое решение должно иметь комплексные журналы активности для интеграции с любым решением SIEM. 131 Предлагаемое решение должно иметь возможность анализа приложений на основе сигнатур, статического/динамического анализа, поведения, структуры, разрешений, источника и т.д. 132 Предлагаемое решение должно иметь обнаружение, блокировку и
--	--

	устранение вредоносных профилей iOS. 133 Предлагаемое решение должно иметь возможность выявлять атаки Man-in-the-Middle, понижение SSL и манипуляции с контентом без нарушения конфиденциальности. 134 Предлагаемое решение должно иметь возможность мониторинга устройств на наличие неисправленных известных уязвимостей и выявления zero-day уязвимостей в приложениях и операционных системах. 135 Предлагаемое решение должно обеспечивать защиту от мобильных угроз для современных операционных систем без зависимости от сторонних решений. Active Directory 136 Предлагаемое решение должно противодействовать скрытым атакам или APT с эффективной защитой Active Directory с конечной точки для обеспечения автономного сдерживания нарушений, реагирования на инциденты и оценки безопасности домена. 137 Предлагаемое решение должно автономно изучать структуру Active Directory организации в полном объёме (серверы, конечные точки, приложения, пользователи, филиалы, соглашения об именовании, конфигурации, атрибуты и т.д.). 138 Предлагаемое решение должно уметь создавать аутентичную и неограниченную обфускацию. 139 Предлагаемое решение должно уметь выполнять runtime-оценку процессов, контекста и активности Active Directory. 140 Предлагаемое решение должно иметь высокоточные оповещения и возможность автоматической блокировки атаки. 141 Предлагаемое решение должно предоставлять криминалистическую отчётность в реальном времени, фиксирующую реальные фазы разведки, кражи учётных данных и горизонтального перемещения, выполненные атакующим, и документирующую цепочку атак. 142 Предлагаемое решение должно уметь автоматически останавливать вредоносный процесс на конечной точке для сдерживания нарушения в реальном времени, лишая его возможности породить другой процесс, перезаписывать другую часть памяти, выполнять команды разведки или связываться с сетью. 143 Предлагаемое решение должно иметь возможность непрерывно зондировать домен на предмет неправильных конфигураций, уязвимостей и persistence, представлять домен с точки зрения атакующего и позволять немедленное снижение рисков. 144 Предлагаемое решение должно предотвращать горизонтальное перемещение с помощью защиты AD и технологии deception на основе ML. 145 Предлагаемое решение должно иметь автоматизированный процесс оценки, использующий симуляции атак для сбора подробной информации о конфигурации домена, привилегированных учётных записях, настройках безопасности, GPO, конечных точках, контроллере домена и Kerberos. 146 Предлагаемое решение должно автономно анализировать каждый компонент домена и структуры Active Directory на предмет неправильных конфигураций и бэкдоров в AD и всей доменной среде. Управление и отчётность (Management and Reporting) 153 Решение должно развёртываться, администрироваться и обновляться в составе единого пакета агента и механизма обновления. Не должно быть необходимости в многократном развёртывании агента и получении обновлений для достижения всей требуемой
--	---

	функциональности продукта. 154 Предлагаемое решение должно иметь возможность развёртывания в вариантах Cloud, On-Prem и Hybrid. 155 Находить неуправляемые конечные точки и развёртывать единый легковесный агент для полной защиты. 156 Проверки безопасности и соответствия должны управляться единым сервером администрирования и консолью. 157 Решение должно обеспечивать интеграцию с RSA для аутентификации консоли управления в дополнение к аутентификации по учётным данным пользователя при необходимости, а также должно интегрироваться с LDAP, Syslog и Active Directory. 158 Серверы управления, установленные в разных локациях, должны иметь возможность репликации данных, логов и контента через заданные интервалы в архитектуре Multi-Server с репликацией политик и логов. 159 Агент должен иметь возможность защиты паролем от удаления, пароля для отключения службы и пароля для открытия GUI клиента, чтобы пользователи не могли удалить агент. 160 Агент должен иметь возможность защищать службу от остановки, даже если администратор выполнил вход. 161 Механизм обновления должен включать обновления контента клиентов с сервера управления, внутренних серверов обновлений, внешних серверов обновлений вендора, а также от клиента, выступающего в роли прокси между сервером управления и клиентами в группе, и с использованием сторонних инструментов, таких как Microsoft SMS. 162 Предлагаемое антивирусное решение должно иметь единый и тот же агент для физических и виртуальных клиентов.
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)	