KUPNÍ SMLOUVA

uzavřená dle ustanovení § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník,
v platném znění (dále jen „občanský zákoník“)

mezi

Město Bučovice
Se sídlem: Jiráskova 502, 68501 Bučovice
Zastoupeno: PhDr. Jiřím Horákem, PhD.
IČ: 00291676
Číslo účtu: [redacted]

(dále jen „**objednatel**“ na straně jedné)

a

Aricoma Systems a.s.
se sídlem: Hornopolní 3322/34, 702 00 Ostrava
zastoupena: Tomáš Jančík ředitelem krajského zastoupení na základě plné moci
IČ: 04308697
DIČ: CZ04308697
Číslo účtu: [redacted]

(dále jen **"dodavatel"** na straně druhé)

objednatel a dodavatel dále též označováni jako „**smluvní strany**"

na základě výsledku výběrového řízení k plnění veřejné zakázky s názvem

„POŘÍZENÍ A INSTALACE PRVKŮ ZVYŠUJÍCÍ KYBERBEZPEČNOST“

I. Základní ustanovení

1. Není-li ve smlouvě stanoveno jinak, práva a povinnosti smluvních stran touto smlouvou neupravená, se řídí příslušnými ustanoveními občanského zákoníku.
2. Smluvní strany prohlašují, že údaje uvedené v záhlaví této smlouvy odpovídají skutečnosti v době uzavření smlouvy. Změny údajů se zavazují bez zbytečného odkladu oznámit druhé straně.

3. Dodavatel prohlašuje, že je odborně způsobilý k zajištění realizace předmětu plnění této smlouvy, zejména dodání předmětu koupě a plnění dalších svých souvisejících povinností, a že k tomu disponuje všemi příslušnými oprávněními vyžadovanými právními předpisy.

   Dodavatel dále potvrzuje, že se detailně seznámil s rozsahem a povahou předmětu plnění, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k dodání předmětu koupě v souladu se smlouvou a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění za dohodnutou smluvní cenu uvedenou v čl. III. odst. 1 této smlouvy.

4. Objednatel prohlašuje, že je plně schopen splnit své závazky z této smlouvy, a to zejména finančně. Dále objednatel prohlašuje, že není v likvidaci ani v úpadku, nebylo a není proti němu zahájeno insolvenční řízení a nemá závazky po splatnosti vůči státu, zejména vůči finančnímu úřadu, zdravotním pojišťovnám a správám sociálního zabezpečení.

5. Tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „POŘÍZENÍ A INSTALACE PRVKŮ ZVYŠUJÍCÍ KYBERBEZPEČNOST“, zadávanou objednatelem jakožto zadavatelem dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

6. Technická specifikace objednatele k veřejné zakázce a technická specifikace z nabídky dodavatele tvoří nedílnou součást této smlouvy.

7. Objednatel předpokládá spolufinancování předmětu smlouvy z fondu Evropské unie prostřednictvím Národního plánu obnovy/Ministerstva vnitra ČR z 41. výzvy – Kybernetická bezpečnost obce v rámci projektu s registračním číslem „CZ.31.2.0/0.0/0.0/23_093/0008822“ a názvem „Bezpečný digitalizovaný úřad města Bučovice“, a dodavatel bere tuto informaci na vědomí.

II. Předmět smlouvy

1. Dodavatel se zavazuje dodat objednateli hardware, software a služby kvantitativně i kvalitativně odpovídající technické dokumentaci a specifikaci dle odst. 3 tohoto článku (dále jen „předmět koupě“), poskytnout mu související služby v rozsahu dle čl. II. odst. 3 této smlouvy a umožnit nabýt objednateli neomezené vlastnické právo k předmětu koupě. Všechny licence na software, dodané v rámci předmětu koupě zahrnují 60 měsíců podporu a aktualizace vývojářem SW a jsou udělené ve prospěch objednatele.

2. Objednatel se zavazuje převzít řádně a včas dodaný předmět koupě a uhradit za něj sjednanou kupní cenu dle čl. III. odst. 1 této smlouvy.

3. Předmětem smlouvy se pro účely této smlouvy rozumí:

   a) pořízení nástrojů pro zajišťování úrovně dostupnosti informací, backup server, zálohovací SW, vytvoření recovery plánu,
   b) pořízení a implementace nástroje pro ověřování identity uživatelů,
   c) pořízení a implementace NAS - Network Attached Storage,
   d) pořízení a implementace nástroje z kategorie Advanced Threat Protection (Ochrana koncových stanic před internetovými útoky (ATP) přinese sjednocenou platformu pro

preventivní ochranu, detekci porušení zabezpečení, automatizované prověřování a reakci na útoky,

e) pořízení a implementace nástroje pro analýzu a monitoring síťového provozu (Systém pro správu bezpečnostních událostí, který obsahuje detekční prvky pro neobvyklé a potenciálně škodlivé události včetně schopnosti automatické reakce na incident) ,
f) pořízení a implementace nástroje pro log management (Nástroj pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele),
g) pořízení a implementace nástroje na perimetrickou ochranu sítě – Firewall,
h) pořízení a implementace ochrany proti výpadku proudu, záložní zdroj napětí – UPS,
i) poskytnutí veškeré potřebné licence k dodanému řešení,
j) provedení zaškolení administrátorů a uživatelů na straně objednatele,
k) provedení zkušebního provozu a akceptačních testů,
l) zpracování a předání veškeré dokumentace dodaného a implementovaného řešení do infrastruktury zadavatele,
m) zajištění projektového vedení po celou dobu realizace plnění.

III. Kupní cena a platební podmínky

1. Celková kupní cena za předmět koupě bez DPH: 4 005 500,00 Kč

   Sazba DPH v 21% a její celková výše 841 155,00 Kč

   Celková kupní cena za předmět koupě včetně DPH: 4 846 655,00 Kč

2. Celková kupní cena za předmět koupě uvedená v odst. 1 tohoto článku je konečná a maximální a může být měněna pouze v souvislosti se změnou sazeb DPH či jiných daňových předpisů majících vliv na cenu předmětu kupní smlouvy. Rozhodným dnem pro změnu kupní ceny z důvodu zákonné změny sazby DPH je den účinnosti takové změny.

3. Sjednaná celková kupní cena za předmět koupě uvedená v odst. 1 tohoto článku v sobě zahrnuje veškeré náklady dodavatele za poskytnutí zejména níže uvedených souvisejících služeb:

   a. doprava předmětu koupě na místo plnění a jeho vybalení,

   b. instalace předmětu koupě, kterou se rozumí jeho usazení v místě plnění, případně jeho sestavení či propojení a dále napojení předmětu koupě na zdroje,

   c. uvedení předmětu koupě do provozu, jeho odzkoušení, ověření správné funkce a seřízení, provedení případných dalších úkonů a činností nezbytných pro to, aby předmět koupě mohl plnit sjednaný či obvyklý účel,

   d. předání dokladů nutných k převzetí a užívání předmětu koupě, tj. např.

      - technické (uživatelské) dokumentace a licenčních oprávnění k předmětu koupě v českém či anglickém jazyce,

      - instrukcí, záručních listů, návodů k obsluze a údržbě předmětu koupě v českém či anglickém jazyce,

4. Kupní cena bude objednatelem uhrazena v českých korunách na základě řádně a oprávněně vystaveného účetního a daňového dokladu (faktury). Lhůta splatnosti faktury se sjednává na 30 dnů ode dne jejího prokazatelného doručení objednateli. V případě prodlení objednatele s úhradou faktury se objednatel zavazuje uhradit dodavateli úrok z prodlení ve výši 0,01 % z příslušné dlužné částky za každý den prodlení.

   a) Řádným vystavením faktury se rozumí vystavení faktury dodavatelem, jež má veškeré náležitosti účetních a daňových dokladů ve smyslu zákona č. 563/1991 Sb., o účetnictví, v platném znění, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. V případě, že faktura nebude vystavena řádně, a dále pokud bude obsahovat věcné či formální nesprávnosti, pokud nebude splňovat zákonné požadavky, a dále pokud nebude obsahovat stanovenou přílohu, je objednatel oprávněn vrátit ji dodavateli k doplnění či opravení, aniž se dostane do prodlení se splatností takových faktur. Lhůta splatnosti začíná běžet znovu dnem doručení náležitě opravené či doplněné faktury objednateli.

   b) Oprávněným vystavením faktury se rozumí vystavení faktury dodavatelem na základě předání a převzetí předmětu koupě dle čl. II. odst. 3 této smlouvy, včetně podpisu akceptačního protokolu oběma smluvními stranami. Řádně vystavené faktury budou doručeny, resp. předány objednateli v den řádného dodání předmětu koupě, a to v listinné podobě.

5. V případě, že faktura nebude vystavena oprávněně, není objednatel povinen ji proplatit.

6. Přílohou faktury musí být akceptační protokol. V případě požadavku objednatele bude přílohou faktury rovněž tabulka, v rámci níž bude celková kupní cena za předmět koupě explicitně rozdělena do položek dle požadavku objednatele.

7. Dodavatel a objednatel se dohodli, že objednatel je oprávněn započíst své pohledávky vzniklé na základě této smlouvy oproti pohledávce dodavatele na zaplacení kupní ceny.

8. Kupní cena bude hrazena bez poskytování záloh.

IV. Předání a převzetí předmětu koupě a jeho instalace

1. Dodavatel je povinen dodat předmět plnění do 120 kalendářních dnů od podpisu smlouvy. Samotné dodávky plnění nebo jeho části budou realizovány vždy po domluvě se zástupcem objednatele v technických záležitostech tak, aby bylo minimalizováno omezení chodu Městského úřadu v Bučovicích. Jednotlivé termíny dodávek plnění budou sjednány výhradně e-mailem před samotnou realizací.

