# Licenční smlouva č. 21/600/0429

**„Pořízení nástroje pro dohled nad vzdáleným přístupem dodavatelů ISCS“**

Smluvní strany:

## Česká republika – Generální ředitelství cel

se sídlem: Budějovická 7, 140 96, Praha 4
IČ: 71214011,
DIČ: CZ71214011
bankovní spojení: ČNB Praha 1,
číslo účtu: 1020011/0710
jednající: [redacted]
Spojení: [redacted]

(dále jen „**nabyvatel**“)

a

## ALEF NULA, a.s.

se sídlem: Pernerova 691/42, 186 00 Praha 8
IČ: 61858579,
DIČ: CZ61858579
společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze,
oddíl B., vložka 2727
bankovní spojení: Komerční banka, a.s.,
číslo účtu: 51-3717150237/0100
zastoupená: Milan Zinek, předseda představenstva
(dále jen „**poskytovatel**“)

uzavírají v souladu s ustanovením § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**OZ**“) s přihlédnutím k zákonu č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorský zákon**“) a zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) ve znění pozdějších předpisů (dále jen „**ZOK**“), a zákonem č. 134/2016 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), tuto

**licenční smlouvu**

(dále jen „**Smlouva**“)

**Smluvní strany, vědomy si svých závazků v této Smlouvě obsažených a s úmyslem býti touto Smlouvou vázány, dohodly se na následujícím znění Smlouvy:**

## Čl. 1 Úvodní ustanovení

1.1 Poskytovatel prohlašuje, že je právnickou osobou řádně založenou a existující podle českého právního řádu, splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Poskytovatel prohlašuje, že je oprávněným prodejcem produktů společnosti BeyondTrust (11695 Johns Creek Parkway, Suite 200, Johns Creek, Georgia 30097, USA) (dále jen „BeyondTrust“) .

1.3 Poskytovatel prohlašuje, že je oprávněn poskytovat práva užití k produktům společnosti BeyondTrust.

1.4 Výše uvedený profesní kvalifikační předpoklad se v plném rozsahu vztahuje i na případné subdodavatele, pokud dodavatel zamýšlí jimi plnit příslušnou část zakázky.

1.5 Poskytovatel dále prohlašuje, že má dostatečné množství certifikovaných specialistů, aby mohl nabyvateli řádně poskytovat konzultace spojené s používáním dodaných produktů. Poskytovatel prohlašuje, že je ve smyslu ust. § 5 OZ odbornou osobou v dané oblasti.

1.6 Poskytovatel se dále zavazuje, že po celou dobu účinnosti Smlouvy bude disponovat dostatečným množstvím certifikovaných specialistů v místě plnění, a to nejméně v rozsahu 1 analytik/konzultant, tak aby mohl nabyvateli řádně poskytovat konzultace spojené s používáním dodaných produktů.

## Čl. 2 Předmět Smlouvy

2.1 Předmět této Smlouvy je definován v Příloze č. 1 Smlouvy – Technická specifikace předmětu veřejné zakázky, a to co do množství, druhu a délky poskytnutí softwaru (dále jen „**Software**“) a dalšího souvisejícího plnění.

2.2 Poskytovatel se touto Smlouvou zavazuje zajistit nabyvateli v souladu s autorským zákonem a OZ právo užití software (dále jen „**Licence**“) způsobem, v rozsahu a za podmínek stanovených v této Smlouvě. Licence bude účinná po celou dobu účinnosti této Smlouvy, tj. nejméně po dobu minimálně 12 měsíců.

2.3 Poskytovatel se zavazuje dodat nabyvateli licenční klíče a přístupové kódy, které budou zaslány na email nabyvatele [redacted]

2.4 Zdrojové kódy k Software nejsou předmětem dodávky.

2.5 Nabyvatel se zavazuje za řádně poskytnuté plnění uhradit poskytovateli odměnu za Licenci ve výši a za podmínek stanovených v této Smlouvě.

2.6 Licence poskytovaná poskytovatelem je účinná od okamžiku potvrzení přijetí licenčních klíčů prostřednictvím emailu nabyvatele [redacted] na e-mail poskytovatele [redacted]

## Čl. 3 Místo a doba plnění

3.1 Místem dodání Software se rozumí sídlo nabyvatele uvedené v této Smlouvě. Dodáním Software se rozumí předání klíčů a přístupů dle bodu 2.3 této Smlouvy. Převzetí klíčů potvrdí nabyvatel poskytovateli prostřednictvím emailu.

3.2 Poskytovatel se zavazuje dodat nabyvateli Software do 30 kalendářních dnů účinnosti této Smlouvy.

## Čl. 4 Odměna a platební podmínky

4.1 Odměna za předmět plnění (za poskytnutí Software a zajištění Licence) byla stanovena na základě cenové nabídky poskytovatele a celkově činí:

991 893,- Kč bez DPH

1 200 190,53 Kč včetně 21 % DPH

(dále jen „**Odměna**“)

4.2 Odměna za Licenci zahrnuje též cenu přenosového média, pokud je Software na něm dodáván, a veškeré náklady související s dodáním do místa plnění.

4.3 Poskytovatel je oprávněn vystavit fakturu na úhradu Odměny po dodání Software, přičemž dodáním se rozumí postup uvedený v bodu 3.1 Smlouvy.

4.4 Splatnost řádně vystaveného daňového dokladu – faktury obsahující náležitosti dle příslušných právních předpisů činí 90 (slovy: devadesát) dnů ode dne doručení nabyvateli do sídla uvedeného v této Smlouvě nebo do datové schránky s následujícími parametry: ID datové schránky „Generální ředitelství cel“: 7puaa4c.

4.5 Faktura(y) musí obsahovat náležitosti daňového dokladu podle § 435 OZ, podle § 7 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), podle zákona č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů a podle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a odkaz na tuto Smlouvu.

4.6 Faktura musí obsahovat také evidenční čísla této Smlouvy. Pokud faktura nebude obsahovat stanovené náležitosti dle této Smlouvy, nebo v ní nebudou správně uvedené údaje, je objednatel oprávněn vrátit ji ve lhůtě 10 (slovy: deseti) pracovních dnů od jejího obdržení poskytovateli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě bude faktura poskytovatelem opravena a nová lhůta splatnosti v délce 90 (slovy: devadesát) dnů začne plynout doručením opravené faktury zpět objednateli. V případě, že objednatel fakturu vrátí, přestože faktura je správná a předepsané náležitosti obsahuje, zůstává v platnosti původní lhůta splatnosti faktury a pokud objednatel fakturu nezaplatí v původním termínu splatnosti, je v prodlení.

4.7 Peněžní závazek nabyvatele se považuje za včas splněný dnem připsání příslušné částky ve prospěch účtu poskytovatele. Platba faktur(y) bude provedena bezhotovostním převodem na bankovní účet poskytovatele, jenž je uveden v této Smlouvě.

4.8 Platby budou probíhat výhradně v Kč a rovněž veškeré cenové údaje budou v této měně.

4.9 Smluvní strany si dojednaly, že nabyvatel je oprávněn provést zajišťovací úhradu daně z přidané hodnoty ve smyslu ust. § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, na účet příslušného správce daně, jestliže se poskytovatel stane ke dni poskytnutí úplaty za uskutečněné zdanitelné plnění nespolehlivým plátcem daně ve smyslu ust. § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

## Čl. 5 Ochrana obchodního tajemství a důvěrných informací

5.1 Obě smluvní strany berou na vědomí, že tato Smlouva a veškerá práva, povinnosti a závazky z ní vyplývající, jsou považovány za důvěrné a smluvní strany se zavazují zachovávat o nich mlčenlivost. To neplatí, je-li poskytnutí informace třetí osobě nezbytné pro plnění závazků z této Smlouvy nebo je-li poskytnutí informace dáno právním předpisem nebo na základě rozhodnutí orgánu veřejné moci.

5.2 Smluvní strany tímto souhlasně prohlašují, že nepovažují za porušení ochrany obchodního tajemství ve smyslu ustanovení § 504 OZ a ustanovení § 1730 odst. 2 OZ situace, pokud smluvní strana poskytne v rozsahu nezbytně nutném důvěrné informace dle této Smlouvy svým právním, účetním nebo daňovým poradcům, za předpokladu, že jsou tyto osoby vázány zákonnou nebo smluvní povinností mlčenlivosti alespoň v rozsahu stanoveném v této Smlouvě.

5.3 V případě přístupu k osobním údajům, které jsou v rámci Celní správy ČR zpracovávány, se tímto poskytovatel zavazuje k tomu, že při své činnosti bude postupovat v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 a zákona č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů, zejména:

a) přijme taková opatření, která zajistí náležité zabezpečení zpřístupněných osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a náhodnou ztrátou, zničením nebo poškozením,

b) bude se zpřístupněnými osobními údaji nakládat pouze v rozsahu nezbytně nutném k plnění předmětu díla,

c) bude zachovávat mlčenlivost ohledně zpřístupněných osobních údajů.

d) V případě zapojení třetí strany do plnění předmětu díla je poskytovatel povinen tuto stranu smluvně zavázat k plnění výše uvedených povinností v oblasti ochrany osobních údajů.

## Čl. 6 Servisní a reklamační podmínky, řešení vad a záruky

6.1 Záruka na Software je poskytována ze strany poskytovatele autorských práv Software a vyplývá z užívacích práv k provozování dodaného Software dle licenčních podmínek poskytovatele ALEF NULA, a.s., které jsou nedílnou součástí a přílohou č. 3 této Smlouvy.

6.2 Poskytovatel poskytuje na dodávaný SW záruku na bezvadnou funkci v délce trvání 12 měsíců. V případě, že bude na faktuře nebo na protokolu o předání a převzetí vyznačena

delší záruční doba, má tato přednost před ustanovením této Smlouvy. Záruční doba začíná běžet ode dne převzetí předmětu plnění nabyvatelem.

6.3 Nabyvatel odpovídá za užívání licencovaného Software v souladu s licenčními podmínkami (užívacími právy) poskytovatele ALEF NULA, a.s. vztahujícími se k danému Softwaru.

6.4 Software je produkt poskytovatele. Případné reklamace nebo nároky z odpovědnosti za vady Software nebo ze související odpovědnosti za škodu bude uplatňovat nabyvatel přímo vůči poskytovateli na základě přílohy č. 3 této Smlouvy.

**Čl. 7 Sankční ujednání**

7.1 V případě, že nabyvatel bude v prodlení s platbou faktury dle článku 4. Odměna a platební podmínky o více než 90 (slovy: devadesát) dnů a nedoloží prokazatelně, že zpoždění spočívá v systémových překážkách nabyvatelem neovlivnitelných (jako je zejména důvod vazby financování nabyvatele na státní rozpočet), je poskytovatel oprávněn žádat po nabyvateli zaplacení úroku z prodlení dle nařízení vlády č.351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob a evidence svěřenských fondů a evidence údajů o skutečných majitelích, ve znění pozdějších předpisů. Smluvní strany výslovně sjednávají, že výše úroků v takovém případě odpovídá náhradě škody.

7.2 V případě prodlení poskytovatele s předáním Software vzniká nabyvateli nárok na smluvní pokutu ve výši 0,05 % z Odměny včetně DPH za každý započatý den prodlení.

7.3 V případě nedodržení bodu 10.7 zaplatí poskytovatel nabyvateli sankci ve výši 50.000,- Kč.

7.4 Žádná ze smluvních stran neodpovídá za škodu způsobenou porušením svých povinností vyplývajících z této Smlouvy, bylo-li způsobeno okolnostmi vylučujícími odpovědnost ve smyslu ust. § 2913 odst. 2 OZ.

7.5 Sankce i náhrada způsobené škody jsou splatné do 30 kalendářních dnů ode dne doručení písemné výzvy k zaplacení společně s příslušným daňovým dokladem – fakturou smluvní straně, která je povinná příslušnou sankci nebo náhradu škody zaplatit.

7.6 Není-li dále stanoveno jinak, zaplacení jakékoliv sjednané smluvní pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky a rovněž jí nezbavuje povinnosti uhradit náhradu škody vzniklé v souvislosti s porušením jejího závazku v plné výši.

7.7 Smluvní strany si výslovně ujednaly, že k jiným než zde uvedeným a dále např. ústně sjednaným smluvním sankcím, jakož i k smluvním sankcím sjednaným dodatečně nebude přihlíženo.

7.8 Smluvní strany si vyloučily aplikaci ust. § 1806 OZ tzn. že úroky z úroků nelze požadovat.

## Čl. 8 Rozhodné právo a řešení sporů

8.1 Práva a povinnosti smluvních stran vyplývající z této Smlouvy se řídí autorským zákonem a OZ.

8.2 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě Smlouvy nebo v souvislosti s ní, včetně sporů o její výklad či platnost a usilovat se o smírné vyřešení těchto sporů nejprve prostřednictvím jednání kontaktních osob nebo pověřených zástupců.