2. Předmět koupě bude dodavatelem řádně dodán, včetně instalace, uvedení do provozu, otestování a odzkoušení, dalších souvisejících služeb uvedených v čl. II. odst. 3 této smlouvy s tím, že celý předmět plnění této smlouvy musí být splněn nejpozději do 120 kalendářních dnů od podpisu této smlouvy.

3. Místem předání a převzetí je Městský úřad Bučovice, Jiráskova 502, 685 01 Bučovice.

4. Při řádném a včasném dodání předmětu koupě a poskytnutí dalších souvisejících služeb dle čl. II. odst. 3 této smlouvy bude smluvními stranami podepsán akceptační protokol. Teprve podpisem písemného akceptačního protokolu oběma smluvními stranami se považuje předmět koupě za řádně dodaný a dodavateli vzniká právo na zaplacení celkové kupní ceny dle čl. III. odst. 1 této smlouvy.

5. Objednatel není povinen převzít předmět koupě s vadami.

V. Záruka za jakost

1. Dodavatel poskytuje objednateli záruku za jakost předmětu koupě, a to po dobu 5 let ode dne předání a převzetí předmětu koupě dle čl. II. této smlouvy. Záruční doba počíná běžet dnem podpisu akceptačního protokolu oběma smluvními stranami.
2. V případě výskytu vady na předmětu koupě v záruční době má objednatel právo a dodavatel povinnost odstranit vadu na vlastní náklady, bezplatně a bezodkladně poté, co obdrží oznámení objednatele o vadě předmětu koupě, a to nejpozději do 3 týdnů ode dne oznámení objednatele o vadě předmětu koupě. Dodavatel je povinen zahájit práce na odstranění vady nejpozději následující pracovní den po dni, kdy mu byla vada objednatelem oznámena. V případě, že odstranění vady vzhledem k jejímu rozsahu nebo technické složitosti není možné provést ve lhůtách dle věty první tohoto odstavce, je dodavatel povinen v této lhůtě objednatele o této skutečnosti písemně informovat, tuto skutečnost řádně odůvodnit a navrhnout konkrétní lhůtu, v níž se zaváže takovou vadu odstranit, lhůta však může činit max. 2 pracovní dny ode dne uplatnění práva z odpovědnosti za vady. Dodavatel je povinen při odstraňování vady postupovat v souladu s nároky objednatele z vad předmětu koupě uplatněnými v oznámení vady.
3. Záruční doba neběží po dobu, po kterou objednatel nemůže užívat předmět koupě pro jeho vady, za které odpovídá dodavatel.
4. Objednatel je oprávněn uplatnit nároky z vad předmětu koupě nejpozději poslední den záruční doby, přičemž za řádně uplatněné se považují i nároky uplatněné objednatelem ve formě doporučeného dopisu či datové zprávy do datové schránky odeslané dodavateli poslední den záruční doby.
5. Dodavatel se zavazuje pro účely odstraňování reklamovaných vad zajistit servis dodávaného předmětu koupě na místě, kde se předmět koupě nachází, a to na vlastní náklady a na vlastní odpovědnost, minimálně po dobu trvání záruční doby.
6. Záruka za jakost se netýká vad prokazatelně způsobených neodbornou manipulací nebo mechanickým poškozením předmětu koupě objednatelem.
7. Záruka za jakost u dodávaného softwaru se vztahuje i na požadavek objednatele na maintenance, tj. přímý support výrobce, a bezplatný nárok na nové verze softwaru (firmwaru, operačních systémů) k předmětu koupě po dobu záruky předmětu koupě.

VI. Smluvní pokuty

1. Za prodlení s termínem řádného dodání předmětu koupě objednateli či poskytnutí souvisejících služeb dle čl. II. této smlouvy zaplatí dodavatel objednateli smluvní pokutu ve výši 0,2 % z celkové kupní ceny za předmět koupě bez DPH dle čl. III. odst. 1 této smlouvy, a to za každý započatý den prodlení se splněním kterékoliv povinnosti.

2. V případě prodlení dodavatele se zahájením odstraňování vad se dodavatel zavazuje uhradit objednateli smluvní pokutu ve výši 0,05 % z celkové kupní ceny za předmět koupě bez DPH za každý i jen započatý den prodlení a za každou jednotlivou vadu.
3. Smluvní pokuta sjednaná dle tohoto článku je splatná do 15 kalendářních dnů ode dne doručení písemného uplatnění práva na smluvní pokutu, a to na účet objednatele nebo na jiný jím písemně určený bankovní účet. Smluvní pokutu je objednatel oprávněn započíst oproti splatným fakturám dodavatele.
4. Uhrazením kterékoliv smluvní pokuty dle této smlouvy není dotčen nárok na náhradu škody. Pro případ, že by byla smluvní pokuta soudem snížena, dohodly se zároveň smluvní strany, že zůstává zachováno právo na náhradu škody ve výši, v jaké škoda převyšuje částku určenou soudem jako přiměřenou.

VII. Účinnost smlouvy, odstoupení

1. Tato smlouva nabývá platnosti okamžikem jejího podpisu posledním účastníkem této smlouvy.
2. Odstoupit od smlouvy lze pouze z důvodů stanovených v této smlouvě nebo zákonem.
3. Objednatel má právo odstoupit od této smlouvy:
   a) neodstraní-li dodavatel vadu předmětu koupě ve lhůtě do 3 týdnů ode dne reklamace – oznámení vzniku vady objednatelem dodavateli nebo oznámí-li dodavatel před jejím uplynutím, že vadu neodstraní;
   b) jestliže bylo proti dodavateli zahájeno insolvenční řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), v platném znění;
   c) jestliže je dodavatel více jak 5 pracovních dnů v prodlení s dodáním předmětu koupě nebo poskytnutím souvisejících služeb;
   d) v případě, že by předmět koupě neměl požadované vlastnosti stanovené dle čl. II. odst. 3 této smlouvy;
   e) v případě, že by předmět koupě byl zatížen právy třetích osob.
4. Odstoupením od smlouvy zanikají všechna práva a povinnosti smluvních stran z této smlouvy. Odstoupení od smlouvy se nedotýká nároku na náhradu škody, nároků na smluvní pokuty, a ty závazky smluvních stran, které dle smlouvy nebo vzhledem ke své povaze mají trvat i nadále nebo u kterých tak stanoví zákon.

VIII. Ustanovení o doručování, kontaktní osoby

1. Smluvní strany se dohodly a dodavatel určil, že osobou oprávněnou jednat za dodavatele ve všech věcech, které se týkají realizace této smlouvy, je: Tomáš Jančík

2. Smluvní strany se dohodly a objednatel určil, že osobou oprávněnou jednat za objednatele ve všech věcech, které se týkají realizace této smlouvy, je: Mgr. Andrea Kovářová.
3. Veškerá korespondence, pokyny, oznámení, odstoupení, žádosti, záznamy a jiné dokumenty vzniklé na základě této smlouvy mezi smluvními stranami nebo v souvislosti s ní budou vyhotoveny v písemné formě v českém jazyce a doručují se buď osobně, doporučenou poštou nebo datovou schránkou k rukám a na doručovací adresy oprávněných osob dle této smlouvy.
4. Má se za to, že došlá zásilka odeslaná s využitím provozovatele poštovních služeb došla třetí pracovní den po odeslání, byla-li však odeslána na adresu v jiném státu, pak patnáctý pracovní den po odeslání.
5. Smluvní strany se dohodly, že pro vzájemnou komunikaci může být používána také elektronická pošta; ve věcech týkajících se změny či ukončení účinnosti této kupní smlouvy je však nutné použít doručení prostřednictvím pošty, datové schránky, příp. osobně.
6. Pokud v době účinnosti této smlouvy dojde ke změně adresy některé ze smluvních stran, resp. jejich zástupců dle odst. 1 a 2 tohoto článku, je dotčená smluvní strana povinna neprodleně písemně oznámit druhé smluvní straně tuto změnu, a to způsobem uvedeným v tomto článku.

IX. Ustanovení o nabytí vlastnického práva

1. Vlastnické právo k předmětu koupě nabývá objednatel podpisem akceptačního protokolu oběma smluvními stranami.
2. Do doby stanovené v čl. IX. odst. 1 této smlouvy nese nebezpečí škody na předmětu koupě dodavatel.

X. Závěrečná ustanovení

1. Veškeré změny či doplnění této smlouvy lze učinit pouze na základě písemné dohody smluvních stran, přičemž za písemnou formu nebude pro tento účel považována výměna e-mailových či jiných elektronických zpráv. Takové dohody musí mít podobu datovaných, číslovaných a oběma smluvními stranami podepsaných dodatků smlouvy.
2. Vztahuje-li se důvod neplatnosti jen na některé ustanovení smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy, obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu smlouvy. Smluvní strany se zavazují, že bezodkladně nahradí neplatné ustanovení této smlouvy jiným platným ustanovením svým obsahem podobným neplatnému ustanovení.
3. Dodavatel je povinen archivovat originální vyhotovení této smlouvy včetně jejích dodatků, originály účetních dokladů a dalších dokladů vztahujících se k realizaci předmětu této smlouvy po dobu 10 let ode dne nabytí účinnosti této smlouvy. Po tuto dobu je dodavatel povinen umožnit osobám oprávněným k výkonu kontroly projektu provést kontrolu dokladů souvisejících s plněním této smlouvy.
4. Dodavatel není oprávněn postoupit jakákoliv práva anebo povinnosti z této smlouvy na třetí osoby bez předchozího písemného souhlasu objednatele.

5. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a s jejím obsahem bez výhrad souhlasí. Smlouva je vyjádřením jejich pravé, skutečné, svobodné a vážné vůle. Na důkaz pravosti a pravdivosti těchto prohlášení připojují oprávnění zástupci smluvních stran své vlastnoruční podpisy.
6. Smlouva se vyhotovuje ve dvou stejnopisech, z nichž každý má platnost originálu a každý z účastníků této smlouvy obdrží po jednom stejnopise.
7. Smluvní strany prohlašují, že před uzavřením této smlouvy řádně splnily všechny hmotněprávní podmínky pro platné uzavření této smlouvy vyplývající z platných právních předpisů, jakož i z jejich platných vnitřních předpisů, a dále prohlašují, že uzavřením této smlouvy nedojde k porušení jakýchkoliv jejich zákonných či smluvních povinností.
8. Dodavatel souhlasí se zveřejněním smlouvy v registru smluv.

V Bučovicích dne 08.10.2025

…… ……..

Objednatel Dodavatel

Příloha 1

TECHNICKÁ SPECIFIKACE

Pořízení a instalace prvků zvyšující kyberbezpečnost

Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
(b) mají plnou záruku od výrobce,
(c) jsou podporovány výrobcem a jsou součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou určeny pro provoz v České republice (EU).

Tyto skutečnosti dodavatel doloží:

a) potvrzením výrobce daného zařízení, nebo
b) čestným prohlášením distributora, nelze-li prohlášení výrobce získat, nebo
c) jiným rovnocenným dokladem (doklady) v případě, že doklady dle předchozích písm. a) a b) není dodavatel z důvodů, které mu nelze přičítat, schopen předložit (takové důvody musí dodavatel doložit).

Zadavatel si vyhrazuje právo na ověření všech dodaných informací od výrobce daného zařízení a zjištění původu výrobků nejpozději při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Dodavatel doloží toto potvrzení dle předchozího odstavce ke všem nabídnutým technologiím v níže uvedeným kapitolám technické specifikace:

1) Nástroj pro zajišťování úrovně dostupnosti informací

- **Backup Server**
- **Zálohovací SW**

2) Systém pro analýzu síťového provozu a bezpečnostní monitoring

3) NAS - Network Attached Storage

4) Nástroj pro ochranu koncových stanic

5) Nástroj pro ověřování identity uživatelů

6) Nástroj pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.

7) Firewall 2 kusy

8) Záložní zdroj napětí - UPS

1) Nástroj pro zajišťování úrovně dostupnosti informací

Backup Server

Položka	Počet ks	Označení výrobku a výrobce
Backup server	**1 ks**	
Minimální požadavky	**Splňuje (ANO / NE)** (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)	**Naplnění požadavku – upřesnění dodavatele (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)**
Provedení max. 2U.	ANO / NE	ANO
Server osazený 1x CPU, s výkonem ve výkonovém testu uvedeným na stránkách https://www.cpubenchmark.net/, minimálně 18.000 bodů v testu pro jednoprocesorové systémy při maximálním TDP procesoru 125 W, s možností doplnění druhého CPU.	ANO / NE (uveďte parametry CPU)	ANO Intel Xeon Silver 4509Y 2.6G, 8C/16T, 16GT/s, 22.5M Cache, Turbo, HT (125W), Benchmark 18749
RAM 64 GB, rovnoměrně obsazené paměťové kanály CPU.	ANO / NE (uveďte typ a počet modulů)	ANO 2ks 32GB RDIMM, 5600MT/s, Dual Rank
LAN min. 2x 10GbE BASE-T	ANO / NE	ANO
LAN min. 2x 1Gbit	ANO / NE	ANO
SSD o min. velikosti 3.84TB (min. 5ks 3.84TB SSD disků) Read Intensive 6Gbps 512 2.5 in Hot-plug AG Drive, 1 DWPD	ANO / NE (uveďte popis nabízených disků)	ANO 5ks 3.84TB SSD SATA Read Intensive 6Gbps 512 2.5in Hot- plug AG Drive, 1 DWPD

Licence serverového OS Windows, verze standard s pokrytím všech jader nabízeného CPU.	ANO / NE	ANO
BOSS card 2 M.2 480GB (RAID 1)	ANO / NE	ANO
Možnost vzdálené správy serveru “Lights-Out Management“ včetně patřičných licencí	ANO / NE	ANO
HW pro instalaci do RACKU včetně kabelového ramene	ANO / NE	ANO
Redundantní Hot-Plug zdroje 2x 700W	ANO / NE	ANO
Záruka a technická podpora: • v délce minimálně 5 let, • reakční doba „Next Business Day Onsite“, • možnost automatického generování chybového hlášení přímo k výrobci hardware (resp. Poskytovateli) – např. automaticky generovaná emailová notifikace, • technická podpora je poskytována výrobcem, resp. autorizovaným partnerem výrobce v českém nebo slovenském jazyce.	ANO / NE	ANO

Zálohovací SW včetně vytvoření recovery plánu

Požadavek	**Splňuje ANO / NE** (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)	**Popis plnění (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)**
Obecné požadavky		
Požadujeme dodání perpetuálních licencí na pokrytí 4 socketů CPU včetně servisní podpory výrobce na dobu 5 let	ANO	
Zálohovací řešení musí podporovat infrastrukturu VMware ve verzích 6.x, 7.x, 8.x a 9.x, včetně VMware Cloud Foundation, VMware Cloud on AWS, VMware cloud on Dell a Azure VMware Solution	ANO	
Řešení musí podporovat hostitele spravované serverem VMware vCenter ve verzích 6.x, 7.x a 8.0 i samostatné ESXi hostitele.	ANO	
Zálohovací řešení musí podporovat Windows Server Hyper- V 2012 až 2025 včetně Server Core, Azure Stack HCI i Microsoft Hyper-V Server	ANO	
Řešení musí podporovat hostitele spravované pomocí Microsoft System Center Virtual Machine Manager 2012 R2 až 2019, klastrové i samostatné hostitele Hyper-V	ANO	
Řešení musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz na těchto hypervizorech	ANO	
Řešení musí podporovat zálohování platformy Red Hat Virtualization 4.4 SP1	ANO	
Řešení musí podporovat zálohování celých zařízení NAS, jednotlivých sdílených složek SMB a NFS a souborových serverů Windows a Linux.	ANO	
Software musí být možné licencovat pomocí trvalé licence i formou časově omezené subscripce.	ANO	

TCO		
Řešení nesmí být závislé na jednom poskytovateli HW, virtualizační, nebo cloudové platformy a to jak pro výpočetní část, tak pro část ukládání dat.	ANO	
Licence musí být přenositelná mezi různými fyzickými, virtuálními a cloudovými chráněnými objekty	ANO	
Všechny součásti řešení musí plně podporovat komunikaci po IPv6	ANO	
Řešení musí mít mechanismy k úspoře objemu úložného prostoru pro ukládání záloh. Jejich využití musí být volitelné a nesmí omezit žádné funkcionality zálohování a obnovy dat.	ANO	
Řešení musí poskytovat jednotnou konzoli pro přehled o zálohách fyzických, virtuálních, cloudových, NAS i Kubernetes prostředí	ANO	
Řešení musí umožnit vytvoření jednoho logického úložiště pro ukládání záloh z neomezeného počtu různorodých diskových úložišť	ANO	
Řešení musí umožňovat ukládání záloh do různých diskových úložišť, souborových systémů, objektových úložišť, nebo deduplikačních diskových zařízení.	ANO	
Řešení musí umožňovat rozšíření logického úložiště o vrstvy pro automatické vytváření sekundární a archivní kopie záloh, zajišťující soulad s pravidlem 3-2-1 ukládání záloh.	ANO	
Řešení musí umožňovat "single pass backup“ s možností vyloučit zpracování jednotlivých souborů a složek. „Jednoprůchodová záloha“ je vyžadována pro všechny druhy obnovení včetně granulárních obnov na úrovni aplikačních položek	ANO	
Řešení musí umožňovat připojování a spouštění jakéhokoli skriptu pro zálohování před nebo po spuštěním zálohovací úlohy, nebo před a po snapshotu VM	ANO	
Řešení musí podporovat technologie klonování datových bloků u souborových systémů pro Windows i Linux pro zajištění dalších úspor konzumované kapacity	ANO	
Řešení musí disponovat technologií pro snadnou migraci a kopírování záloh mezi jednotlivými úložnými zařízeními, při zachování datových úspor	ANO	
Řešení musí umožňovat kopírovat body obnovení a replikovat virtuální počítače do vzdáleného umístění pomocí technologie založené na vestavěné WAN akceleraci	ANO	
Řešení musí být schopen integrace s jinými systémy pomocí zabudovaného rozhraní REST API	ANO	
Řešení musí umožňovat samostatně škálovat výkonově i geograficky výpočetní, úložné i administrativní komponenty	ANO	

Požadavky na RPO		
Řešení musí využívat mechanismus sledování změn bloku. Pro všechny podporované hypervizory musí být implementace CBT certifikována výrobcem hypervizoru; dodavatel doloží v nabídce	ANO	
Výše uvedená funkce musí být konfigurovatelná na úrovni datastore virtualizační platformy	ANO	
Řešení musí mít oficiální podporu pro VMware vSAN certifikovanou společností VMware	ANO	
Řešení musí podporovat NDMP protokol pro zálohování NAS zařízení	ANO	
Řešení musí využívat protokol DD BOOST pokud je Dell EMC Data Domain používán jako záložní úložiště. To musí být podporováno pomocí připojení k síti LAN nebo FC	ANO	
Řešení musí využívat protokol Catalyst (včetně Catalyst Copy) pokud je HPE StoreOnce používán jako záložní úložiště. To musí být podporováno pomocí připojení k síti LAN nebo FC	ANO	
Řešení musí mít replikaci produkčních VM přímo z infrastruktury VMware vSphere, mezi hostiteli ESXi, včetně asynchronní nepřetržité replikace. Řešení musí navíc umožnit jako zdroj replikačních úloh využít soubory záloh	ANO	
Řešení musí umožňovat „seeding“ replik ze stávajícího virtuálního počítače	ANO	
Řešení musí mít stejné funkce replikace pro Hyper-V	ANO	
Řešení musí umožňovat technologii replikace VM v prostředí Vmware založené na VAIO filtru (CDP, Continuous Data Protection).	ANO	
Řešení musí využívat všechny režimy přenosu zálohy podporované hypervizorem (network, hotadd, direct SAN a direct NFS)	ANO	
Řešení musí být schopen vytvořit zálohu „ad-hoc“ pomocí nativní konzole nebo webového klienta vSphere	ANO	
Řešení musí umožňovat paralelní zpracování virtuálních disků a jejich disků, včetně paralelní obnovy virtuálních disků v úplném režimu obnovy VM	ANO	
Požadavky na RTO		
Řešení musí umožňovat okamžitou obnovu více virtuálních strojů současně, přímo ze záložních souborů z libovolného bodu obnovení (vestavěný NFS server). Tato funkce musí být podporována pro prostředí VMware a Hyper-V a musí fungovat bez ohledu na hardware používaný k ukládání záložních souborů VM	ANO	

Uvedená funkce musí umožňovat spuštění zálohy vytvořené z různých platforem (různých virtuálních, fyzických a veřejných cloudových virtuálních strojů)	ANO	
Řešení musí umožňovat online migraci virtuálních počítačů, zpuštěných z úložiště záloh, do produkčního úložiště pomocí funkcí hypervizoru. Řešení musí také poskytovat svou vlastní funkci, která takové schopnosti poskytne.	ANO	
Řešení musí umožňovat prezentaci disků přímo ze záložního souboru do spuštěné VMware VM	ANO	
Řešení musí umožňovat úplné obnovení VM, obnovu souborů VM nebo disků VM	ANO	
Řešení musí umožňovat úplné obnovení VM přímo do Microsoft Azure, Azure Stack, Amazon EC2, Google Cloud Platform	ANO	
Řešení musí umožňovat přímou obnovu ze záloh uložených v S3-kompatibilním objektovém úložišti, bez nutnosti mezikroku a to jak pro obnovi jednotlivých VM, souborů, aplikačních položek, nebo okamžitého spuštění GuestOS, databází, či NAS z úložiště záloh	ANO	
Řešení musí umožňovat vytvářet aplikačně konzistentní snímky VM na úrovni diskových polí s možností granulární obnovy přímo z těchto snímků na úrovni celých VM, jednotlivých souborů, nebo položek aplikací, či okamžitého spuštění VM ze zvoleného snímku.	ANO	
Řešení musí umožňovat okamžitou dostupnost NAS ze zvoleného bodu v čase pro čtení i zápis přímo z úložiště záloh se souběžnou obnovou do původní, nebo nové lokality	ANO	
Řešení musí umožňovat obnovu souborů na strojoperátora nebo přímo do produkční VM bez potřeby agenta nainstalovaného uvnitř VM. Během obnovy bez agentů nesmí existovat žádné omezení na velikost souboru ani omezení počtu souborů	ANO	
Řešení musí umožňovat obnovu souborů přímo do virtuálního počítače pomocí síťového připojení a rozhraní VIX API v prostředích VMware a PowerShell Direct v prostředích Hyper-V	ANO	
Řešení musí podporovat obnovu souborů z Linux LVM a Windows Storage Spaces	ANO	
Řešení musí umožňovat při obnově na úrovni souborů zobrazení změněných souborů od zvoleného bodu obnovy v produkčním prostředí	ANO	
Řešení musí umožňovat rychlou a podrobnou obnovu aplikačních objektů bez použití jakéhokoli agenta nainstalovaného uvnitř virtuálních počítačů	ANO	
Řešení musí podporovat granulární obnovení libovolného objektu a všech atributů tohoto objektu včetně hesla, GPO, AD configuration partition, AD integrovaných záznamů	ANO	

DNS, Microsoft System Objects, informací o certifikátu CA a AD Sites subnet		
Řešení musí podporovat Microsoft Exchange 2013 a novější, granulární obnovení jakéhokoli objektu včetně objektů ve složce „Permanently deleted objects“	ANO	
Řešení musí podporovat granulární obnovení Microsoft SQL 2008 a novějších, včetně databází s možností obnovení v čase (PiT), obnovy na úrovni tabulky, schéma	ANO	
Řešení musí podporovat podrobné obnovení Microsoft Sharepoint Server 2013 a novějších. Možnost obnovit položky, weby, oprávnění	ANO	
Řešení musí podporovat granulární obnovu databází Oracle s obnovou v čase (PiT) a podporou Oracle DataGuard. Toto musí být nabídnuto pro databáze spuštěné v operačních systémech Windows a Linux	ANO	
Řešení musí umožňovat publikování MS SQL a Oracle DB přímo ze záložního souboru na spuštěný databázový server	ANO	
Řešení musí umožňovat okamžitou obnovu databází MS SQL a Oracle v režimu Instant Recovery do libovolného umístění.	ANO	
Řešení musí umožňovat integraci nativního pluginu pro zálohování Oracle RMAN	ANO	
Řešení musí umožňovat integraci nativního pluginu pro zálohování SAP HANA	ANO	
Řešení musí umožňovat integraci nativního pluginu pro zálohování MS SQL	ANO	
Řešení musí umožňovat „reverzní CBT“ a obnovu pomocí Direct SAN	ANO	
Předcházení rizik		
Přístup do řídící konzole musí být chráněný vícefaktorovou autentizací bez nutnosti přístupu k internetu.	ANO	
Řešení musí umožňovat vytváření záloh odolných vůči náhodnému, či úmyslnému smazání, nebo ransomware útokům na komoditním serverovém HW, nebo jakémkoliv S3-kompatibilním objektovém úložišti	ANO	
Řešení musí podporovat gMSA účty pro zajištění aplikačně-konzistentních záloh v GuestOS bez nutnosti ukládání přístupových oprávnění na úrovni administrátora pro daný GuestOS.	ANO	
Řešení nesmí použít centrální databázi pro ukládání jakýchkoli metadat deduplikace. Ztráta databáze nemůže způsobit, že záložní soubory budou nestabilní. Metadata deduplikace musí být uložena v záložních souborech	ANO	

Řešení musí umožňovat pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosi jednotlivých služeb a kontrolou obsahu na kybernetické hrozby pomocí řešení třetích stran.	ANO	
Řešení musí umožnit přiřadit jednotlivým komponentám zálohovací infrastruktury geografické identifikátory	ANO	
Řešení musí disponovat mechanizmem řízení životního cyklu šifrovacích klíčů	ANO	
Řešení musí disponovat nástrojem pro analýzu konfigurace z pohledu bezpečnostních "Best Practices" doporučení.	ANO	
Řešení musí umožňovat v průběhu obnovy dat ověřovat obsah obnovovaných dat na kybernetické hrozby pomocí produktů třetích stran	ANO	
Řešení musí disponovat API pro zpřístupnění obsahu záloh aplikacím třetích stran	ANO	
Řešení musí nabízet šifrování celého síťového provozu mezi všemi komponentami a také šifrování souborů záloh "na cíli" na diskovém, cloudovém nebo páskovém úložišti.	ANO	
Řešení musí nabízet způsoby, jak omezit stres na úložišti zdrojových dat během zálohování tak, aby záloha kontrolovatelným způsobem ovlivňovala latenci produkčního úložiště.	ANO	
Zálohování NAS zařízení musí podporovat přímé ukládání záloh do S3-kompatibilních objektových úložišť s podporou ObjectLock funkce	ANO	
Řešení musí podporovat vytváření sekundárních kopií záloh z S3-kompatibilních objektových úložišť na datové pásky pro zajištění "off-line", či "air-gapped" sady záloh	ANO	
Součástí záloh musí být všechny informace, potřebné pro zajištění obnovy i v případě nedostupnosti původního zálohovacího serveru, nebo databáze s katalogem záloh.	ANO	
Řešení musí nabízet automatickou detekci "orphaned snapshots" a musí provést jejich konsolidaci automaticky bez zásahu uživatele	ANO	
Řešení musí umožňovat automatizovanou dvoustupňovou obnovu virtuálních strojů, což umožňuje vložení vlastních skriptů za účelem změny dat před obnovením do produkčního prostředí.	ANO	

2) Systém pro analýzu síťového provozu a bezpečnostní monitoring

TECHNICKÁ SPECIFIKACE:

Systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.

Nabízená technologie musí být určená pro provoz v ČR. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může zadavatel přímo kontaktovat.

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci Systému dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimální možné, dodavatel může nabídnout charakteristiky (funkce) lepší.