8.3 Smluvní strany podle § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů určují jako místně příslušný soud Obvodní soud pro Prahu 1; v případě, že podle procesních předpisů je k rozhodování věci v prvním stupni příslušný krajský soud, určují smluvní strany jako místně příslušný soud Městský soud v Praze.

## Čl. 9 Trvání Smlouvy

9.1 Tato Smlouva se uzavírá na období 1 roku, přičemž nabývá platnosti podpisem zástupců obou smluvních stran a účinnosti dnem, kdy bude uveřejněna v registru smluv.

9.2 Smluvní strany si výslovně ujednaly, že poskytovatel není oprávněn tuto Smlouvu vypovědět po dobu platnosti Licence zakoupené nabyvatelem.

9.3 Nabyvatel i poskytovatel jsou oprávněni od této Smlouvy odstoupit v případě jejího podstatného porušení druhou smluvní stranou. Odstoupení se provádí písemným oznámením a je účinné jeho doručením na adresu uvedenou v této Smlouvě.

9.4 Za podstatné porušení se považuje:

a) ze strany poskytovatele prodlení při plnění termínu předání Software stanoveného v bodu 3.2 této Smlouvy delším než 30 (slovy: třicet) dnů,

b) ze strany objednatele zejména prodlení při hrazení smluvní ceny poskytovateli delším než 30 (slovy: třicet) dnů a/nebo porušení kterékoliv licenční podmínky vztahující se k nakládání se Software.

## Čl. 10 Závěrečná ustanovení

10.1 Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy a nahrazuje veškerá předešlá ujednání smluvních stran ústní i písemná.

10.2 Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě vzestupně číslovaných dodatků této Smlouvy, podepsaných za každou smluvní stranu osobou nebo osobami oprávněnými zastupovat jménem smluvních stran. Smluvní strany si dále ujednaly, že k jiným formám nebude přihlíženo a nebudou jimi vázány.

10.3 Pokud by se kterékoliv ustanovení této Smlouvy ukázalo být neplatným nebo nevynutitelným nebo se jím stalo po uzavření této Smlouvy, pak tato skutečnost nepůsobí neplatnost ani nevynutitelnost ostatních ustanovení této Smlouvy, nevyplývá-li z donucujících ustanovení právních předpisů jinak. Smluvní strany se zavazují takové neplatné či nevynutitelné ustanovení nahradit platným a vynutitelným ustanovením, které je svým obsahem nejbližší účelu neplatného či nevynutitelného ustanovení.

10.4 Poskytovatel výslovně souhlasí s tím, že nabyvatel tuto Smlouvu uveřejní na svém profilu v plném znění v souladu se ZZVZ.

10.5 Smluvní strany si ujednaly, že závazky vyplývající z této Smlouvy se promlčují ve lhůtě 10 let ode dne, kdy smluvní strana mohla poprvé toto právo uplatnit.

10.6 V souladu se zákonem č. 340/2015 Sb., o registru smluv, se strany dohodly, že nabyvatel zašle tuto Smlouvu správci registru smluv k uveřejnění ve lhůtě, stanovené tímto zákonem. Osobní údaje stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

10.7 V souladu s vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, se poskytovatel zavazuje k bezpečné likvidaci dat bez možnosti obnovení v okamžiku ukončení smluvního vztahu.

10.8 Smluvní strany si výslovně ujednaly, že tuto Smlouvu nelze postoupit na řad. Žádná ze smluvních stran není oprávněna vtělit jakékoliv právo plynoucí jí ze Smlouvy nebo z jejího porušení do podoby cenného papíru.

10.9 V případě rozporu mezi touto Smlouvou a jejími přílohami, případně dalšími licenčními podmínkami má vždy přednost ustanovení této Smlouvy.

10.10 Nedílnou součást Smlouvy tvoří tyto přílohy:

| | |
|---|---|
| Příloha č. 1: | Technická specifikace |
| Příloha č. 2: | Nabídka poskytovatele |
| Příloha č. 3 | Licenční podmínky |

10.11 Každá ze smluvních stran si ponechá jednu elektronicky podepsanou verzi této Smlouvy.

**Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.**

**Poskytovatel**

**V Praze dne dle el. podpisu**

Ing. Milan Zinek

Digitally signed by Ing. Milan Zinek
Date: 2025.12.15 11:52:08 +01'00'

.....

**ALEF NULA, a.s.**

Milan Zinek

předseda představenstva

**Nabyvatel**

**V _____ dne _____**

[redacted]

## Příloha č. 1

## Technická specifikace

**Poskytovatel musí splnit následující požadavky:**

### 1. Požadavky na kvalifikaci poskytovatele:

Tento systém je součástí řešení „Kybernetické bezpečnosti organizace v souladu s požadavky ZKB“, kdy se jedná především o splnění požadavků definovaných zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a jeho prováděcích vyhlášek. Z tohoto důvodu je nutné navrhnout a implementovat řešení, které bude vyhovovat aktuálním potřebám nabyvatele a umožní splnění těchto požadavků.

Z tohoto důvodu musí poskytovatel řešení splňovat příslušné kvalifikační předpoklady ke zvládnutí tohoto úkolu a musí být schopný implementovat nabízené řešení do stávajícího systému ISCS jako podpůrné aktivum prvku KII a VIS CS. Poskytovatel musí mít praktické zkušenosti s detekcí, vyhodnocováním a řešením bezpečnostních událostí i incidentů, a proto musí být registrován v databázi TF-CSIT týmů, provozovanou **Trusted Introducers**, alespoň na úrovni „**ACCREDITED**“. Nabyvatel má ze zákona povinnost udržovat intenzivní komunikaci se zahraničními subjekty, zejména s členskými státy EU a zajišťovat bezpečnost prvku KII a VIS CS. Nabyvatel požaduje po poskytovateli aby:

1) prokázal technickou kvalifikaci doložením popisu opatření poskytovatele k zajištění kvality dodávky předložením certifikátu vydaného certifikační autoritou (akreditovaným subjektem), z něhož bude vyplývat splnění podmínek dle normy **ISO 27001**

2) disponoval dostatečným množstvím certifikovaných specialistů, kteří budou schopni nabyvateli řádně poskytovat konzultace spojené s používáním dodaných produktů. Alespoň jeden specialista týmu poskytovatele musí mít certifikaci **Specialista řízení bezpečnosti informací** s následujícími požadavky:

Praxe a vzdělání:

- Minimálně ukončené středoškolské vzdělání a 5 let prokazatelné praxe v oblasti návrhu, implementace a řízení ISMS dle ISO/IEC 27001 řady nebo podle zákona 181/2014 Sb. ve znění pozdějších předpisů.