Řešení musí splňovat **VŠECHNY** níže uvedené požadavky:

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno
Systém pro analýzu síťového provozu	
Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.	[redacted]
Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.	**Splňuje**
Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.	**Splňuje**
Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.	**Splňuje**
Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.	**Splňuje**
Aktualizace systému musí být možné provádět uživatelsky v offline režimu.	**Splňuje**
Zpracování a ukládání síťových toků	

Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.	**Splňuje**
Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.	**Splňuje**
Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 3 měsíců složené z SSD nebo NVMe disků.	**Splňuje**
Analýza aplikačních a systémových logů	
Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity.	**Splňuje**
Uživatelské rozhraní	
Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.	**Splňuje**
Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	**Splňuje**
● granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),	**Splňuje**
● granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),	**Splňuje**
● vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,	**Splňuje**
● vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	**Splňuje**
Automatické hlášení (alerty) a reporting	
Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.	**Splňuje**
Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.	**Splňuje**
Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).	**Splňuje**
Je požadováno vytváření automatizovaných reportů v českém jazyce.	**Splňuje**

Integrace systému	
Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně:	**Splňuje**
● syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)	**Splňuje**
● přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní	**Splňuje**
● export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP	**Splňuje**
● integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému – minimálně Microsoft Active Directory	**Splňuje**
● integrace s firewall řešením pro automatické a manuální reakce vyvolané systémem	**Splňuje**
● integrace s nástroji pro řízení přístupu k síti pro automatickou a manuální reakci systému.	**Splňuje**

Požadavky na architekturu nasazení

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno
Obecné požadavky pro nasazení	
Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“.	**Splňuje**
Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.	**Splňuje**
Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.	**Splňuje**
Požadavky pro pokrytí IT prostředí	
Je požadován 1x HW datový kolektor/sensor o celkové propustnosti minimálně 100Mbps pro 200 monitorovaných IP adres s monitorovacím rozhraním 2x1GbE.	**Splňuje**

Požadavky na schopnost detekce bezpečnostních událostí

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno
Monitorování zařízení, segmentů sítě a využívaných síťových služeb	
Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:	**Splňuje**
● změna IP/MAC adresy hosta,	**Splňuje**
● duplicitní IP/MAC adresa,	**Splňuje**

● změna VLAN,	**Splňuje**
● vytvoření nové podsítě,	**Splňuje**
● připojení nového zařízení,	**Splňuje**
● použití nebo vznik nové služby,	**Splňuje**
● nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,	**Splňuje**
● přístup nového zařízení ke službě či zařízení	**Splňuje**
● ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.	**Splňuje**
Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.	**Splňuje**
Samostatné učení behaviorálních aktivit a detekce anomálií	
Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.	**Splňuje**
Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:	**Splňuje**
● odchylku od modelu pro přenos dat, toků a paketů,	**Splňuje**
● odchylku od modelu pro počet komunikačních partnerů,	**Splňuje**
● odchylku od modelu entropie na komunikačních portech,	**Splňuje**
● odchylku od modelu pro počet síťových toků a využitých síťových služeb,	**Splňuje**
● odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).	**Splňuje**
Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.	**Splňuje**
Identifikace neznámých hrozeb a podezřelých chování	
Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:	**Splňuje**
● průzkumné aktivity v síti,	**Splňuje**
● detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,	**Splňuje**
● detekce repetitivních vzorců chování na síti,	**Splňuje**
● detekce botnetů a ovládání kompromitované stanice,	**Splňuje**

● detekce příznaků těžení kryptoměn,	**Splňuje**
● útoky hrubou silou a enumerace dat,	**Splňuje**
● rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.	**Splňuje**
Detekce na základě databáze známých hrozeb	
Systém musí být schopen identifikovat hrozby a reportovat události na základě	**Splňuje**
● detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik,	**Splňuje**
● reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.	**Splňuje**
Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.	**Splňuje**
Uživatel musí být schopen importovat vlastní záznamy.	**Splňuje**
Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.	**Splňuje**
Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).	**Splňuje**
Uživatel musí být schopen prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel. Příklad možné syntaxe detekčního pravidla: *alert tcp $HOME_NET any -> any any (msg:”Command Shell Access”; content:”C:\\Users\\Administrator\\Desktop\\hfs2.3b”;)*	**Splňuje**
Analýza šifrované komunikace	
Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.	**Splňuje**
Asistované učení	
Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:	**Splňuje**
● IP adresa,	**Splňuje**
● MAC adresa,	**Splňuje**
● hostname,	**Splňuje**
● segment sítě / podsíť,	**Splňuje**

● lokalita – ASN, země apod.	**Splňuje**
● směr komunikace – určení klienta, nebo serveru,	**Splňuje**
● detekovaná událost – kategorie, název apod.	**Splňuje**
● použité služby, protokolu, portu,	**Splňuje**
● libovolné kombinaci výše popsaných.	**Splňuje**
Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.	**Splňuje**

Požadavky na zajištění síťové viditelnosti

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno
Vyhledávání, filtrování a vizualizace dat	
Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.	**Splňuje**
Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:	**Splňuje**
● podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,	**Splňuje**
● prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.	**Splňuje**
Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.	**Splňuje**
Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.	**Splňuje**
Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS. Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry.	**Splňuje**
Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.	**Splňuje**
Kontextuální informace	

Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:	**Splňuje**
● jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie	**Splňuje**
● hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu	**Splňuje**
● IP geolokace	**Splňuje**
● IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá	**Splňuje**
● historie použitých MAC adresa a výrobce zařízení	**Splňuje**
● operační systém a jeho historie na zařízení	**Splňuje**
● uživatelem zadané poznámky a informace k zařízení	**Splňuje**
● automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	**Splňuje**
● seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat.	**Splňuje**
● seznam detekovaných bezpečnostních a provozních událostí daného zařízení.	**Splňuje**
Zaznamenávání, ukládání a zpětná analýza plného provozu	
Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.	**Splňuje**
Je požadována schopnost importu vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětná analýza všemi detekčními a analytickými prostředky kolektoru.	**Splňuje**
Je požadována schopnost zobrazení plného obsahu PCAP souboru v prostředí webového rozhraní aplikace a dále pak automatizovaná analýza surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru.	**Splňuje**

Další požadované oblasti využití

Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje/nesplňuje,** vč. vysvětlení, jak je zadání splněno
Monitorování politik kybernetické bezpečnosti	
Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně:	**Splňuje**
● monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase.	**Splňuje**
● detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.	**Splňuje**

Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí:	**Splňuje**
● uživatelem definované podsítě na základě rozsahů IP adres	**Splňuje**
● uživatelsky libovolně definovaných skupin zařízení	**Splňuje**
● automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	**Splňuje**
Management bezpečnostních událostí a incidentů	
Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	**Splňuje**
● spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,	**Splňuje**
● jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,	**Splňuje**
● možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.),	**Splňuje**
● možnost exportování dat do emailu, csv, pdf, syslogu a podobně,	**Splňuje**
● možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.	**Splňuje**
Detekce úniku dat	
Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).	**Splňuje**
Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.	**Splňuje**
V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:	**Splňuje**
● název souboru,	**Splňuje**
● velikost souboru,	**Splňuje**
● HASH souboru.	**Splňuje**
Monitoring výkonu aplikací a sítě	
Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně:	**Splňuje**
● přenosová rychlost sítě,	**Splňuje**
● rychlost odezvy aplikace,	**Splňuje**

● odezva systému z pohledu uživatele.	**Splňuje**
Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:	**Splňuje**
● všechny porty a služby TCP,	**Splňuje**
● pro všechny kombinace služeb a zařízení.	**Splňuje**
Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.	**Splňuje**
Monitoring cloudových služeb	
Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.	**Splňuje**
Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran.	**Splňuje**
Inventarizace sítě a grafická vizualizace topologie	
Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.	**Splňuje**
Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.	**Splňuje**
Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.	**Splňuje**
Systém umožňuje všechny inventarizační informace řadit dle různých parametrů.	**Splňuje**

Implementační služby

Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekováné nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupraci s kompetenními osobami zadavatele. Dodavatel zajistí integraci nástroje s aktuálním log managementem zadavatele, dále pak nastavení aktivních alertů a reportů dle potřeb zadavatele.

Produktová podpora výrobce

Dodavatel musí zajistit:

- softwarovou produktovou podporu řešení v délce 60 měsíců od podepsání akceptačního protokolu po předáním monitorovacího systému.
- záruku na veškerá dodaná HW zařízení minimálně v rozsahu 5 let NBD ode dne akceptace (Next Business Day) On-Site.

Administrátorské školení

V rámci realizace je požadováno administrátorské a uživatelské školení pro zaměstnance zadavatele v rozsahu nezbytném pro kvalifikovanou obsluhu včetně videozáznamu pro zpětné použití, který bude dostupný online na zabezpečeném úložišti dodavatele.

Dále je požadováno opakované proškolení uživatelů jednou ročně v rozsahu minimálně 1MD, včetně revize analýzy bezpečnostních událostí ve všech lokalitách.