Certifikace:

- Certifikace Certified Information Security Manager (CISM), řízení kybernetické bezpečnosti nebo obdobné (v případě, že poskytovatel bude chtít doložit obdobný certifikát vydaný jinou autoritou, nabyvatel požaduje po poskytovateli doložení rozdílové analýzy rozsahu oblastí, které jsou pokryty certifikační zkouškou, jíž je certifikát podložen, oproti rozsahu pokrytém certifikační zkouškou uvedeného certifikátu.)

### 2. Požadavky na zkušenosti poskytovatele – reference:

Účastník předloží seznam dvou zakázek, ze kterého bude zřejmé, že účastník v posledních pěti letech před zahájením zadávacího řízení realizoval obdobné služby v oblasti zabezpečení IS v součtu minimálně v hodnotě 500.000,- Kč bez DPH.

Pro účely zjištění zkušeností s nabízeným systémem, musí být alespoň jedna z uvedených referencí provedena u klienta spravujícího prvek Kritické Informační infrastruktury (KII) podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

### 3. Požadavky na nasazení produktu a součinnost při realizaci projektu

Požadujeme dodat **nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů** dodavatelů CS. Projekt musí obsahovat kompletní dodávku a instalaci PAM systému, integraci cílových systémů, podpůrné činnosti, servis, podporu provozu a školení.

Projekt musí být řešen v celé své šíři uvedených požadavků pouze produktem s integrovaným uživatelským interface a centralizovaným managementem všech jeho funkcionalit z centrální konzole.

Veškerá zařízení i software musí zahrnovat aktualizace software, zákaznickou podporu telefonem a emailem v českém nebo slovenském jazyce v režimu 8x5, případnou hardwarovou záruku s reakcí následující pracovní den v sídle zadavatele (on-site NBD).

Požadavky na řešení jsou uvedeny v níže přiložené tabulce „Správa privilegovaných přístupů“.

| Správa privilegovaných přístupů | | | |
|---|---|---|---|
| **Oblast** | **Požadavky na řešení** | **Odpověď uchazeče (Ano / NE)** | **Popis skutečného naplnění požadavku** |
| Řízení přístupů | Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné. | ANO | Řešení poskytuje kompletní správu privilegovaných účtů s RBAC řízením přístupu. |
| Striktní oddělení přístupových oprávnění | Systém plně podporuje oddělení přístupových oprávnění. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci. | ANO | Smart Rules umožňují granulární oddělení oprávnění pro uživatele, účty, systémy i auditní záznamy. |
| Víceúrovňové schvalování přístupů | Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům – přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem, vytvořením ticketu v helpdesk systému atp. | ANO | Workflow schvalování s více úrovněmi, e-mailové notifikace a integrace s ticketing systémy. |
| Bezpečnostní parametry | Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi. Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám, bez autorizace vlastníků dat. Systém musí být certifikovaný bezpečnostním standardem Common Criteria anebo ekvivaletní certifikaci. | ANO | Certifikace Common Criteria EAL2+, šifrování AES-256, FIPS 140-3. |
| Jednotná centrální správa | Správa řešení je umožněna pomocí jednotné centrální správy. Řešení musí umožňovat konfiguraci systému pomocí RestAPI – správa uživatelů, zakládání a editace účtů, změny přihlašovacích údajů, terminace spojení atp. | ANO | Jednotná webová konzole s plným REST API pro automatizaci všech operací. |

| | | | |
|---|---|---|---|
| Integrace s ticketing nástroji | Řešení musí umožňovat integraci s ticketing nástroji třetích stran – žádost o schválení přístupu, přístup na základě existujícího tiketu, atp. | ANO | Nativní integrace se ServiceNow, Jira, BMC Remedy a dalšími ITSM nástroji. |
| Podpora MS Active Directory | Řešení nabízí plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD. | ANO | Plná integrace s AD/LDAP včetně synchronizace skupin, uživatelů a mapování rolí. |
| Uživatelské rozhraní | Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (minimálně PKI karty, RSA ID, Radius server, ...). | ANO | HTML5 webový portál s podporou LDAP, RADIUS, PKI, SAML a dalších MFA metod. |
| Správa řešení pomocí Rest API | Řešení je možné spravovat pomocí Rest API a to minimálně na úrovni - vytváření uživatelů a účtů, nastavení oprávnění, system health monitoring, schvalování požadavků, autentizace atp. | ANO | Kompletní REST API pro správu uživatelů, účtů, oprávnění, health monitoring i schvalování. |
| Silná autentizace | Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, PKI, certifikát, atp ...). Řešení umožňuje integraci s MFA nástroji třetích stran. | ANO | Podpora RADIUS, PKI, SAML, Kerberos, FIDO2 a dalších MFA řešení třetích stran. |
| Šifrování a zabezpečení dat | Řešení musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. Řešení umožňuje společnostem splnit compliance požadavky pro ZKB, GDPR, PCI-DSS, SOX, HIPAA, atd. | ANO | FIPS 140-3 validace, AES-256, RSA-2048, podpora compliance ZKB, GDPR, PCI-DSS, SOX. |
| **Password Management** | | | |
| Vyhledávání a přidávání privilegovaných účtů | Řešení umožňuje vyhledávat privilegované účty v operačních systémech/LDAP/Active Directory a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Vyhledávání účtů nevyužívá instalaci agentů na koncová zařízení. Systém umožňuje vyhledávání v on-premise i cloud prostředí (např. AWS). | ANO | Discovery skenování AD, LDAP, sítě bez agentů, včetně on-premise i cloud (AWS, Azure). |

| | | | |
|---|---|---|---|
| Řízení hesel a SSH klíčů | Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i uživatelem. Hesla a SSH klíče se vyměňují bezagentsky. Řešení musí podporovat změnu přihlašovacích údajů minimálně pro typy systémů viz. bod "Podpora řízení hesel a bezpečné přístupy pro systémy", zároveň řešení musí umožňovat tzv. customizaci password management modulu pro další systémy zadavatele. | ANO | Řešení podporuje automatickou rotaci hesel a SSH klíčů po ukončení relace (check-out/check-in) i v pravidelných intervalech dle definované politiky. Uživatel může vynutit rotaci manuálně. Změna hesel probíhá bezagentově přes nativní protokoly. |
| Ověřování hesel | Řešení kontroluje v pravidelných intervalech shodu uloženého hesla v systému řízení přístupů a cílovém bodu. V případě neshody vynutí synchronizaci, nebo zašle upozornění správci. | ANO | Pravidelná verifikace hesel s automatickou synchronizací nebo alertingem při neshodě. |
| Řízení servisních účtů | Systém umožňuje vyhledat účty v MS Windows prostředí a jejich návaznost na další služby/aplikace (services, sheduled tasks, IIS pool, COM+ object, ...). Při přidávání účtů na návaznosti upozorňuje, nebo automaticky integruje do systému. Při vynucení změny hesla je heslo propsáno i do návazných služeb. | ANO | Řešení poskytuje kompletní správu privilegovaných účtů s RBAC řízením přístupu. |
| Vyhledání tzv. backdoor účtů a automatický onboarding | Systém umožňuje pravidelné vyhledávání účtů, které nejsou řešením spravovány, ale jsou používány pro přístupy na koncové systémy. Systém takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. Řešení zároveň umožňuje detekci nespravovaných účtů v reálném čase a automatické uložení a vynucení změny hesla. | ANO | Automatická detekce nespravovaných účtů, alerting a automatický onboarding do správy. |
| Customizace Password Management | Řešení musí umožňovat možnost úpravy systému password management, tak aby bylo možné integrovat další systémy zadavatele. Úpravy je možné provádět pomocí nástroje dodávaného výrobcem a případně úpravou konfiguračních souborů. | ANO | Platform Customization Framework pro vytváření vlastních konektorů. |
| | | | |
| Session Management | Nabízené řešení musí obsahovat Privileged Session management minimálně pro RDP a SSH spojení, navázaných z administrátorské stanice. | ANO | Řešení obsahuje integrovaný session management pro RDP, SSH i další protokoly. |

| | | | |
|---|---|---|---|
| Izolace relací | Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. terminal/proxy serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace...např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP a RADIUS). | ANO | Proxy-based přístup bez odhalení hesel, izolace až na úroveň aplikací (MMC, SQL Studio). |
| Izolace SSH relací | Správcovský přístup prostřednictvím SSH protokolu se bude provádět přes SSH Proxy, kde bude uživatel ověřený svými přihlašovacími údaji (je možné spárovat s MS Active Directory) a bude připojený zvoleným privilegovaným účtem na cílový systém bez zadávání hesla a dle bezpečnostní politiky. Pro připojení pomocí SSH Proxy je vyžadována podpora silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí SSH klíče). | ANO | SSH Proxy s AD/LDAP autentizací, RADIUS MFA a transparentním připojením k cílům. |
| Vzdálené připojení pomocí prohlížeče | Vzdálené připojení zajišťuje řešení tak, aby nebylo potřeba dalších licencí třetích stran, např. MS CAL, a tak, aby nebylo potřeba pro tento účel instalovat zvláštní server ať již fyzický, nebo virtuální, za účelem minimalizace nákladů na řešení. V případě potřeby MS CAL licencí, musí být tyto licence součástí nabídky. | ANO | HTML5 webový klient bez nutnosti dalších licencí nebo serverů. |
| Nahrávání relací | Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace permanentních agentů na koncový systém. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat – minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp...) a je dostupné z GUI dodávaného řešení. | ANO | Video nahrávky s indexováním příkazů, aplikací, URL. Přehrávání přímo v GUI bez pluginů. |
| Automatické označení podezřelých aktivit v nahrávkách | Systém poskytuje možnost automaticky vyhodnocovat a reportovat nahrávky relací na základě vybraných spuštěných příkazů a aplikací, tak aby bylo možné vyhledávat potenciálně nebezpečné činnosti. Systém zároveň umožňuje alerting takových událostí, včetně možnosti exportu logů v reálném čase pomocí syslog na SIEM atp. | ANO | Pravidla pro detekci podezřelých aktivit, alerting a real-time export do SIEM. |

| | | | |
|---|---|---|---|
| Pozastavení/terminace relací | Řešení nabízí možnost automatického pozastavení, nebo terminace potenciálně nebezpečných SSH relací. Pravidla pro detekci potenciálně nebezpečných SSH relací je možné plně editovat. | ANO | Automatická terminace SSH relací na základě konfigurovatelných pravidel. |
| Možnost sledování relací v reálném čase | Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci. Sledování "živých" relací je také možné pomocí prohlížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol). | ANO | Live session monitoring s možností terminace, dostupné přes HTTPS v prohlížeči. |
| Kontrola relací | Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu. | ANO | Centrální vyhledávání nahrávek dle data, uživatele, příkazů a dalších metadat. |
| Analýza a detekce potenciálně škodlivého chování | Součástí řešení nebo pomocí integrace na SIEM nebo SOAR, je možnost provádět průběžnou analýzu využívání privilegovaných účtů a následnou detekci potenciálně škodlivého chování – uživatel se připojuje z nestandardní IP, uživatel se připojuje na systémy, na které běžně nemá přístup, uživatel používá privilegovaný přístupy v nestandardní časy, atp ... | ANO | Řešení nabízí integrace se SIEM/SOAR pro korelaci událostí. |
| Detekce a blokování podezřelých aktivit | Součástí řešení nebo pomocí integrace na SIEM nebo SOAR, systém umožňuje detekci podezřelých aktivit chování uživatelů v reálném čase a musí umožňovat automatické vynucení nápravných opatření - alerting, změna přihlašovacích údajů, terminace/pozastavení relací. | ANO | Real-time detekce s automatickou reakcí - alerting, změna hesel, terminace relací. |
| **Bezpečný vzdálený přístup** | | | |
| Okamžité zavedení uživatelů do systému | Řešení umožňuje okamžité zavedení nových uživatelů do systému. Správce řešení dokáže přes webové rozhraní vytvořit uživatele, přiřadit mu oprávnění s jakými privilegovanými účty může disponovat a pro jaké časového období. Řešení následně zašle email novému uživateli a umožní mu bezpečné vzdálené připojení k PAM řešení. | ANO | Řešení umožňuje rychlé zavedení uživatelů s oprávněními a časovým omezením. |
| Vícefaktorová autentizace | Před bezpečným vzdáleným připojením uživatele k řešení PAM je uživatel ověřen pomocí druhého faktoru. | ANO | Vynucení MFA před přístupem k webového portálu. |
| Šifrované spojení | Spojení mezi externím uživatelem a řešením PAM musí být plně šifrované. Není umožněno přímé spojení mezi stanicí uživatele a cílovým systémem – je využit princip bezpečného 'jump' serveru. | ANO | FIPS 140-3 validace, AES-256, RSA-2048, podpora compliance ZKB, GDPR, PCI-DSS, SOX. |