3) NAS

Výrobce a model	1 Synology RS2423+ Rack Station 1 Sada ližin Synology, RKS-02 1 Synology Kombinovaný adaptér M.2 SSD a 10GbE E10M20-T1 2 Synology SNV3510/800GB/SSD/M.2 NVMe/5R 4 Synology HAT5310-8T 3.5" SATA HDD 1 Synology NBD HW rpl RS2423+

Parametry	• NAS, rackmount provedení včetně lyžin
	• Čtyřjádrový procesor v architektuře x86 64 bit
	• Systémová paměť 8 GB DDR4 2666 MHz, rozšiřitelná do 32GB
	• Pozice pro diskové jednotky
	  ○ 12 x 3,5" nebo 2,5" SATA HDD/SSD
	• Kompatibilita diskových jednotek
	  ○ 3,5" SATA jednotky pevných disků
	  ○ 2,5" SATA SSD
	• Diskové jednotky vyměnitelné za provozu
	• Min.2x Gigabitový Ethernet port (RJ45)
	• 1x 10GbE Base-T (RJ45)
	• 2x pozice pro M.2 SSD NVMe, Podporovaný rozměr: 22110 / 2280
	• 2x disk SSD M.2 800GB, TWB 1022TB, stejný výrobce jako NAS
	• USB port
	  ○ 2x USB 3.0
	• Disky:
	  ○ 4x8T HDD stejný výrobce jako NAS a určen pro provoz v NAS
	  ○ rozhraní SATA III (6 Gb/s),
	  ○ rychlost 7 200 ot./min.
	• Záruka 5LET NBD

Další informace čiodkazy dodavatele k nabízenému plnění *(nepovinné pole)*	

4) Nástroj pro ochranu koncových stanic

Ochrana koncových stanic a serverů

Specifikace pokročilé ochrany koncových bodů včetně ochrany virtualizačních platforem a EDR.

Zadavatel požaduje zabezpečit komplexně všechny koncové body, včetně fyzických PC s OS Windows, Mac a Linux, virtuálních PC (VDI) s OS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS Windows a Linux s možností rozšíření ochrany pro mobilních zařízení. Požadovaný počet licencí je 100.

Základní požadavky na řešení

Řešení pro komplexní ochranu PC, Linux, Mac, fyzické a virtuální serverové infrastruktury musí být spravováno z jedné webové konzole. Výrobce nesměl získat na av-comparatives (https://www.av-comparatives.org/awards/) za poslední 2 roky ani jednou méně než 3 hvězdy v kategorii „Real World Protection“ u firemních řešení.

Detailní požadavky na správu a funkcionalitu naleznete podle kategorií a funkcí níže.

Následující funkce jsou bezvýhradně nutné k splnění podmínek výběrového řízení:

1. Konzole pro centrální správu řešení:

Požadovaná funkce	Splňuje ANO/NE	Popis, jak je řešeno (volitelné)
Všechny komponenty řešení musejí být v českém jazyce – včetně konzole správy, klientské aplikace a manuálů	ANO	[redacted]
Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí	ANO	
Konzole pro centrální správu je kompletně multi-tenantní	ANO	
Základní vlastnosti		
Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu	ANO	
Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem	ANO	
Možnost zasílat upozornění napojením na Syslog server	ANO	
Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce	ANO	
Úlohy správy bezpečnosti		
Řešení musí umožnit integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.	ANO	
Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery	ANO	
Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity	ANO	

Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy	ANO	
Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy	ANO	
Možnost restartovat serveru nebo desktopu přímo z konzole centrální správy	ANO	
Centralizované místo pro záznam všech úloh	ANO	
Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)	ANO	
Nastavení úrovně bezpečnosti		
Více možností přiřazení pravidel: podle uživatele či skupiny v Active Directory, podle síťové lokality, ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy) či dle OU, ve které se nachází v AD	ANO	
Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulárně dle sekcí a subsekcí nastavení bezpečnostních pravidel	ANO	
Reportování		
Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě	ANO	
Možnost zasílání vygenerovaných reportů e-mailem	ANO	
Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv	ANO	
Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen	ANO	
Karanténa		
Vzdálená obnova či smazání souboru v karanténě	ANO	
Možnost automaticky přidat soubor do výjimky při obnově z karantény	ANO	
Uživatelé		
Více předdefinovaných rolí: Root, administrátor, reportér 1. Root: spravuje komponenty řešení 2. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení 3. Reportér: spravuje a vytváří reporty	ANO	
Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví)	ANO	
Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny	ANO	
Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení	ANO	

Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat	ANO	
Logy		
Zaznamenávání uživatelských akcí	ANO	
Detailní log pro každou akci	ANO	
Komplexní vyhledávání v logách	ANO	
Správa a instalace ochrany		
Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány	ANO	
Instalace může být provedena několika způsoby, alespoň: 1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován 2. Instalace vzdáleně přímo z konzole správy 3. Distribuce instalačního balíčku pomocí GPO či SCCM	ANO	
Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN	ANO	
Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou	ANO	
Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci	ANO	
Konzole správy obsahuje detailní informace o chráněných strojích: mimo jiné název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích	ANO	
Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů	ANO	
Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou	ANO	
Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat	ANO	
Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti	ANO	
Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)	ANO	
Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body	ANO	
Možnost spustit Network discovery z kteréhokoli již instalovaného klienta	ANO	

2. Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):

Požadovaná funkce	Splňuje ANO/NE	Popis, jak je řešeno (volitelné)
Podpora operačních systémů: Windows 10 1507 a vyšší Windows 8.1 Windows 8 Windows 7 Windows 10 IoT Enterprise Windows Embedded 8.1 Industry Windows Embedded 8 Standard Windows Embedded Standard 7 Windows Embedded Compact 7 Windows Embedded POSReady 7 Windows Embedded Enterprise 7 Windows Server 2019 Windows Server 2019 Core Windows Server 2016 Windows Server 2016 Core Windows Server 2012 R2 Windows Server 2012 Windows Small Business Server 2011 Windows Server 2008 R2 Ubuntu 14.04 LTS a vyšší Red Hat Enterprise Linux CentOS 6.0 a vyšší SUSE Linux Enterprise Server 11 SP4 a vyšší OpenSUSELeap 42.x Fedora 25 a vyšší Debian 8.0 a vyšší Oracle Linux 6.3 a vyšší Amazon Linux AMI 2016.09 a vyšší Mac OS X El Capitan (10.11) a vyšší	ANO	
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)	ANO	
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů	ANO	
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru	ANO	
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu	ANO	

Detekce na základě virových definicí (tzn. signatur)	ANO	
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)	ANO	
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)	ANO	
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)	ANO	
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení	ANO	
Detekce 0-day útoků na základě odhalování anomálního chování	ANO	
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení	ANO	
Detekce 0-day bezsouborových útoků	ANO	
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)	ANO	
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností	ANO	
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)	ANO	
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně	ANO	
Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno	ANO	
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky	ANO	
Možnost automatické detonace podezřelých souborů v Sandboxu	ANO	
Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne	ANO	
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu	ANO	
Možnost ručního vložení vzorku do Sandboxu	ANO	
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení	ANO	

Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP	ANO	
Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy	ANO	
Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.	ANO	
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.	ANO	
Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem	ANO	
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku	ANO	
Řešení umožňuje analýzu vektoru útoku	ANO	
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování	ANO	
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)	ANO	
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní	ANO	
Možnost prověřovat http provoz	ANO	
Možnost prověřovat provoz šifrovaný pomocí SSL	ANO	
Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic	ANO	
Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)	ANO	
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů	ANO	
Ochrana proti podvodným a phishingovým webovým stránkám	ANO	
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID	ANO	
Možnost rozšíření o správu patchů aplikací třetích stran	ANO	
Možnost rozšíření o správu šifrování pevných disků	ANO	
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)	ANO	
Firewall		
Možnost blokovat skenování portů	ANO	

Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS	ANO	
Firewall obsahuje systém IDS včetně funkce odhalování neznámých hrozeb	ANO	
Možnost vypnout IDS	ANO	
Možnost nastavit profily známých sítí	ANO	
Možnost blokace Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu	ANO	
Karanténa		
Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě	ANO	
Možnost obnovy souboru do originální či do nově zadané lokality	ANO	
Automatické mazání souborů v karanténě starších než zadaná maximální doba stáří (maximum nesmí být kratší než 30 dní)	ANO	
Kontrola přístupu k internetu		
• Zablokování přístupu na internet pro specifické stanice / skupiny stanic • Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic • Zablokování přístupu k internetu v určený čas • Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (např. násilí, hazard a jiné) • Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén)	ANO	

3. Ochrana virtualizovaných koncových bodů (Windows, Linux)

Požadovaná funkce	Splňuje ANO/NE	Popis, jak je řešeno (volitelné)
Produkt nepotřebuje VMware vShield či NSX, aby poskytl tzn. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale není nutné aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen	ANO	
„Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením	ANO	
„Skenovací“ zařízení musí být možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže	ANO	
Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení	ANO	
Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za	ANO	

předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace)		
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)	ANO	
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů	ANO	
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru	ANO	
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu	ANO	
Detekce na základě virových definicí (tzn. signatur)	ANO	
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)	ANO	
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)	ANO	
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)	ANO	
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení	ANO	
Detekce 0-day útoků na základě odhalování anomálního chování	ANO	
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení	ANO	
Detekce 0-day bezsouborových útoků	ANO	
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)	ANO	
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností	ANO	
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)	ANO	
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně	ANO	
Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno	ANO	
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky	ANO	
Možnost automatické detonace podezřelých souborů v Sandboxu	ANO	

Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne	ANO	
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu	ANO	
Možnost ručního vložení vzorku do Sandboxu	ANO	
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení	ANO	
Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP	ANO	
Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy	ANO	
Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.	ANO	
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.	ANO	
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku	ANO	
Řešení umožňuje analýzu vektoru útoku	ANO	
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování	ANO	
Možnost prověřovat http provoz	ANO	
Možnost prověřovat provoz šifrovaný pomocí SSL	ANO	
Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic	ANO	
Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)	ANO	
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů	ANO	
Ochrana proti podvodným a phishingovým webovým stránkám	ANO	
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID	ANO	
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)	ANO	
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní	ANO	

Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)	ANO	
Podpora 60 měsíců	ANO	
Akceptační podmínky: • Veškeré komponenty systému jsou řádně licencované. Produkt je dostupný jak v rámci standardního licencování, tak prostřednictvím flexibilního měsíčního licenčního modelu, který je vhodný například pro přechodná období při migraci na jiný software. • Bylo dodáno zařízení dle požadované technické specifikace • Všechny komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele. • Byla vytvořena a dodána provozní dokumentace. • Bylo provedeno školení v požadovaném rozsahu	ANO	
Produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky • jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce, • mají plnou záruku od výrobce, • mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce, • obsahují všechny nezbytné licence na používání příslušného softwaru, • jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt • jsou určeny pro provoz v České republice. • Tyto skutečnosti dodavatel doloží potvrzením výrobce nebo oficiálního distributora tohoto zařízení	ANO	

5) Nástroj pro ověřování identity uživatelů

Vyžadujeme použití hardwarových tokenů bez nutnosti vlastnit mobilní zařízení v počtu 90 ks a mobilních tokenů (pro mobilní zařízení) v počtu 5 ks

1	Centralizované ověřování a autorizace uživatelů	ANO
2	Podpora vícefaktorové autentizace (MFA)	ANO
3	Podpora Single Sign-On (SSO)	ANO
4	Možnost bezheslové autentizace (například prostřednictvím FIDO2)	ANO
5	Správa certifikátů (včetně tvorby, importu a správy životního cyklu certifikátů)	ANO
6	Plná podpora a integrace ze strany firewallu	ANO
7	Podpora autentizačních protokolů jako RADIUS, TACACS+, LDAP, SAML, OAuth, OIDC	ANO
8	Podpora autentizace 802.1X pro přístup k síti	ANO
9	Funkce pro adaptivní (kontextově závislou) autentizaci na základě uživatelského chování a okolností přihlášení	ANO
10	Centralizované ověřování prostřednictvím integrovaných či vzdálených identitních úložišť (například Active Directory)	ANO

11	Správa víceuživatelských skupin a zásad přístupu založených na identitě	ANO
12	Podpora více metod autentizace včetně hardwarových a mobilních tokenů, SMS, e-mailových jednorázových hesel a push notifikace	ANO
13	Podpora protokolů SCEP a CMP pro automatizovanou správu certifikátů	ANO
14	Možnost nasazení jako fyzické zařízení, virtuální stroj i cloudové řešení	ANO
15	Podpora systémů pro komplexní správu identit (SCIM) pro automatizaci synchronizace uživatelů	ANO
16	Podpora offline aktivace tokenů pro prostředí bez připojení k internetu	ANO
17	Integrace s bezpečnostními produkty a dalšími aplikacemi pro zajištění jednotné bezpečnosti	ANO
18	Funkce transparentní autentizace uživatelů (Single Sign-On mobilitní agent, AD polling)	ANO
19	Možnost explicitního uživatelského přihlašovacího portálu a integrovaných widgetů pro usnadnění autentizace	ANO
20	Podpora záznamu a sledování autentizačních událostí pro audit a reporting	ANO
21	Podpora vysoké dostupnosti a synchronizace konfigurace v rámci clusteru zařízení	ANO
22	Podpora správy a kontrola přístupu k síti na základě identity a politik	ANO
Další informace či odkazy dodavatele k nabízenému plnění (nepovinné pole)		

6) Dodávka a implementace nástroje pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.

Centrální systém pro sběr, archivaci a správu logů s vysokou dostupností	[redacted]
Systém jako hardwarová appliance s jednotným webovým rozhraním	Splňuje
Podpora zpracování událostí z různých zdrojů logů napříč výrobci	Splňuje
Možnost konfigurace a ovládání bez znalosti kódování	Splňuje

Možnost vytvářet uživatelské parsery pro nepodporovaná zařízení bez úprav konfiguračních souborů	Splňuje
Podpora příjmu a zpracování logů přes definované protokoly: Syslog, RELP, CEF, FEEF, JSON	Splňuje
Možnost sběru strojových dat z databází, minimálně MySQL, Oracle a PostgreSQL	Splňuje
Převod logů do jednotného formátu s automatickou normalizací a zachováním originální zprávy	Splňuje
Automatické přidávání meta informací k událostem a podpora uživatelských parserů	Splňuje
Možnost přetypování a standardizace hodnot v parseru na základní datové typy	Splňuje
Automatické obohacování logů v uživatelských parserech	Splňuje
Real-time ladění uživatelsky definovaných parserů s okamžitým náhledem výsledků	Splňuje
Uchování původní časové značky a vytvoření důvěryhodného časového razítka při přijetí logu	Splňuje
Zabezpečení uložených logů proti mazání nebo úpravě po celou dobu retence	Splňuje
Jednoznačná identifikace každého zpracovaného logu	Splňuje
Filtrace nerelevantních událostí přes grafické rozhraní bez nutnosti kódování	Splňuje
Konsolidace logů na interním úložišti systému	Splňuje
Dynamická vizualizace logů, událostí a strojových dat	Splňuje
Okamžité prohledávání historických dat bez nutnosti importu nebo dekomprese	Splňuje
Zachování integrity logů při krátkodobém přetížení systému (alespoň 10 minut)	Splňuje
Jednotné vyhledávání napříč všemi typy dat a zařízeními	Splňuje
Vytváření uživatelských pohledů a export dat	Splňuje
Lokalizace konfiguračního rozhraní a dokumentace do českého a anglického jazyka	Splňuje
Jednotná správa uživatelských rolí s definicí přístupových práv	Splňuje
All-in-one řešení pro parsování a normalizaci událostí bez potřeby externích aplikací	Splňuje
Ověřování uživatelů přes externí LDAP/AD s možností záložního lokálního ověření	Splňuje

Hardwarová appliance s maximální velikostí 1U a montážním příslušenstvím do racku	Splňuje

Hardwarová appliance s vysokým výpočetním výkonem - 64 GB RAM	Splňuje
Minimální kapacita systému 12 TB	Splňuje
Síťová konektivita 2x1 Gb s dedikovaným management portem 1Gb	Splňuje
Redundantní ventilátory vyměnitelné za provozu	Splňuje
Redundantní napájecí zdroje vyměnitelné za provozu	Splňuje
Integrované řešení pro vzdálenou správu serveru (ekvivalentní technologiím jako HP iLO, Dell iDRAC apod.)	Splňuje
Ochrana dat pomocí RAID5	Splňuje

Distribuce a instalace aktualizací přes webové rozhraní	Splňuje
Trvalá výkonnost systému při zpracování událostí alespoň 2000 událostí za sekundu při zprávách o průměrné délce minimálně 700 bajtů.	Splňuje
Odolnost systému vůči špičkovému zatížení alespoň 4000 událostí za sekundu při zprávách o průměrné délce minimálně 700 bajtů po dobu alespoň 10 minut.	Splňuje
Neomezený příjem událostí bez licenčních omezení	Splňuje
Podpora vysoké dostupnosti a škálovatelnosti v clusteru	Splňuje
Export dat ve formátu pro strojové zpracování bez omezení	Splňuje
Zálohování a obnovení konfigurace celého systému	Splňuje
Důvěryhodné zálohování a obnovení dat na externí systém. Je požadováno jak plánovatelné tak i vyžádané zálohování. Zálohy musí být komprimovány a jejich obnova nesmí být závislé na verzi systému.	Splňuje

Generování upozornění na základě definovaných podmínek	Splňuje
Uživatelsky definovatelný text e-mailového alertu s podporou proměnných	Splňuje
Nastavení alertů a korelací bez nutnosti znalosti programování	Splňuje
Odesílání alertovaných událostí na externí systémy	Splňuje
Použití a přiřazování značek/tagů v alertech	Splňuje

Podpora základních funkcí SIEM a to minimálně v rozsahu detekce, alertování a korelace událostí na základě stanovených limitů.	Splňuje

Nativní získávání logů z Office 365/Microsoft 365 bez vazby na typ licence (plánu)	Splňuje
Sběr logů z prostředí Microsoft s centrální konfigurací logovacích politik	Splňuje
Možnost vyloučení konkrétních Event ID při sběru logů z Microsoft prostředí	Splňuje
Filtrování událostí při sběru logů z Windows	Splňuje
Šifrovaný sběr logů z Windows s podporou certifikátové autentizace	Splňuje

Centrálně řízený sběr událostí na pobočkách s odolností vůči zatížení linek	Splňuje
Automatické navázání spojení s centrálou a šifrování přenosu dat	Splňuje
Komunikace přes definovaný TCP/UDP port s podporou firewall konfigurace a QoS	Splňuje
Dostupnost řešení pro vzdálené pobočky v hardwarové i virtuální podobě	Splňuje

5letá servisní podpora NBD hardwaru s opravou na místě	Splňuje
5letá podpora pro aktualizace systému a technickou pomoc pro SW	Splňuje

7) Firewall 2 kusy

Výrobce a model	[redacted]	**Splňuje Ano**
Provedení	Do racku 1U, včetně montážního kitu	Ano
Porty	min. 10x GE RJ45	Ano
NGFW	Min. základní funkce Next-generation firewall - viz https://en.wikipedia.org/wiki/Next-generation_firewall - firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.	Ano