| | | | |
|---|---|---|---|
| Bezagentské řešení | Řešení nevyžaduje instalaci agenta na stanice uživatelů a na cílové systémy. Uživatelům je umožněno bezpečně přistupovat pomocí webového prohlížeče do řešení PAM. | ANO | Bezagentový přístup přes webový prohlížeč pro uživatele i cílové systémy. |
| **Single Sign On** | | | |
| SSO portál | Řešení musí poskytovat zabezpečení přístupu k veřejným webovým aplikacím pomocí SSO portálu. | ANO | Řešení nabízí SSO portál pro bezpečný přístup k webovým aplikacím. |
| Ověření uživatele | Pro autentizaci k SSO portálu se používá jméno+heslo a vynucení vícefaktorového ověření. | ANO | Řešení nabízí SSO autentizaci pomocí SAML nebo OICD protokolu. |
| Podporované integrace - SSO | Systém musí podporovat minimálně následující integrace:<br>- NTLM<br>- Basic auth<br>- SAML<br>- Uživatelské heslo | ANO | Podpora NTLM, Basic auth, SAML i uživatelského hesla. |
| **Audit a reporting** | | | |
| Zobrazení aktivit uživatele | Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty – zobrazení hesla, změny uložených údajů, vytvoření relace. | ANO | Kompletní audit všech akcí - zobrazení hesel, změny, vytvoření relací. |
| Audit administrátorských akcí | Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení. | ANO | Audit trail všech administrátorských akcí s možností exportu reportů. |
| Přístup k reportům | Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele. | ANO | Řešení nabízí RBAC roli určenou pro čtení reportů. |
| Export auditních dat | Systém musí umožňovat export auditních záznamů pro nástroje typu Crystal reports atp. | ANO | Export auditních dat ve formátech kompatibilních s |

| | | | |
|---|---|---|---|
| | | | Crystal Reports a dalšími nástroji. |
| Nezpochybnitelný auditní záznam | Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy. | ANO | Tamper-proof logy s digitálním podpisem pro nezpochybnitelnost. |
| Zabezpečení auditních záznamů | Řešení musí umožňovat nesmazatelnost logů po dobu minimálně 30 dní. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel. | ANO | Šifrované logy s konfigurovatelnou retencí, přístup pouze pro oprávněné uživatele. |
| Monitoring pomocí RestAPI | Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI – integrace s monitoring systémy zadavatele. | ANO | REST API pro monitoring zdraví systému a integraci s monitoring nástroji. |
| **Integrace a Podporované platformy** | | | |
| Podpora systémů zadavatele | Systém musí umožňovat správu privilegovaných účtů pro různé druhy koncových systémů – minimálně v rozsahu viz. bod: "Podpora řízení hesel a bezpečné přístupy pro systémy". Případně možnost konfigurace a vývoje vlastních konektorů pro změnu hesel a vzdálených přístupů. | ANO | Široká podpora platforem s možností vytváření vlastních konektorů. |
| Seznam podporovaných systémů | Výrobce musí poskytovat veřejně dostupný (ideálně URL na veřejnou webovou stránku) seznam integrovaných řešení na úrovni Password Management, Remote Session Management, SIEM, atp. | ANO | Veřejně dostupný seznam integrací na www.beyondtrust.com/docs. |
| Rest API | Nabízený systém musí obsahovat API a mít jej plně zalicencované, jako rozhraní pro automatizaci a integraci třetích stran. Řešení musí umožňit integraci s nástroji typu Vulnerability Management, nebo RPA pro automatické a bezpečné vyzvedávání secrets pomocí API rozhraní. | ANO | Kompletní REST API pro správu uživatelů, účtů, oprávnění, health monitoring i schvalování. |
| MFA - multi factor autentizace | Řešení musí podporovat integraci s nástroji třetích stran pro vynucení multi factor autentizace. Minimálně na úrovní LDAP/S, RADIUS, PKI, RSA, atp. | ANO | Integrace s LDAP/S, RADIUS, PKI, RSA SecurID, Duo a dalšími MFA poskytovateli. |

| | | | |
|---|---|---|---|
| SIEM integrace | Systém musí umožňovat integraci s nástroji SIEM – přenos logovaných auditních záznamů, nejlépe v reálném čase pomocí Syslog. | ANO | Syslog export v reálném čase pro integraci se SIEM systémy. |
| HSM integrace | Systém musí umožňovat integraci s nástroji HSM – uložení šifrovacích klíčů k databázi řešení. | ANO | Podpora HSM pro bezpečné uložení šifrovacích klíčů. |
| **Podpora řízení hesel a bezpečné přístupy pro systémy** | | | |
| Windows 7, 8, 8.1, 10, Windows Server 2008, 2012, 2016, 2019<br>Active Directory,<br>HP iLO, Dell DRAC, IBM<br>Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+<br>VMWare, HyperV, Citrix<br>Red Hat, Suse, Unix, AIX<br>MS SQL, MySQL, PostreSQL, Oracle,<br>Checkpoint, Fortinet, Palo Alto, Symantec<br>Cisco, Juniper, F5, HP,<br>Amazon Web Services, Office 365, Microsoft Azure Application Keys | | ANO | Řešení podporuje řízení hesel pro vyjmenované systémy. |
| **Architektura** | | | |
| Architektura řešení | Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno. | ANO | Hardened appliance s automatickým hardeningem a zabezpečeným úložištěm. |
| Vysoká dostupnost řešení | Řešení musí podporovat nasazení ve vysoké dostupnosti pro zabezpečení High Availability, Disaster Recovery a zálohování tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat. | ANO | HA clustering, DR a geo-redundance s šifrovanými zálohami. |
| Disaster recovery | Disaster recovery a HA proces je plně automatický. | ANO | Automatický DR a HA failover bez manuální intervence. |

| | | | |
|---|---|---|---|
| Souběžná spojení RDP | Systém musí umožňovat velký počet otevřených spojení a to až 8 na jednoho administrátora. Systém musí umožňovat alespoň 120 souběžných RDP spojení v jeden moment. | ANO | Podpora 8+ spojení na administrátora, 120+ souběžných RDP relací. |
| Souběžná spojení SSH | Systém musí umožňovat velký počet otevřených spojení a to až 8 na jednoho administrátora. Systém musí umožňovat alespoň 120 souběžných SSH spojení v jeden moment. | ANO | Podpora 8+ spojení na administrátora, 120+ souběžných SSH relací. |
| Zálohování systému | Řešení musí umožňovat bezpečné zálohování dat systému – zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených postupů, které zajišťují integritu zálohovaných dat. | ANO | Řešení nabízí šifrované zálohy vč. kontroly integrity. |
| **Projektová podpora** | | | |
| Síť certifikovaných partnerů na lokálním trhu | Výrobce garantuje síť certifikovaných partnerů na lokálním trhu, kde je zaručena technická znalost řešení, zkušenosti s implementací a řízením projektů PAM. | ANO | BeyondTrust má v ČR síť certifikovaných partnerů včetně AVENET Distribution s.r.o. s technickou expertízou a zkušenostmi s implementací PAM projektů. |
| Konzultační služby | Výrobce poskytuje vlastní konzultační služby v rámci projektů implementace PAM řešení. V rámci služeb jsou poskytovány konzultace a best practices ohledně zabezpečení privilegovaných účtů, vedení PAM projektů a postupná analýza aktuálního stavu zabezpečení zadavatele. | ANO | BeyondTrust nabízí Professional Services s best practices pro PAM projekty. |
| Implementační služby | Součástí implementačních služeb je popis architektury nabízeného řešení a popis vazeb na jednotlivé komponenty. | ANO | Dokumentace architektury a vazeb na komponenty součástí implementace. |
| Program zabezpečení privilegovaných účtů | Výrobce poskytuje metodologii postupného zabezpečení privilegovaných účtů, včetně osobních konzultací na lokálním trhu. Metodologie popisuje základní témata a rizika svázaná s oblastí privilegovaných přístupů do IT infrastruktury. | ANO | BeyondTrust poskytuje metodologii PAM Maturity Model pro postupné zabezpečení privilegovaných účtů. Konzultace na českém |

| | | | |
|---|---|---|---|
| | | | trhu zajišťují certifikovaní partneři. |
| Discovery tool | Výrobce poskytuje zdarma nástroj na vyhledání privilegovaných účtů v prostředí zadavatele. Zároveň poskytuje vlastní konzultační služby pro vyhodnocení a před-implementační podporu. | ANO | BeyondTrust nabízí Discovery Tool zdarma s konzultační podporou pro vyhodnocení. |
| **Licenční model** | | | |
| Druh licence | Dodávka musí poskytnout licence pro minimálně 10 správců (dostupné veškeré funkce řešení) a pro minimálně 65 uživatelů s možností rozšíření až na nejméně 300 uživatelů s přístupy typu 'externí uživatel' (poskytnutí bezpečného vzdáleného přístupu) s přístupem k definované množině koncových aktiv. Požadujeme možnost definice minimálně 300 koncových aktiv s neomezeným přístupem uživatelů řešení.<br>Součástí licence je i řešení redundance všech komponent a taktéž geo-redundance (alespoň active-passive) s dodatečnou místní redundancí v druhé geolokaci. Množství licencí lze v budoucnu dále rozšiřovat dle aktuálních potřeb.<br>Zadavatel vyžaduje on-premise řešení a neumožňuje nabídnout cloudovou formu licencování. | ANO | Řešení je licencováno on-premise a splňuje požadovaný rozsah: 10 správců, 65-300 uživatelů, 300+ aktiv. Licence zahrnuje HA a geo-redundanci (active-passive). Rozšíření licencí je možné dle potřeb. |
| MS TS CAL licence | Součástí nabízeného řešení jsou i licence MS CAL, pokud je řešení potřebuje k naplnění jakéhokoliv z uvedených bodů v této tabulce. | ANO | MS CAL licence jsou součástí nabídky, pokud jsou požadovány. |
| Podpora řešení | Dodávka musí obsahovat podporu výrobce po celou dobu účinnosti licence, tj. na období min**. 12** měsíců. Technická podpora musí být minimálně v rozsahu 24x7. | ANO | Součástí dodávky je technická podpora výrobce 24x7 po celou dobu účinnosti licence (min. 12 měsíců). |
| **Volitelné moduly** | | | |
| **Detekce a prevence útoků** | | | |
| Detekce útoků na Kerberos zranitelnosti | Řešení umožňuje detekci útoků na úrovni zranitelností Kerberos typu OverPass the Hash, PAC attack a Golden ticket. | ANO | Řešení detekuje Kerberos útoky typu OverPass the Hash, PAC attack a Golden Ticket. |

| | | | |
|---|---|---|---|
| Vynucení nápravy probíhajícího útoku | Řešení musí umožňovat vynucení nápravy na probíhající útoky na zneužití privilegovaných účtů a přihlašovacích údajů v reálném čase (například změna přihlašovacích údajů, zaslání události na SIEM, atp...). | ANO | Řešení umožňuje automatickou reakci na probíhající útoky v reálném čase - změna hesel, zaslání alertu na SIEM, terminace relací. |
| Druh licence | Licence umožňuje zabezpečit současně více doménových řadičů. | ANO | Licence umožňuje zabezpečit více doménových řadičů současně. |
| **Řízení aplikačních účtů** | | | |
| Řízení aplikačních účtů | Řešení poskytuje zabezpečení aplikačních a technických privilegovaných účtů a jejich přihlašovacích údajů. Řešení umožňuje odstranění tzv. hard-coded přihlašovacích údajů ze skriptů, konfiguračních souborů a aplikací. Systém musí umožňovat různé API pro bezpečné vyzvedávání přihlašovacích údajů pro aplikace a skripty. | ANO | Řešení zabezpečuje aplikační a technické účty, umožňuje odstranění hard-coded credentials ze skriptů a konfiguračních souborů. Pro vyzvedávání hesel poskytuje různá API (REST, SDK). |
| Bezpečná autentizace aplikací | Řešení musí umožňovat silnou autentizaci skriptů a aplikací pro vyzvedávání přihlašovacích údajů a to minimálně na úrovni - hostname/IP adresa aplikačního serveru, certifikátu, uživatele pod kterým je aplikace/skript spuštěna, cesty k aplikaci, případně MD5 hash. | ANO | Řešení umožňuje silnou autentizaci aplikací a skriptů na úrovni hostname/IP, certifikátu, uživatele, cesty k aplikaci a hash souboru. |
| Lokální cache | Systém umožňuje poskytování přihlašovacích údajů aplikacím a skriptům pomocí agentského řešení, které obsahuje možnost bezpečné cache. V případě síťového výpadku bude aplikace/skript mít stále k dispozici přihlašovací údaje k privilegovanému účtu. | ANO | Řešení poskytuje agenta s lokální šifrovanou cache pro offline dostupnost přihlašovacích údajů při síťovém výpadku. |