Počet současných spojení	min. 1,4 miliónu	Ano
Propustnost IPsec VPN	min. 7,1 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 100 klientů	Ano
Propustnost SSL inspekce	min. 1.4 Gbps	Ano
Propustnost firewallu	min. 10 Gbps pro pakety 512 bytů a větší	Ano
Propustnost NGFW	min. 1,5 Gbps	Ano
Propustnost IPS	min. 2.5 Gbps	Ano
Propustnost detekce škodlivého kódu	min. 1.3 Gbps	Ano
Logování	min. 7 dnů historie v zabezpečeném cloud prostředí	Ano
Zabezpečení VPN	Umožňuje dvoufaktorové ověřování pomocí mobilní aplikace	Ano
Virtualizace	min. 5 virtuálních kontextů	Ano
Vysoká dostupnost	Podporují režimy Active/Passive i Active/Active se společnou konfigurací v případě zapojení druhého firewallu , zadavatel požaduje takové licence aby bylo možno provozovat dodávané zařízení v režimu Active/Active	Ano
Dualstack	podpora současného běhu IPv4 a IPv6	Ano
Aplikační kontrola	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S, …)	Ano
Antivir	Integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)	Ano

Kategorizace a blokace provozu	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne	Ano
Antispam	antispamová a antivirová inspekce elektronické pošty	Ano
Sandbox	Možnost integrovaného sandboxu (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba není součástí dodávky)	Ano
Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení	Ano
Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu	Ano
Management a monitoring	HTTP/S, SSH, SNMP, syslog	Ano
Záruka	min. 60 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Doručení náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalvare, antispam, aplikační kontrola)	Ano

8) Záložní zdroj napětí - UPS

Položka	**Počet ks**	**Označení výrobku a výrobce**
Záložní zdroj – UPS	**1 ks**	
Minimální požadavky	**Splňuje (ANO / NE)** (vyplní účastník v rámci své nabídky; nesplnění byť jediného požadavku představuje nesplnění zadávacích podmínek)	**Naplnění požadavku – upřesnění dodavatele (upřesnění povinné pouze o položek, u kterých zadavatel výslovně požaduje uvedení parametrů apod.)**

Provedení Rack mount	ANO	APC Smart-UPS SRT 5000VA RM 230V, SRT5KRMXLI
Topologie online s dvojí konverzí	ANO	
Kapacita min. 5kVA	ANO	
Požadujeme rozšíření externím bateriovým modulem o minimálně 1 sadu baterií 6kVA	ANO	APC Smart-UPS SRT 192V 5kVA and 6kVA RM Battery Pack, SRT192RMBP
Požadujeme PDU RACK mount lištu, ZeroU, 16A, 230V, minimálně 21xC13 a minimálně 3xC19, která má funkci měření spotřeby energie na jednotlivých zásuvkách a umožňuje vzdálené přepínání jednotlivých zásuvek	ANO	Rack PDU 2G, Metered by Outlet with Switching, ZeroU, 16A, 100-240V, (21) C13 & (3) C19, AP8659
K řešení záložního zdroje a jeho příslušenství musí být dodány všechny potřebné napájecí kabely (power cordy)	ANO	
K řešení bude dodán power cord IEC 320 C19 to IEC 320 C20	ANO	Power Cord, C19 to C20, 2.0m
Bezúdržbové baterie	ANO	
Rozsah vstupního napětí pro napájení z rozvodné sítě min. 160 – 275 V	ANO	
SNMP včetně TRAPů, IPv4	ANO	
Zkreslení vstupního napětí méně než 2%	ANO	
Baterie vyměnitelné za chodu	ANO	
Automatické testování kapacity	ANO	
Upozorňování e-mailem	ANO	
Management přes prohlížeč bez nutnosti instalovat klienta	ANO	
Porty: 1x Ethernet, 1x sériová linka	ANO	
Minimálně 5 let podpora výrobcem	ANO	Potřebné rozšíření záruky a podpory pro všechny komponenty se skládá z těchto licencí: 2x Service Pack 1 Year Warranty Extension (for new product purchases) 1x Service Pack 3 Year Warranty Extension (for new product purchases) 3x

		1 Year Warranty Extension for (1) Accessory (Renewal or High Volume) 1x NMC3 for Smart-UPS & 1- Ph Symmetra - 5 Year Secure NMC Subscription 1x NMC3 for 1-Ph rPDU - 5 Year Secure NMC Subscription

Implementační služby

Obecné požadavky

Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:

Zajištění projektového vedení realizace předmětu plnění.

Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení, implementace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.

Provedení školení, Zajištění zkušebního provozu, Provedení akceptačních testů,

Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.

Předání do ostrého provozu,

Dodavatel je dále povinen zahrnout do nabídky i další související potřebné služby nutné pro úspěšnou realizaci díla.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných zadavatelem.

Harmonogram realizace

Dodavatel zajistí projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky.

HARMONOGRAM

Aktivita	Začátek	Termín
Předání místa plnění	D	D
Zahájení projektu – úvodní projektová schůzka - detailní harmonogram včetně návaznosti implementačních prací	D	D+10
Realizace předmětu plnění - implementace kyberbezpečnostních opatření	D+10	D+114
Školení administrátorů	D+114	D+118
Akceptační testy	D+118	D+119
Zahájení ostrého provozu	D+120	-

jednotka = 1 kalendářní den

Dodavatel může dle svého uvážení výše uvedené maximální lhůty zkrátit

Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

Požadavky na školení

Dodavatel zajistí školení pracovníků Zadavatele – administrátorů a uživatelů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin a pracovníkům bude vystaveno osvědčení o školení s uvedením rozsahu školení. Budou provedena tato školení:

Školení administrátorů – minimální rozsah školení je 8 hodin, předpokládá se účast max. 2 účastníků, školení bude probíhat v sídle Zadavatele.

Školení uživatelů – minimální rozsah školení je 6 hodin, předpokládá se účast max. 5 účastníků, školení bude probíhat v sídle Zadavatele.

Náklady na školení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Požadavky na provedení akceptačních testů a přechod do zkušebního (testovacího) provozu

Dodavatel navrhne způsob a provedení akceptačních testů. Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně:

Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků. Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

Prokázání registrace / aktivace podpory hardware a software výrobce, je-li podpora součástí dodávky a její aktivace potřebná

O provedení akceptace a jejím výsledku musí být vyhotoven písemný akceptační protokol. Šablony akceptačních protokolů budou předány zadavatelem při zahájení projektu, pro zapracování dodavatelem do prováděcí dokumentace.

Dodavatel zajistí pro každou komoditu zkušební (testovací) provoz v délce minimálně 14 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 4 hodin od nahlášení požadavku v pracovní den v době od 7h do 17h. Dojezd do 4 hodin od nahlášení požadavku (v rámci pracovní doby) je zásadní pro udržení provozu kritických informačních systémů v potřebném rozsahu při plnění zákonných povinností zadavatele. V případě předávání díla po částech je uchazeč povinen zajistit zkušební (testovací) provoz pro předávané části díla až do doby zahájení plného provozu díla jako celku, při dodržení minimální požadované lhůty pro zkušební provoz.

Požadavky na dokumentaci

Dodavatel zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.

Provozní dokumentace bude vycházet z prováděcí dokumentace, která bude před předáním do provozu aktualizovaná dle skutečného stavu.

Součástí provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejích provádění a další dokumentaci v rozsahu stanoveném v prováděcí dokumentaci.

Dodavatel uvede do nabídky kompletní podmínky pro zajištění provozu dodaných prvků, včetně požadavků na aktualizace software (maintenance).

Zhotovitel dále dodá uživatelskou dokumentaci, která bude obsahovat minimálně základní popis práce s dodaným řešením, dále bude popisovat funkcionality řešení, a to pro potřebu řádné orientace a práce uživatele. Dokumentace musí být zhotovena v českém jazyce. Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

Zhotovitel dále dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat popis správy a údržby dodaného řešení. Dokumentace musí být zhotovena v českém jazyce.

Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

Požadavky na záruky a MAINTENANCE

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **60 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

Dodavatel ve své nabídce uvede ceny záruky takto:

Standardní záruka a standardní podpora běžně poskytovaná výrobcem infrastrukturní technologie na území České republiky = bude součástí pořizovací ceny zařízení (vždy však alespoň 36 měsíců, není-li výrobcem či dodavatelem poskytnuta jako standardní součást nákupu produktu záruka o délce přesahující 36 měsíců, resp. dosahující minimálně 60 měsíců).

V případě, že výrobce nebo dodavatel neposkytuje jako standardní součást nákupu produktu záruku o délce minimálně 60 měsíců, pak se rozdíl mezi jím nabízenou standardní délkou záruky pro daný produkt a zadavatelem požadovanou délkou záruky minimálně 60 měsíců považuje za nadstandardní (prodlouženou) záruku, kterou je dodavatel povinen k dodávanému produktu (včetně aktualizací software/firmware apod.) pro zadavatele zajistit. Hodnotu takto zajištěné nadstandardní (prodloužené) záruky dodavatel vyjádří v příslušné části cenové kalkulace v položce **"Nadstandardní záruky a podpory výrobců"**.

Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

Hlášení záručních závad, řízení a evidence průběhu jejich řešení bude probíhat stejným způsobem a s využitím stejného helpdeskového systému jako u podpory provozu.

Dodavatel nacení i potřebnou MAINTENANCE - (software maintenance) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou maintenance k řádnému provozovaní dodaného řešení. Potřebnou maintenance dodavatel nacení po dobu udržitelnosti projektu 5let. Maintenance bude dle povahy dodaného řešení pokrývat minimálně níže uvedené scénáře:

Korekční údržba: Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.

Adaptivní údržba: Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.

Perfekcionistická údržba: Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.

Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.