| | | | |
|---|---|---|---|
| Rest API | Pro méně kritické aplikace a skripty systém umožňuje vyzvednutí přihlašovacích údajů pomocí webového volání přes RestAPI. Webový server musí umožňovat vynucení silné autentizace minimálně na úrovni hostname/IP adresa aplikačního serveru a certifikátu. | ANO | Kompletní REST API pro správu uživatelů, účtů, oprávnění, health monitoring i schvalování. |
| Vulnerability Scanners – RPA - Orchestration/Response | Řešení musí umožňovat integraci s nástroji typu Vulnerability Management, nebo RPA pro automatické a bezpečné vyzvedávání secrets pomocí API rozhraní. | ANO | Integrace s Qualys, Tenable a RPA nástroji přes API. |
| Popis SDK | Výrobce musí poskytovat veřejně dostupný (ideálně URL na veřejnou webovou stránku) popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací. Ideálně s konkrétními příklady nasazení. | ANO | Veřejná dokumentace API a SDK na docs.beyondtrust.com s příklady. |
| Druh licence | Licence umožňuje zabezpečit aplikační servery pomocí bezagentského řešení a aplikační servery pomocí agent-based řešení. | ANO | Licence umožňuje zabezpečit aplikační servery bezagentově i pomocí agenta. |
| **Zabezpečení koncových bodů** | | | |
| Řízení privilegií na koncovém bodu | Řešení umožňuje řízení oprávnění uživatelů na koncových systémech (OS platformy Windows, MacOS a UX), tak aby bylo možné granulárně definovat, který příkaz, aplikaci a akci je uživatel schopný spustit a pod jakými oprávněními. | ANO | Řešení poskytují kompletní správu privilegovaných účtů s RBAC řízením přístupu. |
| Schvalování privilegovaných činností | Řešení je schopné vynutit autorizaci (zadání důvodu, schvalování) pro každý úkon, který vyžaduje vyšší oprávnění, jako je spuštění aplikace vyžadující vyšší oprávnění, konfigurace systému, editace systémových nastavení atp. | ANO | Workflow schvalování pro elevaci oprávnění s auditním záznamem. |
| Odstranění práv local administrator | Řešení umožňuje, aby uživatel na koncovém zařízení, ať se jedná o uživatelské pracovní stanice, notebooky nebo servery, mohl pracovat pouze pod standardním neprivilegovaným uživatelským oprávněním. Veškeré požadavky na vyšší oprávnění jsou řízeny podle bezpečnostní politiky. Oprávnění jsou následně povyšována jednorázově pro vybrané aktivity. | ANO | Řešení umožňuje odstranění lokálních admin práv na stanicích a serverech. Uživatelé pracují pod standardním oprávněním, elevace je řízena politikou a udělována jednorázově pro konkrétní aktivity. |

| | | | |
|---|---|---|---|
| Přidělení oprávnění pro vybrané aplikace | Správce řešení může centrálně definovat, jaké aplikace budou spuštěny se standardním oprávněním, a které se budou spouštět s vyšším oprávněním. Díky této funkci je možné umožnit uživatelům bezproblémovou práci se standardními prostředky a zároveň zajistit maximální bezpečnost systému. | ANO | Řešení umožňuje centrálně definovat, které aplikace běží se standardním a které s elevovaným oprávněním. Uživatelé pracují bez omezení při zachování bezpečnosti. |
| Monitoring spuštěných aplikací | Systém dokáže monitorovat spuštěné aplikace na koncových systémech a na základě monitoringu vytvářet politiky, které aplikace následně systém umožní na koncových bodech spustit a které nikoliv. | ANO | Systém dokáže monitorovat spuštěné aplikace na koncových systémech a na základě monitoringu vytvářet politiky, které aplikace následně systém umožní na koncových bodech spustit a které nikoliv. |
| Omezení oprávnění neznámých aplikací | Systém umožňuje spuštění neznámých aplikací na koncových bodech, ale v omezeném režimu (tzn. omezení práv pod kterými je aplikace spuštěna, omezení přístupu ke korporátním datům, omezení přístupu na internet). Umožňuje tedy prevenci škod způsobených neznámým malware, nikoliv závislým na detekci škodlivého kódu, ale omezením přístupů neznámé aplikace. | ANO | Řešení umožňuje spuštění neznámých aplikací v omezeném režimu (sandbox) s limitovanými právy, bez přístupu ke korporátním datům a internetu. Prevence škod bez závislosti na detekci malware. |

Předmětem této veřejné zakázky je prostřednictvím smluvního vztahu zajistit potřebné licence systému BeyondTrust, které umožní zajištění pokračování dříve realizovaných aktivit v oblasti správy privilegovaných účtů (Správa identit PAM).

Jedná se o veřejnou zakázku malého rozsahu. Smlouva se uzavírá na dobu 12 měsíců.

Předmětem VZ je zajištění pokračování dříve realizovaných aktivit za využití systému BeyondTrust v oblasti správy privilegovaných účtů informačního systému celní správy v souladu s příslušnými ustanoveními zákona č. 264/2025 Sb., o kybernetické bezpečnosti a vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, které definují požadavky pro provozovatele a správce prvku kritické informační infrastruktury.

Vzhledem k tomu, že Celní správa ČR je správcem a provozovatelem prvku kritické informační infrastruktury, je povinna zavést požadovaná bezpečnostní opatření, zejména v oblastech řízení provozu a komunikací, ochrany integrity komunikačních sítí, zaznamenávání činností informačního nebo komunikačního systému, jeho uživatelů a administrátorů, správy privilegovaných účtů a bezpečnostního monitoringu ISCS.

**Příloha č. 2**

**Nabídka poskytovatele**

**Příloha č. 3**

**Licenční podmínky (v CZ jazyce) dle podmínek výrobce.**